Dépannage de la redirection basée sur les politiques ACI

Table des matières

Introduction

Ce document décrit les étapes à suivre pour comprendre et dépanner un scénario de redirection basée sur les politiques (PBR) de l'ACI.

Informations générales

Le contenu de ce document a été extrait du livre Troubleshooting Cisco Application Centric Infrastructure, Second Edition (Dépannage de l'infrastructure axée sur les applications Cisco, deuxième édition), en particulier le livre Policy-Based Redirect - Overview, Policy-Based Redirect - Service Graph Deployment, Policy-Based Redirect - Forwarding et Policy-Based Redirect - Other traffic flow example chapitres.

Présentation de la redirection basée sur des stratégies

Ce chapitre explique le dépannage du graphique de services en mode non géré avec redirection basée sur des stratégies (PBR).

Les étapes de dépannage suivantes sont typiques. Ce chapitre explique comment vérifier les étapes 2 et 3 qui sont spécifiques à PBR. Pour les étapes 1 et 4, reportez-vous aux chapitres « Transfert intra-fabric », « Transfert externe » et « Stratégies de sécurité ».

1. Vérifier les travaux de trafic sans le graphique de service PBR :
    - Les terminaux du consommateur et du fournisseur sont appris.
    - Les terminaux des consommateurs et des fournisseurs peuvent communiquer.
2. Vérifier que le graphique de service est déployé :
    - Les instances de graphique déployées sont sans défaut.
    - Les VLAN et les ID de classe du noeud de service sont déployés.
    - Les points de terminaison des noeuds de service sont acquis.
3. Vérifiez le chemin de transfert :
    - La stratégie de vérification est programmée sur les noeuds leaf.
    - Capturez le trafic sur le noeud de service pour confirmer si le trafic est redirigé.
    - Capturez le trafic sur le leaf ACI pour confirmer si le trafic revient au fabric ACI après PBR.
4. Vérifiez que le trafic arrive sur le point de terminaison consommateur et fournisseur et que le point de terminaison génère le trafic de retour.

Ce document ne couvre pas les options de conception ou de configuration. Pour plus d'informations, reportez-vous au livre blanc « ACI PBR » disponible à l'adresse Cisco.com

Dans ce chapitre, le noeud de service et le noeud leaf de service impliquent les éléments suivants :

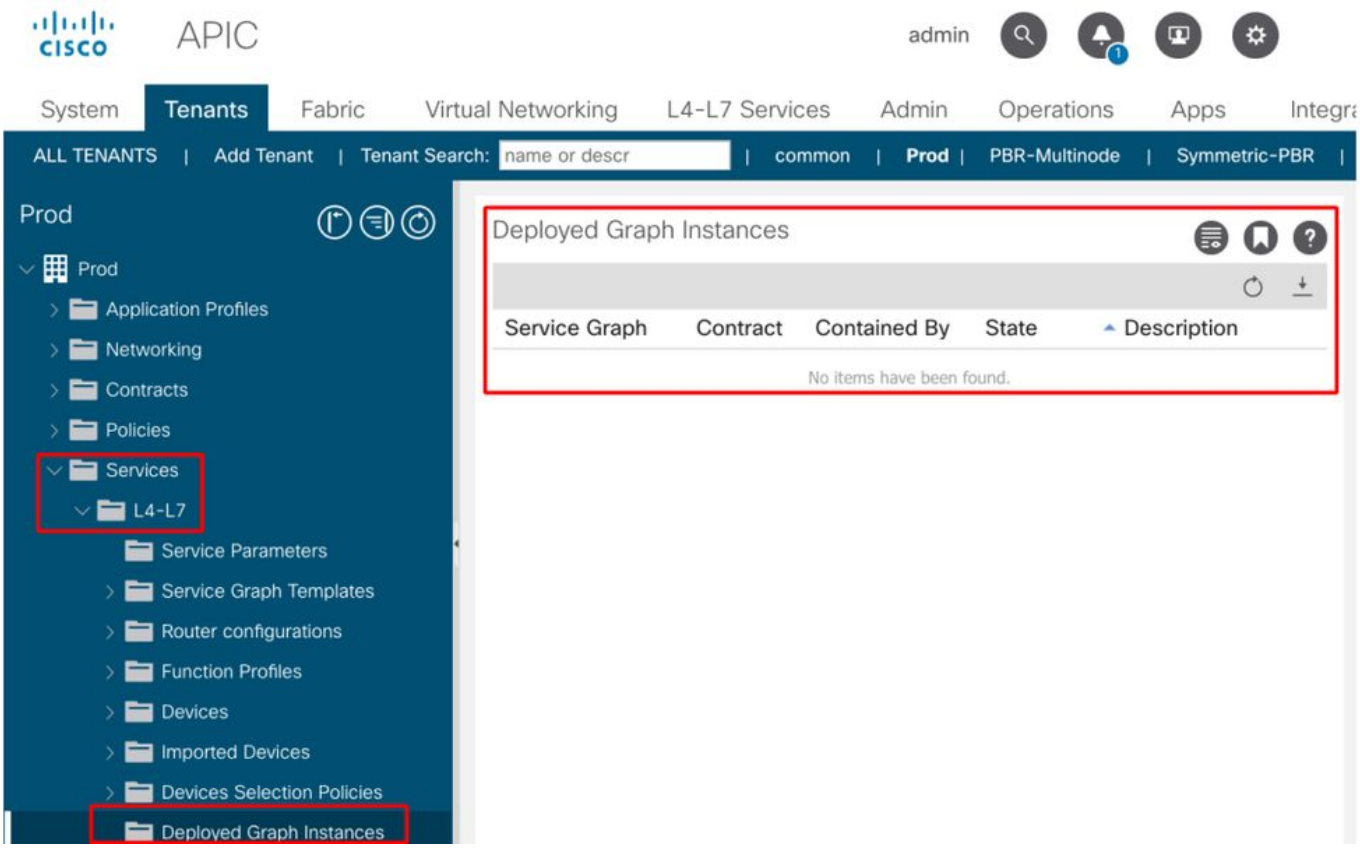
- Noeud de service : noeud externe vers lequel PBR redirige le trafic, tel qu'un pare-feu ou un équilibreur de charge.
- Leaf de service - Leaf ACI connecté à un noeud de service.

Dépannage du déploiement du graphique des services

Ce chapitre décrit un exemple de dépannage dans lequel un graphique de services n'est pas déployé.

Une fois qu'une stratégie Service Graph est définie et appliquée à un objet de contrat, une instance de graphique déployée doit apparaître sur l'interface graphique utilisateur de l'ACI. La figure ci-dessous illustre le scénario de dépannage dans lequel le graphique des services n'apparaît pas comme déployé.

Le graphique de services n'est pas affiché en tant qu'instance de graphique déployée.



1. Vérifier les étapes de configuration et les erreurs

La première étape du dépannage consiste à vérifier que les composants nécessaires ont été configurés sans aucune défaillance. On suppose que les configurations générales ci-dessous sont déjà effectuées :

- VRF et BD pour EPG grand public, EPG fournisseur et noeud de service
- L'EPG consommateur et fournisseur.
- Le contrat et les filtres.

Il est utile de mentionner qu'il n'est pas nécessaire de créer manuellement un EPG pour le noeud de service. Elle sera créée via le déploiement de Service Graph.

Les étapes de configuration de Service Graph avec PBR sont les suivantes :

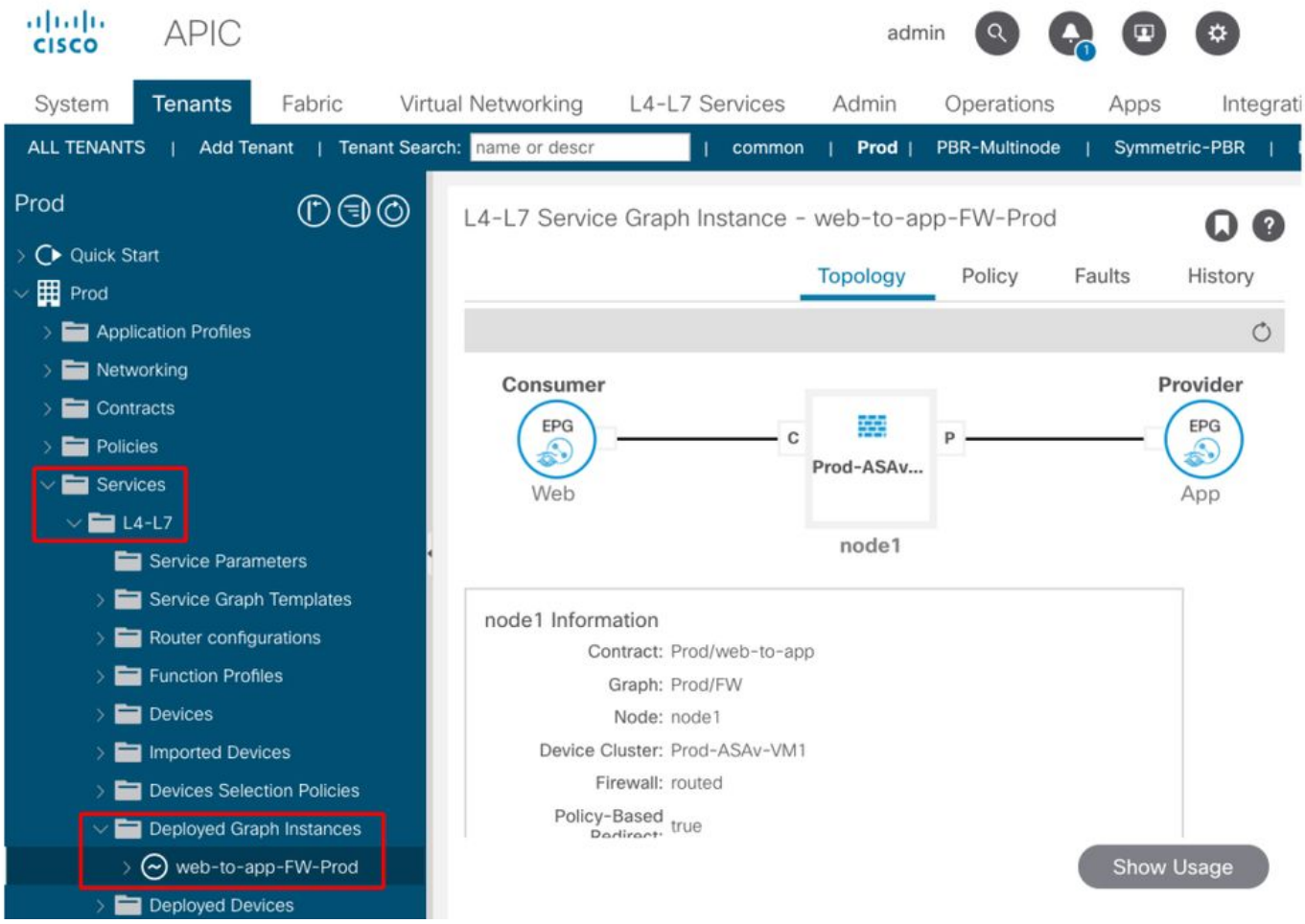
- Créez le périphérique L4-L7 (périphérique logique).
- Créez le graphique des services.
- Créez la stratégie PBR.
- Créez la stratégie Sélection de périphérique.
- Associez le graphique des services à l'objet du contrat.

2. Vérifiez le déploiement de Service Graph dans l'interface utilisateur

Une fois qu'un graphique de services est associé à l'objet du contrat, une instance de graphique déployée doit apparaître pour chaque contrat avec le graphique de services (figure ci-dessous).

L'emplacement est 'Locataire > Services > L4-L7 > Instances de graphique déployées'

Instance de graphique déployée



Si une instance de graphique déployée ne s'affiche pas, la configuration du contrat présente un problème. Les principales raisons peuvent être les suivantes :

- Le contrat n'a pas d'EPG client ou fournisseur.
- L'objet du contrat n'a aucun filtre.
- La portée du contrat est VRF, même si elle est destinée à la communication entre VRF ou EPG entre locataires.

En cas d'échec de l'instanciation de Service Graph, des erreurs sont générées dans l'instance de graphique déployée, ce qui signifie qu'il y a un problème avec la configuration de Service Graph. Les erreurs typiques causées par la configuration sont les suivantes :

F1690 : configuration non valide en raison d'un échec d'allocation d'ID

Cette erreur indique que le VLAN encapsulé pour le noeud de service n'est pas disponible. Par exemple, il n'y a pas de VLAN dynamique disponible dans le pool de VLAN associé au domaine VMM utilisé dans le périphérique logique.

Résolution : vérifiez le pool de VLAN dans le domaine utilisé pour le périphérique logique. Vérifiez le VLAN encapsulé dans l'interface du périphérique logique s'il se trouve dans un domaine

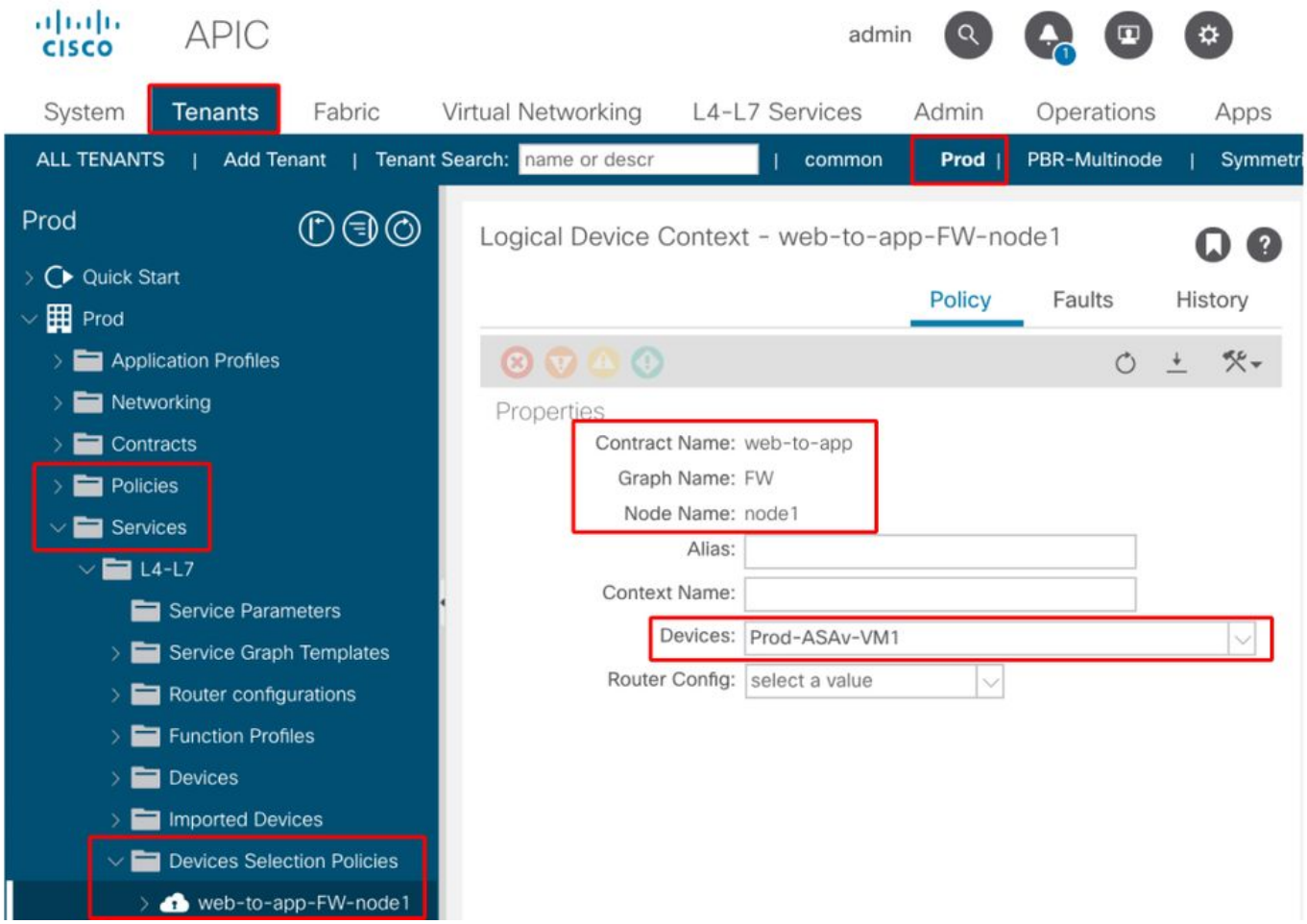
physique. Les emplacements sont 'Locataire > Services > L4-L7 > Périphériques et fabric > Politiques d'accès > Pools > VLAN'.

F1690 : la configuration n'est pas valide en raison de l'absence de contexte de périphérique pour LDev

Cette erreur indique que le périphérique logique est introuvable pour le rendu Service Graph. Par exemple, il n'existe aucune stratégie de sélection de périphérique correspondant au contrat avec le graphique des services.

Résolution : vérifiez que la stratégie de sélection de périphérique est définie. La politique de sélection de périphérique fournit un critère de sélection pour un périphérique de service et ses connecteurs. Les critères sont basés sur un nom de contrat, un nom de graphique de services et un nom de noeud dans le graphique de services. L'emplacement est 'Locataire > Services > L4-L7 > Politique de sélection de périphérique'.

Vérifier la stratégie de sélection des périphériques



F1690 : la configuration n'est pas valide car aucune interface de cluster n'a été trouvée

Cette erreur indique que l'interface de cluster du noeud de service est introuvable. Par exemple, l'interface de cluster n'est pas spécifiée dans la stratégie de sélection de périphérique.

Résolution : vérifiez que l'interface de cluster est spécifiée dans la stratégie de sélection de

périphérique et que le nom du connecteur est correct (Figure ci-dessous).

F1690 : la configuration n'est pas valide car aucun BD n'a été trouvé

Cette erreur indique que le BD du noeud de service est introuvable. Par exemple, le BD n'est pas spécifié dans la stratégie de sélection de périphérique.

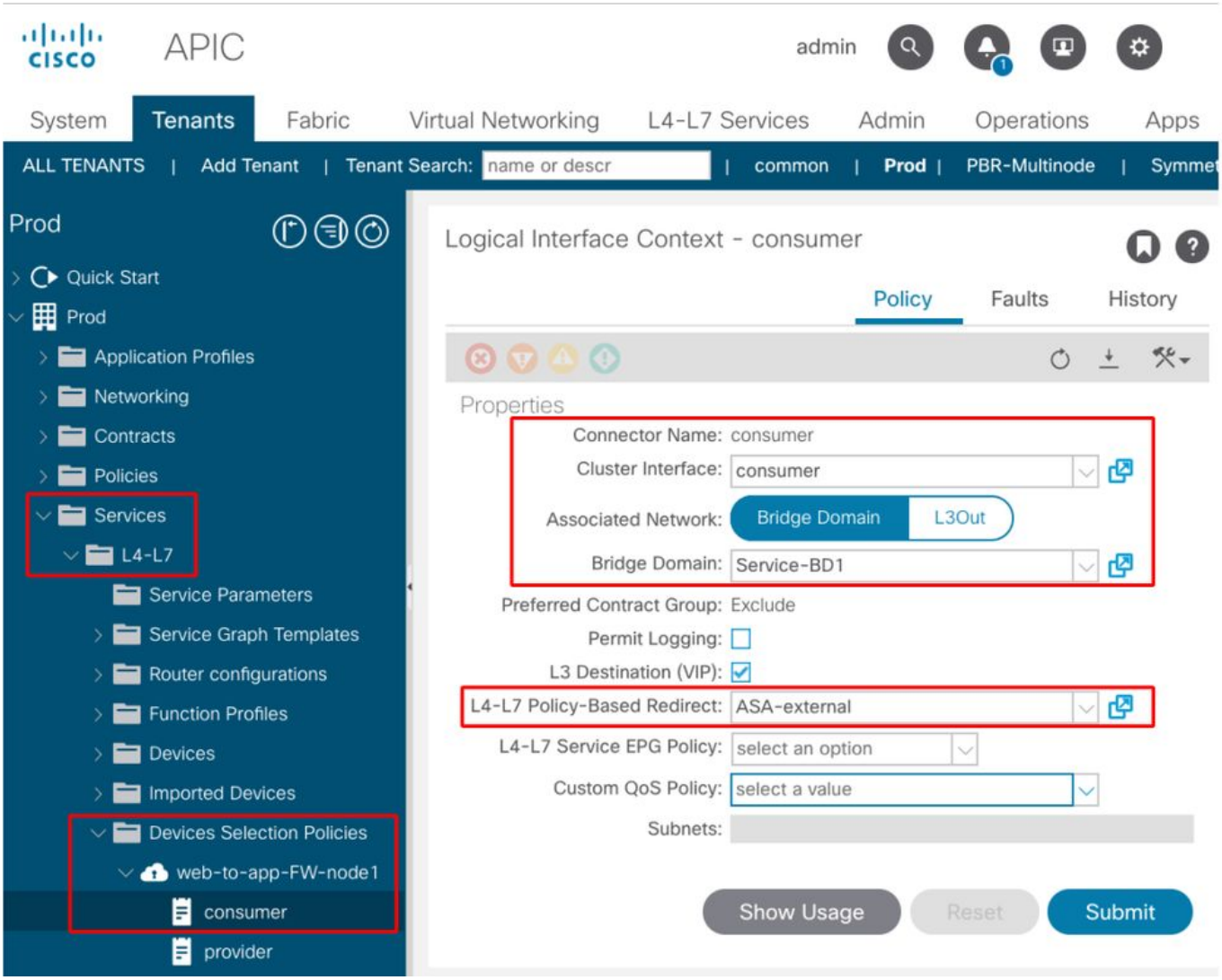
Résolution : cochez la case BD spécifiée dans la stratégie de sélection de périphérique et le nom du connecteur est correct (figure ci-dessous).

F1690 : la configuration n'est pas valide en raison d'une stratégie de redirection de service non valide

Cette erreur indique que la stratégie PBR n'est pas sélectionnée même si la redirection est activée sur la fonction de service dans le graphique des services.

Résolution : sélectionnez la stratégie PBR dans la stratégie de sélection de périphérique (figure ci-dessous).

Configuration d'interface logique dans la stratégie de sélection de périphérique



Dépannage du transfert PBR

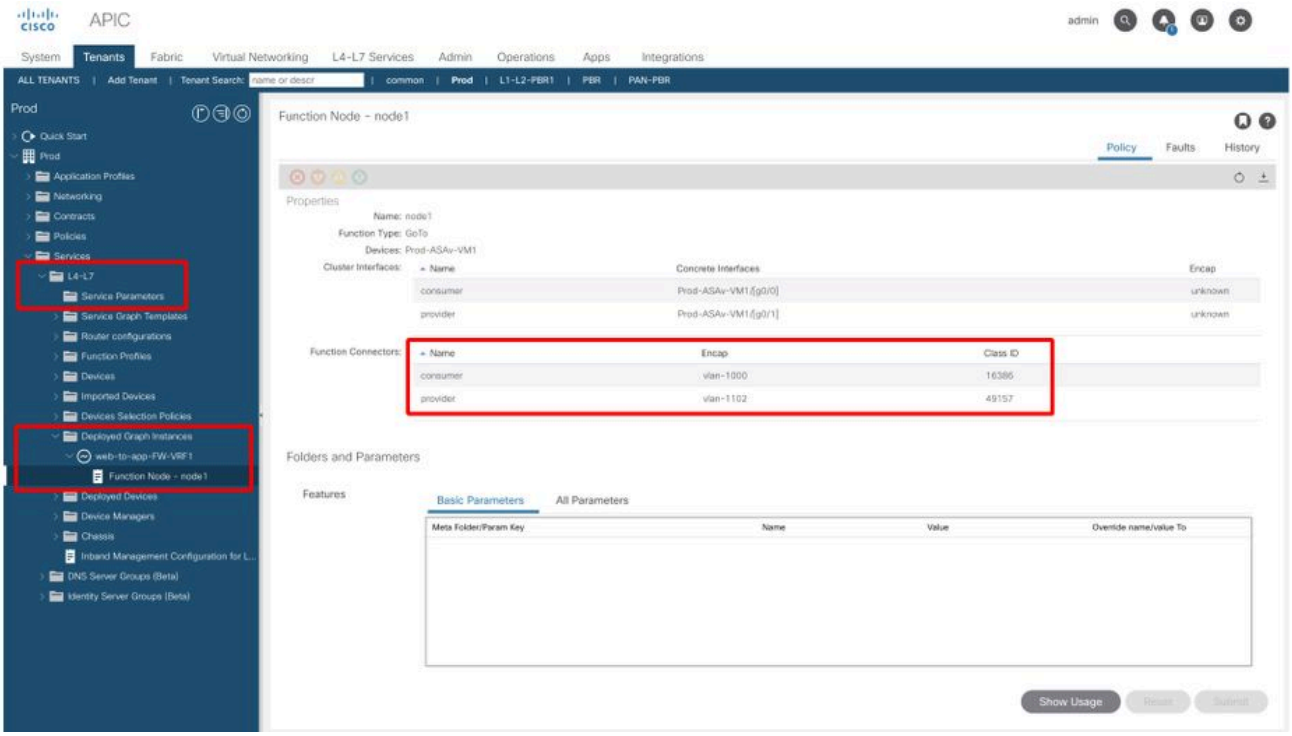
Ce chapitre explique les étapes de dépannage du chemin de transfert PBR.

1. Vérifiez que les VLAN sont déployés et que les points d'extrémité sont appris sur le noeud leaf

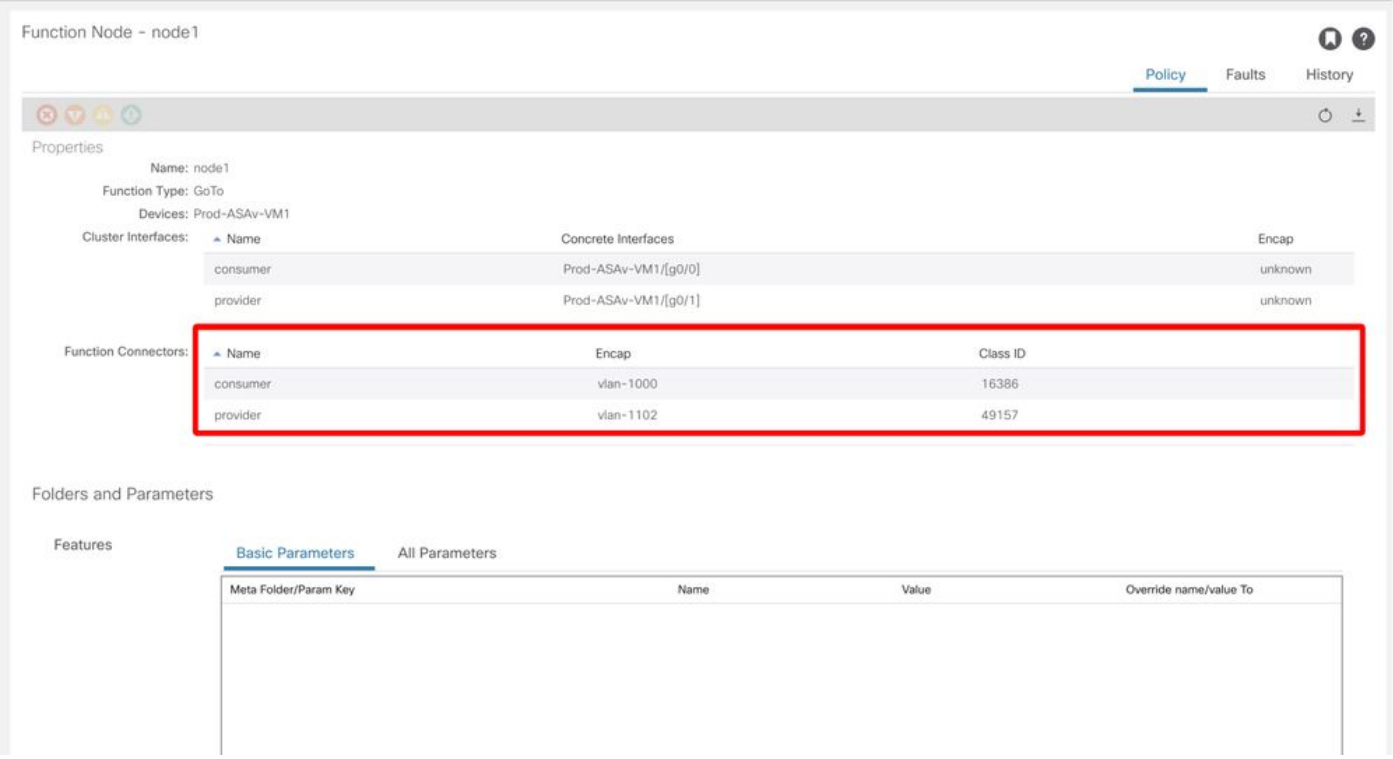
Une fois qu'un graphique de service est déployé sans erreur, des groupes de terminaux et des BD pour un noeud de service sont créés. La figure ci-dessous indique où trouver les ID de VLAN encapsulés et les ID de classe des interfaces de noeud de service (EPG de service). Dans cet exemple, le côté consommateur d'un pare-feu est la classe ID 16386 avec VLAN encap 1000 et le côté fournisseur est la classe ID 49157 avec VLAN encap 1102.

L'emplacement est 'Locataire > Services > L4-L7 > Instances de graphique déployées > Noeuds de fonction'.

Noeud Service



ID de classe d'interface de noeud de service



Ces réseaux locaux virtuels sont déployés sur les interfaces de noeud terminal de service où les noeuds de service sont connectés. Le déploiement VLAN et l'état d'apprentissage des points de terminaison peuvent être vérifiés à l'aide des commandes « show vlan extended » et « show endpoint » dans l'interface de ligne de commande du noeud de feuille de service.

<#root>

```
Pod1-Leaf1#
```

show endpoint vrf Prod:VRF1

```
Legend:
s - arp              H - vtep             V - vpc-attached     p - peer-aged
R - peer-attached-rl B - bounce           S - static           M - span
D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
L - local            E - shared-service
+------------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+------------------------------------+---------------+-----------------+--------------+-------------+
53                                      vlan-1000     0050.56af.3c60 LV                      po1
Prod:VRF1                               vlan-1000    192.168.101.100 LV                      po1
59                                      vlan-1102     0050.56af.1c44 LV                      po1
Prod:VRF1                               vlan-1102    192.168.102.100 LV                      po1
```

Si les adresses IP des points d'extrémité des noeuds de service ne sont pas apprises en tant que points d'extrémité dans le fabric ACI, il s'agit très probablement d'un problème de connectivité ou de configuration entre le noeud terminal et le noeud de service. Vérifiez les états suivants :

- Le noeud de service est connecté au port de liaison descendante leaf correct.

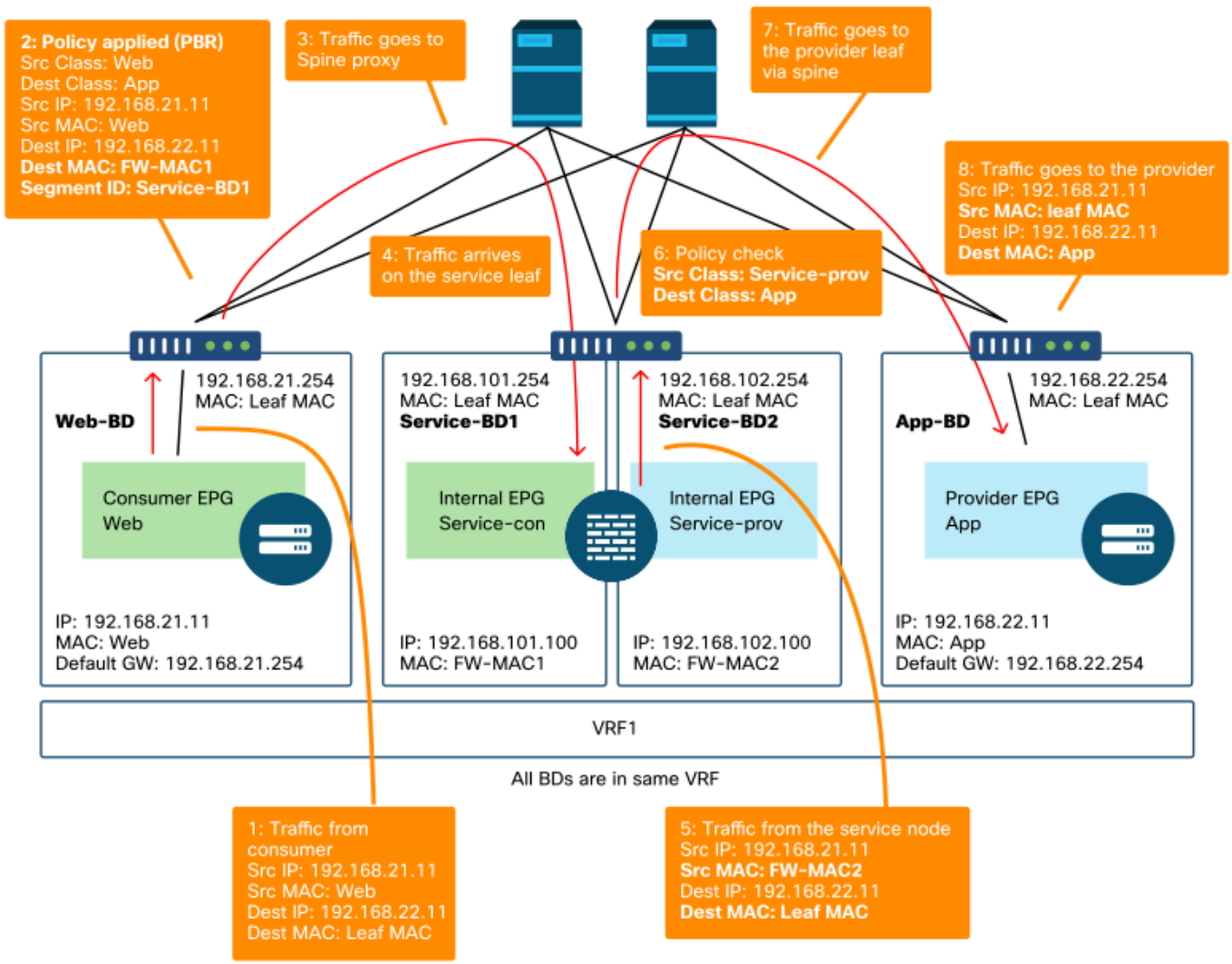
    - Si le noeud de service se trouve dans un domaine physique, le VLAN d'encapsulation d'extrémité de chemin statique feuille doit être défini dans le périphérique logique.
    - Si le noeud de service se trouve dans un domaine VMM, vérifiez que le domaine VMM fonctionne et que le groupe de ports créé via le graphique de services est correctement connecté à la machine virtuelle du noeud de service.
- Le port de liaison descendante leaf connecté au noeud de service ou à l'hyperviseur où réside la VM du noeud de service est UP.
- Le noeud de service a le VLAN et l'adresse IP corrects.
- Le commutateur intermédiaire entre le noeud terminal de service et le noeud de service a la configuration VLAN correcte.

2. Vérifiez les chemins de trafic attendus

Si le trafic de bout en bout cesse de fonctionner une fois que PBR est activé, même si les points d'extrémité du noeud de service sont appris dans le fabric ACI, l'étape de dépannage suivante consiste à vérifier quels sont les chemins de trafic attendus.

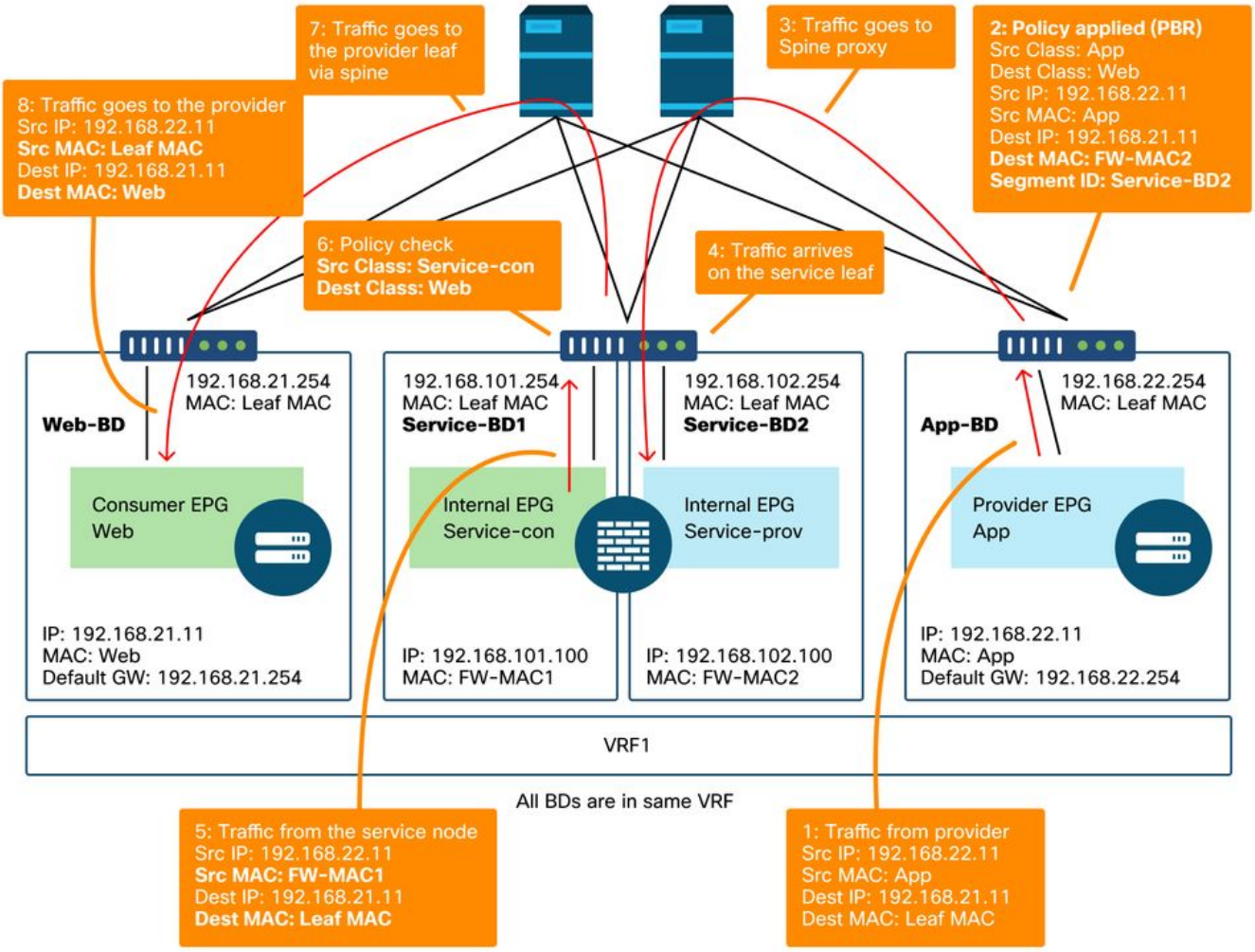
Les figures « Exemple de chemin de transfert PBR - consommateur à fournisseur » et « Exemple de chemin de transfert PBR - fournisseur à consommateur » illustrent un exemple de chemin de transfert d'insertion de pare-feu utilisant PBR entre un point d'extrémité consommateur et un point d'extrémité fournisseur. L'hypothèse est que les points d'extrémité sont déjà acquis sur les noeuds leaf.

Exemple de chemin de transfert PBR - du consommateur au fournisseur



Remarque : puisque l'adresse MAC source n'est pas remplacée par l'adresse MAC leaf ACI, le noeud PBR ne doit pas utiliser le transfert basé sur l'adresse MAC source si le point d'extrémité consommateur et le noeud PBR ne se trouvent pas dans le même BD

Exemple de chemin de transfert PBR - du fournisseur au consommateur



Remarque : il est utile de mentionner que la politique PBR est appliquée sur le client ou le fournisseur Leaf et que l'ACI PBR effectue une réécriture MAC de destination comme illustré dans les figures « Exemple de chemin de transfert PBR - consommateur à fournisseur » et « Exemple de chemin de transfert PBR - fournisseur à consommateur ». L'accès à l'adresse MAC de destination PBR utilise toujours un proxy spine, même si le point d'extrémité source et l'adresse MAC de destination PBR se trouvent sous le même noeud leaf.

Bien que les figures « Exemple de chemin de transfert PBR - consommateur à fournisseur » et « Exemple de chemin de transfert PBR - fournisseur à consommateur » montrent un exemple de redirection du trafic, l'application de la stratégie dépend de la configuration du contrat et de l'état d'apprentissage du point d'extrémité. Le tableau « Emplacement d'application de la stratégie » indique l'emplacement d'application de la stratégie sur un seul site ACI. L'application d'une stratégie dans Multi-Site est différente.

Où la stratégie est-elle appliquée ?

Scénario	Mode d'application VRF	Consommateur	Fournisseur	Stratégie appliquée sur
Intra-VRF	Entrée/sortie	EPG	EPG	· Si le terminal de destination est appris : leaf en entrée* · Si le terminal de destination n'est pas appris : leaf de sortie
	Entrée	EPG	EPG L3Out	Leaf consommateur (Leaf non-border)
	Entrée	EPG L3Out	EPG	Leaf du fournisseur (leaf non frontalier)
	Sortie	EPG	EPG L3Out	leaf en limite -> trafic leaf non en limite · Si le terminal de destination est appris : leaf en limite · Si le terminal de destination n'est pas appris : leaf non frontalier Trafic leaf non frontalier-> leaf frontalier · Feuille de bordure
	Sortie	EPG L3Out	EPG	
	Entrée/sortie	EPG L3Out	EPG L3Out	Feuille d'entrée*
Inter-VRF	Entrée/sortie	EPG	EPG	Feuille de consommateur
	Entrée/sortie	EPG	EPG L3Out	Leaf consommateur (Leaf non-border)
	Entrée/sortie	EPG L3Out	EPG	Feuille d'entrée*
	Entrée/sortie	EPG L3Out	EPG L3Out	Feuille d'entrée*

*L'application de la stratégie est appliquée au premier noeud leaf touché par le paquet.

Voici quelques exemples :

- Si un terminal externe dans L3Out EPG dans VRF1 tente d'accéder à un terminal dans Web EPG dans VRF1 et que VRF1 est configuré pour le mode d'application d'entrée, le trafic est redirigé par le terminal où réside le terminal dans Web EPG, quelle que soit la direction du contrat.
- Si un terminal dans le Web EPG consommateur dans VRF1 tente d'accéder à un terminal dans l'App EPG fournisseur dans VRF1, et que les terminaux sont appris sur les noeuds leaf consommateur et fournisseur, le trafic est redirigé par le leaf d'entrée.
- Si un point d'extrémité du Web EPG consommateur dans VRF1 tente d'accéder à un point d'extrémité dans l'App EPG fournisseur dans VRF2, le trafic est redirigé par le terminal consommateur où réside le point d'extrémité consommateur, quel que soit le mode d'application VRF.

3. Vérifiez si le trafic est redirigé vers le noeud de service

Une fois que le chemin de transfert attendu est libre, ELAM peut être utilisé pour vérifier si le trafic arrive sur les noeuds de commutation et vérifier la décision de transfert sur les noeuds de commutation. Reportez-vous à la section « Outils » du chapitre « Transfert intra-fabric » pour obtenir des instructions sur l'utilisation d'ELAM.

Par exemple, pour suivre le flux de trafic dans la figure « Exemple de chemin de transfert PBR - consommateur à fournisseur », ces données peuvent être capturées pour confirmer si le trafic consommateur à fournisseur est redirigé.

- Port de liaison descendante sur le terminal client pour vérifier 1 et 2 (le trafic arrive sur le terminal client et PBR est appliqué).
- Port de fabric sur les noeuds spine pour vérifier 3 (le trafic va au proxy spine).
- Port de fabric sur le noeud leaf de service pour vérifier 4 (le trafic arrive sur le noeud leaf de service).

Ensuite, ils peuvent être capturés pour confirmer si le trafic qui revient du noeud de service va au fournisseur.

- Port de liaison descendante sur le noeud leaf de service pour vérifier 5 et 6 (le trafic revient du noeud de service et est autorisé).
- Port de fabric sur les noeuds spine pour vérifier 7 (le trafic est transmis au noeud leaf du fournisseur via le noeud spine).
- Port de fabric sur le noeud leaf du fournisseur pour vérifier 8 (le trafic arrive sur le noeud leaf du service et va au point terminal du fournisseur).

Remarque : si le consommateur et le noeud de service se trouvent sous le même noeud leaf, spécifiez une interface ou un MAC source en plus de l'adresse IP source/de destination pour qu'ELAM vérifie 1 ou 5 dans la figure « Exemple de chemin de transfert PBR - consommateur vers fournisseur », car les deux utilisent la même adresse IP source et la même adresse IP de destination.

Si le trafic consommateur-fournisseur est redirigé vers le noeud de service mais ne revient pas au noeud leaf de service, veuillez vérifier les points suivants car il s'agit d'erreurs courantes :

- La table de routage du noeud de service atteint le sous-réseau du fournisseur.
- La stratégie de sécurité du noeud de service telle que ACL autorise le trafic.

Si le trafic est redirigé et arrive sur le fournisseur, veuillez vérifier le chemin de trafic de retour du fournisseur au consommateur d'une manière similaire.

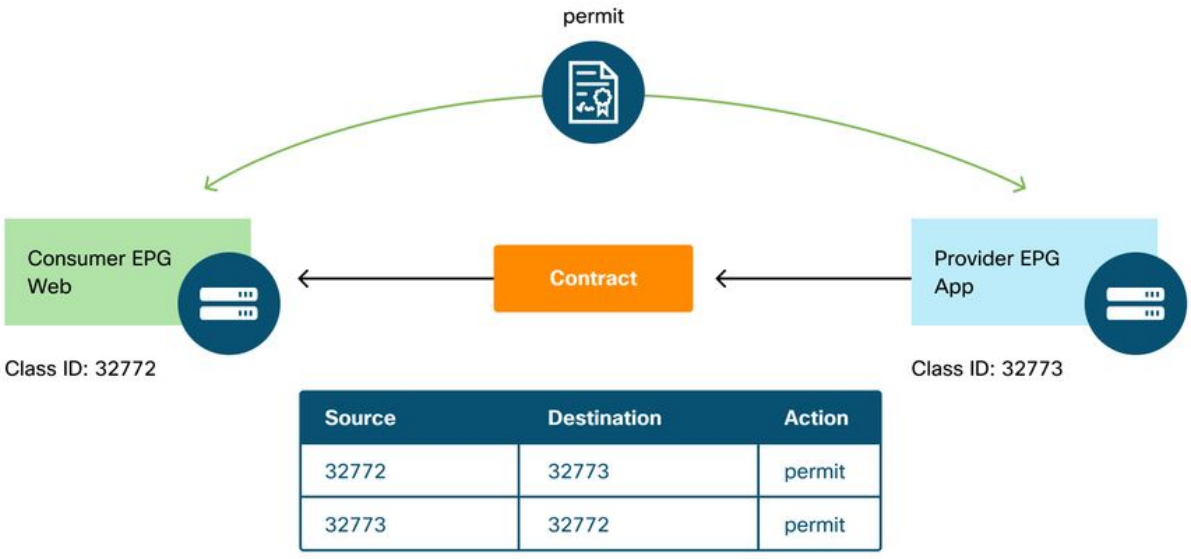
4. Vérifiez les stratégies programmées sur les noeuds leaf

Si le trafic n'est pas transféré ou redirigé en conséquence, la prochaine étape de dépannage consiste à vérifier les politiques programmées sur les noeuds leaf. Cette section présente zoning-rule et contract_parser à titre d'exemples. Pour plus d'informations sur la vérification des règles de zonage, reportez-vous à la section « Outils » du chapitre « Stratégies de sécurité ».

Remarque : les stratégies sont programmées en fonction de l'état de déploiement EPG sur le leaf. Le résultat de la commande show dans cette section utilise le noeud terminal qui a des EPG consommateur, fournisseur et EPG pour le noeud de service.

Utilisation de la commande « show zoning-rule »

La figure et le résultat « show zoning-rule » ci-dessous décrivent les règles de zonage avant le déploiement de Service Graph.



L'ID d'étendue VRF se trouve dans 'Locataire > Mise en réseau > VRF'.

<#root>

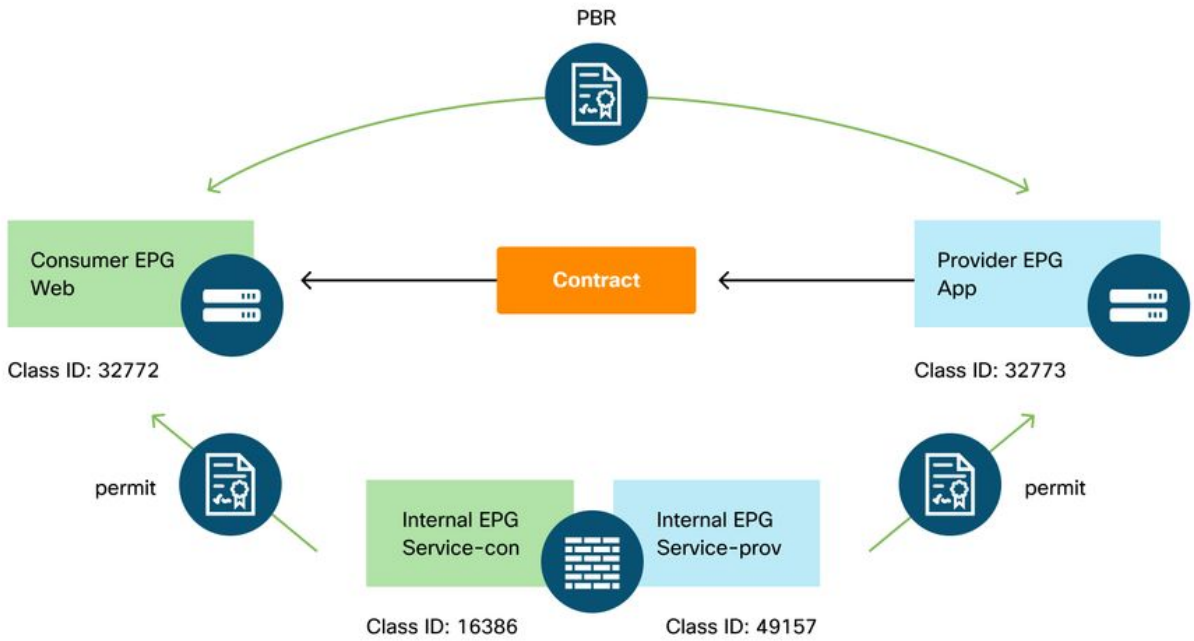
```
Pod1-Leaf1#
```

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------------+----------+--
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |    Name    |  Action  |
+---------+--------+--------+----------+----------------+---------+---------+------------+----------+--
|   4237  | 32772  | 32773  |    8     |     bi-dir     | enabled | 2752513 | web-to-app |  permit  |
|   4172  | 32773  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 | web-to-app |  permit  |
+---------+--------+--------+----------+----------------+---------+---------+------------+----------+--
```

Une fois le graphique de services déployé, les groupes de terminaux pour le noeud de service sont créés et les stratégies sont mises à jour pour rediriger le trafic entre les groupes de terminaux du consommateur et du fournisseur. La figure ci-dessous et le résultat « show zoning-rule » ci-dessous décrivent les règles de zonage après le déploiement de Service Graph. Dans cet exemple, le trafic de pcTag 32772 (Web) vers pcTag 32773 (App) est redirigé vers « destgrp-27 » (côté consommateur du noeud de service) et le trafic de pcTag 32773 (App) vers pcTag 32772 (Web) est redirigé vers « destgrp-28 » (côté fournisseur du noeud de service).

Règles de zonage après le déploiement de Service Graph



Source	Destination	Action
32772	32773	PBR to the consumer side of the service node
49157	32773	permit
32773	32772	PBR to the provider side of the service node
16386	32772	permit

<#root>

```
Pod1-Leaf1#
```

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+---------------+---------+---------+------+------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir      |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+---------------+---------+---------+------+------------------
...
|   4213  | 16386  | 32772  |    9     |    uni-dir    | enabled | 2752513 |      |       permit
|   4249  | 49157  | 32773  | default  |    uni-dir    | enabled | 2752513 |      |       permit
|   4237  | 32772  | 32773  |    8     |     bi-dir    | enabled | 2752513 |      | redir(destgrp-27)
|   4172  | 32773  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      | redir(destgrp-28)
+---------+--------+--------+----------+---------------+---------+---------+------+------------------
```

Les informations de destination de chaque destgrp peuvent être trouvées à l'aide de la commande « show service redir info ».

<#root>

Pod1-Leaf1#

show service redir info

```
========================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |
========================================================================================
List of Dest Groups
GrpID Name            destination                                HG-name           BAC  operSt     ope
===== ====            ===========                                ==============    ===  =======    ===
28    destgrp-28      dest-[192.168.102.100]-[vxlan-2752513]     Not attached      N    enabled    no-
27    destgrp-27      dest-[192.168.101.100]-[vxlan-2752513]     Not attached      N    enabled    no-

List of destinations
Name                                        bdVnid            vMac                   vrf          op
====                                        ======            ====                   ====         ==
dest-[192.168.102.100]-[vxlan-2752513]      vxlan-16023499    00:50:56:AF:1C:44      Prod:VRF1    en
dest-[192.168.101.100]-[vxlan-2752513]      vxlan-16121792    00:50:56:AF:3C:60      Prod:VRF1    en
...
```

Si les règles de zonage sont programmées en conséquence, mais que le trafic n'est pas redirigé ou transféré en conséquence, veuillez vérifier les points suivants, car il s'agit d'erreurs courantes :

- Vérifiez si l'ID de classe source ou de destination est résolu comme prévu à l'aide d'ELAM. Si ce n'est pas le cas, vérifiez l'ID de classe incorrect et les critères de dérivation EPG tels que le chemin et le VLAN d'encapsulation.
- Même si les ID de classes source et de destination sont résolus en conséquence et que la stratégie PBR est appliquée mais que le trafic n'arrive pas sur le noeud PBR, vérifiez que les adresses IP, MAC et VRF du destgrp dans l'action de redirection (« show service redir info ») sont correctes.

Par défaut, les règles d'autorisation d'un EPG consommateur vers un noeud de service (côté consommateur) et d'un EPG fournisseur vers un noeud de service (côté fournisseur) ne sont pas

programmées si PBR est activé. Par conséquent, un point d'extrémité consommateur ou fournisseur ne peut pas communiquer directement avec le noeud de service par défaut. Pour autoriser ce trafic, l'option Connexion directe doit être activée. L'exemple d'utilisation est expliqué dans la section « Autres exemples de flux de trafic ».

Utilisation de contract_parser

L'outil contract_parser peut également vous aider à vérifier les politiques. C-consommateur est le côté consommateur du noeud de service et C-fournisseur est le côté fournisseur du noeud de service.

```
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}] [hi

[7:4213] [vrf:Prod:VRF1] permit ip tcp tn-Prod/G-Prod-ASAv-VM1ctxVRF1/C-consumer(16386) eq 80 tn-Prod/a
[7:4237] [vrf:Prod:VRF1] redir ip tcp tn-Prod/ap-app1/epg-Web(32772) tn-Prod/ap-app1/epg-App(32773) eq
                         destgrp-27 vrf:Prod:VRF1 ip:192.168.101.100 mac:00:50:56:AF:3C:60 bd:uni
[7:4172] [vrf:Prod:VRF1] redir ip tcp tn-Prod/ap-app1/epg-App(32773) eq 80 tn-Prod/ap-app1/epg-Web(3277
                         destgrp-28 vrf:Prod:VRF1 ip:192.168.102.100 mac:00:50:56:AF:1C:44 bd:uni
[9:4249] [vrf:Prod:VRF1] permit any tn-Prod/G-Prod-ASAv-VM1ctxVRF1/C-provider(49157) tn-Prod/ap-app1/ep
```

...

Autres exemples de flux de trafic

Cette section examine d'autres exemples courants de flux de trafic pour identifier les flux souhaités pour le dépannage. Pour connaître les étapes de dépannage, reportez-vous au chapitre précédent de cette section.

1. Équilibreur de charge sans SNAT :
    - Dans cet exemple, le site Web EPG grand public et l'application EPG du fournisseur ont un contrat avec un graphique de service d'équilibrage de charge. Les terminaux de l'App EPG sont de véritables serveurs associés au VIP sur l'équilibreur de charge.
    - PBR vers équilibreur de charge est activé pour la direction du trafic fournisseur vers consommateur.
2. Pare-feu et équilibrage de charge sans SNAT :
    - Dans cet exemple, le site Web EPG grand public et l'application EPG du fournisseur ont un contrat avec un pare-feu et un graphique de service d'équilibrage de charge. Les terminaux de l'App EPG sont de vrais serveurs associés au VIP sur l'équilibreur de charge.
    - PBR vers pare-feu est activé pour les deux directions.
    - PBR vers équilibreur de charge est activé pour la direction du trafic fournisseur vers consommateur.
3. Service partagé (contrat inter-VRF) :
    - Dans cet exemple, le site Web EPG grand public et l'application EPG du fournisseur

ont un contrat avec un graphique de service de pare-feu. Les applications EPG Web et EPG se trouvent dans des VRF différents.
- PBR vers pare-feu est activé pour les deux directions.
- Le pare-feu se trouve entre les VRF.

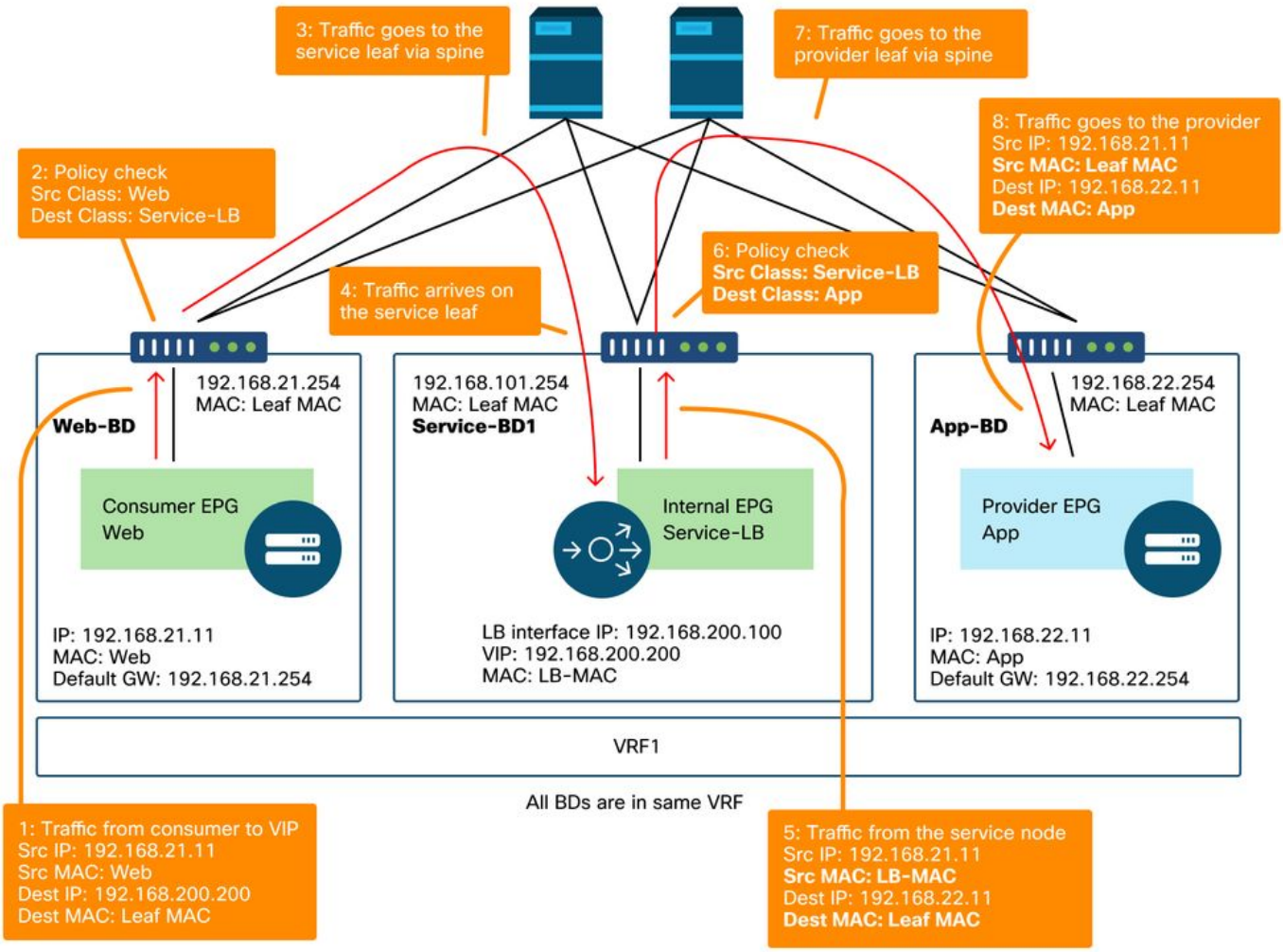
1. Équilibreur de charge sans SNAT

PBR peut être déployé en tant que PBR bidirectionnel ou PBR unidirectionnel. Un exemple d'utilisation du PBR unidirectionnel est l'intégration de l'équilibreur de charge sans traduction d'adresses de réseau (NAT) source. Si l'équilibreur de charge effectue la NAT source, PBR n'est pas requis.

Exemple de chemin de trafic

La figure ci-dessous illustre un exemple de flux de trafic entrant du consommateur EPG Web vers l'application EPG du fournisseur avec deux connexions : l'une est d'un point d'extrémité dans le consommateur EPG Web vers le programme VIP d'équilibrage de charge, et l'autre est de l'équilibreur de charge vers un point d'extrémité dans l'application EPG du fournisseur. Étant donné que le trafic entrant est destiné au VIP, le trafic atteindra l'équilibreur de charge sans PBR si le VIP est accessible. L'équilibreur de charge modifie l'adresse IP de destination en l'un des points d'extrémité de l'application EPG associée au VIP, mais ne traduit pas l'adresse IP source. Par conséquent, le trafic est acheminé vers le point d'extrémité du fournisseur.

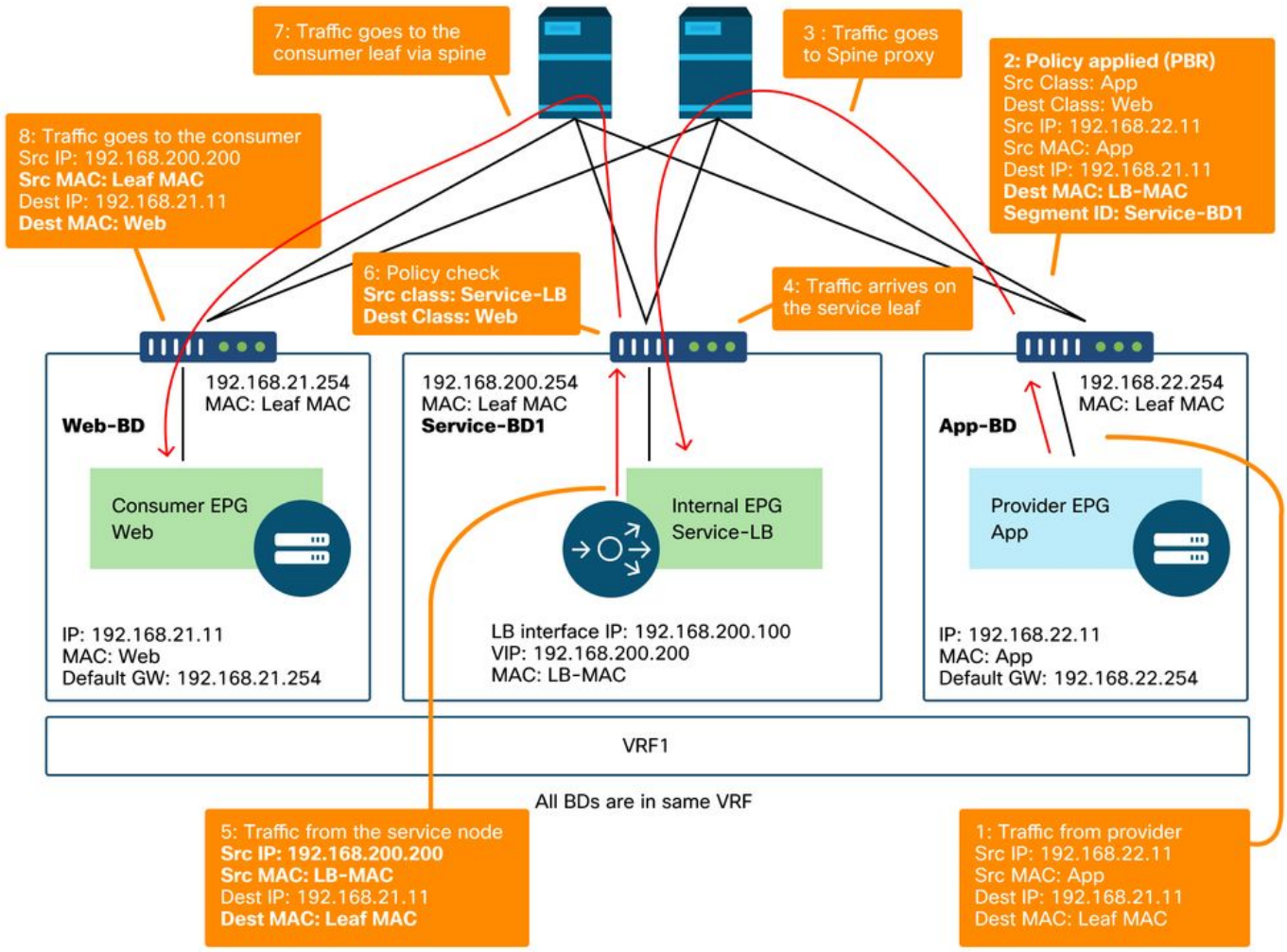
Exemple d'équilibreur de charge sans chemin de transfert SNAT - consommateur vers VIP et équilibreur de charge vers fournisseur sans PBR



La figure ci-dessous illustre le flux de trafic de retour de l'application EPG du fournisseur vers le Web EPG du consommateur. Étant donné que le trafic de retour est destiné à l'IP source d'origine, PBR est requis pour que le trafic de retour retourne à l'équilibreur de charge. Dans le cas contraire, le point d'extrémité consommateur reçoit le trafic où l'IP source est le point d'extrémité fournisseur au lieu du VIP. Ce trafic sera abandonné car le terminal consommateur n'a pas initié de trafic vers le terminal fournisseur, même si le réseau intermédiaire tel que le fabric ACI transfère le paquet au terminal consommateur.

Une fois que le trafic du point d'extrémité fournisseur vers le point d'extrémité consommateur est redirigé vers l'équilibreur de charge, l'équilibreur de charge change l'IP source en VIP. Ensuite, le trafic revient de l'équilibreur de charge et le trafic retourne au point d'extrémité consommateur.

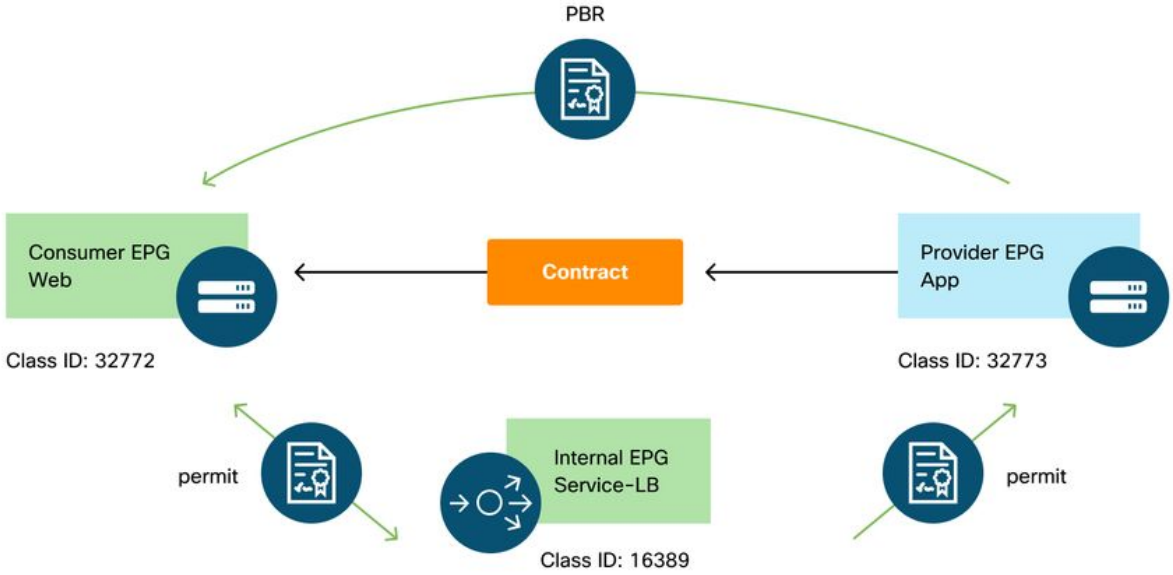
Exemple d'équilibreur de charge sans chemin de transfert SNAT - fournisseur au consommateur avec PBR



Les politiques programmées sur les noeuds leaf.

La figure ci-dessous et le résultat « show zoning-rule » ci-dessous décrivent les règles de zonage après le déploiement de Service Graph. Dans cet exemple, le trafic de pcTag 32772 (Web) vers pcTag 16389 (Service-LB) est autorisé, le trafic de pcTag 16389 (Service-LB) vers pcTag 32773 (App) est autorisé et le trafic de pcTag 32773 (App) vers pcTag 32772 (Web) est redirigé vers « destgrp-31 » (équilibreur de charge).

Règles de zonage après le déploiement de Service Graph - équilibreur de charge sans SNAT



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

<#root>

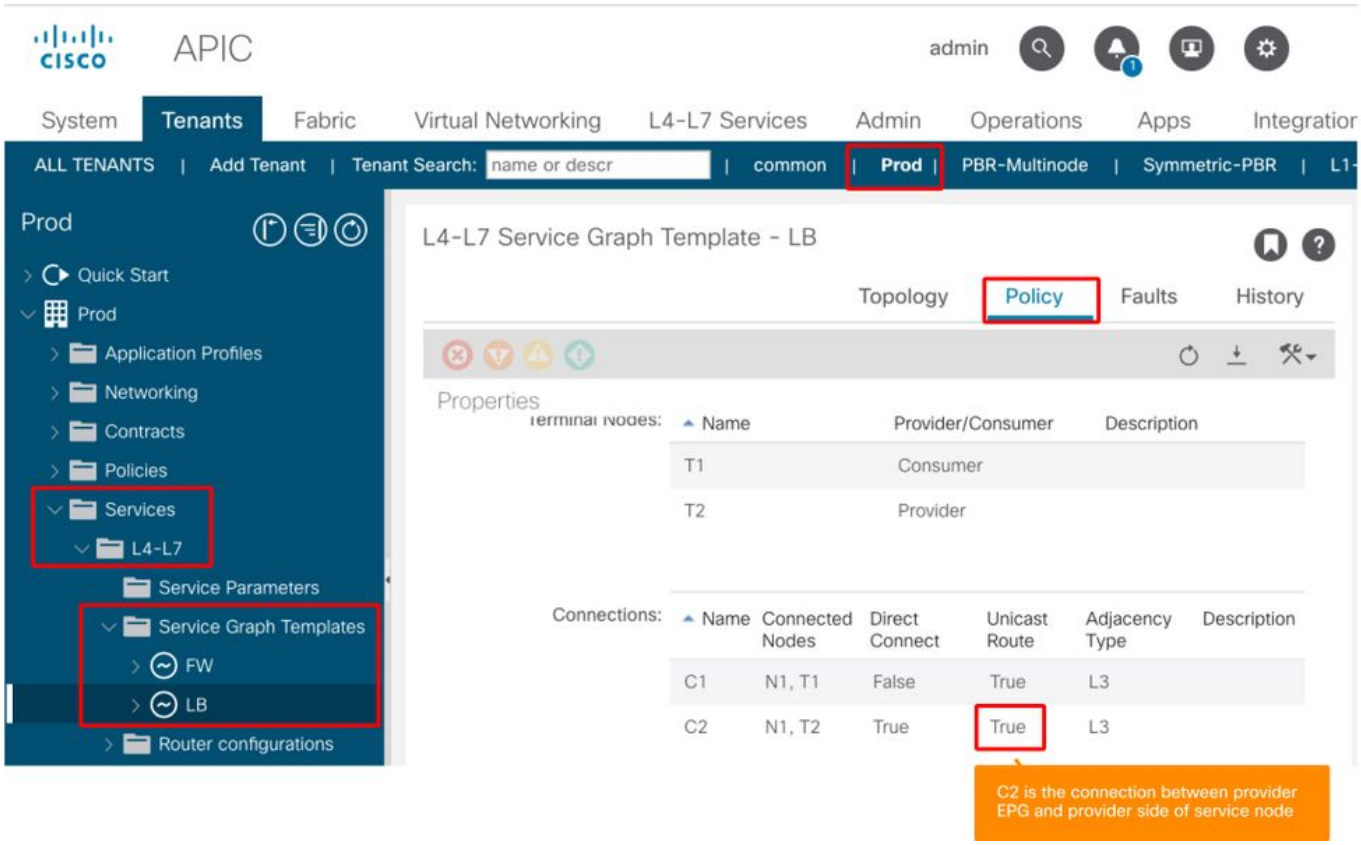
Pod1-Leaf1#

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------
|   4248  | 16389  | 32773  | default  |    uni-dir     | enabled | 2752513 |      |       permit
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      | redir(destgrp-31)
|   4234  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |       permit
|   4133  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      |       permit
...
```

Par défaut, une règle d'autorisation pour le fournisseur EPG (pcTag 32773) vers Service-LB (pcTag 16389) n'est pas programmée. Pour permettre une communication bidirectionnelle entre eux pour les vérifications de l'intégrité de l'équilibreur de charge vers les points d'extrémité du fournisseur, l'option Connexion directe sur la connexion doit être définie sur True. L'emplacement est 'Locataire > L4-L7 > Modèles de graphiques de service > Stratégie'. La valeur par défaut est False.

Définir l'option Connexion directe



Il ajoute une règle d'autorisation pour le fournisseur EPG(32773) à Service-LB(16389) comme ci-dessous.

<#root>

Pod1-Leaf1#

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------+----------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+----------------------
|   4248  | 16389  | 32773  | default  |     bi-dir     | enabled | 2752513 |      |       permit
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      | redir(destgrp-31)
|   4234  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |       permit
|   4133  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      |       permit
|   4214  | 32773  | 16389  | default  | uni-dir-ignore | enabled | 2752513 |      |       permit
+---------+--------+--------+----------+----------------+---------+---------+------+----------------------
```

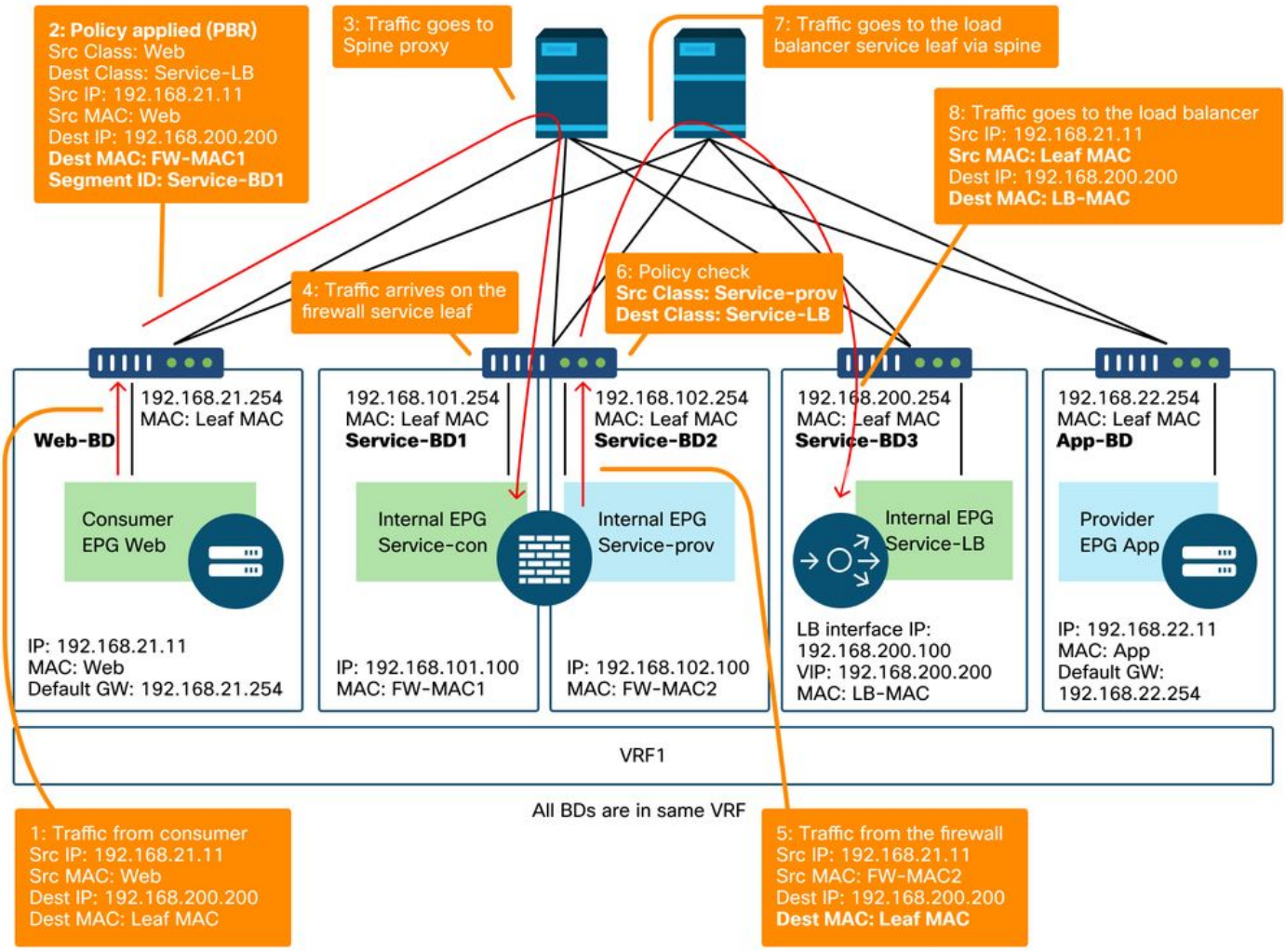
2. Exemple de flux de trafic - Pare-feu et équilibreur de charge sans SNAT

PBR peut être déployé avec plusieurs fonctions de service dans un graphique de services, telles que le pare-feu comme premier noeud et l'équilibreur de charge comme second noeud.

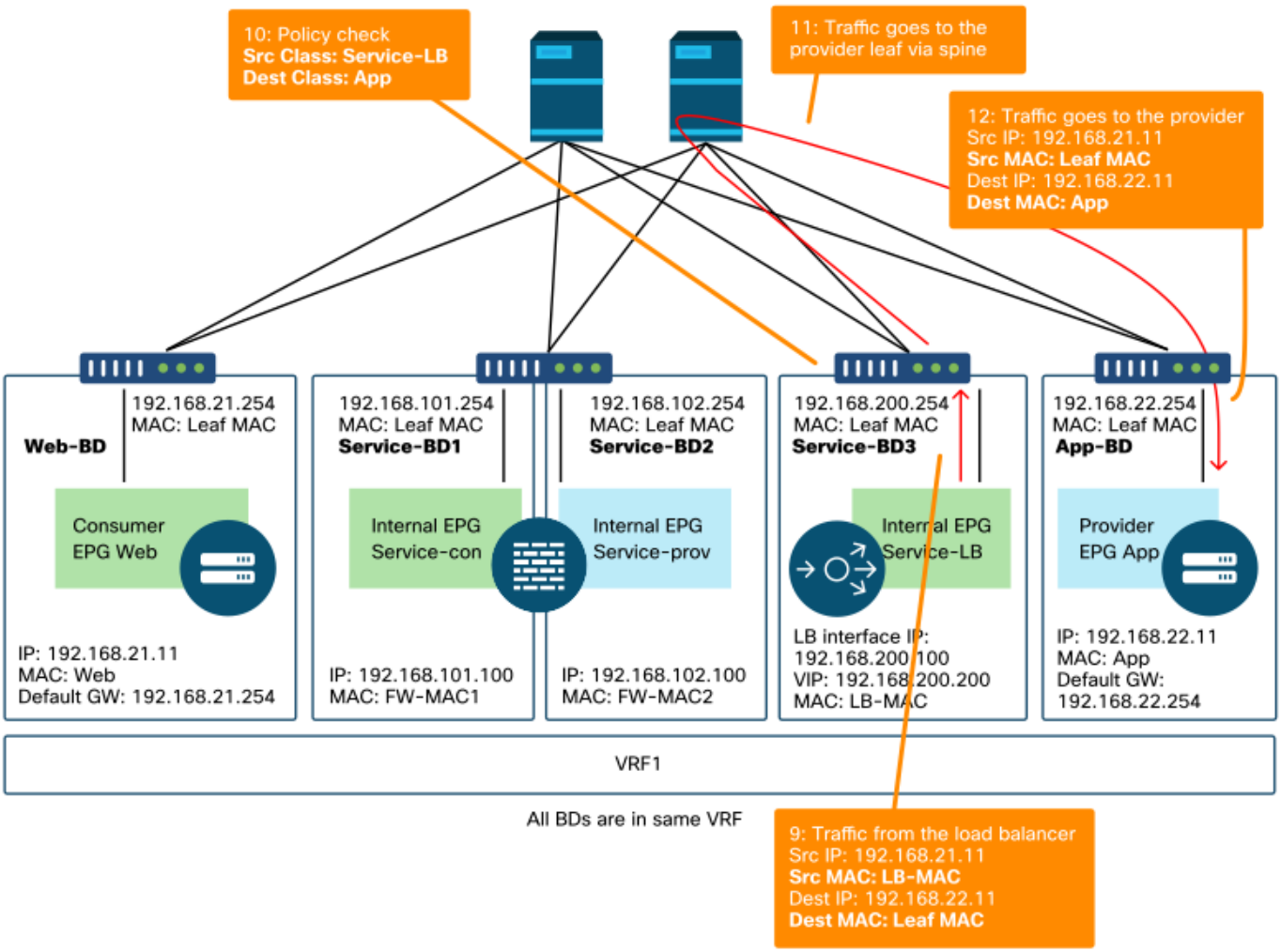
Exemple de chemin de trafic

La figure ci-dessous illustre un exemple de flux de trafic entrant du consommateur EPG Web vers l'application EPG du fournisseur avec deux connexions : l'une est d'un point d'extrémité dans le consommateur EPG Web vers l'équilibreur de charge VIP via un pare-feu et l'autre est de l'équilibreur de charge vers un point d'extrémité dans l'application EPG du fournisseur. Le trafic entrant destiné au VIP est redirigé vers le pare-feu, puis dirigé vers l'équilibreur de charge sans PBR. L'équilibreur de charge modifie l'adresse IP de destination en l'un des points d'extrémité dans l'EPG d'application associé au VIP, mais ne traduit pas l'adresse IP source. Ensuite, le trafic est acheminé vers le terminal du fournisseur.

Exemple de pare-feu et d'équilibreur de charge sans chemin de transfert SNAT - consommateur vers VIP et équilibreur de charge vers fournisseur



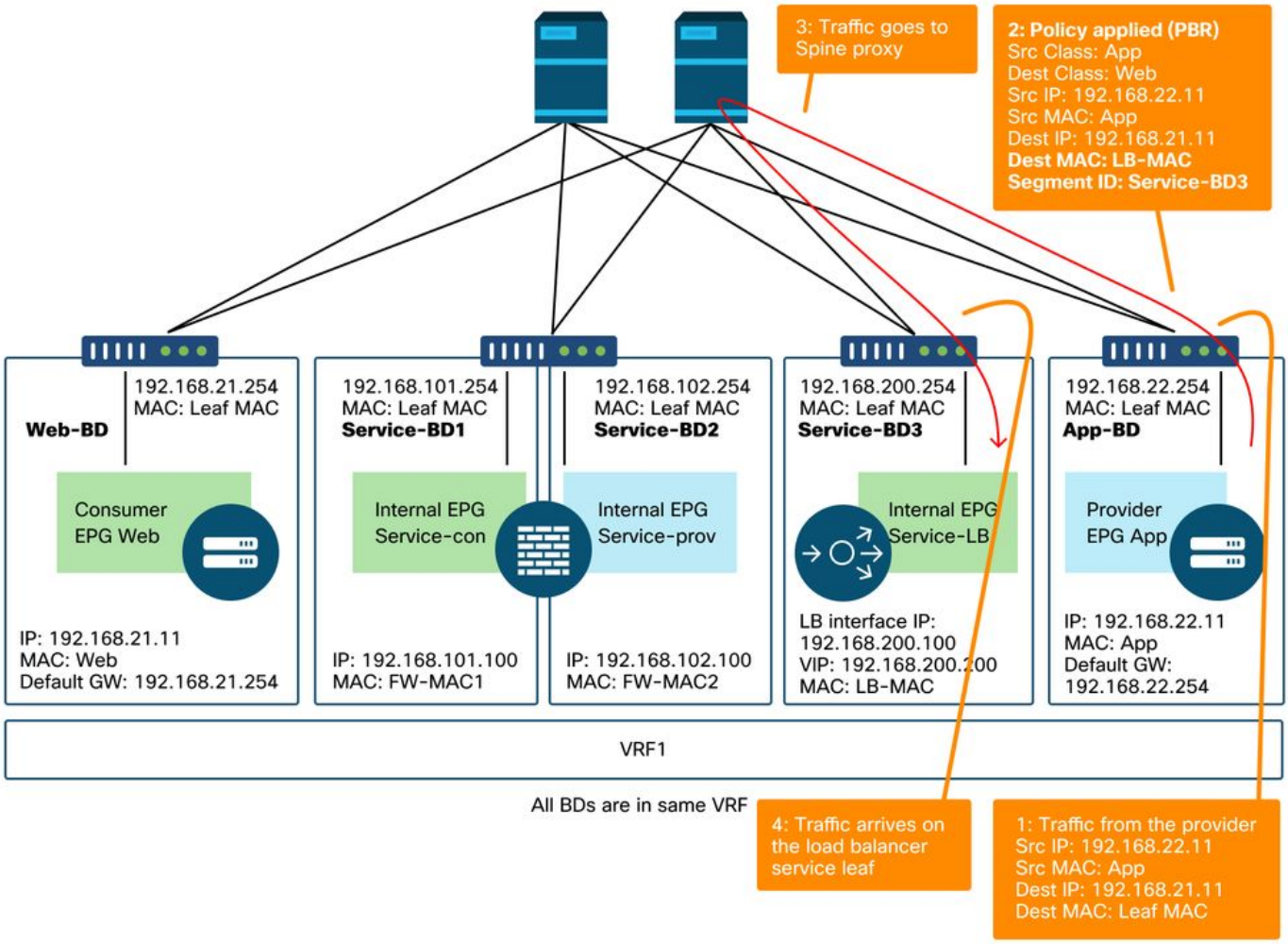
Exemple de pare-feu et d'équilibreur de charge sans chemin de transfert SNAT - consommateur vers VIP et équilibreur de charge vers fournisseur (suite)

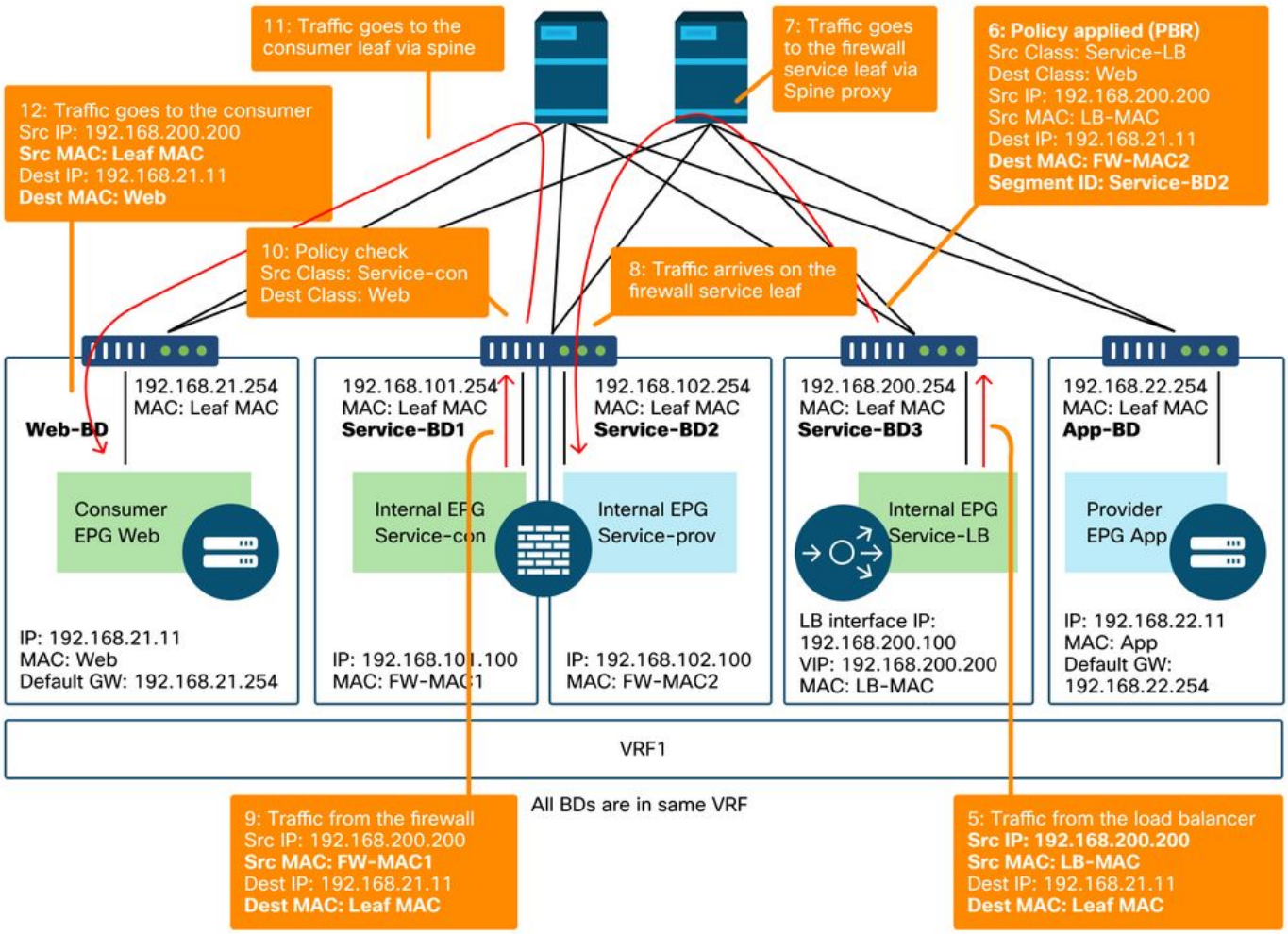


La figure ci-dessous illustre le flux de trafic de retour de l'application EPG du fournisseur vers le Web EPG du consommateur. Étant donné que le trafic de retour est destiné à l'IP source d'origine, PBR est nécessaire pour que le trafic de retour retourne à l'équilibreur de charge.

Une fois que le trafic du point d'extrémité fournisseur vers le point d'extrémité consommateur est redirigé vers l'équilibreur de charge, l'équilibreur de charge change l'IP source en VIP. Le trafic revient de l'équilibreur de charge et est redirigé vers le pare-feu. Ensuite, le trafic revient du pare-feu et retourne au terminal du consommateur.

Exemple de pare-feu et d'équilibreur de charge sans chemin de transfert SNAT - fournisseur au consommateur

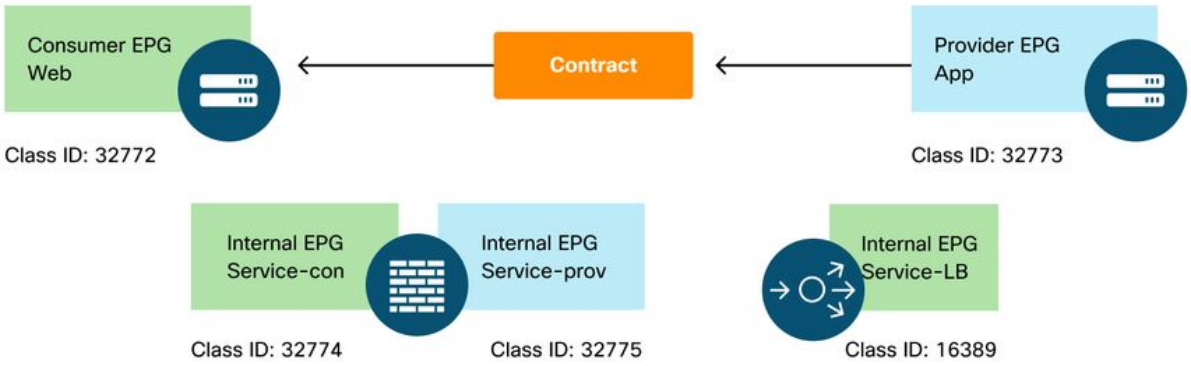

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



Les politiques programmées sur les noeuds leaf

La figure ci-dessous et le résultat « show zoning-rule » ci-dessous décrivent les règles de zonage après le déploiement de Service Graph. Dans cet exemple, le trafic de pcTag 32772 (Web) vers pcTag 16389 (Service-LB) est redirigé vers « destgrp-32 » (côté consommateur du pare-feu), le trafic de pcTag 32773 (App) vers pcTag 32772 (Web) est redirigé vers « destgrp-33 » (équilibreur de charge) et le trafic de pcTag 16389 (Service-LB) vers pcTag 32772 (Web) est redirigé vers « destgrp-34 » (côté fournisseur du pare-feu).

Règles de zonage après le déploiement de Service Graph - pare-feu et équilibreur de charge sans 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

<#root>

```
Pod1-Leaf1#
```

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------+------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+------------------
|   4236  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      | redir(destgrp-32)
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      | redir(destgrp-33)
|   4171  | 16389  | 32773  | default  |     bi-dir     | enabled | 2752513 |      |       permit
|   4248  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      | redir(destgrp-34)
|   4214  | 32774  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |       permit
|   4244  | 32775  | 16389  | default  |    uni-dir     | enabled | 2752513 |      |       permit
|   4153  | 32773  | 16389  | default  | uni-dir-ignore | enabled | 2752513 |      |       permit
+---------+--------+--------+----------+----------------+---------+---------+------+------------------
```

Dans l'exemple ci-dessus, l'option de connexion directe est définie sur « True » sur la connexion entre le côté fournisseur de l'équilibreur de charge et l'EPG fournisseur. Il doit être activé pour la vérification de l'état de l'équilibreur de charge vers les points de terminaison du fournisseur. L'emplacement est 'Locataire > L4-L7 > Modèles de graphiques de service >Stratégie'. Reportez-

vous à la figure « Définir l'option de connexion directe ».

3. Service partagé (contrat inter-VRF)

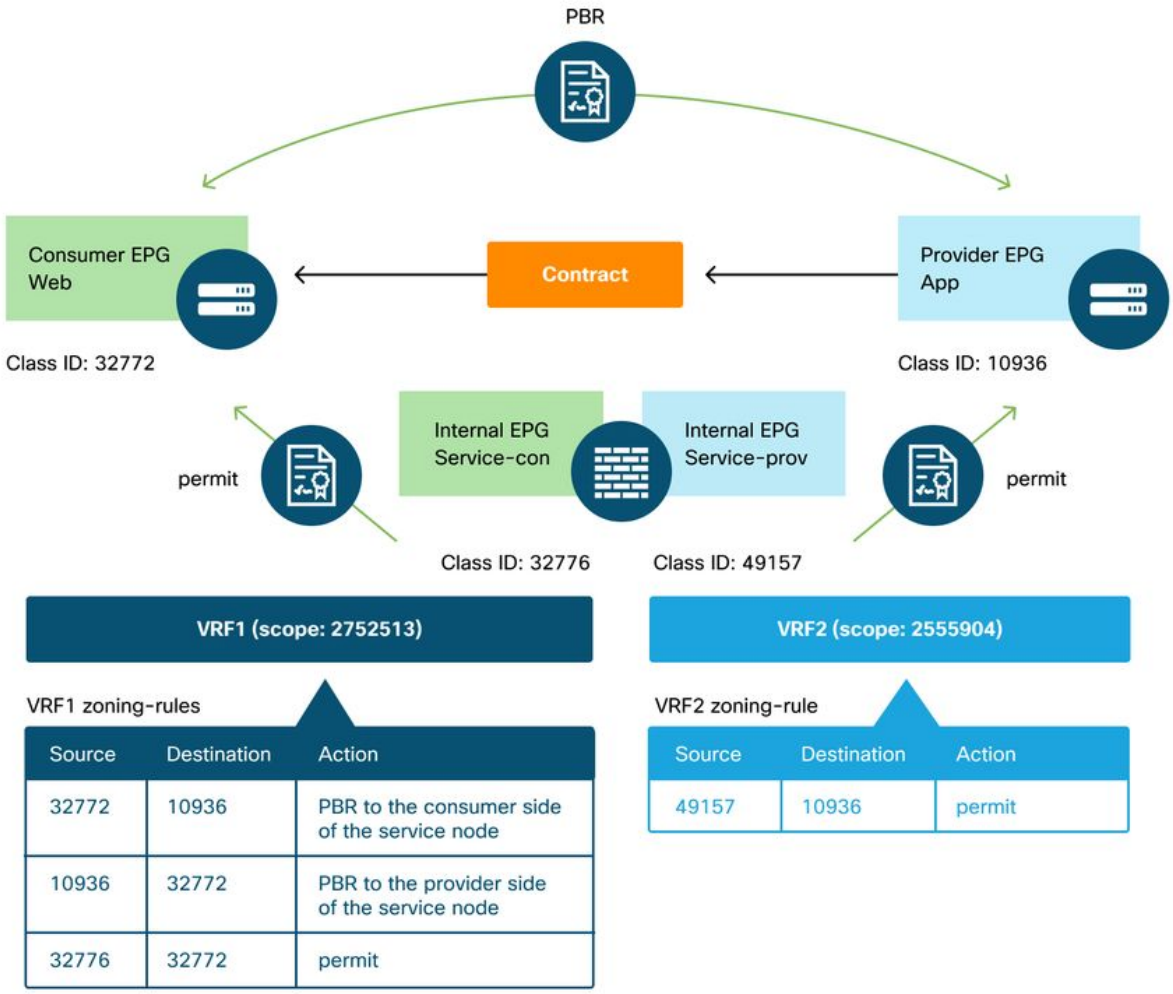
PBR peut être activé dans un contrat inter-VRF. Cette section explique comment les règles de zonage sont programmées dans le cas d'un contrat EPG à EPG inter-VRF.

Les politiques programmées sur les noeuds leaf

En cas de contrat entre EPG et EPG inter-VRF, la politique est toujours appliquée dans le VRF consommateur. Ainsi, la redirection se produit sur le VRF consommateur. Pour les autres combinaisons, reportez-vous au tableau « Où la stratégie est-elle appliquée ? » de la section « Transmission ».

La figure ci-dessous et le résultat « show zoning-rule » ci-dessous décrivent les règles de zonage après le déploiement de Service Graph. Dans cet exemple, le trafic de pcTag 32772 (Web) vers pcTag 10936 (App) est redirigé vers « destgrp-36 » (côté consommateur du noeud de service) et le trafic de pcTag 10936 (App) vers pcTag 32772 (Web) est redirigé vers « destgrp-35 » (côté fournisseur du noeud de service). Les deux sont appliqués dans VRF1 qui est un VRF consommateur. Le trafic entre pcTag 32776 (côté consommateur du pare-feu) et pcTag 32772 (Web) est autorisé dans VRF1.

Règles de zonage après le déploiement de Service Graph - contrat inter-VRF




```
Pod1-Leaf1# show zoning-rule scope 2752513
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------
|   4191  | 32776  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |       permit
|   4143  | 10936  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      | redir(destgrp-35)
|   4136  | 32772  | 10936  |    8     |     bi-dir     | enabled | 2752513 |      | redir(destgrp-36)
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------
```

Le trafic entre pcTag 49157 (côté fournisseur du pare-feu) et pcTag 10936 (App) est autorisé dans VRF2, car les deux sont dans VRF2.

<#root>

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
+---------+--------+--------+----------+---------+---------+---------+------+----------+---------------
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.