Risoluzione dei problemi di reindirizzamento ACI basato su criteri

Sommario

Introduzione

In questo documento viene descritto come comprendere e risolvere i problemi relativi a uno scenario ACI Policy-Based Redirect (PBR).

Premesse

Il materiale di questo documento è stato estratto dal libro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, in particolare i capitoli **Reindirizzamento basato su policy - Panoramica, Reindirizzamento basato su policy - Distribuzione del grafico dei servizi, Reindirizzamento basato su policy - Inoltro e Reindirizzamento basato su policy - Altri flussi di traffico di esempio**.

Panoramica del reindirizzamento basato su criteri

In questo capitolo viene illustrata la risoluzione dei problemi relativi al grafico dei servizi in

modalità non gestita con Policy-Based Redirect (PBR).

Di seguito sono riportati alcuni passaggi tipici per la risoluzione dei problemi. In questo capitolo viene illustrato come verificare i passaggi 2 e 3 specifici di PBR. Per i punti 1 e 4, fare riferimento ai capitoli: "Inoltro intra-fabric", "inoltro esterno" e "Policy di sicurezza".

1. Verificare che il traffico funzioni senza il grafico del servizio PBR: Vengono appresi gli endpoint consumer e provider.Gli endpoint di tipo consumer e provider possono comunicare.
2. Verifica distribuzione del grafico del servizio: Le istanze di Graph distribuite non hanno errori.Verranno distribuiti le VLAN e gli ID di classe per il nodo del servizio.Vengono appresi gli endpoint del nodo del servizio.
3. Controllare il percorso di inoltro: Il criterio di controllo è programmato sui nodi foglia.Acquisire il traffico sul nodo del servizio per verificare se viene reindirizzato.Catturare il traffico sulla foglia ACI per verificare se ritorna alla struttura ACI dopo il PBR.
4. Verificare che il traffico arrivi sull'endpoint del provider e del consumer e che l'endpoint generi il traffico di ritorno.

In questo documento non vengono descritte le opzioni di progettazione o configurazione. Per maggiori informazioni, consultare il "White Paper ACI PBR" su Cisco.com

In questo capitolo, il nodo di servizio e la foglia di servizio implicano quanto segue:

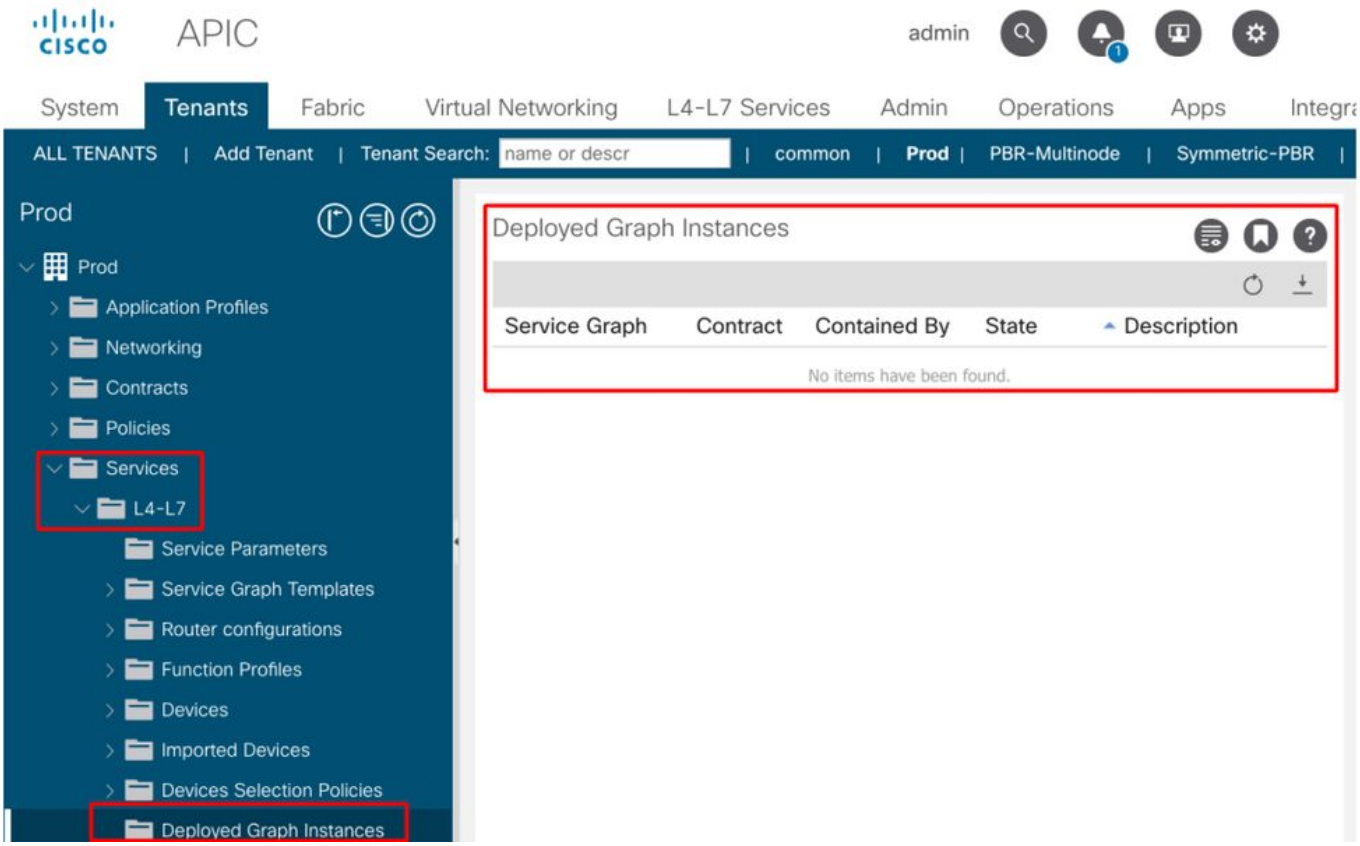
- Nodo di servizio: un nodo esterno al quale PBR reindirizza il traffico, ad esempio un firewall o un bilanciamento del carico.
- Foglia di servizio: una foglia ACI connessa a un nodo di servizio.

Risoluzione dei problemi di distribuzione del grafico del servizio

In questo capitolo viene illustrato un esempio di risoluzione dei problemi in cui non viene distribuito un grafico dei servizi.

Dopo aver definito e applicato una policy di Service Graph a un soggetto del contratto, dovrebbe essere presente un'istanza di grafico distribuita nell'interfaccia utente grafica (GUI) di ACI. Nella figura seguente viene illustrato lo scenario di risoluzione dei problemi in cui il grafico del servizio non viene visualizzato come distribuito.

Service Graph non viene visualizzato come istanza di Graph distribuita.



1. Controllare le fasi di configurazione e il guasto

Il primo passaggio della procedura di risoluzione dei problemi consiste nel verificare che i componenti necessari siano stati configurati senza errori. Si presume che le configurazioni generali seguenti siano già state eseguite:

- VRF e BD per EPG consumer, EPG provider e service node
- Il consumatore e il fornitore EPG.
- Il contratto e i filtri.

Èopportuno ricordare che non è necessario creare manualmente un EPG per il nodo di servizio. Verrà creato tramite la distribuzione di Service Graph.

Di seguito sono riportati i passi di configurazione di Service Graph con PBR:

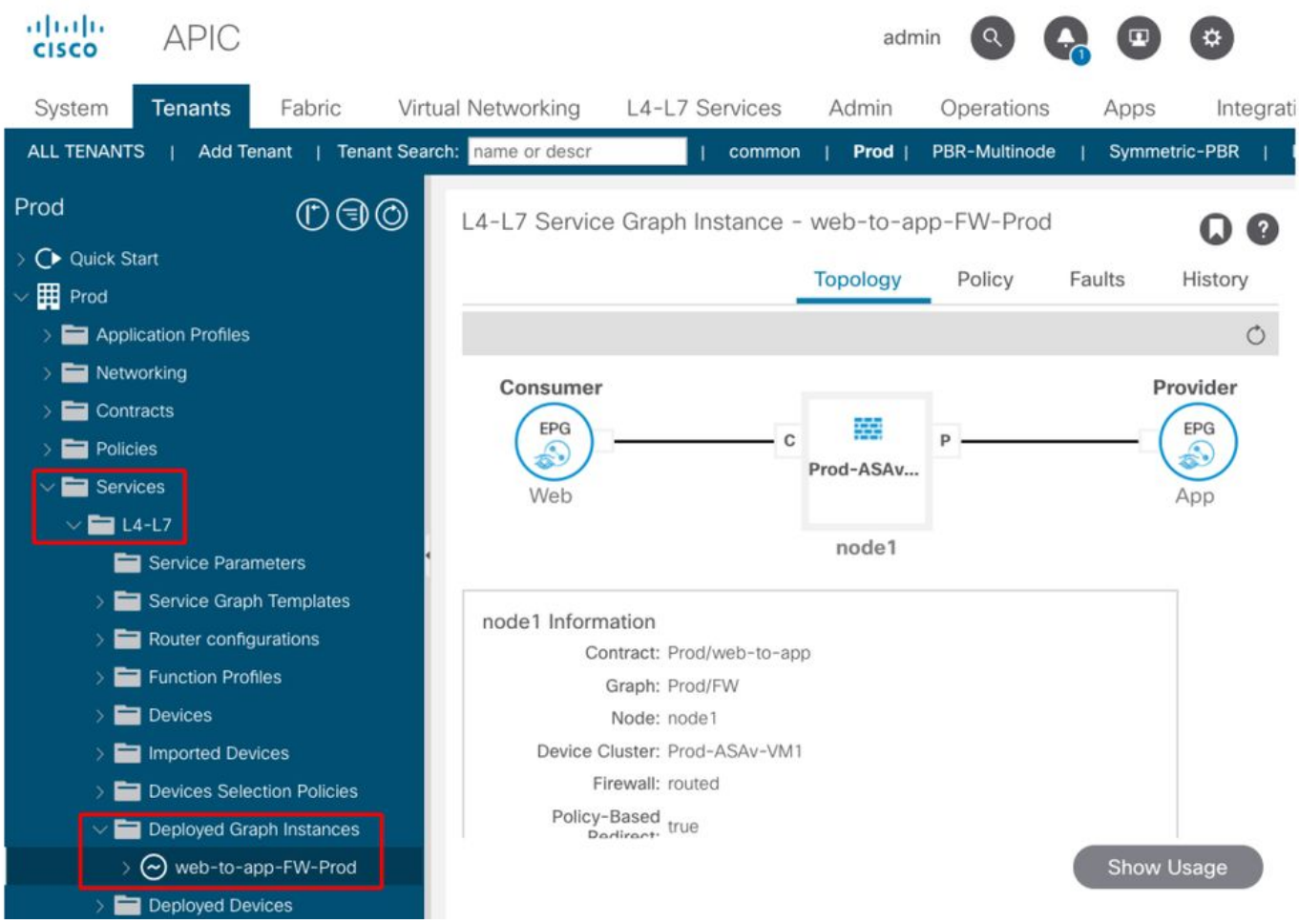
- Creare la periferica L4-L7 (periferica logica).
- Creare il grafico del servizio.
- Creare il criterio PBR.
- Creare il criterio Selezione dispositivo.
- Associare il grafico del servizio all'oggetto del contratto.

2. Controllare la distribuzione di Service Graph nell'interfaccia utente

Dopo l'associazione di un grafico del servizio all'oggetto del contratto, per ogni contratto con il grafico del servizio deve essere visualizzata un'istanza del grafico distribuito (figura seguente).

Il percorso è 'Tenant > Servizi > L4-L7 > Istanze grafico distribuite'

Istanza di Graph distribuita



Se un'istanza di grafico distribuito non viene visualizzata, si è verificato un errore nella configurazione del contratto. Le ragioni principali possono essere:

- Il contratto non prevede un EPG fornitore o utente.
- L'oggetto del contratto non dispone di alcun filtro.
- L'ambito del contratto è VRF anche se è per la comunicazione tra VRF o tra tenant EPG.

Se la creazione dell'istanza di Service Graph ha esito negativo, nell'istanza di Service Graph distribuita vengono generati errori, ovvero si è verificato un errore nella configurazione di Service Graph. Gli errori tipici causati dalla configurazione sono i seguenti:

F1690: Configurazione non valida a causa di un errore di allocazione ID

Questo errore indica che la VLAN incapsulata per il nodo del servizio non è disponibile. Ad esempio, nel pool di VLAN associato al dominio VMM utilizzato nella periferica logica non è disponibile alcuna VLAN dinamica.

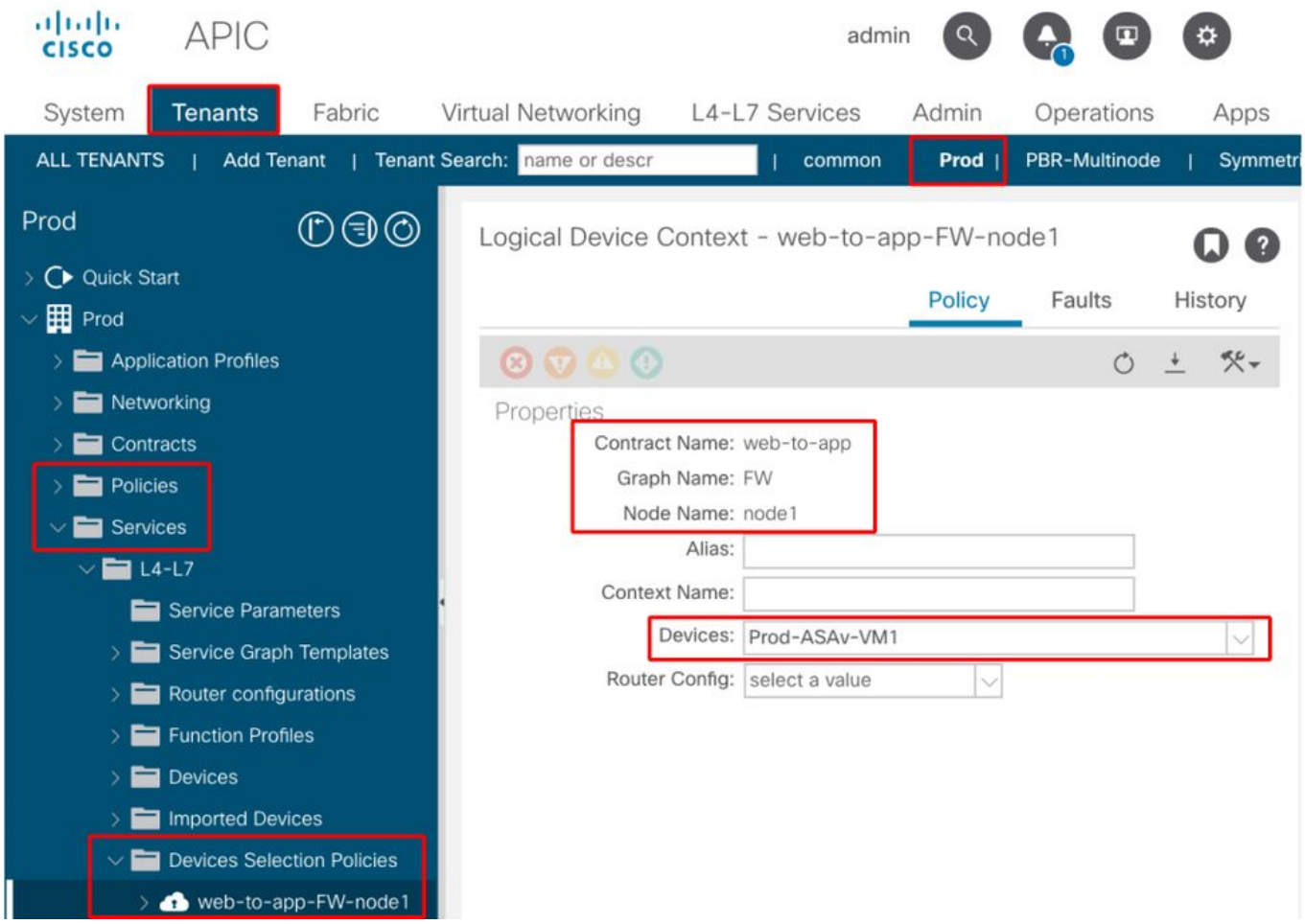
Risoluzione: Controllare il pool VLAN nel dominio utilizzato per la periferica logica. Verificare la VLAN incapsulata nell'interfaccia del dispositivo logico se si trova in un dominio fisico. Le posizioni sono 'Tenant > Servizi > L4-L7 > Dispositivi e infrastruttura > Criteri di accesso > Pool > VLAN'.

F1690: Configurazione non valida a causa di nessun contesto di dispositivo trovato per LDev

Questo errore indica che non è possibile trovare la periferica logica per il rendering di Service Graph. Ad esempio, non esiste alcun criterio di selezione dei dispositivi corrispondente per il contratto con il grafico del servizio.

Risoluzione: Verificare che il criterio di selezione del dispositivo sia definito. I criteri di selezione dei dispositivi forniscono un criterio di selezione per un dispositivo di servizio e i relativi connettori. I criteri si basano sul nome di un contratto, di un grafico del servizio e di un nodo nel grafico del servizio. Il percorso è 'Tenant > Servizi > L4-L7 > Criteri di selezione dispositivi'.

Verifica criterio di selezione dispositivo



F1690: Configurazione non valida. Nessuna interfaccia cluster trovata

Questo errore indica che non è possibile trovare l'interfaccia cluster per il nodo del servizio. Ad esempio, l'interfaccia cluster non è specificata in Criteri di selezione periferica.

Risoluzione: Verificare che l'interfaccia del cluster sia specificata nel criterio di selezione delle periferiche e che il nome del connettore sia corretto (figura seguente).

F1690: Configurazione non valida. BD non trovato

Questo errore indica che non è possibile trovare il BD per il nodo del servizio. Ad esempio, BD non è specificato in Criteri di selezione dispositivi.

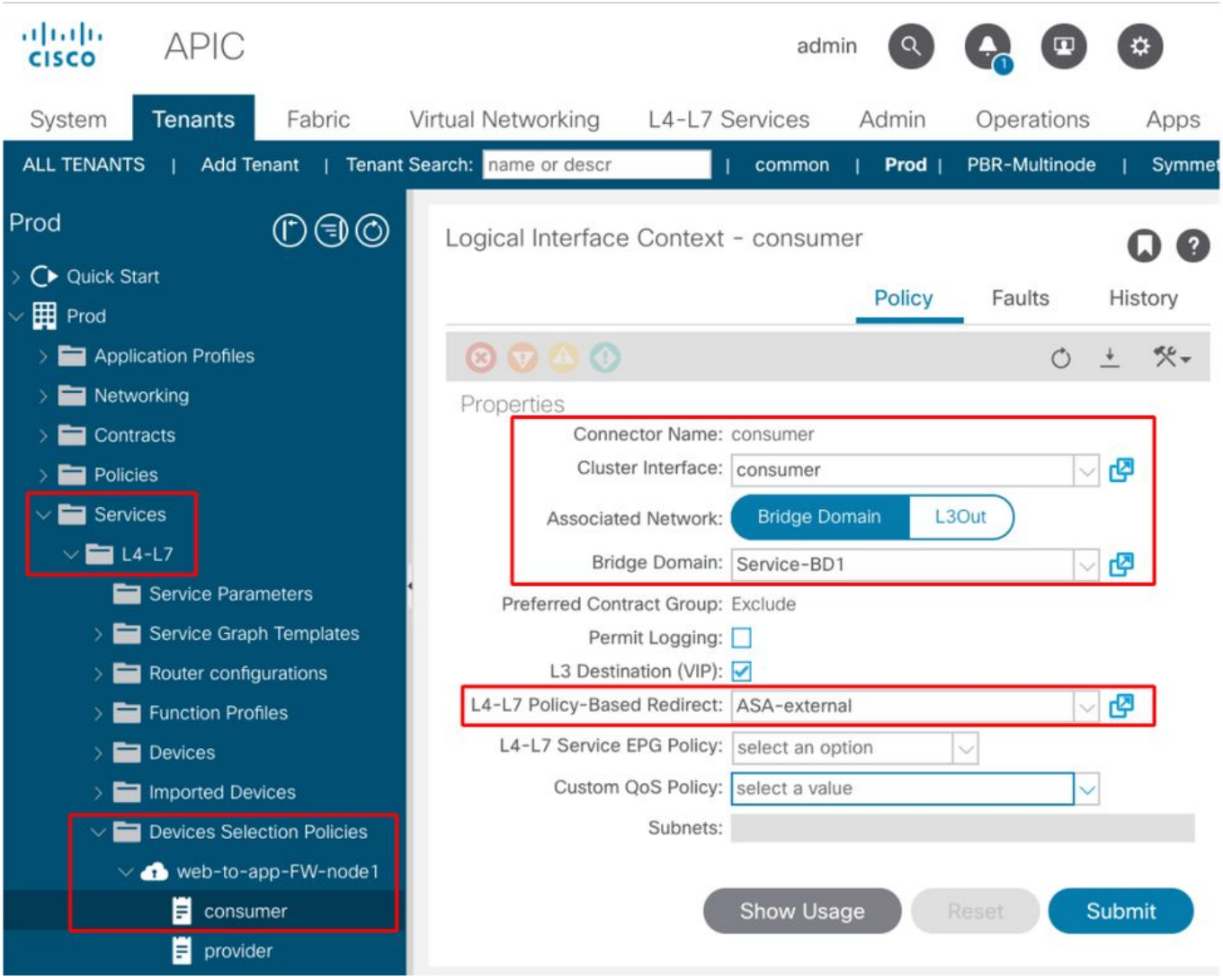
Risoluzione: Verificare che BD sia specificato in Criteri di selezione periferiche e che il nome del connettore sia corretto (Figura seguente).

F1690: Configurazione non valida a causa di criteri di reindirizzamento del servizio non validi

Questo errore indica che il criterio PBR non è selezionato anche se il reindirizzamento è abilitato sulla funzione di servizio nel grafico del servizio.

Risoluzione: Selezionare PBR policy in Device Selection Policy (Figura seguente).

Configurazione dell'interfaccia logica nel criterio di selezione del dispositivo



Risoluzione dei problemi di inoltro PBR

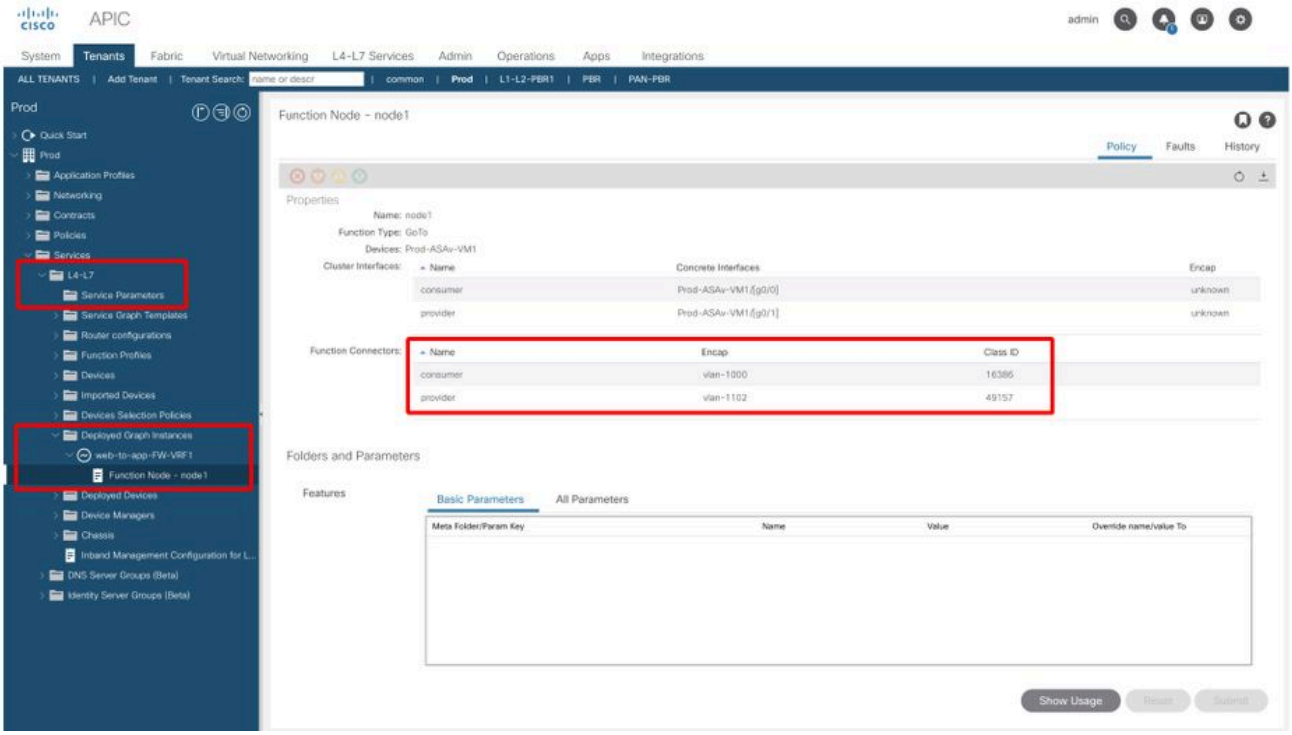
In questo capitolo vengono illustrati i passaggi per la risoluzione dei problemi relativi al percorso di inoltro PBR.

1. Verificare che le VLAN siano state distribuite e che gli endpoint siano stati appresi sul nodo foglia

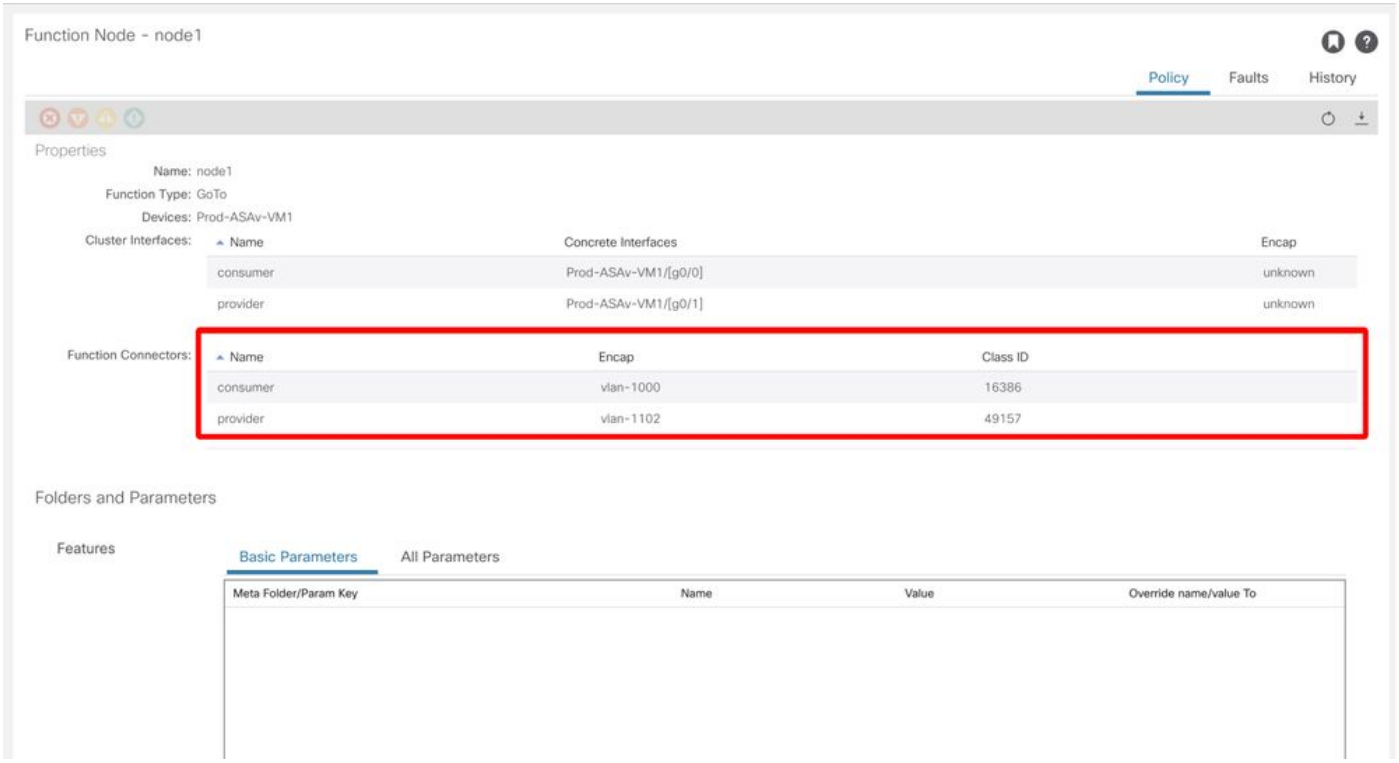
Una volta distribuito correttamente un service graph senza errori, vengono creati EPG e BD per un nodo di servizio. La figura seguente mostra dove trovare gli ID VLAN incapsulati e gli ID classe delle interfacce dei nodi di servizio (EPG del servizio). Nell'esempio, il lato consumer di un firewall è la classe ID 16386 con VLAN encap 1000 e il lato provider di un firewall è la classe ID 49157 con VLAN encap 1102.

Il percorso è 'Tenant > Servizi > L4-L7 > Istanze grafico distribuite > Nodi funzione'.

Nodo di servizio



ID classe interfaccia nodo del servizio



Queste VLAN vengono distribuite sulle interfacce del nodo foglia di servizio a cui sono connessi i nodi di servizio. Lo stato di apprendimento e distribuzione VLAN può essere controllato utilizzando 'show vlan extended' e 'show endpoint' nella CLI del nodo foglia di servizio.

```
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 gli IP degli endpoint dei nodi di servizio non vengono appresi come endpoint nella struttura ACI, è molto probabile che si sia verificato un problema di connettività o configurazione tra la foglia di servizio e il nodo di servizio. Verificare i seguenti stati:

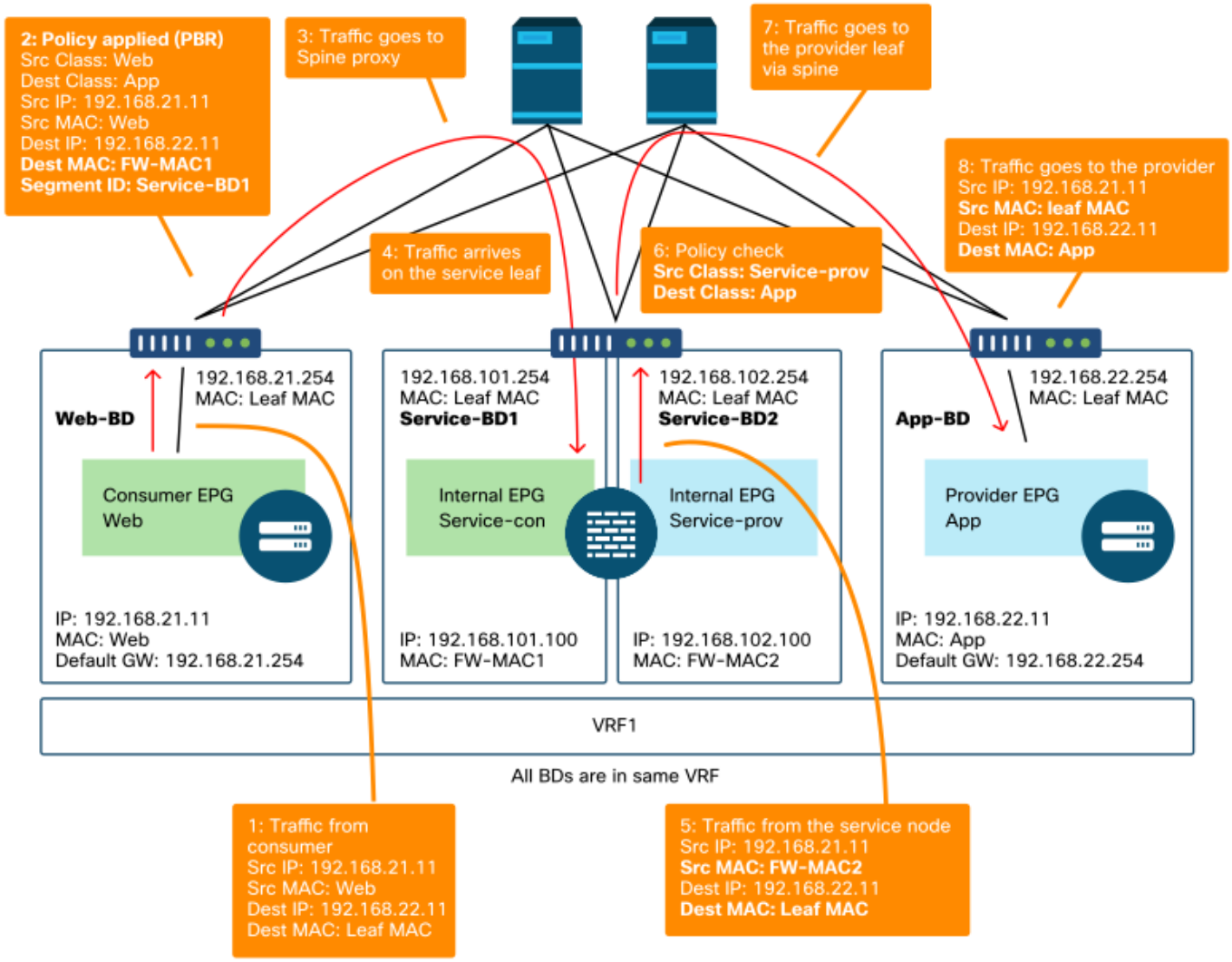
- Il nodo del servizio è collegato alla porta di downlink foglia corretta. Se il nodo del servizio si trova in un dominio fisico, è necessario definire la VLAN di accesso al percorso statico foglia nella periferica logica.Se il nodo del servizio si trova in un dominio VMM, verificare che il dominio VMM funzioni e che il gruppo di porte creato tramite Service Graph sia collegato correttamente alla macchina virtuale del nodo del servizio.
- La porta di downlink foglia connessa al nodo di servizio o all'hypervisor in cui risiede la VM del nodo di servizio è attiva.
- Il nodo del servizio ha la VLAN e l'indirizzo IP corretti.
- Lo switch intermedio tra la foglia di servizio e il nodo di servizio ha la configurazione VLAN corretta.

2. Controllare i percorsi di traffico previsti

Se il traffico end-to-end smette di funzionare dopo l'abilitazione del PBR, anche se gli endpoint del nodo di servizio vengono appresi nell'infrastruttura ACI, il passaggio successivo per la risoluzione dei problemi consiste nel controllare i percorsi del traffico previsti.

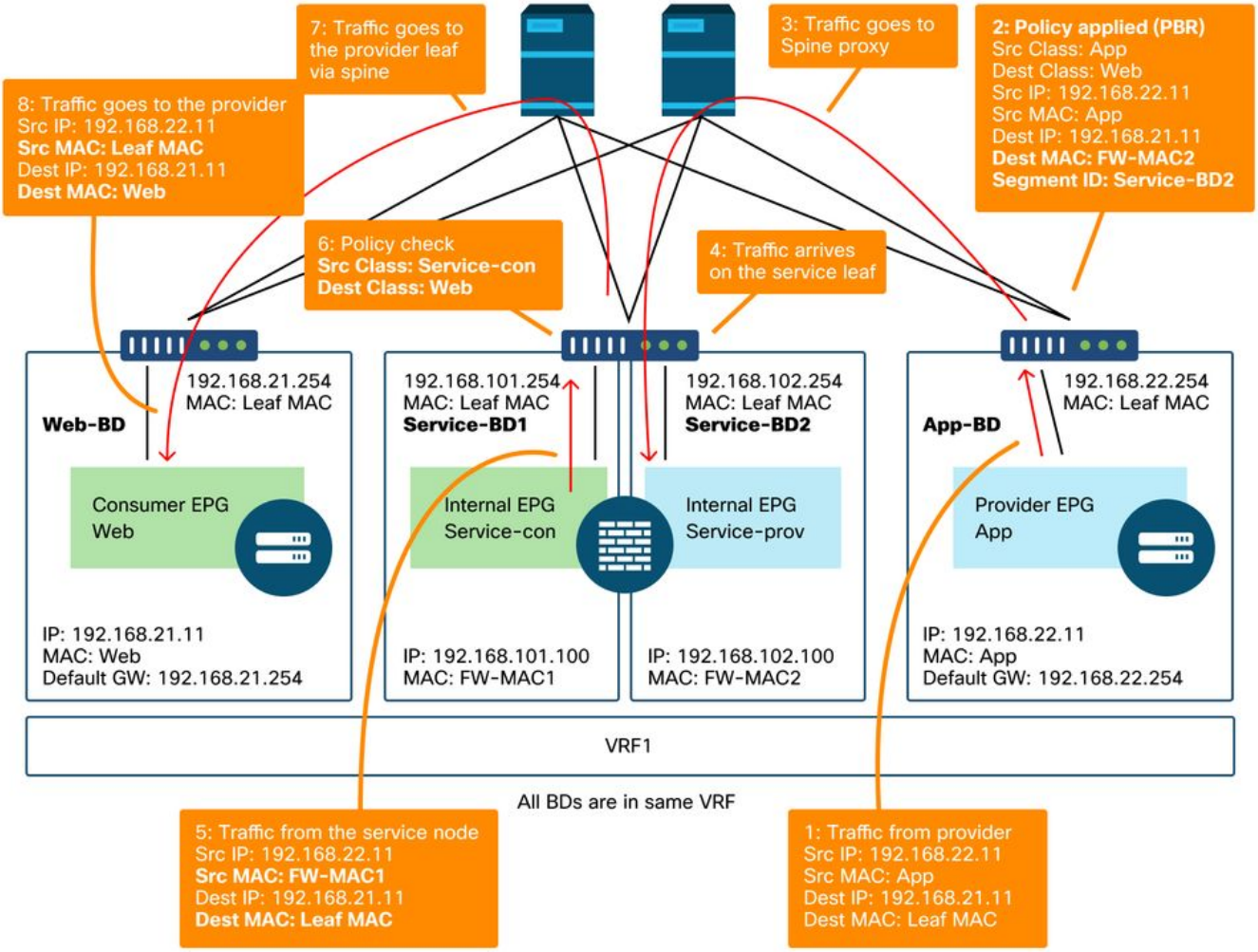
Nelle figure 'Esempio di percorso di inoltro PBR - da consumer a provider' e 'Esempio di percorso di inoltro PBR - da provider a consumer' viene illustrato un esempio di percorso di inoltro dell'inserimento di un firewall tramite PBR tra un endpoint di tipo consumer e un endpoint di tipo provider. Si presume che gli endpoint vengano già appresi nei nodi foglia.

Esempio di percorso di inoltro PBR - da consumer a provider



Nota: Poiché l'indirizzo MAC di origine non viene modificato in indirizzo MAC foglia ACI, il nodo PBR non deve utilizzare l'inoltro basato su indirizzo MAC di origine se l'endpoint consumer e il nodo PBR non si trovano nello stesso BD

Esempio di percorso di inoltro PBR - da provider a consumer



Nota: È opportuno ricordare che la politica PBR viene applicata sia sul consumer che sull'elemento foglia del provider e ciò che fa ACI PBR è la riscrittura MAC di destinazione, come mostrato nelle figure 'PBR forwarding path example - consumer to provider' e 'PBR forwarding path example - provider to consumer'. Per raggiungere il MAC di destinazione PBR viene sempre utilizzato un proxy di spine, anche se l'endpoint di origine e il MAC di destinazione PBR si trovano nella stessa foglia.

Anche se le figure 'PBR forwarding path example - consumer to provider' e 'PBR forwarding path example - provider to consumer' mostrano un esempio di dove il traffico verrebbe reindirizzato, dove la policy viene applicata dipende dalla configurazione del contratto e dallo stato di apprendimento dell'endpoint. La tabella 'Dove viene applicato il criterio' riepiloga dove il criterio viene applicato in un singolo sito ACI. Dove i criteri vengono applicati in più siti è diverso.

Dove viene applicata la politica?

Scenario	Modalità di imposizione VRF	Consumer	Provider	Criterio applicato il
Intra-VRF	In entrata/in uscita	EPG	EPG	·Se si apprende l'endpoint di destinazione: foglia in entrata* ·Se non si apprende l'endpoint di destinazione: foglia di uscita
	In ingresso	EPG	EPG L3Out	Foglia di consumo (foglia non transfrontaliera)

	In ingresso	EPG L3Out	EPG	Foglia fornitore (foglia non transfrontaliera)
	In uscita	EPG	EPG L3Out	Foglia di confine -> traffico foglia non di confine
	In uscita	EPG L3Out	EPG	·Se si apprende l'endpoint di destinazione: foglia di bordo ·Se non si apprende l'endpoint di destinazione: foglia non frontaliera
	In entrata/in uscita	EPG L3Out	EPG L3Out	Traffico foglia -> frontiera ·Foglia Foglia in ingresso*
	In entrata/in uscita	EPG	EPG	Foglia
	In entrata/in uscita	EPG	EPG L3Out	Foglia di consumo (Foglia esterna)
Inter-VRF	In entrata/in uscita	EPG L3Out	EPG	Foglia in ingresso*
	In entrata/in uscita	EPG L3Out	EPG L3Out	Foglia in ingresso*

*L'applicazione della policy viene applicata alla prima foglia colpita dal pacchetto.

Ecco alcuni esempi:

- Se un endpoint esterno in L3Out EPG in VRF1 tenta di accedere a un endpoint in Web EPG in VRF1 e VRF1 è configurato per la modalità di imposizione in entrata, il traffico viene reindirizzato dalla foglia in cui risiede l'endpoint in Web EPG, indipendentemente dalla direzione del contratto.
- Se un endpoint in EPG Web consumer in VRF1 tenta di accedere a un endpoint in EPG applicazione provider in VRF1 e gli endpoint vengono appresi nei nodi foglia consumer e provider, il traffico viene reindirizzato dalla foglia in entrata.
- Se un endpoint in Web EPG consumer in VRF1 tenta di accedere a un endpoint nell'app provider EPG in VRF2, il traffico viene reindirizzato dalla foglia consumer in cui risiede l'endpoint consumer, indipendentemente dalla modalità di imposizione VRF.

3. Verificare se il traffico viene reindirizzato al nodo del servizio

Dopo aver cancellato il percorso di inoltro previsto, è possibile utilizzare ELAM per controllare se il traffico arriva sui nodi dello switch e controllare la decisione di inoltro su tali nodi. Fare riferimento alla sezione "Strumenti" nel capitolo "Inoltro intra-fabric" per istruzioni su come utilizzare ELAM.

Ad esempio, per tracciare il flusso di traffico nella figura 'Esempio di percorso di inoltro PBR - da consumer a provider', è possibile catturare questi dati per confermare se il traffico da consumer a provider viene reindirizzato.

- Scollegare la porta sulla foglia del consumatore per controllare 1 e 2 (il traffico arriva sulla foglia del consumatore e viene applicato il PBR).
- Porta fabric sui nodi della spine da controllare 3 (il traffico va al proxy della spine).
- Porta infrastruttura su foglia di servizio per controllare 4 (il traffico arriva sulla foglia di servizio).

Quindi, è possibile acquisirli per verificare se il traffico che torna dal nodo del servizio va al

provider.

- Scollegare la porta sul foglio di servizio per controllare 5 e 6 (il traffico torna dal nodo di servizio ed è autorizzato).
- Porta fabric sui nodi della spine da controllare 7 (il traffico passa alla foglia del provider tramite la spine).
- Porta dell'infrastruttura sull'elemento foglia del provider per controllare 8 (il traffico arriva sull'elemento foglia del servizio e va all'endpoint del provider).

Nota: Se il nodo consumer e il nodo di servizio si trovano nella stessa foglia, specificare un'interfaccia o un indirizzo MAC di origine in aggiunta all'indirizzo IP di origine/destinazione in modo che ELAM verifichi 1 o 5 nella figura 'Esempio di percorso di inoltro PBR - da consumer a provider', in particolare perché entrambi utilizzano lo stesso indirizzo IP di origine e lo stesso indirizzo IP di destinazione.

Se il traffico tra consumer e provider viene reindirizzato al nodo del servizio ma non viene reindirizzato all'elemento foglia del servizio, verificare quanto segue in quanto si tratta di errori comuni:

- La tabella di routing del nodo del servizio raggiunge la subnet del provider.
- I criteri di sicurezza del nodo del servizio, ad esempio ACL, consentono il traffico.

Se il traffico viene reindirizzato e arriva al provider, verificare il percorso del traffico di ritorno da provider a consumatore in modo simile.

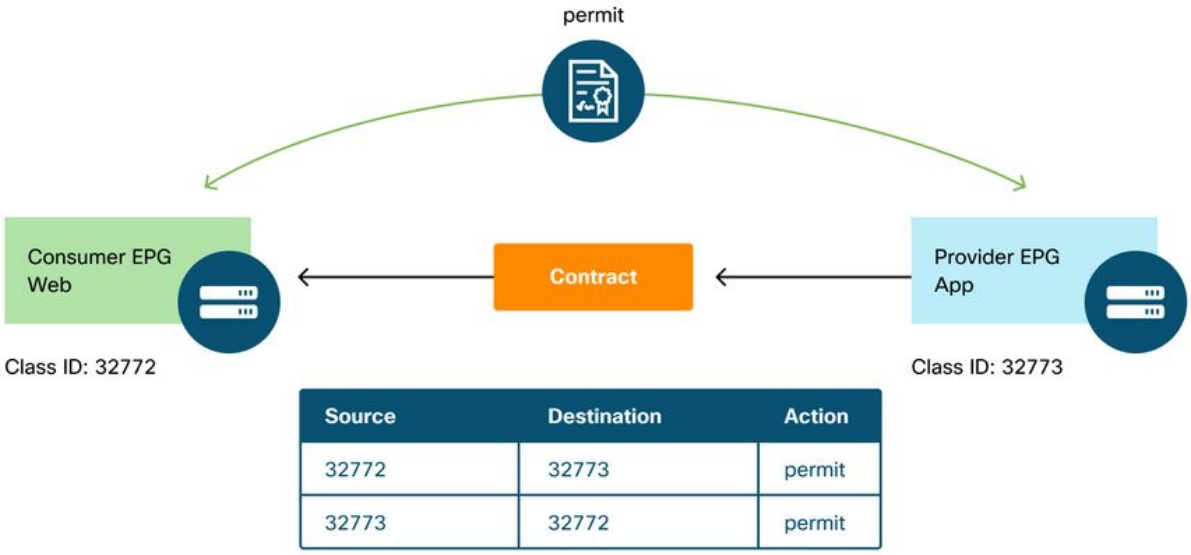
4. Controllare i criteri programmati sui nodi foglia

Se il traffico non viene inoltrato o reindirizzato di conseguenza, il passaggio successivo per la risoluzione dei problemi consiste nel controllare i criteri programmati sui nodi foglia. Questa sezione mostra zoning-rule e contract_parser come esempi. Per maggiori dettagli su come controllare le regole di zoning, fare riferimento alla sezione "Strumenti" nel capitolo "Security Policies".

Nota: I criteri sono programmati in base allo stato di installazione EPG sul foglio. L'output del comando show in questa sezione utilizza la foglia contenente EPG consumer, EPG provider ed EPG per il nodo di servizio.

Uso del comando 'show zoning-rule'

Nella figura e nell'output 'show zoning-rule' seguente vengono descritte le regole di suddivisione in zone prima della distribuzione di Service Graph.

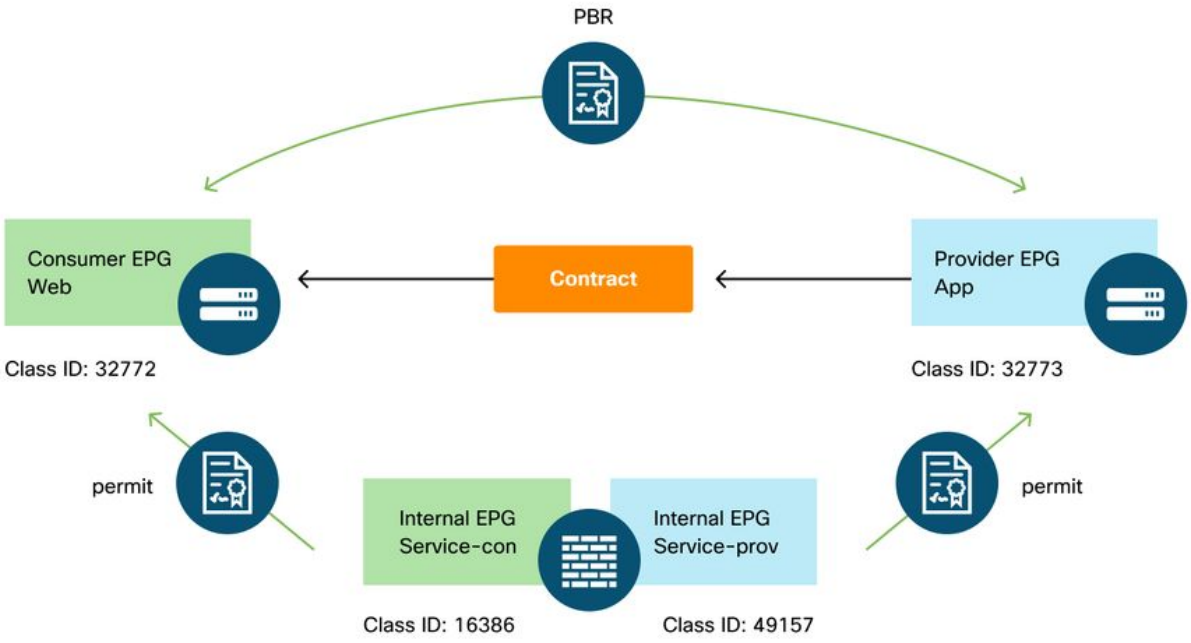


L'ID ambito VRF è disponibile in 'Tenant > Rete > VRF'.

```
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 volta distribuito Service Graph, vengono creati gli EPG per il nodo del servizio e vengono aggiornate le policy per reindirizzare il traffico tra il consumer e gli EPG del provider. La figura seguente e l'output 'show zoning-rule' seguente descrivono le regole di zoning dopo la distribuzione di Service Graph. Nell'esempio, il traffico tra pcTag 32772 (Web) e pcTag 32773 (App) viene reindirizzato a 'destgrp-27' (lato consumer del nodo del servizio) e il traffico tra pcTag 32773 (App) e pcTag 32772 (Web) viene reindirizzato a 'destgrp-28' (lato provider del nodo del servizio).

Regole di zoning dopo la distribuzione di 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)     |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

Le informazioni di destinazione di ogni destgrp possono essere trovate utilizzando il 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 le regole di zoning sono programmate di conseguenza, ma il traffico non viene reindirizzato o inoltrato di conseguenza, verificare quanto segue in quanto si tratta di errori comuni:

- Verificare se l'ID classe di origine o di destinazione viene risolto come previsto utilizzando ELAM. In caso contrario, verificare l'ID di classe errato e i criteri di derivazione EPG, ad esempio il percorso e la VLAN di incapsulamento.
- Anche se gli ID delle classi di origine e di destinazione vengono risolti di conseguenza e viene applicato il criterio PBR ma il traffico non arriva sul nodo PBR, verificare che IP, MAC e VRF del destgrp nell'azione redir ('show service redir info') siano corretti.

Per impostazione predefinita, le regole di autorizzazione per un EPG consumer a un nodo di servizio (lato consumer) e un EPG provider a un nodo di servizio (lato provider) non vengono programmate se PBR è abilitato. Pertanto, un endpoint di tipo consumer o provider non può comunicare direttamente con il nodo del servizio per impostazione predefinita. Per autorizzare questo traffico, è necessario abilitare l'opzione Connessione diretta. Lo scenario di utilizzo è spiegato nella sezione "Altri esempi di flussi di traffico**"**.

Uso di contract_parser

Lo strumento contract_parser consente inoltre di verificare i criteri. C-consumer è il lato consumer del nodo di servizio e C-provider è il lato provider del nodo di servizio.

```
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]
...
```

Altri esempi di flussi di traffico

In questa sezione vengono illustrati altri esempi di flussi di traffico comuni per identificare i flussi desiderati per la risoluzione dei problemi. Per la risoluzione dei problemi, fare riferimento al capitolo precedente di questa sezione.

1. Bilanciamento del carico senza SNAT: In questo esempio, il Web EPG consumer e l'app EPG provider hanno un contratto con un grafico del servizio di bilanciamento del carico. Gli endpoint in App EPG sono server reali associati all'indirizzo VIP nel bilanciamento del carico.PBR per il bilanciamento del carico abilitato per la direzione del traffico dal provider al consumer.
2. Firewall e bilanciamento del carico senza SNAT: In questo esempio, il Web EPG consumer e il provider EPG App hanno un contratto con un firewall e un grafico del servizio di bilanciamento del carico. Gli endpoint in App EPG sono server reali associati all'indirizzo VIP nel bilanciamento del carico.PBR al firewall attivato per entrambe le direzioni.PBR per il bilanciamento del carico abilitato per la direzione del traffico dal provider al consumer.
3. Servizio condiviso (contratto Inter-VRF): In questo esempio, il Web EPG consumer e il provider EPG App hanno un contratto con un grafo del servizio firewall. EPG Web e EPG App si trovano in VRF diverse.PBR al firewall attivato per entrambe le direzioni.Il firewall si trova tra due VRF.

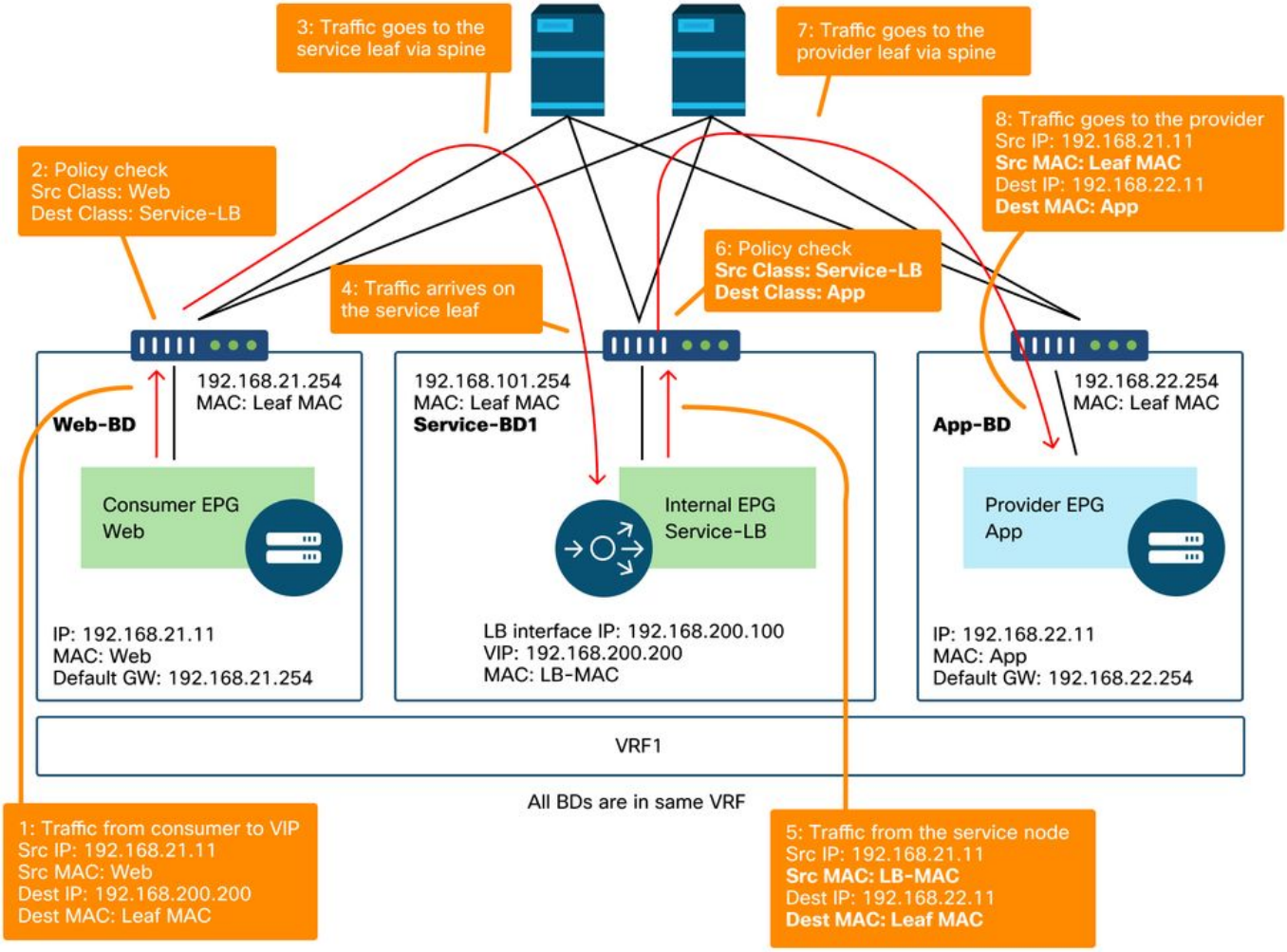
1. Bilanciamento del carico senza SNAT

PBR può essere implementato come PBR bidirezionale o PBR unidirezionale. Un caso di utilizzo per il PBR unidirezionale è l'integrazione del bilanciamento del carico senza NAT (Network Address Translation) di origine. Se il bilanciamento del carico esegue NAT di origine, il PBR non è necessario.

Esempio di percorso del traffico

Nella figura seguente viene illustrato un esempio di flusso di traffico in entrata dal Web EPG consumer al provider EPG App con due connessioni: Uno viene inviato da un endpoint nel Web EPG del consumer all'indirizzo VIP del servizio di bilanciamento del carico, l'altro viene inviato dal servizio di bilanciamento del carico a un endpoint nell'app EPG del provider. Poiché il traffico in ingresso è destinato al VIP, raggiungerà il bilanciamento del carico senza PBR se il VIP è raggiungibile. Il load balancer cambia l'IP di destinazione in uno degli endpoint nell'app EPG associata all'indirizzo VIP, ma non converte l'IP di origine. Di conseguenza, il traffico viene indirizzato all'endpoint del provider.

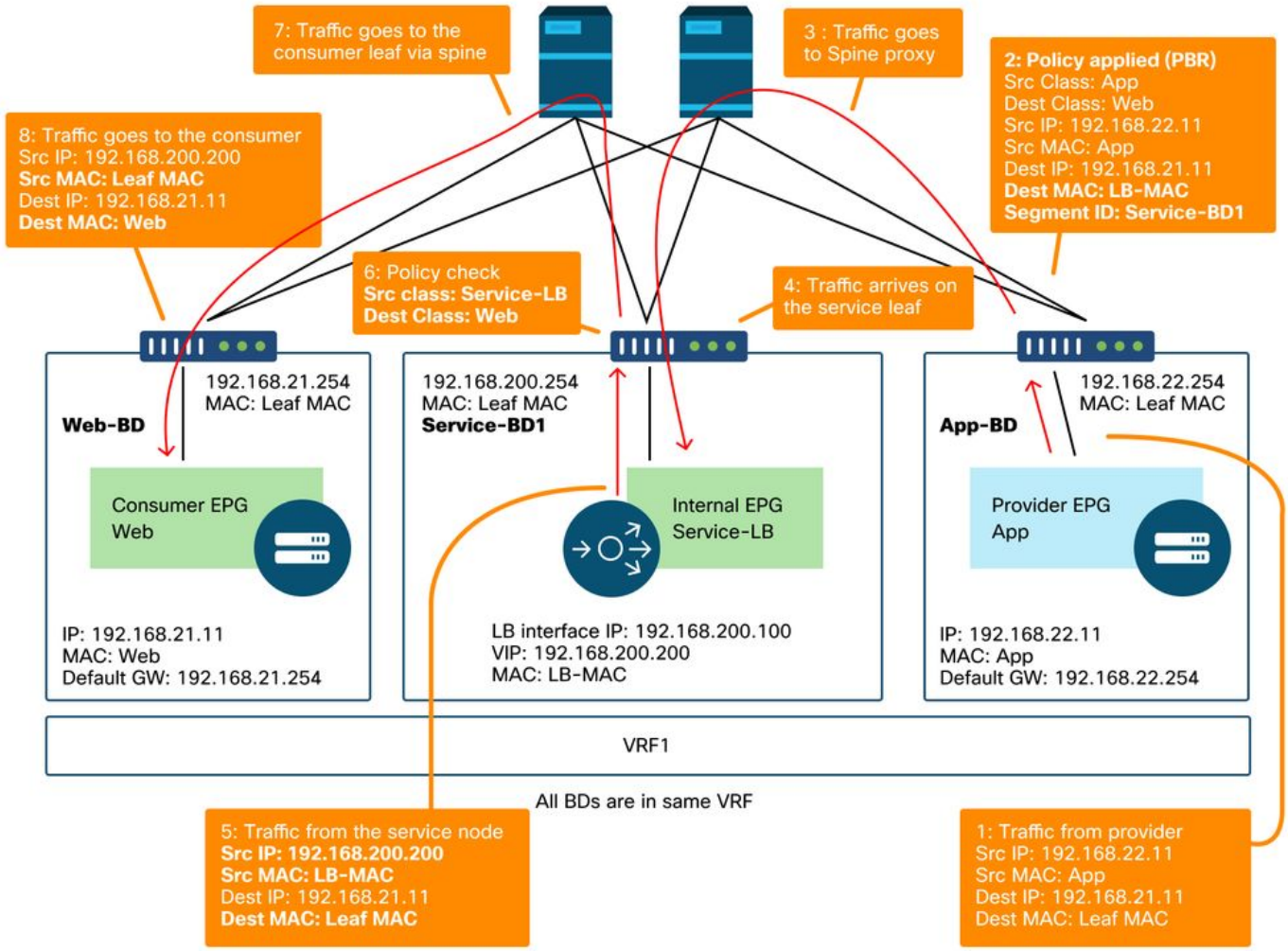
Esempio di bilanciamento del carico senza percorso di inoltro SNAT: da consumer a VIP e da bilanciamento del carico a provider senza PBR



Nella figura seguente viene illustrato il flusso del traffico di ritorno dall'app EPG del provider al Web EPG del consumer. Poiché il traffico di ritorno è destinato all'IP di origine, il PBR è necessario per rendere il traffico di ritorno di nuovo al servizio di bilanciamento del carico. In caso contrario, l'endpoint consumer riceve il traffico in cui l'IP di origine è l'endpoint provider anziché il VIP. Il traffico verrà scartato perché l'endpoint consumer non ha avviato il traffico verso l'endpoint provider anche se la rete intermedia, ad esempio la struttura ACI, inoltra il pacchetto all'endpoint consumer.

Dopo il reindirizzamento del traffico dall'endpoint del provider all'endpoint del consumer al bilanciamento del carico, il bilanciamento del carico modifica l'IP di origine in VIP. Quindi, il traffico torna dal bilanciamento del carico e torna all'endpoint di tipo consumer.

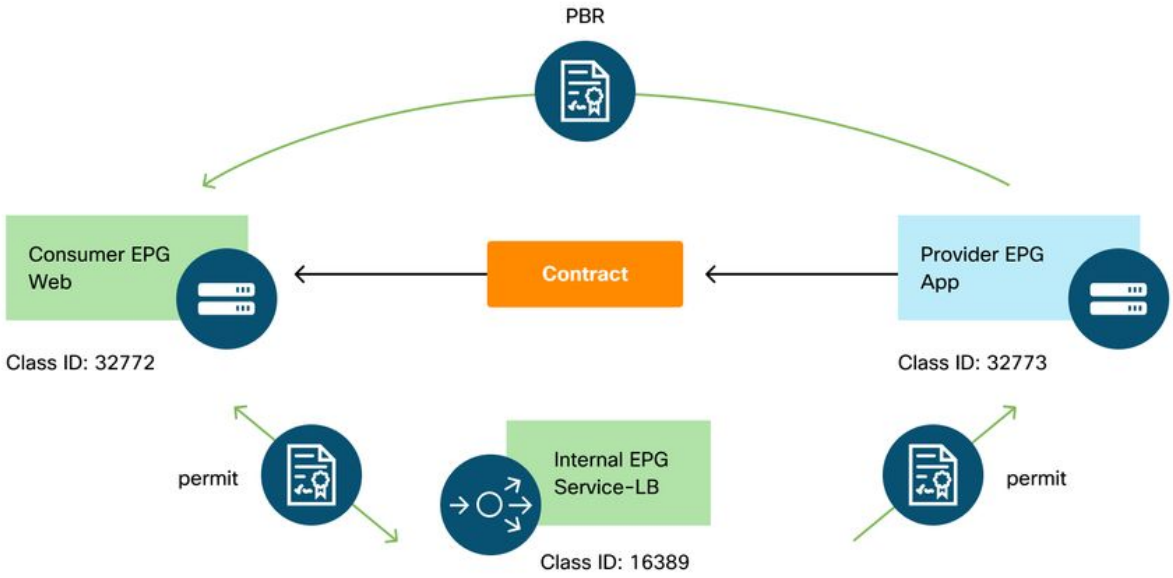
Esempio di bilanciamento del carico senza percorso di inoltro SNAT - da provider a consumer con PBR



I criteri programmati sui nodi foglia.

La figura seguente e l'output 'show zoning-rule' seguente descrivono le regole di zoning dopo la distribuzione di Service Graph. Nell'esempio, il traffico da pcTag 32772 (Web) a pcTag 16389 (Service-LB) è consentito, il traffico da pcTag 16389 (Service-LB) a pcTag 32773 (App) è consentito e il traffico da pcTag 32773 (App) a pcTag 32772 (Web) è reindirizzato a 'destgrp-31' (bilanciamento del carico).

Regole di zoning dopo l'installazione di Service Graph - servizio di bilanciamento del carico senza SNAT

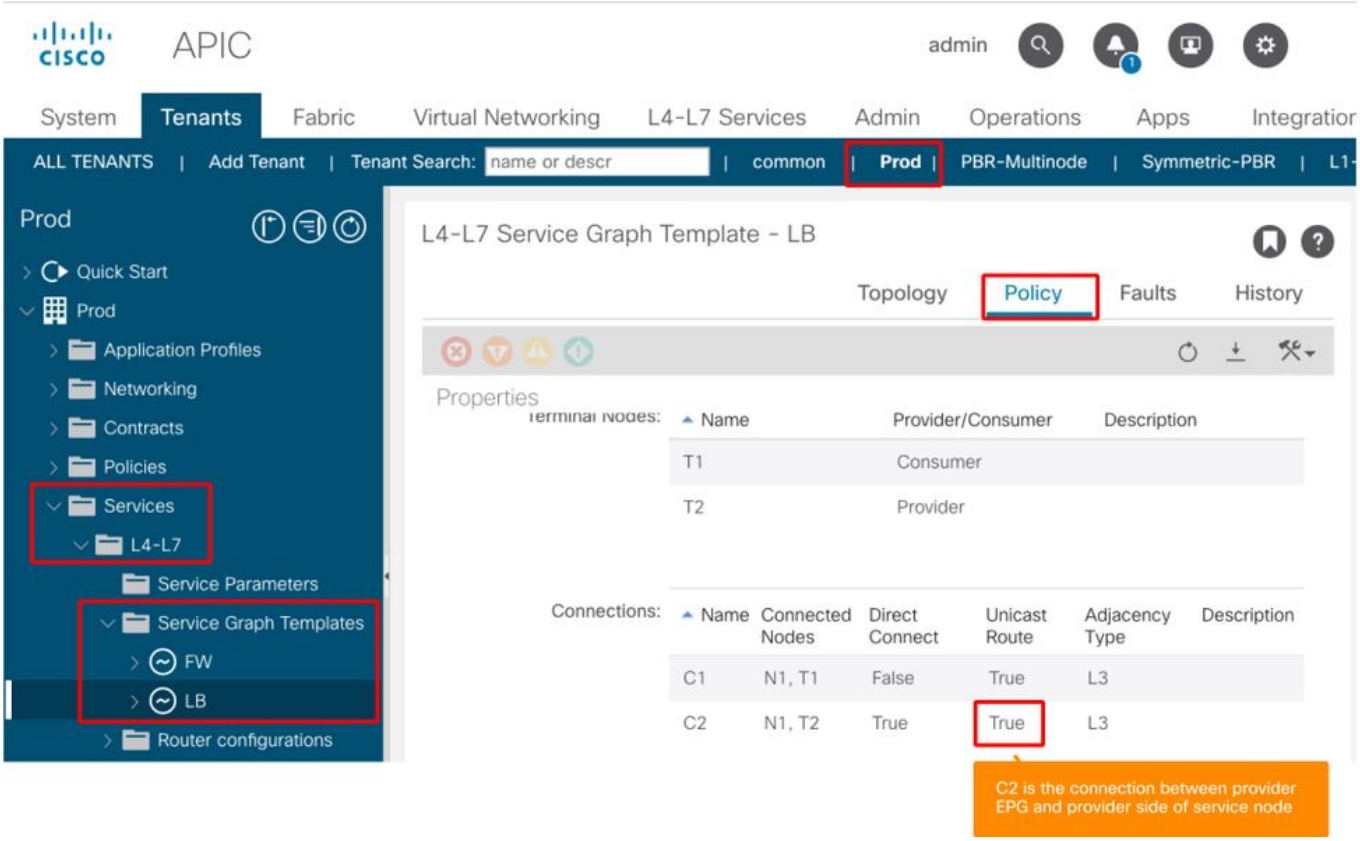


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
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)     |
...
```

Per impostazione predefinita, una regola di autorizzazione per il provider da EPG (pcTag 32773) a Service-LB (pcTag 16389) non è programmata. Per consentire la comunicazione bidirezionale tra di essi per i controlli di integrità dal bilanciamento del carico agli endpoint del provider, l'opzione Connessione diretta sulla connessione deve essere impostata su True. Il percorso è 'Tenant > L4-L7 > Service Graph Templates > Policy'. Il valore predefinito è False.

Imposta opzione di connessione diretta



Viene aggiunta una regola di autorizzazione per il provider EPG(32773) a Service-LB(16389) come indicato di seguito.

```
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. Esempio di flusso di traffico - Firewall e bilanciamento del carico senza SNAT

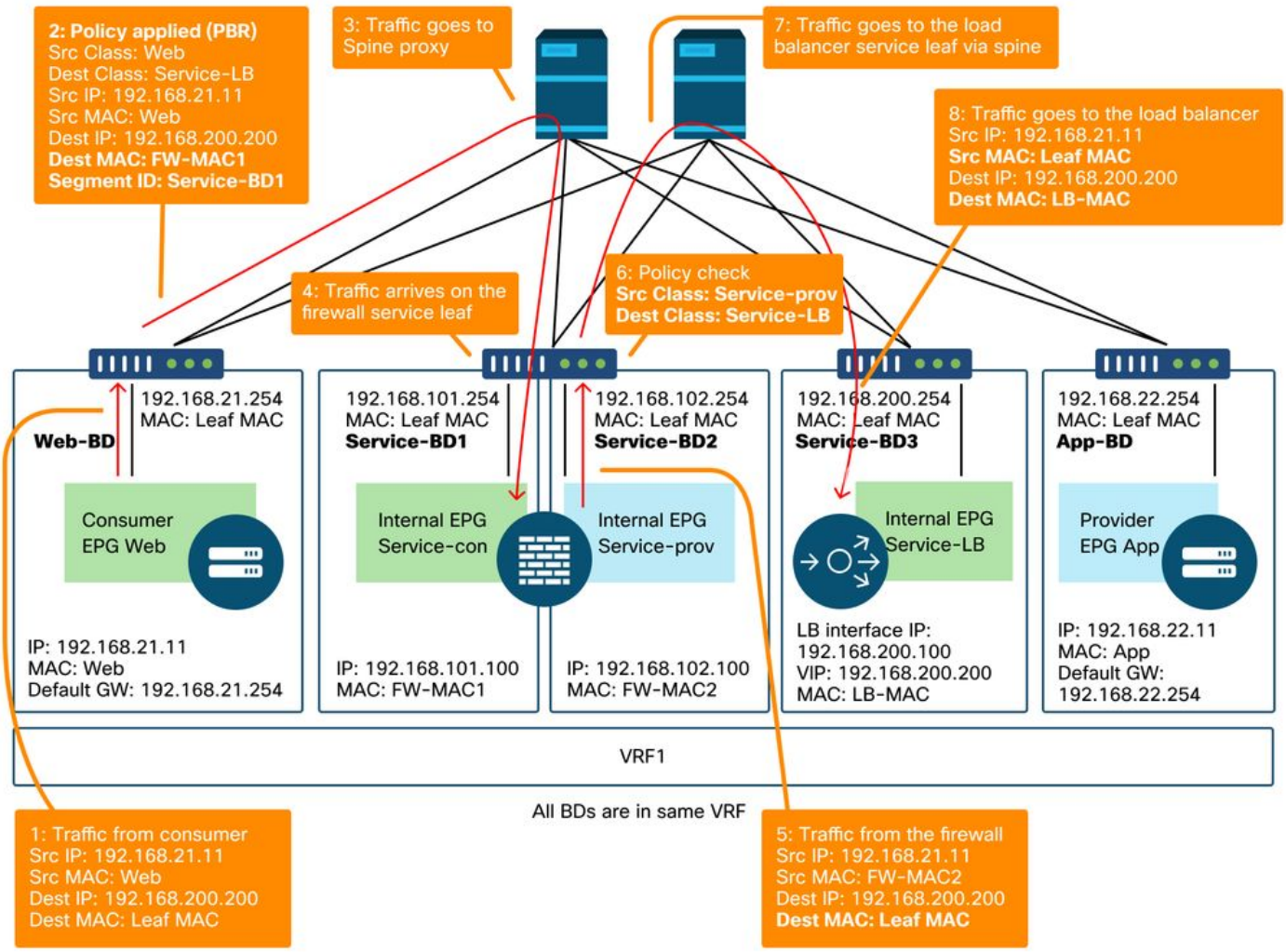
Èpossibile distribuire PBR con più funzioni di servizio in un grafico dei servizi, ad esempio firewall come primo nodo e bilanciamento del carico come secondo nodo.

Esempio di percorso del traffico

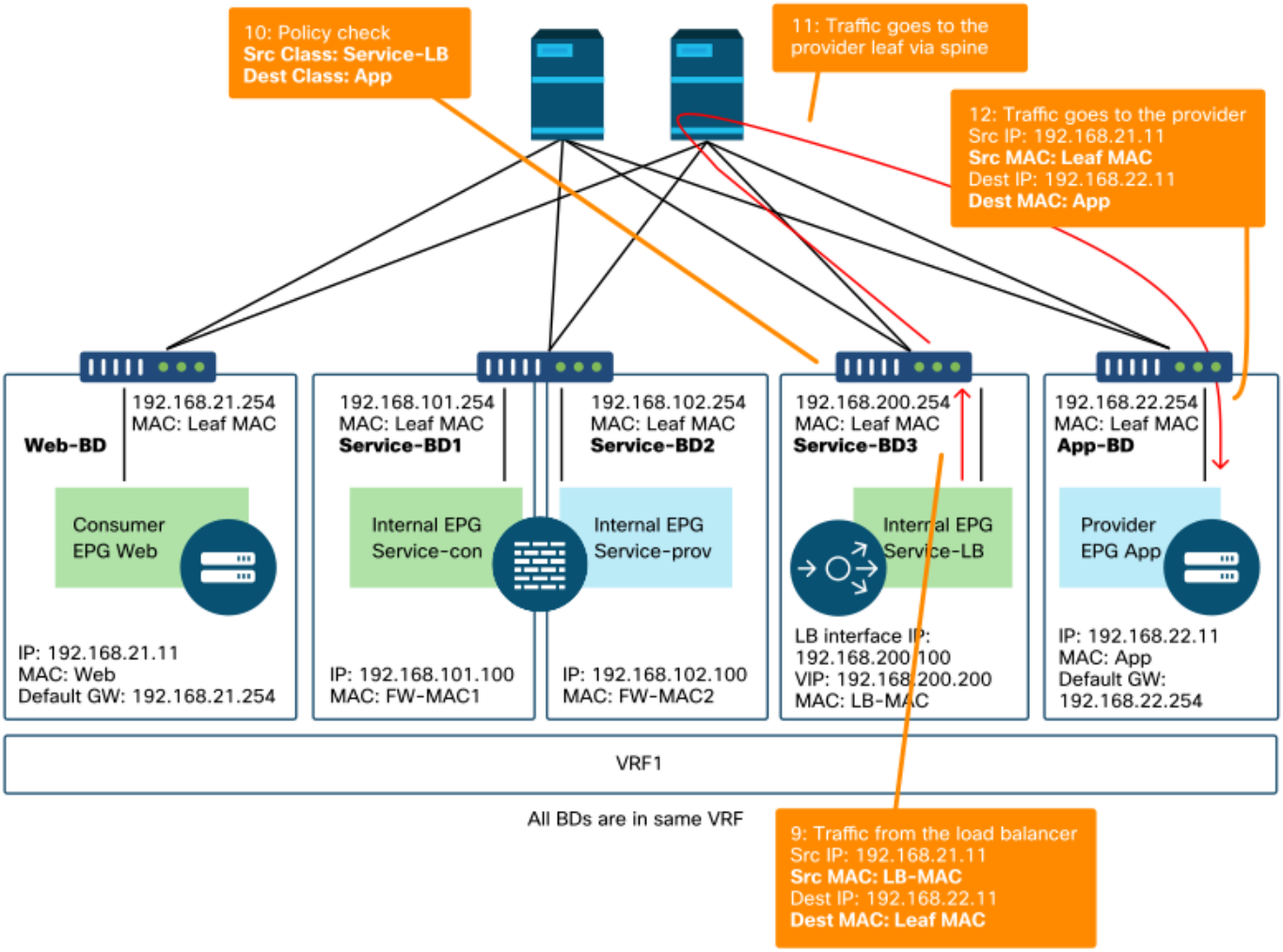
Nella figura seguente viene illustrato un esempio di flusso di traffico in entrata dal Web EPG consumer al provider EPG App con due connessioni: Uno viene inviato da un endpoint nel Web

EPG del consumer all'indirizzo VIP del servizio di bilanciamento del carico tramite il firewall, l'altro viene inviato dal servizio di bilanciamento del carico a un endpoint nell'app EPG del provider. Il traffico in ingresso destinato al VIP viene reindirizzato al firewall e quindi viene indirizzato al bilanciamento del carico senza PBR. Il bilanciamento del carico modifica l'IP di destinazione in uno degli endpoint in App EPG associati all'indirizzo VIP, ma non converte l'IP di origine. Quindi, il traffico passa all'endpoint del provider.

Esempio di percorso di inoltro del firewall e del bilanciamento del carico senza SNAT - da consumer a VIP e da bilanciamento del carico a provider



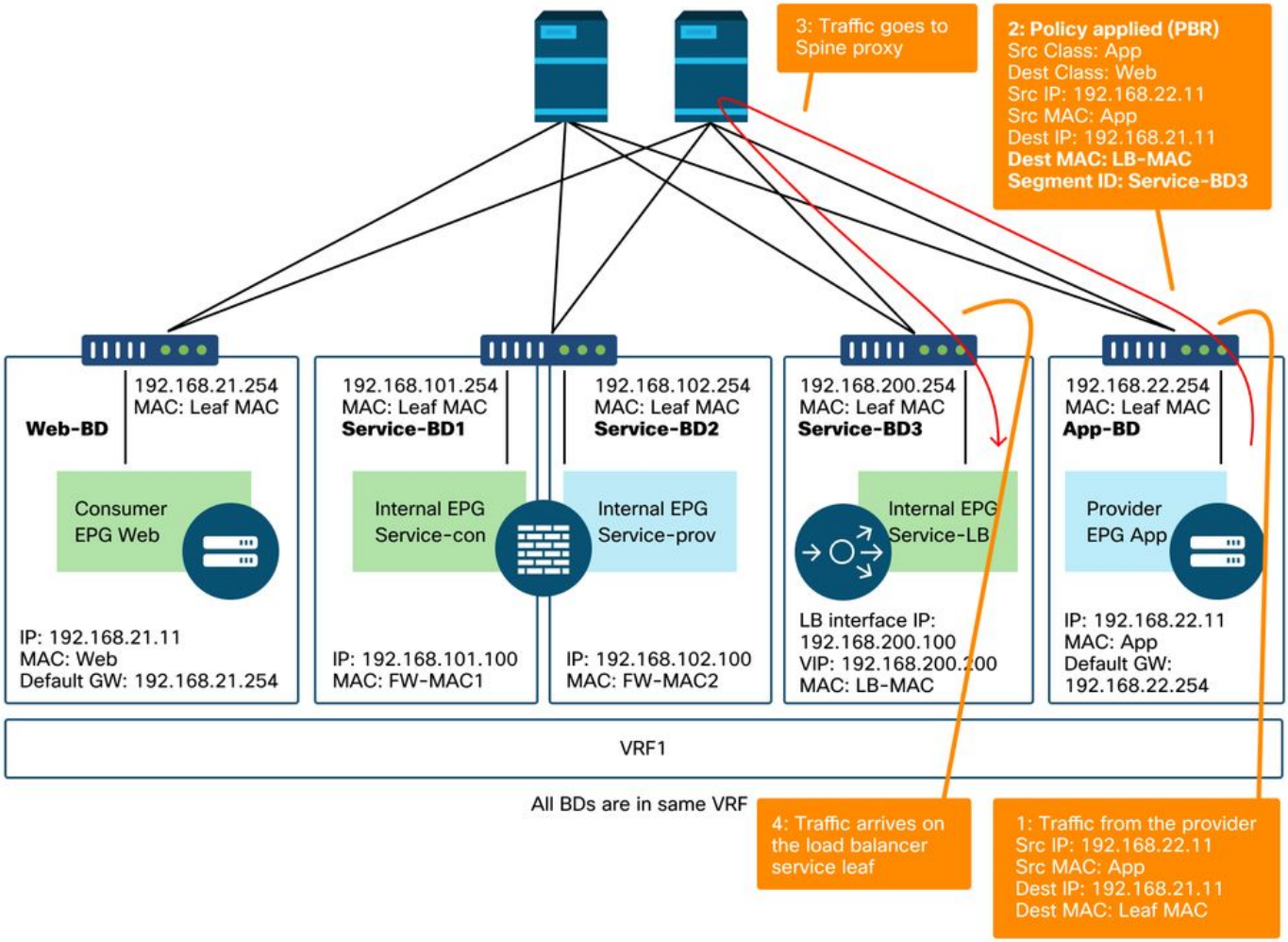
Esempio di percorso di inoltro del firewall e del bilanciamento del carico senza SNAT - da consumer a VIP e da bilanciamento del carico a provider (continua)

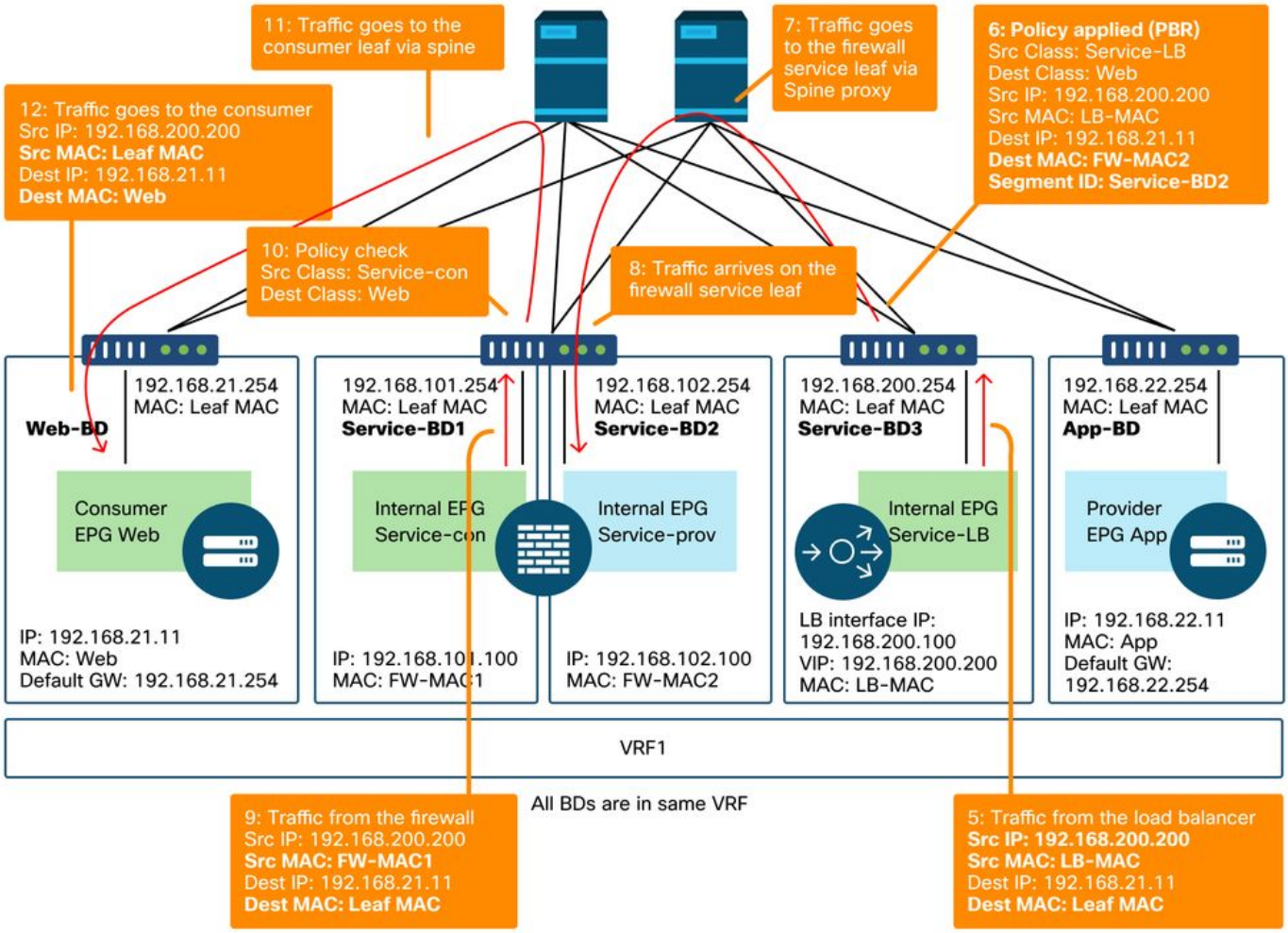


Nella figura seguente viene illustrato il flusso del traffico di ritorno dall'app EPG del provider al Web EPG del consumer. Poiché il traffico di ritorno è destinato all'IP di origine, il PBR è necessario per riportare il traffico di ritorno nel bilanciamento del carico.

Dopo il reindirizzamento del traffico dall'endpoint del provider all'endpoint del consumer al bilanciamento del carico, il bilanciamento del carico modifica l'IP di origine in VIP. Il traffico torna dal bilanciamento del carico e viene reindirizzato al firewall. Quindi, il traffico torna dal firewall e torna all'endpoint di tipo consumer.

Esempio di firewall e bilanciamento del carico senza percorso di inoltro SNAT - da provider a consumer

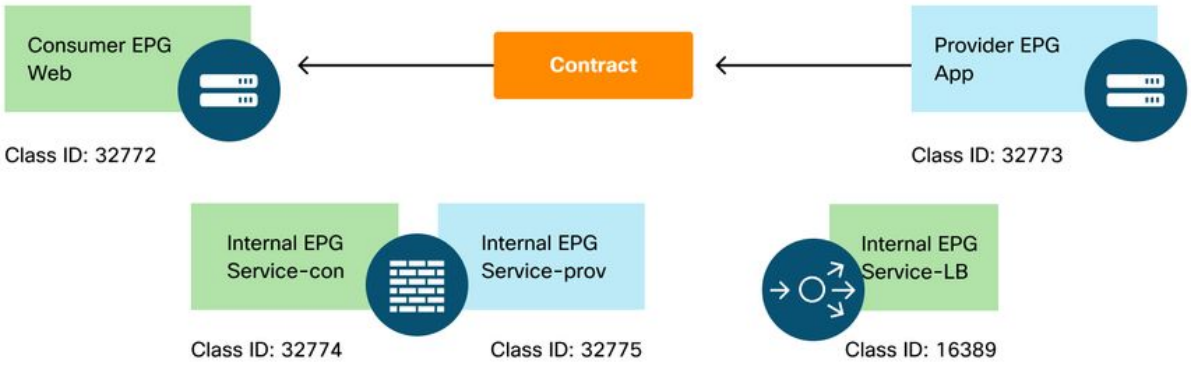

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



I criteri programmati sui nodi foglia

La figura seguente e l'output 'show zoning-rule' mostrato di seguito descrivono le regole di zoning dopo la distribuzione di Service Graph. Nell'esempio, il traffico da pcTag 32772 (Web) a pcTag 16389 (Service-LB) viene reindirizzato a 'destgrp-32' (lato consumer del firewall), il traffico da pcTag 32773 (App) a pcTag 32772 (Web) viene reindirizzato a 'destgrp-33' (load balancer) e il traffico da pcTag 16389 (Service-LB) a pcTag32 772 (Web) viene reindirizzato a 'destgrp-34' (lato provider del firewall).

Regole di zoning dopo la distribuzione di Service Graph: firewall e bilanciamento del carico senza 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)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

Nell'esempio precedente, l'opzione Connessione diretta è impostata su 'True' nella connessione tra il lato provider del servizio di bilanciamento del carico e il provider EPG. Deve essere abilitato per il controllo dello stato dal bilanciamento del carico agli endpoint del provider. Il percorso è 'Tenant > L4-L7 > Service Graph Templates > Policy'. Fare riferimento alla figura 'Imposta opzione

di connessione diretta'.

3. Servizio condiviso (contratto Inter-VRF)

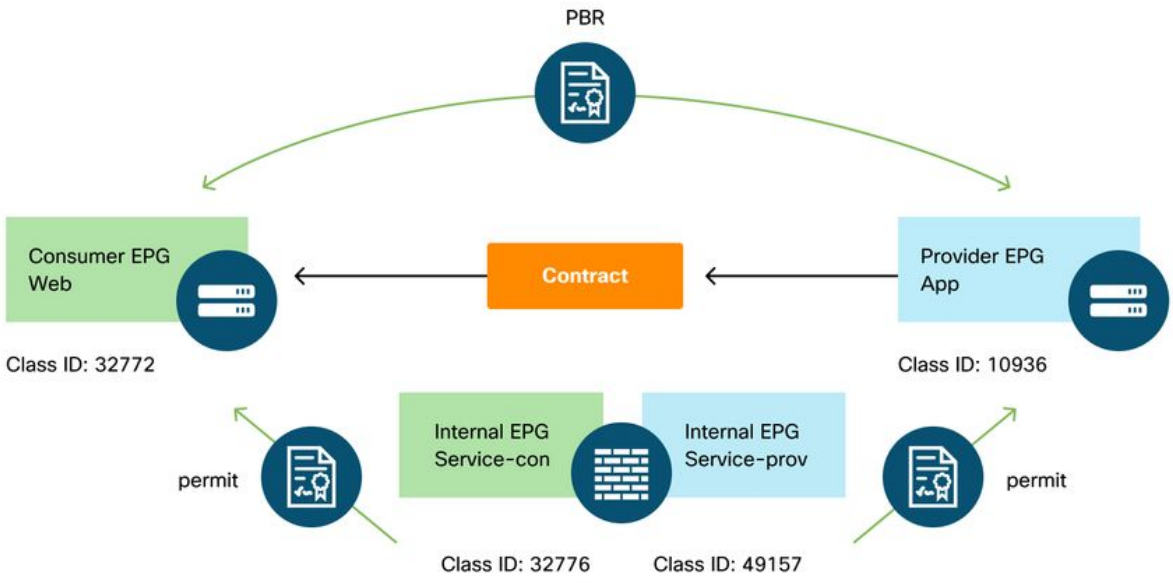
La funzione PBR può essere abilitata nel contratto inter-VRF. Questa sezione spiega come le regole di zoning sono programmate nel caso di un contratto EPG-EPG inter-VRF.

I criteri programmati sui nodi foglia

In caso di contratto tra EPG e EPG inter-VRF, la politica viene sempre applicata nel VRF consumer. Pertanto, il reindirizzamento avviene sul VRF consumer. Per altre combinazioni, fare riferimento alla tabella "Dove viene applicata la policy?" nella sezione "Inoltro".

La figura seguente e l'output 'show zoning-rule' seguente descrivono le regole di zoning dopo la distribuzione di Service Graph. Nell'esempio, il traffico tra pcTag 32772 (Web) e pcTag 10936 (App) viene reindirizzato a 'destgrp-36' (lato consumer del nodo del servizio) e il traffico tra pcTag 10936 (App) e pcTag 32772 (Web) viene reindirizzato a 'destgrp-35' (lato provider del nodo del servizio). Entrambe sono applicate nel VRF1, che è VRF consumer. Il traffico da pcTag 32776 (lato consumer del firewall) a pcTag 32772 (Web) è consentito in VRF1.

Regole di zoning dopo l'installazione di Service Graph - contratto inter-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)      |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+------------------------+
```

Il traffico da pcTag 49157 (lato provider del firewall) a pcTag 10936 (app) è consentito in VRF2 perché entrambi si trovano in 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)    |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).