Solucionar problemas de redirección basada en políticas de ACI

Contenido

Introducción

Este documento describe los pasos para comprender y resolver problemas de un escenario de redirección basada en políticas (PBR) de ACI.

Antecedentes

El material de este documento se extrajo del libro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, específicamente los capítulos **Policy-Based Redirect - Overview, Policy-Based Redirect - Service Graph Deployment, Policy-Based Redirect - Forwarding** y Policy-Based Redirect - Other traffic flow samples.

Descripción general de la redirección basada en políticas

En este capítulo se explica la solución de problemas de Service Graph en modo no administrado con Policy-Based Redirect (PBR).

A continuación se indican los pasos típicos de solución de problemas. Este capítulo explica cómo verificar los pasos 2 y 3 que son específicos de PBR. Para los pasos 1 y 4, consulte los capítulos: "Reenvío dentro del fabric", "Reenvío externo" y "Políticas de seguridad".

1. Verifique que el tráfico funcione sin PBR Service Graph: Se detectan los terminales del proveedor y del consumidor.Los terminales del proveedor y del consumidor pueden comunicarse.
2. Compruebe que Service Graph está implementado: Las instancias de gráficos implementadas no tienen ningún error.Se implementan las VLAN y los ID de clase para el nodo de servicio.Se aprenden los extremos del nodo de servicio.
3. Compruebe la ruta de reenvío: La directiva de comprobación se programa en los nodos de hoja.Capture el tráfico en el nodo de servicio para confirmar si se redirige el tráfico.Capture el tráfico en la hoja de ACI para confirmar si el tráfico vuelve al fabric de ACI después de PBR.
4. Compruebe que el tráfico llega al terminal del proveedor y del consumidor, y que el terminal genera el tráfico de retorno.

Este documento no trata las opciones de diseño o configuración. Para obtener más información, consulte el "Informe técnico de ACI PBR" en Cisco.com

En este capítulo, el nodo de servicio y la hoja de servicio implican lo siguiente:

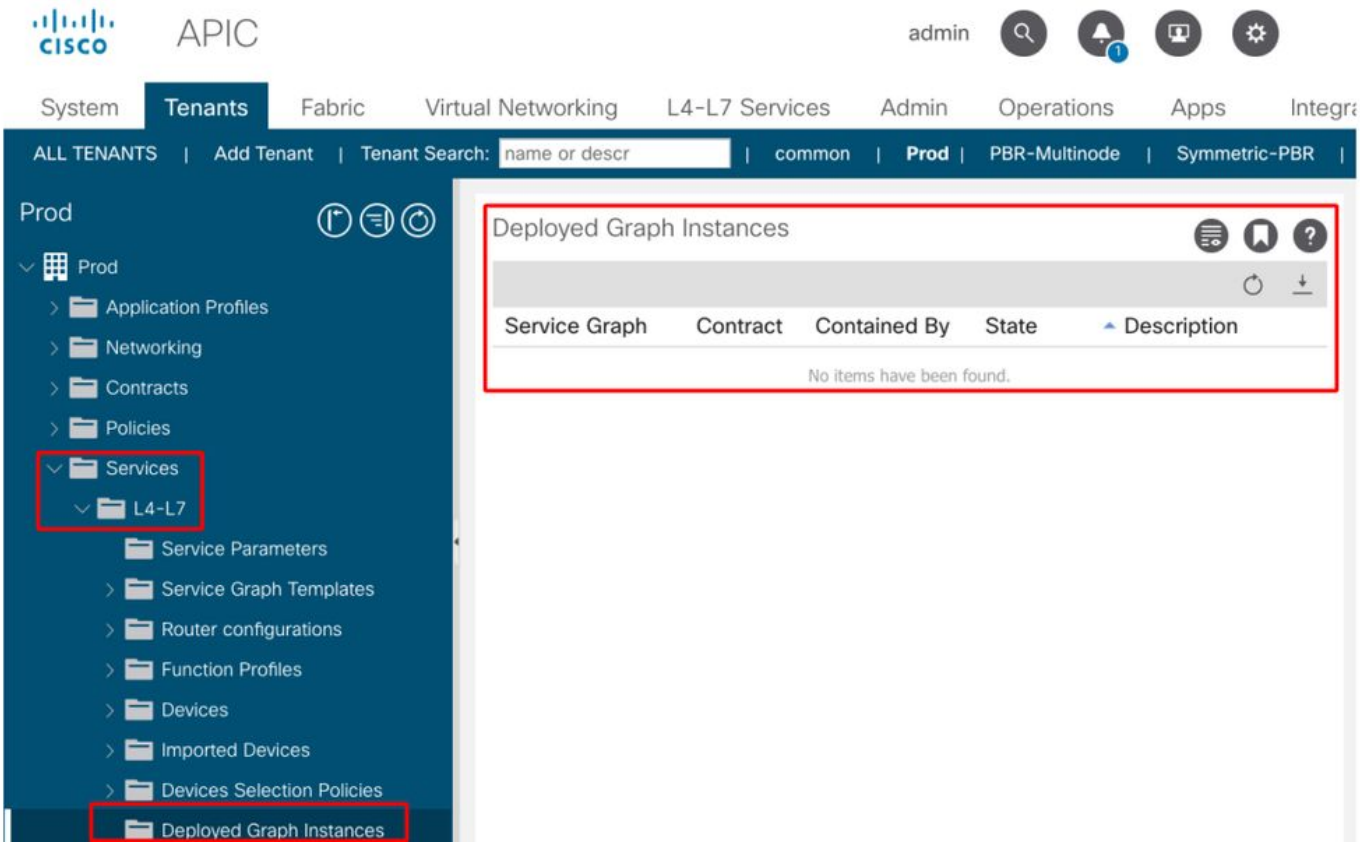
- Nodo de servicio: nodo externo al que PBR redirige el tráfico, como un firewall o un equilibrador de carga.
- Hoja de servicio: hoja de ACI conectada a un nodo de servicio.

Solución de problemas de Service Graph Deployment

En este capítulo se explica un ejemplo de solución de problemas en el que no se ha implementado un Service Graph.

Después de definir y aplicar una política de Service Graph a un asunto de contrato, debe aparecer una instancia de gráfico implementada en la GUI de ACI. La siguiente figura muestra el escenario de solución de problemas en el que el Gráfico de servicios no aparece como desplegado.

Service Graph no se muestra como instancia de gráfico desplegado.



1. Compruebe los pasos de configuración y el fallo

El primer paso de la localización de averías es comprobar que los componentes necesarios se han configurado sin ningún fallo. Se supone que las siguientes configuraciones generales ya se han realizado:

- VRF y BD para EPG de consumidor, EPG de proveedor y nodo de servicio
- El EPG del consumidor y del proveedor.
- El contrato y los filtros.

Cabe mencionar que no es necesario crear manualmente un EPG para el nodo de servicio. Se creará mediante la implementación de Service Graph.

Los pasos de configuración de Service Graph con PBR son los siguientes:

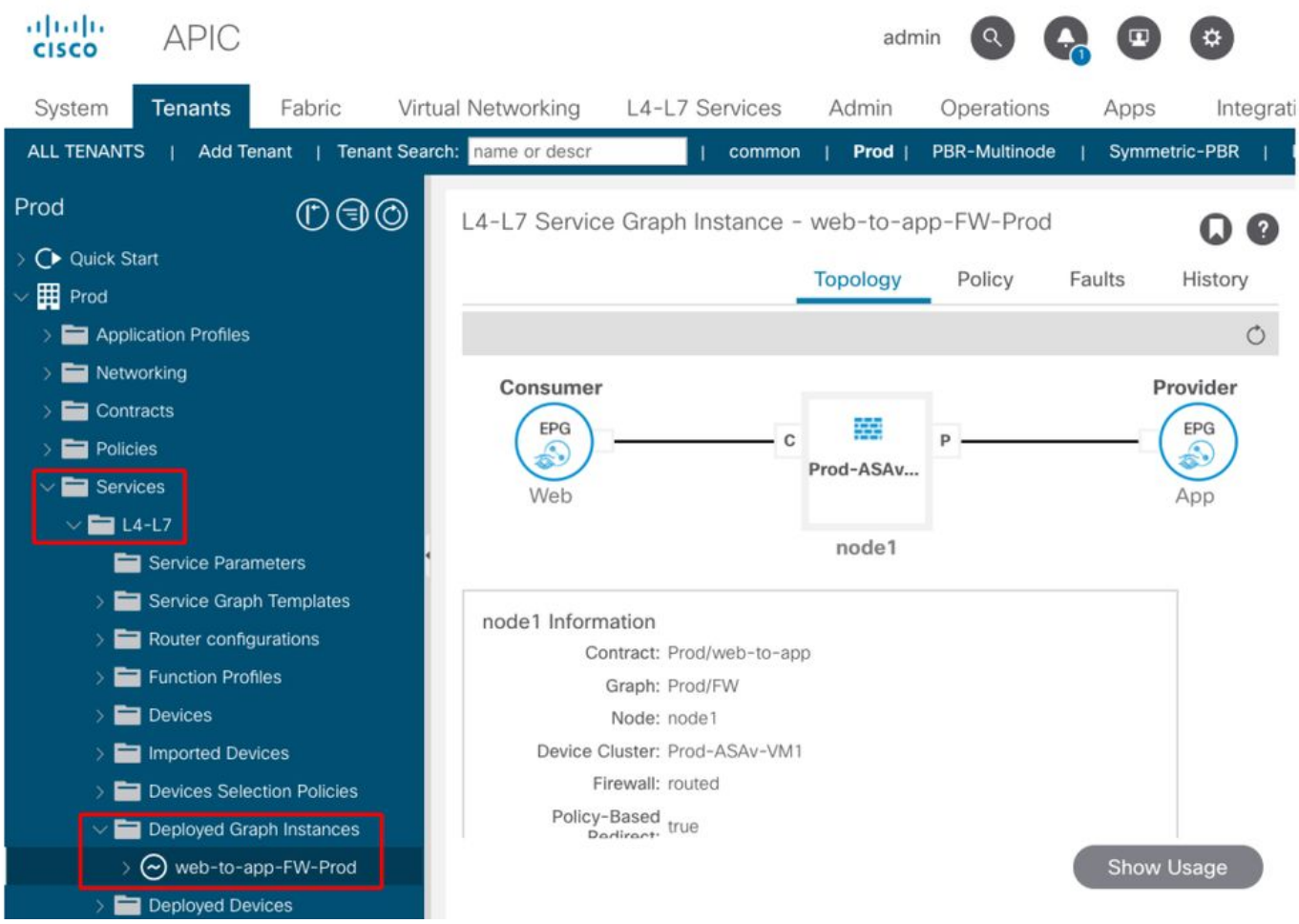
- Crear el dispositivo L4-L7 (dispositivo lógico).
- Cree el Service Graph.
- Cree la política PBR.
- Cree la directiva Selección de dispositivo.
- Asocie el Gráfico de servicios al asunto del contrato.

2. Compruebe la implementación de Service Graph en la interfaz de usuario

Después de asociar un gráfico de servicios al asunto del contrato, debe aparecer una instancia de gráfico desplegada para cada contrato con el gráfico de servicios (figura siguiente).

La ubicación es 'Arrendatario > Servicios > L4-L7 > Instancias de gráfico implementadas'

Instancia de gráfico desplegada



Si no aparece una instancia de gráfico desplegada, hay algún problema con la configuración del contrato. Las principales razones pueden ser:

- El contrato no tiene un EPG de consumidor o proveedor.
- El asunto del contrato no tiene ningún filtro.
- El alcance del contrato es VRF aunque sea para la comunicación entre VRF o EPG entre arrendatarios.

Si falla la instanciación de Service Graph, se producen errores en la instancia de Deployed Graph, lo que significa que hay algún problema con la configuración de Service Graph. Los errores típicos causados por la configuración son los siguientes:

F1690: La configuración no es válida debido a un error de asignación de ID

Este error indica que la VLAN encapsulada para el nodo de servicio no está disponible. Por ejemplo, no hay ninguna VLAN dinámica disponible en el grupo de VLAN asociada al dominio VMM utilizado en el dispositivo lógico.

Resolución: Verifique el conjunto de VLAN en el dominio utilizado para el dispositivo lógico. Verifique la VLAN encapsulada en la interfaz del dispositivo lógico si está en un dominio físico. Las ubicaciones son 'Arrendatario > Servicios > L4-L7 > Dispositivos y fabric > Políticas de acceso > Conjuntos > VLAN'.

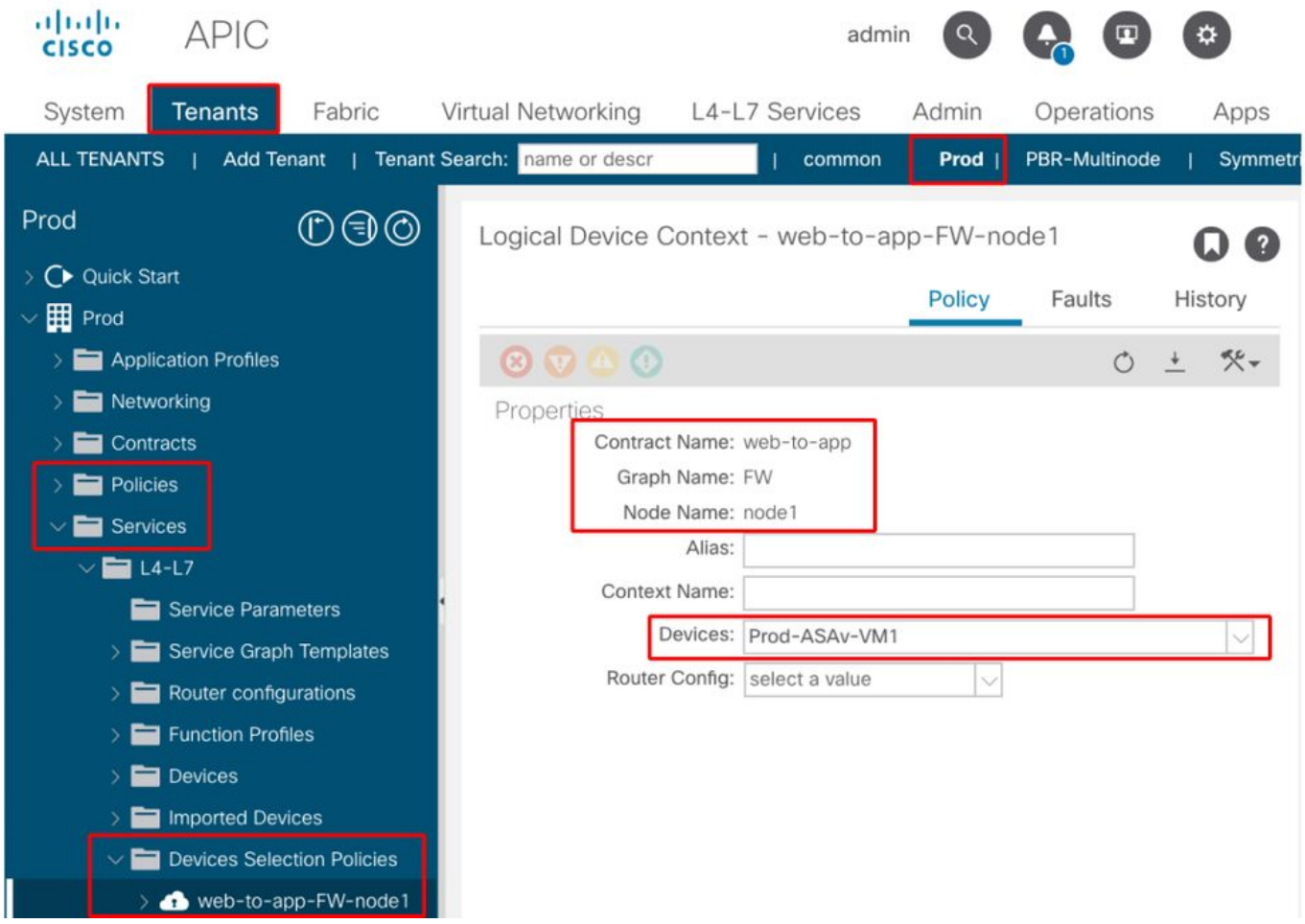
F1690: La configuración no es válida debido a que no se encontró contexto de dispositivo para LDev

Este error indica que no se puede encontrar el dispositivo lógico para la representación del gráfico

de servicios. Por ejemplo, no hay ninguna política de selección de dispositivos que coincida con el contrato de Service Graph.

Resolución: Compruebe que la directiva de selección de dispositivos está definida. La directiva de selección de dispositivos proporciona un criterio de selección para un dispositivo de servicio y sus conectores. Los criterios se basan en un nombre de contrato, un nombre de Service Graph y un nombre de nodo en Service Graph. La ubicación es 'Arrendatario > Servicios > L4-L7 > Política de selección de dispositivos'.

Comprobar directiva de selección de dispositivos



F1690: La configuración no es válida porque no se encontró ninguna interfaz de clúster

Este error indica que no se encuentra la interfaz de clúster para el nodo de servicio. Por ejemplo, la interfaz de clúster no se especifica en Directiva de selección de dispositivos.

Resolución: Compruebe que la interfaz del clúster está especificada en la directiva Selección de dispositivos y que el nombre del conector es correcto (Figura siguiente).

F1690: La configuración no es válida debido a que no se encontró BD

Este error indica que no se puede encontrar el BD para el nodo de servicio. Por ejemplo, el BD no se especifica en la política de selección de dispositivos.

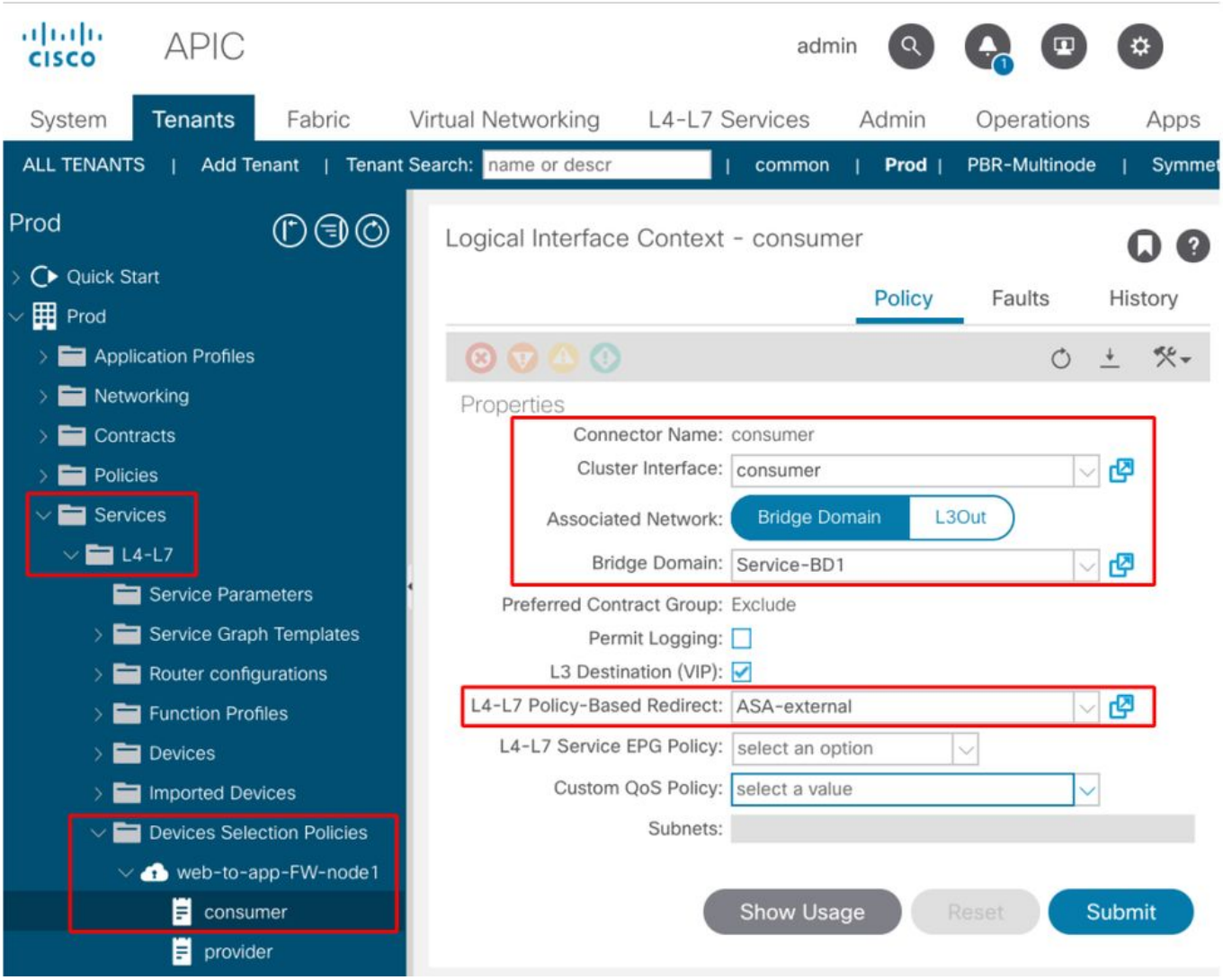
Resolución: Compruebe que BD está especificado en la política de selección de dispositivos y que el nombre del conector es correcto (figura siguiente).

F1690: La configuración no es válida debido a una política de redirección de servicios no válida

Este error indica que la política PBR no está seleccionada aunque la redirección esté habilitada en la función de servicio en el Gráfico de servicios.

Resolución: Seleccione la política PBR en la política de selección de dispositivos (Figura a continuación).

Configuración de interfaz lógica en la directiva de selección de dispositivos



Troubleshooting de PBR Forwarding

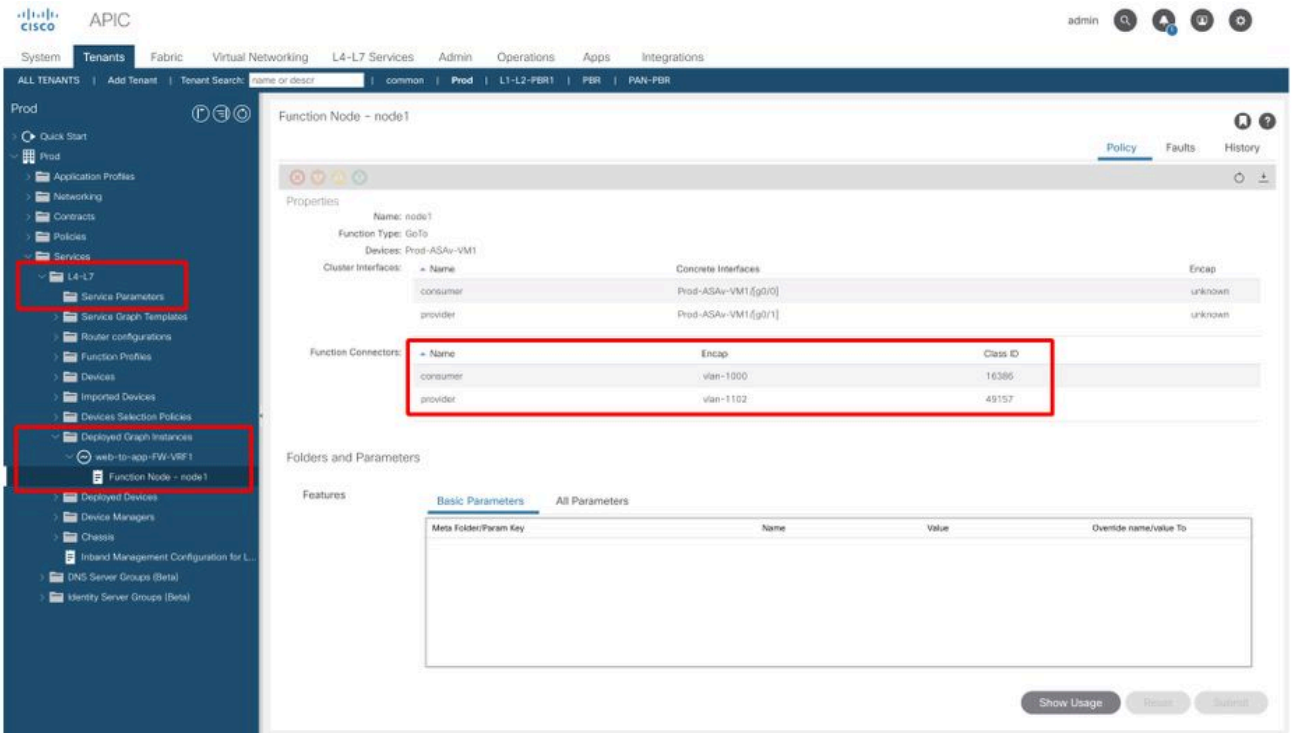
Este capítulo explica los pasos de troubleshooting para la trayectoria de reenvío PBR.

1. Verifique que las VLAN estén implementadas y que los terminales se aprendan en el nodo de hoja

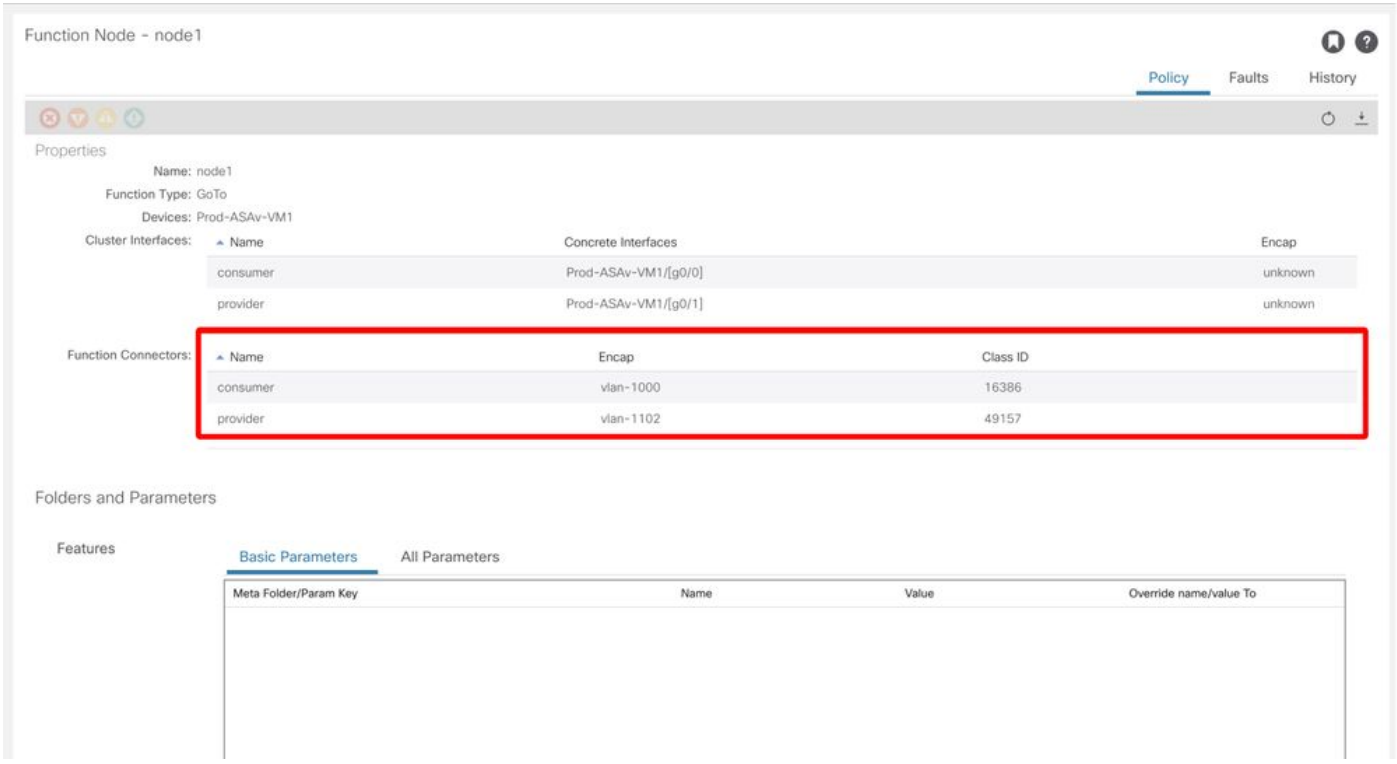
Una vez que se implementa correctamente un Service Graph sin ningún error, se crean los EPG y los BD para un nodo de servicio. La siguiente figura muestra dónde encontrar los ID de VLAN encapsuladas y los ID de clase de las interfaces de nodo de servicio (EPG de servicio). En este ejemplo, el lado del consumidor de un firewall es la clase ID 16386 con VLAN encap 1000 y el lado del proveedor de un firewall es la clase ID 49157 con VLAN encap 1102.

La ubicación es 'Arrendatario > Servicios > L4-L7 > Instancias de gráficos implementados > Nodos de función'.

Nodo de servicio



ID de clase de interfaz de nodo de servicio



Estas VLAN se implementan en las interfaces de nodo de hoja de servicio donde se conectan los nodos de servicio. La implementación de VLAN y el estado de aprendizaje del terminal se pueden comprobar mediante 'show vlan extended' y 'show endpoint' en la CLI del nodo de hoja de servicio.

```
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
```

Si las IP de los terminales de los nodos de servicio no se aprenden como terminales en el fabric de ACI, lo más probable es que se trate de un problema de conectividad o configuración entre la hoja de servicio y el nodo de servicio. Compruebe los siguientes estados:

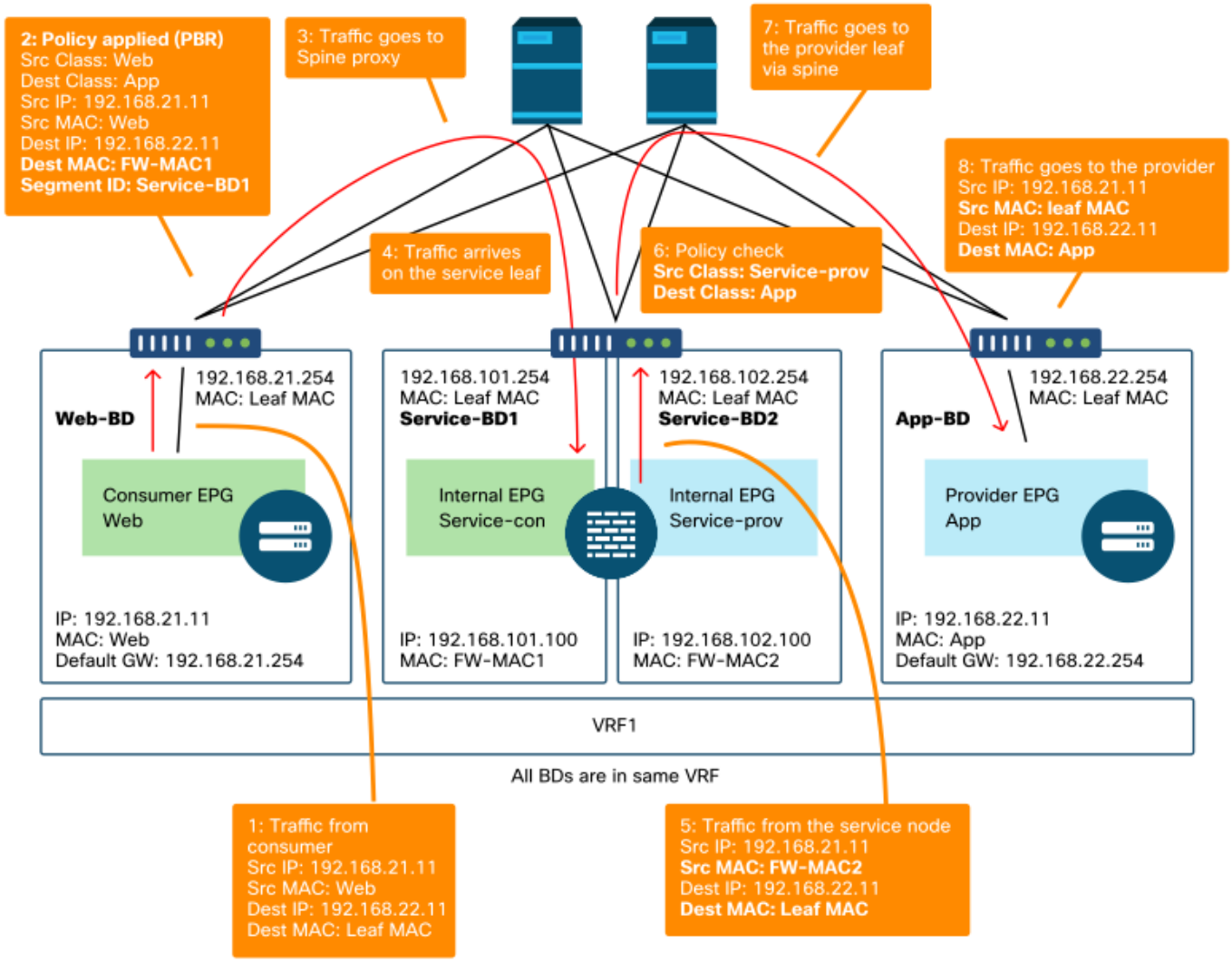
- El nodo de servicio está conectado al puerto de enlace descendente de hoja correcto. Si el nodo de servicio está en un dominio físico, la VLAN de extremo de ruta estática de hoja debe definirse en el dispositivo lógico.Si el nodo de servicio está en un dominio VMM, compruebe que el dominio VMM funciona y que el grupo de puertos creado mediante Service Graph está conectado correctamente a la máquina virtual del nodo de servicio.
- El puerto de enlace descendente de hoja conectado al nodo de servicio o al hipervisor donde reside la VM del nodo de servicio está ACTIVO.
- El nodo de servicio tiene la VLAN y la dirección IP correctas.
- El switch intermedio entre la hoja de servicio y el nodo de servicio tiene la configuración de VLAN correcta.

2. Compruebe las rutas de tráfico esperadas

Si el tráfico de extremo a extremo deja de funcionar una vez que PBR está habilitado, aunque los extremos del nodo de servicio se aprendan en el fabric ACI, el siguiente paso para solucionar problemas consiste en comprobar cuáles son las rutas de tráfico esperadas.

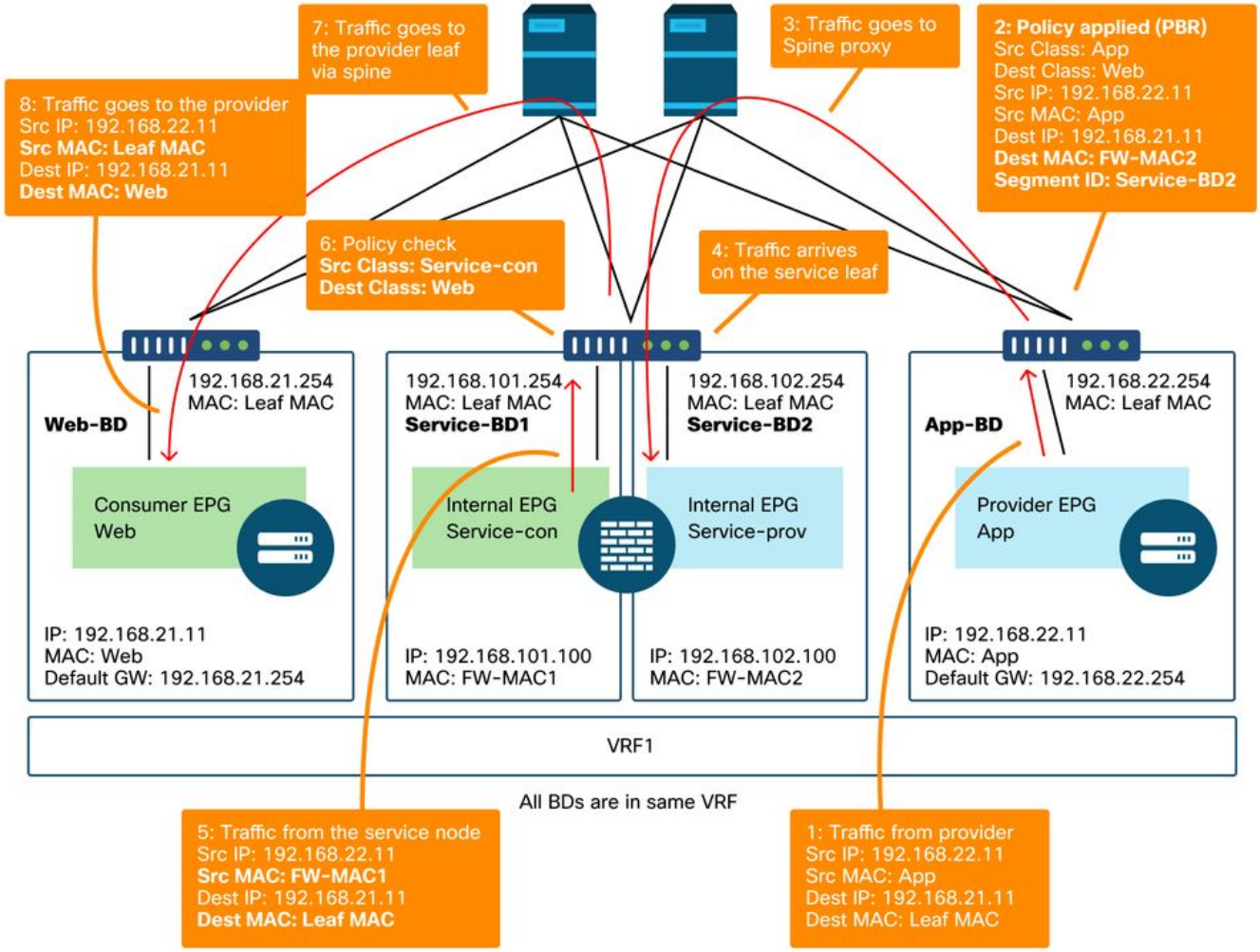
Las figuras 'Ejemplo de ruta de reenvío PBR - de consumidor a proveedor' y 'Ejemplo de ruta de reenvío PBR - de proveedor a consumidor' ilustran un ejemplo de ruta de reenvío de inserción de firewall mediante PBR entre un extremo de consumidor y un extremo de proveedor. Se supone que los extremos ya se aprenden en los nodos de hoja.

Ejemplo de ruta de reenvío PBR: de consumidor a proveedor



Nota: Dado que la MAC de origen no se cambia a MAC de hoja de ACI, el nodo PBR no debe utilizar el reenvío basado en MAC de origen si el terminal de consumidor y el nodo PBR no están en el mismo BD

Ejemplo de ruta de reenvío PBR: del proveedor al consumidor



Nota: Vale la pena mencionar que la política PBR se aplica en la hoja de consumidor o proveedor y lo que ACI PBR hace es la reescritura de MAC de destino, como se muestra en las figuras 'Ejemplo de ruta de reenvío PBR - consumidor a proveedor' y 'Ejemplo de ruta de reenvío PBR - proveedor a consumidor'. Al alcanzar la MAC de destino PBR siempre se utiliza un proxy de columna, incluso si el extremo de origen y la MAC de destino PBR están bajo la misma hoja.

Aunque las figuras 'Ejemplo de trayectoria de reenvío PBR - de consumidor a proveedor' y 'Ejemplo de trayectoria de reenvío PBR - de proveedor a consumidor' muestran un ejemplo de dónde se redirigiría el tráfico, donde la política se aplica depende de la configuración del contrato y del estado de aprendizaje del terminal. La tabla "Dónde se aplica la política" resume dónde se aplica la política en un único sitio de ACI. El lugar donde se aplica la política en varios sitios es diferente.

¿Dónde se aplica la política?

Situación	modo de aplicación VRF	Consumidor	Proveedor	Política aplicada el
Intra-VRF	Entrada/salida	EPG	EPG	·Si se descubre el terminal de destino: hoja de ingreso* ·Si no se aprende el punto final de destino: hoja de salida
	Acceso	EPG	L3Out EPG	Hoja de consumidor (hoja no fronteriza)

	Acceso	L3Out EPG	EPG	Hoja de proveedor (hoja no fronteriza)
	Egress	EPG	L3Out EPG	Tráfico de hoja fronterizo -> no fronterizo
	Egress	L3Out EPG	EPG	·Si se descubre el terminal de destino: hoja de borde ·Si no se aprende el punto final de destino: hoja no fronteriza Tráfico de hoja no fronterizo -> tráfico de hoja fronterizo
	Entrada/salida	L3Out EPG	L3Out EPG	·Hoja fronteriza Hoja de ingreso*
	Entrada/salida	EPG	EPG	Hoja de consumidor
	Entrada/salida	EPG	L3Out EPG	Hoja de consumidor (hoja no fronteriza)
Inter-VRF	Entrada/salida	L3Out EPG	EPG	Hoja de ingreso*
	Entrada/salida	L3Out EPG	L3Out EPG	Hoja de ingreso*

*La aplicación de políticas se aplica en la primera hoja que recibe el paquete.

Estos son ejemplos:

- Si un terminal externo en L3Out EPG en VRF1 intenta acceder a un terminal en Web EPG en VRF1 y VRF1 está configurado para el modo de aplicación de ingreso, el tráfico es redirigido por la hoja donde reside el terminal en Web EPG, independientemente de la dirección del contrato.
- Si un terminal en el Web EPG del consumidor en VRF1 intenta acceder a un terminal en el App EPG del proveedor en VRF1, y los terminales se aprenden en los nodos de hoja del consumidor y del proveedor, la hoja de ingreso redirige el tráfico.
- Si un terminal en el cliente Web EPG en VRF1 intenta acceder a un terminal en el proveedor App EPG en VRF2, el tráfico es redirigido por la hoja del consumidor donde reside el terminal del consumidor, independientemente del modo de aplicación VRF.

3. Compruebe si el tráfico se redirige al nodo de servicio

Una vez despejada la trayectoria de reenvío esperada, se puede utilizar ELAM para verificar si el tráfico llega a los nodos del switch y verificar la decisión de reenvío en los nodos del switch. Consulte la sección "Herramientas" en el capítulo "Reenvío dentro del fabric" para obtener instrucciones sobre cómo utilizar ELAM.

Por ejemplo, para rastrear el flujo de tráfico en la figura 'Ejemplo de trayectoria de reenvío PBR - de consumidor a proveedor', se pueden capturar para confirmar si el tráfico de consumidor a proveedor es redirigido.

- Puerto de enlace descendente en la hoja de consumidor para verificar 1 y 2 (el tráfico llega a la hoja de consumidor y se aplica PBR).
- Puerto de fabric en los nodos de columna para comprobar 3 (el tráfico va al proxy de columna).

- Puerto de fabric en la hoja de servicio para comprobar 4 (el tráfico llega a la hoja de servicio).

A continuación, se pueden capturar para confirmar si el tráfico que vuelve del nodo de servicio va al proveedor.

- Enlace descendente en la hoja de servicio para comprobar 5 y 6 (el tráfico vuelve del nodo de servicio y está permitido).
- Puerto de fabric en los nodos de columna para comprobar 7 (el tráfico va a la hoja del proveedor a través de la columna).
- Puerto del fabric en la hoja del proveedor para comprobar 8 (el tráfico llega a la hoja del servicio y va al terminal del proveedor).

Nota: Si el consumidor y el nodo de servicio están bajo la misma hoja, especifique una interfaz o MAC de origen además de la IP de origen/destino para tomar ELAM para verificar 1 o 5 en la figura 'Ejemplo de trayectoria de reenvío PBR - de consumidor a proveedor' específicamente porque ambos utilizan la misma IP de origen e IP de destino.

Si el tráfico de consumidor a proveedor se redirige al nodo de servicio pero no vuelve a la hoja de servicio, verifique lo siguiente, ya que son errores comunes:

- La tabla de routing del nodo de servicio alcanza la subred del proveedor.
- La política de seguridad del nodo de servicio, como ACL, permite el tráfico.

Si el tráfico se redirige y llega al proveedor, verifique la ruta de tráfico de retorno del proveedor al consumidor de manera similar.

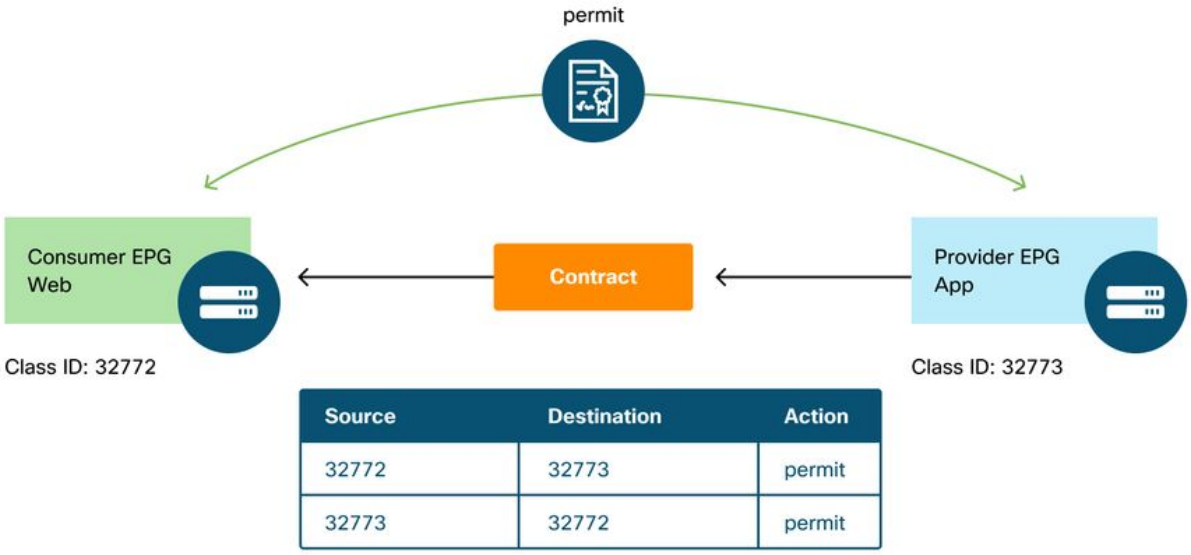
4. Compruebe las políticas programadas en los nodos de hoja

Si el tráfico no se reenvía o redirige en consecuencia, el siguiente paso de troubleshooting es verificar las políticas programadas en los nodos de hoja. Esta sección muestra zoning-rule y contract_parser como ejemplos. Para obtener más información sobre cómo comprobar las reglas de zonificación, consulte la sección "Herramientas" del capítulo "Políticas de seguridad".

Nota: Las políticas se programan en función del estado de implementación de EPG en la hoja. El resultado del comando show de esta sección utiliza la hoja que tiene EPG de consumidor, EPG de proveedor y EPG para el nodo de servicio.

Uso del comando 'show zoning-rule'

La figura y el resultado 'show zoning-rule' a continuación describen las reglas de zonificación antes de la implementación de Service Graph.

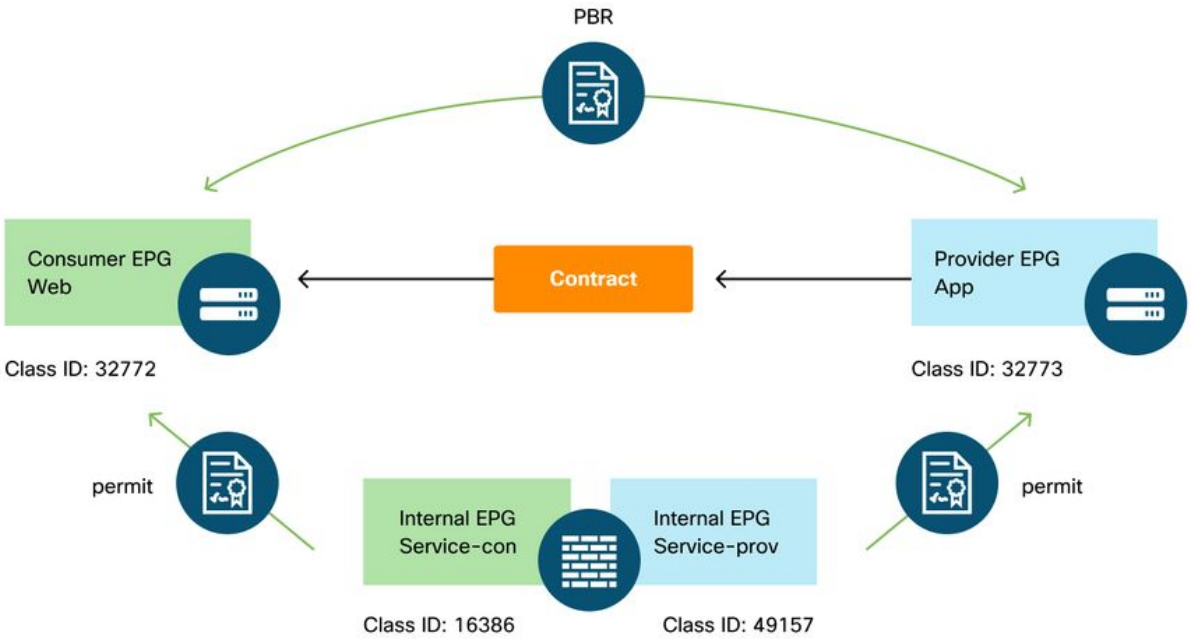


La ID de alcance de VRF se puede encontrar en 'Arrendatario > Redes > VRF'.

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

Una vez que se ha implementado Service Graph, se crean los EPG para el nodo de servicio y se actualizan las políticas para redirigir el tráfico entre los EPG del proveedor y del consumidor. La siguiente figura y el resultado 'show zoning-rule' describe las reglas de zonificación después de la implementación de Service Graph. En este ejemplo, el tráfico de pcTag 32772 (Web) a pcTag 32773 (App) se redirige a 'destgrp-27' (lado del consumidor del nodo de servicio) y el tráfico de pcTag 32773 (App) a pcTag 32772 (Web) se redirige a 'destgrp-28' (lado del proveedor del nodo de servicio).

Reglas de división en zonas tras la implementación de Service Graph



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

Puede encontrar la información de destino de cada escritorio mediante el 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
...
```

Si las reglas de zonificación se programan en consecuencia, pero el tráfico no se redirige o reenvía en consecuencia, verifique lo siguiente ya que son errores comunes:

- Verifique si el ID de clase de origen o de destino se resuelve como se esperaba mediante ELAM. Si no es así, verifique cuál es el ID de clase incorrecto y los criterios de derivación de EPG, como la VLAN de encapsulamiento y la ruta de acceso.
- Aunque los ID de clase de origen y destino se resuelven en consecuencia y se aplica la política PBR pero el tráfico no llega al nodo PBR, verifique que la IP, la MAC y el VRF del escritorio en la acción de redireccionamiento ('show service redir info') sean correctos.

De forma predeterminada, las reglas de permiso para un EPG de consumidor a un nodo de servicio (lado de consumidor) y un EPG de proveedor a un nodo de servicio (lado de proveedor) no se programan si PBR está habilitado. Por lo tanto, un extremo de consumidor o proveedor no puede comunicarse directamente con el nodo de servicio de forma predeterminada. Para permitir este tráfico, es necesario activar la opción Conexión directa. El caso práctico se explica en la sección "Otros ejemplos de flujo de tráfico".

Uso de contract_parser

La herramienta contract_parser también puede ayudar a verificar las políticas. C-consumer es el lado consumidor del nodo de servicio y C-provider es el lado proveedor del nodo de servicio.

```
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]
```

...

Otros ejemplos de flujo de tráfico

Esta sección considera otros ejemplos comunes de flujo de tráfico para identificar los flujos deseados para la resolución de problemas. Para conocer los pasos de resolución de problemas, consulte el capítulo anterior de esta sección.

1. Equilibrador de carga sin SNAT: En este ejemplo, la Web de EPG del consumidor y la aplicación de EPG del proveedor tienen un contrato con un Service Graph del equilibrador de carga. Los terminales en App EPG son servidores reales asociados al VIP en el equilibrador de carga.El equilibrador de carga PBR está habilitado para la dirección del tráfico de proveedor a consumidor.
2. Firewall y equilibrador de carga sin SNAT: En este ejemplo, la Web de EPG del consumidor y la aplicación de EPG del proveedor tienen un contrato con un firewall y un Service Graph del equilibrador de carga. Los terminales en App EPG son servidores reales asociados con el equilibrador de carga VIP on.PBR a firewall está habilitado para ambas direcciones.El equilibrador de carga PBR está habilitado para la dirección del tráfico de proveedor a consumidor.
3. Servicio compartido (contrato Inter-VRF): En este ejemplo, la Web de EPG del consumidor y la aplicación de EPG del proveedor tienen un contrato con un Service Graph del firewall. EPG Web y EPG App se encuentran en diferentes VRF.PBR a firewall está habilitado para ambas direcciones.El firewall está entre los VRF.

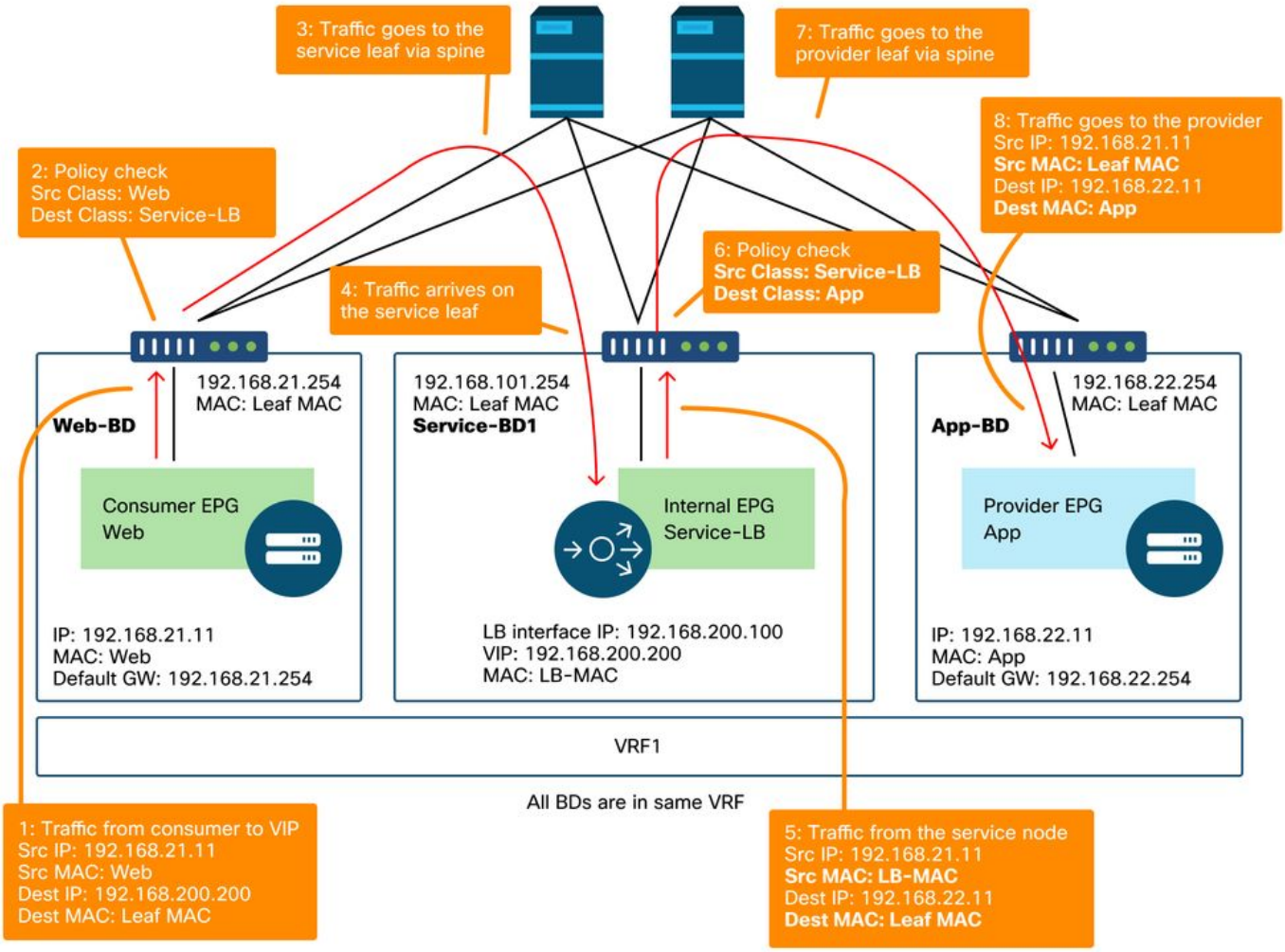
1. Equilibrador de carga sin SNAT

PBR se puede implementar como PBR bidireccional o PBR unidireccional. Un caso práctico de PBR unidireccional es la integración del equilibrador de carga sin traducción de direcciones de red (NAT) de origen. Si el balanceador de carga realiza la NAT de origen, no se requiere PBR.

Ejemplo de trayecto de tráfico

La siguiente figura ilustra un ejemplo de un flujo de tráfico entrante desde la Web de EPG de consumidor a la aplicación de EPG de proveedor con dos conexiones: Uno va desde un terminal en la Web EPG del consumidor al VIP del equilibrador de carga, y el otro va desde el equilibrador de carga a un terminal en la aplicación EPG del proveedor. Debido a que el tráfico entrante está destinado al VIP, el tráfico alcanzará el equilibrador de carga sin PBR si el VIP es alcanzable. El equilibrador de carga cambia la IP de destino a uno de los terminales de la aplicación EPG asociado al VIP, pero no traduce la IP de origen. En consecuencia, el tráfico va al terminal del proveedor.

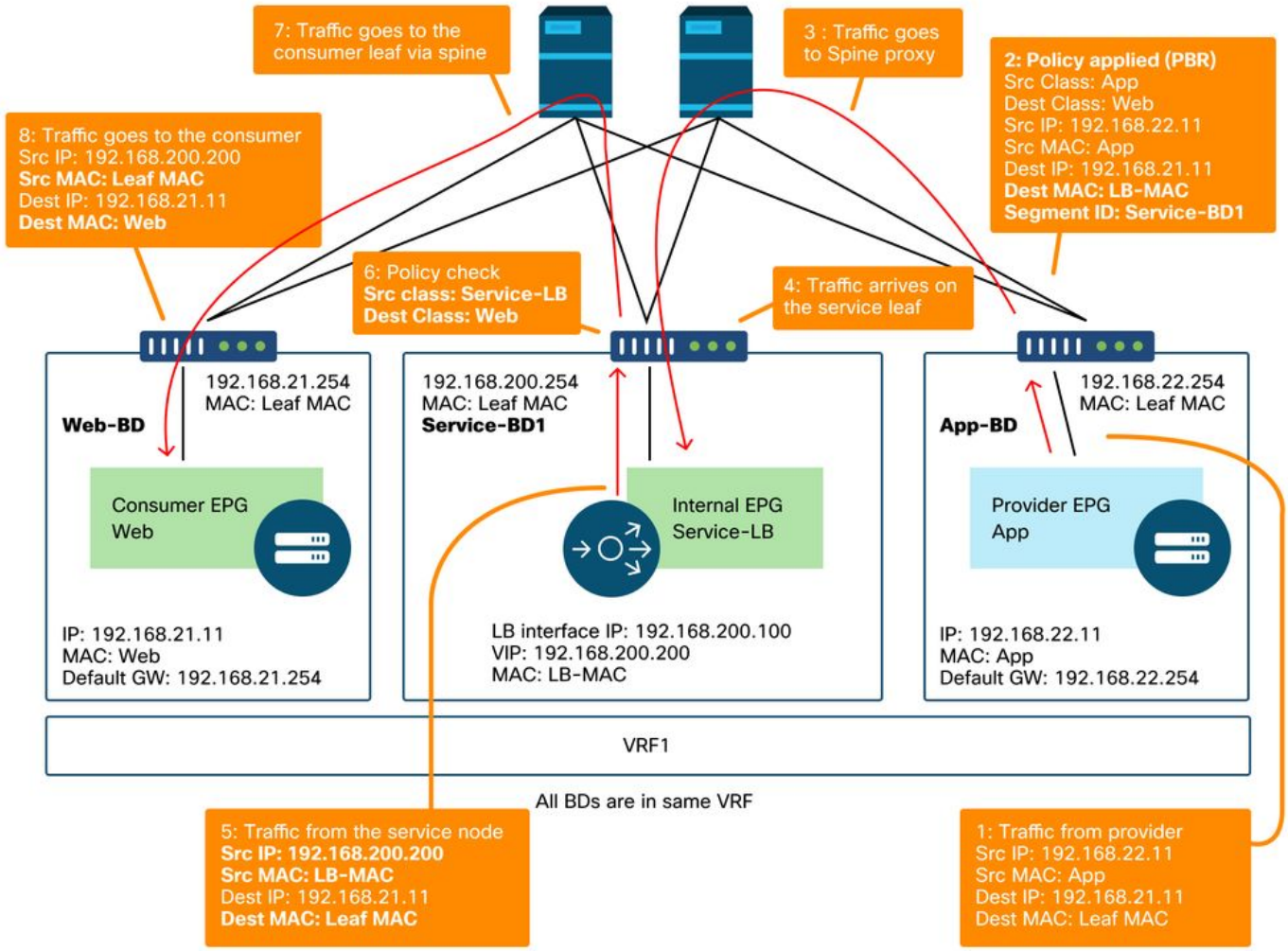
Ejemplo de equilibrador de carga sin ruta de reenvío SNAT: de consumidor a VIP y equilibrador de carga a proveedor sin PBR



La siguiente figura ilustra el flujo de tráfico de retorno desde la aplicación EPG del proveedor a la Web EPG del consumidor. Debido a que el tráfico de retorno está destinado a la IP de origen original, se requiere PBR para que el tráfico de retorno regrese al equilibrador de carga. De lo contrario, el extremo de consumidor recibe el tráfico donde la IP de origen es el extremo del proveedor en lugar del VIP. Este tráfico se descartará porque el terminal del consumidor no inició el tráfico al terminal del proveedor, incluso si la red intermedia, como el fabric de ACI, reenvía el paquete al terminal del consumidor.

Después de que el tráfico del extremo del proveedor al extremo del consumidor se redirige al equilibrador de carga, el equilibrador de carga cambia la IP de origen al VIP. Luego, el tráfico regresa del equilibrador de carga y el tráfico regresa al punto final del consumidor.

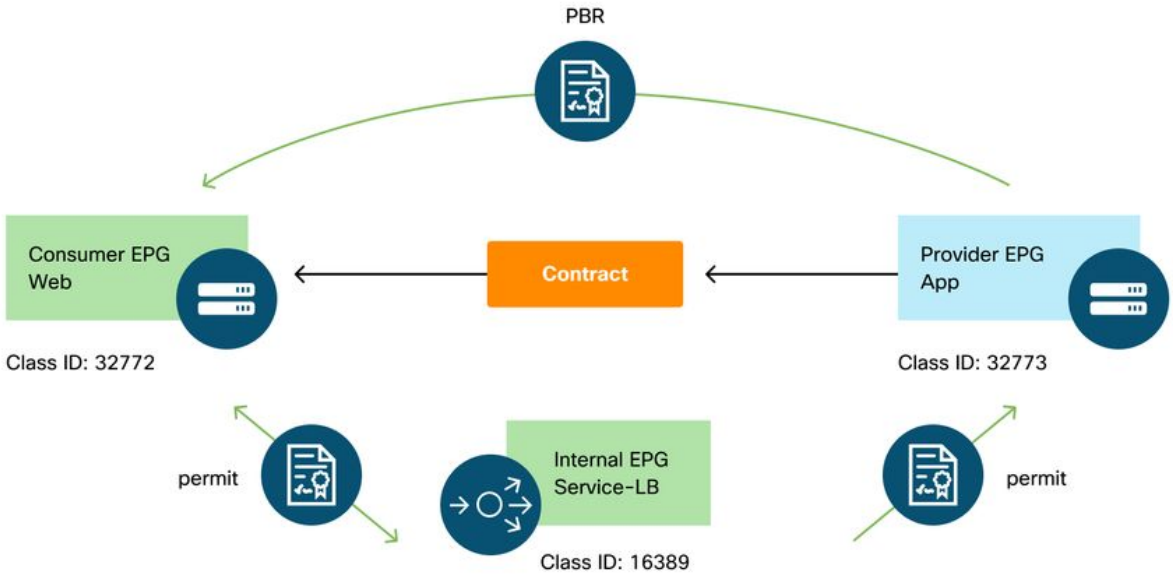
Ejemplo de equilibrador de carga sin ruta de reenvío SNAT: de proveedor a consumidor con PBR



Las políticas programadas en los nodos de hoja.

La siguiente figura y el resultado 'show zoning-rule' a continuación describen las reglas de zonificación después de la implementación de Service Graph. En este ejemplo, se permite el tráfico de pcTag 32772 (Web) a pcTag 16389 (Service-LB), se permite el tráfico de pcTag 16389 (Service-LB) a pcTag 32773 (App) y se redirige el tráfico de pcTag 32773 (App) a pcTag 32772 (Web) a 'destgrp-31' (equilibrador de carga).

Reglas de zonificación después de la implementación de Service Graph: equilibrador de carga sin SNAT

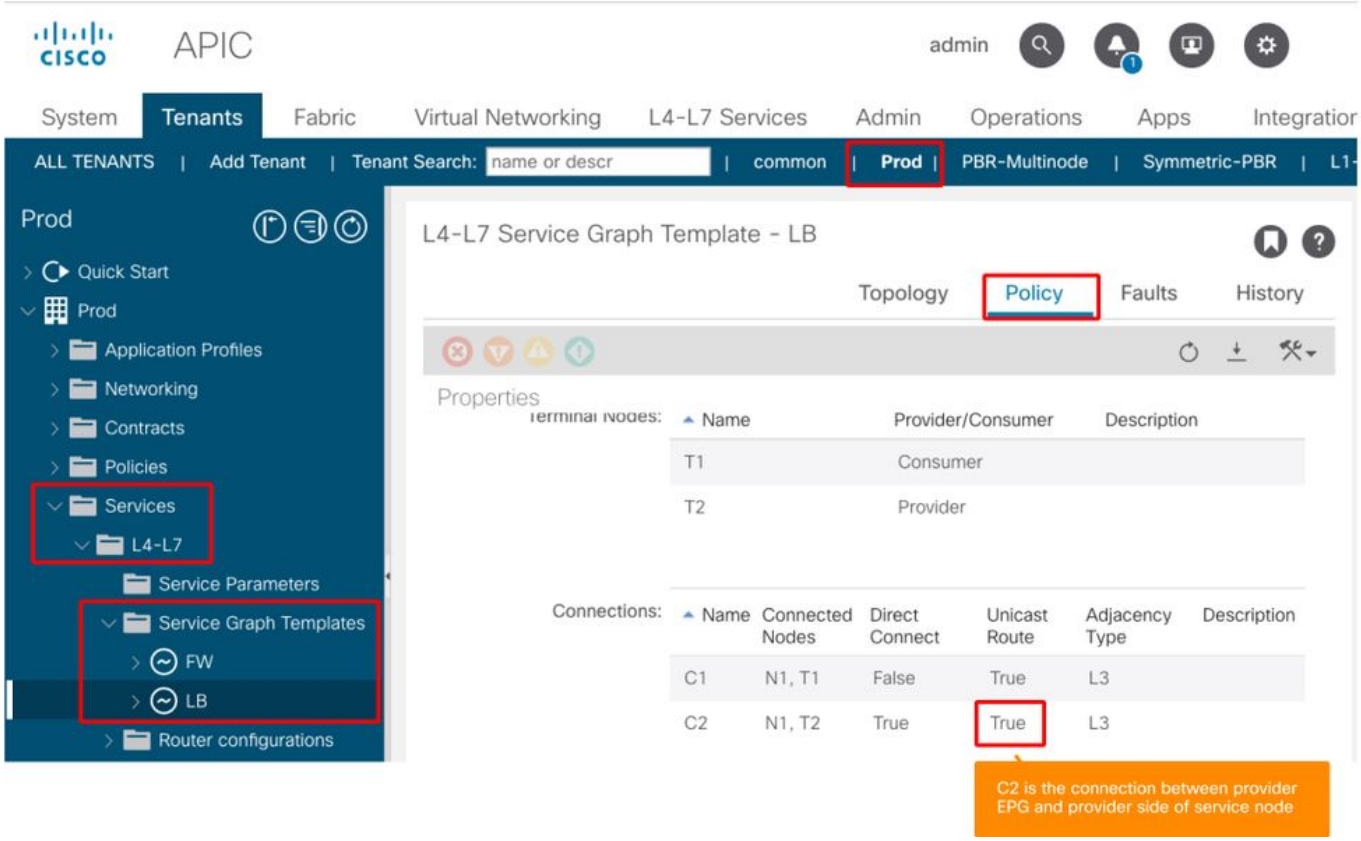


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
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)     |
...
```

De forma predeterminada, una regla de permiso para el proveedor EPG (pcTag 32773) a Service-LB (pcTag 16389) no está programada. Para permitir la comunicación bidireccional entre ellos para las comprobaciones de estado del equilibrador de carga a los extremos del proveedor, la opción Conexión directa de la conexión debe establecerse en True. La ubicación es 'Arrendatario > L4-L7 > Plantillas de Service Graph > Política'. El valor predeterminado es False.

Establecer la opción Conexión directa



Agrega una regla de permiso para el proveedor EPG(32773) a Service-LB(16389) como se muestra a continuación.

```
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. Ejemplo de flujo de tráfico: firewall y equilibrador de carga sin SNAT

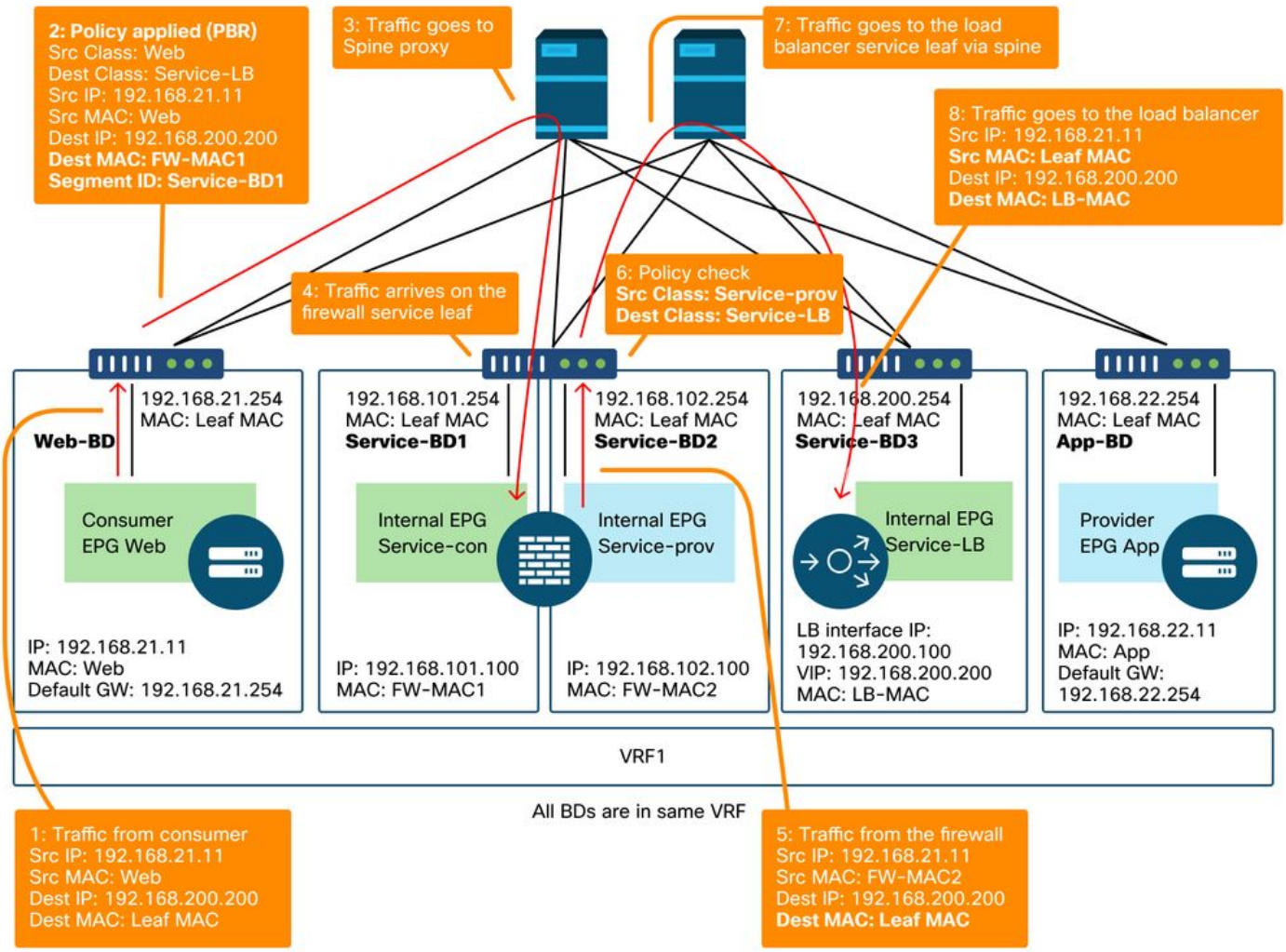
PBR se puede implementar con varias funciones de servicio en un Service Graph, como firewall como primer nodo y equilibrador de carga como segundo nodo.

Ejemplo de trayecto de tráfico

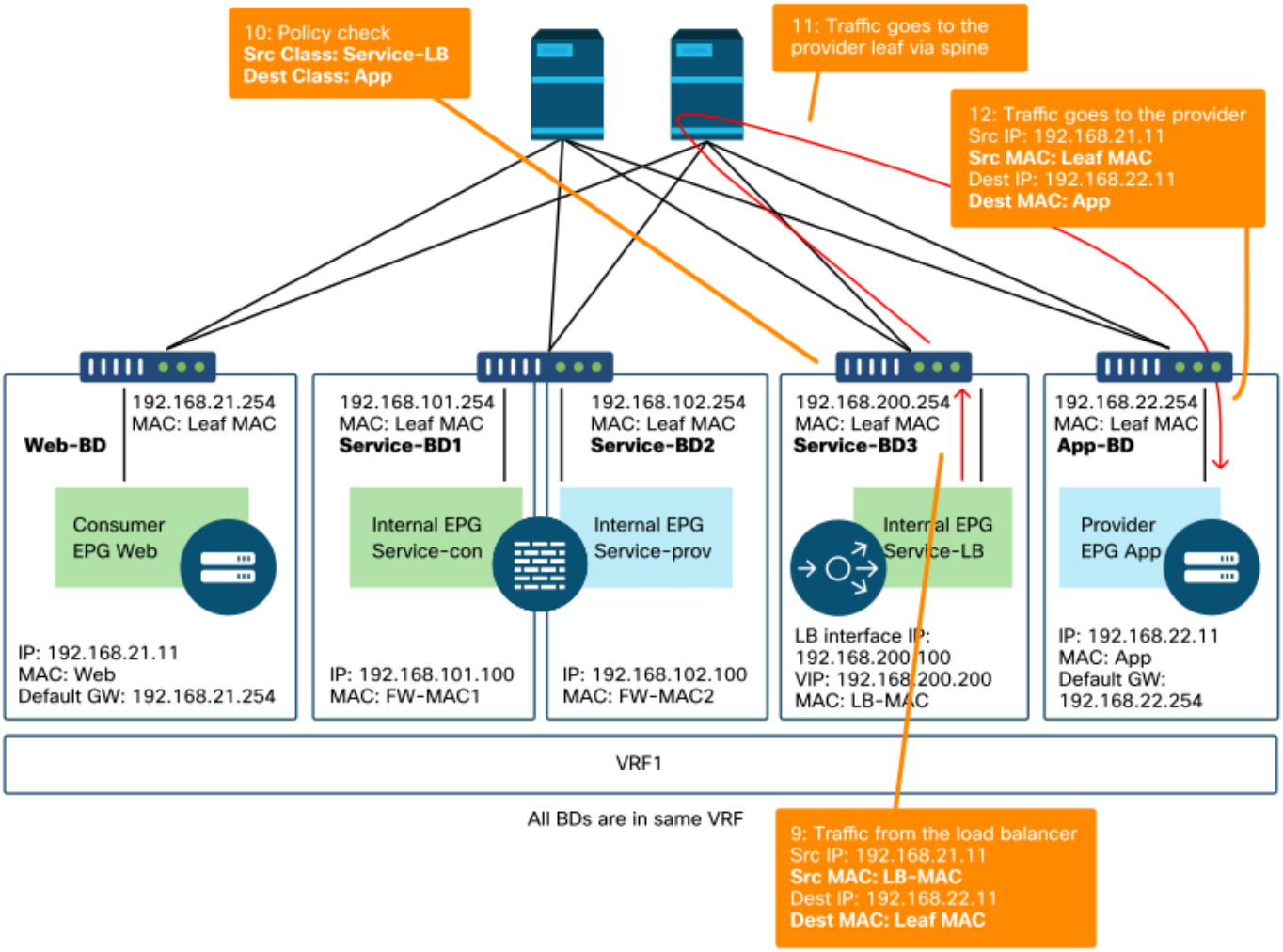
La siguiente figura ilustra un ejemplo de un flujo de tráfico entrante desde la Web de EPG de consumidor a la aplicación de EPG de proveedor con dos conexiones: Uno va desde un terminal

en la Web EPG del consumidor al VIP del equilibrador de carga a través del firewall y el otro va desde el equilibrador de carga a un terminal en la aplicación EPG del proveedor. El tráfico entrante destinado al VIP se redirige al firewall y luego va al balanceador de carga sin PBR. El equilibrador de carga cambia la IP de destino a uno de los terminales en el EPG de la aplicación asociado al VIP, pero no traduce la IP de origen. A continuación, el tráfico va al terminal del proveedor.

Ejemplo de firewall y equilibrador de carga sin ruta de reenvío SNAT: de consumidor a VIP y equilibrador de carga al proveedor



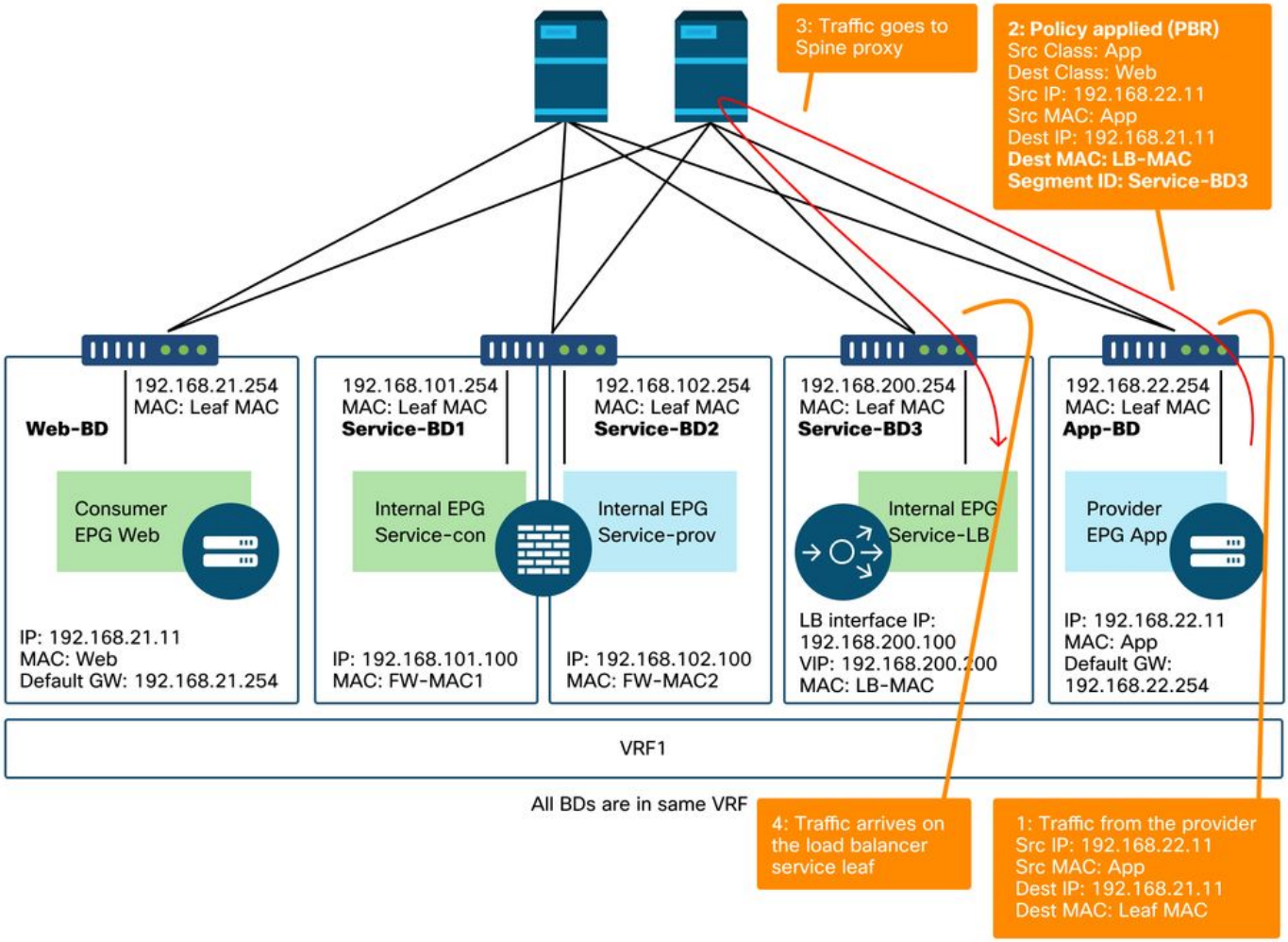
Ejemplo de firewall y equilibrador de carga sin ruta de reenvío SNAT: de consumidor a VIP y equilibrador de carga al proveedor (continuación)

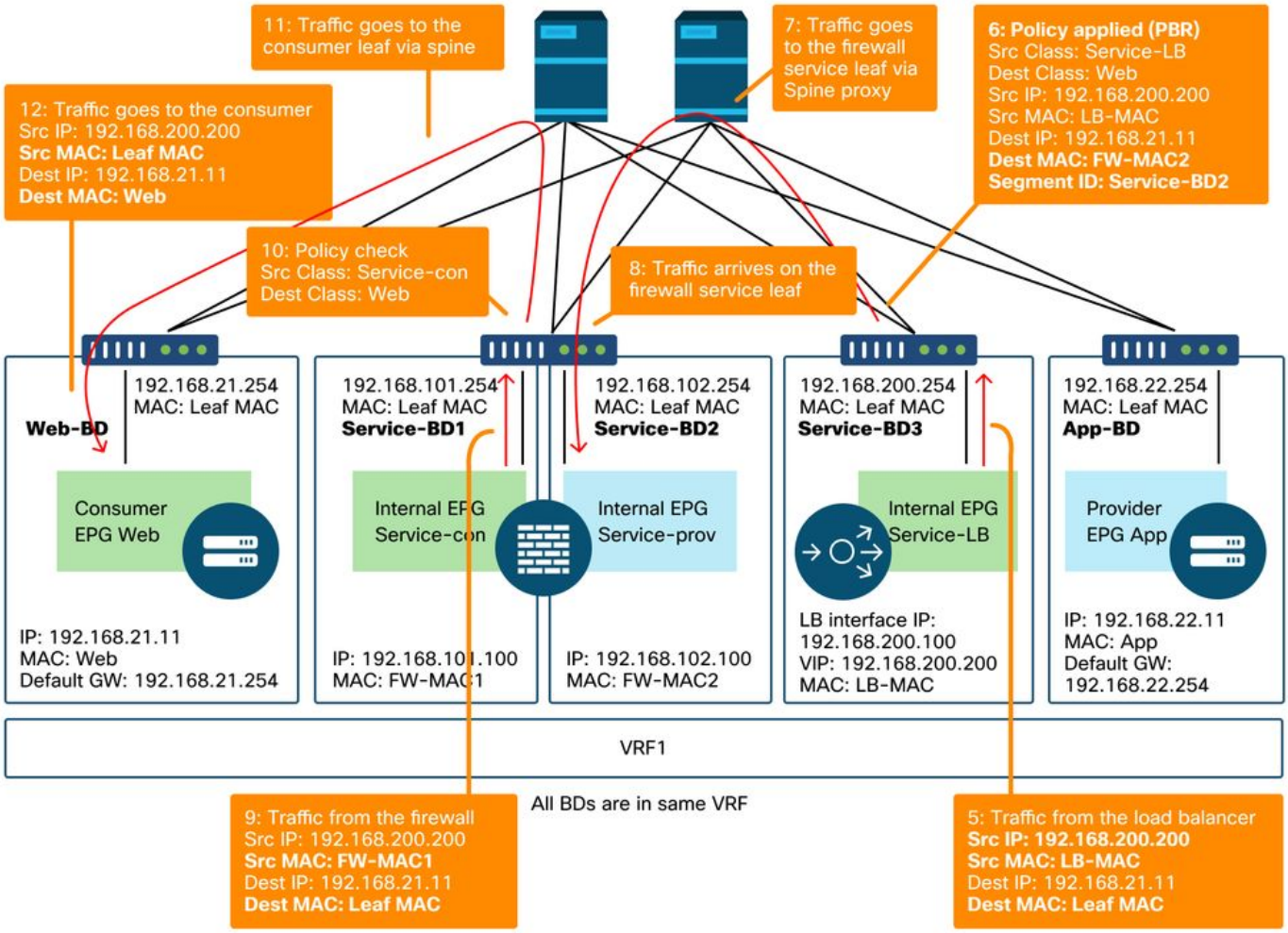


La siguiente figura ilustra el flujo de tráfico de retorno desde la aplicación EPG del proveedor a la Web EPG del consumidor. Debido a que el tráfico de retorno está destinado a la IP de origen original, se requiere PBR para que el tráfico de retorno regrese al equilibrador de carga.

Después de que el tráfico del extremo del proveedor al extremo del consumidor se redirige al equilibrador de carga, el equilibrador de carga cambia la IP de origen al VIP. El tráfico vuelve del equilibrador de carga y se redirige al firewall. A continuación, el tráfico vuelve del firewall y vuelve al terminal del consumidor.

Ejemplo de firewall y equilibrador de carga sin ruta de reenvío SNAT: del proveedor al consumidor

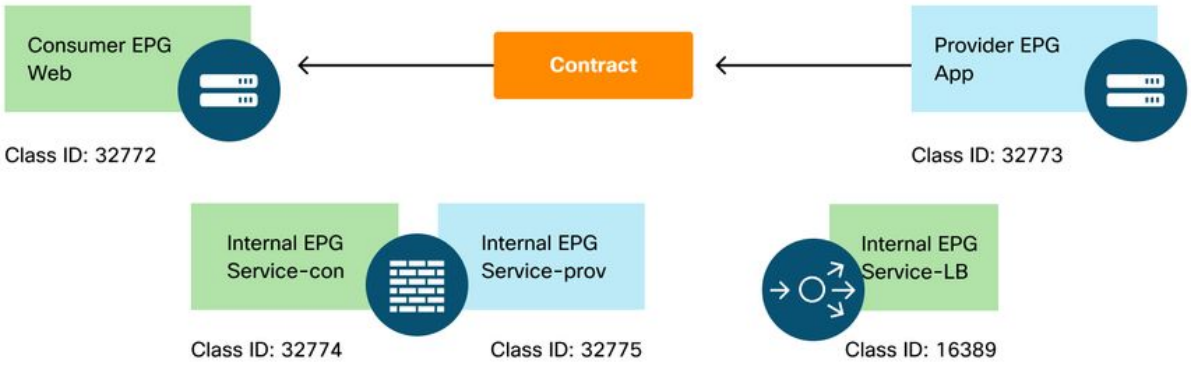

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



Las políticas programadas en los nodos de hoja

La siguiente figura y el resultado 'show zoning-rule' que se muestra a continuación describen las reglas de zonificación después de la implementación de Service Graph. En este ejemplo, el tráfico de pcTag 32772 (Web) a pcTag 16389 (Service-LB) se redirige a 'destgrp-32' (lado del consumidor del firewall), el tráfico de pcTag 32773 (App) a pcTag 32772 (Web) se redirige a 'destgrp-33' (equilibrador de carga) y el tráfico de pcTag 16389 (Service-LB) a pcTag 32772 (Web) se redirige a 'destgrp-34' (lado del proveedor del firewall).

Reglas de zonificación tras la implementación de Service Graph: firewall y equilibrador de carga sin 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)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

En el ejemplo anterior, la opción Direct Connect se establece en 'True' en la conexión entre el lado del proveedor del equilibrador de carga y el proveedor EPG. Se debe habilitar para la comprobación de estado desde el equilibrador de carga hasta los extremos del proveedor. La ubicación es 'Arrendatario > L4-L7 > Plantillas de Service Graph > Política'. Consulte la figura

"Establecer la opción de conexión directa".

3. Servicio compartido (contrato Inter-VRF)

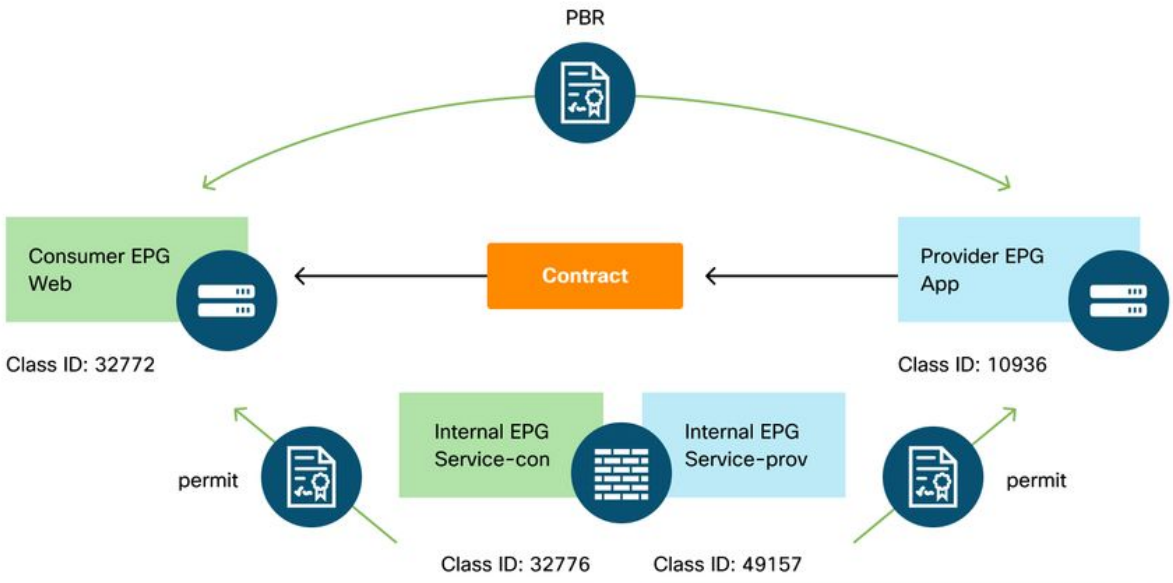
PBR se puede habilitar en un contrato entre VRF. Esta sección explica cómo se programan las reglas de zonificación en el caso de un contrato entre VRF de EPG a EPG.

Las políticas programadas en los nodos de hoja

En el caso de un contrato entre VRF de EPG a EPG, la política siempre se aplica en el VRF de consumidor. Por lo tanto, la redirección ocurre en el VRF de consumidor. Para otras combinaciones, consulte la tabla "¿Dónde se aplica la política?" en la sección "Reenvío".

La siguiente figura y el resultado 'show zoning-rule' describe las reglas de zonificación después de la implementación de Service Graph. En este ejemplo, el tráfico de pcTag 32772 (Web) a pcTag 10936 (App) se redirige a 'destgrp-36' (lado del consumidor del nodo de servicio) y el tráfico de pcTag 10936 (App) a pcTag 32772 (Web) se redirige a 'destgrp-35' (lado del proveedor del nodo de servicio). Ambos se aplican en VRF1 que es VRF de consumidor. El tráfico de pcTag 32776 (lado del consumidor del firewall) a pcTag 32772 (Web) está permitido en VRF1.

Reglas de zonificación tras la implementación de 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)      |
+---------+--------+--------+----------+----------------+---------+---------+------+------------
-------+------------------------+
```

El tráfico de pcTag 49157 (lado del proveedor del firewall) a pcTag 10936 (App) está permitido en VRF2 porque ambos están en 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)    |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).