Solucionar problemas de redirecionamento baseado em políticas da ACI

Contents

Introduction
Informações de Apoio
Visão geral do redirecionamento baseado em políticas
Solução de problemas de implantação de gráfico de serviço
1. Verifique as etapas de configuração e a falha
2. Verificar a implantação do Gráfico de Serviço na interface do usuário
Troubleshooting de Encaminhamento PBR
1. Verifique se as VLANs estão implantadas e se os pontos de extremidade são aprendidos no nó folha
2. Verifique os caminhos de tráfego esperados
Onde a política é aplicada?
3. Verifique se o tráfego é redirecionado para o nó de serviço
4. Verifique as políticas programadas nos nós de folha
Outros exemplos de fluxo de tráfego
1. Balanceador de carga sem SNAT
Exemplo de caminho de tráfego
As políticas programadas nos nós de folha.
2. Exemplo de fluxo de tráfego - Firewall e balanceador de carga sem SNAT
Exemplo de caminho de tráfego
As políticas programadas nos nós de folha
3. Serviço compartilhado (Contrato Inter-VRF)
As políticas programadas nos nós de folha

Introduction

Este documento descreve as etapas para entender e solucionar problemas de um cenário de Redirecionamento baseado em políticas (PBR) da ACI.

Informações de Apoio

O material deste documento foi extraído do livro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, especificamente os capítulos **Redirecionamento Baseado em Políticas - Visão Geral, Redirecionamento Baseado em Políticas - Implantação do Gráfico de Serviço, Redirecionamento Baseado em Políticas** e Redirecionamento Baseado em Políticas - Outros exemplos de fluxo de tráfego.

Visão geral do redirecionamento baseado em políticas

Este capítulo explica a solução de problemas do Gráfico de serviço do modo não gerenciado com

Redirecionamento baseado em política (PBR).

A seguir estão algumas etapas típicas de solução de problemas. Este capítulo explica como verificar as etapas 2 e 3 que são específicas do PBR. Para as etapas 1 e 4, consulte os capítulos: "Encaminhamento dentro da malha", "Encaminhamento externo" e "Políticas de segurança".

1. Verifique se o tráfego funciona sem o PBR Service Graph: Os endpoints do consumidor e do provedor são aprendidos.Endpoints de consumidor e provedor podem se comunicar.
2. Verificar se o Gráfico de serviço está implantado: As Instâncias de Gráfico Implantadas não têm falhas.VLANs e IDs de classe para o nó de serviço são implantados.Os pontos de extremidade do nó de serviço são aprendidos.
3. Verifique o caminho de encaminhamento: Verifique se a política está programada nos nós de folha.Capture o tráfego no nó de serviço para confirmar se o tráfego é redirecionado.Capture o tráfego na folha da ACI para confirmar se o tráfego retorna à estrutura da ACI após o PBR.
4. Verifique se o tráfego chega ao consumidor e ao endpoint do provedor e se o endpoint gera o tráfego de retorno.

Este documento não aborda opções de design ou configuração. Para obter essas informações, consulte o "White Paper ACI PBR" em Cisco.com

Neste capítulo, o nó de serviço e o leaf de serviço implicam no seguinte:

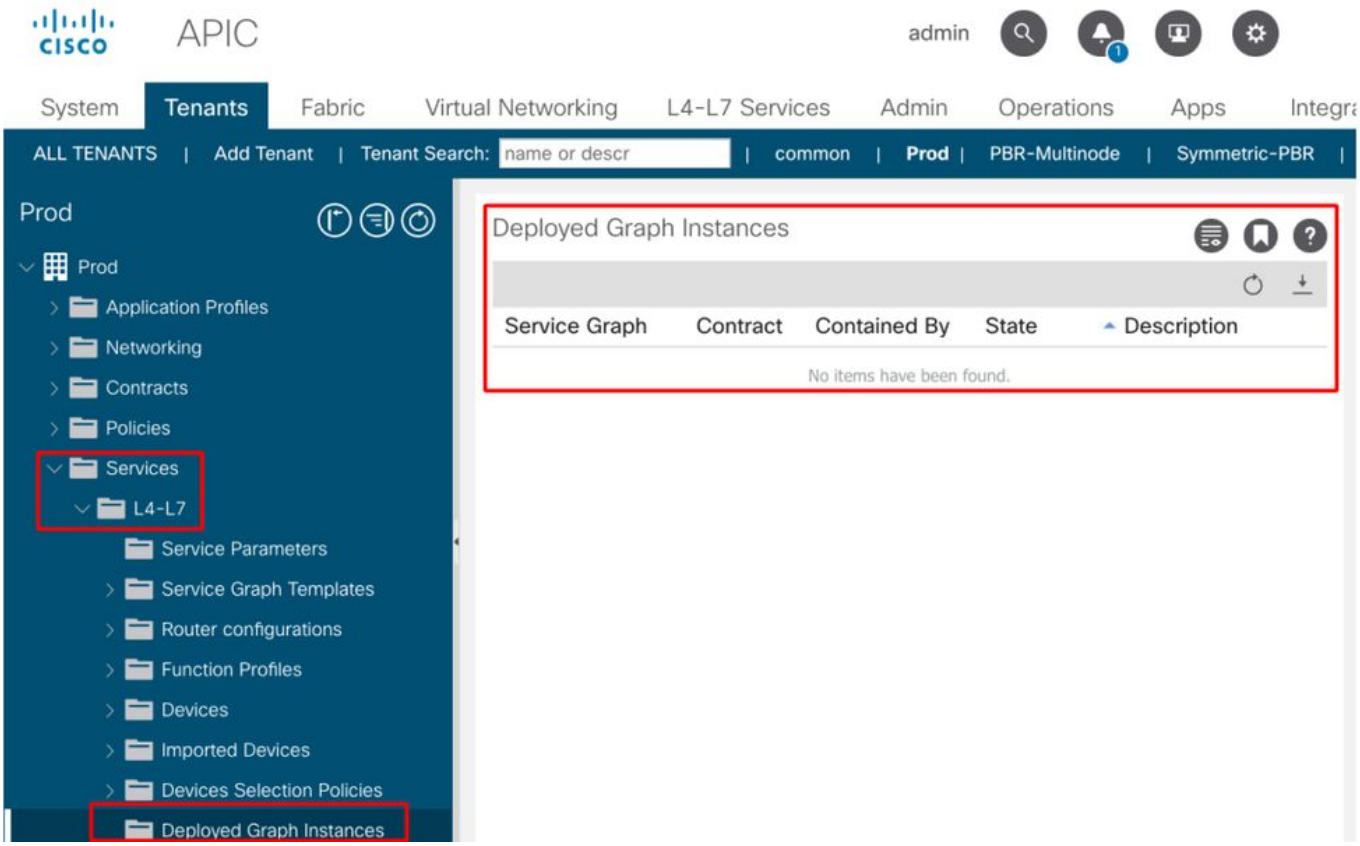
- Nó de serviço — um nó externo para o qual o PBR está redirecionando o tráfego, como um firewall ou balanceador de carga.
- Folha de serviço — uma folha de ACI conectada a um nó de serviço.

Solução de problemas de implantação de gráfico de serviço

Este capítulo explica um exemplo de Troubleshooting em que um Service Graph não está implantado.

Depois que uma política do Service Graph é definida e aplicada a um sujeito de contrato, deve haver uma instância de gráfico implantada aparecendo na GUI da ACI. A figura abaixo mostra o cenário de solução de problemas em que o Gráfico de serviço não aparece como implantado.

O gráfico de serviço não é mostrado como uma instância do gráfico implantado.



1. Verifique as etapas de configuração e a falha

A primeira etapa da solução de problemas é verificar se os componentes necessários foram configurados sem falhas. A suposição é que as configurações gerais abaixo já estão feitas:

- VRF e BDs para EPG de consumidor, EPG de provedor e nó de serviço
- O EPG do consumidor e do provedor.
- O contrato e os filtros.

Vale mencionar que um EPG para o nó de serviço não precisa ser criado manualmente. Ele será criado por meio da implantação do Gráfico de serviço.

O Service Graph com as etapas de configuração do PBR são as seguintes:

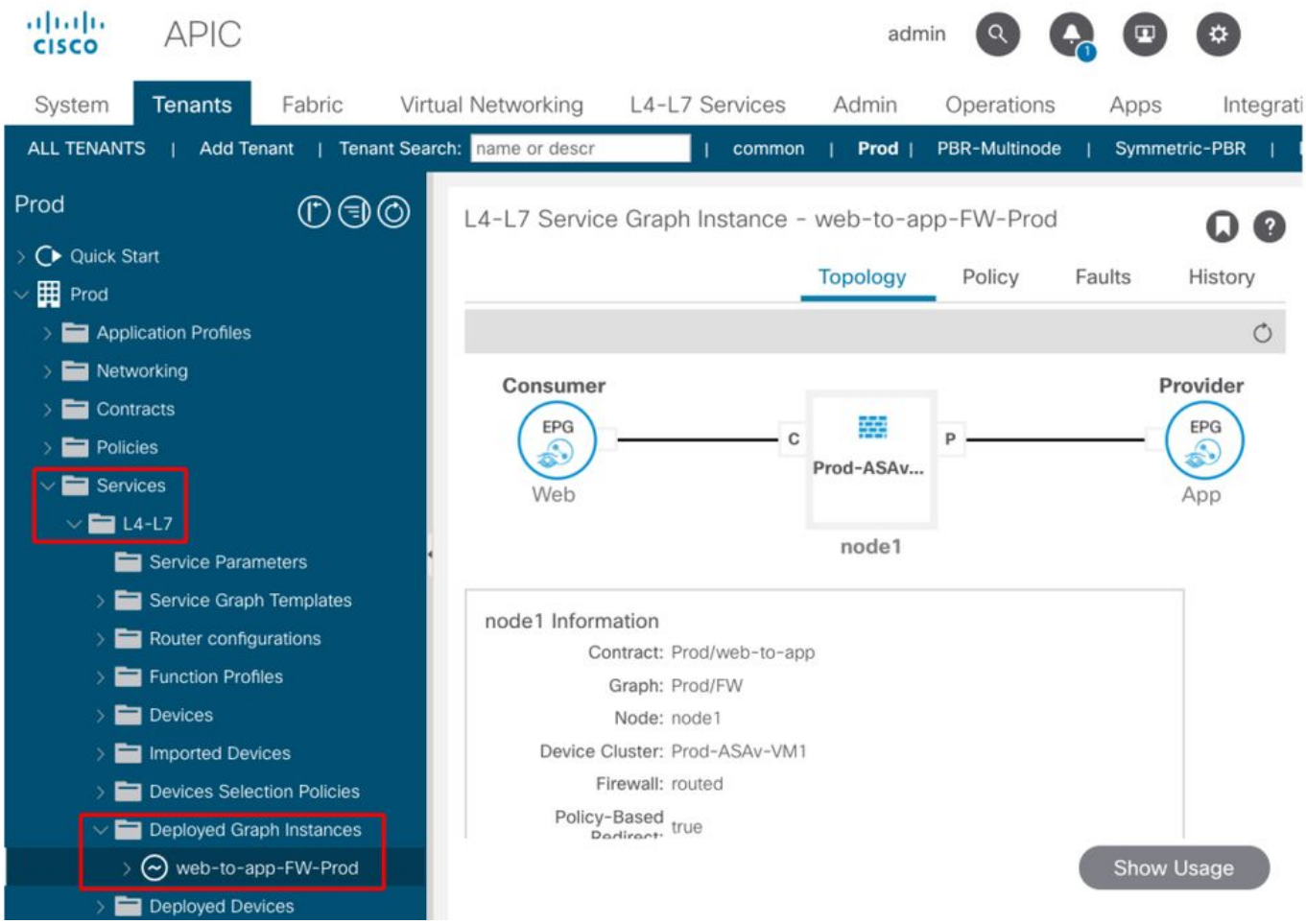
- Crie o dispositivo L4-L7 (dispositivo lógico).
- Crie o Gráfico de serviços.
- Crie a política de PBR.
- Crie a política de Seleção de Dispositivo.
- Associe o Gráfico de serviços ao assunto do contrato.

2. Verificar a implantação do Gráfico de Serviço na interface do usuário

Depois que um Gráfico de serviço é associado ao assunto do contrato, uma instância de gráfico implantado deve aparecer para cada contrato com o Gráfico de serviço (figura abaixo).

O local é 'Locatário > Serviços > L4-L7 > Instâncias de Gráfico Implantadas'

Instância do Gráfico Implantada



Se uma instância do gráfico implantado não aparecer, há algo errado com a configuração do contrato. Os principais motivos podem ser:

- O contrato não tem um EPG de consumidor ou provedor.
- O assunto do contrato não tem nenhum filtro.
- O escopo do contrato é VRF, embora seja para comunicação entre VRF ou EPG entre usuários.

Se a instanciação do gráfico de serviço falhar, as falhas serão geradas na instância do gráfico implantado, o que significa que há algo errado com a configuração do gráfico de serviço. As falhas típicas causadas pela configuração são as seguintes:

F1690: A configuração é inválida devido à falha de alocação de ID

Essa falha indica que a VLAN encapsulada para o nó de serviço não está disponível. Por exemplo, não há VLAN dinâmica disponível no pool de VLANs associado ao domínio do VMM usado no dispositivo lógico.

Resolução: Verifique o pool de VLANs no domínio usado para o Dispositivo lógico. Verifique a VLAN encapsulada na interface do dispositivo lógico se ela estiver em um domínio físico. Os locais são 'Locatário > Serviços > L4-L7 > Dispositivos e Estrutura >Políticas de Acesso > Pools > VLAN'.

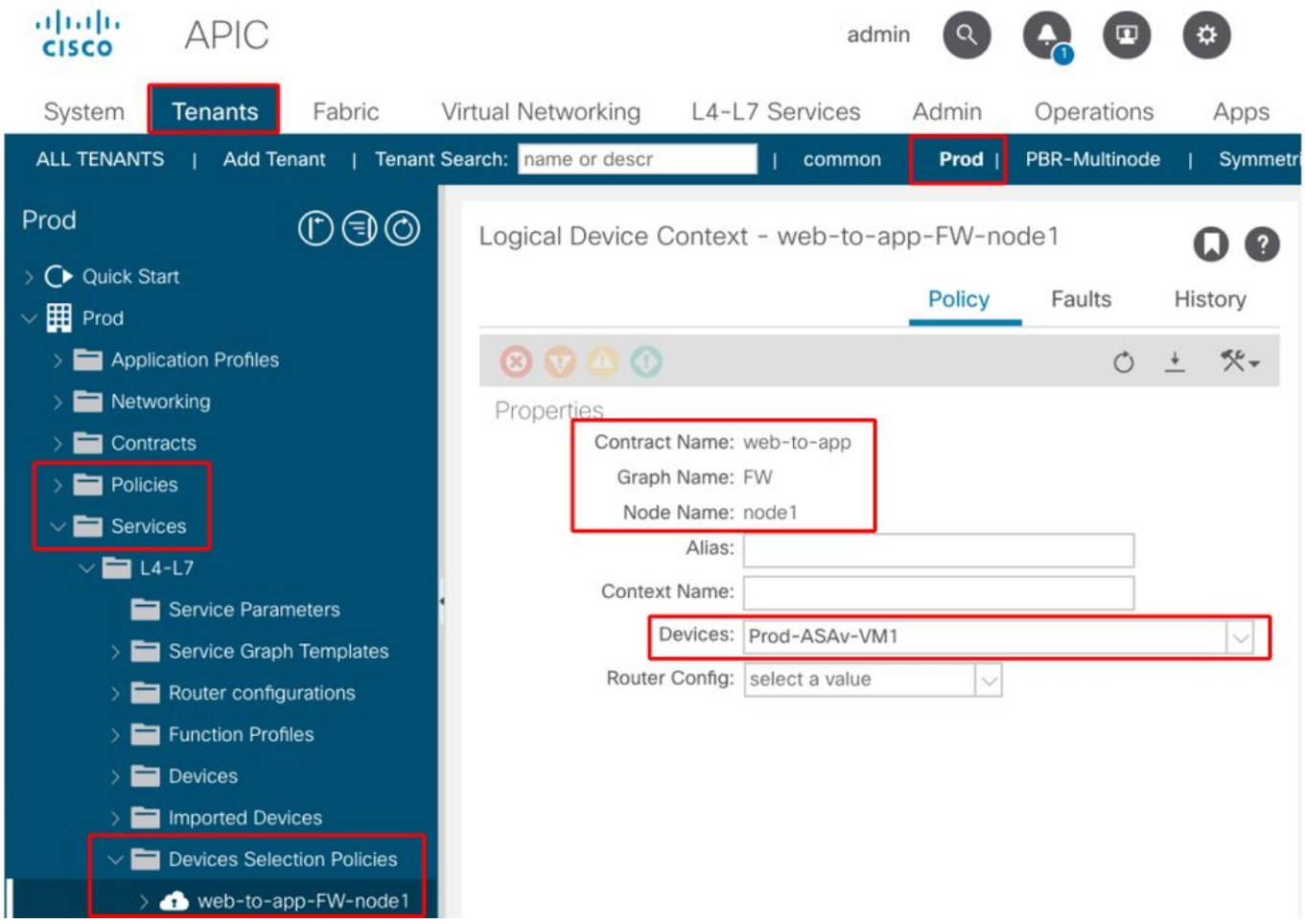
F1690: A configuração é inválida porque nenhum contexto de dispositivo foi encontrado para LDev

Esta falha indica que o Dispositivo Lógico não foi encontrado para a renderização do Gráfico de

Serviço. Por exemplo, não há nenhuma Política de seleção de dispositivo correspondente ao contrato com o Gráfico de serviço.

Resolução: Verifique se a política de seleção de dispositivos está definida. A Política de seleção de dispositivos fornece um critério de seleção para um dispositivo de serviço e seus conectores. Os critérios são baseados em um nome de contrato, um nome de Gráfico de serviço e um nome de nó no Gráfico de serviço. O local é 'Locatário > Serviços > L4-L7 > Política de Seleção de Dispositivo'.

Verificar Política de Seleção de Dispositivo



F1690: Configuração inválida porque nenhuma interface de cluster foi encontrada

Esta falha indica que a interface de cluster do nó de serviço não foi encontrada. Por exemplo, a interface de cluster não está especificada na Política de Seleção de Dispositivo.

Resolução: Verifique se a interface de cluster está especificada na política de Seleção de Dispositivo e se o nome do conector está correto (Figura abaixo).

F1690: A configuração é inválida porque nenhum BD foi encontrado

Essa falha indica que o BD do nó de serviço não pode ser encontrado. Por exemplo, o BD não é especificado na Política de seleção de dispositivo.

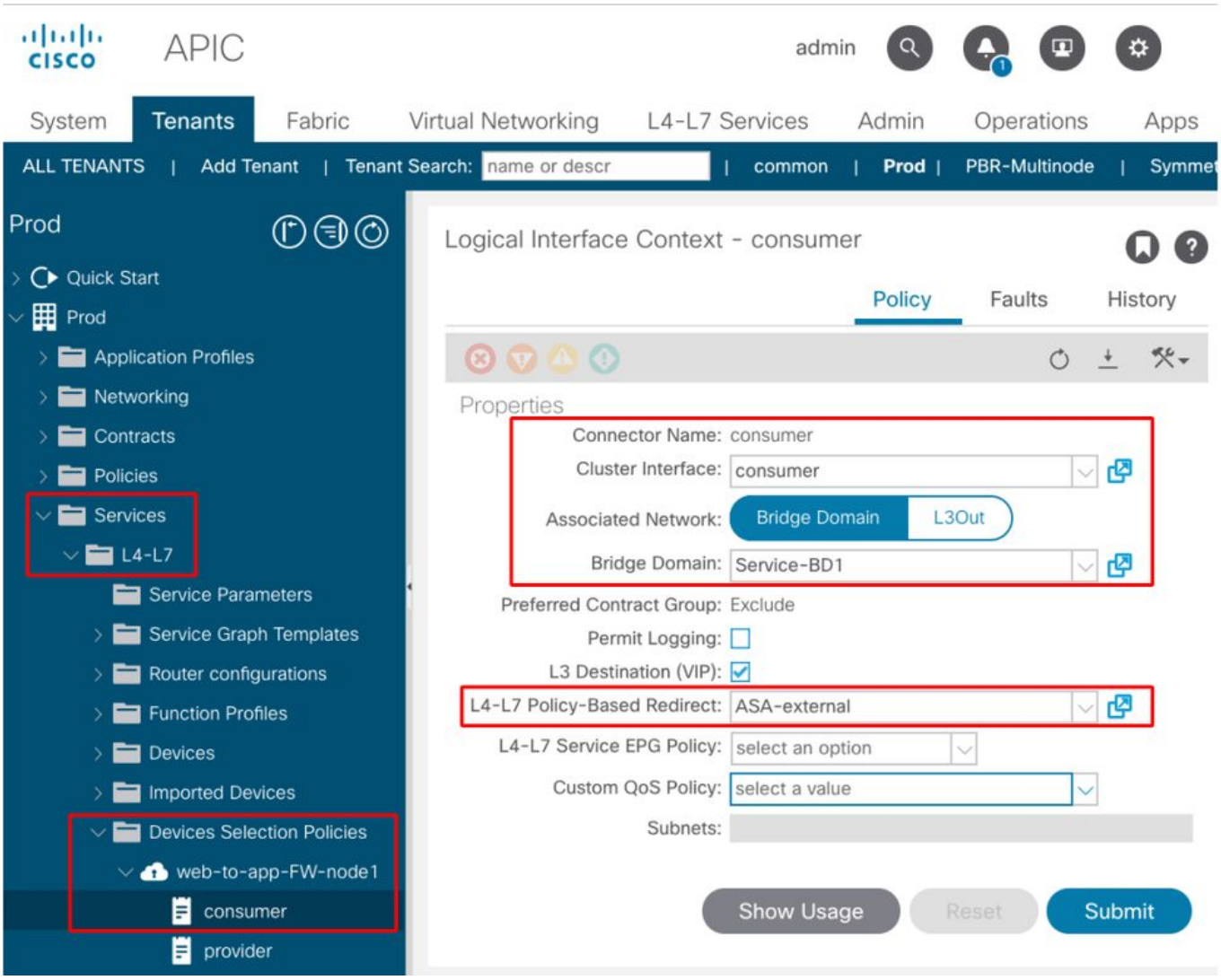
Resolução: Verifique se BD está especificado na política de Seleção de Dispositivo e se o nome do conector está correto (Figura abaixo).

F1690: Configuração inválida devido à política de redirecionamento de serviço inválida

Essa falha indica que a política de PBR não está selecionada, embora o redirecionamento esteja habilitado na função de serviço no Gráfico de serviço.

Resolução: Selecione a política PBR na Política de seleção de dispositivos (Figura abaixo).

Configuração de interface lógica na Política de Seleção de Dispositivo



Troubleshooting de Encaminhamento PBR

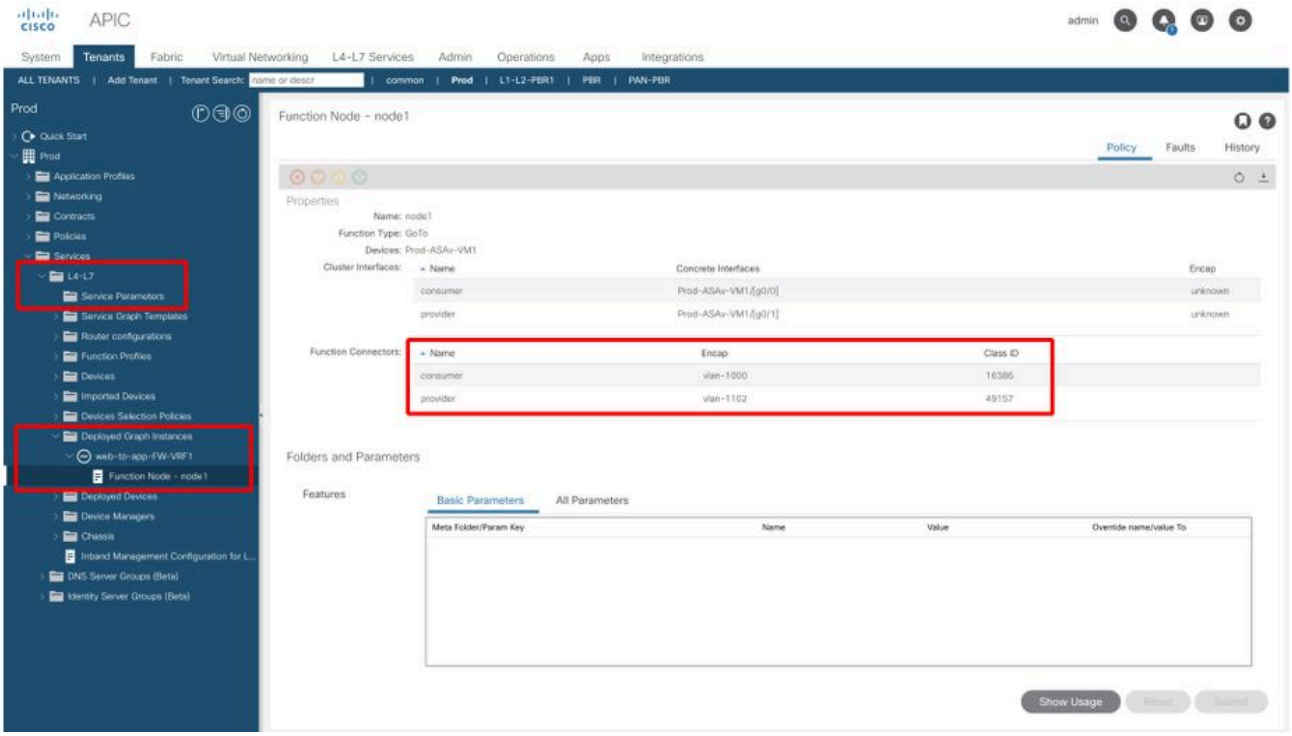
Este capítulo explica as etapas de Troubleshooting para o caminho de encaminhamento de PBR.

1. Verifique se as VLANs estão implantadas e se os pontos de extremidade são aprendidos no nó folha

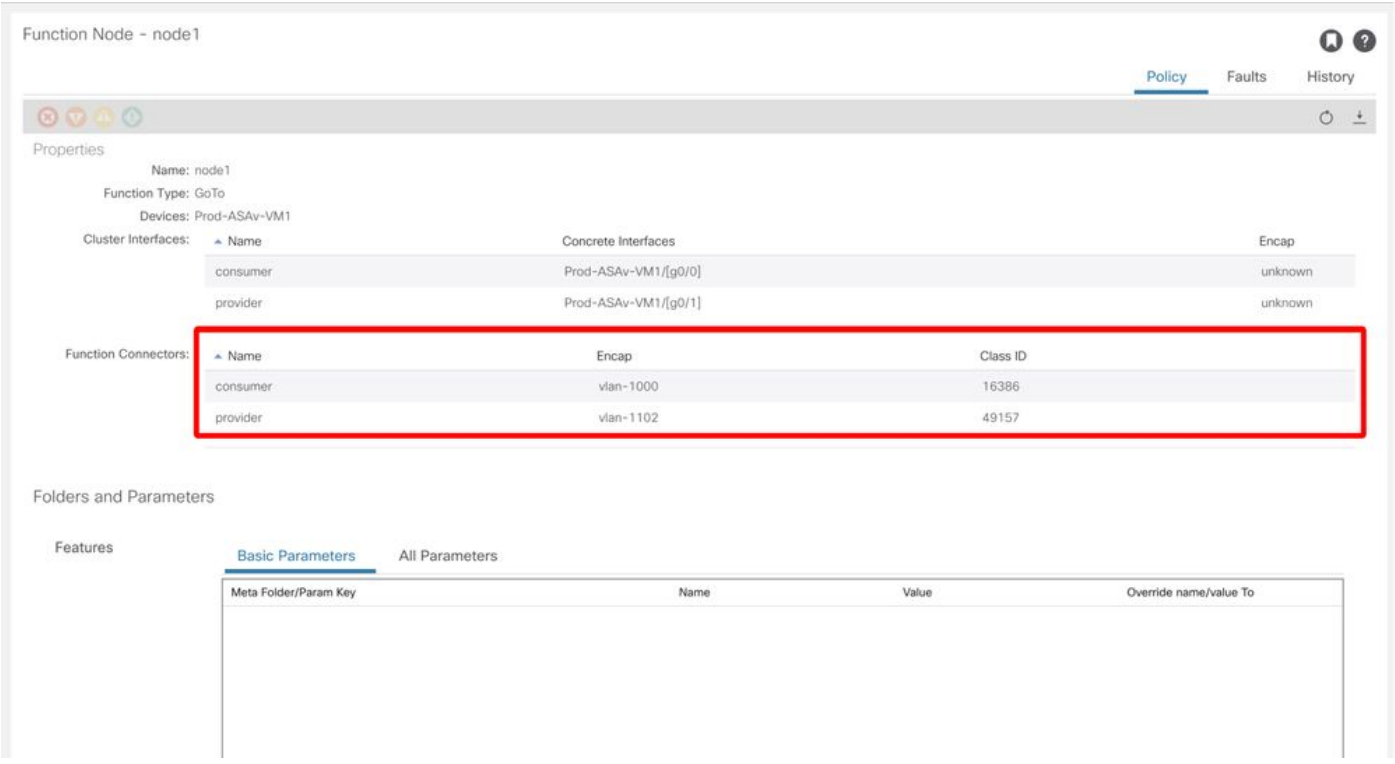
Quando um Gráfico de serviço é implantado com êxito sem nenhuma falha, são criados EPGs e BDs para um nó de serviço. A figura abaixo mostra onde encontrar as IDs de VLAN encapsuladas e as IDs de classe das interfaces de nó de serviço (EPGs de serviço). Neste exemplo, o lado do consumidor de um firewall é o ID de classe 16386 com VLAN encap 1000 e o lado do provedor de um firewall é o ID de classe 49157 com VLAN encap 1102.

O local é 'Inquilino > Serviços > L4-L7 > Instâncias do gráfico implantado > Nós de função'.

Nó de serviço



ID da classe da interface do nó de serviço



Essas VLANs são implantadas nas interfaces de nó folha de serviço onde os nós de serviço estão conectados. O status de aprendizagem de implantação e de endpoint de VLAN pode ser verificado usando-se 'show vlan extended' e 'show endpoint' na CLI do nó folha do serviço.

```
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
```

Se os IPs de endpoint dos nós de serviço não forem aprendidos como endpoints na estrutura da ACI, é mais provável que seja um problema de conectividade ou configuração entre a folha de serviço e o nó de serviço. Verifique os seguintes status:

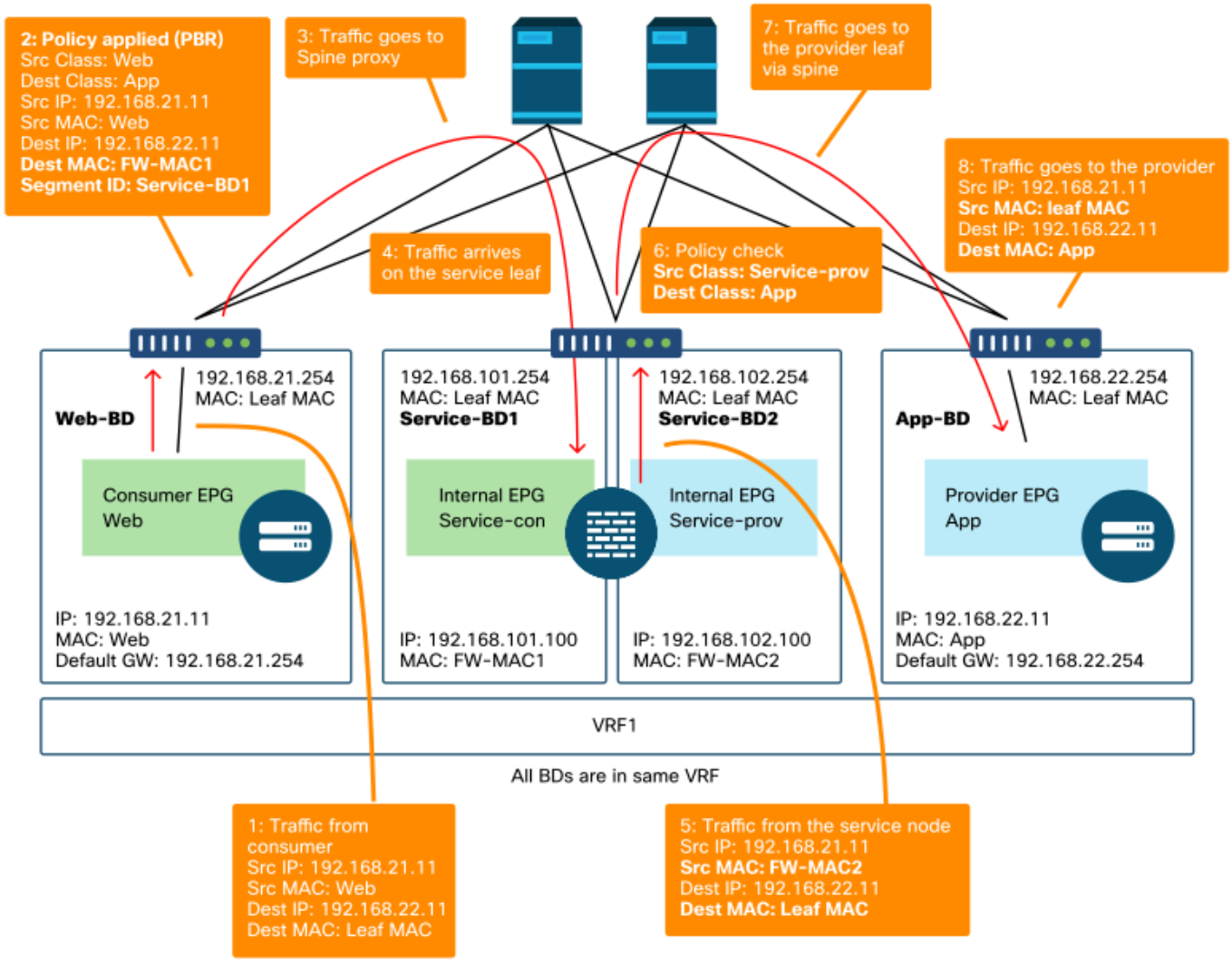
- O nó de serviço está conectado à porta de downlink folha correta. Se o nó de serviço estiver em um domínio físico, o caminho estático leaf end encap VLAN precisará ser definido no dispositivo lógico.Se o nó de serviço estiver em um domínio do VMM, verifique se o domínio do VMM está funcionando e se o grupo de portas criado pelo Gráfico de Serviço está anexado corretamente à VM do nó de serviço.
- A porta de downlink folha conectada ao nó de serviço ou ao hipervisor onde o nó de serviço VM reside está ATIVADO.
- O nó de serviço tem a VLAN e o endereço IP corretos.
- O switch intermediário entre o leaf de serviço e o nó de serviço tem a configuração de VLAN correta.

2. Verifique os caminhos de tráfego esperados

Se o tráfego de ponta a ponta parar de funcionar depois que o PBR for habilitado, mesmo que os endpoints de nó de serviço sejam aprendidos na estrutura da ACI, a próxima etapa de solução de problemas é verificar quais são os caminhos de tráfego esperados.

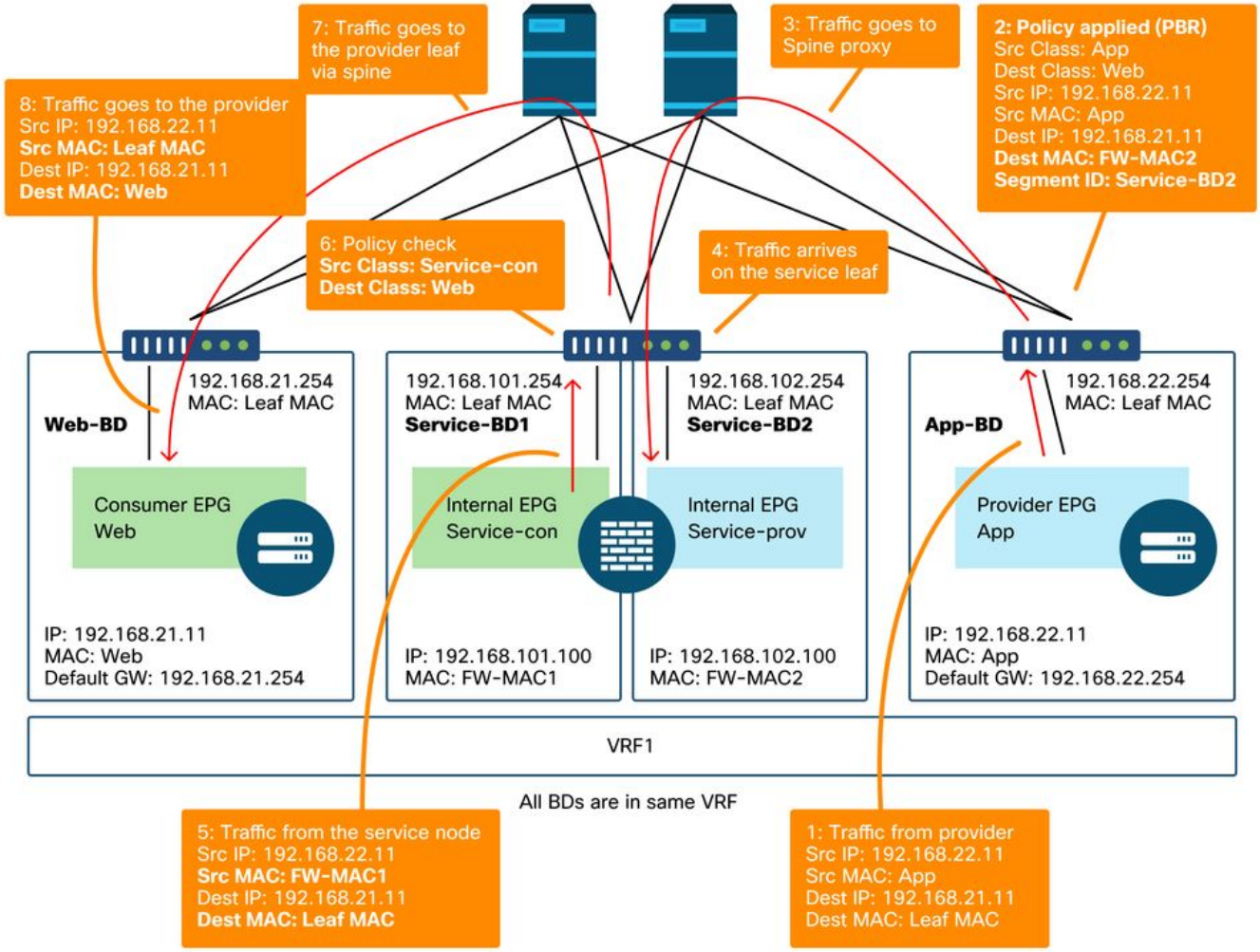
As figuras 'exemplo de caminho de encaminhamento PBR - consumidor para provedor' e 'exemplo de caminho de encaminhamento PBR - provedor para consumidor' ilustram um exemplo de caminho de encaminhamento de inserção de firewall usando PBR entre um ponto final de consumidor e um ponto final de provedor. A suposição é que os endpoints já foram aprendidos em nós folha.

Exemplo de caminho de encaminhamento PBR - do consumidor para o provedor



Nota: Como o MAC origem não é alterado para o MAC folha da ACI, o nó PBR não deve usar o encaminhamento baseado no MAC origem se o endpoint do consumidor e o nó PBR não estiverem no mesmo BD

Exemplo de caminho de encaminhamento PBR - provedor para consumidor



Note: Vale mencionar que a política de PBR é aplicada na folha do consumidor ou do provedor e o que a ACI PBR faz é a regravação de MAC de destino, como mostrado nas figuras 'Exemplo de caminho de encaminhamento de PBR - de consumidor para provedor' e 'Exemplo de caminho de encaminhamento de PBR - de provedor para consumidor'. Alcançar o MAC destino de PBR sempre usa um proxy spine, mesmo que o ponto final de origem e o MAC destino de PBR estejam sob a mesma folha.

Embora as figuras 'exemplo de caminho de encaminhamento de PBR - de consumidor para provedor' e 'exemplo de caminho de encaminhamento de PBR - de provedor para consumidor' mostrem um exemplo de onde o tráfego seria redirecionado, onde a política é aplicada depende da configuração do contrato e do status de aprendizagem do ponto final. A tabela "Onde a política é aplicada" resume onde a política é aplicada em um único site da ACI. Onde a política é aplicada em vários sites é diferente.

Onde a política é aplicada?

Cenário	modo de aplicação de VRF	Consumidor	Provedor	Política aplicada em
IntraVRF	Entrada/saída	EPG	EPG	·Se o endpoint de destino for aprendido: folha de entrada* ·Se o endpoint de destino não for aprendido: folha de saída
	Ingresso	EPG	EPG de	Folha de consumo (folha não

			saída L3	fronteiriça)
	Ingresso	EPG de saída L3	EPG	Folha do provedor (folha fora da borda)
	Saída	EPG	EPG de saída L3	Borda leaf -> tráfego de folha não borda
	Saída	EPG de saída L3	EPG	·Se o endpoint de destino for aprendido: folha de borda ·Se o endpoint de destino não for aprendido: folha não borda Tráfego leaf-> border leaf ·Borda
	Entrada/saída	EPG de saída L3	EPG de saída L3	Folha de entrada*
	Entrada/saída	EPG	EPG	Folha de consumidor
	Entrada/saída	EPG	EPG de saída L3	Folha de consumo (folha não fronteiriça)
Inter-VRF	Entrada/saída	EPG de saída L3	EPG	Folha de entrada*
	Entrada/saída	EPG de saída L3	EPG de saída L3	Folha de entrada*

*A aplicação da política é aplicada na primeira folha atingida pelo pacote.

Estes são exemplos:

- Se um endpoint externo no EPG L3Out no VRF1 tentar acessar um endpoint no EPG da Web no VRF1 e o VRF1 estiver configurado para o modo de imposição de entrada, o tráfego será redirecionado pela folha onde o endpoint no EPG da Web reside, independentemente da direção do contrato.
- Se um endpoint no EPG da Web do consumidor no VRF1 tentar acessar um endpoint no EPG do aplicativo do provedor no VRF1 e os endpoints forem aprendidos nos nós de folha do consumidor e do provedor, o tráfego será redirecionado pela folha de entrada.
- Se um endpoint no EPG da Web do consumidor no VRF1 tenta acessar um endpoint no EPG do aplicativo do provedor no VRF2, o tráfego é redirecionado pelo leaf do consumidor onde o endpoint do consumidor reside, independentemente do modo de aplicação do VRF.

3. Verifique se o tráfego é redirecionado para o nó de serviço

Quando o caminho de encaminhamento esperado estiver limpo, o ELAM poderá ser usado para verificar se o tráfego chega aos nós do switch e verificar a decisão de encaminhamento nos nós do switch. Consulte a seção "Ferramentas" no capítulo "Encaminhamento de estrutura interna" para obter instruções sobre como usar o ELAM.

Por exemplo, para rastrear o fluxo de tráfego na figura 'exemplo de caminho de encaminhamento de PBR - de consumidor para provedor', eles podem ser capturados para confirmar se o tráfego de consumidor para provedor é redirecionado.

- Porta de downlink na folha do consumidor para verificar 1 e 2 (o tráfego chega na folha do consumidor e o PBR é aplicado).
- Porta de malha em nós spine para verificar 3 (o tráfego vai para o proxy spine).
- Porta de malha na folha de serviço para verificação 4 (o tráfego chega na folha de serviço).

Em seguida, eles podem ser capturados para confirmar se o tráfego que volta do nó de serviço vai para o provedor.

- Porta downlink no leaf de serviço para verificar 5 e 6 (o tráfego volta do nó de serviço e é permitido).
- Porta de estrutura em nós spine para verificação 7 (o tráfego vai para a folha do provedor via spine).
- Porta de malha na folha do provedor para verificação 8 (o tráfego chega à folha do serviço e vai para o endpoint do provedor).

Note: Se o nó de consumidor e de serviço estiver sob a mesma folha, especifique uma interface ou MAC de origem além do IP de origem/destino para que o ELAM verifique 1 ou 5 na figura 'exemplo de caminho de encaminhamento PBR - do consumidor ao provedor' especificamente porque ambos usam o mesmo IP de origem e IP de destino.

Se o tráfego do consumidor para o provedor for redirecionado para o nó de serviço, mas não voltar para o leaf de serviço, verifique o seguinte, pois são erros comuns:

- A tabela de roteamento do nó de serviço alcança a sub-rede do provedor.
- A política de segurança do nó de serviço, como ACL, permite o tráfego.

Se o tráfego for redirecionado e chegar ao provedor, verifique o caminho do tráfego de retorno do provedor para o consumidor de maneira semelhante.

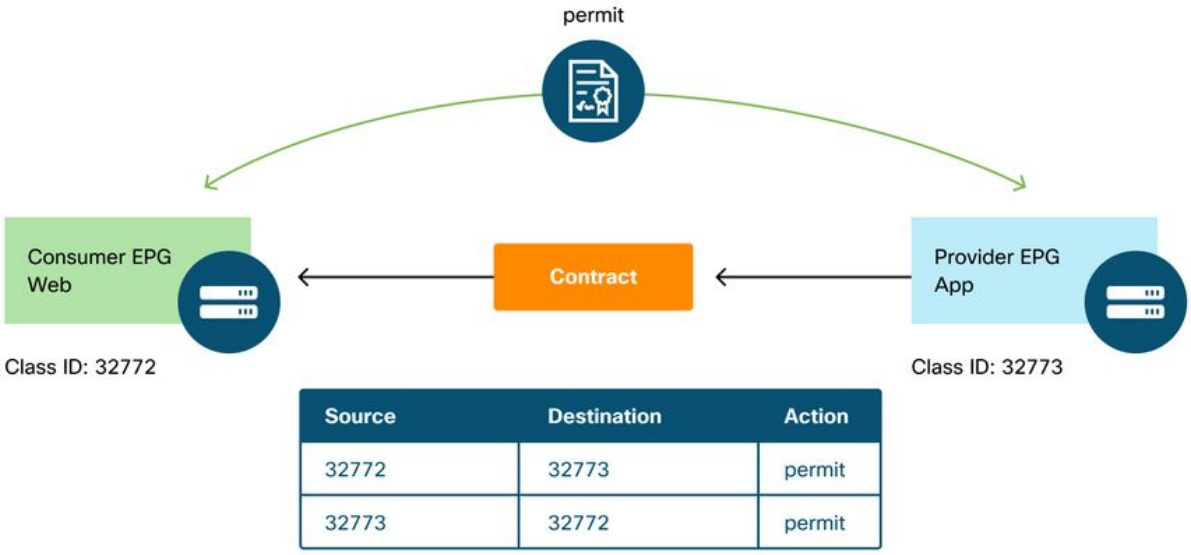
4. Verifique as políticas programadas nos nós de folha

Se o tráfego não for encaminhado ou redirecionado de acordo, a próxima etapa da solução de problemas será verificar as políticas programadas nos nós de folha. Esta seção mostra zoning-rule e contract_parser como exemplos. Para obter mais detalhes sobre como verificar as regras de zoneamento, consulte a seção "Ferramentas" no capítulo "Políticas de segurança".

Note: As políticas são programadas com base no status de implantação do EPG no leaf. A saída do comando show nesta seção usa o leaf que tem EPG de consumidor, EPG de provedor e EPGs para o nó de serviço.

Uso do comando 'show zoning-rule'

A figura e a saída de 'show zoning-rule' abaixo descrevem as regras de zoneamento antes da implantação do Gráfico de serviço.

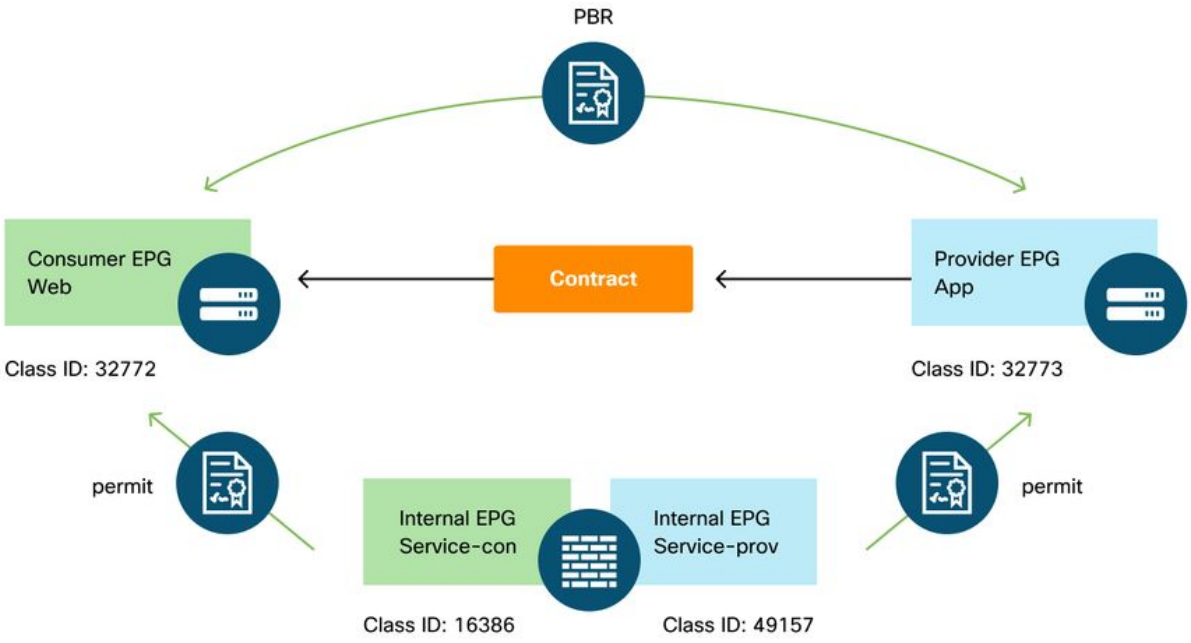


O ID de escopo do VRF pode ser encontrado em 'Locatário > Rede > VRF'.

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

Quando o Gráfico de serviços é implantado, os EPGs do nó de serviço são criados e as políticas são atualizadas para redirecionar o tráfego entre os EPGs do consumidor e do provedor. A figura abaixo e a saída de 'show zoning-rule' abaixo descrevem as regras de zoneamento após a implantação do gráfico de serviço. Neste exemplo, o tráfego de pcTag 32772 (Web) para pcTag 32773 (App) é redirecionado para 'destgrp-27' (lado do consumidor do nó de serviço) e o tráfego de pcTag 32773 (App) para pcTag 32772 (Web) é redirecionado para 'destgrp-28' (lado do provedor do nó de serviço).

Regras de zoneamento após a implantação do Gráfico de serviço



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

As informações de destino de cada desgrp podem ser encontradas usando o comando 'show service redir info'.

```
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
...
```

Se as regras de zoneamento forem programadas de acordo, mas o tráfego não for redirecionado ou encaminhado de acordo, verifique o seguinte, pois são erros comuns:

- Verifique se a ID da classe de origem ou de destino foi resolvida conforme esperado usando ELAM. Caso contrário, verifique qual é o ID de classe errado e os critérios de derivação do EPG, como o caminho e a VLAN encap.
- Mesmo que as IDs de classe de origem e destino sejam resolvidas de acordo, e a política de PBR seja aplicada, mas o tráfego não chegue no nó de PBR, verifique se o IP, o MAC e o VRF do desgrp na ação de redirecionamento ('show service redir info') estão corretos.

Por padrão, as regras de permissão de um EPG de consumidor para um nó de serviço (lado do consumidor) e de um EPG de provedor para um nó de serviço (lado do provedor) não são programadas se o PBR estiver ativado. Assim, um consumidor ou ponto final do provedor não pode se comunicar diretamente com o nó de serviço por padrão. Para permitir esse tráfego, a opção Direct Connect precisa ser habilitada. O caso de uso é explicado na seção "Outros exemplos de fluxo de tráfego**"**.

Uso de contract_parser

A ferramenta contract_parser também pode ajudar a verificar as políticas. O consumidor C é o lado do consumidor do nó de serviço e o provedor C é o lado do provedor do nó de serviço.

```
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]
...
```

Outros exemplos de fluxo de tráfego

Esta seção considera outros exemplos de fluxo de tráfego comum para identificar os fluxos desejados para a solução de problemas. Para obter as etapas de Troubleshooting, consulte o capítulo anterior desta seção.

1. Balanceador de carga sem SNAT: Neste exemplo, a Web do EPG do consumidor e o aplicativo EPG do provedor têm um contrato com um Gráfico de serviço de balanceador de carga. Os endpoints no App EPG são servidores reais associados ao VIP no balanceador de carga.O PBR para balanceador de carga está habilitado para o provedor para direção de tráfego de consumidor.
2. Firewall e balanceador de carga sem SNAT: Neste exemplo, a Web do EPG do consumidor e o aplicativo EPG do provedor têm um contrato com um firewall e um Gráfico de serviço de balanceador de carga. Os endpoints no App EPG são servidores reais associados ao VIP no balanceador de carga.PBR para firewall está habilitado para ambas as direções.O PBR para balanceador de carga está habilitado para o provedor para direção de tráfego de consumidor.
3. Serviço compartilhado (contrato Inter-VRF): Neste exemplo, a Web do EPG do consumidor e o aplicativo EPG do provedor têm um contrato com um gráfico de serviço de firewall. EPG Web e EPG App estão em VRFs diferentes.PBR para firewall está habilitado para ambas as direções.O firewall está entre VRFs.

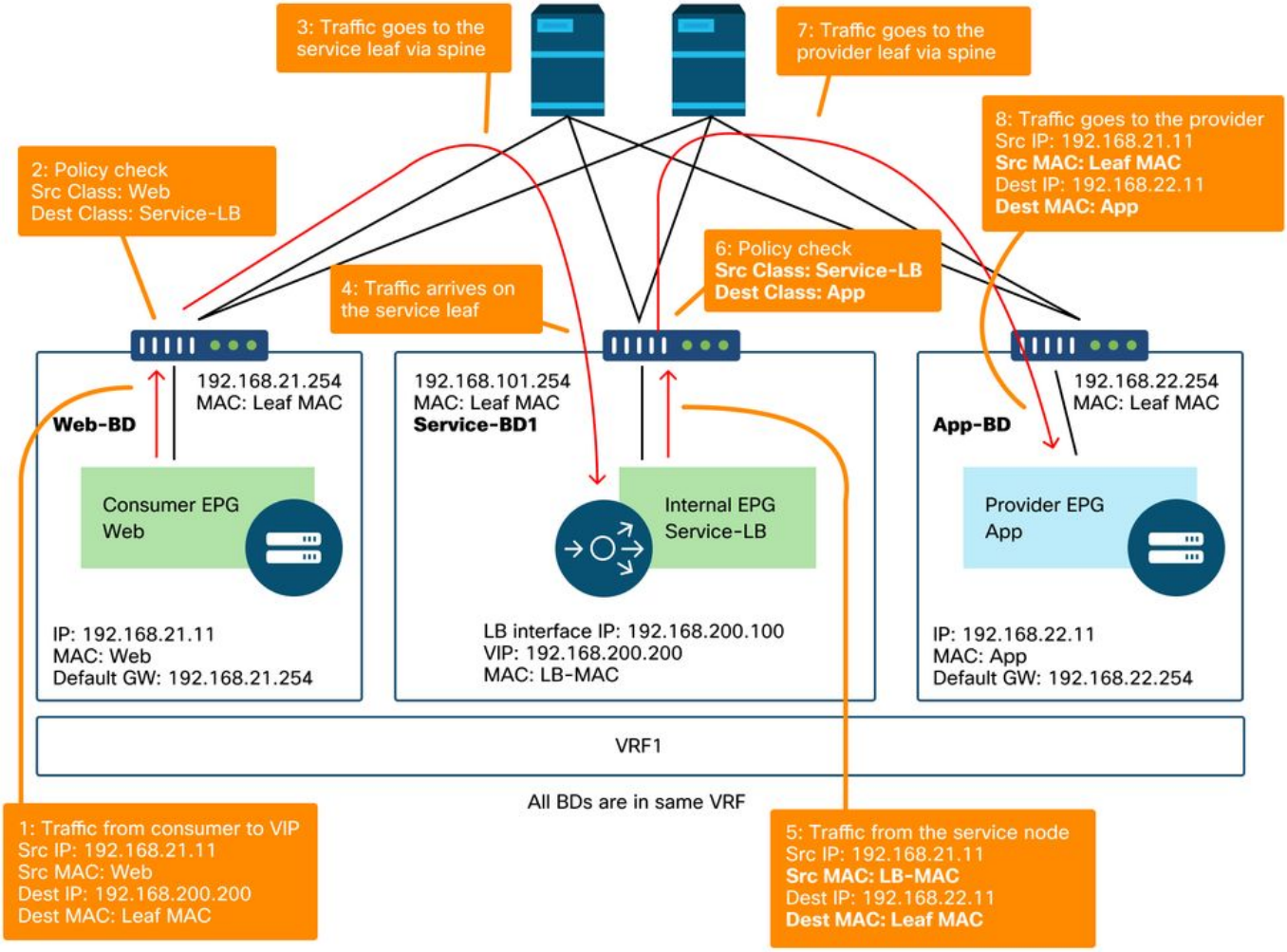
1. Balanceador de carga sem SNAT

O PBR pode ser implantado como PBR bidirecional ou PBR unidirecional. Um caso de uso do PBR unidirecional é a integração do balanceador de carga sem a conversão de endereço de rede (NAT) de origem. Se o balanceador de carga executar o NAT de origem, o PBR não será necessário.

Exemplo de caminho de tráfego

A figura abaixo ilustra um exemplo de um fluxo de tráfego de entrada da Web de EPG de consumidor para o aplicativo EPG de provedor com duas conexões: Um é de um ponto final na Web do EPG do consumidor para o VIP do balanceador de carga e o outro é do balanceador de carga para um ponto final no EPG do provedor. Como o tráfego de entrada é destinado ao VIP, o tráfego atingirá o balanceador de carga sem PBR se o VIP estiver acessível. O balanceador de carga altera o IP de destino para um dos pontos finais no EPG App associado ao VIP, mas não converte o IP de origem. Assim, o tráfego vai para o endpoint do provedor.

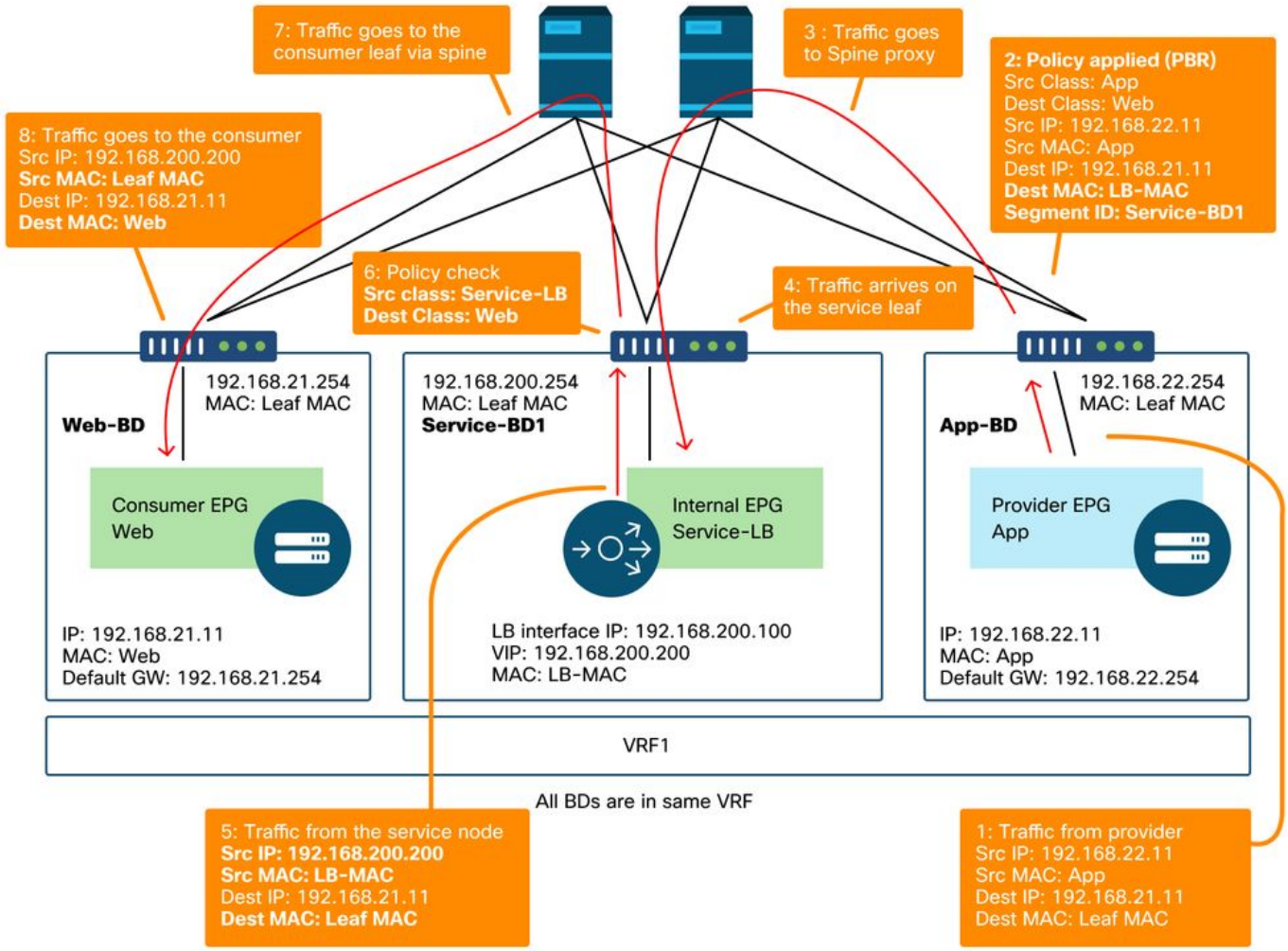
Exemplo de balanceador de carga sem caminho de encaminhamento SNAT — consumidor para VIP e balanceador de carga para provedor sem PBR



A figura abaixo ilustra o fluxo de tráfego de retorno do EPG App do provedor para o EPG Web do consumidor. Como o tráfego de retorno é destinado ao IP de origem original, o PBR precisa fazer o tráfego de retorno voltar ao balanceador de carga. Caso contrário, o ponto final do consumidor recebe o tráfego onde o IP de origem é o ponto final do provedor em vez do VIP. Esse tráfego será descartado porque o endpoint do consumidor não iniciou o tráfego para o endpoint do provedor, mesmo que a rede intermediária, como a estrutura da ACI, encaminhe o pacote de volta para o endpoint do consumidor.

Depois que o tráfego do ponto final do provedor para o ponto final do consumidor é redirecionado para o balanceador de carga, o balanceador de carga altera o IP de origem para o VIP. Em seguida, o tráfego volta do balanceador de carga e volta para o endpoint do consumidor.

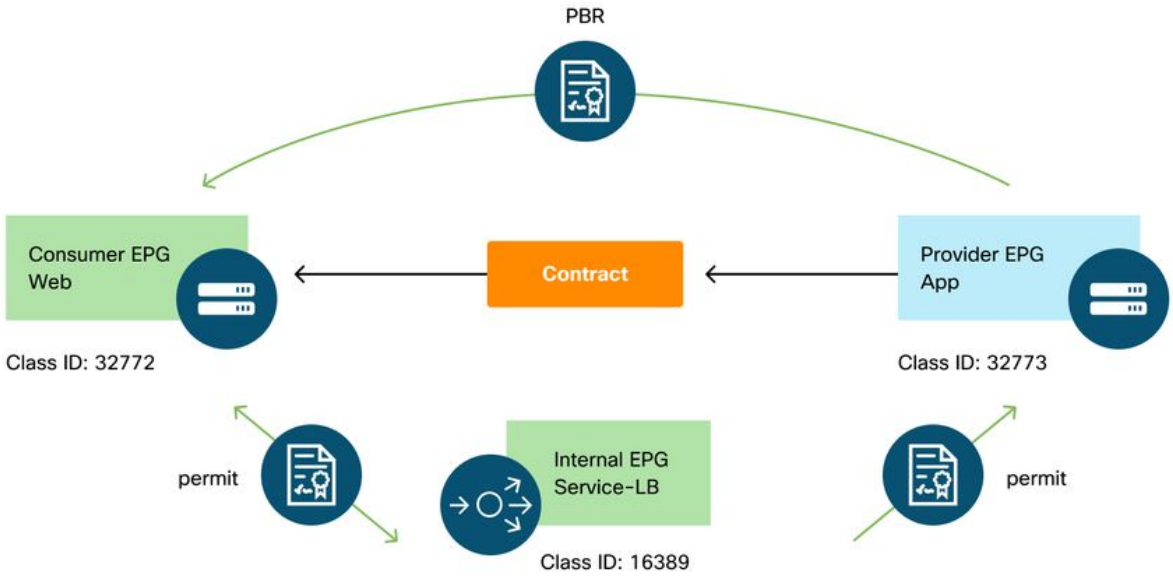
Exemplo de balanceador de carga sem caminho de encaminhamento SNAT - provedor para consumidor com PBR



As políticas programadas nos nós de folha.

A figura abaixo e a saída de 'show zoning-rule' abaixo descrevem as regras de zoneamento após a implantação do gráfico de serviço. Neste exemplo, o tráfego de pcTag 32772 (Web) para pcTag 16389 (Service-LB) é permitido, o tráfego de pcTag 16389 (Service-LB) para pcTag 32773 (App) é permitido e o tráfego de pcTag 32773 (App) para pcTag 32772 (Web) é redirecionado para 'destgrp-31' (balanceador de carga).

Regras de zoneamento após implantação do Gráfico de Serviço - balanceador de carga sem SNAT

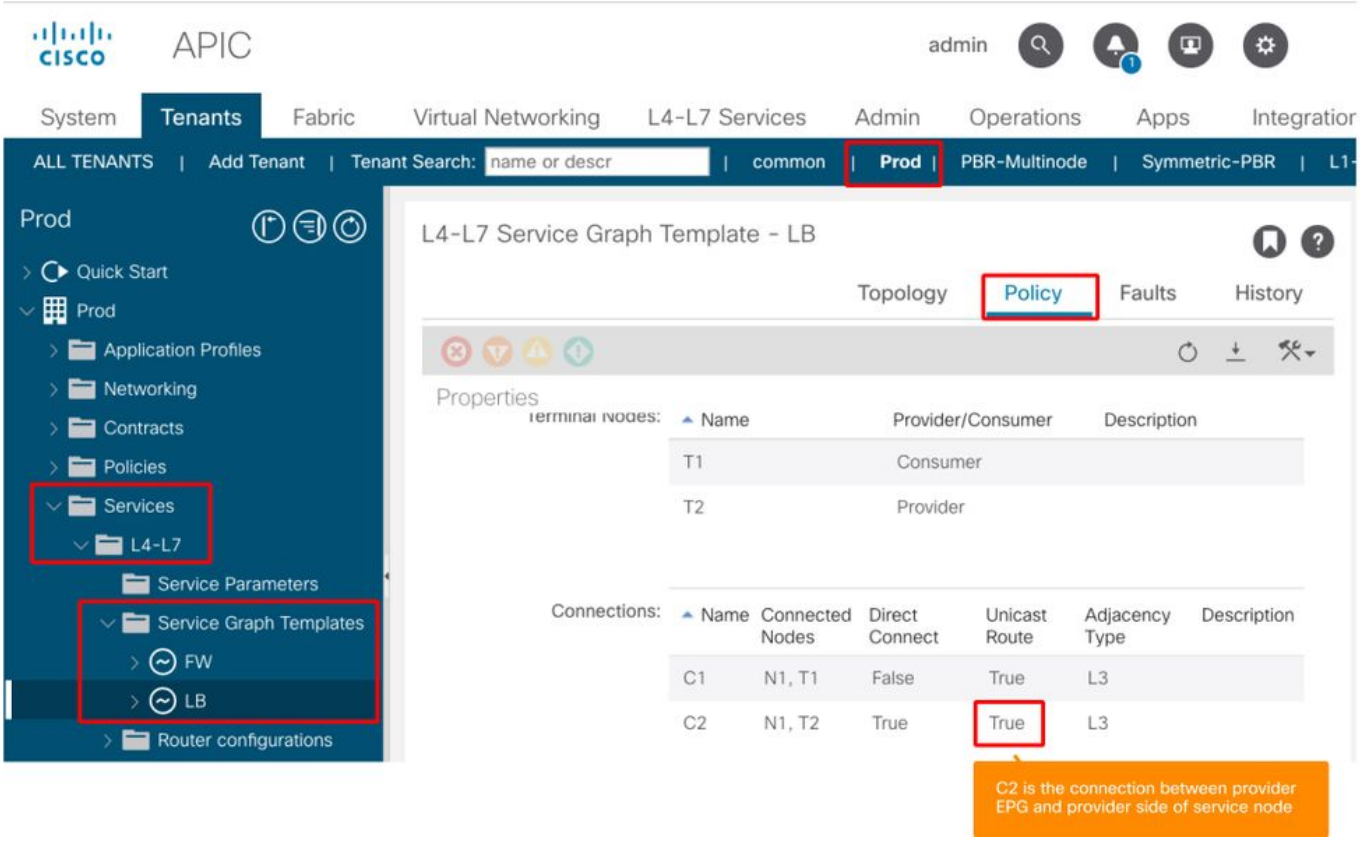


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
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)     |
...
```

Por padrão, uma regra de permissão para o provedor EPG (pcTag 32773) para Service-LB (pcTag 16389) não está programada. Para permitir a comunicação bidirecional entre eles para verificações de integridade do balanceador de carga para os pontos de extremidade do provedor, a opção Direct Connect na conexão deve ser definida como True. O local é 'Locatário > L4-L7 > Modelos de gráfico de serviço > Política'. O valor padrão é Falso.

Definir opção de conexão direta



Adiciona uma regra de permissão para o provedor EPG(32773) ao Service-LB(16389) conforme abaixo.

```
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. Exemplo de fluxo de tráfego - Firewall e balanceador de carga sem SNAT

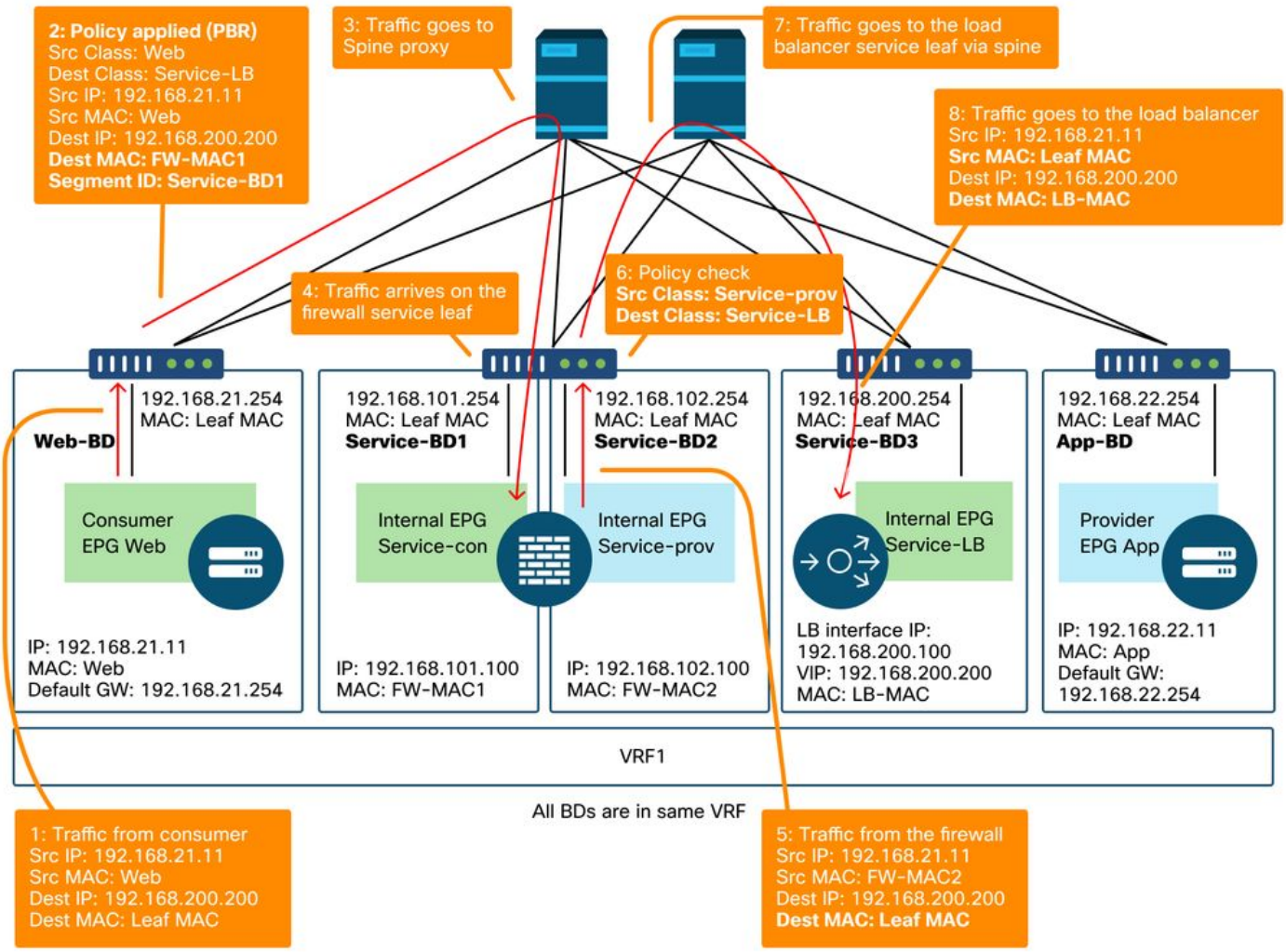
O PBR pode ser implantado com várias funções de serviço em um Gráfico de serviço, como firewall como primeiro nó e balanceador de carga como segundo nó.

Exemplo de caminho de tráfego

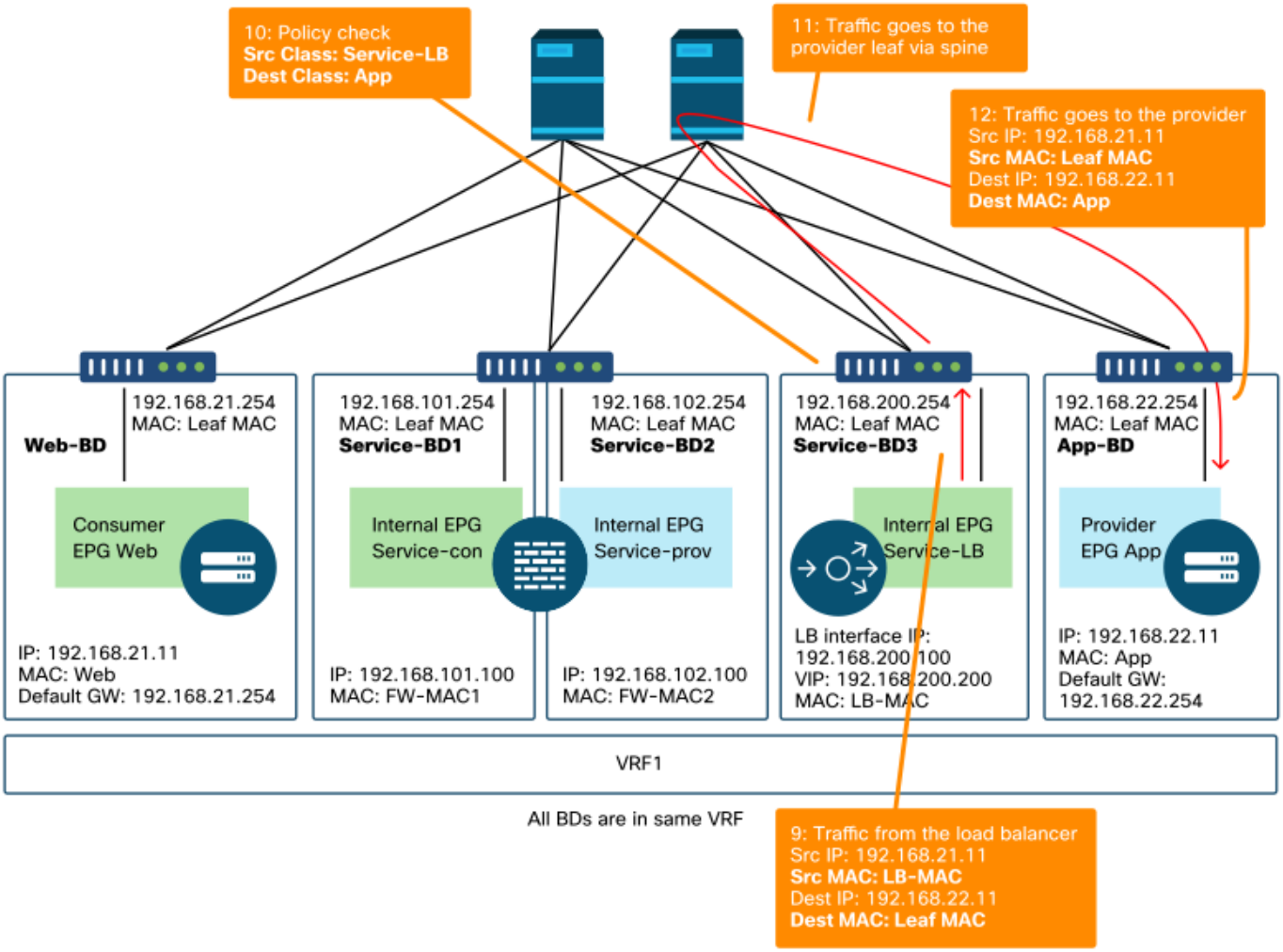
A figura abaixo ilustra um exemplo de um fluxo de tráfego de entrada da Web de EPG de consumidor para o aplicativo EPG de provedor com duas conexões: Um é de um ponto final na

Web do EPG do consumidor para o VIP do balanceador de carga via firewall e o outro é do balanceador de carga para um ponto final no EPG do provedor. O tráfego de entrada destinado ao VIP é redirecionado para o firewall e, em seguida, vai para o balanceador de carga sem PBR. O balanceador de carga altera o IP de destino para um dos pontos de extremidade no EPG do aplicativo associado ao VIP, mas não converte o IP de origem. Em seguida, o tráfego vai para o endpoint do provedor.

Firewall e balanceador de carga sem exemplo de caminho de encaminhamento SNAT - consumidor para VIP e balanceador de carga para provedor



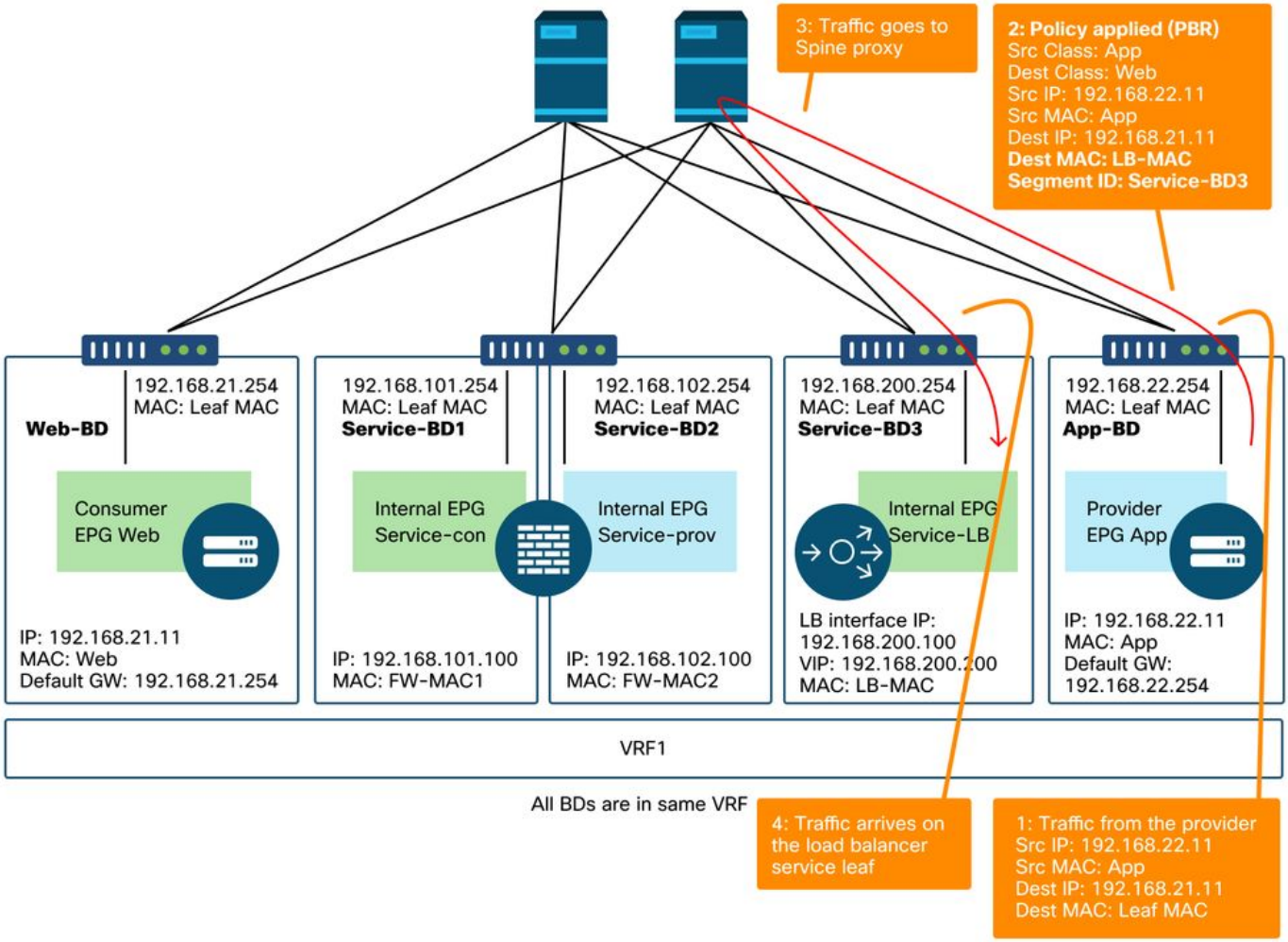
Firewall e balanceador de carga sem exemplo de caminho de encaminhamento SNAT - consumidor para VIP e balanceador de carga para provedor (continuação)

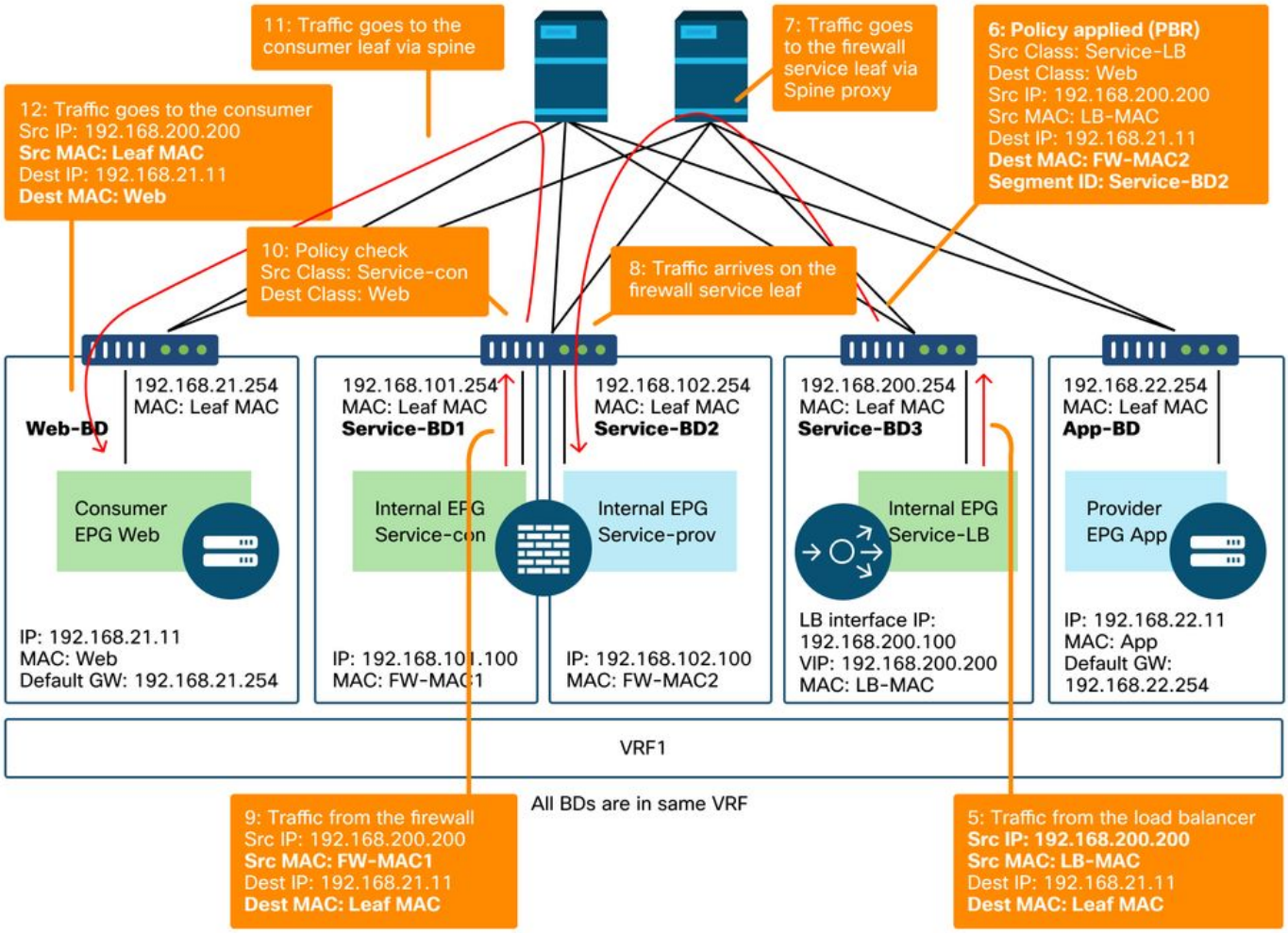


A figura abaixo ilustra o fluxo de tráfego de retorno do EPG App do provedor para o EPG Web do consumidor. Como o tráfego de retorno é destinado ao IP de origem original, o PBR é necessário para fazer o tráfego de retorno voltar ao balanceador de carga.

Depois que o tráfego do ponto final do provedor para o ponto final do consumidor é redirecionado para o balanceador de carga, o balanceador de carga altera o IP de origem para o VIP. O tráfego volta do balanceador de carga e é redirecionado para o firewall. Em seguida, o tráfego volta do firewall e volta para o endpoint do consumidor.

Firewall e balanceador de carga sem exemplo de caminho de encaminhamento SNAT - provedor para consumidor

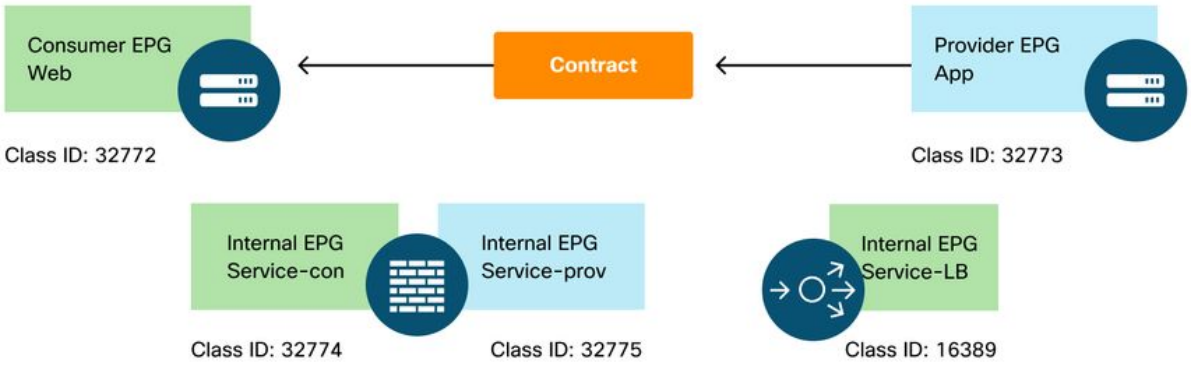

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



As políticas programadas nos nós de folha

A figura abaixo e a saída 'show zoning-rule' mostrada abaixo descrevem as regras de zoneamento após a implantação do Gráfico de serviço. Neste exemplo, o tráfego de pcTag 32772 (Web) para pcTag 16389 (Service-LB) é redirecionado para 'destgrp-32' (lado do consumidor do firewall), o tráfego de pcTag 32773 (App) para pcTag 32772 (Web) é redirecionado para 'destgrp-33' (balanceador de carga) e o tráfego de pcTag 16389 (Service-LB) para pcTag 32772 (Web) é redirecionado para 'destgrp-34' (lado do provedor do firewall).

Regras de zoneamento após implantação do Gráfico de serviço - firewall e balanceador de carga sem SNAT



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

No exemplo acima, a opção Direct Connect é definida como 'True' na conexão entre o lado do provedor do balanceador de carga e o EPG do provedor. Ele deve ser habilitado para verificação de integridade do balanceador de carga para pontos de extremidade de provedor. O local é 'Locatário > L4-L7 > Modelos de gráfico de serviço >Política'. Consulte a figura 'Definir opção de

conexão direta'.

3. Serviço compartilhado (Contrato Inter-VRF)

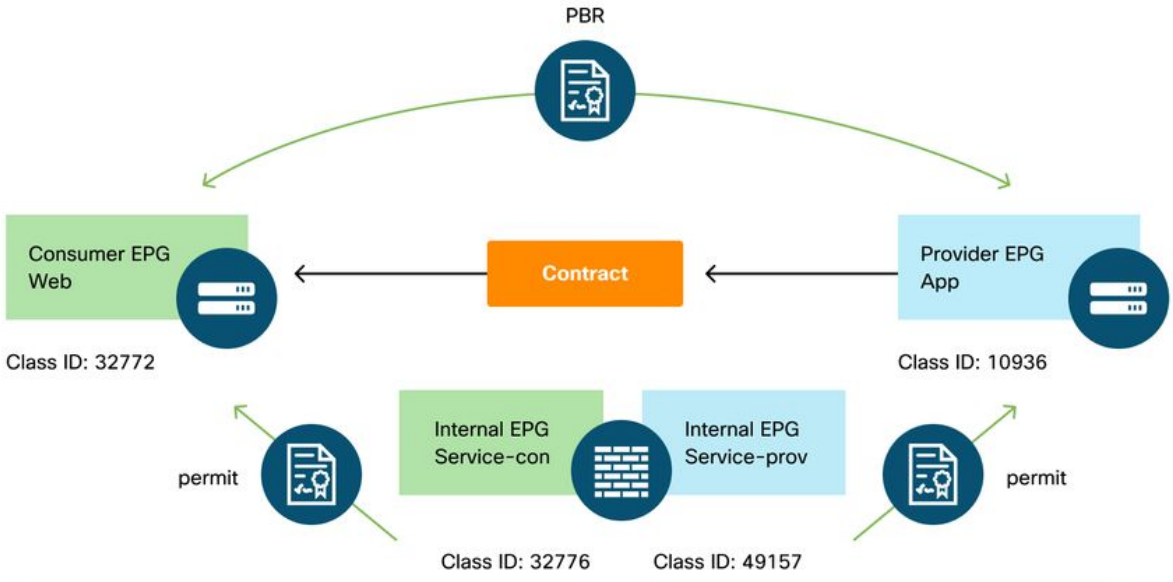
O PBR pode ser ativado no contrato entre VRF. Esta seção explica como as regras de zoneamento são programadas no caso de EPG para contrato EPG entre VRF.

As políticas programadas nos nós de folha

No caso de EPG para contrato EPG entre VRF, a política é sempre aplicada no VRF do consumidor. Assim, o redirecionamento acontece no VRF do consumidor. Para outras combinações, consulte a tabela "Onde a política é aplicada?" na seção "Encaminhamento".

A figura abaixo e a saída de 'show zoning-rule' abaixo descrevem as regras de zoneamento após a implantação do gráfico de serviço. Neste exemplo, o tráfego de pcTag 32772 (Web) para pcTag 10936 (App) é redirecionado para 'destgrp-36' (lado do consumidor do nó de serviço) e o tráfego de pcTag 10936 (App) para pcTag 32772 (Web) é redirecionado para 'destgrp-35' (lado do provedor do nó de serviço). Ambos são aplicados no VRF1, que é o VRF de consumidor. O tráfego do pcTag 32776 (lado do consumidor do firewall) para o pcTag 32772 (Web) é permitido no VRF1.

Regras de zoneamento após a implantação do Service Graph - contrato entre VRF



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

O tráfego do pcTag 49157 (lado do provedor do firewall) para o pcTag 10936 (App) é permitido no VRF2 porque ambos estão no VRF2.

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.