排除ACI基于策略的重定向故障

目录

简介
背景信息
基于策略的重定向概述
服务图部署故障排除
1.检查配置步骤和故障
2.检查UI中的Service Graph部署
排除PBR转发故障
1.检查在枝叶节点上部署了VLAN并学习了终端
2.检查预期的流量路径
在哪里实施策略？
3.检查流量是否重定向到服务节点
4.检查在枝叶节点上编程的策略
其他流量示例
1.无SNAT的负载均衡器
流量路径示例
在枝叶节点上编程的策略。
2.流量示例 — 不带SNAT的防火墙和负载均衡器
流量路径示例
在枝叶节点上编程的策略
3.共享服务（VRF间合同）
在枝叶节点上编程的策略

简介

本文档介绍了解基于ACI策略的重定向(PBR)方案并对其进行故障排除的步骤。

背景信息

本文档中的材料摘自Troubleshooting Cisco Application Centric Infrastructure， Second Edition书，特别是**Policy-Based Redirect - Overview、Policy-Based Redirect - Service Graph Deployment、Policy-Based Redirect - Forwarding和Policy-Based Redirect — 其他流量示例**章。

基于策略的重定向概述

本章介绍使用基于策略的重定向(PBR)对非托管模式服务图进行故障排除。

以下是典型的故障排除步骤。本章说明如何验证特定于PBR的步骤2和步骤3。有关步骤1和4，请参阅各章：“交换矩阵内转发”、“外部转发”和“安全策略”。

1. 检查不带PBR服务图的流量是否工作： 获取消费者和提供商端点。消费者和提供商终端可以

通信。
2. 已部署检查服务图： 部署的图形实例没有故障。部署服务节点的VLAN和类ID。获取服务节点终端。
3. 检查转发路径： 检查策略在枝叶节点上编程。捕获服务节点上的流量以确认是否重定向流量。捕获ACI枝叶上的流量以确认流量在PBR之后是否返回到ACI交换矩阵。
4. 检查流量到达消费者和提供商端点，并且终端生成返回流量。

本文档不包括设计或配置选项。有关详情，请参阅Cisco.com上的“ACI PBR白皮书”

在本章中，服务节点和服务枝叶表示以下内容：

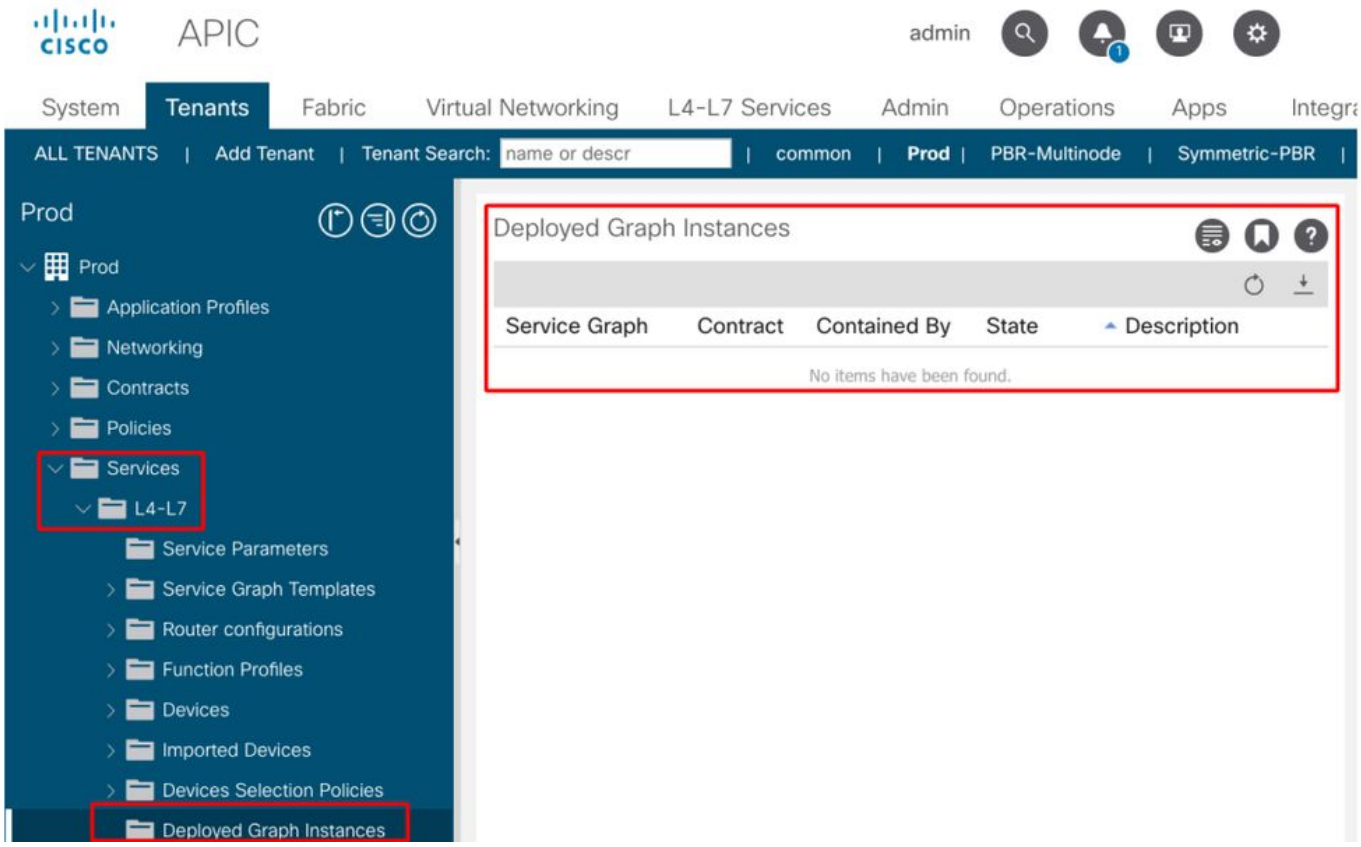
- 服务节点 — PBR将流量重定向到的外部节点，例如防火墙或负载均衡器。
- 服务枝叶 — 连接到服务节点的ACI枝叶。

服务图部署故障排除

本章介绍未部署服务图的故障排除示例。

定义服务图策略并将其应用于合同主题后，ACI GUI中应显示一个已部署的图实例。下图显示了服务图未显示为部署的故障排除场景。

Service Graph不显示为Deployed Graph Instance。



1.检查配置步骤和故障

故障排除的第一步是检查已配置的必要组件没有任何故障。假设以下常规配置已经完成：

- 适用于消费者EPG、提供商EPG和服务节点的VRF和BD

- 消费者和提供商EPG。
- 合同和过滤器。

值得一提的是，服务节点的EPG不需要手动创建。将通过服务图部署创建。

带PBR的服务图配置步骤如下：

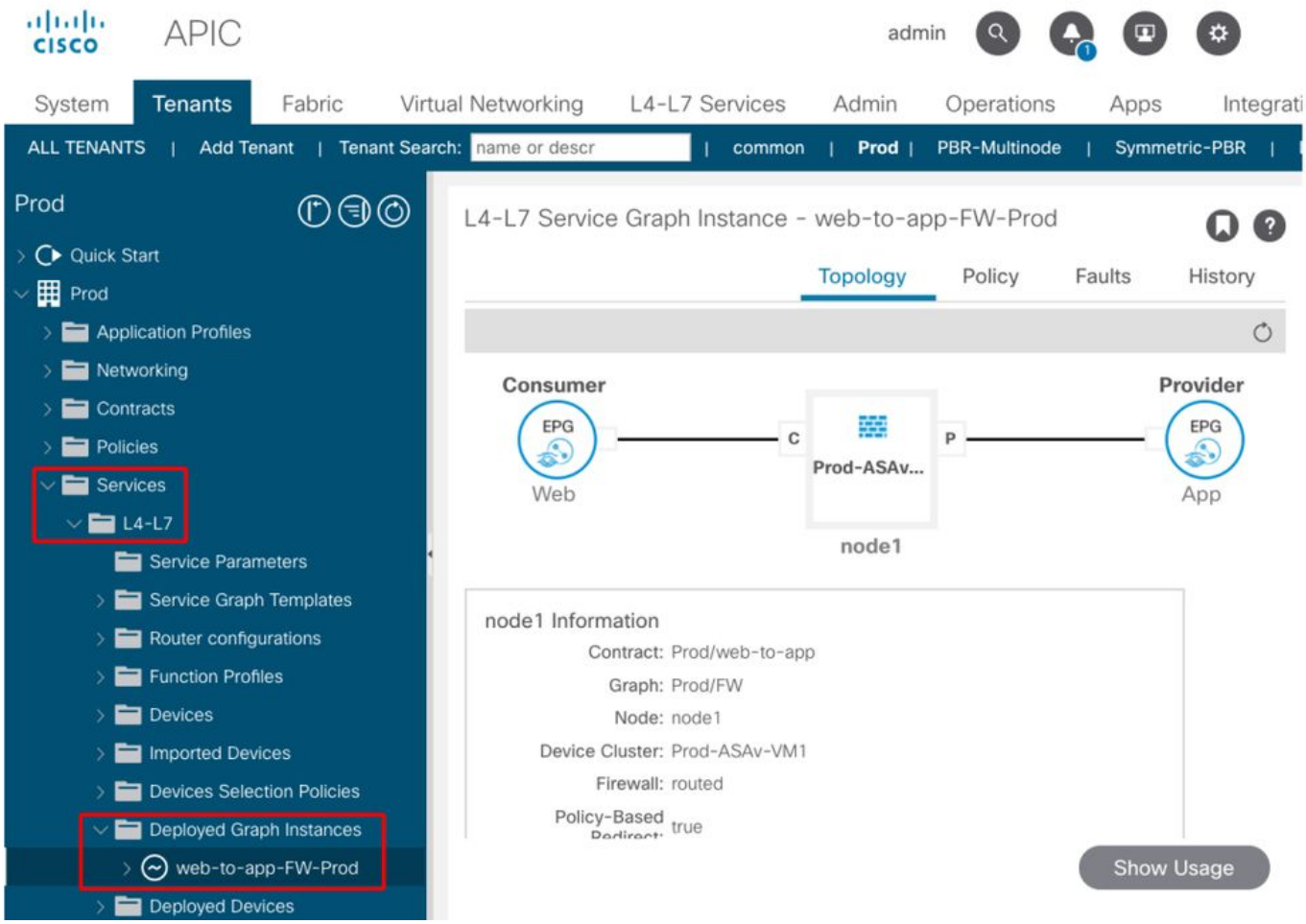
- 创建L4-L7设备（逻辑设备）。
- 创建服务图。
- 创建PBR策略。
- 创建设备选择策略。
- 将服务图与合同主题相关联。

2.检查UI中的Service Graph部署

将Service Graph与合同主题关联后，应为具有Service Graph的每个合同显示一个已部署的图实例（如下图）。

位置为“租户>服务> L4-L7 >部署的图形实例”

部署的图形实例



如果未显示已部署的图形实例，则合同配置存在问题。主要原因包括：

- 合同没有消费者或提供商EPG。
- 合同主题没有任何筛选器。

- 合同范围是VRF，即使它用于VRF间或租户间EPG通信。

如果Service Graph实例化失败，则会在Deployed Graph Instance中引发故障，这意味着Service Graph配置存在问题。由配置引起的典型故障如下：

F1690:由于ID分配失败，配置无效

此故障表示服务节点的封装VLAN不可用。例如，与逻辑设备中使用的VMM域关联的VLAN池中没有可用的动态VLAN。

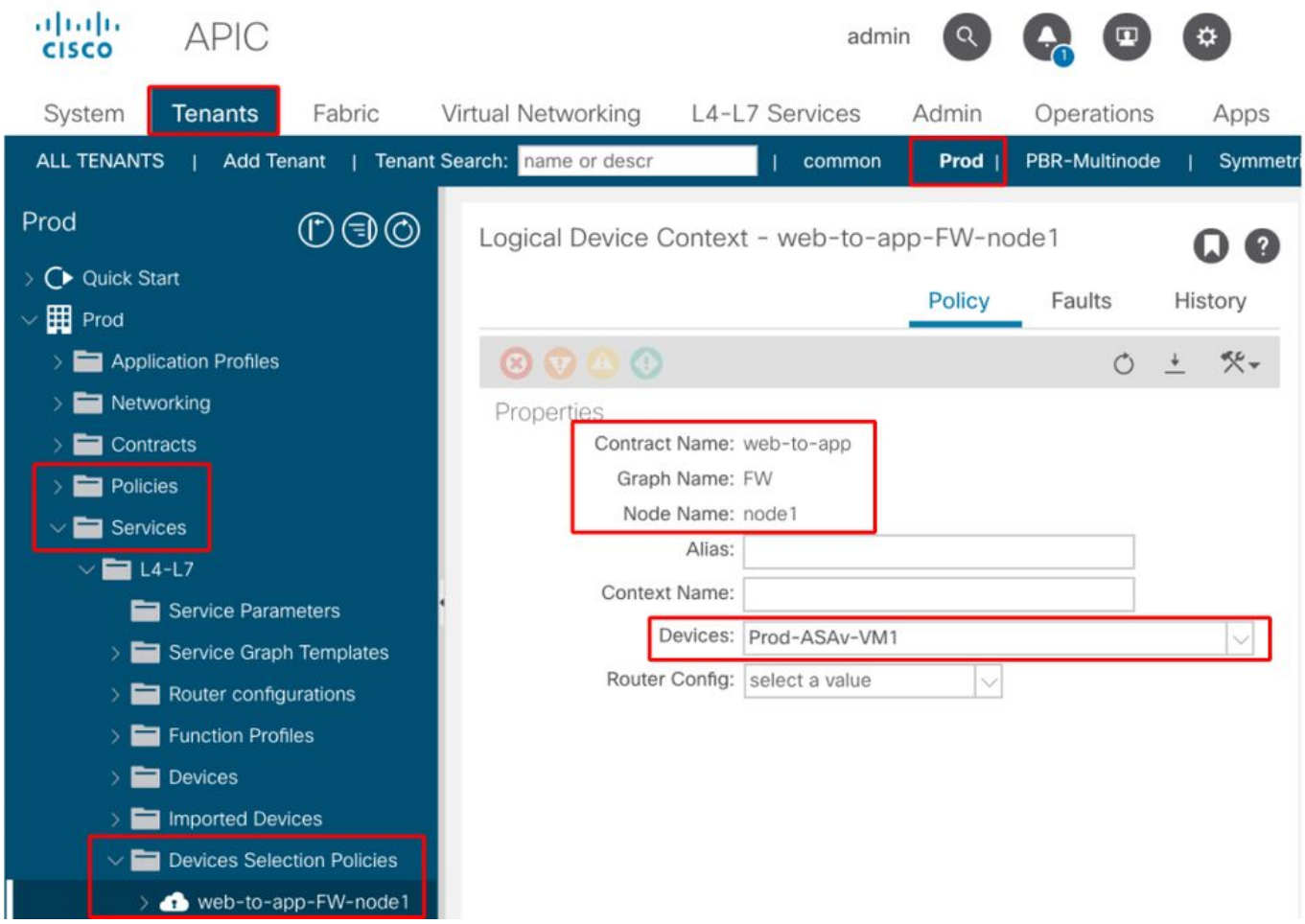
分辨率：检查用于逻辑设备的域中的VLAN池。检查逻辑设备接口中封装的VLAN（如果它在物理域中）。位置为“租户>服务> L4-L7 >设备和交换矩阵>访问策略>池> VLAN”。

F1690:配置无效，因为没有找到LDev的设备上下文

此故障表示找不到服务图呈现的逻辑设备。例如，没有与服务图合同匹配的设备选择策略。

分辨率：检查设备选择策略是否已定义。设备选择策略为服务设备及其连接器提供选择标准。条件基于合同名称、服务图名称和服务图中的节点名称。位置为“租户>服务> L4-L7 >设备选择策略”。

检查设备选择策略



F1690:配置无效，因为没有找到群集接口

此故障表示找不到服务节点的群集接口。例如，未在设备选择策略中指定集群接口。

分辨率：检查集群接口是否在“设备选择”策略中指定，以及连接器名称是否正确（如下图）。

F1690:由于未找到BD，配置无效

此故障表示找不到服务节点的BD。例如，设备选择策略中未指定BD。

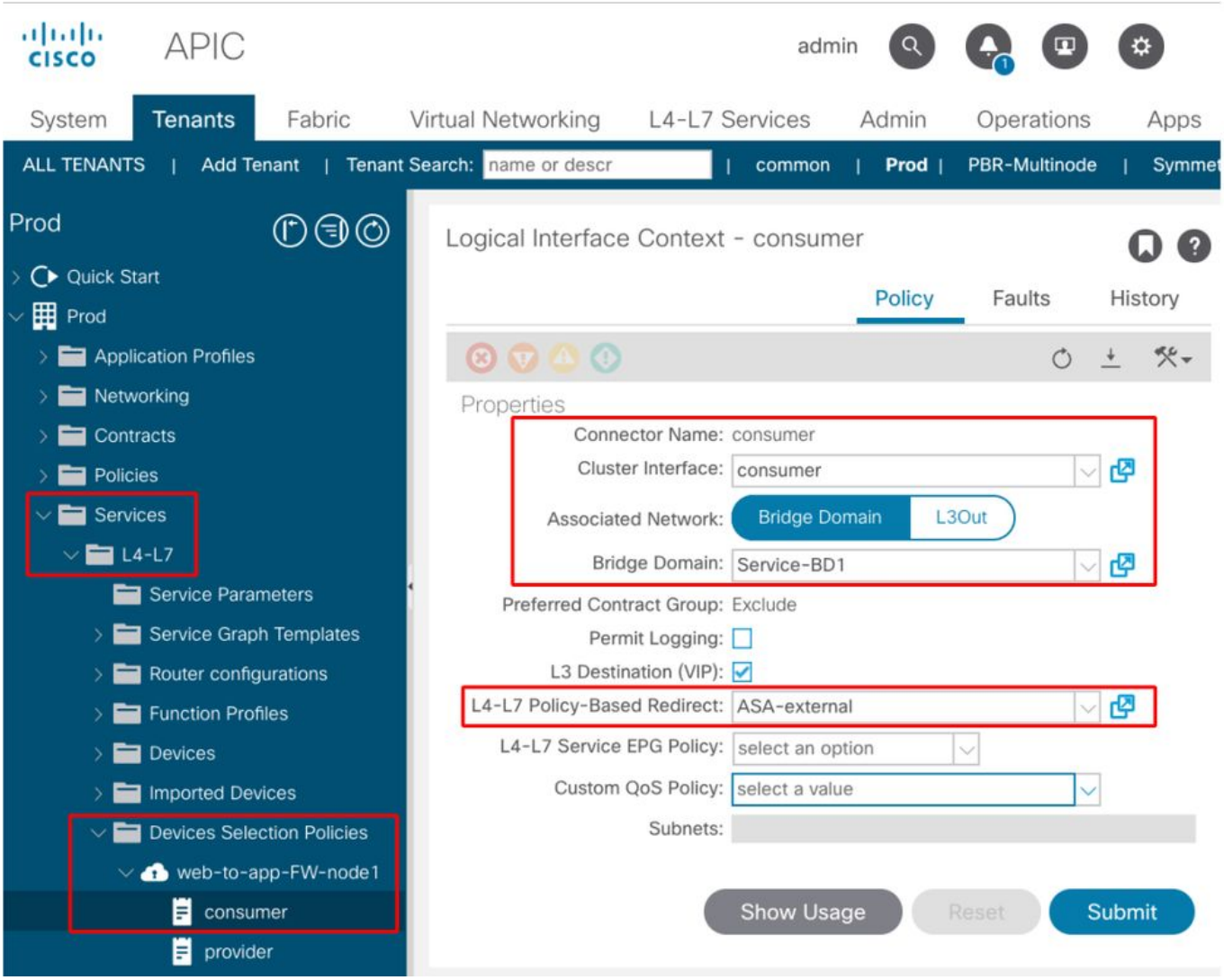
分辨率：检查BD是否在“设备选择”策略中指定，以及连接器名称是否正确（如下图）。

F1690:由于服务重定向策略无效，配置无效

此故障表示未选择PBR策略，即使已在服务图中的服务功能上启用重定向。

分辨率：在设备选择策略（下图）中选择PBR策略。

设备选择策略中的逻辑接口配置



排除PBR转发故障

本章介绍PBR转发路径的故障排除步骤。

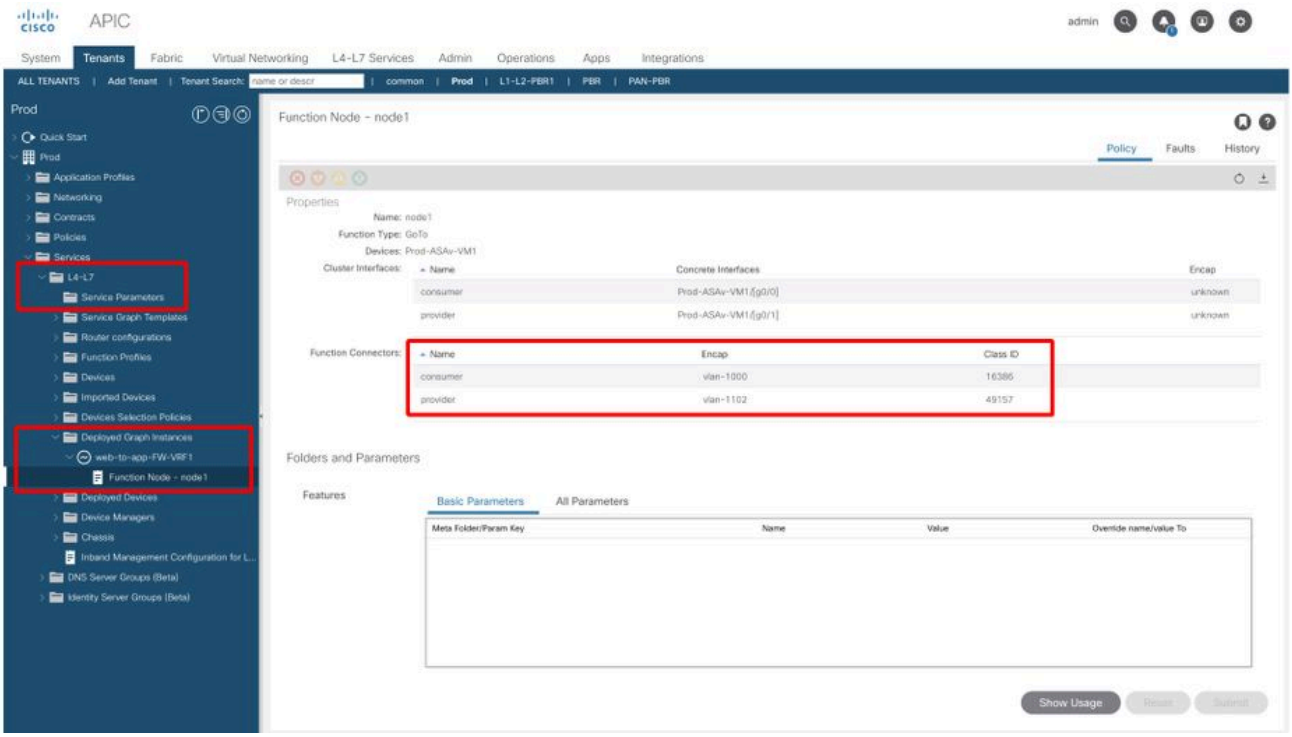
1.检查在枝叶节点上部署了VLAN并学习了终端

成功部署服务图而不出现任何故障后，即会为服务节点创建EPG和BD。下图显示了在何处查找服务节点接口（服务EPG）的封装VLAN ID和类ID。 在本示例中，防火墙的消费者端是具有VLAN封装

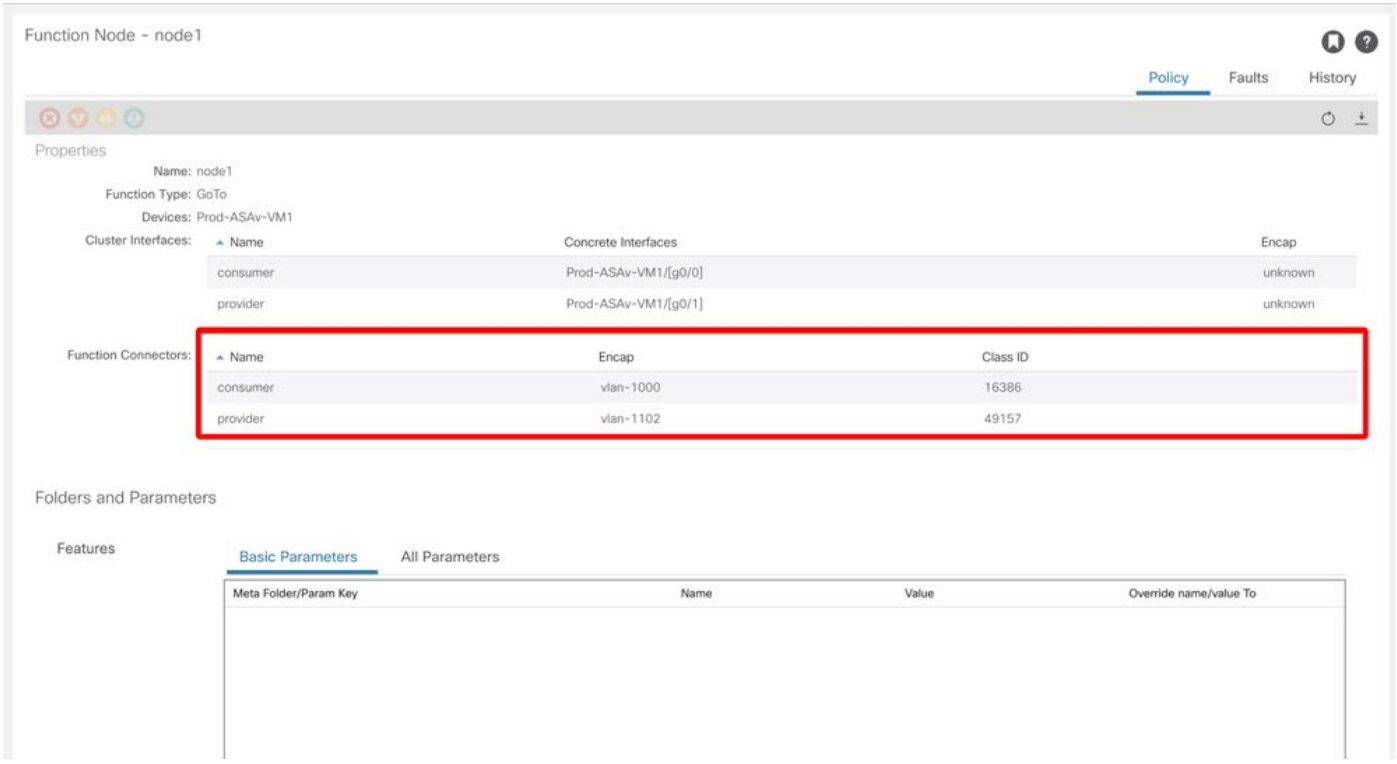
1000的类ID 16386，而防火墙的提供商端是具有VLAN封装1102的类ID 49157。

位置为“Tenant > Services > L4-L7 > Deployed Graph instances > Function Nodes”。

服务节点



服务节点接口类ID



这些VLAN部署在连接服务节点的服务枝叶节点接口上。在服务枝叶节点CLI上使用“show vlan extended”和“show endpoint”可检查VLAN部署和终端学习状态。

```
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
```

如果未将服务节点的终端IP获知为ACI交换矩阵中的终端，则很可能是因为服务枝叶和服务节点之间的连接或配置问题。请检查以下状态：

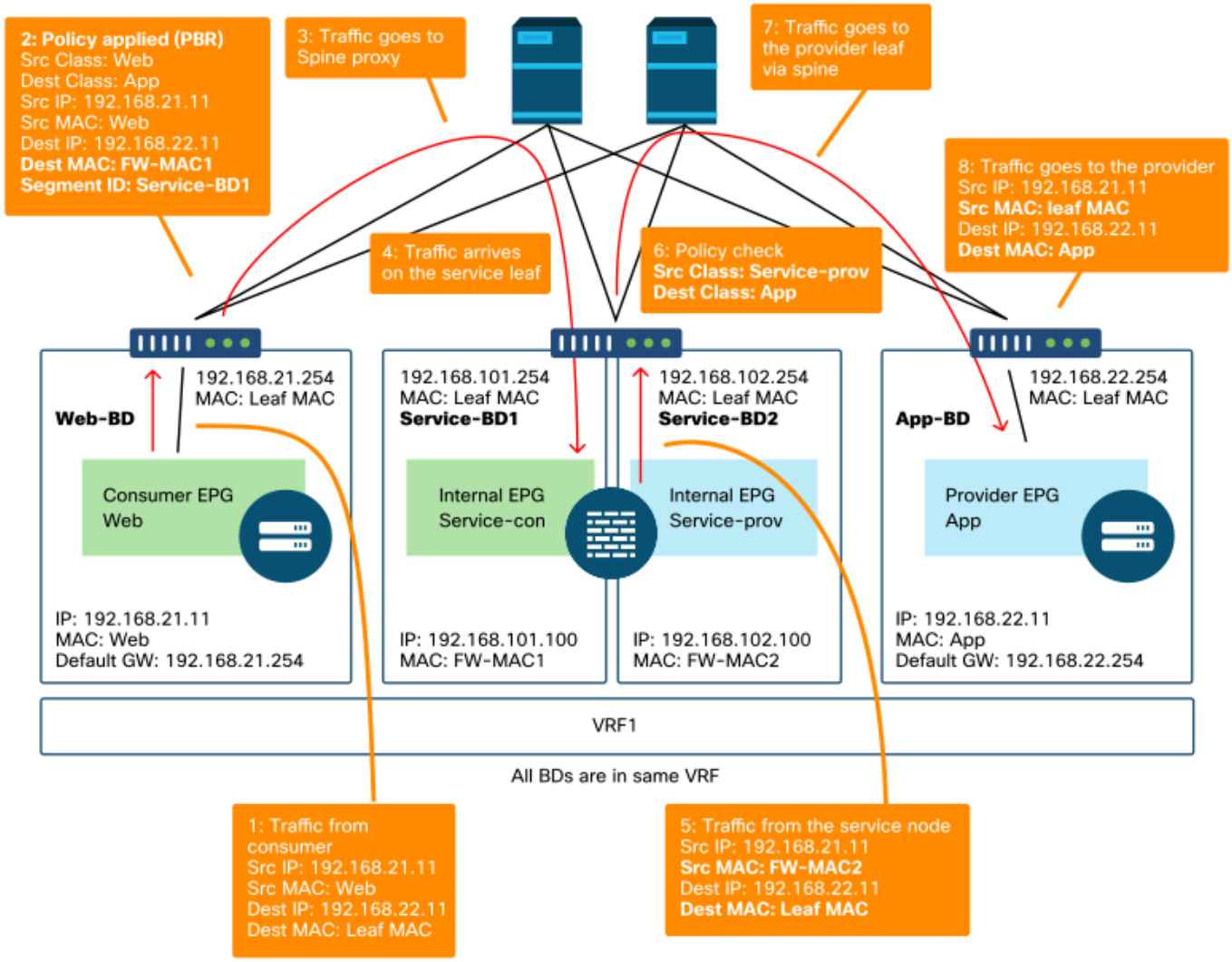
- 服务节点连接到正确的枝叶下行链路端口。 如果服务节点在物理域中，则需要在逻辑设备中定义枝叶静态路径终端封装VLAN。如果服务节点在VMM域中，请检查VMM域是否工作以及通过Service Graph创建的端口组是否已正确连接到服务节点VM。
- 连接到服务节点或服务节点VM所在的虚拟机监控程序的枝叶下行链路端口为UP。
- 服务节点具有正确的VLAN和IP地址。
- 服务枝叶和服务节点之间的中间交换机具有正确的VLAN配置。

2.检查预期的流量路径

启用PBR后，如果端到端流量停止工作，即使在ACI交换矩阵中学习服务节点终端，下一个故障排除步骤是检查预期流量路径。

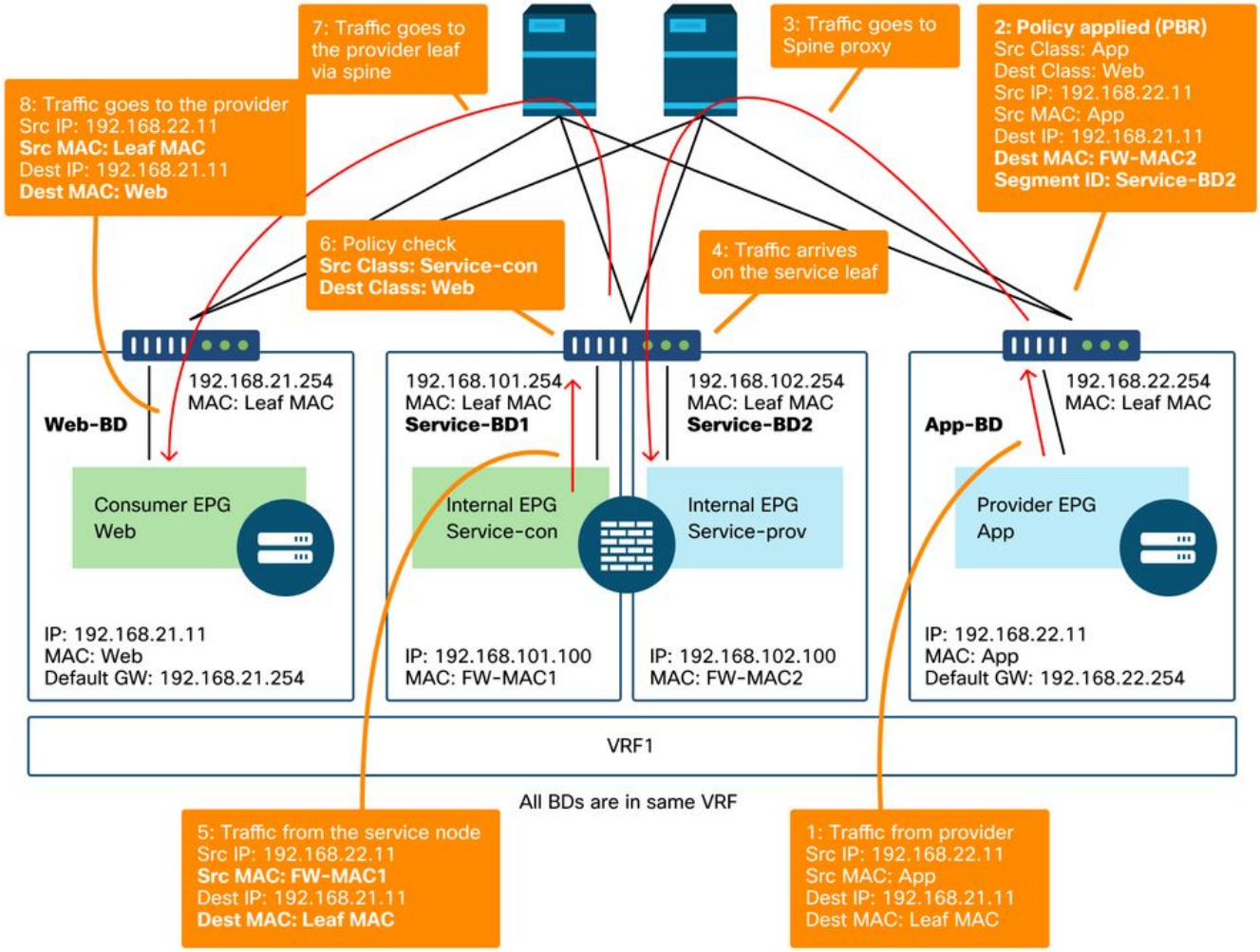
图“PBR转发路径示例 — 消费者到提供商”和“PBR转发路径示例 — 提供商到消费者”说明了在消费者终端和提供商终端之间使用PBR插入防火墙的转发路径示例。假设终端已在枝叶节点上学习。

PBR转发路径示例 — 消费者到提供商



注意：由于源MAC未更改为ACI枝叶MAC，因此，如果使用者终端和PBR节点不在同一BD中，则PBR节点不得使用基于源MAC的转发

PBR转发路径示例 — 提供商到消费者



注意：值得一提的是，PBR策略在消费者或提供商枝叶上实施，ACI PBR所做的就是目标MAC重写，如图“PBR转发路径示例 — 消费者到提供商”和“PBR转发路径示例 — 提供商到消费者”所示。 即使源终端和PBR目标MAC位于同一枝叶下，到达PBR目标MAC始终使用主干代理。

虽然图“PBR转发路径示例 — 使用者到提供商”和“PBR转发路径示例 — 使用者到消费者”显示了流量将被重定向到的示例，其中策略的执行取决于合同配置和终端学习状态。表“策略实施位置”汇总了策略在单个ACI站点实施的位置。在多站点中实施策略的位置不同。

在哪里实施策略？

场景	VRF实施模式	消费者	提供商	策略实施于
VRF内	入口/出口	EPG	EPG	·如果获知目标终端：入口枝叶* ·如果未获知目标终端：出口枝叶
	入口	EPG	L3Out EPG	消费者枝叶（非边界枝叶）
	入口	L3Out EPG	EPG	提供商枝叶（非边界枝叶）
	出口	EPG	L3Out EPG	边界枝叶 — >非边界枝叶流量 ·如果获知目标终端：边界枝叶 ·如果未获知目标终端：非边界枝叶
	出口	L3Out EPG	EPG	非边界枝叶 — >边界枝叶流量 ·边界枝叶
	入口/出口	L3Out	L3Out	入口枝叶*

		EPG EPG	EPG EPG	
	入口/出口	EPG	EPG	消费者枝叶
	入口/出口	EPG	L3Out EPG	消费者枝叶（非边界枝叶）
VRF间	入口/出口	L3Out EPG	EPG	入口枝叶*
	入口/出口	L3Out EPG	L3Out EPG	入口枝叶*

*策略实施应用于数据包命中后的第一个枝叶。

以下是一些示例：

- 如果VRF1中L3Out EPG中的外部终端尝试访问VRF1中Web EPG中的终端，并且VRF1配置为入口实施模式，则无论合同方向如何，流量都由Web EPG中的终端所在的枝叶重定向。
- 如果VRF1中消费者Web EPG中的终端尝试访问VRF1中提供商App EPG中的终端，且终端在消费者和提供商枝叶节点上获知，则流量由入口枝叶重定向。
- 如果VRF1中消费者Web EPG中的终端尝试访问VRF2中提供商App EPG中的终端，则不论VRF实施模式如何，流量都会由消费者终端所在的消费者枝叶重定向。

3.检查流量是否重定向到服务节点

一旦清除预期的转发路径，ELAM可用于检查流量是否到达交换机节点并检查交换机节点的转发决策。有关如何使用ELAM的说明，请参阅“交换矩阵内转发”一章中的“工具”一节。

例如，要跟踪图“PBR转发路径示例 — 消费者到提供商”中的流量，可以捕获这些流量以确认是否重定向了消费者到提供商的流量。

- 消费者枝叶上的下行链路端口，用于检查1和2（流量到达消费者枝叶并实施PBR）。
- 要检查的主干节点上的交换矩阵端口3（流量流向主干代理）。
- 要检查的服务枝叶上的交换矩阵端口4（流量到达服务枝叶）。

然后，可以捕获这些流量以确认从服务节点返回的流量是否流向提供商。

- 服务枝叶上的下行链路端口，用于检查5和6（流量从服务节点返回并被允许）。
- 要检查的主干节点上的交换矩阵端口7（流量通过主干流向提供商枝叶）。
- 提供商枝叶上的交换矩阵端口以检查8（流量到达服务枝叶并转到提供商终端）。

注意：如果消费者和服务节点位于同一枝叶下，则除了源/目标IP外，请指定一个接口或源MAC以使ELAM在图“PBR转发路径示例 — 消费者到提供商”中检查1或5，特别是因为两者使用相同的源IP和目标IP。

如果消费者到提供商的流量被重定向到服务节点，但没有返回服务枝叶，请检查以下项，因为它们是常见错误：

- 服务节点路由表到达提供商子网。
- 服务节点安全策略（例如ACL）允许流量。

如果流量被重定向并到达提供商，请以类似方式检查从提供商到消费者的返回流量路径。

4.检查在枝叶节点上编程的策略

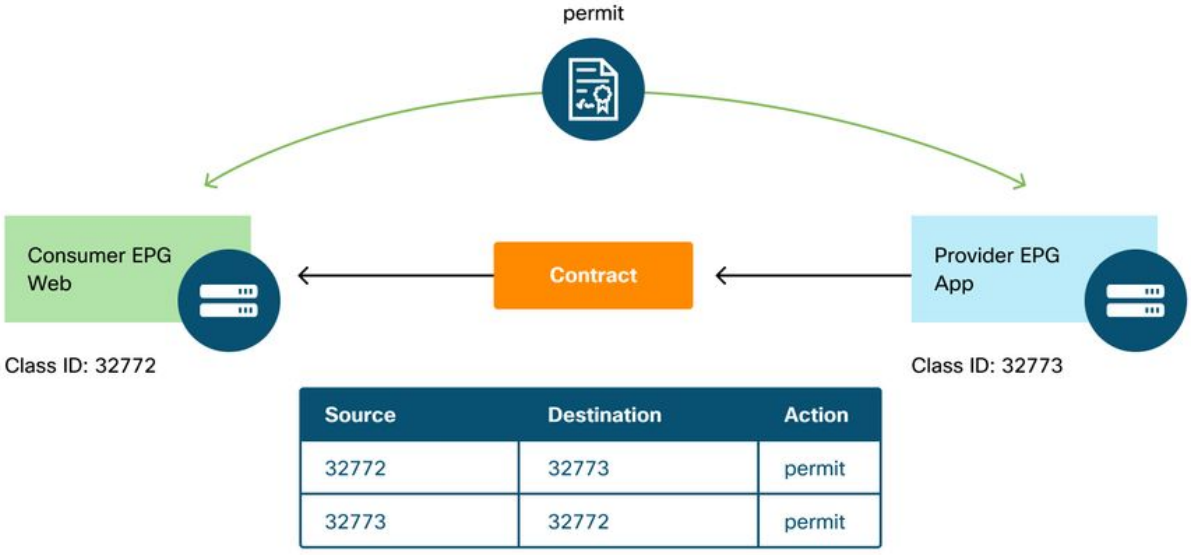
如果没有相应地转发或重定向流量，则下一个故障排除步骤是检查在枝叶节点上编程的策略。本节

以区域划分规则和合同解析器为例。有关如何检查分区规则的更多详细信息，请参阅“安全策略”一章的“工具”一节。

注意：策略根据枝叶上的EPG部署状态进行编程。本部分中的show命令输出使用具有服务节点的消费者EPG、提供商EPG和EPG的枝叶。

使用“show zoning-rule”命令

下图和“show zoning-rule”输出描述了Service Graph部署之前的分区规则。



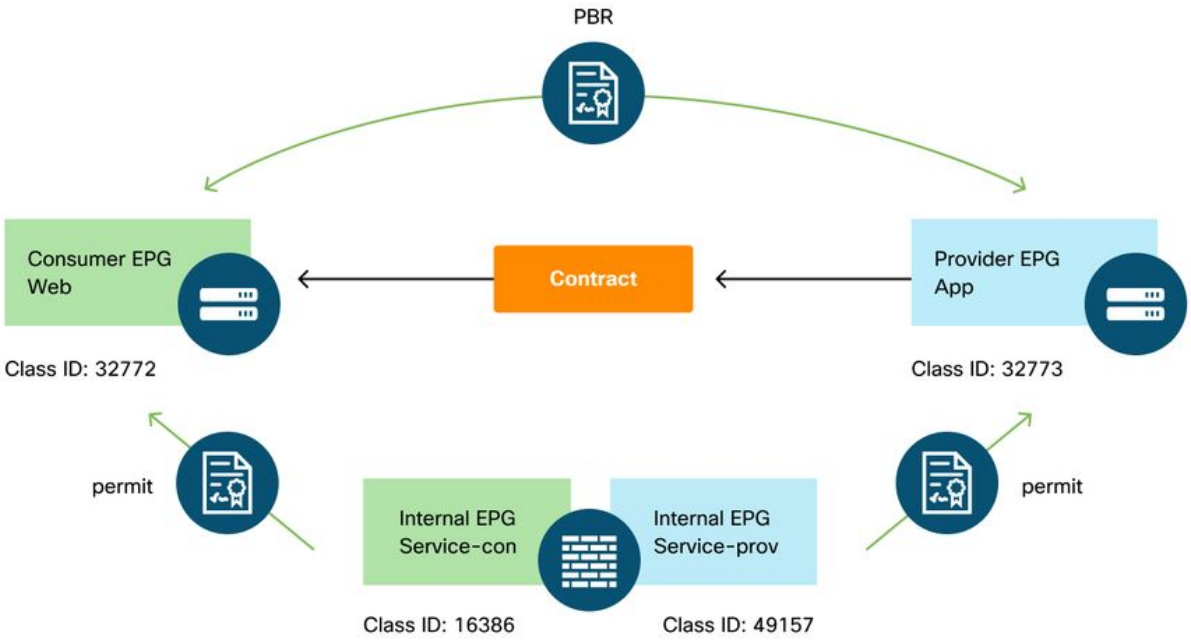
Source	Destination	Action
32772	32773	permit
32773	32772	permit

VRF范围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Service Graph后，将创建服务节点的EPG并更新策略，以重定向消费者和提供商EPG之间的流量。下图和下面的“show zoning-rule”输出描述了服务图部署后的分区规则。在本示例中，从pcTag 32772(Web)到pcTag 32773(App)的流量重定向到“destgrp-27”（服务节点的消费者端），而从pcTag 32773(App)到pcTag 32772(Web)的流量重定向到“destgrp-28”（服务节点的提供商端）。

服务图部署后的分区规则



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”命令可以找到每个目标的目标信息。

```
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
...
```

如果分区规则已相应编程，但流量未相应地重定向或转发，请检查以下错误：

- 检查使用ELAM是否能按预期解析源或目标类ID。如果不是，请检查错误的类ID以及EPG派生条件，如路径和封装VLAN。
- 即使源和目标类ID相应地解析，并且应用PBR策略，但流量未到达PBR节点，请在redir操作(“show service redir info”)中检查destgrp的IP、MAC和VRF是否正确。

默认情况下，如果启用PBR，则不会将消费者EPG的允许规则编程到服务节点（消费者侧）和运营商EPG编程到服务节点（运营商侧）。因此，默认情况下，消费者或提供商终端无法直接与服务节点通信。要允许此流量，需要启用Direct Connect选项。“其他流量示例”一节将介绍该用**例**。

contract_parser的使用

contract_parser工具还可帮助验证策略。C-consumer是服务节点的消费者端，C-provider是服务节点的提供商端。

```
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

本节考虑其他常见流量示例，以确定故障排除所需的流量。有关故障排除步骤，请参阅本节的前一

章。

1. 无SNAT的负载均衡器： 在本示例中，消费者EPG Web和提供商EPG应用与负载均衡器服务图具有合同。应用EPG中的终端是与负载均衡器上的VIP关联的实际服务器。已为提供商到消费者流量方向启用负载均衡器的PBR。
2. 无SNAT的防火墙和负载均衡器： 在本示例中，消费者EPG Web和提供商EPG应用与防火墙和负载均衡器服务图具有合同。应用EPG中的终端是与负载均衡器上的VIP关联的实际服务器。两个方向都启用了PBR到防火墙。已为提供商到消费者流量方向启用负载均衡器的PBR。
3. 共享服务（VRF间合同）： 在本示例中，消费者EPG Web和提供商EPG应用与防火墙服务图具有合同。EPG Web和EPG应用位于不同的VRF中。两个方向都启用了PBR到防火墙。防火墙位于VRF之间。

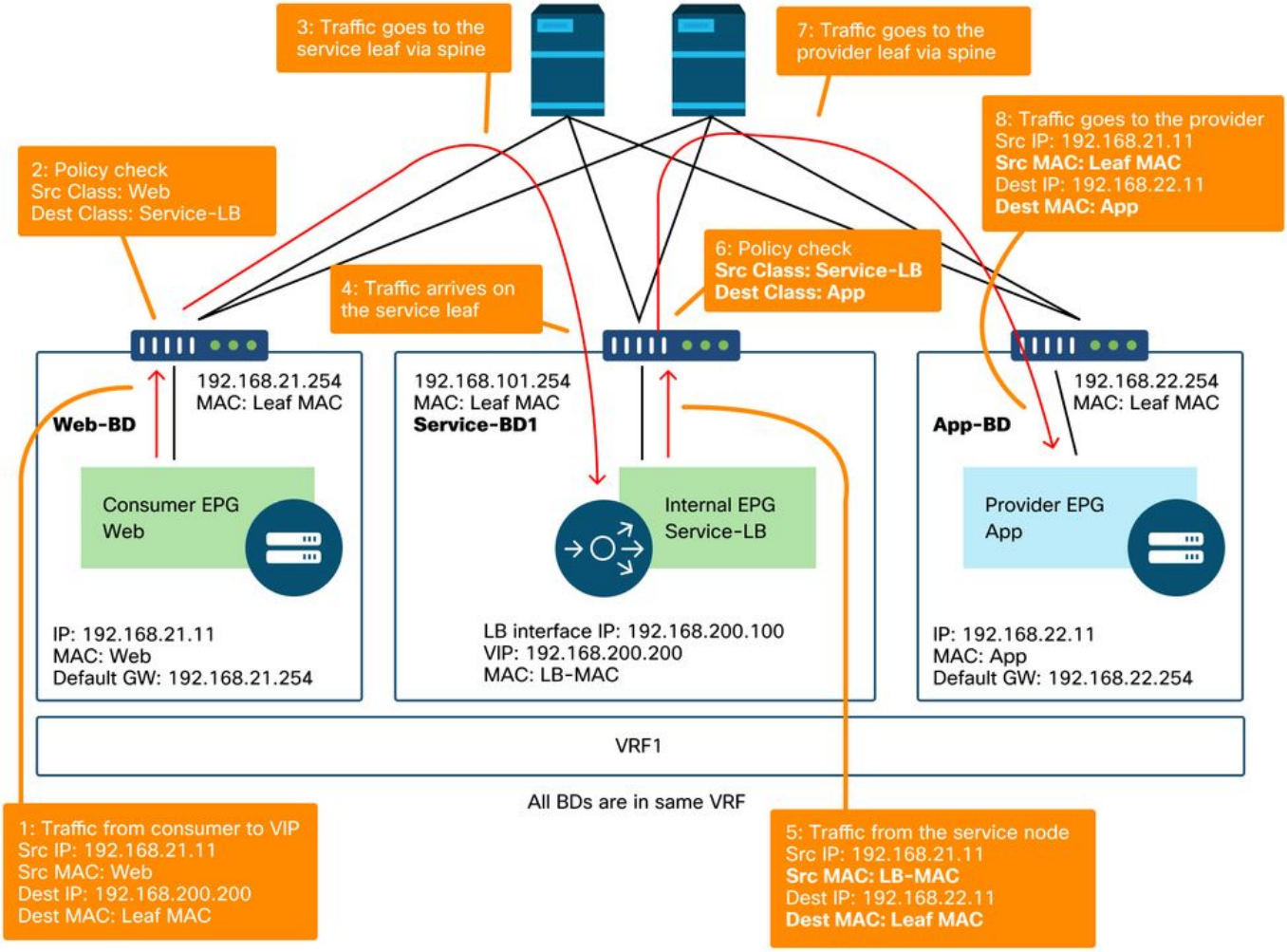
1.无SNAT的负载均衡器

PBR可以部署为双向PBR或单向PBR。单向PBR的一个使用案例是不使用源网络地址转换(NAT)的负载均衡器集成。 如果负载均衡器执行源NAT，则不需要PBR。

流量路径示例

下图显示了从消费者EPG Web到具有两个连接的提供商EPG应用的传入流量的示例：一个是从消费者EPG Web中的终端到负载均衡器VIP，另一个是从负载均衡器到提供商EPG应用中的终端。由于传入流量是发往VIP的，因此，如果VIP可访问，流量将到达负载均衡器，而没有PBR。负载均衡器将目标IP更改为与VIP关联的EPG应用中的一个终端，但不转换源IP。因此，流量将转至提供商终端。

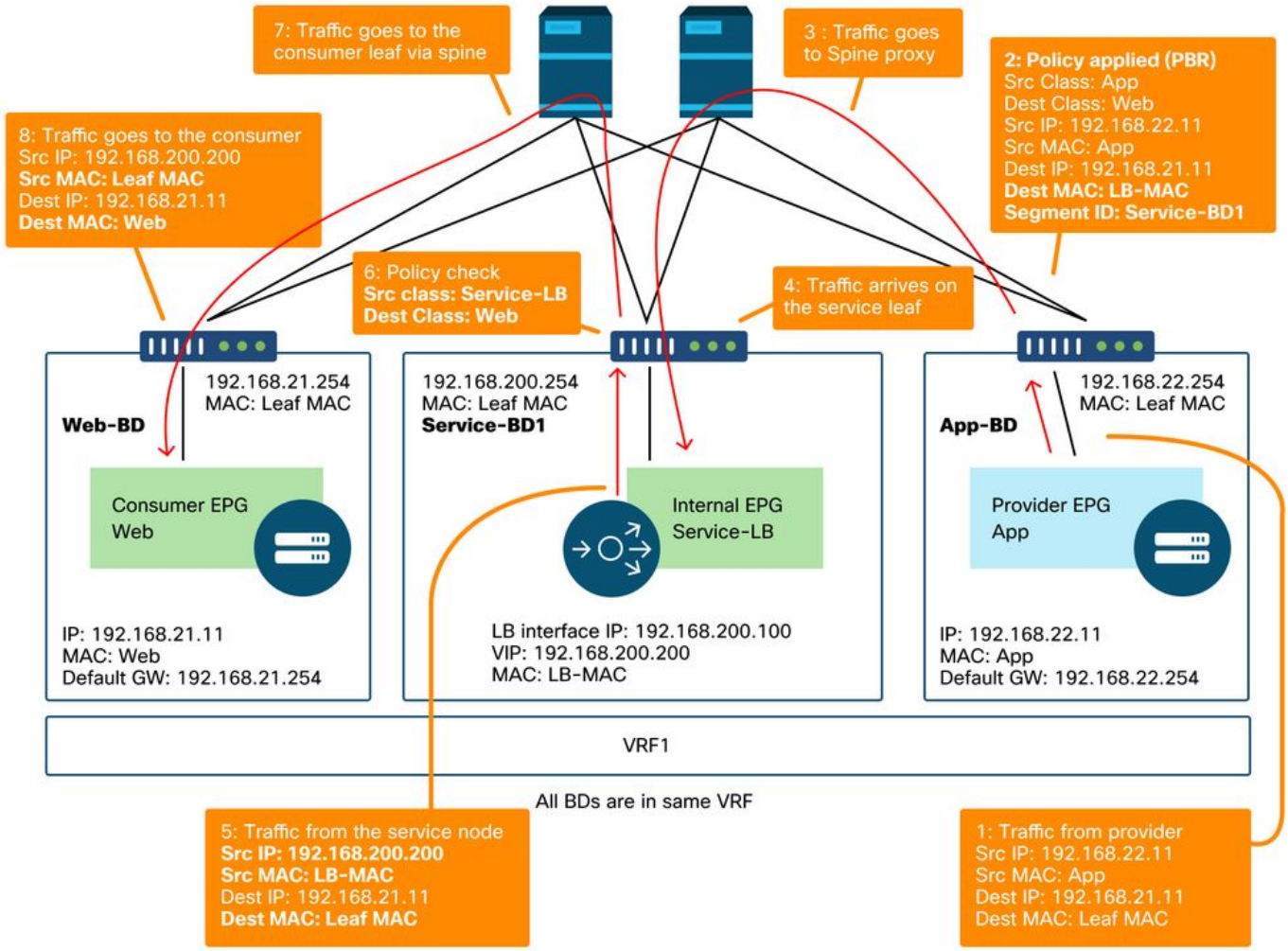
无SNAT的负载均衡器转发路径示例 — 消费者到VIP以及负载均衡器到无PBR的提供商



下图显示了从提供商EPG应用到消费者EPG网络的返回流量。由于返回流量发往原始源IP，因此PBR需要使返回流量返回负载均衡器。否则，消费者终端接收源IP为提供商终端而非VIP的流量。此类流量将被丢弃，因为即使中间网络（例如ACI交换矩阵）将数据包转发回消费者终端，消费者终端也不会向提供商终端发起流量。

从提供商终端到消费者终端的流量重定向到负载均衡器后，负载均衡器会将源IP更改为VIP。然后，流量从负载均衡器返回，流量返回消费者终端。

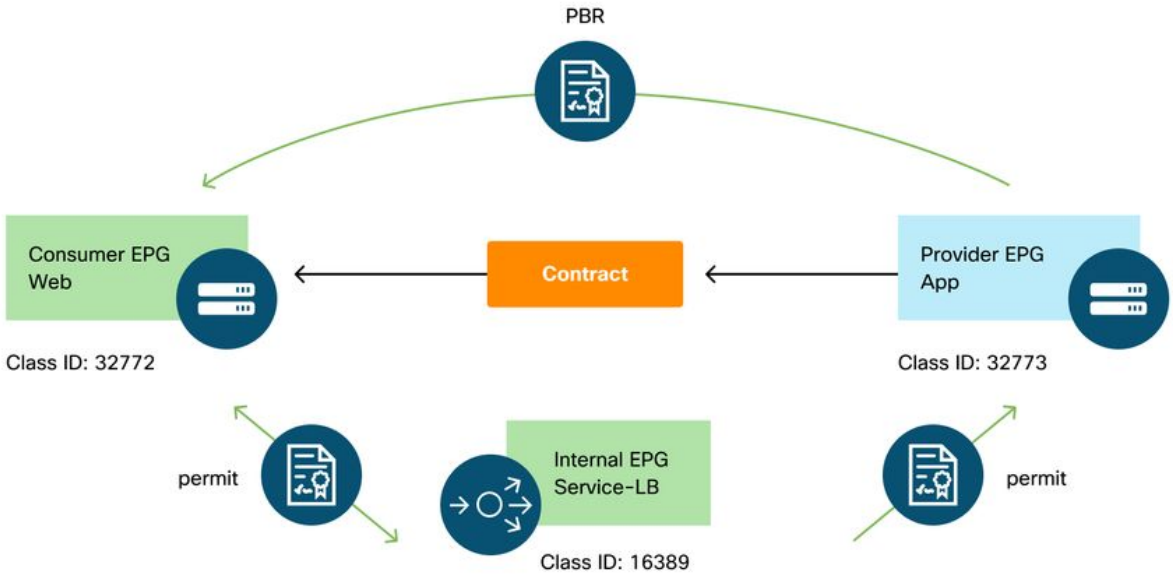
无SNAT的负载均衡器转发路径示例 — 使用PBR的提供商到消费者



在枝叶节点上编程的策略。

下图和下面的“show zoning-rule”输出描述了Service Graph部署后的分区规则。在本示例中，允许从pcTag 32772(Web)到pcTag 16389(Service-LB)的流量，允许从pcTag 16389(Service-LB)到pcTag 32773(App)的流量，并将从pcTag 32773(App)到pcTag 32772(Web)的流量重定向到“destgrp-31”（负载均衡器）。

服务图部署后的分区规则 — 无SNAT的负载均衡器

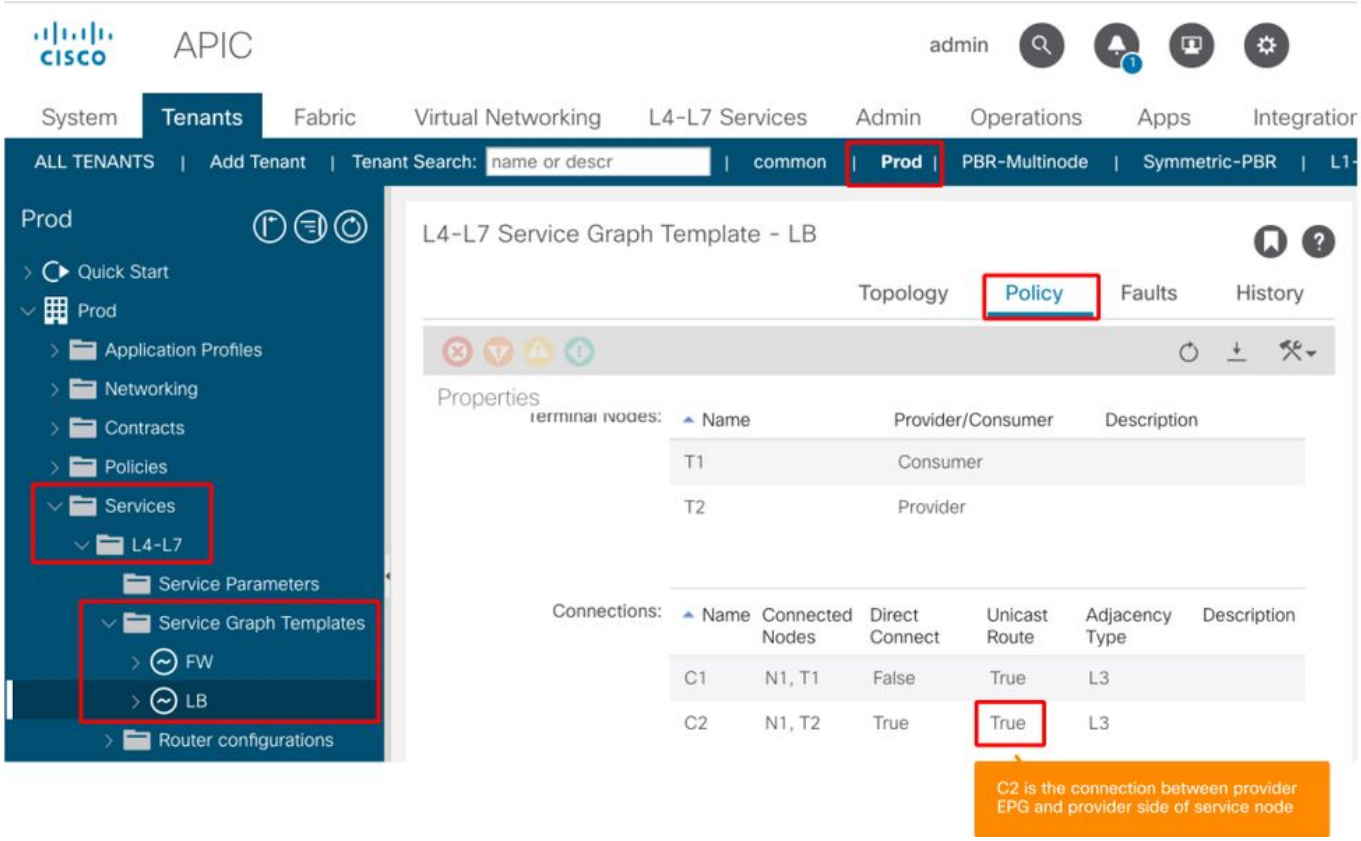


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
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)     |
...
```

默认情况下，不会将提供商EPG(pcTag 32773)到Service-LB(pcTag 16389)的允许规则编程。要允许它们之间进行双向通信以进行从负载均衡器到提供商终端的运行状况检查，必须将连接上的直接连接选项设置为True。位置为“租户> L4-L7 >服务图模板>策略”。 默认值为False。

设置直接连接选项



如下所述，它将提供商EPG(32773)的允许规则添加到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 — 不带SNAT的防火墙和负载均衡器

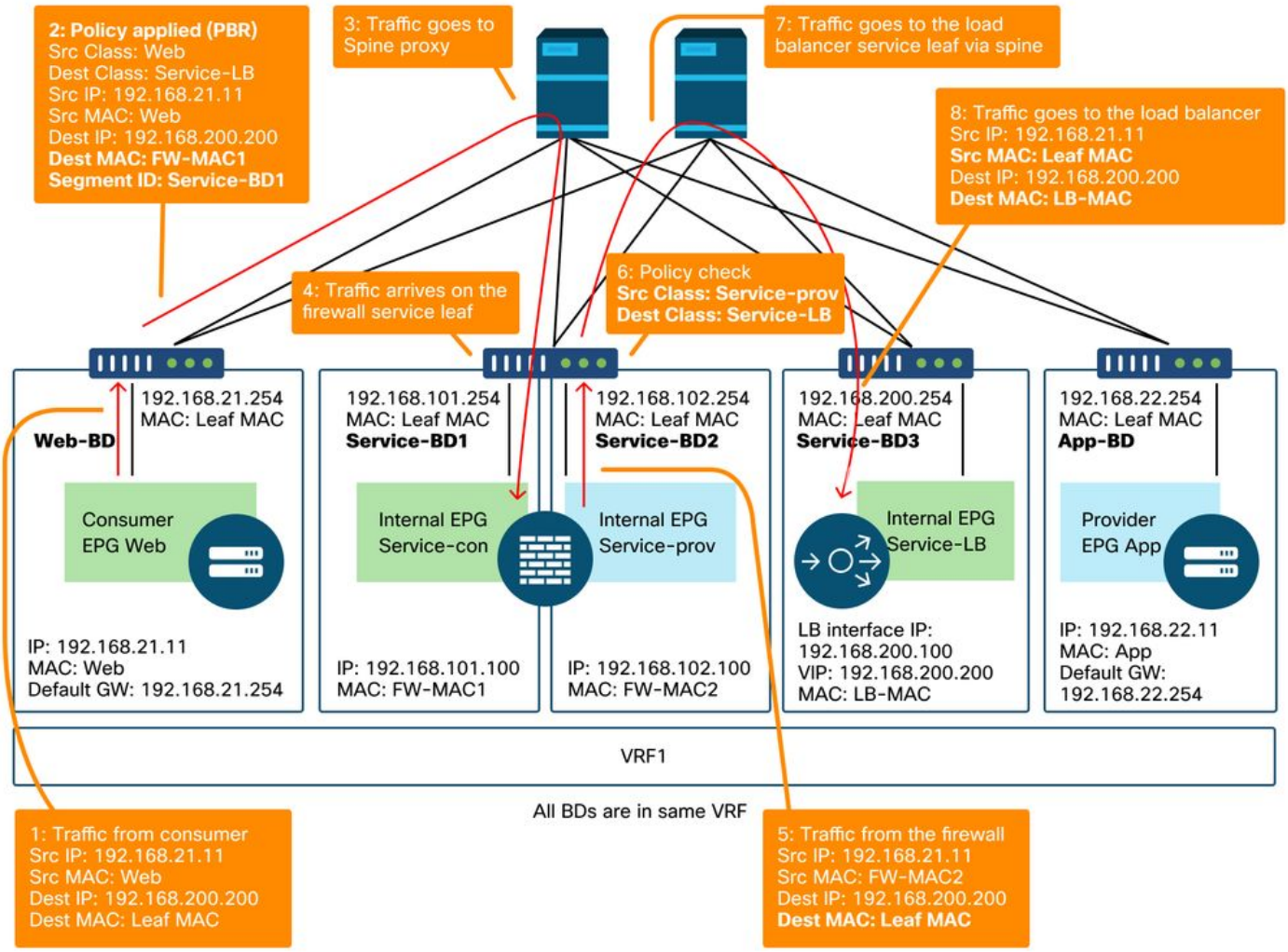
PBR可以部署为服务图中的多个服务功能，例如防火墙作为第一节点，负载均衡器作为第二节点。

流量路径示例

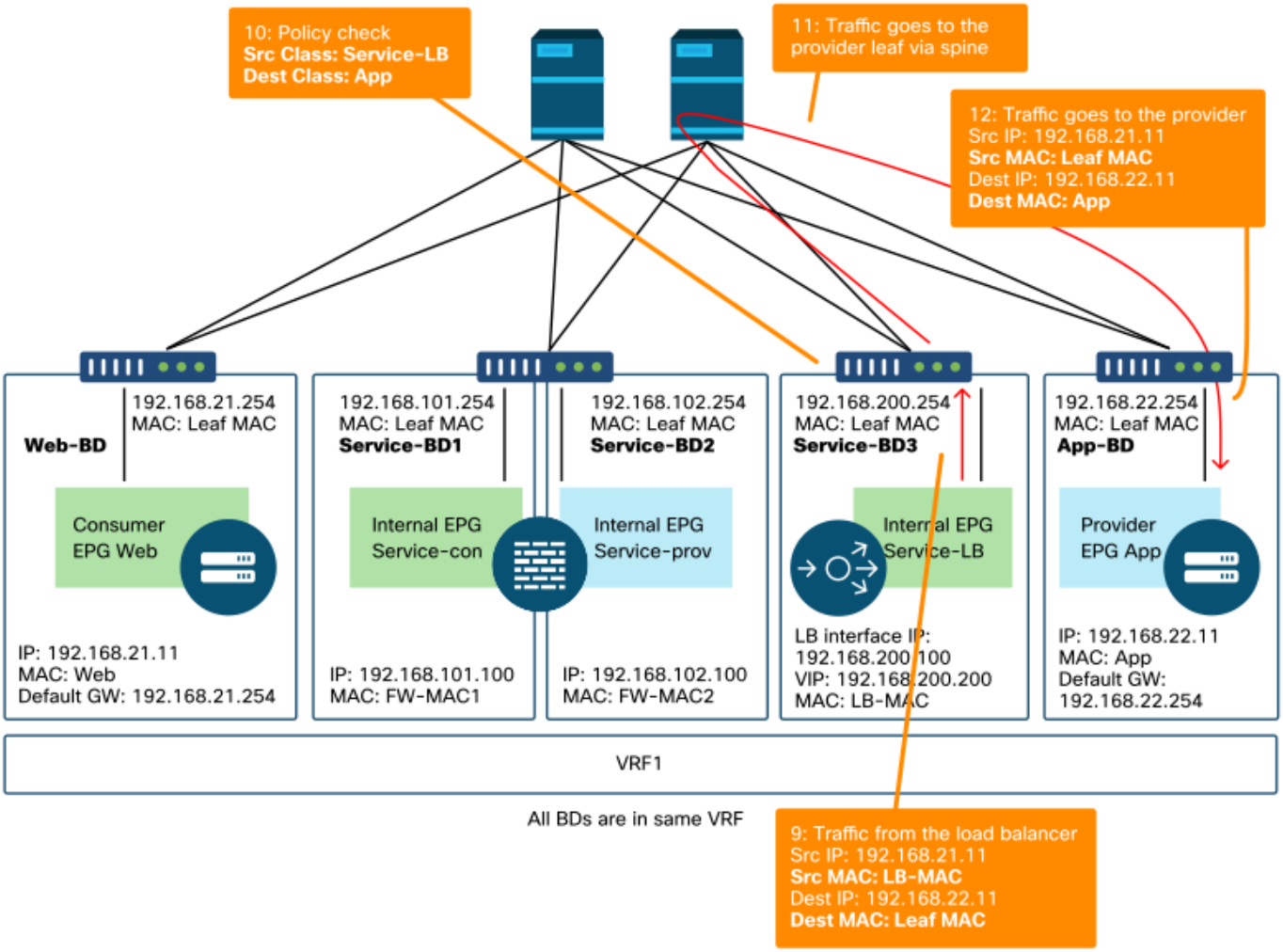
下图显示了从消费者EPG Web到具有两个连接的提供商EPG应用的传入流量的示例：一个是从消费者EPG Web中的终端通过防火墙连接到负载均衡器VIP，另一个是从负载均衡器连接到提供商EPG应用中的终端。流向VIP的传入流量重定向到防火墙，然后转至没有PBR的负载均衡器。负载均衡器将目标IP更改为与VIP关联的App EPG中的一个终端，但不转换源IP。然后，流量进入提供

商终端。

无SNAT的防火墙和负载均衡器转发路径示例 — 消费者到VIP和负载均衡器到提供商



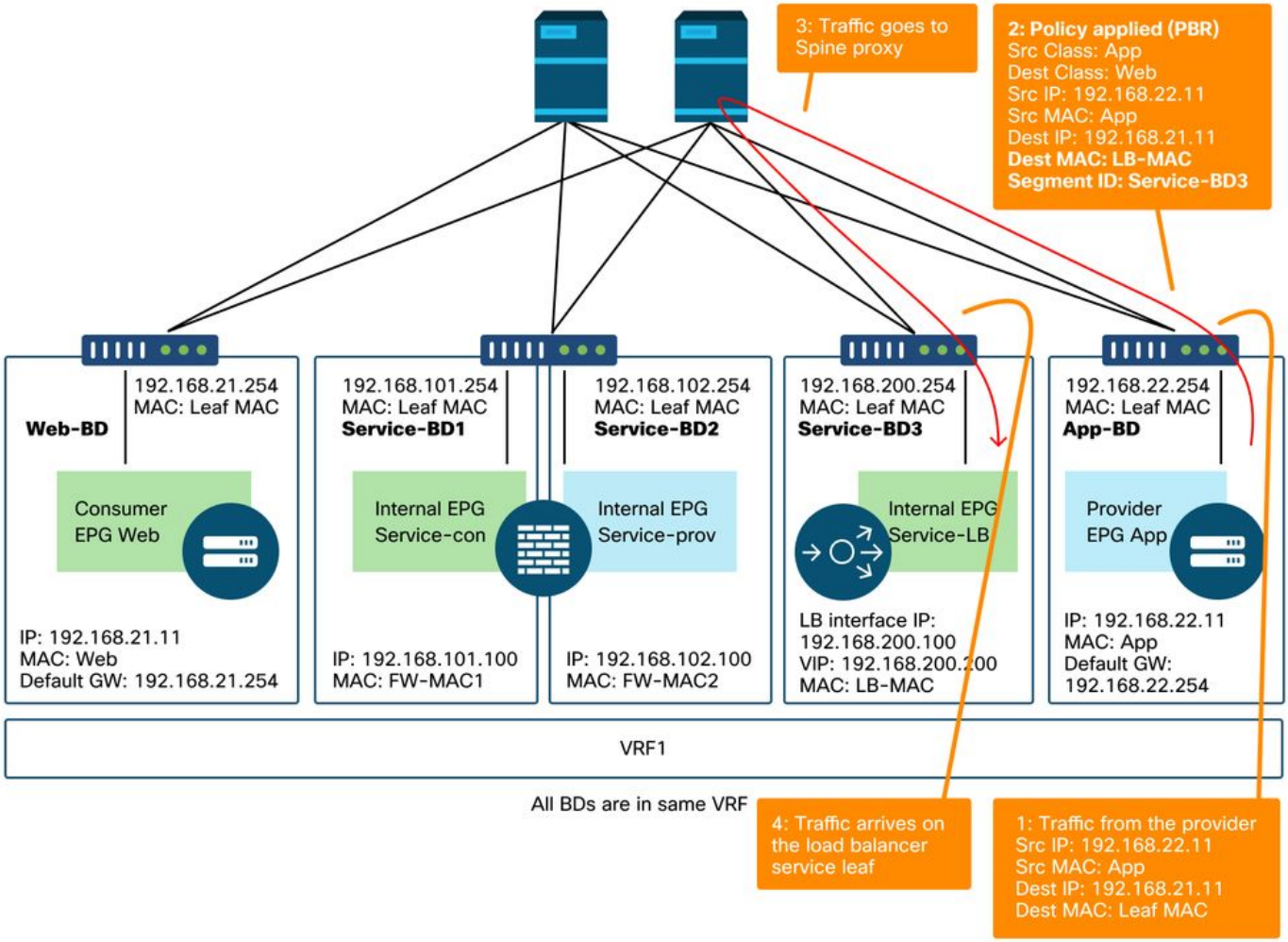
无SNAT的防火墙和负载均衡器转发路径示例 — 消费者到VIP和负载均衡器到提供商（续）

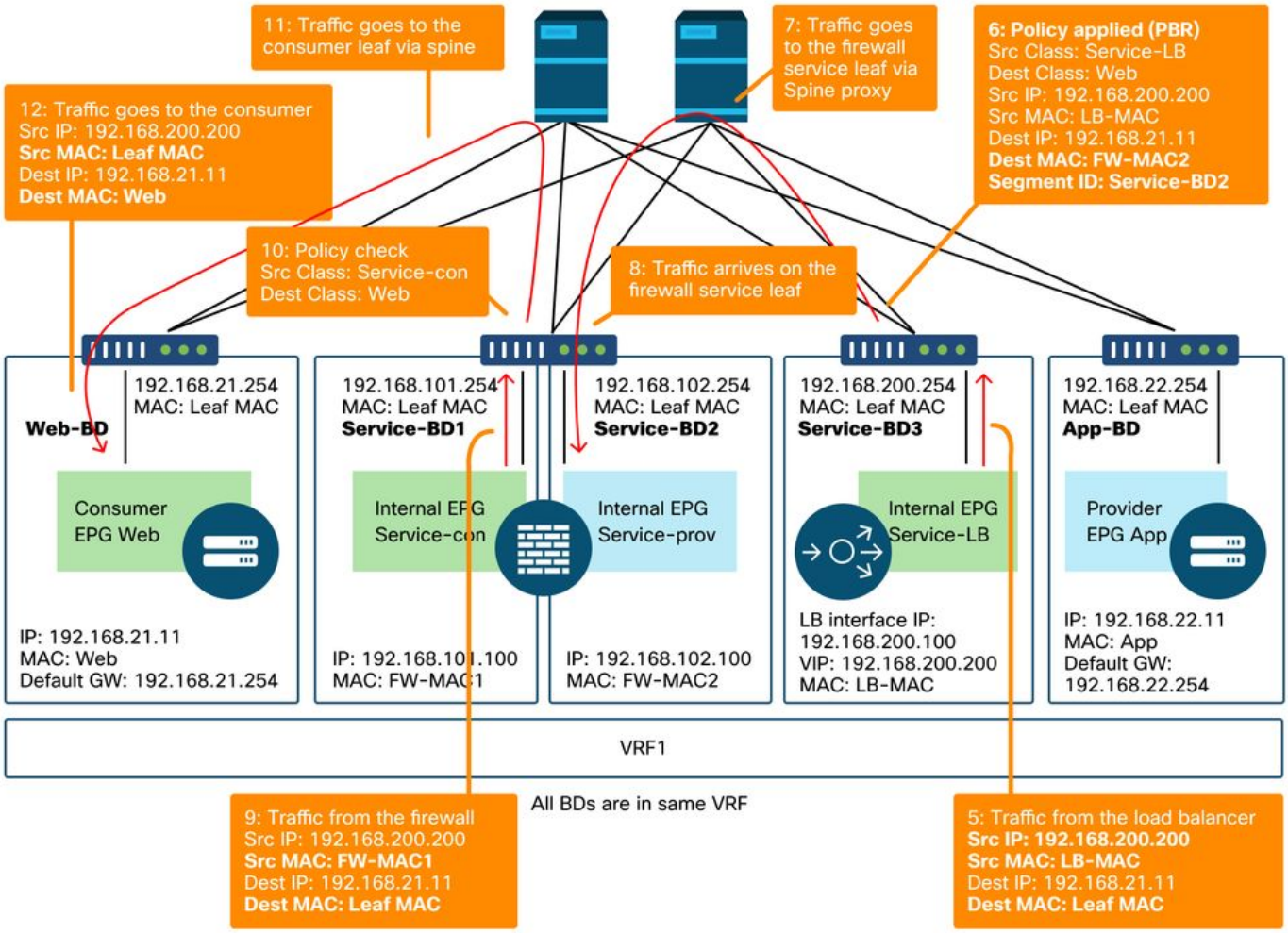


下图显示了从提供商EPG应用到消费者EPG网络的返回流量。由于返回流量发往原始源IP，因此PBR需要使返回流量返回负载均衡器。

从提供商终端到消费者终端的流量重定向到负载均衡器后，负载均衡器会将源IP更改为VIP。流量从负载均衡器返回并被重定向到防火墙。然后，流量从防火墙返回至消费者终端。

无SNAT的防火墙和负载均衡器转发路径示例 — 提供商到消费者

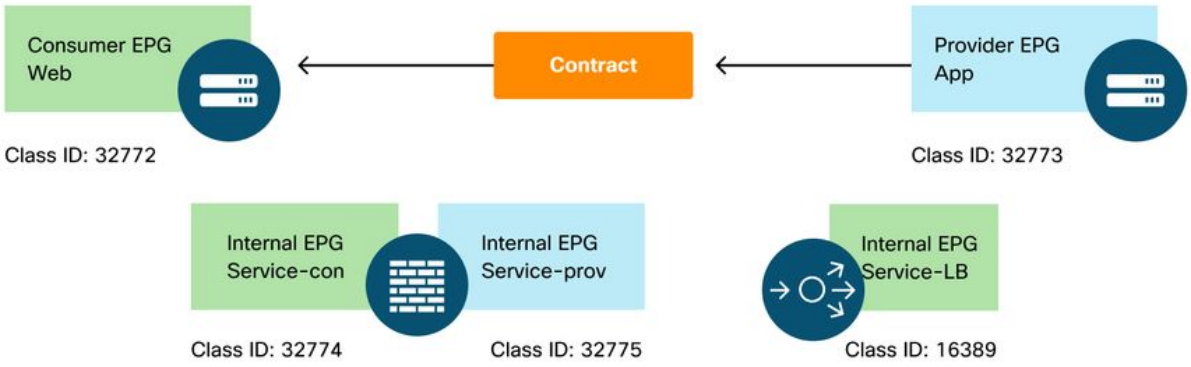

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



在枝叶节点上编程的策略

下图和下图所示的“show zoning-rule”输出描述了Service Graph部署后的分区规则。在本示例中，从pcTag 32772(Web)到pcTag 16389(Service-LB)的流量重定向到“destgrp-32”（防火墙的消费者端），从pcTag 32773(App)到pcTag 32772(Web)的流量重定向到“destgrp-33”（负载均衡器），从pcTag 16389(Service-LB)到pcTag 32772(Web)的流量重定向到“destgrp-34”（防火墙的提供商端）。

Zoning-rules after Service Graph deployment — 不带SNAT的防火墙和负载均衡器



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)    |
+---------+--------+--------+----------+----------------+---------+---------+------+------------
-------+----------------------+
```

在上面的示例中，负载均衡器的提供商端与提供商EPG之间的连接上的Direct Connect选项设置为“True”。必须启用它以进行从负载均衡器到提供程序端点的运行状况检查。位置为“租户> L4-L7 >服务图模板>策略”。 请参阅图“设置直接连接选项”。

3.共享服务（VRF间合同）

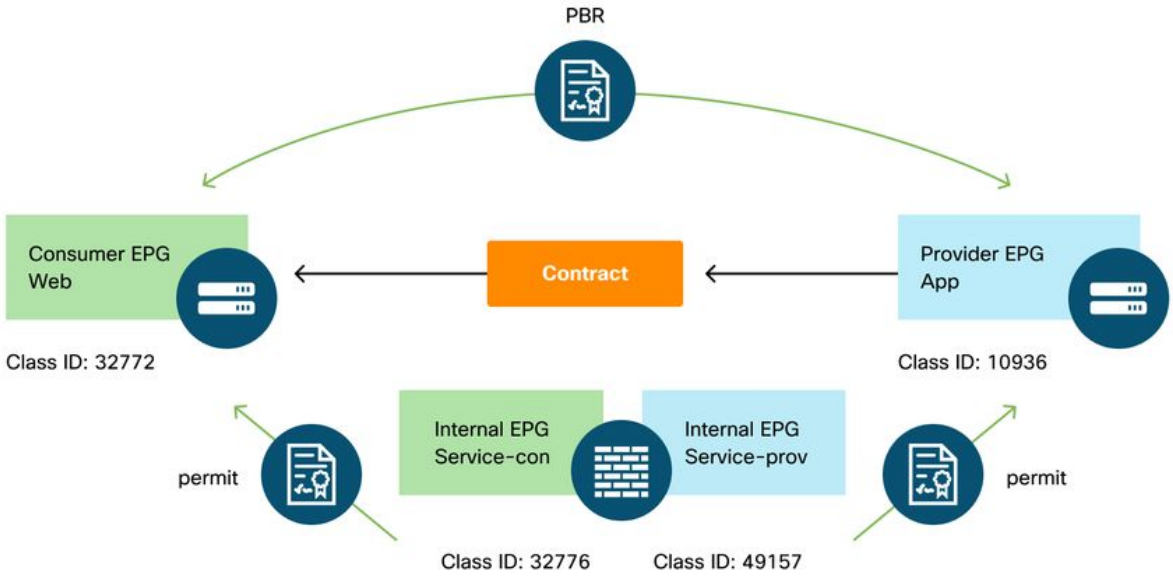
可以在VRF间合同中启用PBR。本节介绍如何在EPG到EPG VRF间合同的情况下编程分区规则。

在枝叶节点上编程的策略

在EPG到EPG间VRF合同的情况下，策略始终在消费者VRF中实施。因此，重定向发生在使用者VRF上。有关其他组合，请参阅表“在何处实施策略？” 在“转发”部分。

下图和下面的“show zoning-rule”输出描述了服务图部署后的分区规则。在本示例中，从pcTag 32772(Web)到pcTag 10936(App)的流量重定向到“destgrp-36”（服务节点的消费者端），而从pcTag 10936(App)到pcTag 32772(Web)的流量重定向到“destgrp-35”（服务节点的提供商端）。 两者都在作为使用者VRF的VRF1中实施。VRF1中允许从pcTag 32776（防火墙的消费者端）到pcTag 32772(Web)的流量。

服务图部署后的分区规则 — VRF间合同



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中允许从pcTag 49157（防火墙的提供商端）到pcTag 10936（应用）的流量，因为两者都在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)    |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。