ACI-beleidsgebaseerde omleiding voor probleemoplossing

Inhoud

Inleiding
Achtergrondinformatie
Beleidsgebaseerde omleiding - Overzicht
Implementatie van servicegrafiek voor probleemoplossing
1. Controleer de configuratiestappen en de fout
2. Controleer de implementatie van een servicegrafiek in de gebruikersinterface
Doorsturen van PBR voor probleemoplossing
1. Controleer VLAN's worden geïmplementeerd en endpoints worden geleerd op het bladknooppunt
2. Controleer de verwachte verkeerspaden
Waar wordt het beleid uitgevoerd?
3. Controleer of verkeer wordt omgeleid naar het serviceknooppunt
4. Controleer het op de bladknooppunten geprogrammeerde beleid
Andere voorbeelden van verkeersstromen
1. Taakverdeling zonder SNAT
Voorbeeld van verkeerspad
Het geprogrammeerde beleid op de bladknooppunten.
2. Traffic flow-voorbeeld - firewall en taakverdeling zonder SNAT
Voorbeeld van verkeerspad
Het geprogrammeerde beleid op de bladknooppunten
3. Gedeelde service (Inter-VRF-contract)
Het geprogrammeerde beleid op de bladknooppunten

Inleiding

Dit document beschrijft stappen om een ACI-scenario (PBR) op basis van beleid te begrijpen en problemen op te lossen.

Achtergrondinformatie

Het materiaal van dit document is afgeleid uit het boek Problemen oplossen van Cisco Application Centric Infrastructure, Second Edition, met name het **Policy-Based Redirect - Overview, Policy-Based Redirect - Service Graph Implementation, Policy-Based Redirect - Forwarding en Policy-Based Redirect - Andere** hoofdstukken met **verkeersstromen**.

Beleidsgebaseerde omleiding - Overzicht

Dit hoofdstuk verklaart het oplossen van problemen voor unmanaged mode Service Graph met op beleid gebaseerde Redirect (PBR).

Het volgende is de typische stappen voor probleemoplossing. In dit hoofdstuk wordt uitgelegd hoe u stap 2 en 3 kunt verifiëren, die specifiek zijn voor PBR. Raadpleeg voor stap 1 en 4 de hoofdstukken: "Intra-Fabric-doorsturen", "Extern doorsturen" en "Beveiligingsbeleid".

1. Controleer het verkeer zonder PBR-servicegrafiek: De eindpunten van de consument en van de leverancier worden geleerd.De eindpunten van de consument en van de leverancier kunnen communiceren.
2. Controleer of de servicegrafiek is geïmplementeerd: Geïmplementeerde grafiekinstanties hebben geen fout.VLAN's en class ID's voor serviceknooppunten worden geïmplementeerd.De serviceknooppunten worden geleerd.
3. Controleer het verzendpad: Het controlebeleid is geprogrammeerd op de bladknooppunten.Leg het verkeer op het serviceknooppunt vast om te bevestigen of het verkeer wordt omgeleid.Leg het verkeer op het ACI-blad vast om te bevestigen of het verkeer na PBR naar de ACI-structuur terugkeert.
4. Controleer of het verkeer op het eindpunt van de consument en de provider aankomt en of het eindpunt het retourverkeer genereert.

Dit document heeft geen betrekking op ontwerp- of configuratieopties. Zie voor deze informatie het "ACI PBR White Paper" op Cisco.com

In dit hoofdstuk impliceren serviceknooppunt en serviceknooppunt het volgende:

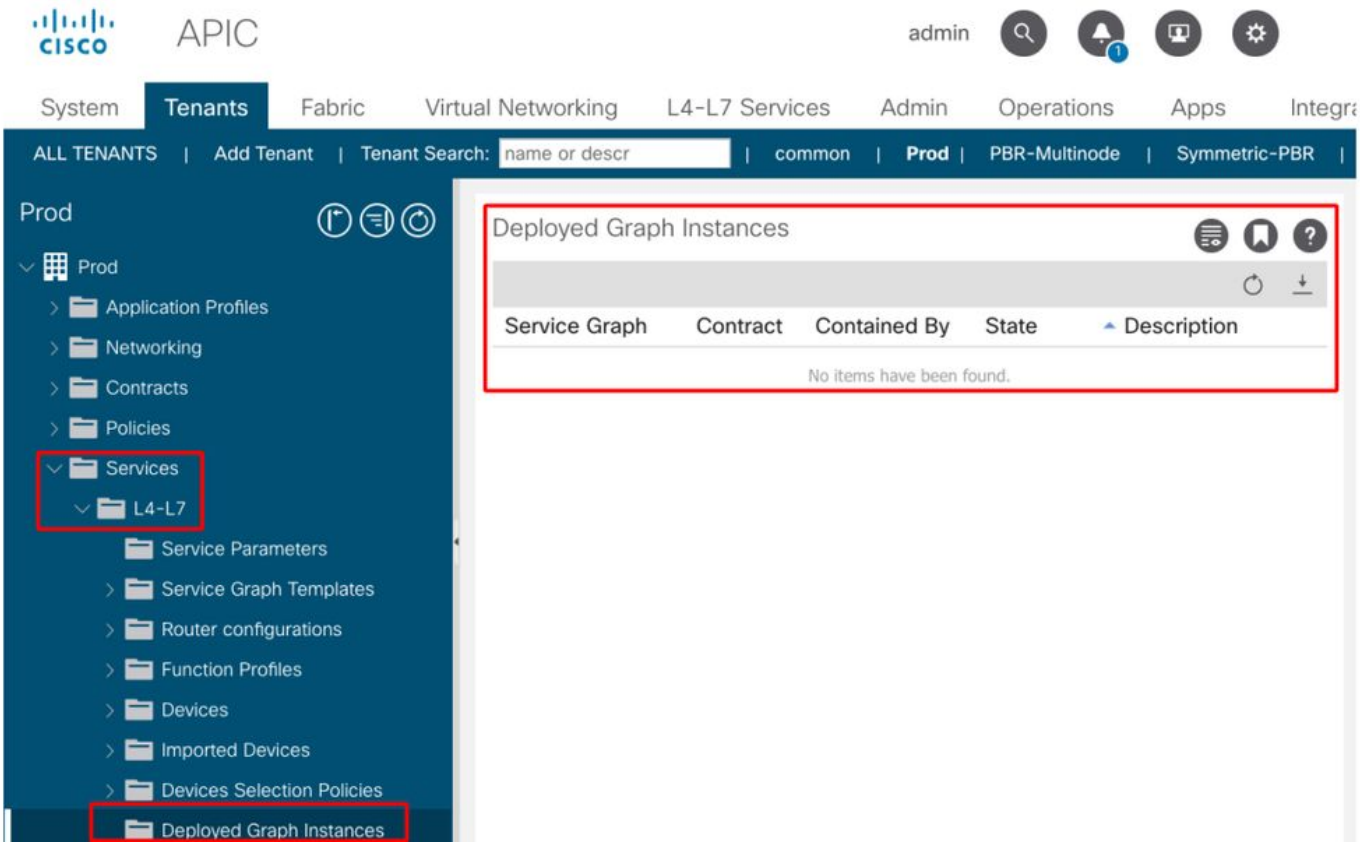
- Service-knooppunt — een extern knooppunt waarnaar PBR het verkeer omleidt, zoals een firewall of taakverdeling.
- Serviceblad — een ACI-blad dat is verbonden met een serviceknooppunt.

Implementatie van servicegrafiek voor probleemoplossing

In dit hoofdstuk wordt een voorbeeld van probleemoplossing uitgelegd waarbij geen servicegrafiek wordt geïmplementeerd.

Nadat een beleid voor servicegrafiek is gedefinieerd en op een contractonderwerp is toegepast, moet er een geïmplementeerd grafiekvoorbeeld op de ACI GUI staan. In de onderstaande afbeelding ziet u het scenario voor probleemoplossing waarbij de servicegrafiek niet wordt weergegeven zoals geïmplementeerd.

Service Graph wordt niet weergegeven als een geïmplementeerde grafische instantie.



1. Controleer de configuratiestappen en de fout

De eerste stap van het oplossen van problemen is te controleren de noodzakelijke componenten zijn geconfigureerd zonder enige fout. Er wordt van uitgegaan dat onderstaande algemene configuraties al zijn uitgevoerd:

- VRF en BD's voor consumenten-EPG, provider-EPG en serviceknooppunt
- De consument en leverancier EPG.
- Het contract en de filters.

Het is de moeite waard om te vermelden dat een EPG voor het serviceknooppunt niet handmatig hoeft te worden gemaakt. Het wordt gemaakt via Service Graph-implementatie.

De stappen voor de Service Graph met PBR-configuratie zijn als volgt:

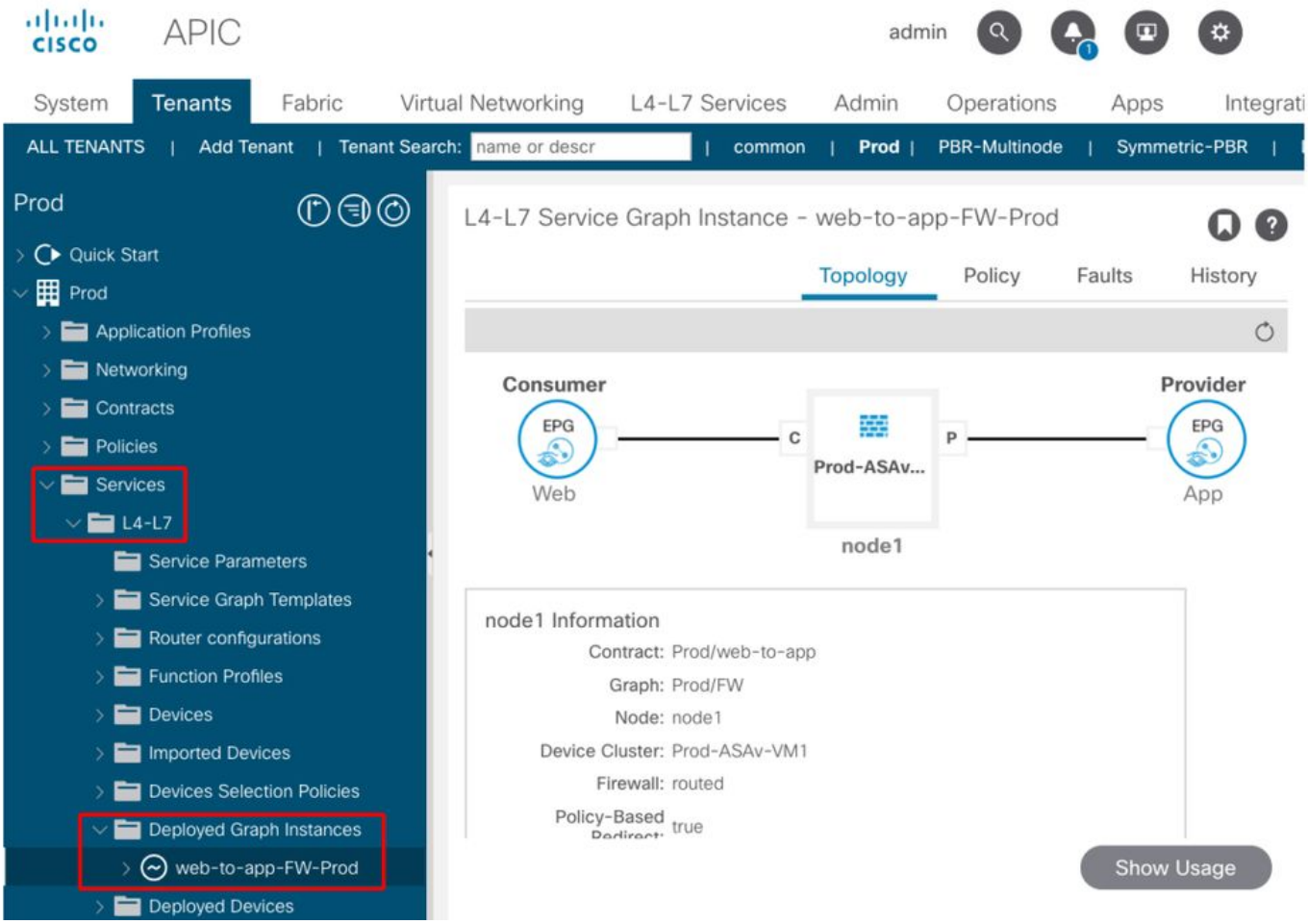
- Maak het L4-L7 apparaat (logisch apparaat).
- Maak de servicegrafiek.
- Maak het PBR beleid.
- Maak het apparaatselectiebeleid.
- Koppel de servicegrafiek aan het contractonderwerp.

2. Controleer de implementatie van een servicegrafiek in de gebruikersinterface

Nadat een servicegrafiek is gekoppeld aan het contractonderwerp, moet voor elk contract met Service Graph een geïmplementeerd grafiekexemplaar worden weergegeven (zie onderstaande afbeelding).

De locatie is 'Huurder > Diensten > L4-L7 > Gebruikte Grafische Instanties'

Geïmplementeerd grafiekexemplaar



Als een geïmplementeerde grafische instantie niet verschijnt, is er iets mis met de contractconfiguratie. Belangrijke redenen kunnen zijn:

- Het contract heeft geen consument of leverancier EPG.
- De contractant heeft geen filter.
- Het contractwerkingsgebied is VRF alhoewel het voor de communicatie tussen VRF of inter-tenant EPG is.

Als de Service Graph-instantiatie mislukt, worden fouten in de geïmplementeerde graph-instantie verhoogd, wat betekent dat er iets mis is met de configuratie van de Service Graph. De typische die fouten door configuratie worden veroorzaakt zijn de volgende:

F1690: Configuratie is ongeldig vanwege fout bij toewijzing van id

Deze fout geeft aan dat het ingesloten VLAN voor het serviceknooppunt niet beschikbaar is. Er is bijvoorbeeld geen beschikbaar dynamisch VLAN in de VLAN-pool die is gekoppeld aan het VMM-domein dat wordt gebruikt in het logische apparaat.

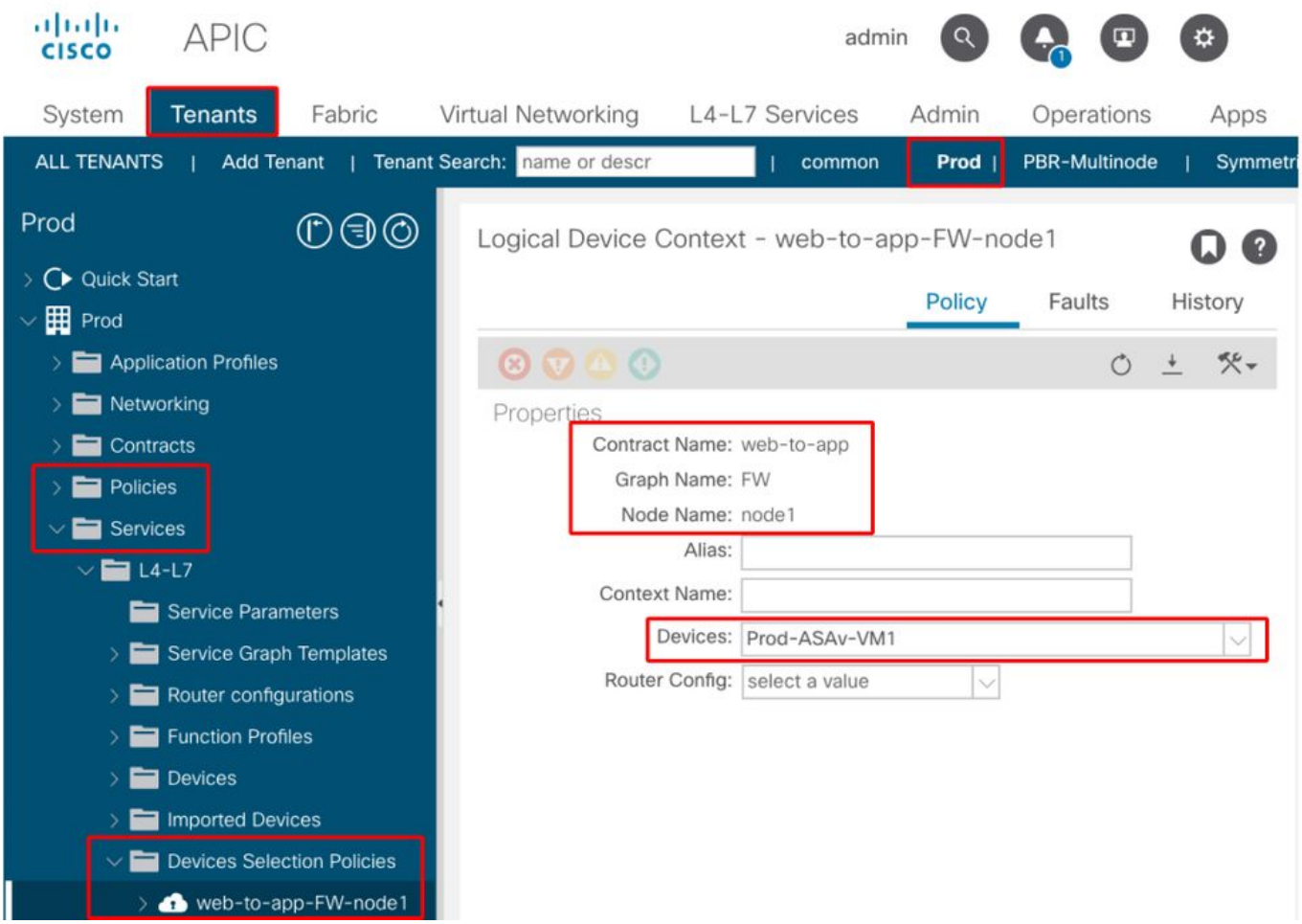
Resolutie: Controleer de VLAN-pool in het domein dat wordt gebruikt voor het logische apparaat. Controleer ingesloten VLAN in de interface van het logische apparaat als het zich in een fysiek domein bevindt. De locaties zijn 'Huurder > Diensten > L4-L7 > Apparaten en Fabric > Toegangsbeleid > Pools > VLAN'.

F1690: De configuratie is ongeldig vanwege het ontbreken van een apparaatcontext voor LDev

Deze fout geeft aan dat het logische apparaat niet kan worden gevonden voor de Service Graph-rendering. Er is bijvoorbeeld geen beleid voor apparaatselectie dat voor het contract is afgestemd op de servicegrafiek.

Resolutie: Controleer of het beleid voor apparaatselectie is gedefinieerd. Het Beleid van de Selectie van het apparaat verstrekt een selectiecriterium voor een de dienstapparaat en zijn connectors. De criteria zijn gebaseerd op een contractnaam, een Service Graph-naam en een nodenaam in de Service Graph. De locatie is 'Huurder > Diensten > L4-L7 > Apparaatselectiebeleid'.

Beleid voor apparaatselectie controleren



F1690: De configuratie is ongeldig omdat er geen clusterinterface is gevonden

Deze fout geeft aan dat de clusterinterface voor het serviceknooppunt niet kan worden gevonden. De clusterinterface wordt bijvoorbeeld niet gespecificeerd in het beleid voor apparaatselectie.

Resolutie: Controleer of de clusterinterface in het selectiebeleid voor apparaten is gespecificeerd en of de naam van de connector correct is (afbeelding hieronder).

F1690: Configuratie is ongeldig vanwege geen BD gevonden

Deze fout geeft aan dat de BD voor het serviceknooppunt niet kan worden gevonden. De BD wordt bijvoorbeeld niet gespecificeerd in het beleid voor apparaatselectie.

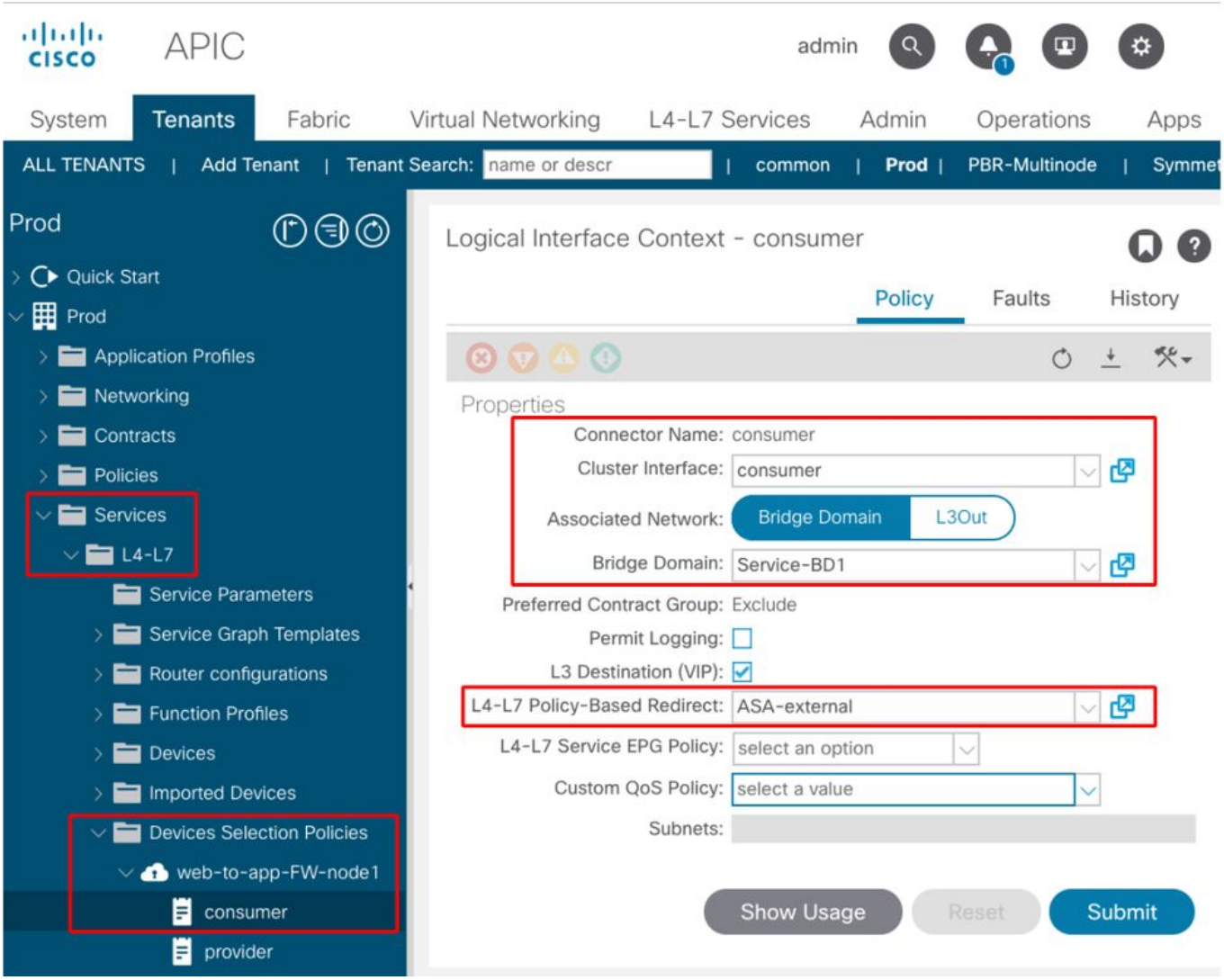
Resolutie: Controleer BD in het beleid voor apparaatselectie is gespecificeerd en de naam van de connector correct is (afbeelding hieronder).

F1690: De configuratie is ongeldig vanwege het ongeldige beleid voor serviceomleiding

Deze fout geeft aan dat het PBR-beleid niet is geselecteerd, ook al is redirect ingeschakeld voor de servicefunctie in de Servicegrafiek.

Resolutie: Selecteer PBR-beleid in het beleid voor apparaatselectie (afbeelding hieronder).

Logische interfaceconfiguratie in beleid voor apparaatselectie



Doorsturen van PBR voor probleemoplossing

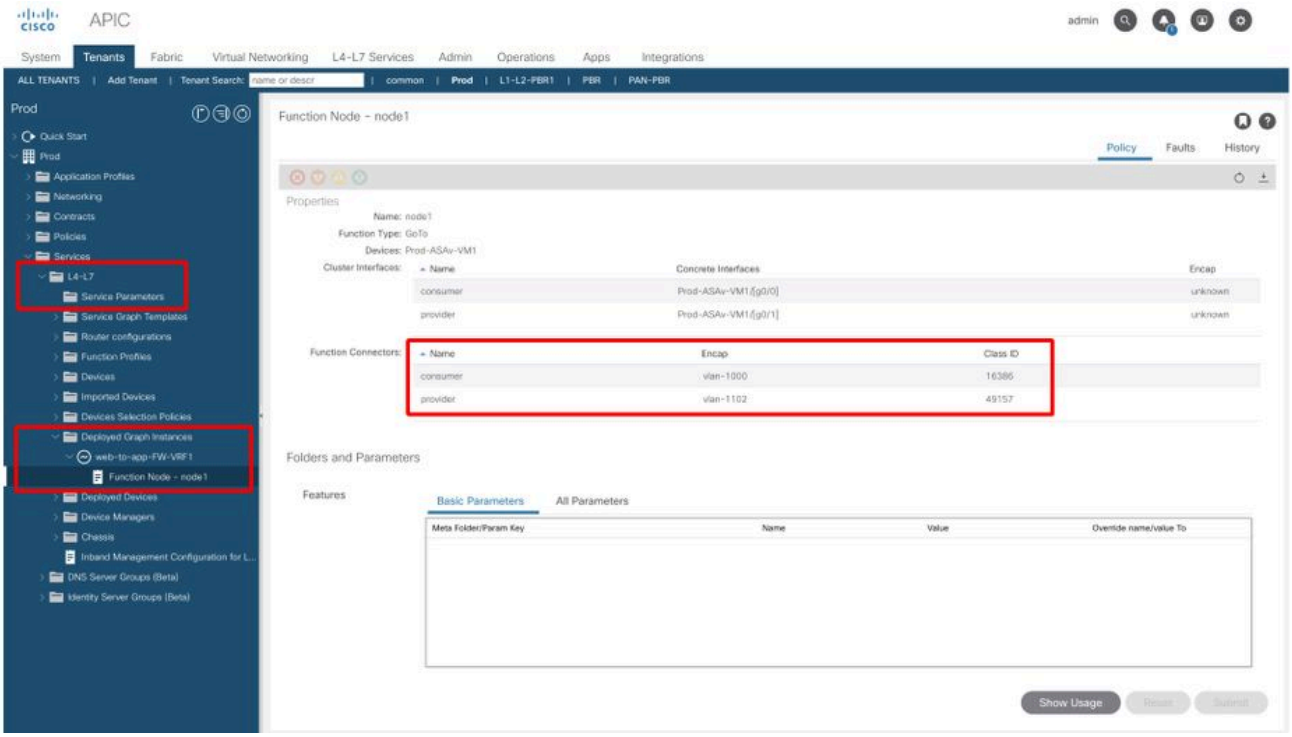
Dit hoofdstuk legt de stappen voor probleemoplossing uit voor het PBR-verzendpad.

1. Controleer VLAN's worden geïmplementeerd en endpoints worden geleerd op het bladknooppunt

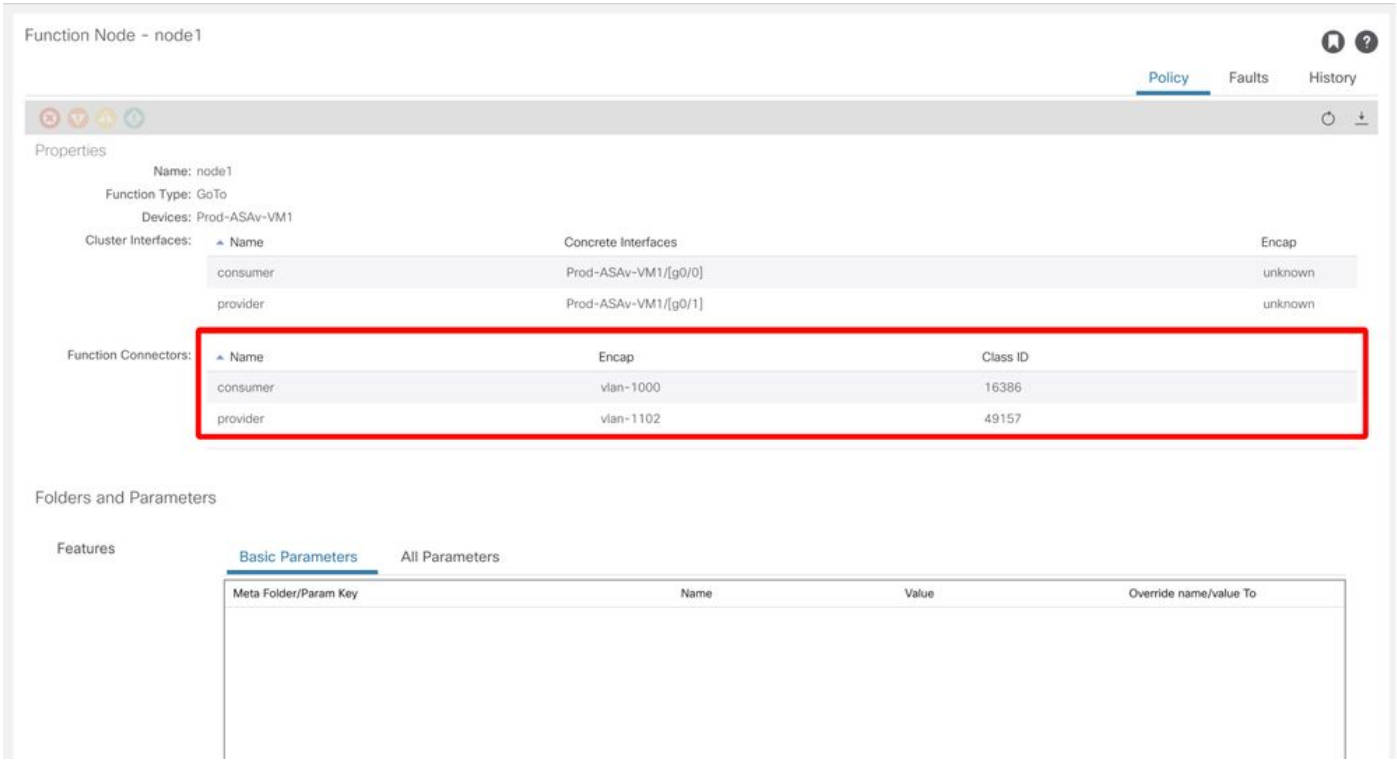
Zodra een servicegrafiek zonder fouten is geïmplementeerd, worden EPG's en BD's voor een serviceknooppunt gemaakt. De onderstaande afbeelding toont waar de ingekapselde VLAN-ID's en klasse-ID's van serviceknoopinterfaces (Service EPG's) moeten worden gevonden. In dit voorbeeld, is de kant van de consument van een firewall klasse-ID 16386 met VLAN-encap 1000 en is de leverancierskant van een firewall klasse-ID 49157 met VLAN-encap 1102.

De locatie is 'Huurder > Diensten > L4-L7 > Geïmplementeerde Grafiek instanties > Functie knooppunten'.

Service-knooppunt



ID voor interfaceklasse-id voor serviceknooppunt



Deze VLAN's worden geïmplementeerd op de interfaces van de servicelaag waar de serviceknooppunten zijn aangesloten. De plaatsing van VLAN en eindpunt het leren status kunnen worden gecontroleerd door "uitgebreid tonen VLAN"en "tonen eindpunt"op de de dienstbladknoop CLI te gebruiken.

```
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
```

Als IP-eindpunten van de serviceknooppunten niet worden geleerd als eindpunten in de ACI-fabric, is het waarschijnlijk dat er een connectiviteits- of configuratieprobleem is tussen het servicelaag en het serviceknooppunt. Controleer de volgende status:

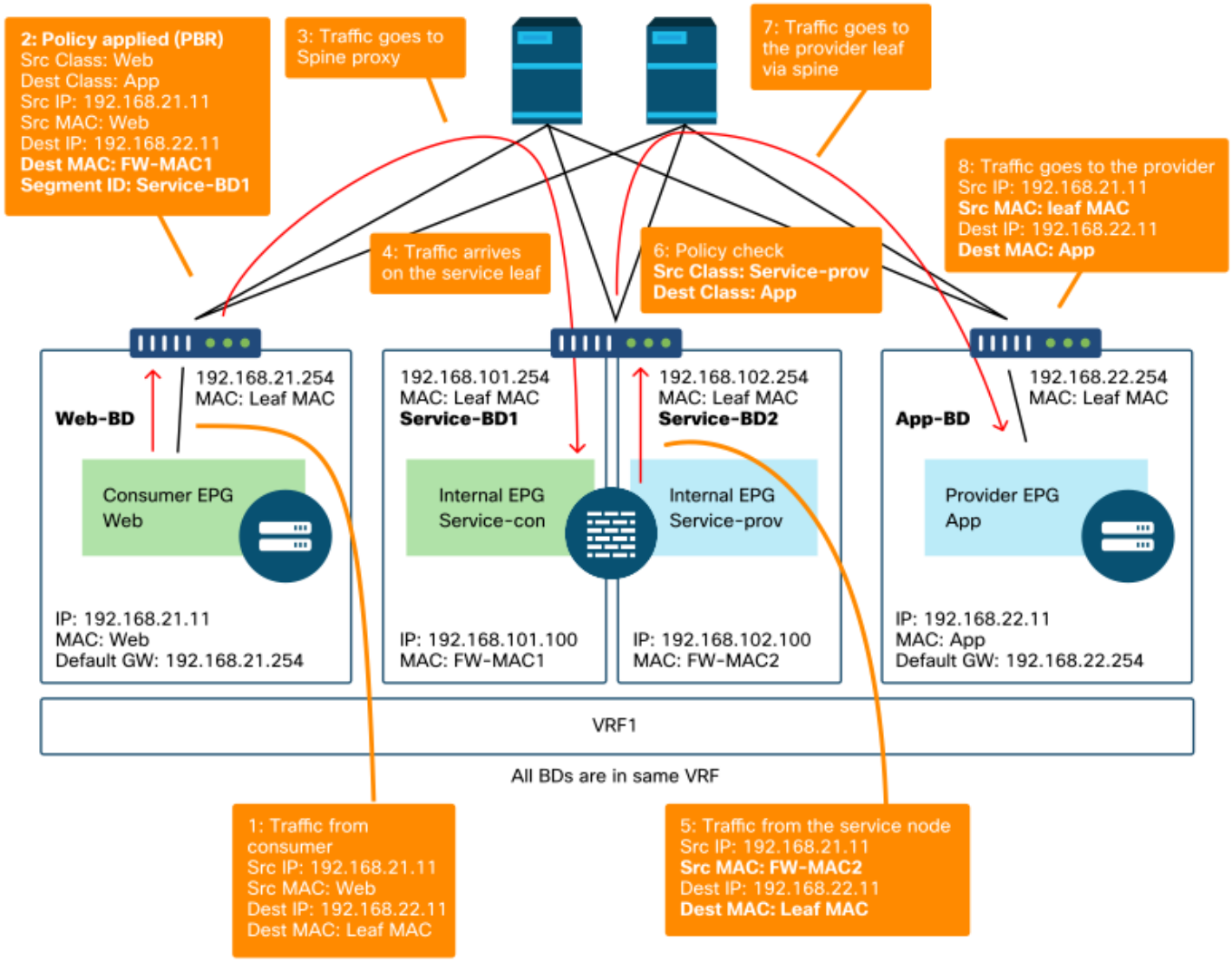
- Het serviceknooppunt is verbonden met de juiste bladneerwaartse poort. Als het serviceknooppunt zich in een fysiek domein bevindt, moet de leaf statische path end encap VLAN worden gedefinieerd in het logische apparaat.Als het serviceknooppunt zich in een VMM-domein bevindt, controleer dan of het VMM-domein werkt en of de poortgroep die via Service Graph is gemaakt, correct aan de serviceknooppunt VM is gekoppeld.
- De bladeserverpoort die is aangesloten op het serviceknooppunt of de hypervisor waar de serviceknooppunt VM zich bevindt, is UP.
- Het serviceknooppunt heeft het juiste VLAN- en IP-adres.
- De intermediaire switch tussen het de dienstblad en de de dienstknoop heeft de correcte configuratie van VLAN.

2. Controleer de verwachte verkeerspaden

Als het verkeer van begin tot eind ophoudt met werken zodra PBR is ingeschakeld, zelfs als de serviceknooppunten in de ACI-fabric zijn geleerd, is de volgende stap van probleemoplossing om te controleren wat de verwachte verkeerspaden zijn.

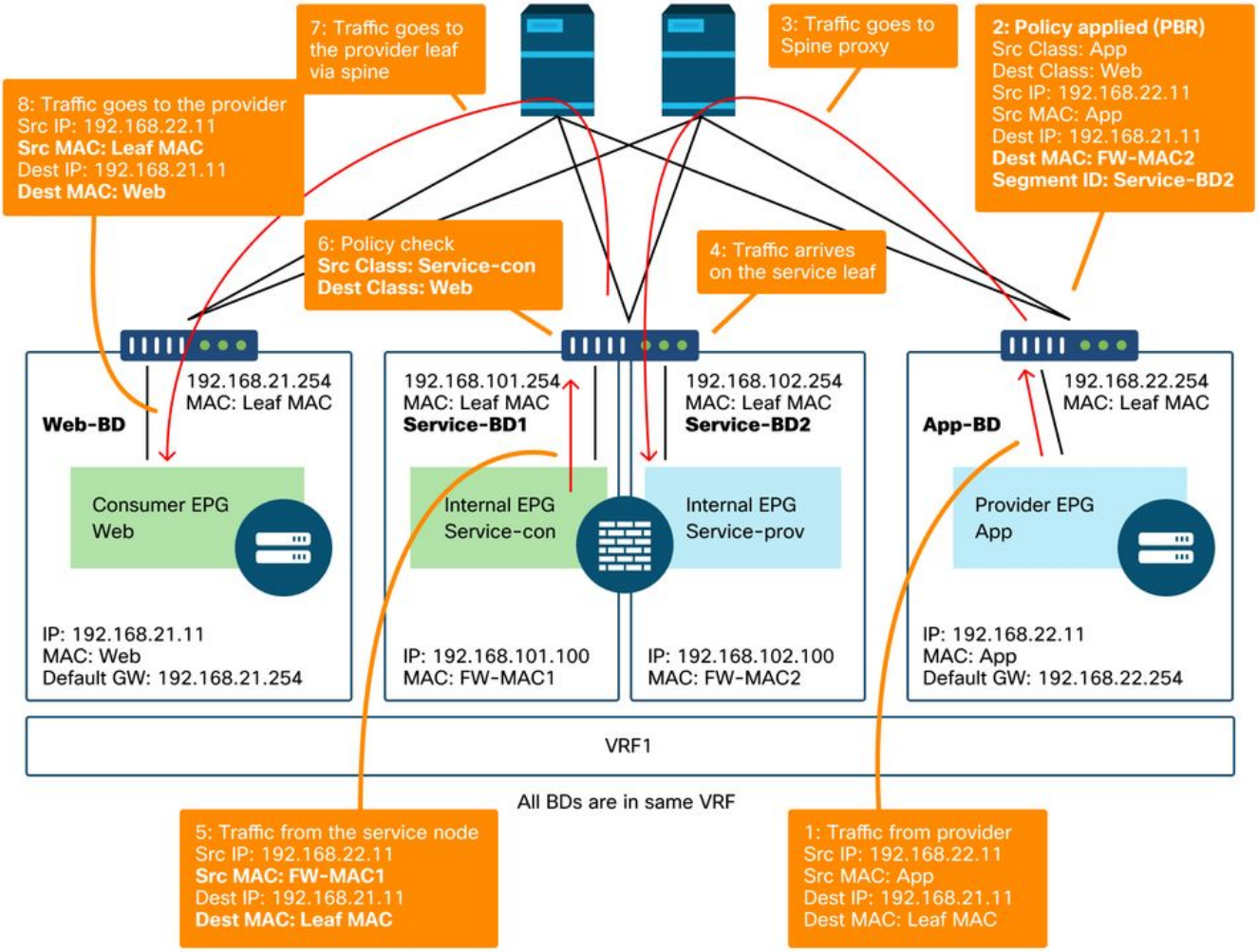
Cijfers 'PBR Forwarding Path Voorbeeld - Consumer to Provider' en 'PBR Forwarding Path Voorbeeld - Provider to Consumer' illustreren een voorbeeld van een doorsturen pad van het invoegen van een firewall met PBR tussen een consumenteneindpunt en een provider-eindpunt. De veronderstelling is dat de eindpunten reeds op bladknooppunten worden geleerd.

PBR-voorbeeld van verzendpad - consument naar provider



Opmerking: Aangezien de bron-MAC niet wordt gewijzigd in ACI-bladMAC, mag de PBR-knooppunt geen op MAC gebaseerde brondoorgifte gebruiken als het eindpunt voor consumenten en de PBR-knooppunt niet in dezelfde BD staan

PBR-voorbeeld van verzendpad - provider naar consument



Opmerking: Het is vermeldenswaard dat het beleid PBR op of consument of leveranciersblad wordt afgedwongen en wat ACI PBR doet is bestemming MAC herschrijven zoals getoond in cijfers "PBR die wegvoorbeeld door:sturen - consument aan leverancier"en "PBR die wegvoorbeeld door:sturen - leverancier aan consument". Het bereiken van de PBR-bestemming MAC gebruikt altijd een spinproxy, zelfs als het broneindpunt en de PBR-bestemming MAC onder hetzelfde blad liggen.

Hoewel de cijfers 'PBR die wegvoorbeeld door:sturen - consument aan leverancier' en 'PBR die wegvoorbeeld door:sturen - leverancier aan consument' een voorbeeld tonen van waar het verkeer zou worden opnieuw gericht, waar het beleid wordt afgedwongen afhankelijk van contractconfiguratie en eindpunt het leren status. De tabel "Waar beleid wordt afgedwongen" vat samen waar beleid wordt afgedwongen één ACI-site. Waar beleid wordt afgedwongen in Multi-Site is anders.

Waar wordt het beleid uitgevoerd?

scenario	VRF-afdwingingsmodus	Consument	Provider	Gedwongen beleid
Intra-VRF	Ingang/uitgang	EPG	EPG	·Als eindpunt bestemming wordt aangeleerd: indringblad* ·Als eindpunt bestemming niet wordt geleerd: uitreisblad
	Ingress	EPG	L3Out-	Consumentenblad (niet-grensblad)

			EPG	
	Ingress	L3Out-EPG	EPG	Dienstenblad (niet-grensblad)
	uitgang	EPG	L3Out-EPG	Grensblad -> niet-grensverkeer ·Als eindpunt bestemming wordt aangeleerd: grensblad
	uitgang	L3Out-EPG	EPG	·Als eindpunt bestemming niet wordt geleerd: niet-grensblad Buitengrensblad-> grensbladverkeer ·Grensblad
	Ingang/uitgang	L3Out-EPG	L3Out-EPG	Ingress leaf*
	Ingang/uitgang	EPG	EPG	Consumentenblad
	Ingang/uitgang	EPG	L3Out-EPG	Consumentenblad (niet-grensblad)
Inter-VRF	Ingang/uitgang	L3Out-EPG	EPG	Ingress leaf*
	Ingang/uitgang	L3Out-EPG	L3Out-EPG	Ingress leaf*

*Beleidshandhaving wordt toegepast op het eerste blad dat door het pakket wordt geraakt.

Dit zijn voorbeelden:

- Als een extern eindpunt in L3Out EPG in VRF1 probeert om toegang te krijgen tot een eindpunt in Web EPG in VRF1 en VRF1 is geconfigureerd voor de toegangscontrolemodus, wordt verkeer omgeleid door het blad waar het eindpunt in Web EPG zich bevindt, ongeacht de contractrichting.
- Als een eindpunt in het consumentenweb EPG in VRF1 probeert om toegang te krijgen tot een eindpunt in de provider App EPG in VRF1, en de eindpunten worden geleerd op consumenten- en leveranciersbladknooppunten, wordt verkeer omgeleid door het toegangsblad.
- Als een eindpunt in het consumentenweb EPG in VRF1 probeert toegang te krijgen tot een eindpunt in de provider App EPG in VRF2, wordt het verkeer omgeleid door het consumentenblad waar het eindpunt van de consument zich bevindt, ongeacht de VRF-afdwingingsmodus.

3. Controleer of verkeer wordt omgeleid naar het serviceknooppunt

Zodra het verwachte doorsturen pad duidelijk is, kan ELAM worden gebruikt om te controleren of het verkeer op de switch knooppunten aankomt en de doorsturen beslissing op de switch knooppunten te controleren. Raadpleeg de sectie "Tools" in het hoofdstuk "Intra-Fabric Forwarding" voor instructies over het gebruik van ELAM.

Bijvoorbeeld, om de verkeersstroom in het cijfer "PBR die weg door:sturen voorbeeld - consument aan leverancier"te vinden, kunnen deze worden gevangen om te bevestigen als de consument aan provider verkeer wordt opnieuw gericht.

- Downlink poort op consumentenblad om 1 en 2 te controleren (het verkeer komt aan op het consumentenblad en PBR wordt afgedwongen).
- Fabric-poort op wervelkolomknooppunten om 3 te controleren (Traffic gaat naar

wervelkolomproxy).
- Fabric-poort op servicesblad om 4 te controleren (verkeer komt aan op het servicesblad).

Vervolgens kunnen deze worden opgenomen om te bevestigen dat verkeer dat terugkomt van het serviceknooppunt naar de provider gaat.

- Downlink poort op het servicelabel om 5 en 6 te controleren (verkeer komt terug van het serviceknooppunt en is toegestaan).
- Fabric poort op wervelkolom knooppunten om te controleren 7 (Traffic gaat naar provider blad via spine).
- Fabric poort op provider blad om 8 te controleren (Traffic komt op de service blad en gaat naar de provider endpoint).

Opmerking: Als de klant en de dienst de knoop onder het zelfde blad zijn, specificeer een interface of bron MAC naast bron/bestemming IP om ELAM te nemen om 1 of 5 in cijfer "PBR te controleren die wegvoorbeeld door:sturen - consument aan leverancier"specifiek omdat zowel de zelfde bron IP als bestemming IP gebruiken.

Als de consument naar provider-verkeer wordt omgeleid naar het serviceknooppunt, maar niet terugkeert naar het servicelefblad, controleer dan het volgende omdat het vaak voorkomende fouten zijn:

- De routertabel voor serviceknooppunten bereikt het providersubnetje.
- Beveiligingsbeleid voor serviceknooppunten, zoals ACL, maakt verkeer mogelijk.

Als het verkeer wordt omgeleid en op de provider aankomt, controleer dan op dezelfde manier het retourverkeer van provider naar consument.

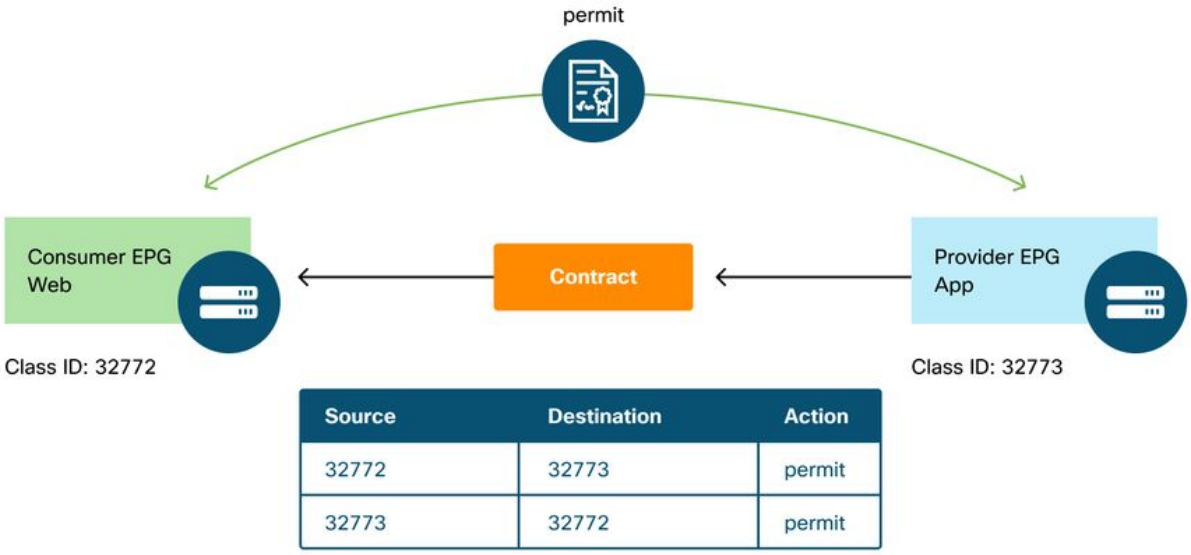
4. Controleer het op de bladknooppunten geprogrammeerde beleid

Als er geen verkeer wordt doorgestuurd of doorgestuurd, is de volgende stap voor probleemoplossing om het beleid te controleren dat op de bladknooppunten is geprogrammeerd. Deze paragraaf laat regels voor zonering en contract_parser als voorbeelden zien. Zie voor meer informatie over het controleren van de regels voor indeling in zones de sectie "Tools" in het hoofdstuk "Beveiligingsbeleid".

Opmerking: Het beleid is geprogrammeerd op basis van de EPG-implementatiestatus op het blad. De output van het showbevel in deze sectie gebruikt het blad dat consument EPG, leverancier EPG, en EPGs voor het de dienstknooppunt heeft.

Gebruik van de opdracht "show zoning-rule"

Het cijfer en de 'toon zoning-regel'-uitvoer hieronder beschrijft de zonering-regels vóór de implementatie van de Service Graph.

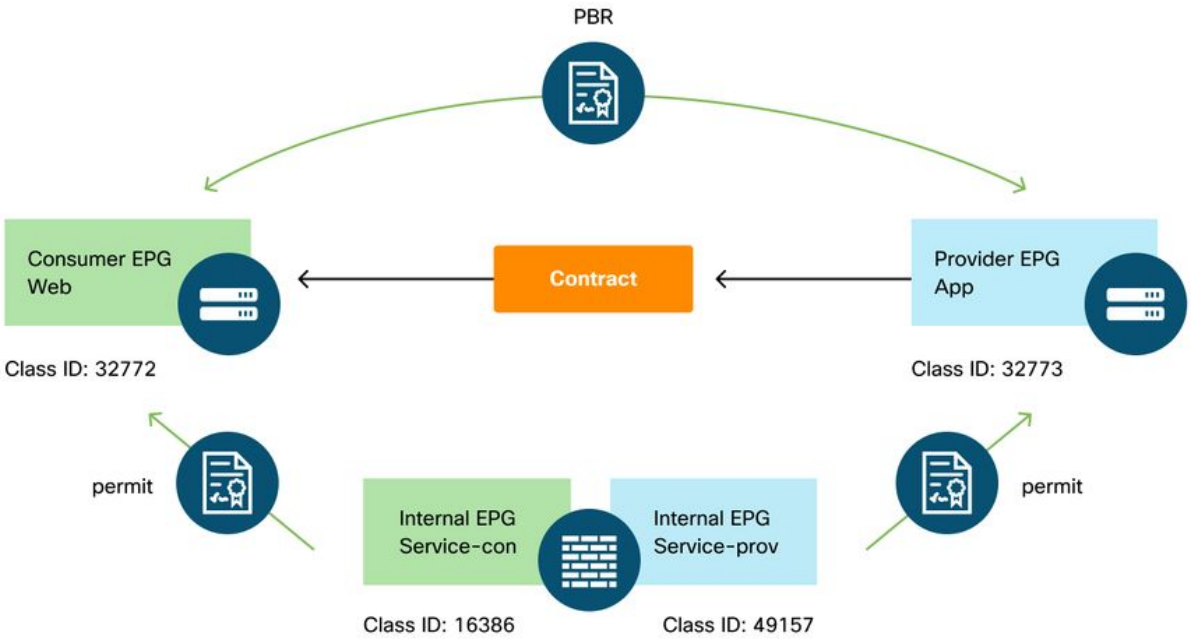


VRF scope id kan worden gevonden in 'Huurder > Netwerken > VRF'.

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

Zodra de Service Graph is geïmplementeerd, worden EPG's voor het serviceknooppunt gemaakt en wordt het beleid bijgewerkt om verkeer tussen de consument en de provider-EPG's om te leiden. In de onderstaande afbeelding en de 'toon zonering-regel'-uitvoer hieronder worden de zoneregels na de implementatie van de servicegrafiek beschreven. In dit voorbeeld wordt het verkeer van pcTag 32772 (Web) naar pcTag 32773 (App) omgeleid naar 'destgrp-27' (consumentenkant van het serviceknooppunt) en het verkeer van pcTag 32773 (App) naar pcTag 32772 (Web) wordt omgeleid naar 'destgrp-28' (leverancierskant van het serviceknooppunt).

Zones-regels na implementatie van 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)     |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

De doelinformatie van elke destgrp kan worden gevonden met behulp van de 'show service redir info' opdracht.

```
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
...
```

Als de zoneringsregels dienovereenkomstig worden geprogrammeerd, maar het verkeer niet dienovereenkomstig wordt omgeleid of doorgestuurd, controleer dan het volgende, aangezien het vaak voorkomende fouten zijn:

- Controleer of de bron- of doelklasse-ID is opgelost zoals verwacht met ELAM. Als dit niet het geval is, controleer dan wat de verkeerde klasse-ID is en de EPG-afleidingscriteria zoals path en encap VLAN.
- Zelfs als de bron en bestemmingsklasse IDs dienovereenkomstig worden opgelost, en het beleid PBR wordt toegepast maar het verkeer komt niet op de PBR knoop aan, te controleren gelieve IP, MAC, en VRF van het destgrp in de herhalingsactie ("toon de dienst herhalingsinfo") correct zijn.

Standaard zijn de vergunningsregels voor een consument-EPG naar een serviceknooppunt (consumentenzijde) en een provider-EPG naar een serviceknooppunt (leverancierskant) niet geprogrammeerd als PBR is ingeschakeld. Aldus, kan een eindpunt van de consument of van de leverancier niet direct aan het de dienstknooppunt door gebrek communiceren. Om dit verkeer toe te laten, moet de optie Direct Connect zijn ingeschakeld. Het gebruik wordt uitgelegd in de sectie "Andere voorbeelden van verkeersstromen**"**.

Gebruik van contract_parser

Het contract_parser hulpmiddel kan ook helpen om het beleid te verifiëren. C-consumer is de consumentenkant van het serviceknooppunt en C-provider is de leverancierskant van het serviceknooppunt.

```
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]
...
```

Andere voorbeelden van verkeersstromen

In deze sectie worden andere veelvoorkomende voorbeelden van verkeersstromen overwogen om de gewenste stromen voor probleemoplossing te identificeren. Raadpleeg het vorige hoofdstuk in deze sectie voor stappen voor probleemoplossing.

1. Taakverdeling zonder SNAT: In dit voorbeeld hebben EPG Web en provider EPG App een contract met een load balancer Service Graph. Endpoints in App EPG zijn echte servers die gekoppeld zijn aan de VIP op de load balancer.PBR to load balancer is ingeschakeld voor providers die de richting van consumentenverkeer bepalen.
2. Firewall en load balancer zonder SNAT: In dit voorbeeld hebben EPG Web en provider EPG App een contract met een firewall en een load balancer Service Graph. Endpoints in App EPG zijn echte servers die gekoppeld zijn aan de VIP on load balancer.PBR naar firewall is voor beide richtingen ingeschakeld.PBR to load balancer is ingeschakeld voor providers die de richting van consumentenverkeer bepalen.
3. Gedeelde service (Inter-VRF-contract): In dit voorbeeld hebben EPG Web en provider EPG App een contract met een firewall Service Graph. EPG Web en EPG App zijn in verschillende VRFs.PBR naar firewall is voor beide richtingen ingeschakeld.De firewall zit tussen VRF's in.

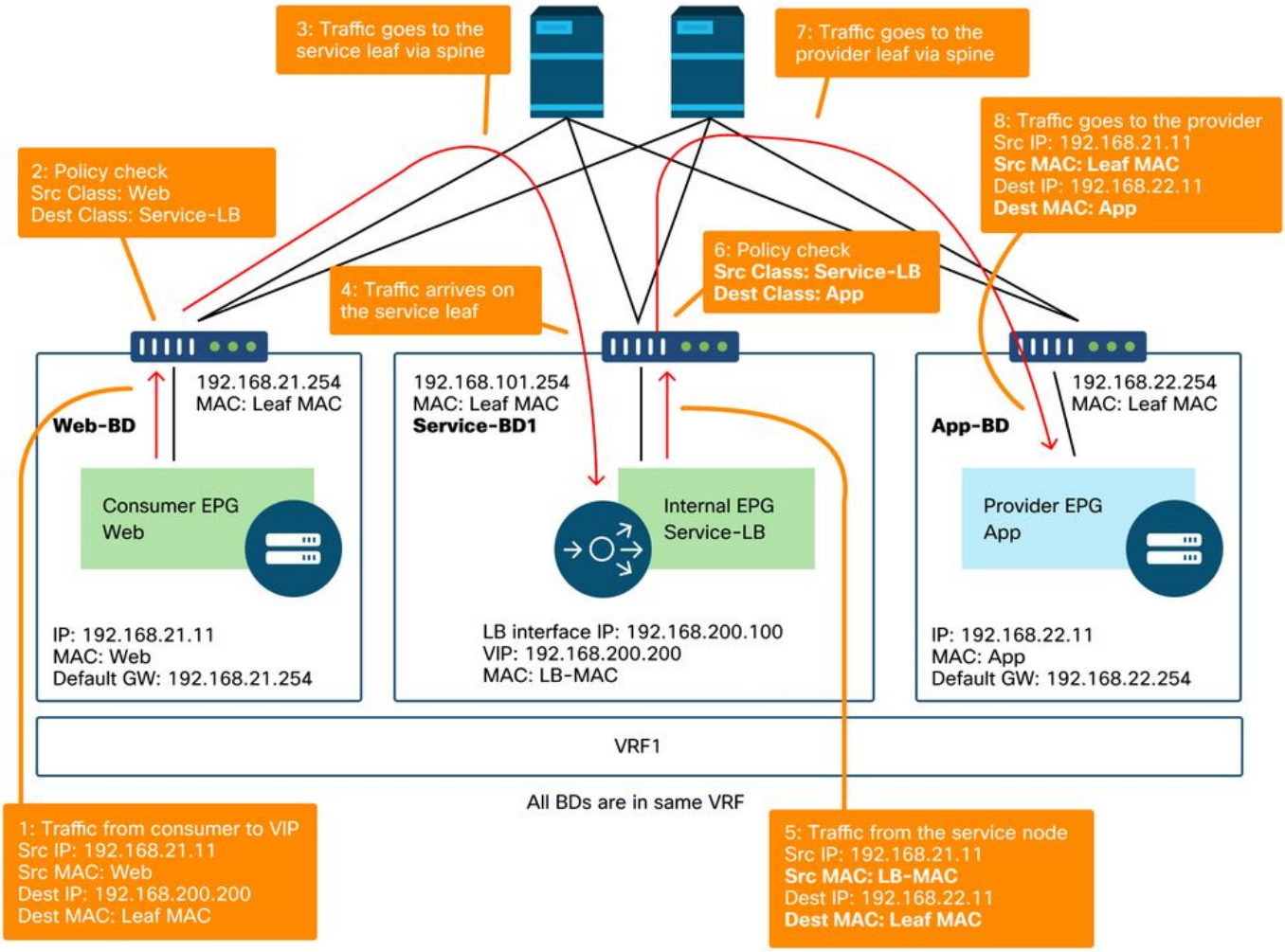
1. Taakverdeling zonder SNAT

PBR kan worden ingezet als bidirectionele PBR of unidirectionele PBR. Eén gebruikscase voor unidirectionele PBR is de integratie van taakverdeling zonder bron-netwerkadresomzetting (NAT). Als de ladingsverdeler bron-NAT uitvoert, is PBR niet vereist.

Voorbeeld van verkeerspad

De onderstaande afbeelding illustreert een voorbeeld van een inkomende verkeersstroom van het EPG Web van de consument naar de provider EPG App met twee verbindingen: De ene is van een eindpunt in het consumenten-EPG Web naar de load balancer VIP, en de andere is van de load balancer naar een eindpunt in de provider EPG App. Omdat het inkomende verkeer bestemd is voor de VIP, zal het verkeer de load balancer zonder PBR bereiken als de VIP bereikbaar is. De load balancer verandert de bestemming IP in een van de eindpunten in EPG App gekoppeld aan de VIP maar vertaalt de bron IP niet. Dienovereenkomstig gaat het verkeer naar het leverancierseindpunt.

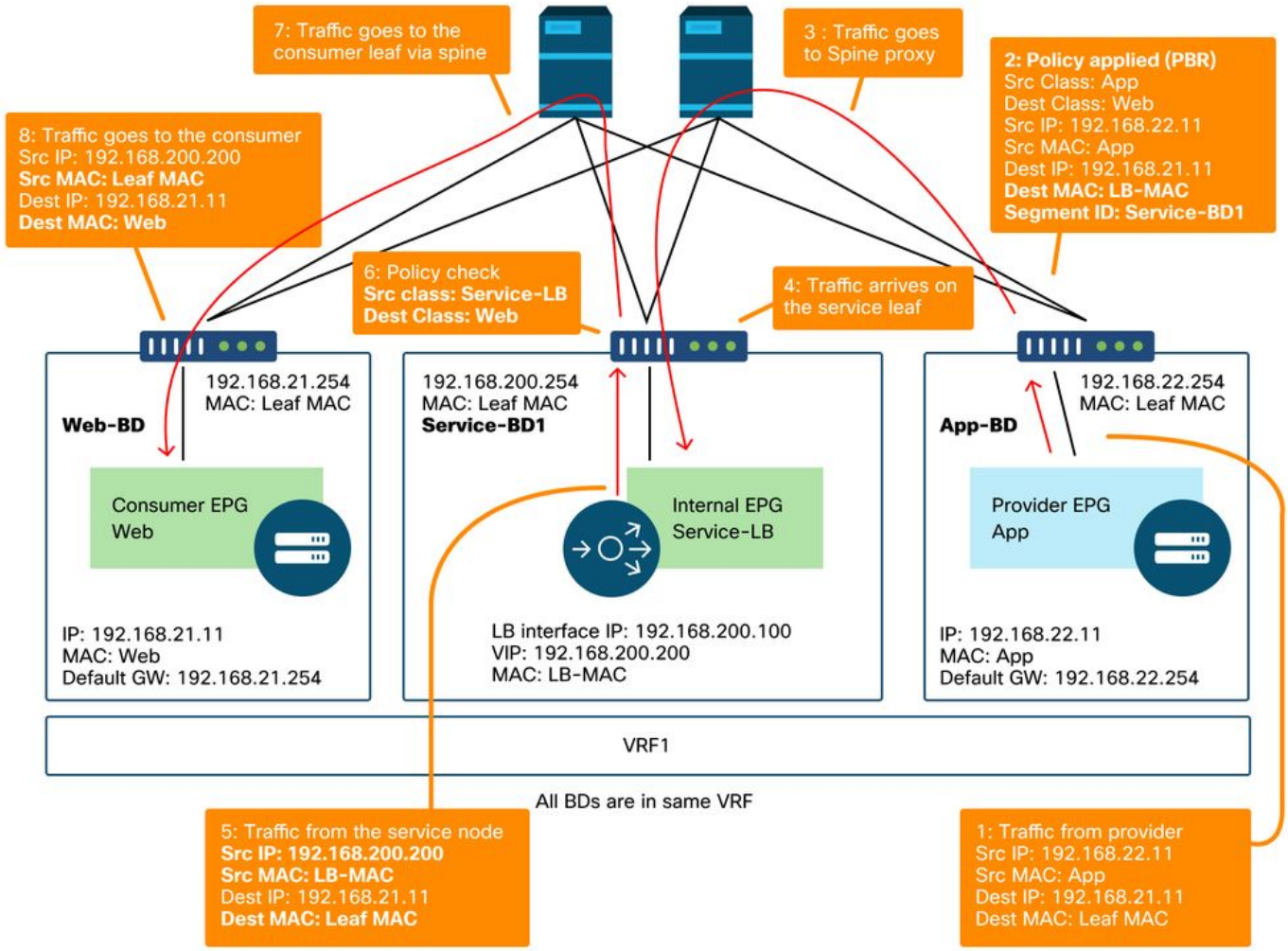
Laadverdeler zonder SNAT-routevoorbeeld — consument naar VIP en ladingsverdeler naar provider zonder PBR



De onderstaande figuur illustreert de terugkeerverkeersstroom van provider EPG App naar consument EPG Web. Omdat het terugkeerverkeer bestemd is voor de oorspronkelijke IP-bron, moet PBR het terugkeerverkeer maken om terug te gaan naar de taakverdeling. Anders ontvangt het eindpunt van de consument het verkeer waar de bron IP het leverancierseindpunt in plaats van VIP is. Zulk verkeer zal worden gelaten vallen omdat het eindpunt van de consument geen verkeer aan het leverancierseindpunt in werking stelde zelfs als het middennetwerk zoals de stof ACI het pakket terug naar het eindpunt van de consument door:sturen.

Nadat het verkeer van het leverancierseindpunt naar het consumentendpoint is omgeleid naar de taakverdeler, verandert de taakverdeler de bron IP in de VIP. Dan, komt het verkeer terug van de ladingsstabilisator en het verkeer gaat terug naar het eindpunt van de consument.

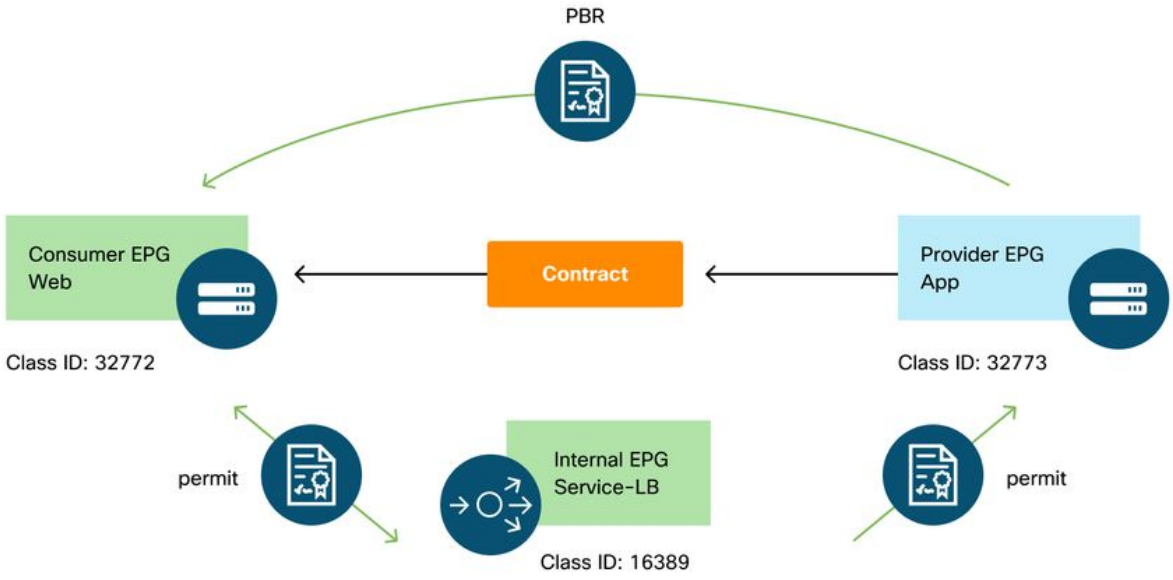
Laadverdeler zonder SNAT-voorbeeld voor doorsturen van pad - leverancier aan consument met PBR



Het geprogrammeerde beleid op de bladknooppunten.

In de onderstaande figuur en de 'toon zoning-regel'-uitvoer hieronder worden de zoneregels na de implementatie van de servicegrafiek beschreven. In dit voorbeeld is het verkeer van pcTag 32772 (Web) naar pcTag 16389 (Service-LB) toegestaan, is het verkeer van pcTag 16389 (Service-LB) naar pcTag 32773 (App) toegestaan en wordt het verkeer van pcTag 32773 (App) naar pcTag 32772 (Web) omgeleid naar 'destgrp-31' (load balancer).

Zones-regels na implementatie van Service Graph - taakverdeling zonder SNAT

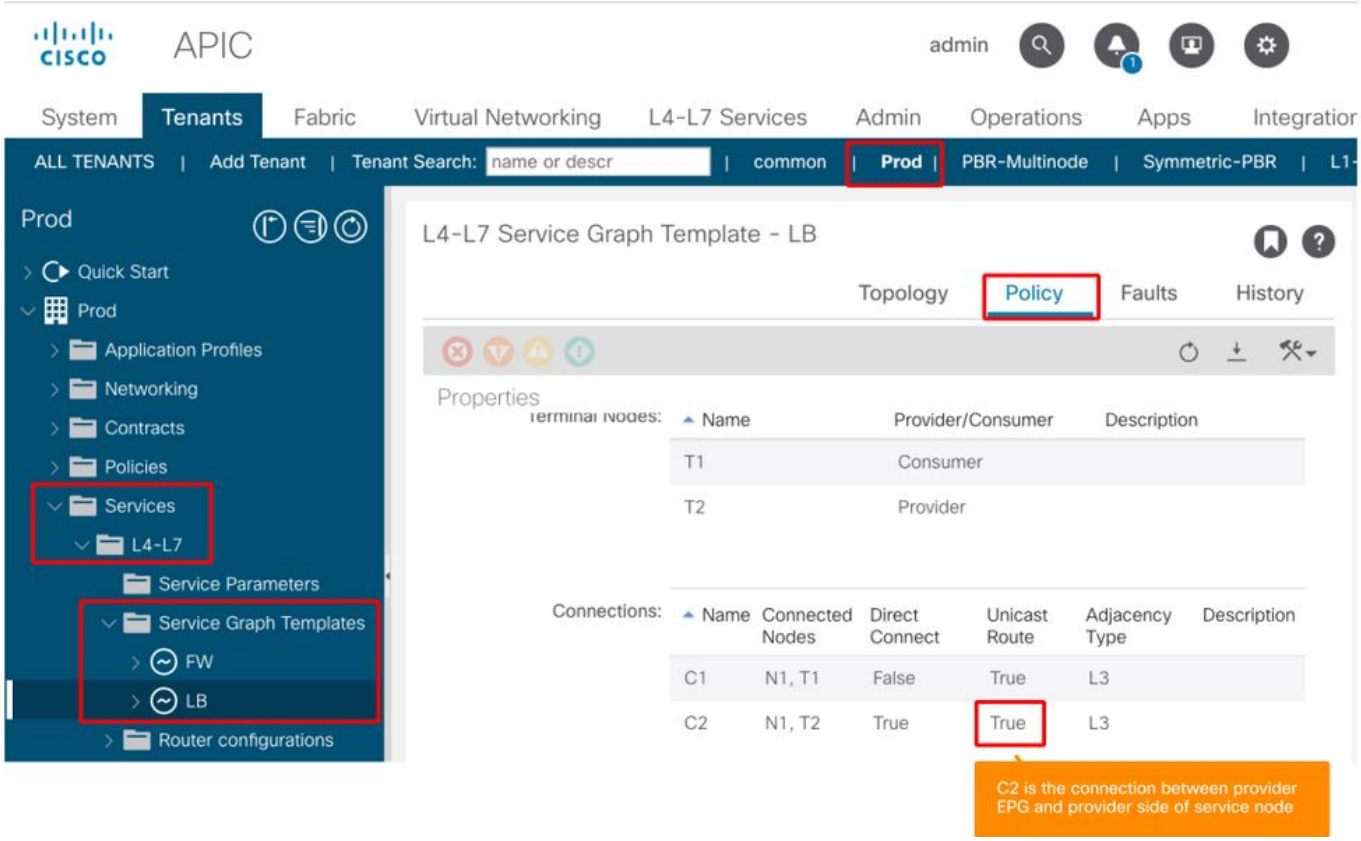


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
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)     |
...
```

Standaard is er geen regel voor de vergunning van de provider EPG (pcTag 32773) naar Service-LB (pcTag 16389). Om bi-directionele communicatie tussen hen toe te staan voor gezondheidscontroles van de lastverdeler aan leverancierseindpunten, moet de Direct Connect optie op de verbinding aan Waar worden geplaatst. De locatie is 'huurder > L4-L7 > Service Graph Templates > Policy'. De standaardwaarde is Vals.

Direct Connect-optie instellen



Het voegt een vergunningsregel voor leverancier EPG(32773) aan Service-LB(16389) toe zoals hieronder.

```
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. Traffic flow-voorbeeld - firewall en taakverdeling zonder SNAT

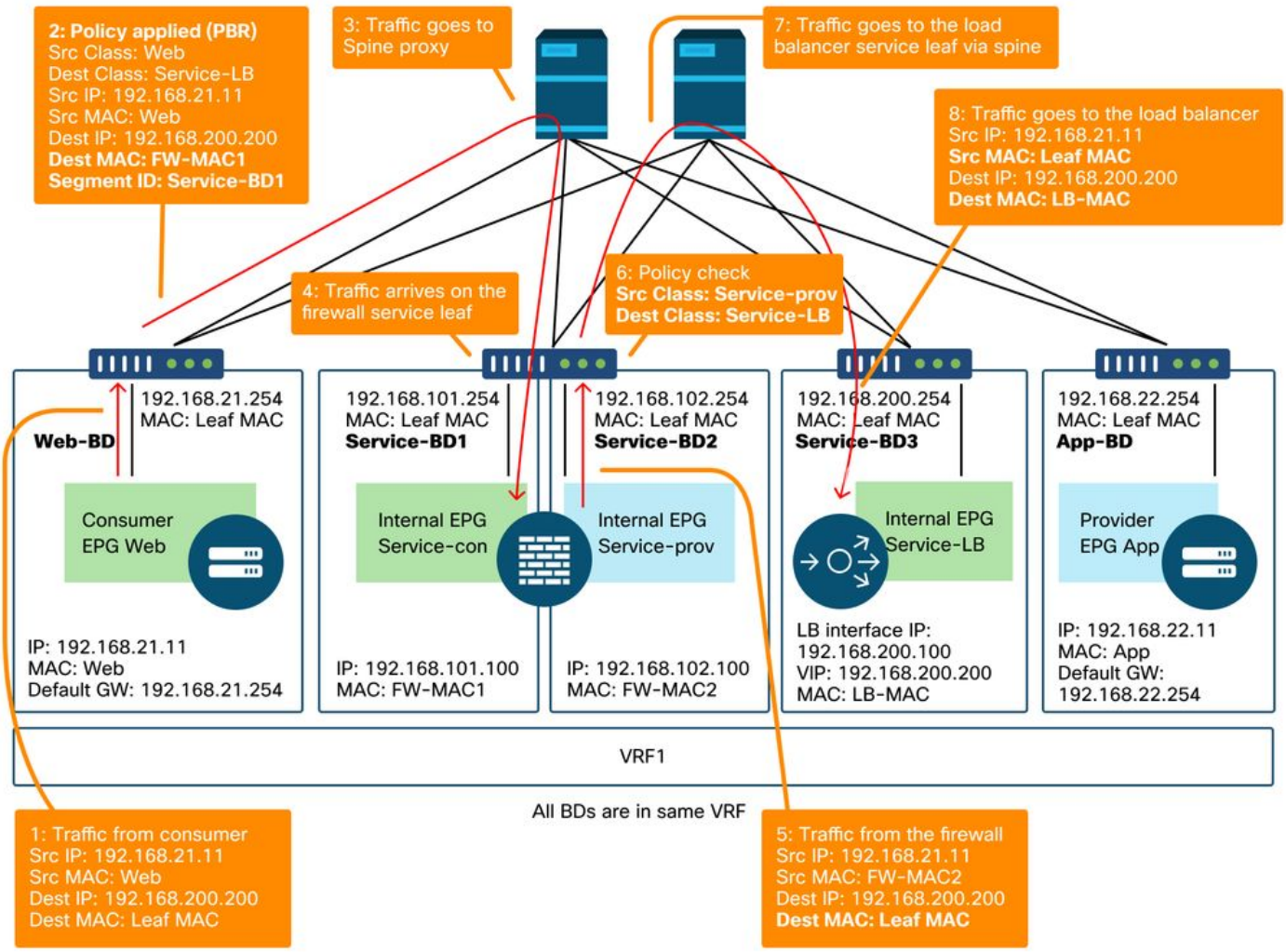
PBR kan worden geïmplementeerd met meerdere servicefuncties in een servicegrafiek zoals firewall als eerste knooppunt en taakverdeling als tweede knooppunt.

Voorbeeld van verkeerspad

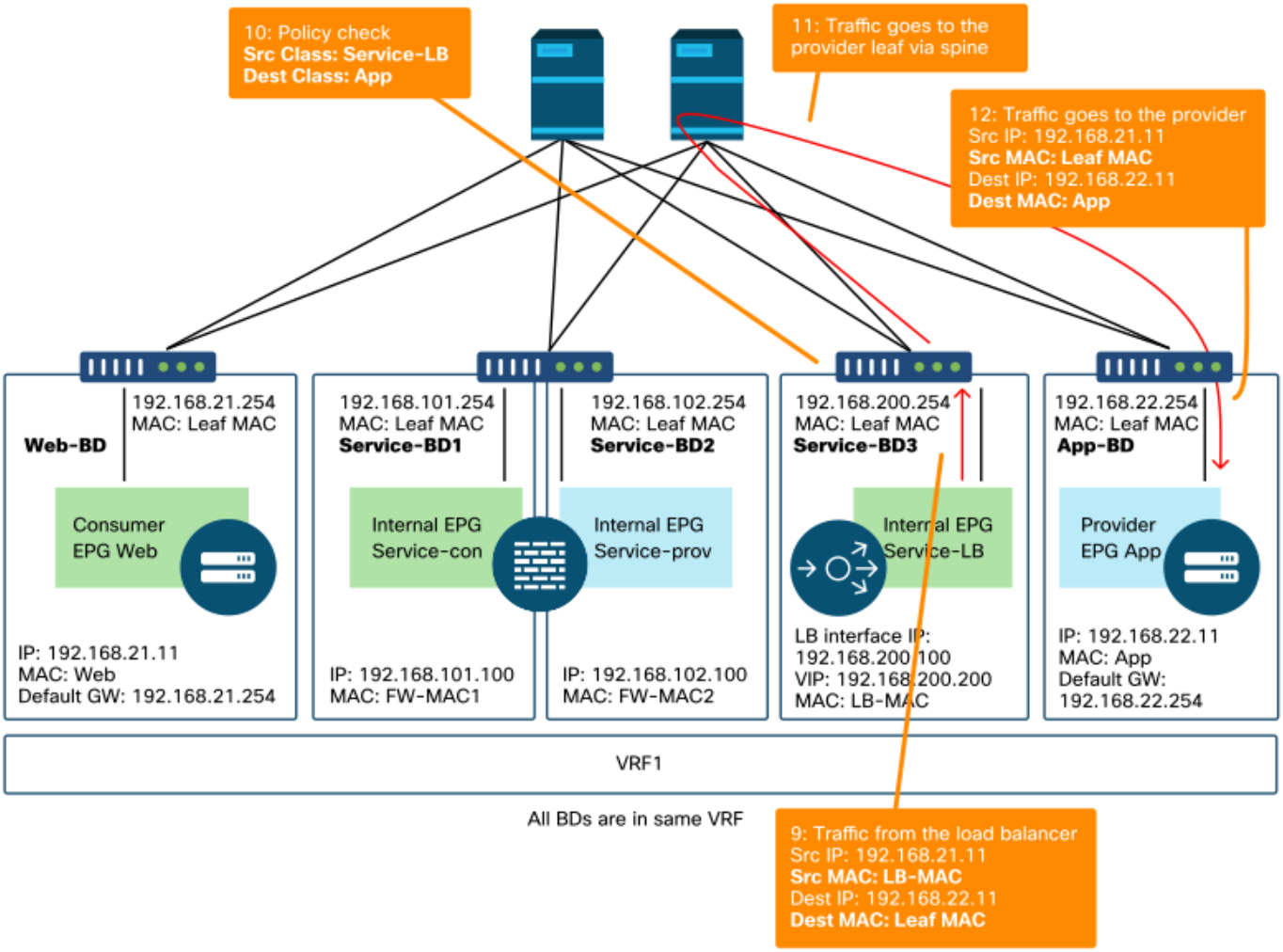
De onderstaande afbeelding illustreert een voorbeeld van een inkomende verkeersstroom van het EPG Web van de consument naar de provider EPG App met twee verbindingen: De ene is van

een eindpunt in het consumenten-EPG-web naar de load balancer VIP via firewall en de andere is van de load balancer naar een eindpunt in de provider EPG App. Het inkomende verkeer dat voor de VIP bestemd is, wordt omgeleid naar de firewall en gaat dan naar de load balancer zonder PBR. De load balancer verandert de bestemming IP in een van de eindpunten in App EPG gekoppeld aan de VIP maar vertaalt de bron IP niet. Vervolgens gaat het verkeer naar het provider-endpoint.

Firewall en load balancer zonder SNAT doorsturen pad voorbeeld - consument naar VIP en load balancer naar provider



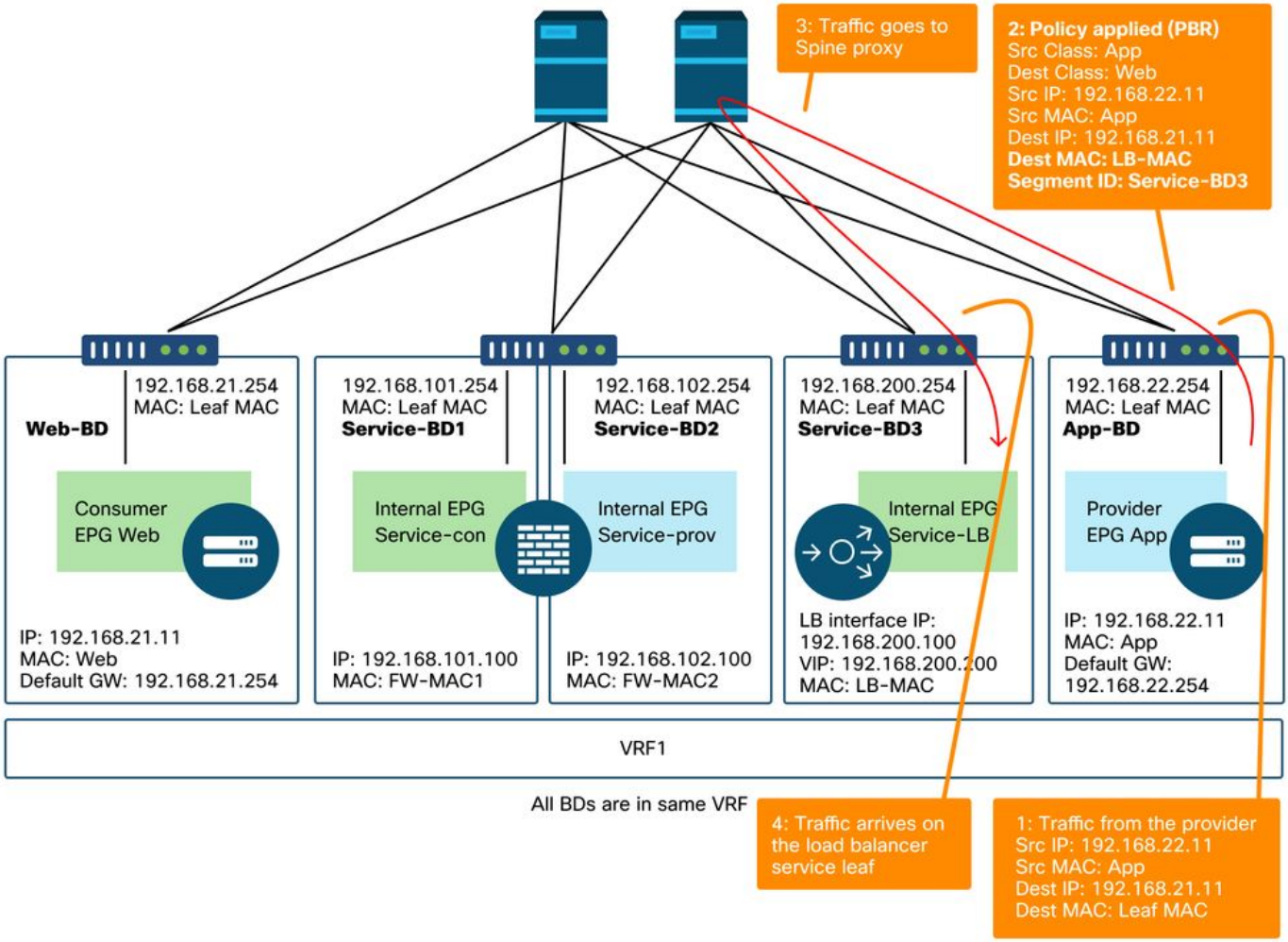
Firewall en load balancer zonder SNAT doorsturen pad voorbeeld - consument naar VIP en load balancer naar provider (vervolg)

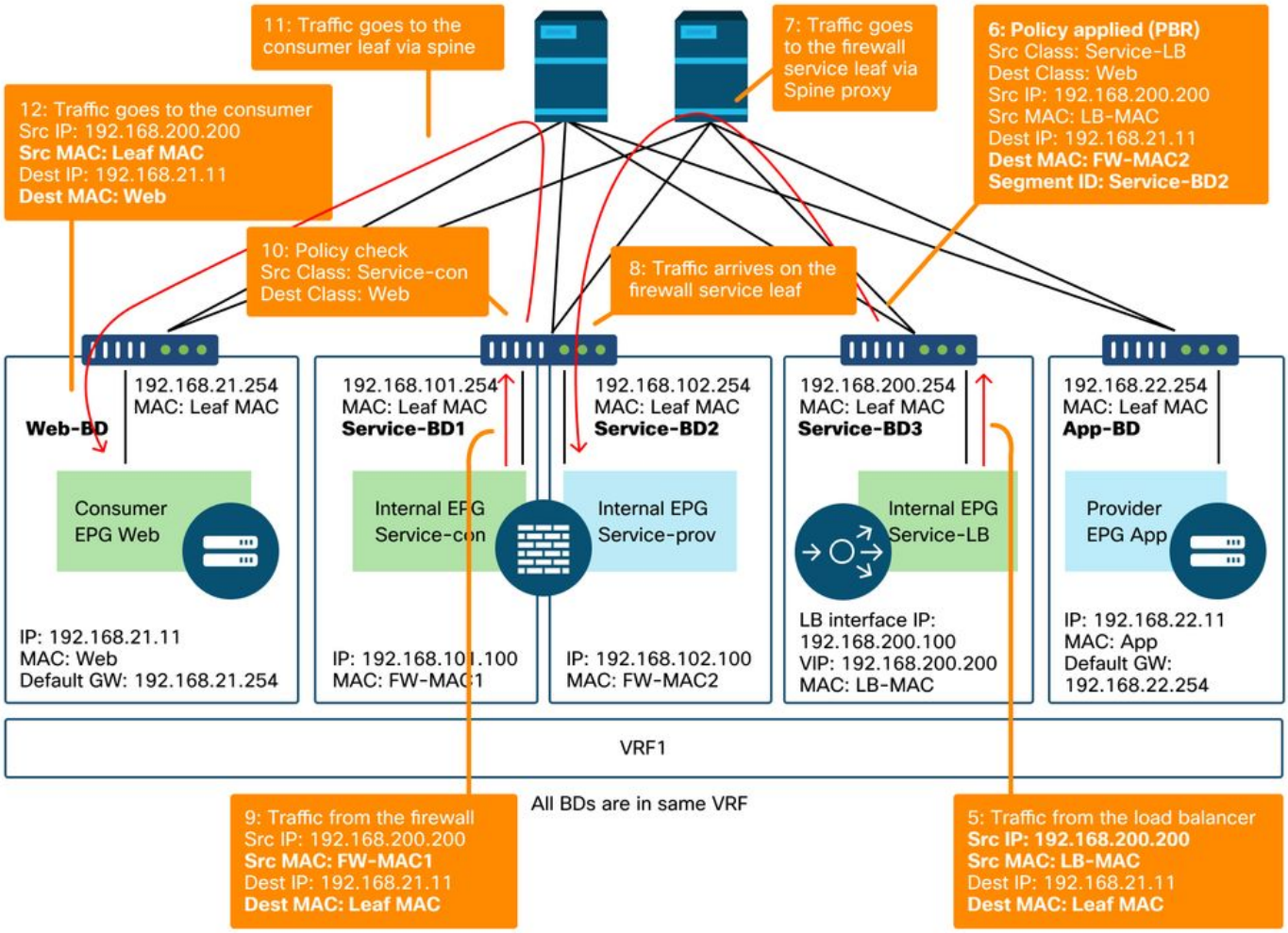


De onderstaande figuur illustreert de terugkeerverkeersstroom van provider EPG App naar consument EPG Web. Omdat het terugkeerverkeer bestemd is voor oorspronkelijke IP-bron, moet PBR het terugkeerverkeer terugsturen naar de taakverdeling.

Nadat het verkeer van het leveranciereindpunt naar het consumentendpoint is omgeleid naar de taakverdeler, verandert de taakverdeler de bron IP in de VIP. Het verkeer wordt via de taakverdeling teruggestuurd naar de firewall. Dan, komt het verkeer terug van de firewall en gaat terug naar het eindpunt van de consument.

Firewall en load balancer zonder SNAT-voorbeeld voor doorsturen van pad - provider naar consument

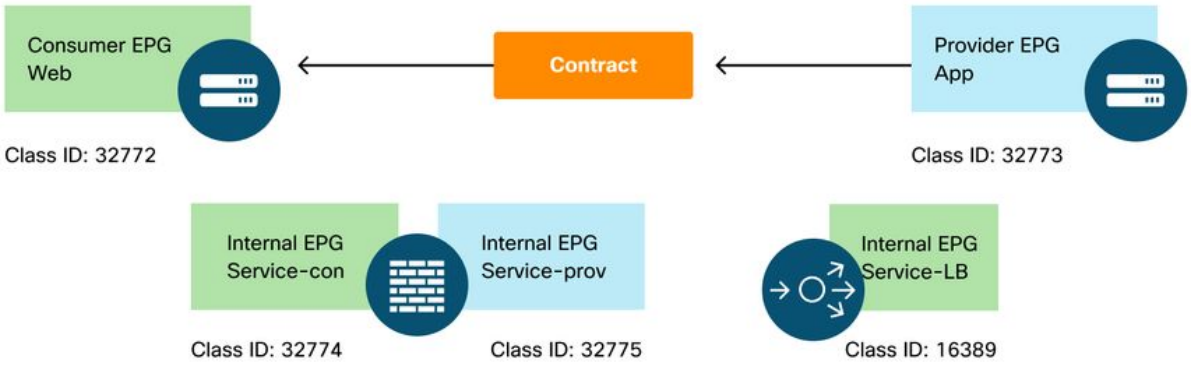

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



Het geprogrammeerde beleid op de bladknooppunten

De onderstaande figuur en de 'show zoning-rule'-output beschrijven de zoning-regels na de implementatie van de Service Graph. In dit voorbeeld wordt het verkeer van pcTag 32772 (Web) naar pcTag 16389 (Service-LB) omgeleid naar 'destgrp-32' (consumentenkant van de firewall), het verkeer van pcTag 32773 (App) naar pcTag 32772 (Web) wordt omgeleid naar 'destgrp-33' (load balancer), en het verkeer van pcTag 16389 (Service-LB) naar pcTag 32772 (Web) wordt omgeleid naar 'destgrp-34' (provider kant van de firewall).

Zones-regels na implementatie van Service Graph - firewall en taakverdeling zonder 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)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

In het bovenstaande voorbeeld is de optie Direct Connect ingesteld op 'True' op de verbinding tussen de aanbodzijde van de taakverdeling en de provider EPG. Het moet ingeschakeld zijn voor een gezondheidscontrole van de taakverdeling naar de providerendpoints. De locatie is 'huurder > L4-L7 > Service Graph Templates >Policy'. Raadpleeg de afbeelding 'Direct Connect optie

instellen'.

3. Gedeelde service (Inter-VRF-contract)

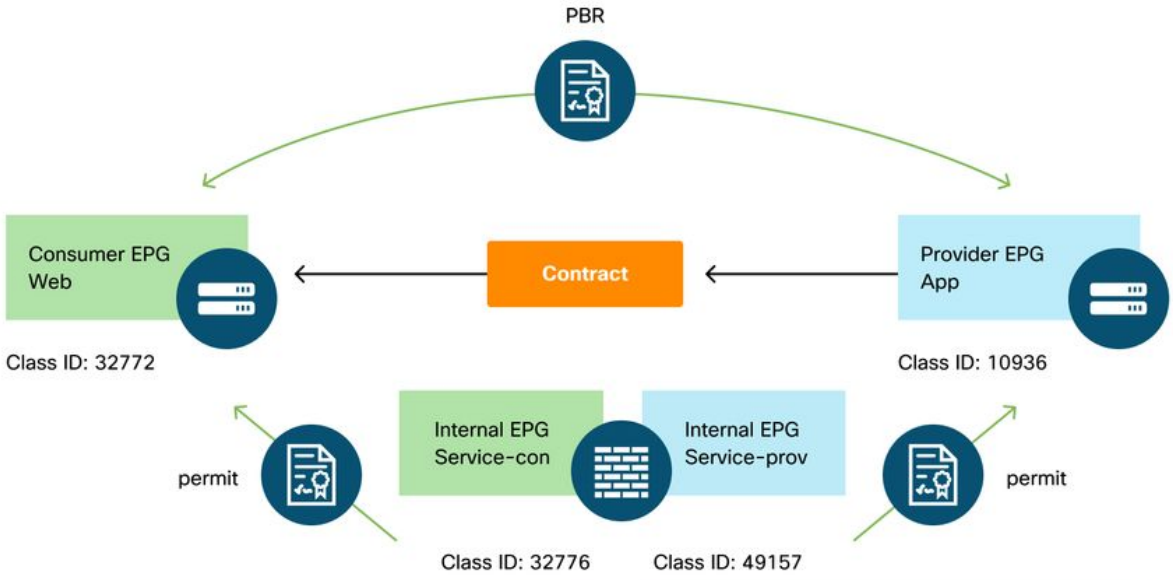
PBR kan in inter-VRF-contract worden ingeschakeld. In dit deel wordt uitgelegd hoe de zoningregels worden geprogrammeerd in het geval van EPG tot EPG inter-VRF-contract.

Het geprogrammeerde beleid op de bladknooppunten

In het geval van EPG tot EPG inter-VRF contract, wordt het beleid altijd afgedwongen in consument VRF. Op deze manier vindt omleiding plaats op de VRF voor consumenten. Raadpleeg voor andere combinaties de tabel "Waar wordt het beleid gehandhaafd?" in de rubriek "Doorsturen".

In de onderstaande afbeelding en de 'toon zonering-regel'-uitvoer hieronder worden de zoneregels na de implementatie van de servicegrafiek beschreven. In dit voorbeeld wordt het verkeer van pcTag 32772 (Web) naar pcTag 10936 (App) omgeleid naar 'destgrp-36' (consumentenkant van het serviceknooppunt) en het verkeer van pcTag 10936 (App) naar pcTag 32772 (Web) wordt omgeleid naar 'destgrp-35' (leverancierskant van het serviceknooppunt). Beiden worden afgedwongen in VRF1 die consument VRF is. Het verkeer van pcTag 32776 (consumentenzijde van de firewall) naar pcTag 32772 (Web) is toegestaan in VRF1.

Zones-regels na implementatie van Service Graph - inter-VRF-contract



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

Het verkeer van pcTag 49157 (provider side van de firewall) naar pcTag 10936 (App) is toegestaan in VRF2 omdat beide in VRF2 zijn.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.