أستكشاف أخطاء إعادة التوجيه المستندة إلى سياسة قائمة على قائمة التحكم في الوصول (ACI) وإصالحها

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لفهم سيناريو إعادة توجيه (PBR) قائم على سياسة واجهة التحكم في الوصول واستكشاف أخطائه وإصالحها.

معلومات أساسية

تم إستخالص المواد من هذا المستند من وصول أستكشاف أخطاء البنية الأساسية وإصالحها، الإصدار الثاني، وخاصة **إعادة التوجيه القائمة على السياسة - نظرة عامة، إعادة التوجيه المستندة إلى السياسة - نشر الرسم البياني للخدمة، إعادة التوجيه المستندة إلى السياسة - إعادة التوجيه وإعادة التوجيه المستندة إلى السياسة - أمثلة تدفق حركة المرور الأخرى.**

نظرة عامة على إعادة التوجيه القائمة على السياسة

يشرح هذا الفصل أستكشاف أخطاء الرسم البياني لخدمة الوضع غير المدار وإصلاحها باستخدام إعادة التوجيه المستند إلى النهج (PBR).

فيما يلي خطوات نموذجية لاستكشاف الأخطاء وإصلاحها. يشرح هذا الفصل كيفية التحقق من الخطوات 1 و 2 الخاصة ب PBR. فيما يتعلق بالخطوتين 3 و 4، يرجى الرجوع إلى الفصول التالية: "إعادة التوجيه داخل البنية" و"إعادة التوجيه الخارجية" و"سياسات الأمان".

1. تحقق من حركة مرور البيانات بدون الرسم البياني لخدمة PBR: تم التعرف على نقاط نهاية المستهلكين والموزعين.يمكن أن تتصل نقاط النهاية للمستهلك والموزع.
2. تحقق من نشر الرسم البياني للخدمة: لا يوجد خطأ في مثيلات الرسم البياني المنشورة.يتم نشر شبكات VLAN ومعرفات الفئة لعقدة الخدمة.تم التعرف على نقاط نهاية عقدة الخدمة.
3. تحقق من مسار إعادة التوجيه: تم برمجة نهج التحقق على العقد الطرفية.التقاط حركة المرور على عقدة الخدمة لتأكيد ما إذا كان قد تم إعادة توجيه حركة المرور.التقط حركة المرور على صفحة قائمة التحكم في الوصول (ACI) لتأكيد ما إذا كانت حركة المرور تعود إلى بنية واجهة التحكم في الوصول (ACI) بعد PBR.
4. تحقق من وصول حركة المرور إلى نقطة نهاية العميل والموزع، وأن نقطة النهاية توقف بإنشاء حركة مرور الإرجاع.

يغطي هذا المستند خيارات التصميم أو التكوين. للحصول على هذه المعلومات، يرجى الرجوع إلى "التقرير الرسمي عن البروتوكول ACI PBR" على العنوان Cisco.com

في هذا الفصل، تتضمن عقدة الخدمة وأوراق الخدمة ما يلي:

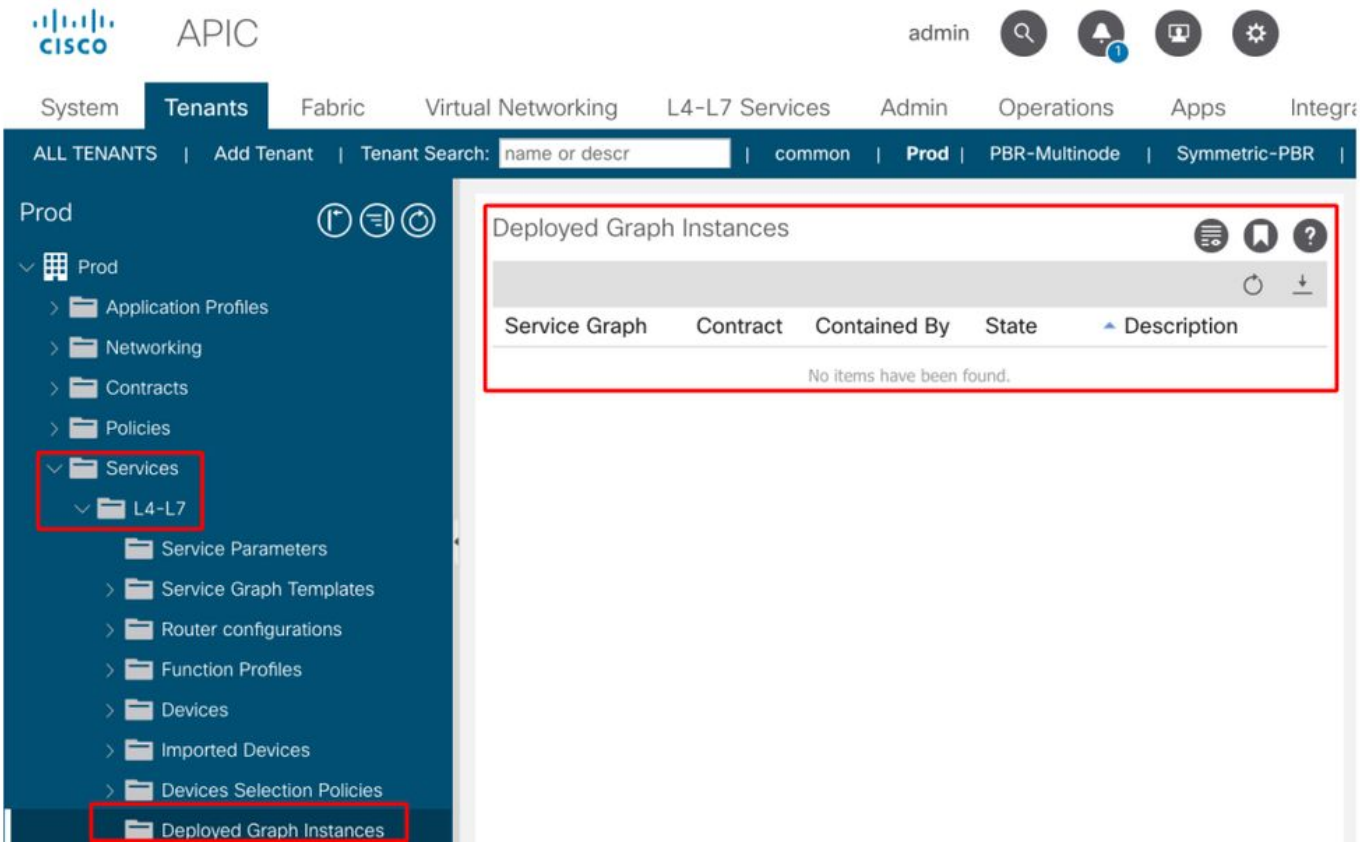
- عقدة الخدمة — عقدة خارجية يتم توجيه حركة مرور البيانات إليها بواسطة PBR، مثل جدار الحماية أو موازن التحميل.
- ورقة الخدمة — عبارة عن صفحة قائمة على التحكم في الوصول (ACI) متصلة بعقدة خدمة.

أستكشاف أخطاء نشر الرسم البياني للخدمة وإصلاحها

يشرح هذا الفصل مثال أستكشاف الأخطاء وإصلاحها في حالة عدم نشر الرسم البياني للخدمة.

بعد تحديد سياسة "الرسم البياني للخدمة" وتطبيقها على موضوع عقد، يجب أن يكون هناك مثيل رسم بياني منشور ظهر على واجهة المستخدم الرسومية (GUI) ل ACI. يوضح الشكل التالي سيناريو أستكشاف الأخطاء وإصلاحها حيث لا يظهر الرسم البياني للخدمة على أنه تم نشره.

لا يتم عرض الرسم البياني للخدمة كمثيل للرسم البياني الذي تم نشره.



1. تحقق من خطوات التكوين والأعطال

تتمثل الخطوة الأولى لاستكشاف الأخطاء وإصلاحها في التحقق من تكوين المكونات الضرورية دون أي خطأ. من المفترض أن التكوينات العامة الموضحة أدناه قد تم إجراؤها بالفعل:

- VRF و BDs لـ EPG للمستهلك و Provider EPG وعقدة الخدمة
- EPG للمستهلك والمزود.
- العقد وعوامل التصفية.

الجدير بالذكر أنه لا يلزم إنشاء EPG لعقدة الخدمة يدويا. سيتم إنشاؤها من خلال نشر "الرسم البياني للخدمة".

فيما يلي رسم Service Graph مع خطوات تكوين PBR:

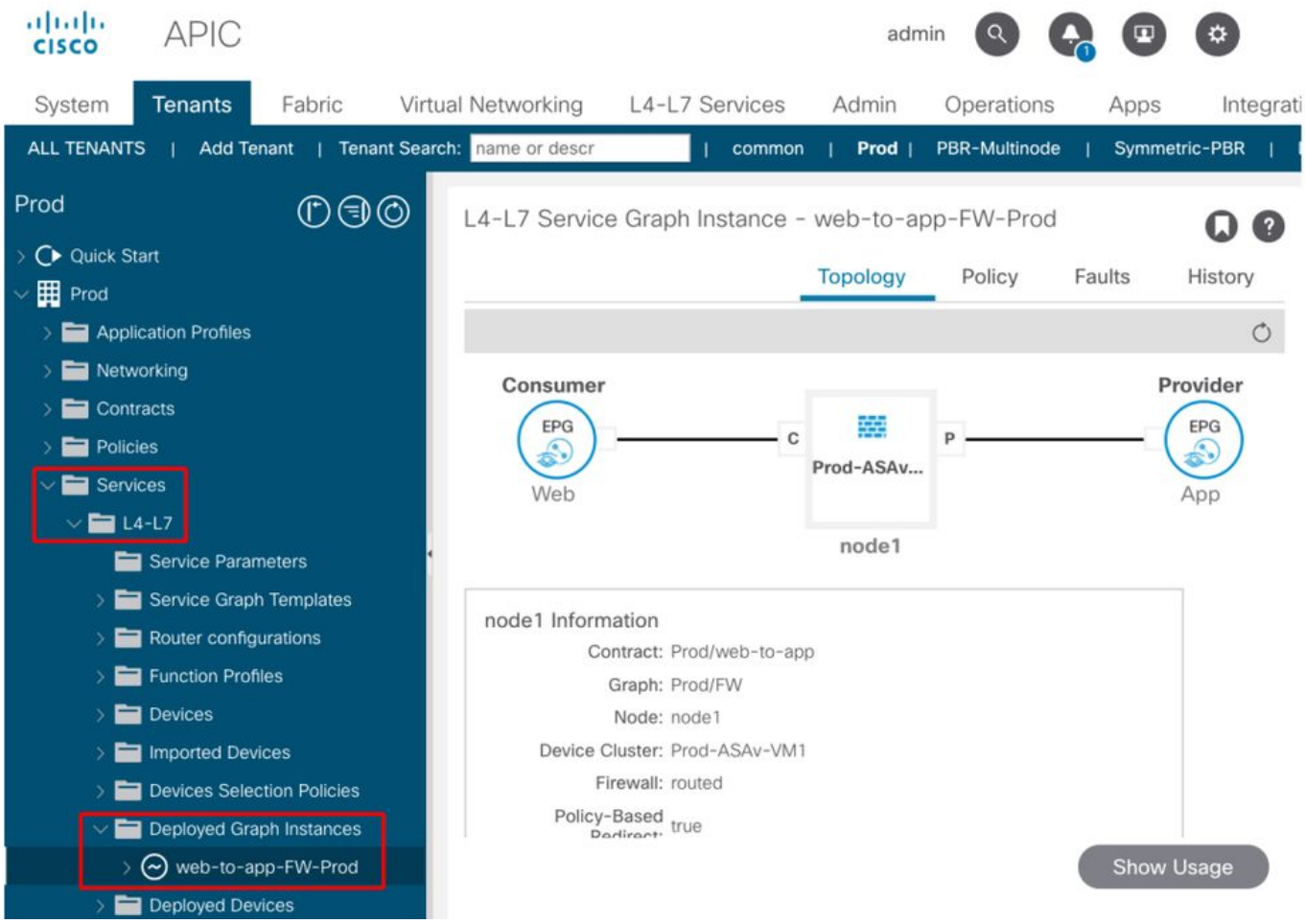
- إنشاء جهاز L4-L7 (جهاز منطقي).
- إنشاء الرسم البياني للخدمة.
- قم بإنشاء نهج PBR.
- إنشاء نهج تحديد الجهاز.
- إقران الرسم البياني للخدمة مع موضوع العقد.

2. التحقق من نشر الرسم البياني للخدمة في واجهة المستخدم

بعد إقران الرسم البياني للخدمة بموضوع العقد، يجب أن يظهر مثيل الرسم البياني المنشور لكل عقد مع الرسم البياني للخدمة (الشكل أدناه).

الموقع هو 'مستأجر > خدمات > L4-L7 > مثيلات الرسم البياني المنشورة'

مثيل الرسم البياني المنتشر



إذا لم يظهر مثيل الرسم البياني المنشور، فهناك خطأ في تكوين العقد. الأسباب الرئيسية يمكن أن تكون:

- لا يحتوي العقد على EPG للمستهلك أو المورد.
- لا يحتوي موضوع العقد على أي عامل تصفية.
- نطاق العقد هو VRF على الرغم من أنه خاص بالاتصال بين VRF أو بين المستأجرين EPG.

في حالة فشل إنشاء مثيل الرسم البياني للخدمة، يتم رفع الأخطاء في مثيل الرسم البياني المنشور، مما يعني وجود خطأ ما في تكوين الرسم البياني للخدمة. فيما يلي الأخطاء النموذجية التي يتسبب فيها التكوين:

F1690: التكوين غير صالح بسبب فشل تخصيص المعرف

يشير هذا الخطأ إلى أن الغلاف VLAN لـ الخدمة العقدة لا يتوفر. على سبيل المثال، لا توجد شبكة VLAN ديناميكية متاحة في تجمع VLAN المرتبط بمجال VMM المستخدم في الجهاز المنطقي.

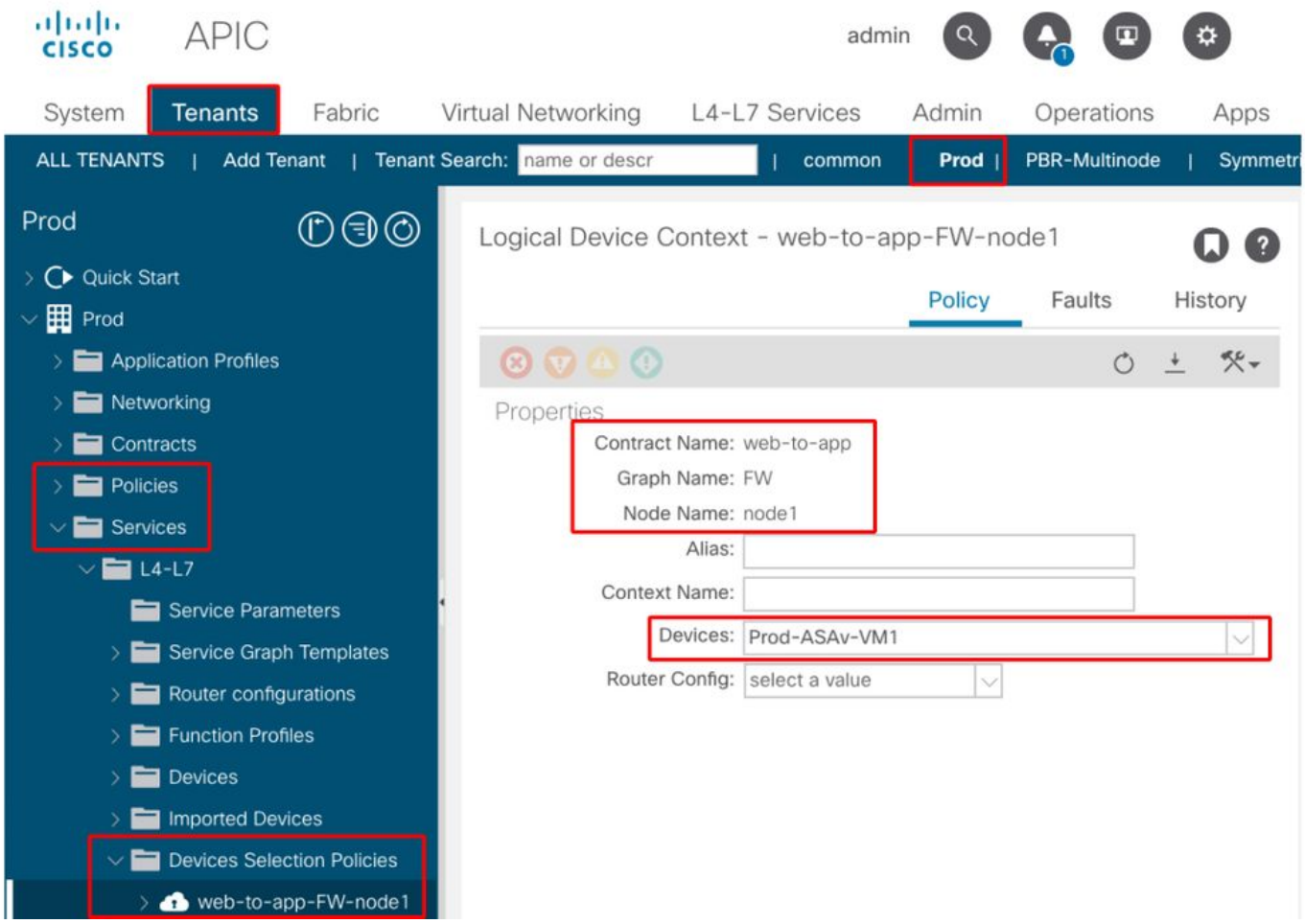
الدقة: تحقق من تجمع VLAN في المجال المستخدم للجهاز المنطقي. فحص الغلاف VLAN في المنطقي الأداة القارن إن هو يكون في مجال طبيعي. الأماكن هي 'Tenant > Services > L4-L7 > Devices and Fabric >Access Policies > Pool > VLAN'.

F1690: التكوين غير صالح لعدم العثور على سياق الجهاز لـ LDev

يشير هذا الخطأ إلى أنه يتعذر العثور على الجهاز المنطقي لعرض الرسم البياني للخدمة. على سبيل المثال، لا يوجد نهج تحديد الجهاز المطابق للعقد مع الرسم البياني للخدمة.

الدقة: تحقق من تحديد نمج تحديد الجهاز. توفر "سياسة تحديد الجهاز" معيار تحديد لجهاز الخدمة وموصلاته. تستند المعايير إلى اسم العقد واسم الرسم البياني للخدمة واسم العقدة في الرسم البياني للخدمة. الموقع هو 'مستأجر > خدمات > L4-L7 > سياسة تحديد الأجهزة'.

التحقق من نمج تحديد الجهاز



F1690: التكوين غير صالح لعدم العثور على واجهة نظام المجموعة

يشير هذا الخطأ إلى عدم العثور على واجهة نظام المجموعة لعقدة الخدمة. على سبيل المثال، لم يتم تحديد واجهة نظام المجموعة في نمج تحديد الأجهزة.

الدقة: تحقق من تحديد واجهة نظام المجموعة في نمج تحديد الأجهزة ومن صحة اسم الموصل (شكل أدناه).

F1690: التكوين غير صالح لعدم العثور على BD

يشير هذا الخطأ إلى عدم العثور على BD لعقدة الخدمة. على سبيل المثال، لم يتم تحديد BD في نمج تحديد الجهاز.

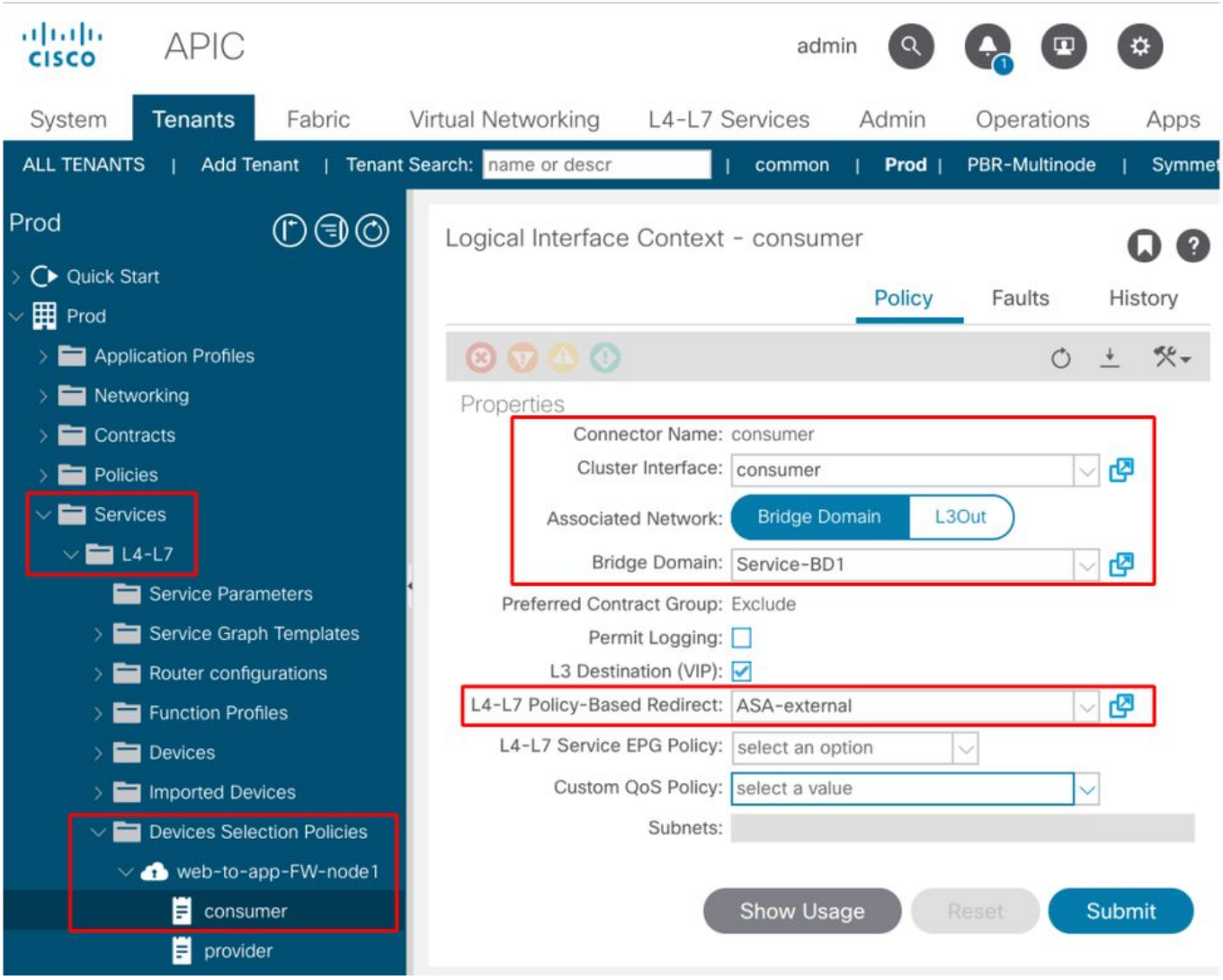
الدقة: تم تحديد BD في نمج تحديد الجهاز واسم الموصل صحيح (شكل أدناه).

F1690: التكوين غير صالح بسبب نمج إعادة توجيه الخدمة غير الصالح

يشير هذا الخطأ إلى أنه لم يتم تحديد نمج PBR حتى على الرغم من تمكين إعادة التوجيه على وظيفة الخدمة في الرسم البياني للخدمة.

الحل: حدد نهج PBR في نهج تحديد الأجهزة (شكل أدناه).

تكوين الواجهة المنطقي في نهج تحديد الجهاز



إعادة توجيه PBR لاستكشاف الأخطاء وإصلاحها

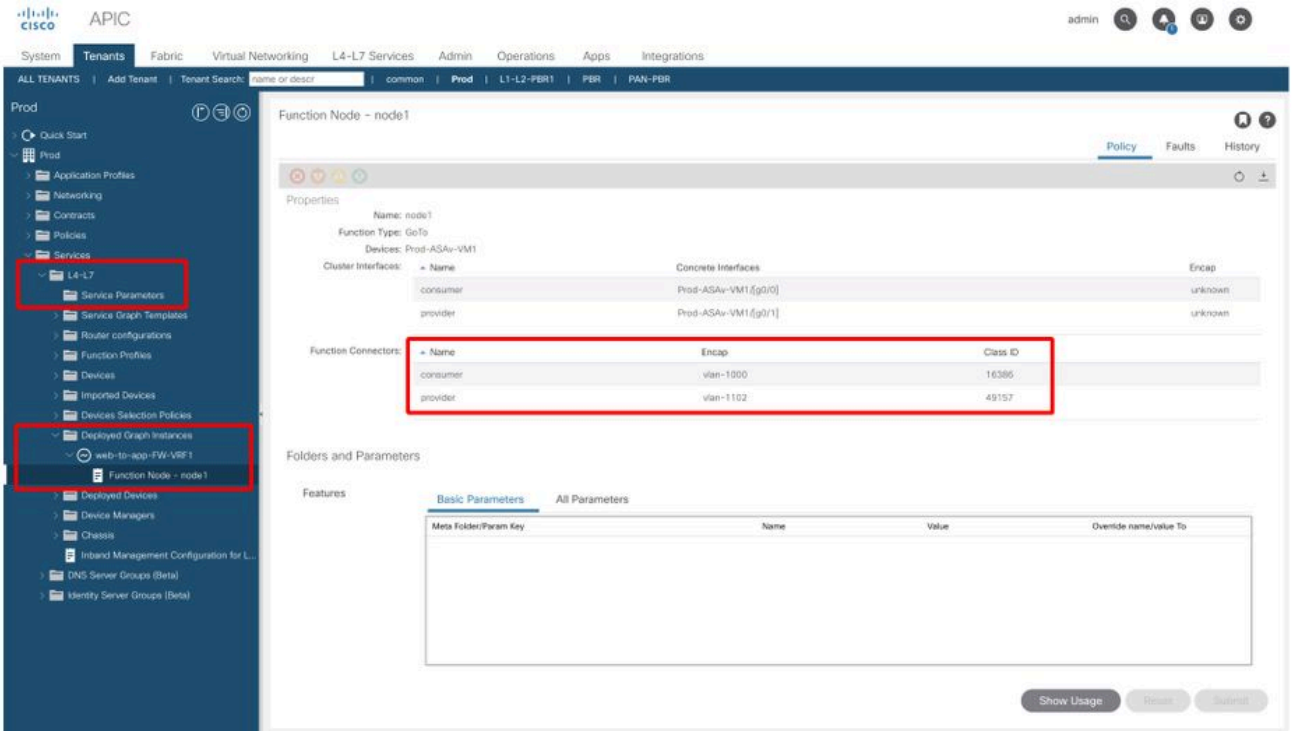
يشرح هذا الفصل خطوات أستكشاف الأخطاء وإصلاحها لمسار إعادة توجيه PBR.

1. تحقق من نشر شبكات VLAN وتعلم نقاط النهاية على العقدة الطرفية

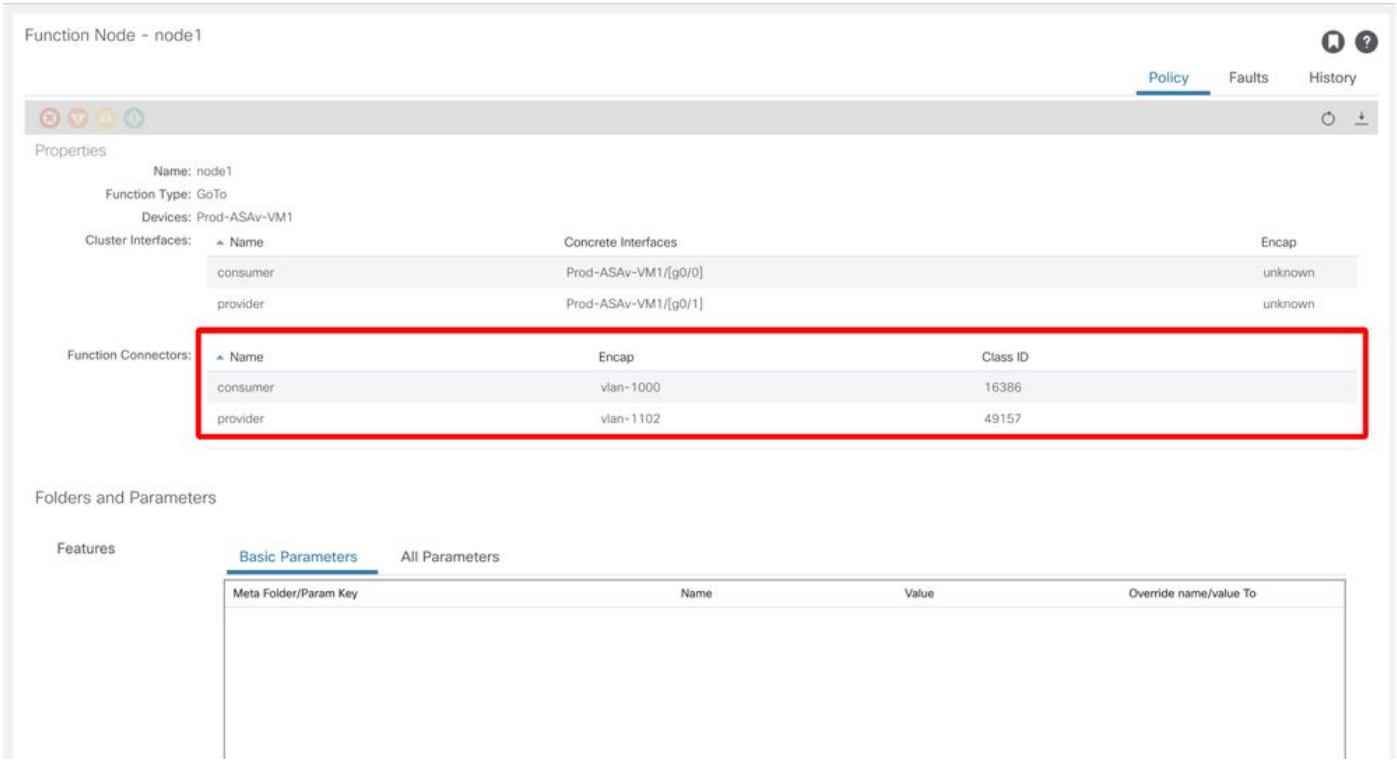
بمجرد نشر الرسم البياني للخدمة بنجاح دون أي خطأ، يتم إنشاء EPG و BDs لعقدة خدمة. يوضح الشكل التالي مكان العثور على معرفات شبكات VLAN التي تم تغليفها ومعرفات الفئة لواجهات عقد الخدمة (وحدات EPG للخدمة). في هذا المثال، يكون جانب المستهلك من جدار الحماية هو معرف الفئة 16386 مع VLAN encap 1000 ويكون جانب المورد لجدار الحماية هو معرف الفئة 49157 مع VLAN Encap 1102.

الموقع هو 'مستأجر > خدمات > L4-L7 > مثيلات الرسم البياني المنشورة > عقد الوظائف'.

عقدة الخدمة



معرف فئة واجهة عقدة الخدمة



يتم نشر شبكات VLAN هذه على واجهات عقدة ورقة الخدمة حيث تكون عقد الخدمة متصلة. يمكن التحقق من حالة نشر شبكة VLAN وتعلم نقطة النهاية باستخدام 'show vlan extended' و'show endpoint' على واجهة سطر الأوامر (CLI) لعقدة ورقة الخدمة.

```
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
```

إذا لم يتم التعرف على عناوين IP الخاصة بنقطة النهاية لعقد الخدمة كنقاط نهاية في بنية تلقائية التحكم في الوصول (ACI)، فإن هناك مشكلة اتصال أو تكوين بين عقدة الخدمة وقرة الخدمة. الرجاء التحقق من الحالات التالية:

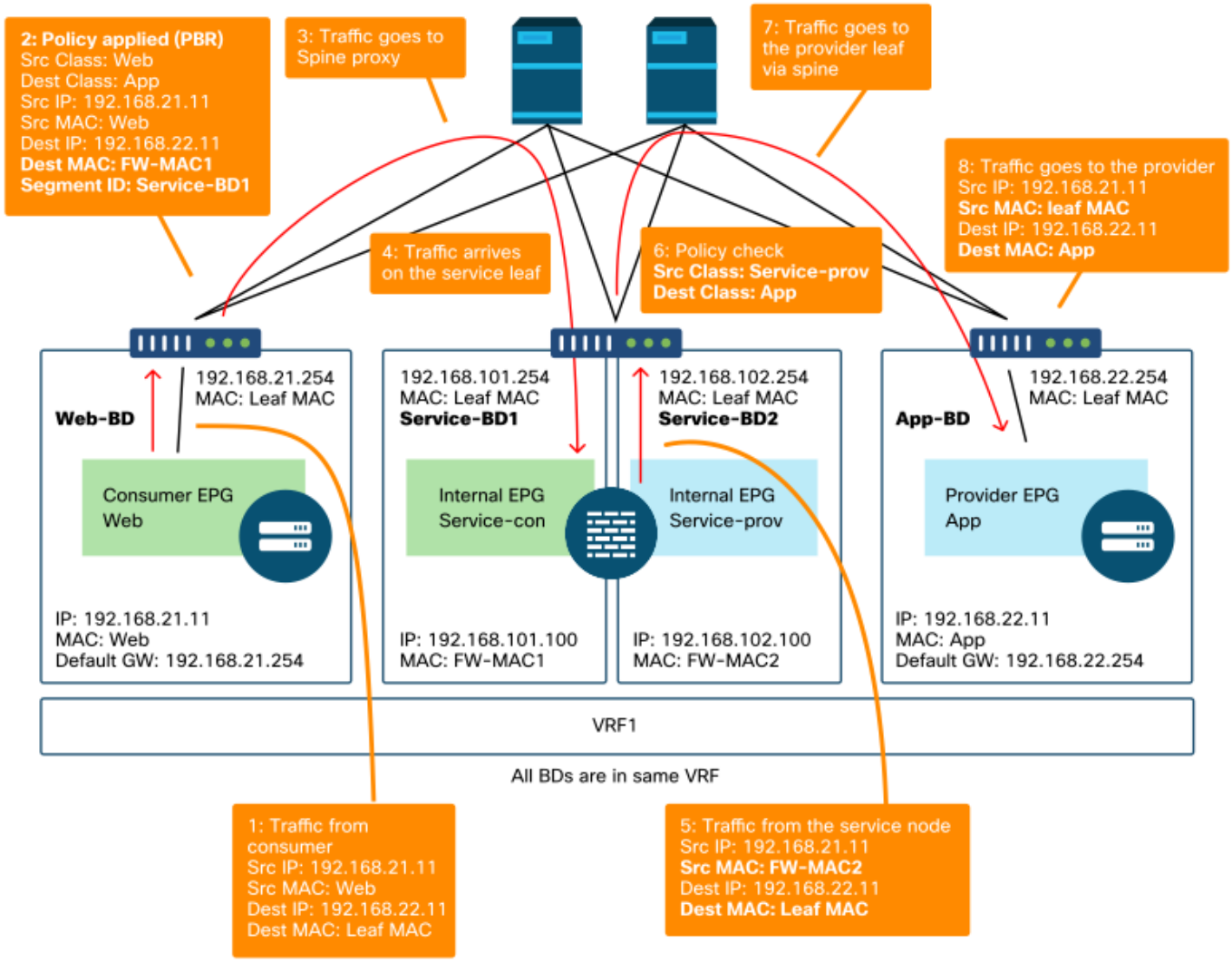
- يتم توصيل عقدة الخدمة بمنفذ إرتباط الرجوع الطرفي الصحيح. إن يكون الخدمة عقدة في مجال طبيعي، القوقة ساكن إستاتيكي نهاية مرم الحافظ داخل VLAN يحتاج أن يكون عينت في الجهاز منطقي.إذا كانت عقدة الخدمة في مجال VMM، فيرجى التحقق من أن مجال متصلة Service Graph من خلال إنشاؤها التي تم إنشاؤها المنافذ المجموعة وأن يعمل VMM بطريقة صحيحة بعقدة الخدمة VM.
- يتم توصيل منفذ الارتباط الطرفي إلى عقدة الخدمة أو مراقب الأجهزة الافتراضية الذي يتواجد به عقدة الخدمة VM.
- تحتوي عقدة الخدمة على شبكة VLAN وعنوان IP الصحيح.
- يتضمن المحول الوسيط بين قرة الخدمة وعقدة الخدمة تكوين VLAN الصحيح.

2. تحقق من مسارات حركة المرور المتوقعة

إذا توقفت حركة المرور من نهاية إلى نهاية عن العمل بمجرد تمكين PBR، حتى على الرغم من تعلم نقاط نهاية عقدة الخدمة في بنية واجهة التحكم في الوصول (ACI)، فإن الخطوة التالية استكشاف الأخطاء وإصلاحها هي التحقق من مسارات حركة المرور المتوقعة.

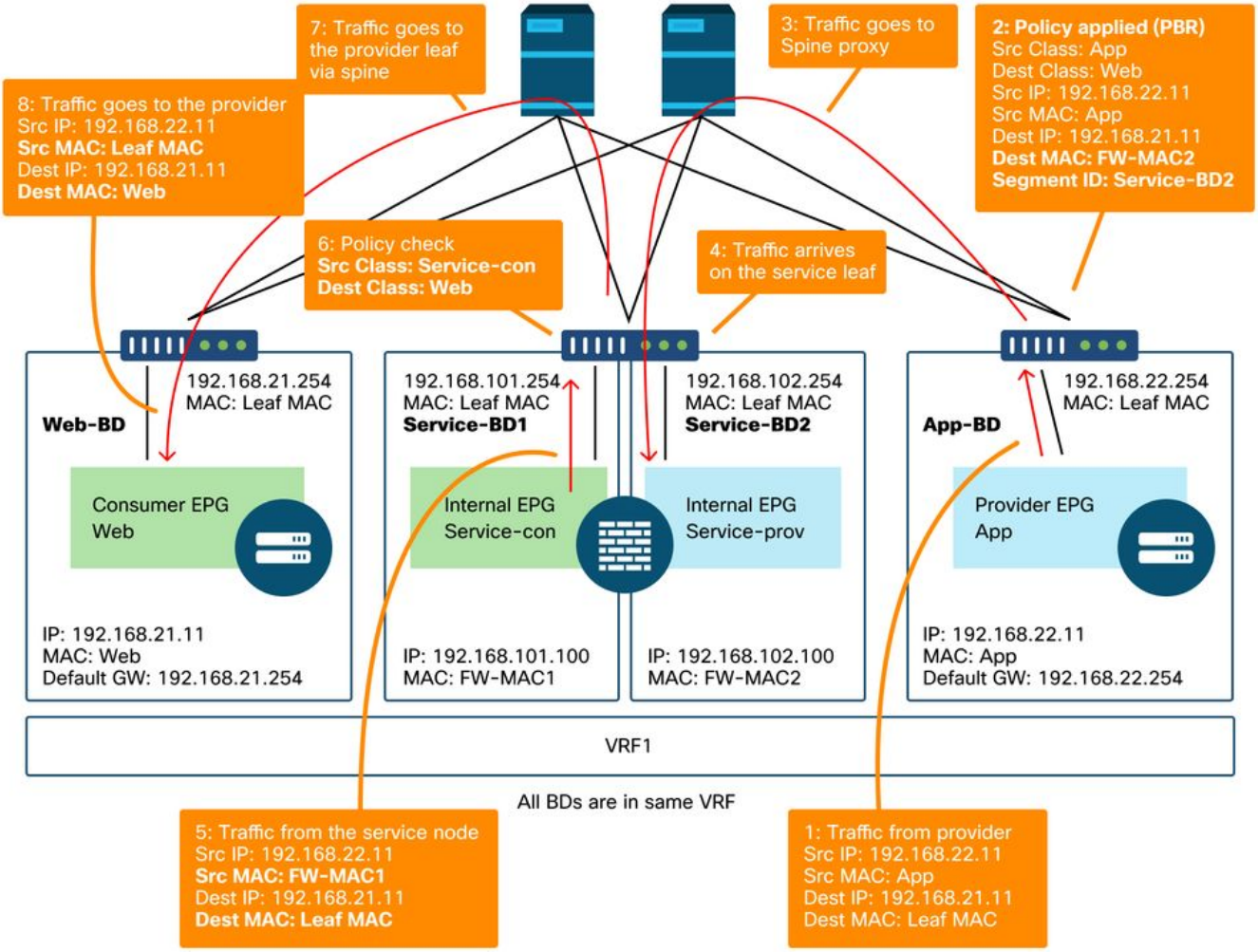
الأشكال 'مثال مسار إعادة توجيه PBR - من المستهلك إلى الموفر' و 'مثال مسار إعادة توجيه PBR - من الموفر إلى المستهلك' توضح مثال مسار إعادة توجيه لإدخال جدار الحماية PBR - من الموفر. وافتراض هو أن نقاط نهاية المستهلك ونقطة نهاية الموفر بين PBR باستخدام النهاية يجري تعلمها الآن على العقد القوقية.

مثال مسار إعادة توجيه PBR - من مستهلك إلى موزع



ملاحظة: بما أن MAC المصدر الذي يتغير إلى MAC الطرفي لقائمة التحكم في الوصول (ACI)، يجب ألا تستخدم عقدة PBR إعادة توجيه قائمة على MAC المصدر إذا لم تكن نقطة نهاية العميل وعقدة PBR في نفس BD

مثال مسار إعادة توجيه PBR - من المورد إلى المستهلك



ملاحظة: تجدر الإشارة إلى أنه يتم فرض سياسة إعادة توجيه المسار العكسي (PBR) على وقة المستهلك أو الموزد، وما تقوم به قائمة التحكم في الوصول الخاصة بالمنفذ (ACI) هو إعادة كتابة مكان الوجهة كما هو موضح في الأشكال 'مثال مسار إعادة توجيه المسار الخاص ببروتوكول الجسر (PBR) - من المستهلك إلى الموزد' و 'مثال مسار إعادة توجيه PBR - من الموفر إلى المستهلك'. الوصول إلى وجهة PBR يستخدم MAC دائما وكيل العمود الرئيسي، حتى إذا كانت نقطة نهاية المصدر وغاية PBR MAC تحت نفس الوقة.

على الرغم من أن الأشكال 'PBR مسار إعادة توجيه مثال - من مستهلك إلى موزد' و 'مثال مسار إعادة توجيه PBR - من موزد إلى مستهلك' تعرض مثال على الأماكن التي سيتم إعادة توجيه حركة مرور البيانات فيها، حيث يعتمد فرض السياسة على تكوين العقد وحالة تعلم نقطة النهاية. يلخص الجدول "حيث يتم فرض السياسة" مكان فرض السياسة موقع واحد ل ACI. حيث يتم فرض النهج في "متعدد المواقع" بشكل مختلف.

أين يتم فرض السياسة؟

سيناريو	وضع فرض التردد اللاسلكي VRF	مستهلك	موفر	تم فرض النهج على
Intra-VRF	مدخل/مخرج	EPG	EPG	إذا تم تعلم نقطة نهاية الوجهة: مدخل صفحة* إذا لم يتم تعلم نقطة نهاية الوجهة: مخرج وقة
	مدخل	EPG	L3Out	وقة مستهلكة (وقة غير حدودية)

			EPG	
	مدخل	L3Out EPG	EPG	ورقة المورف (ورقة غير حدود)
	مخرج	EPG	L3Out EPG	ورقة الحدود -> حركة مرور الأوراق غير الحدودية
	مخرج	L3Out EPG	EPG	إذا· تم تعلم نقطة نهاية الوجهة: ورقة الحدود إذا· لم يتم تعلم نقطة نهاية الوجهة: ورقة غير حدود حركة مرور أوراق الحدود غير الحدودية ورقة الحدود.
	مدخل/مخرج	L3Out EPG	L3Out EPG	ورقة المدخل*
	مدخل/مخرج	EPG	EPG	ورقة إستهلاكية
	مدخل/مخرج	EPG	L3Out EPG	ورقة مستهلكة (ورقة ال حدود لها)
Inter-VRF	مدخل/مخرج	L3Out EPG	EPG	ورقة المدخل*
	مدخل/مخرج	L3Out EPG	L3Out EPG	ورقة المدخل*

*يتم تطبيق تطبيق النهج على أول ورقة يتم الوصول إليها بواسطة الحزمة.

وهذه أمثلة:

- إذا حاولت نقطة نهاية خارجية في L3Out EPG في VRF1 الوصول إلى نقطة نهاية في Web EPG في VRF1 وتم تكوين VRF1 لرفض الدخول، تتم إعادة توجيه حركة مرور البيانات بواسطة الورقة حيث توجد نقطة النهاية في Web EPG، بغض النظر عن إتجاه العقد.
- إذا حاولت نقطة نهاية في Customer Web EPG في VRF1 الوصول إلى نقطة نهاية في Provider App EPG في VRF1، وتم تعلم نقاط النهاية على عقد ورقة المستهلك والمزود، فإن حركة مرور البيانات بواسطة ورقة المدخل يتم إعادة توجيهها.
- إذا حاولت نقطة نهاية في Customer Web EPG في VRF1 الوصول إلى نقطة نهاية في Provider App EPG في VRF2، تتم إعادة توجيه حركة مرور البيانات بواسطة ورقة المستهلك حيث توجد نقطة نهاية المستهلك، بغض النظر عن رفض VRF.

3. التحقق من إعادة توجيه حركة مرور البيانات إلى عقدة الخدمة

إذا كانت حركة المرور تصل إلى عقد المحول والتحقق من قرار إعادة التوجيه على عقد المحول، يمكن إستخدام ELAM للتحقق مما إذا كانت حركة المرور تصل إلى عقد المحول وبمجرد مسح مسار إعادة التوجيه المتوقع. يرجى الرجوع إلى القسم "أدوات" في الفصل "إعادة التوجيه بين البنى" للحصول على تعليمات حول كيفية إستخدام ELAM.

على سبيل المثال، لتتبع تدفق حركة المرور في الشكل 'مثال مسار إعادة توجيه PBR - من مستهلك إلى مزود'، يمكن التقاط هذه للتأكد مما إذا كان قد تم إعادة توجيه حركة مرور المستهلك إلى المورف.

- منفذ التنزيل على ورقة المستهلك للتحقق من 1 و 2 (وصول حركة المرور إلى ورقة المستهلك وفرض PBR).
- منفذ بنيوي على عقد العمود الفقري للتحقق من 3 (تنتقل حركة المرور إلى وكيل العمود الفقري).

- منفذ البنية على ورقة الخدمة للتحقق من 4 (وصول حركة المرور إلى ورقة الخدمة).

بعد ذلك، يمكن التقاط هذه البيانات لتأكيد ما إذا كانت حركة المرور التي ترجع من عقدة الخدمة تنتقل إلى الموفر.

- قم بتنزيل المنفذ على ورقة الخدمة للتحقق من 5 و 6 (حركة المرور تعود من عقدة الخدمة ويتم السماح بها).
- منفذ بنيوي على عقد العمود الفقري للتحقق من 7 (تنتقل حركة المرور إلى ورقة الموفر عبر العمود الفقري).
- منفذ البنية على ورقة الموفر للتحقق من 8 (تصل حركة المرور إلى ورقة الخدمة وتذهب إلى نقطة نهاية الموفر).

ملاحظة: إذا كانت عقدة "المستهلك" و"الخدمة" تضمن نفس الورقة، فحدد واجهة MAC المصدر وأ IP المصدر/الوجهة لأخذ ELAM للتحقق من 1 أو 5 في الشكل "مثال مسار إعادة التوجيه PBR - من المستهلك إلى الموفر" تحديدا لأن كل من هذه الأمور يستخدم IP المصدر نفسه والوجهة IP.

إذا تم إعادة توجيه حركة مرور العميل إلى الموفر إلى عقدة الخدمة ولكنها لا تعود إلى ورقة الخدمة، فيرجى التحقق مما يلي نظرا لأنها أخطاء شائعة:

- يصل جدول توجيه عقدة الخدمة إلى الشبكة الفرعية للموفر.
- يسمح نهج أمان عقدة الخدمة مثل قائمة التحكم في الوصول (ACL) بحركة المرور.

إذا تمت إعادة توجيه حركة المرور ووصلت إلى الموفر، فالرجاء التحقق من مسار حركة المرور العائدة من الموفر إلى المستهلك بطريقة مماثلة.

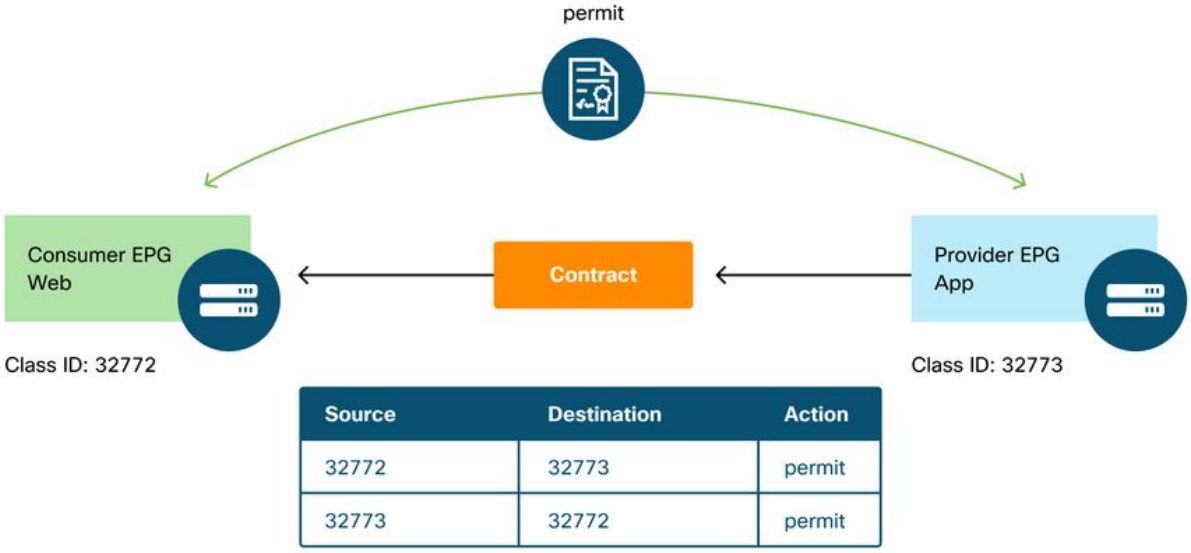
4. تحقق من السياسات المبرمجة على العقد الطرفية

إذا لم تتم إعادة توجيه حركة المرور أو إعادة توجيهها وقف لذلك، فإن الخطوة التالية هي التحقق من السياسات التي تمت برمجتها على العقد الطرفية. وضح هذا القسم قاعدة تقسيم المنطقة و contract_parser كمثال. لمزيد من التفاصيل حول كيفية التحقق من قواعد تقسيم المناطق، الرجاء الرجوع إلى القسم "سياسات الأمان" في الفصل "أدوات".

ملاحظة: تتم برمجة السياسات استنادا إلى حالة نشر EPG على الورقة. يستخدم الأمر show في هذا القسم الورقة التي تحتوي على EPG للمستهلك و EPG للموفر و EPG لعقدة الخدمة.

استخدام الأمر 'show zoning-rule'

يصف الشكل والإخراج "show zoning-rule" أدناه قواعد تقسيم المناطق قبل نشر الرسم البياني للخدمة.

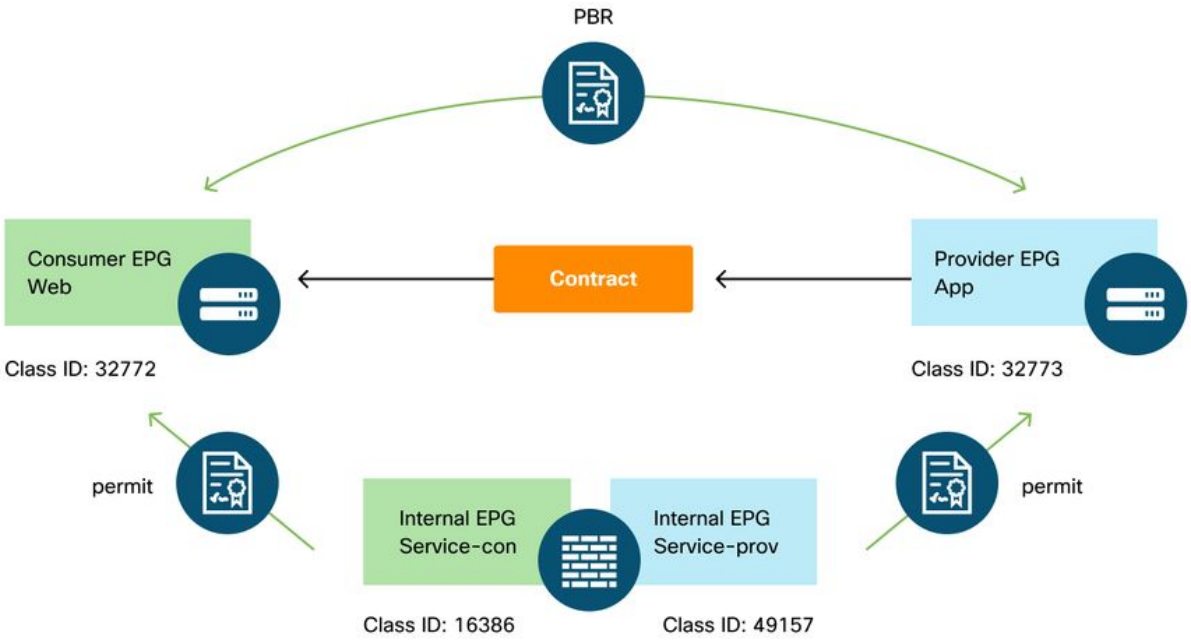


يمكن العثور على معرف نطاق VRF في 'Tenant > Networking > VRF'.

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

بمجرد نشر الرسم البياني للخدمة، يتم إنشاء EPGs لعقدة الخدمة وتحديث السياسات لإعادة توجيه حركة مرور البيانات بين المستهلك والمزود EPG. يصف الشكل أدناه والإخراج "show zoning-rule" أدناه قواعد تقسيم المناطق بعد نشر الرسم البياني للخدمة. في هذا المثال، تتم إعادة توجيه حركة مرور البيانات من pcTag 32772 (Web) إلى pcTag 32773 (App) إلى 'destgrp-27' (جانب المستهلك من عقدة الخدمة) وإعادة توجيه حركة مرور البيانات من pcTag 32773 (App) إلى pcTag 32772 (Web) إلى 'destgrp-28' (جانب المورد لعقدة الخدمة).

قواعد تقسيم المناطق بعد نشر الرسم البياني للخدمة



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

يمكن العثور على معلومات الوجهة لكل مصدر باستخدام الأمر 'show service redir info'.

```
Pod1-Leaf1# show service redir info
========================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-
Dest |  TRA: Tracking  | RES: Resiliency
========================================================================================
List of Dest Groups
```

```
GrpID Name            destination                                  HG-name         BAC
operSt     operStQual      TL   TH   HP   TRAC RES
===== ====            ===========                                  ==============   ===
=======    ============    ===  ===  ===  ===  ===
28    destgrp-28      dest-[192.168.102.100]-[vxlan-2752513]      Not attached      N
enabled    no-oper-grp     0    0    sym  no   no
27    destgrp-27      dest-[192.168.101.100]-[vxlan-2752513]      Not attached      N
enabled    no-oper-grp     0    0    sym  no   no

List of destinations
Name                                          bdVnid           vMac
vrf         operSt     operStQual      HG-name
====                                          ======           ====
====        =====      =========       =======
dest-[192.168.102.100]-[vxlan-2752513]        vxlan-16023499     00:50:56:AF:1C:44
Prod:VRF1   enabled    no-oper-dest    Not attached
dest-[192.168.101.100]-[vxlan-2752513]        vxlan-16121792     00:50:56:AF:3C:60
Prod:VRF1   enabled    no-oper-dest    Not attached
...
```

إذا تم برمجة قواعد تقسيم المناطق وفقا لذلك، ولكن لا يتم إعادة توجيه حركة المرور أو إعادة توجيهها وفقا لذلك، فيرجى التحقق مما يلي لأنها أخطاء شائعة:

- تحقق مما إذا تم حل معرف فئة المصدر أو الوجهة كما هو متوقع باستخدام ELAM. إذا لم تكن هناك مساحة، فيرجى التحقق من معرف الفئة الخطأ ومعايير اشتقاق EPG مثل المسار والتشبيك لشبكة VLAN.
- على الرغم من أنه يتم حل معرفات فئات المصدر والوجهة وفقا لذلك، ويتم تطبيق سياسة PBR ولكن لا تصل حركة مرور البيانات إلى عقدة PBR، الرجاء التحقق من IP و MAC و VRF من الأداة المساعدة في إجراء المرجع ('show service redir info') صحيحة.

وبشكل افتراضي، لا تتم برمجة قواعد السماح ل EPG للمستهلك إلى عقدة خدمة (جانب المستهلك)، و EPG للموفر إلى عقدة خدمة (جانب الموفر) إذا تم تمكين PBR. وبالتالي، لا يمكن لنقطة نهاية العميل أو الموفر الاتصال مباشرة بعقدة الخدمة بشكل افتراضي. للسماح بحركة المرور هذه، يلزم تمكين خيار الاتصال المباشر. يتم شرح حالة الاستخدام في القسم أمثلة تدفق حركة المرور الأخرى".

إستخدام contract_parser

يمكن أن تساعد أداة contract_parser أيضا في التحقق من السياسات. C-consumer هو جانب المستهلك لعقدة الخدمة و C-provider هو جانب الموفر لعقدة الخدمة.

```
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]
```

...

أمثلة أخرى لتدفق حركة المرور

يسرد هذا القسم أمثلة أخرى لتدفق حركة المرور الشائعة لتحديد التدفقات المطلوبة لاستكشاف الأخطاء وإصلاحها. لخطوات استكشاف الأخطاء وإصلاحها، يرجى الرجوع إلى الفصل السابق في هذا القسم.

1. موازن التحميل بدون SNAT: في هذا المثال، لدى Customer EPG Web والموزود EPG App عقد مع Load Balanced Service Graph. نقاط النهاية في App EPG هي خوادم حقيقية موزود لموازن التحميل PBR تمكين تم.التحميل موازن في المهمة الشخصية بالنسبة مقترن الخدمة إلى إتجاه حركة مرور المستهلك.
2. موازن التحميل وجدار الحماية بدون SNAT: في هذا المثال، لدى Customer EPG Web والموزود EPG App عقد مع جدار حماية و Load Balanced Service Graph. نقاط النهاية في App EPG هي خوادم حقيقية مقترنة بالشخصية المهمة في موازن التحميل.تم تمكين PBR لموازن التحميل موزود الخدمة إلى إتجاه.تم تمكين PBR لكلا اتجاهات الحماية إلى جدار حركة مرور المستهلك.
3. الخدمة المشتركة (عقد بين شبكات VRF): في هذا المثال، لدى Customer EPG Web وتطبيق EPG للموفر عقد مع Firewall Service Graph. يوجد كل من EPG وتطبيق EPG في شبكات VRF مختلفة.تم تمكين PBR إلى جدار الحماية لكلا الاتجاهات.جدار الحماية موجود بين VRFs.

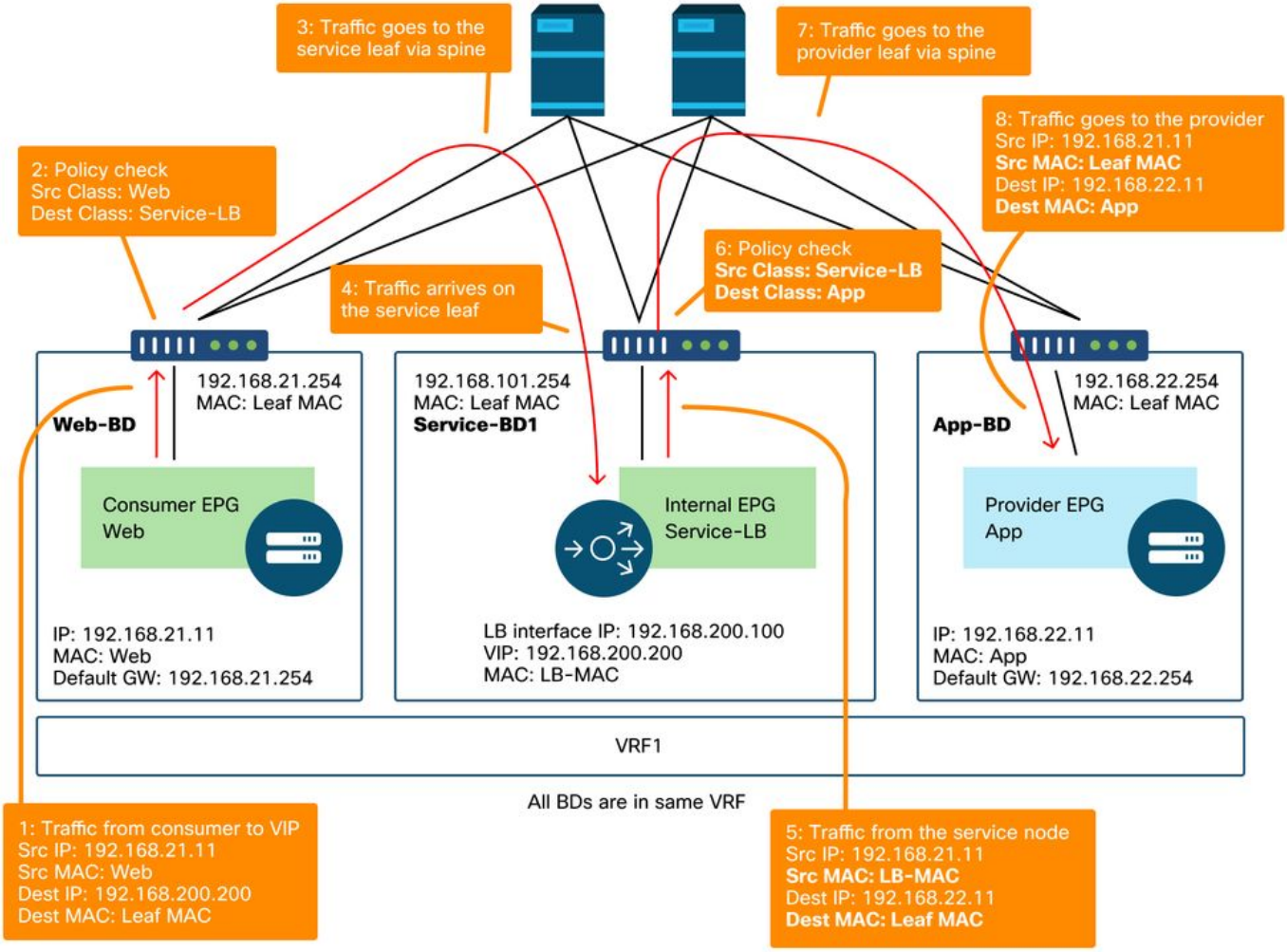
1. موازن التحميل بدون SNAT

يمكن نشر PBR على هيئة PBR ثنائي الإتجاه أو PBR أحادي الإتجاه. إحدى حالات الاستخدام ل PBR أحادي الإتجاه هي تكامل موازن التحميل بدون ترجمة عناوين الشبكة المصدر (NAT). إذا قام موازن التحميل بتنفيذ NAT للمصدر، فلا يلزم وجود PBR.

مثال على رسم حركة المرور

يوضح الشكل التالي مثال لتدفق حركة مرور واردة من موقع EPG الخاص بالمستهلك إلى تطبيق EPG الخاص بالموزود مع إتصالين: أحدهما من نقطة نهاية في موقع EPG الخاص بالمستهلك إلى VIP الخاص بموازن التحميل، والآخر من موازن التحميل إلى نقطة نهاية في تطبيق EPG الخاص بالموزود. لأن حركة المرور الواردة موجهة إلى الشخصية المهمة، فستصل حركة المرور إلى موازن التحميل دون PBR إذا كانت الشخصية المهمة يمكن الوصول إليها. يقوم موازن التحميل بتغيير IP الوجهة إلى إحدى نقاط النهاية في تطبيق EPG المرتبط بالشخصية المهمة ولكنه لا يترجم IP المصدر. وفقا لذلك، تنتقل حركة المرور إلى نقطة نهاية الموفر.

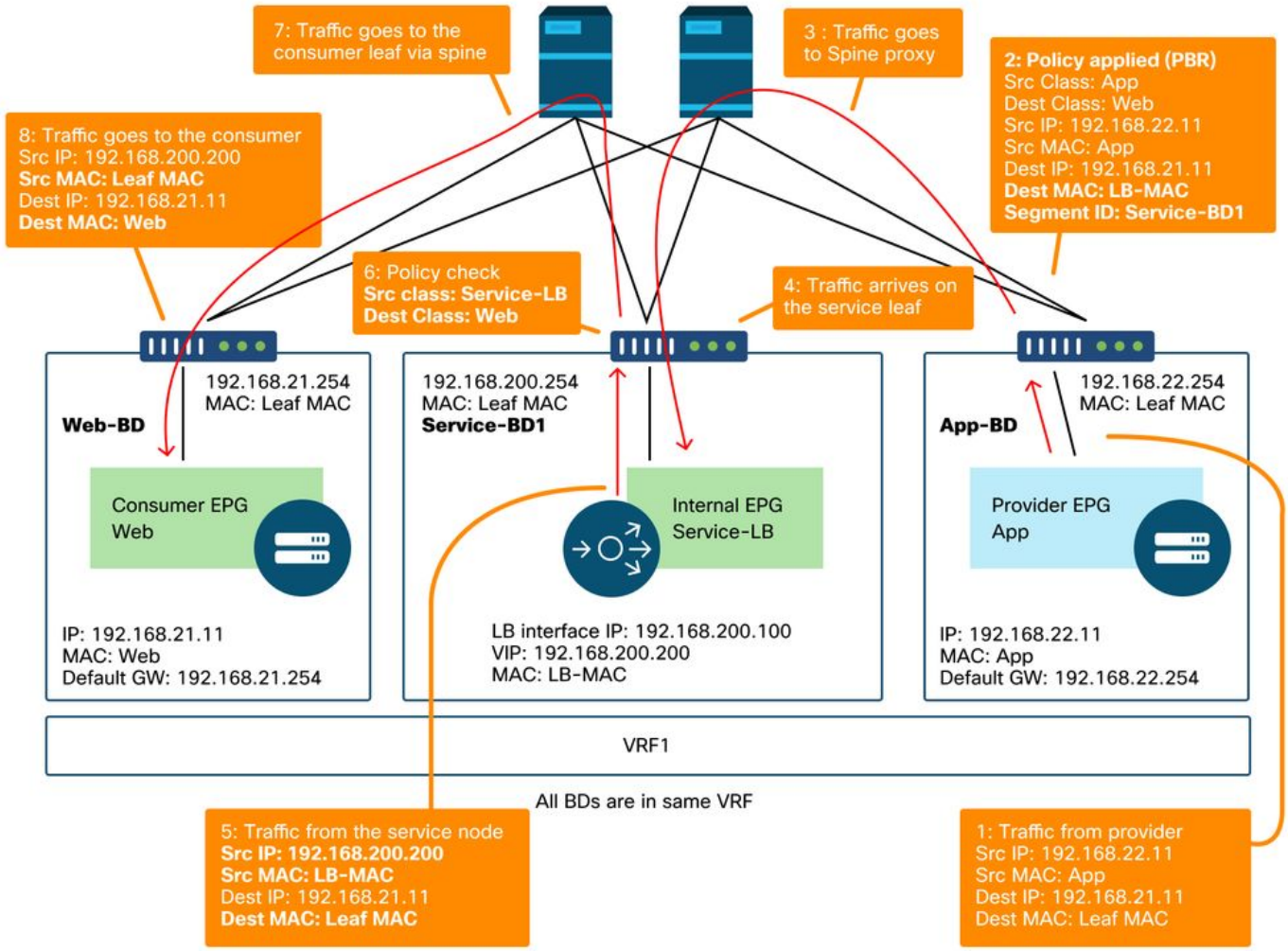
موازن الأحمال بدون مثال رسم إعادة توجيه SNAT — مستهلك لشخصية مهمة وموازن حمل موزود بدون PBR



يوضح الشكل أدناه تدفق حركة مرور الإرجاع من تطبيق EPG للموفر إلى موقع EPG للمستهلك عليه وبه. لأن حركة المرور العائدة موجهة إلى المصدر الأصلي IP، PBR مطلوب لعمل حركة المرور العائدة للعودة إلى موازن التحميل. وإلا فإن نقطة نهاية العميل تستلم حركة مرور البيانات حيث يكون المصدر IP هو نقطة نهاية الموفر بدلا من الشخصية المهمة. سيتم إسقاط حركة المرور هذه لأن نقطة نهاية العميل لم تقم بدء حركة المرور إلى نقطة نهاية الموفر حتى إذا قامت الشبكة الوسيطة مثل بنية واجهة التحكم في الوصول (ACI) بإعادة توجيه الحزمة إلى نقطة نهاية المستهلك.

بعد إعادة توجيه حركة المرور من نقطة نهاية الموفر إلى نقطة نهاية العميل إلى موازن التحميل، يقوم موازن التحميل بتغيير IP المصدر إلى الشخصية المهمة. بعد ذلك، ترجع حركة المرور من موازن التحميل وترجع حركة المرور إلى نقطة نهاية المستهلك.

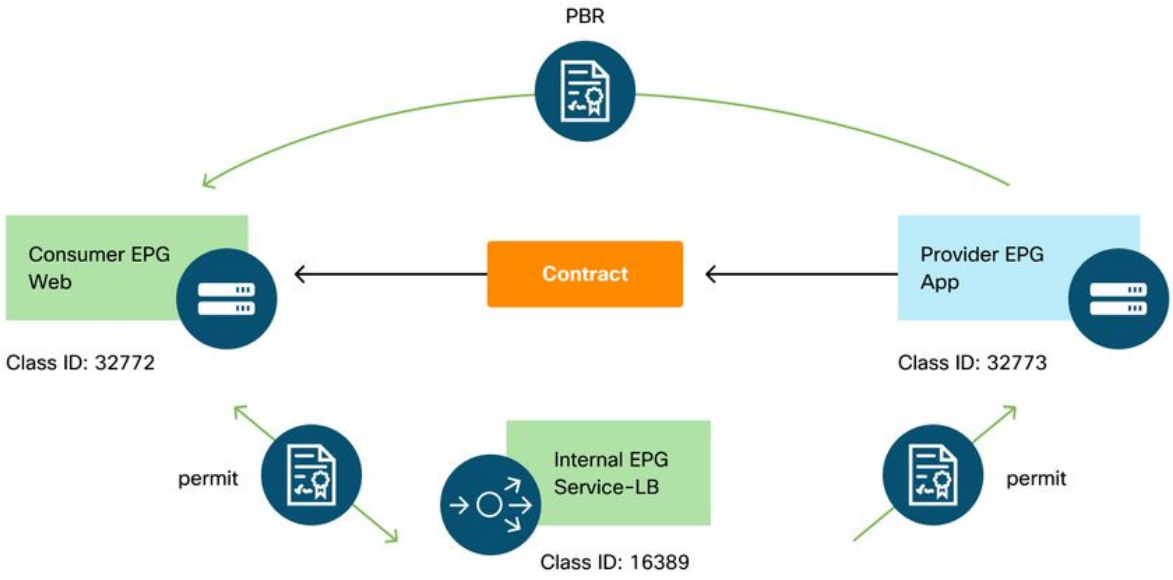
موازن التحميل بدون مثال مسار إعادة توجيه SNAT - موزد للمستهلك باستخدام PBR



السياسات المبرمجة على العقد الطرفية.

يصف الشكل أدناه والإخراج "show zoning-rule" أدناه قواعد تقسيم المناطق بعد نشر الرسم البياني للخدمة. في هذا المثال، يتم السماح بحركة المرور من pcTag 32772 (Web) إلى pcTag 16389 (Service-LB)، وإعادة توجيه حركة المرور من pcTag 16389 (Service-LB) إلى pcTag 32773 (App)، وحركة المرور من pcTag 32773 (App) إلى pcTag 32772 (Web) إلى 'Destgrp-31' (موازن التحميل).

قواعد تقسيم المناطق بعد نشر رسم الخدمة - موازن التحميل بدون SNAT

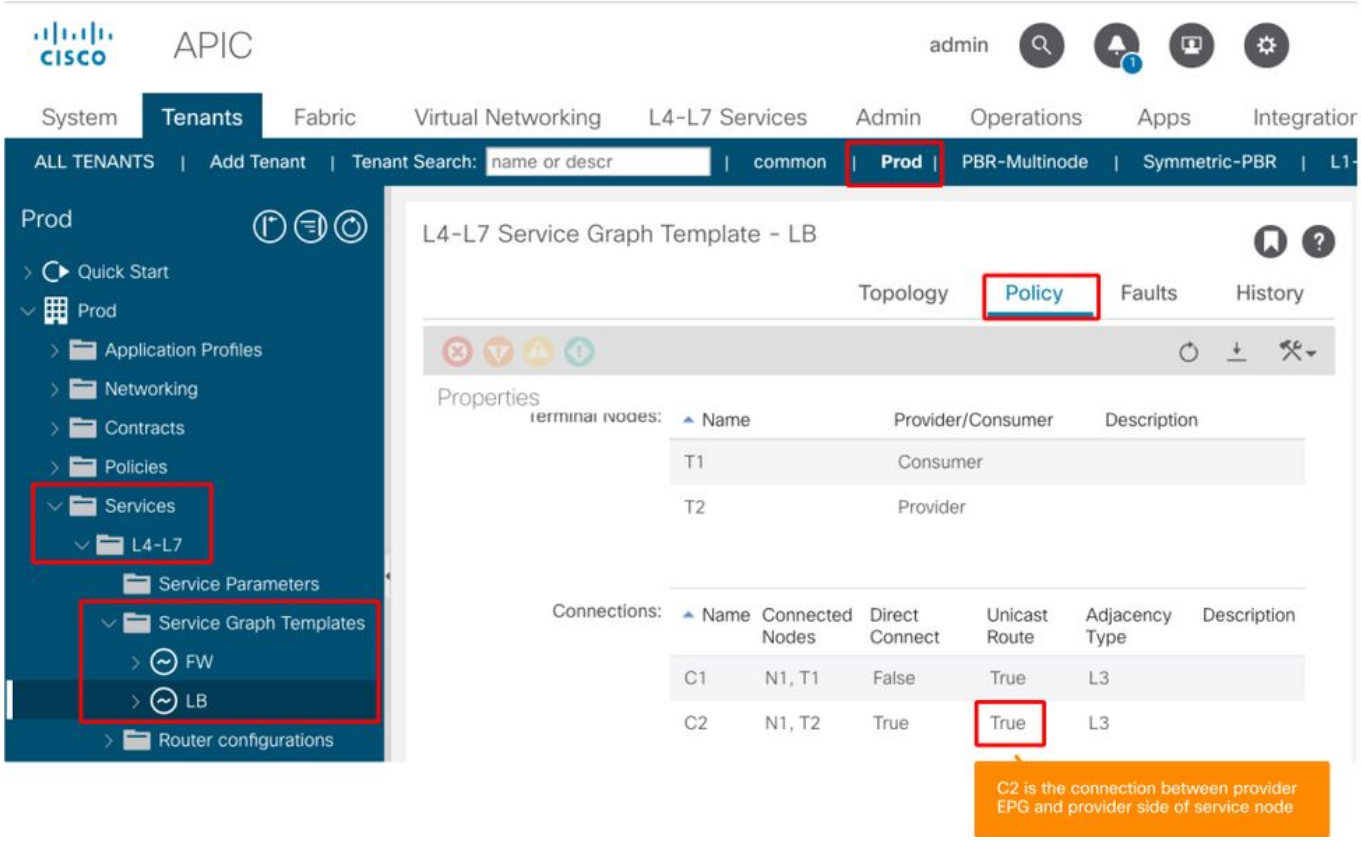


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
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)     |
...
```

بشكل افتراضي، ال تتم برمجة قاعدة السماح للموفر EPG (pcTag 32773) إلى Service-LB (pcTag 16389). للسماح بالاتصال ثنائي الإتجاه فيما بينهم للتحقق من الصحة من موازن التحميل إلى نقاط نهاية الموفر، يجب تعيين خيار الاتصال المباشر على الاتصال إلى "صواب". الموقع هو 'مستأجر > L4-L7 > قوالب الرسم البياني للخدمة > سياسة'. القيمة الافتراضية هي خطأ.

تعيين خيار الاتصال المباشر



كما يضيف قاعدة تصريح للمورد EPG(32773) إلى Service-LB(16389) كما هو موضح أدناه.

```
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. مثال تدفق حركة المرور - موازن التحميل وجدار الحماية دون SNAT

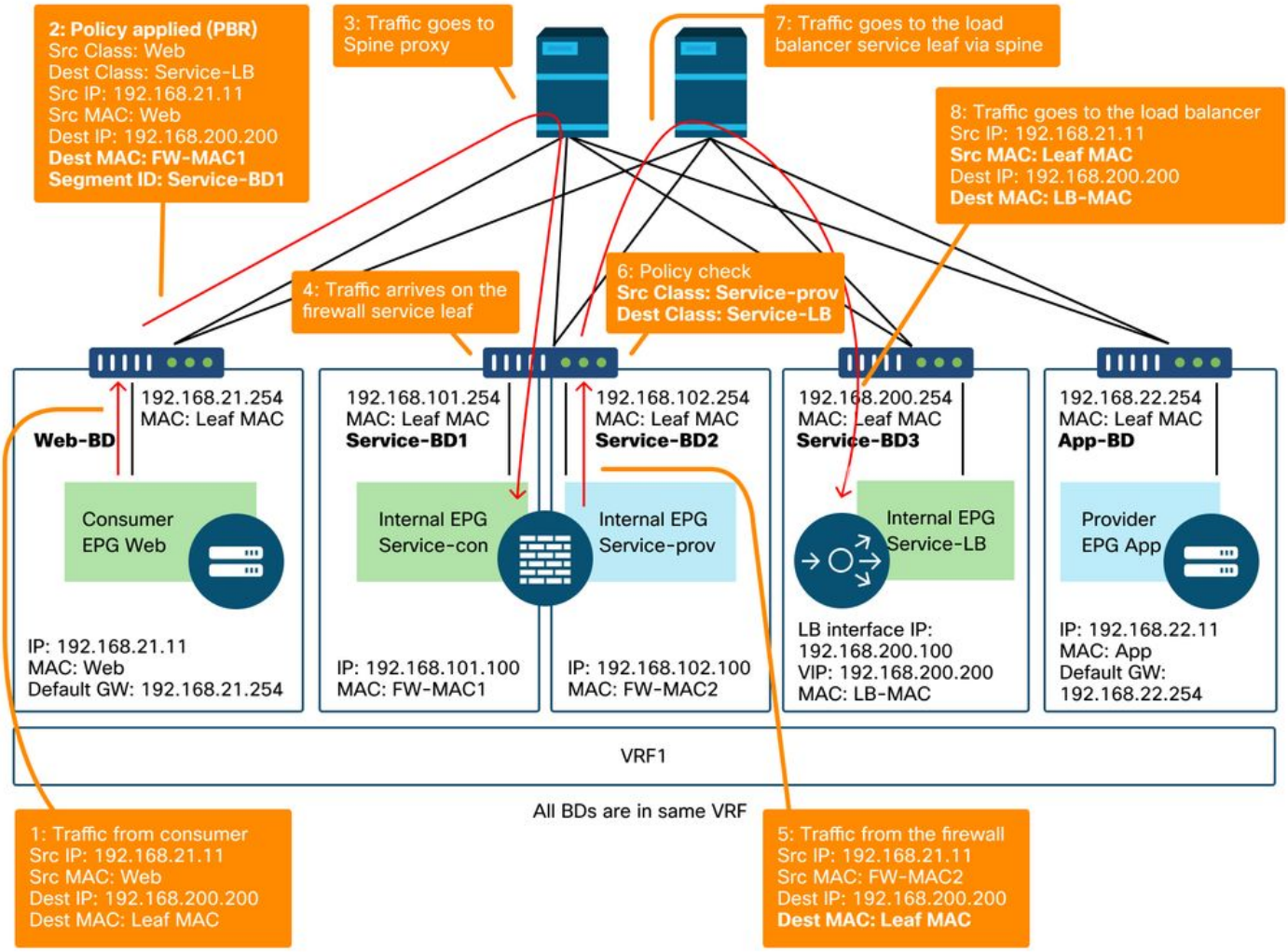
يمكن نشر PBR وظائف خدمة متعددة في الرسم البياني للخدمة مثل جدار الحماية كالعقدة الأولى وموازن التحميل كعقدة ثانية.

مثال على مسار حركة المرور

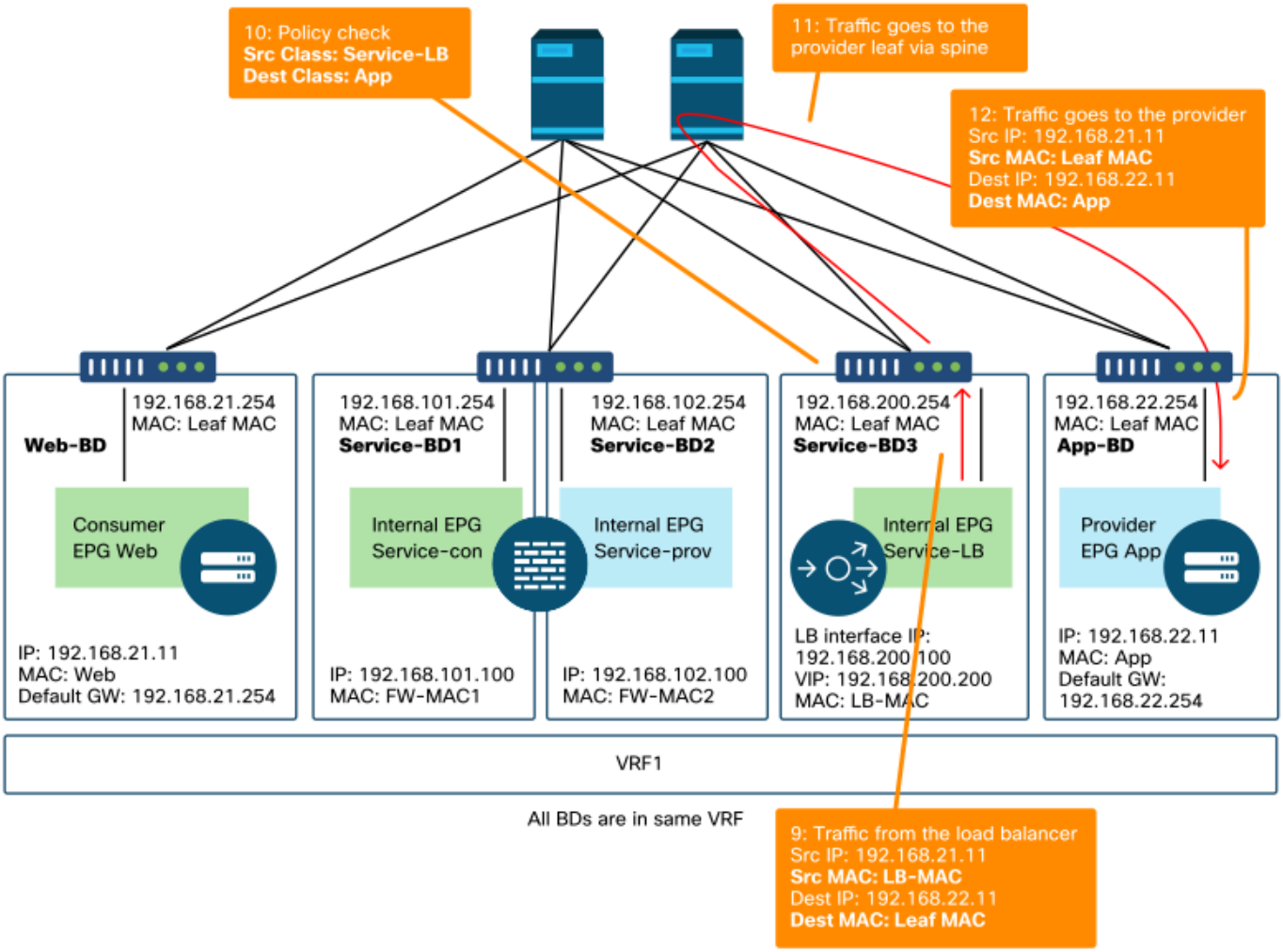
يوضح الشكل التالي مثالا لتدفق حركة مرور قادم من موقع EPG الخاص بالمستهلك إلى تطبيق EPG الخاص بالمزود مع إتصالين: أحدهما من نقطة نهاية في موقع EPG الخاص بالمستهلك إلى VIP الخاص بموازن التحميل عبر جدار الحماية والآخر من موازن التحميل إلى

نقطة نهاية في تطبيق EPG الخاص بالمزود. تتم إعادة توجيه حركة المرور الواردة الموجهة إلى الشخصية المهمة إلى جدار الحماية ثم تنتقل إلى موازن التحميل دون PBR. يقوم موازن التحميل بتغيير IP الوجهة إلى إحدى نقاط النهاية في EPG التطبيق المرتبط بالشخصية المهمة ولكنه لا يترجم IP المصدر. بعد ذلك، تنتقل حركة المرور إلى نقطة نهاية الموفر.

موازن الأحمال وجدار الحماية بدون مثال مسار إعادة توجيه SNAT - المستهلك للشخصيات المهمة وموازن الأحمال للموفر



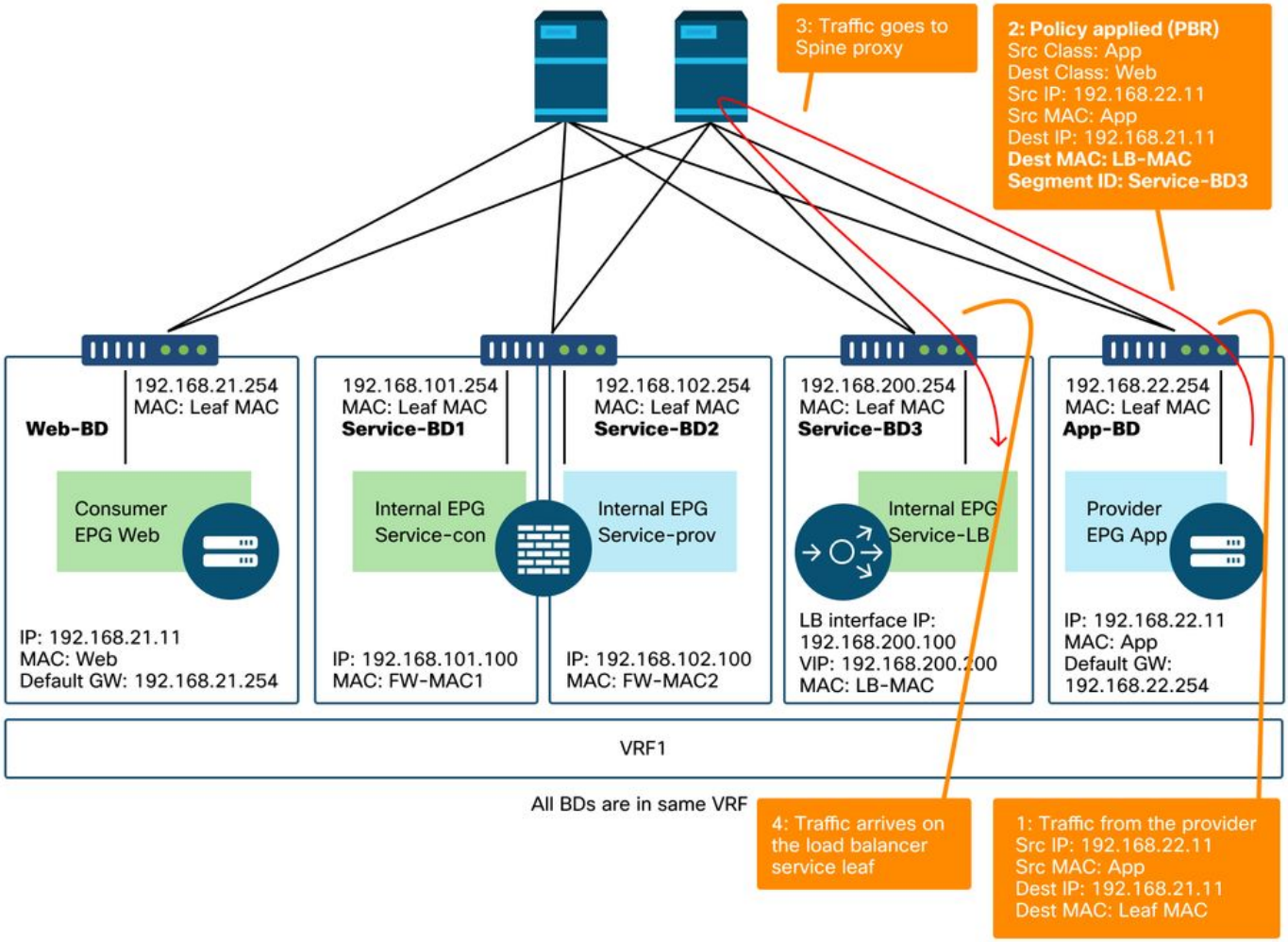
موازن الأحمال وجدار الحماية بدون مثال مسار إعادة توجيه SNAT - المستهلك للشخصيات المهمة وموازن الأحمال للموفر (تابع)

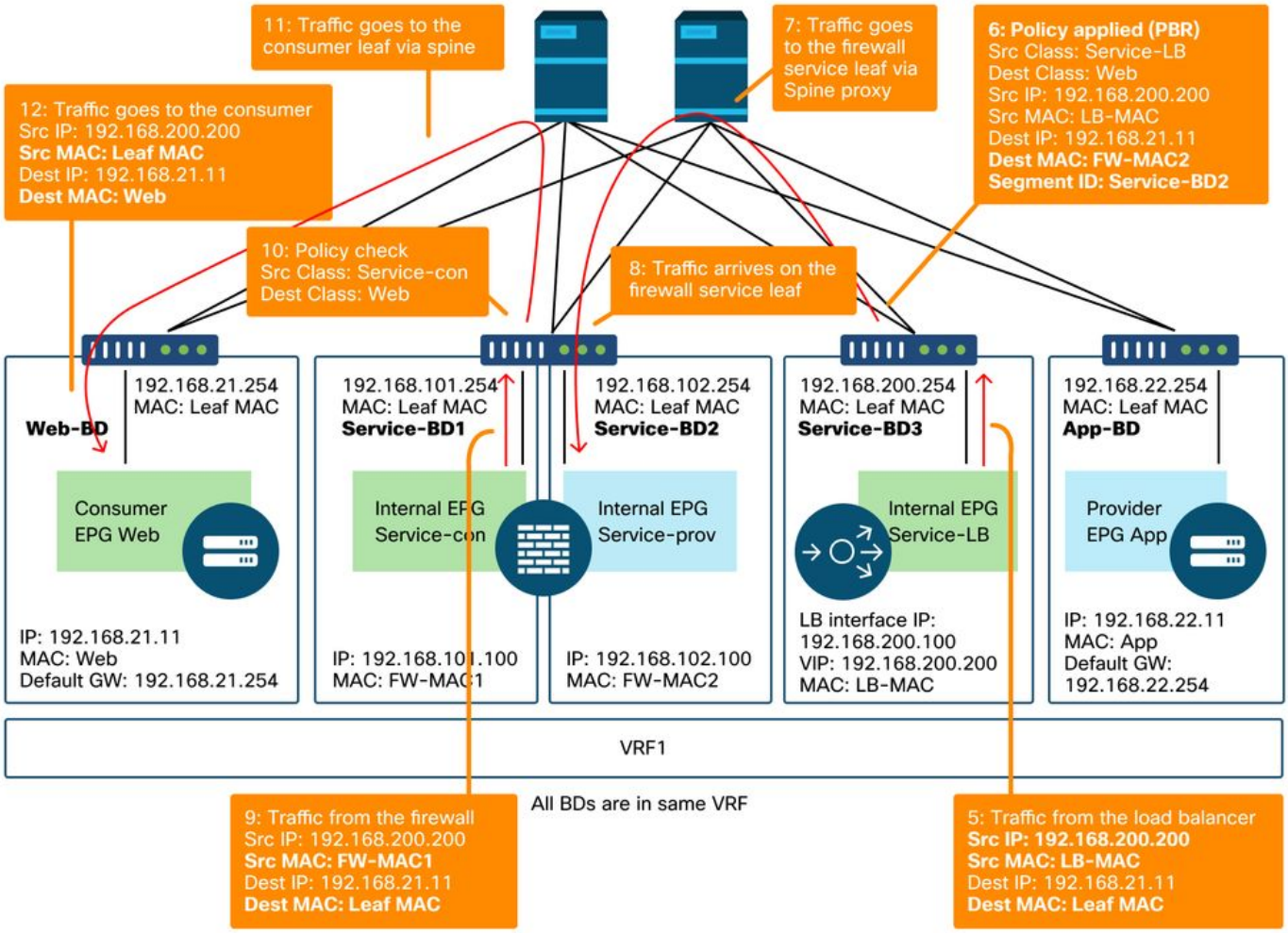


يوضح الشكل أدناه تدفق حركة مرور الإرجاع من تطبيق EPG للموفر إلى موقع EPG للمستهلك على وبب. لأن حركة المرور العائدة موجهة إلى المصدر الأصلي IP، PBR مطلوب لجعل حركة المرور العائدة تعود إلى موازن التحميل.

بعد إعادة توجيه حركة المرور من نقطة نهاية الموفر إلى نقطة نهاية العميل إلى موازن التحميل، يقوم موازن التحميل بتغيير IP المصدر إلى الشخصية المهمة. ترجع حركة المرور من موازن التحميل وتتم إعادة توجيهها إلى جدار الحماية. بعد ذلك، تعود حركة المرور من جدار الحماية وترجع إلى نقطة نهاية المستهلك.

جدار الحماية وموازن التحميل بدون مثال مسار إعادة توجيه SNAT - موفر للمستهلك

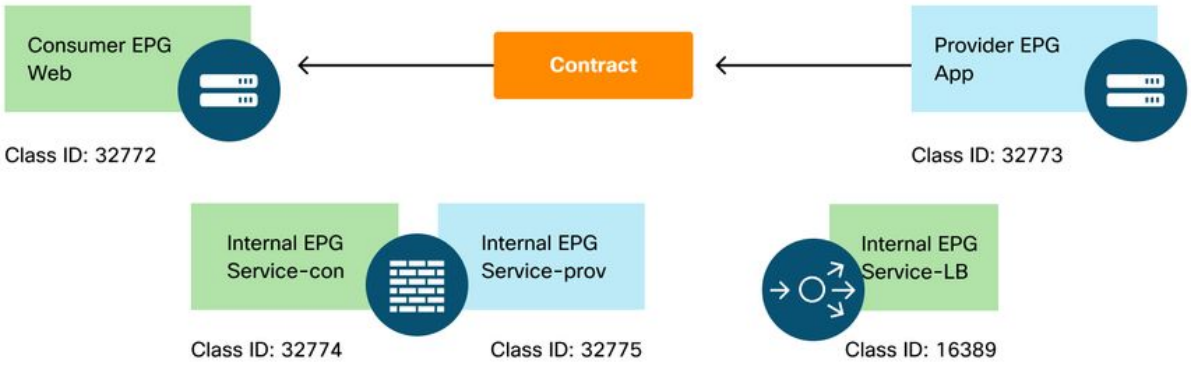

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



السياسات المبرمجة على العقد الطرفية

يصف الشكل أدناه والإخراج "show zoning-rule" الموضح أدناه قواعد تقسيم المناطق بعد نشر الرسم البياني للخدمة. في هذا المثال، تتم إعادة توجيه حركة المرور من pcTag 32772 (Web) إلى pcTag 16389 (Service-LB) إلى 'destgrp-32' (جانب المستهلك من جدار الحماية)، وحركة المرور من pcTag 32773 (App) إلى pcTag 32772 (Web) إلى 'destgrp-33' (موازن التحميل)، وحركة المرور من pcTag 16389 (Service-LB) إلى pcTag 3272 (rea) موجه إلى 'destgrp-34' (جانب المورد لجدار الحماية).

قواعد تقسيم المناطق بعد نشر الرسم البياني للخدمة - موازن التحميل وجدار الحماية بدون 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)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

في المثال أعلاه، يتم تعيين خيار الاتصال المباشر على "صواب" على الاتصال بين جانب الموفر لموازن التحميل و EPG للموفر. يجب تمكينها للتحقق من الصحة من موازن التحميل إلى نقاط نهاية الموفر. الموقع هو 'Tenant > L4-L7 > قوالب الرسم البياني للخدمة >Policy'. يرجى الرجوع إلى شكل "تعيين خيار الاتصال المباشر".

3. الخدمة المشتركة (عقد بين شبكات VRF)

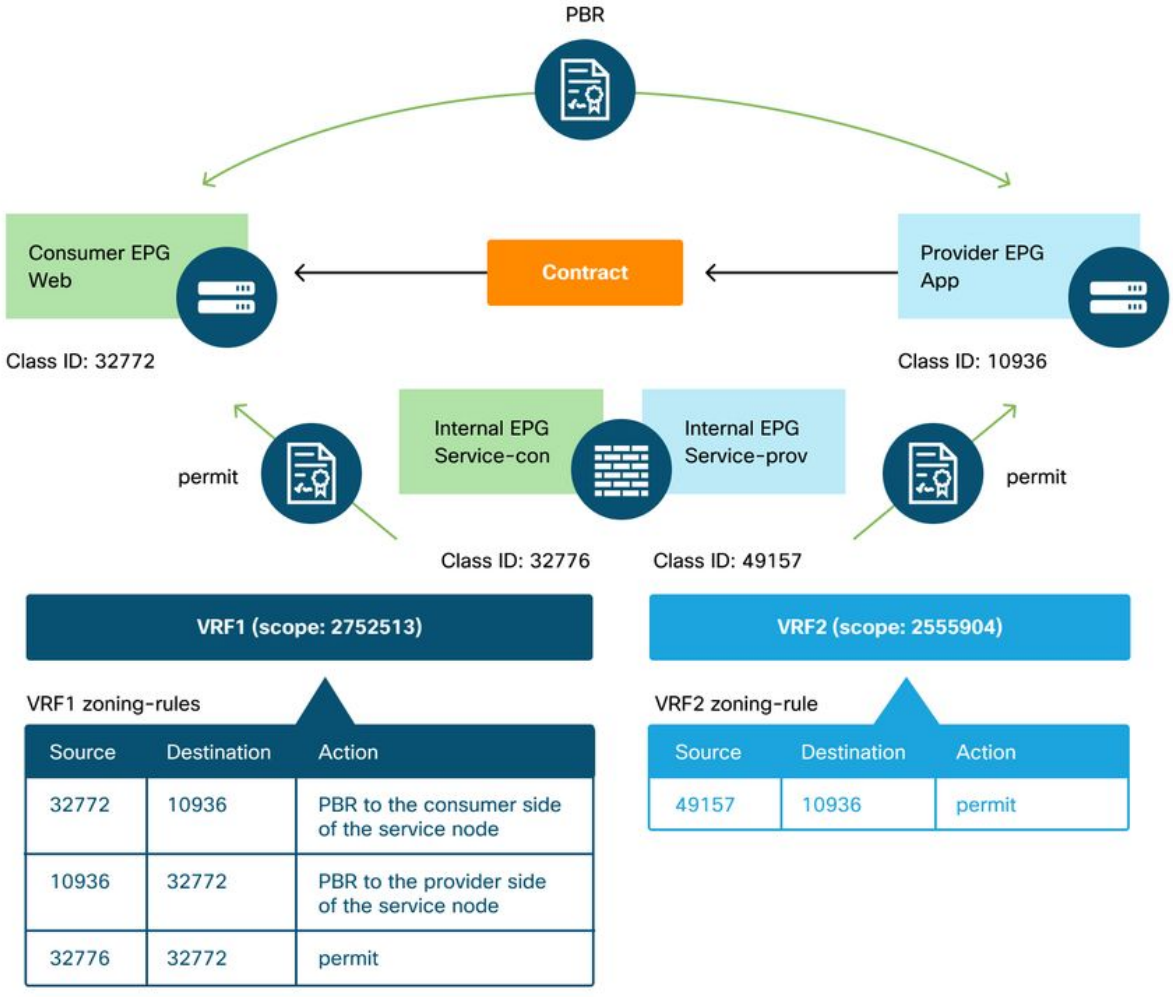
يمكن تمكين PBR في عقد بين شبكات VRF. يشرح هذا القسم كيفية برمجة قواعد تقسيم المناطق في حالة EPG إلى عقد EPG بين VRF.

السياسات المبرمجة على العقد الطرفية

في حالة عقد EPG إلى EPG بين VRF، يتم فرض السياسة دائما في VRF الخاص بالمستهلك. وعلى هذا فإن إعادة التوجيه تحدث على التردد اللاسلكي للمستهلك. بالنسبة للمجموعات الأخرى، يرجى الرجوع إلى الجدول "أين يتم فرض السياسة؟" في القسم "إعادة التوجيه".

يصف الشكل أدناه والإخراج "show zoning-rule" أدناه قواعد تقسيم المناطق بعد نشر الرسم البياني للخدمة. في هذا المثال، تتم إعادة توجيه حركة مرور البيانات من pcTag 32772 (Web) إلى pcTag 10936 (App) إلى 'destgrp-36' (جانب المستهلك من عقدة الخدمة) وإعادة توجيه حركة مرور البيانات من pcTag 10936 (App) إلى pcTag 32772 (Web) إلى 'destgrp-35' (جانب المورد لعقدة الخدمة). كل فرض في VRF1 أن يكون مستهلك VRF. يسمح بحركة المرور من pcTag 32776 (جانب المستهلك من جدار الحماية) إلى pcTag 32772 (Web) في VRF1.

قواعد تقسيم المناطق بعد نشر رسم الخدمة - العقد بين شبكات VRF




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

يسمح بحركة المرور من pcTag 49157 (المورد من جانب جدار الحماية) إلى pcTag 10936 (App) في VRF2 لأن كليهما في VRF2.

```
Pod1-Leaf1# show zoning-rule scope 2555904
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name |  Action  |
Priority       |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
|   4249  | 49157  | 10936  | default  | uni-dir | enabled | 2555904 |      |  permit  |
src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).