ACI 정책 기반 리디렉션 문제 해결

목차

소개

이 문서에서는 ACI PBR(Policy-Based Redirect) 시나리오를 이해하고 문제를 해결하는 단계에 대해 설명합니다.

배경 정보

이 문서의 자료는 Troubleshooting Cisco Application Centric Infrastructure, Second Edition 책, 특히 **정책 기반 리디렉션 - 개요, 정책 기반 리디렉션 - 서비스 그래프 배포, 정책 기반 리디렉션 - 전달 및 정책 기반 리디렉션 - 기타 트래픽 흐름 예제 장에서** 추출되었습니다.

정책 기반 리디렉션 개요

이 장에서는 PBR(정책 기반 리디렉션)을 사용하는 비관리 모드 서비스 그래프의 문제 해결에 대해 설명합니다.

다음은 일반적인 문제 해결 단계입니다. 이 장에서는 PBR에 해당하는 2단계와 3단계를 확인하는 방법에 대해 설명합니다. 1단계와 4단계는 다음 장을 참조하십시오. "패브릭 내 포워딩", "외부 포워딩" 및 "보안 정책"

1. PBR 서비스 그래프 없이 트래픽 작동 확인: 소비자 및 공급자 엔드포인트를 학습합니다.소비자 및 공급자 엔드포인트가 통신할 수 있습니다.
2. 서비스 그래프 구축 확인: 구축된 그래프 인스턴스에는 결함이 없습니다.서비스 노드에 대한 VLAN 및 클래스 ID가 구축됩니다.서비스 노드 엔드포인트를 학습합니다.
3. 전달 경로를 확인합니다. 확인 정책은 리프 노드에 프로그래밍됩니다.서비스 노드에서 트래픽을 캡처하여 트래픽이 리디렉션되는지 확인합니다.ACI 리프의 트래픽을 캡처하여 PBR 이후 트래픽이 ACI 패브릭으로 돌아왔는지 확인합니다.
4. 트래픽이 소비자 및 공급자 엔드포인트에 도착하고 엔드포인트가 반환 트래픽을 생성하는지 확인합니다.

이 문서에서는 설계 또는 구성 옵션을 다루지 않습니다. 자세한 내용은 Cisco.com의 "ACI PBR 백서"를 참조하십시오.

이 장에서 서비스 노드 및 서비스 리프는 다음을 의미합니다.

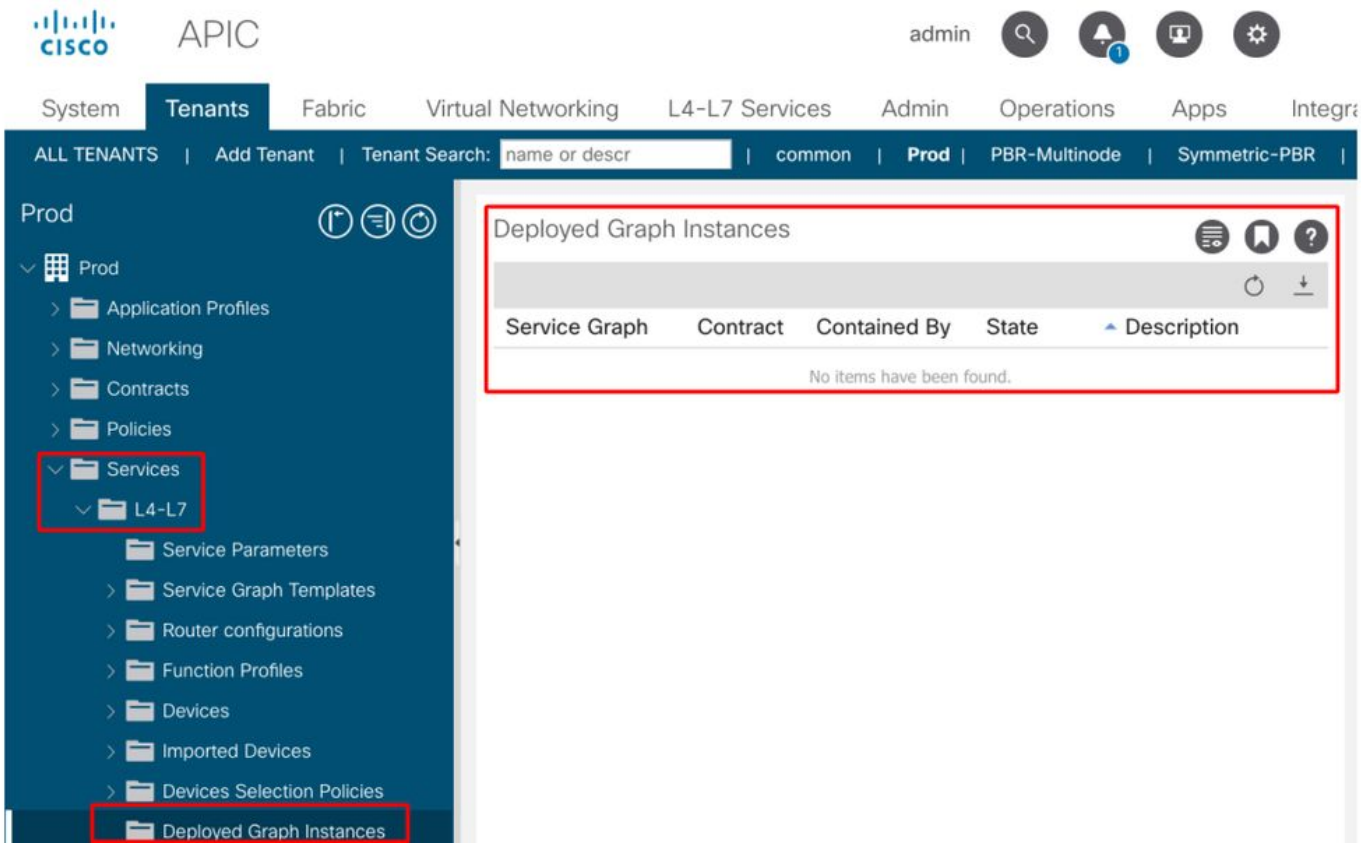
- 서비스 노드 — PBR이 트래픽을 리디렉션하는 외부 노드(예: 방화벽 또는 로드 밸런서)입니다.
- 서비스 리프 — 서비스 노드에 연결된 ACI 리프

서비스 그래프 구축 문제 해결

이 장에서는 서비스 그래프가 구축되지 않은 트러블슈팅 예를 설명합니다.

서비스 그래프 정책을 정의하고 계약 주제에 적용한 후에는 ACI GUI에 표시되는 구축된 그래프 인스턴스가 있어야 합니다. 아래 그림에는 서비스 그래프가 구축된 것으로 표시되지 않는 문제 해결 시나리오가 나와 있습니다.

서비스 그래프는 구축된 그래프 인스턴스로 표시되지 않습니다.



1. 컨피그레이션 단계 및 결함 확인

트러블슈팅의 첫 번째 단계는 필요한 구성 요소가 오류 없이 구성되었는지 확인하는 것입니다. 아래 일반 컨피그레이션은 이미 완료된 것으로 가정합니다.

- 소비자 EPG, 제공자 EPG 및 서비스 노드를 위한 VRF 및 BD
- 소비자 및 제공자 EPG.
- 계약 및 필터

서비스 노드에 대한 EPG를 수동으로 생성할 필요는 없습니다. 서비스 그래프 구축을 통해 생성됩니다.

PBR 컨피그레이션 단계가 포함된 서비스 그래프는 다음과 같습니다.

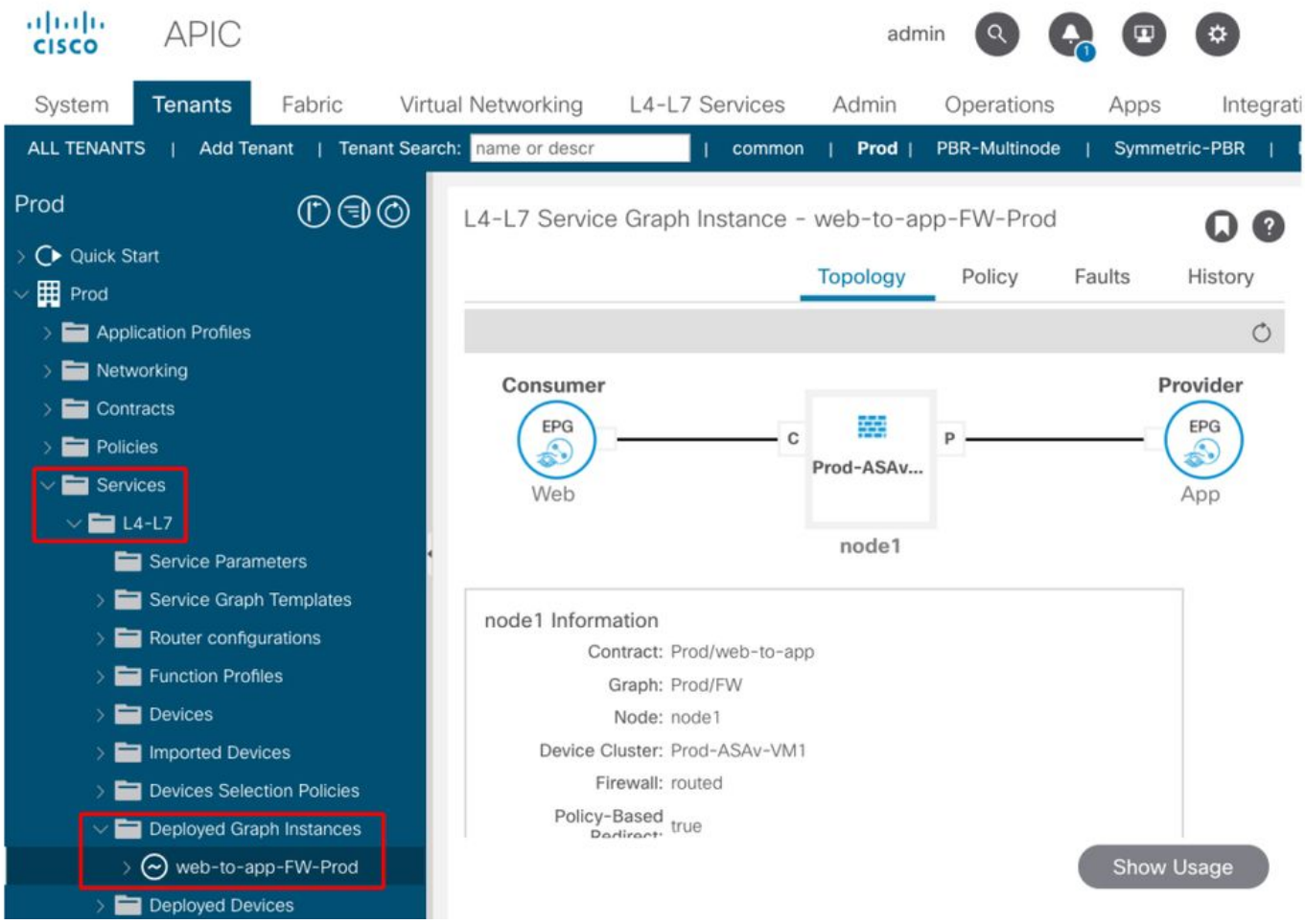
- L4-L7 디바이스(논리적 디바이스)를 생성합니다.
- 서비스 그래프를 생성합니다.
- PBR 정책을 생성합니다.
- 디바이스 선택 정책을 생성합니다.
- 서비스 그래프를 계약 주체와 연결합니다.

2. UI에서 서비스 그래프 구축 확인

서비스 그래프가 계약 주체에 연결되면 서비스 그래프가 있는 각 계약에 대해 구축된 그래프 인스턴스가 표시됩니다(아래 그림).

위치는 'Tenant(테넌트) > Services(서비스) > L4-L7 > Deployed Graph Instances(구축된 그래프 인스턴스)'입니다.

구축된 그래프 인스턴스



구축된 그래프 인스턴스가 표시되지 않으면 계약 컨피그레이션에 문제가 있는 것입니다. 주요 원인은 다음과 같습니다.

- 계약에 소비자 또는 공급자 EPG가 없습니다.
- 계약 주체에 필터가 없습니다.
- VRF 간 또는 테넌트 간 EPG 통신을 위한 경우에도 계약 범위는 VRF입니다.

Service Graph 인스턴스화가 실패하면 Deployed Graph Instance에서 fault가 발생합니다. 즉, Service Graph 컨피그레이션에 문제가 있습니다. 컨피그레이션으로 인한 일반적인 결함은 다음과 같습니다.

F1690: ID 할당 실패로 인해 구성이 잘못되었습니다.

이 결함은 서비스 노드의 캡슐화된 VLAN을 사용할 수 없음을 나타냅니다. 예를 들어 논리적 디바이스에 사용된 VMM 도메인과 연결된 VLAN 풀에 사용 가능한 동적 VLAN이 없습니다.

해결 방법: 논리적 디바이스에 사용되는 도메인에서 VLAN 풀을 확인합니다. 물리적 도메인에 있는 경우 논리적 디바이스 인터페이스에서 캡슐화된 VLAN을 선택합니다. 위치는 'Tenant(테넌트) > Services(서비스) > L4-L7 > Devices and Fabric(디바이스 및 패브릭) > Access Policies(액세스 정책) > Pools(풀) > VLAN'입니다.

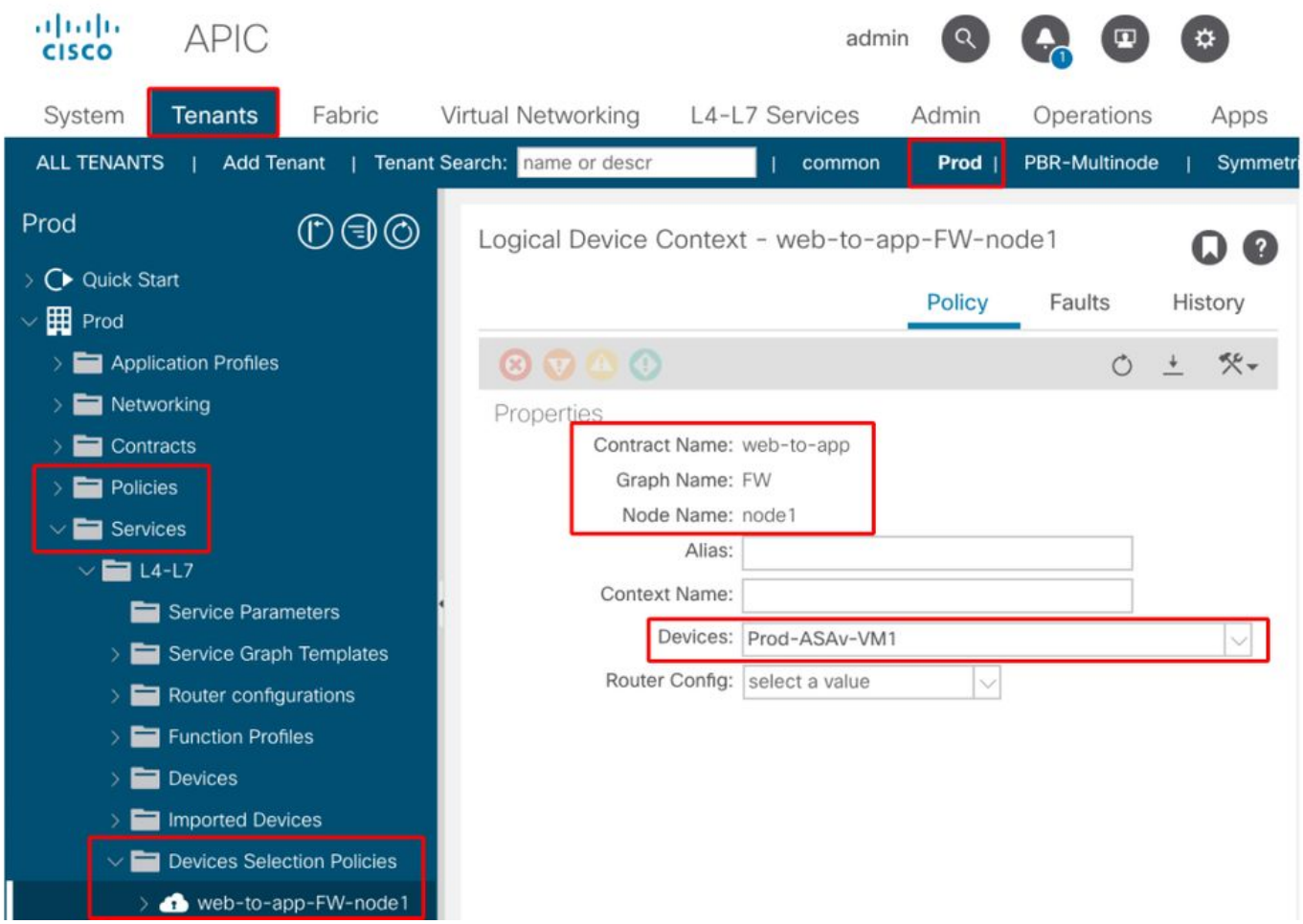
F1690: LDev에 대한 디바이스 컨텍스트를 찾을 수 없으므로 구성이 잘못되었습니다.

이 결함은 서비스 그래프 렌더링에 대해 논리적 장치를 찾을 수 없음을 나타냅니다. 예를 들어 서비스 그래프와 계약에 대해 일치하는 디바이스 선택 정책이 없습니다.

해결 방법: 디바이스 선택 정책이 정의되었는지 확인합니다. 디바이스 선택 정책은 서비스 디바이

스 및 해당 커넥터에 대한 선택 기준을 제공합니다. 기준은 계약 이름, 서비스 그래프 이름 및 서비스 그래프의 노드 이름을 기준으로 합니다. 위치는 'Tenant(테넌트) > Services(서비스) > L4-L7 > Device Selection Policy(디바이스 선택 정책)'입니다.

디바이스 선택 정책 확인



F1690: 클러스터 인터페이스를 찾을 수 없으므로 구성이 잘못되었습니다.

이 결함은 서비스 노드에 대한 클러스터 인터페이스를 찾을 수 없음을 나타냅니다. 예를 들어 클러스터 인터페이스는 디바이스 선택 정책에 지정되지 않습니다.

해결 방법: 클러스터 인터페이스가 디바이스 선택 정책에 지정되어 있고 커넥터 이름이 올바른지 확인하십시오(아래 그림).

F1690: BD를 찾을 수 없어 구성이 잘못되었습니다.

이 결함은 서비스 노드에 대한 BD를 찾을 수 없음을 나타냅니다. 예를 들어, BD는 Device Selection Policy(디바이스 선택 정책)에 지정되어 있지 않습니다.

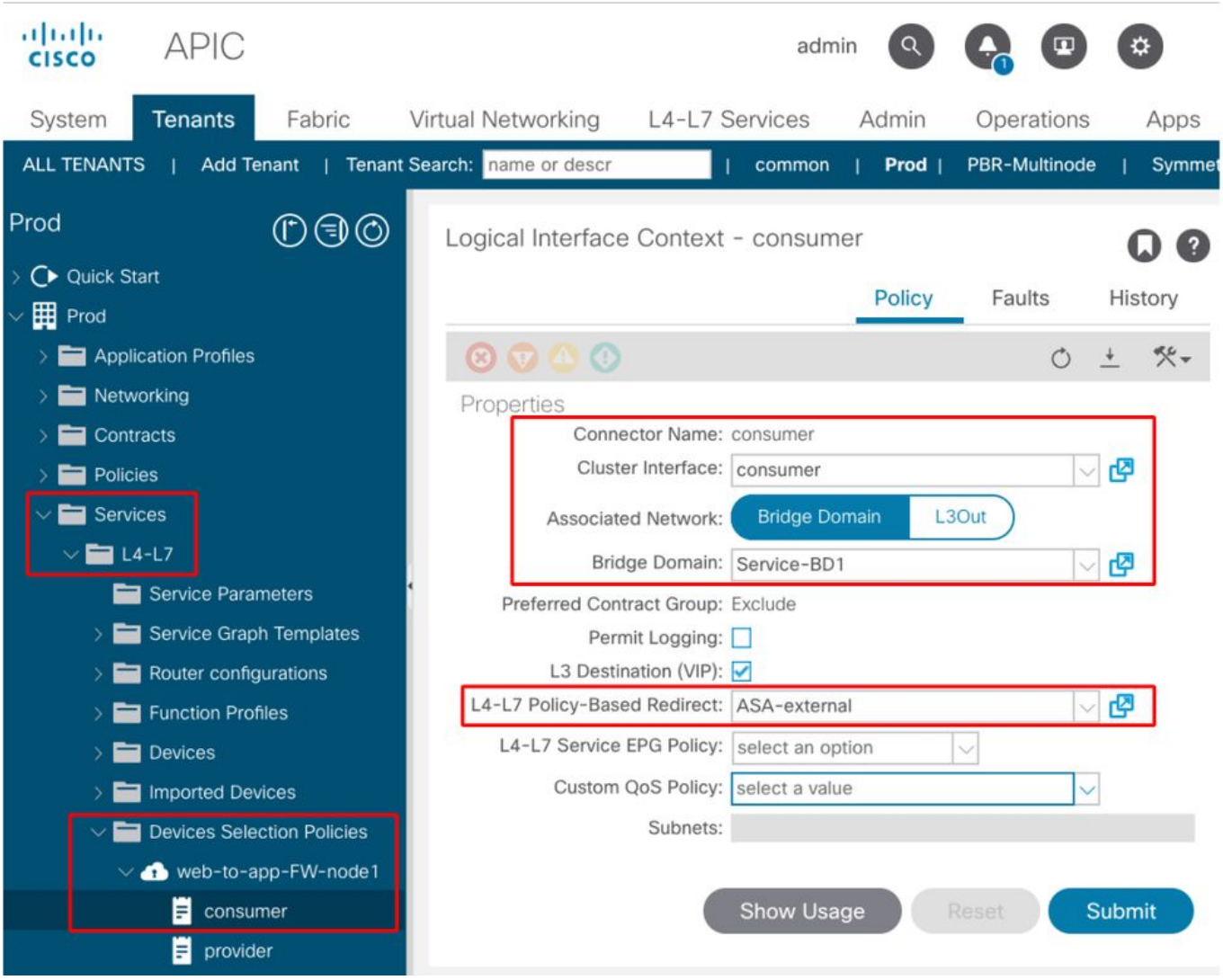
해결 방법: BD가 장치 선택 정책에 지정되어 있고 커넥터 이름이 정확한지 확인하십시오(아래 그림).

F1690: 잘못된 서비스 리디렉션 정책으로 인해 컨피그레이션이 잘못되었습니다.

이 결함은 서비스 그래프의 서비스 함수에서 리디렉션이 활성화되어 있어도 PBR 정책이 선택되지 않았음을 나타냅니다.

해결 방법: 디바이스 선택 정책에서 PBR 정책을 선택합니다(아래 그림).

디바이스 선택 정책의 논리적 인터페이스 컨피그레이션



PBR 전달 문제 해결

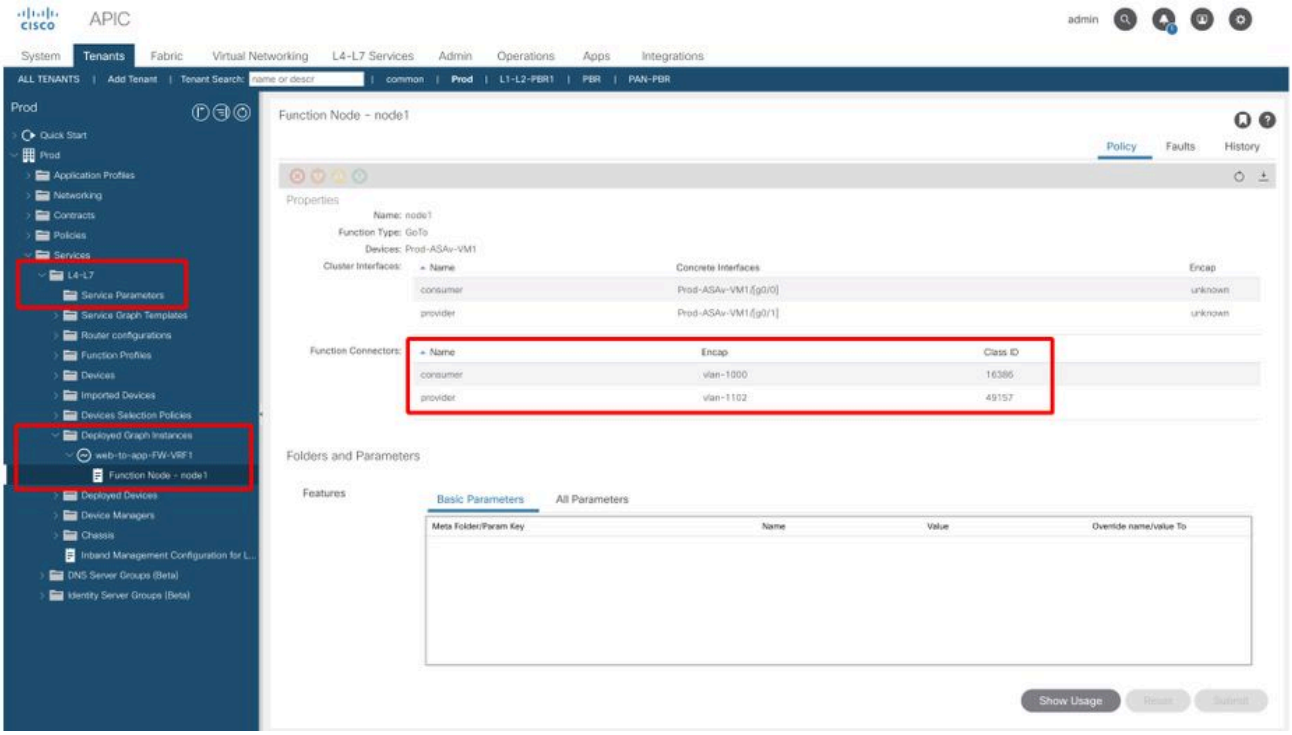
이 장에서는 PBR 전달 경로의 문제 해결 단계에 대해 설명합니다.

1. VLAN이 구축되어 있고 엔드포인트가 리프 노드에서 학습되는지 확인합니다.

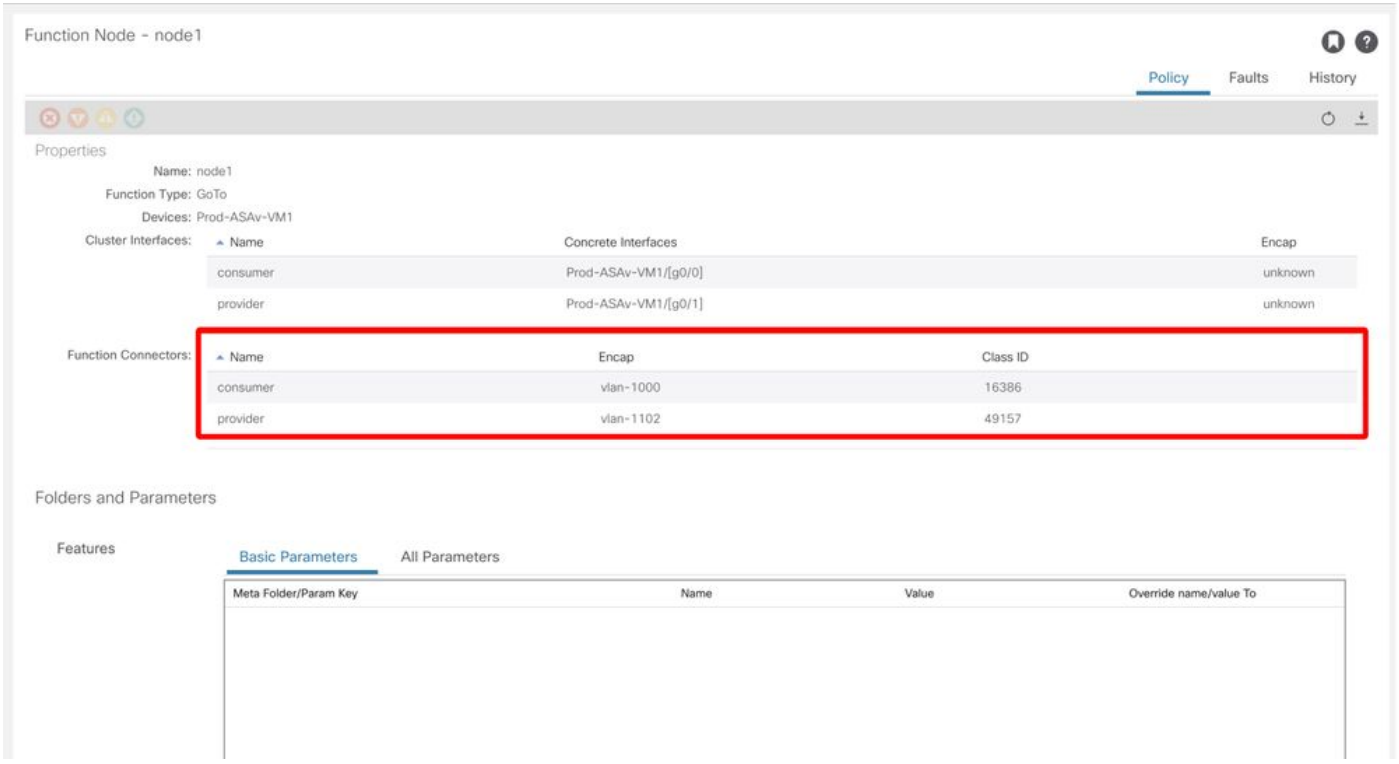
장애 없이 서비스 그래프가 성공적으로 구축되면 서비스 노드에 대한 EPG 및 BD가 생성됩니다. 아래 그림에는 서비스 노드 인터페이스(서비스 EPG)의 캡슐화된 VLAN ID 및 클래스 ID를 찾을 수 있는 위치가 나와 있습니다. 이 예에서 방화벽의 소비자측은 VLAN 인캡 1000의 클래스 ID 16386이고 방화벽의 사업자측은 VLAN 인캡 1102의 클래스 ID 49157입니다.

위치는 'Tenant(테넌트) > Services(서비스) > L4-L7 > Deployed Graph instances(구축된 그래프 인스턴스) > Function Nodes(기능 노드)'입니다.

서비스 노드



서비스 노드 인터페이스 클래스 ID



이러한 VLAN은 서비스 노드가 연결된 서비스 리프 노드 인터페이스에 구축됩니다. 서비스 리프 노드 CLI에서 'show vlan extended'와 'show endpoint'를 사용하여 VLAN 구축 및 엔드포인트 학습 상태를 확인할 수 있습니다.

```
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
```

서비스 노드의 엔드포인트 IP가 ACI 패브릭에서 엔드포인트로 학습되지 않으면 서비스 leaf와 서비스 노드 간의 연결 또는 컨피그레이션 문제일 가능성이 높습니다. 다음 상태를 확인하십시오.

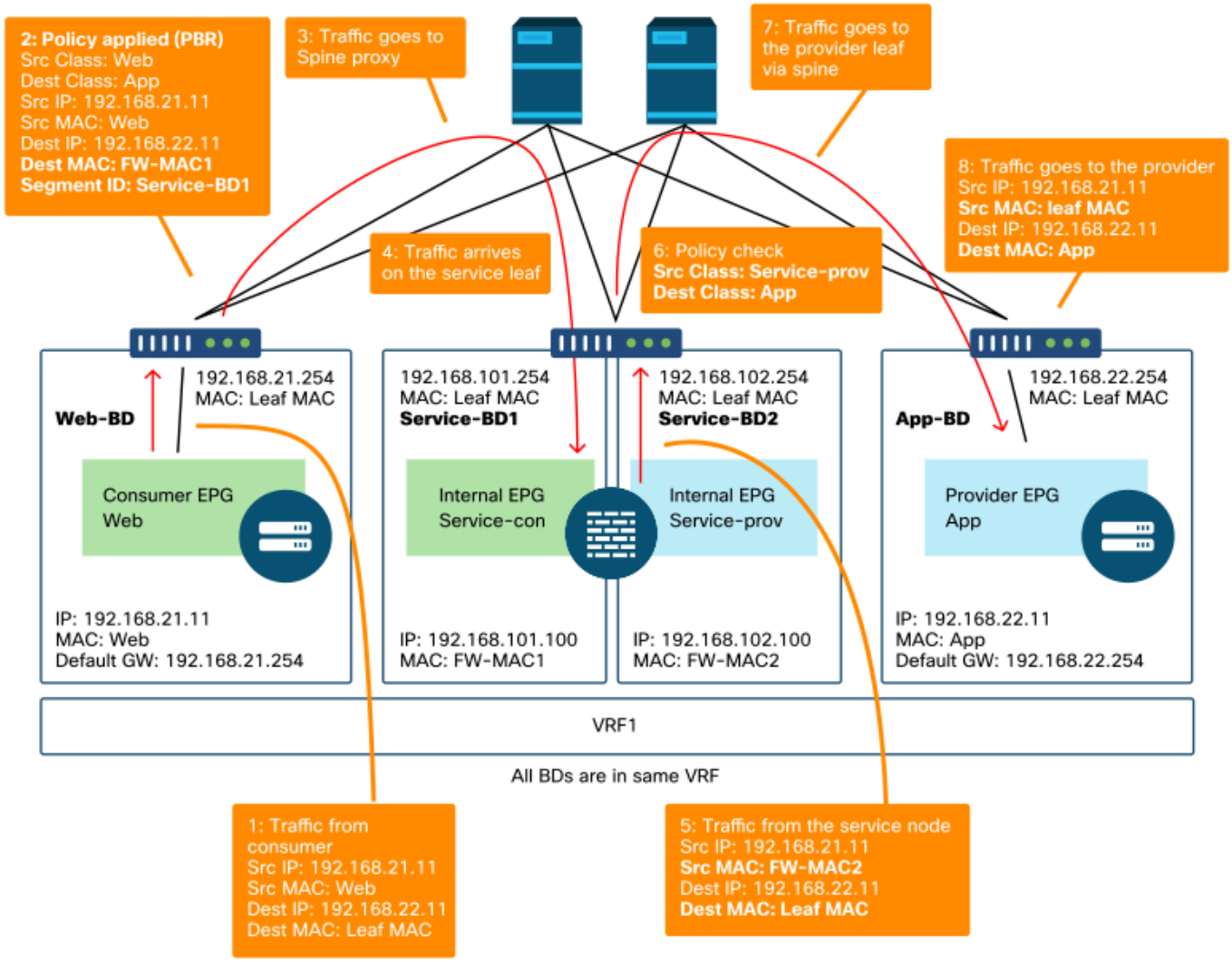
- 서비스 노드는 올바른 leaf 다운링크 포트에 연결됩니다. 서비스 노드가 물리적 도메인에 있는 경우 논리적 디바이스에 리프 고정 경로 엔드캡 VLAN을 정의해야 합니다.서비스 노드가 VMM 도메인에 있는 경우 VMM 도메인이 작동하는지, 서비스 그래프를 통해 생성된 포트 그룹이 서비스 노드 VM에 올바르게 연결되었는지 확인하십시오.
- 서비스 노드 VM이 상주하는 서비스 노드 또는 하이퍼바이저에 연결된 리프 다운링크 포트가 UP입니다.
- 서비스 노드에 올바른 VLAN 및 IP 주소가 있습니다.
- 서비스 리프와 서비스 노드 간의 중간 스위치에는 올바른 VLAN 컨피그레이션이 있습니다.

2. 예상 트래픽 경로 확인

PBR이 활성화된 후 엔드 투 엔드 트래픽이 작동하지 않을 경우, 서비스 노드 엔드포인트가 ACI 패브릭에서 학습되더라도 다음 트러블슈팅 단계는 예상되는 트래픽 경로를 확인하는 것입니다.

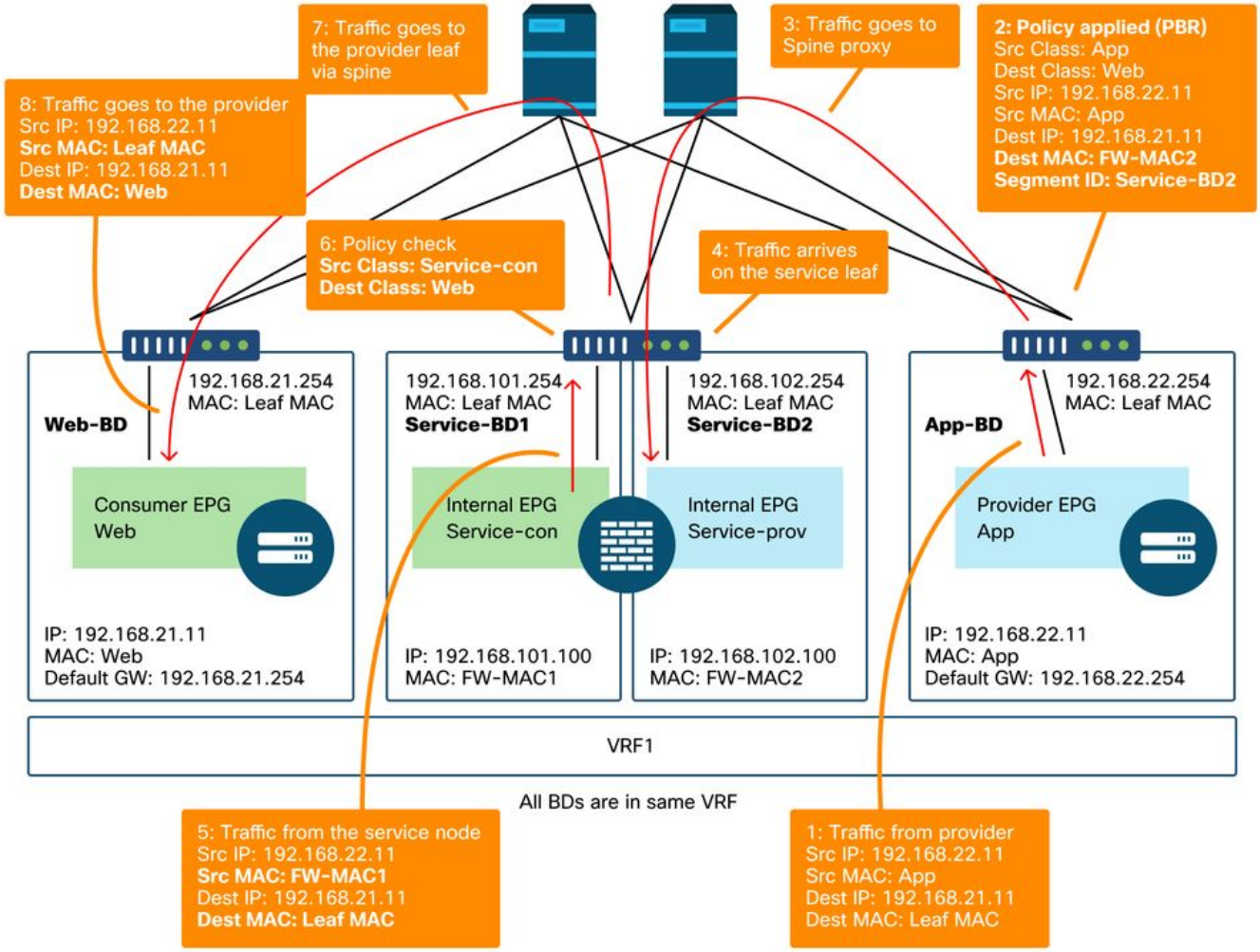
그림 'PBR 전달 경로 예 - 소비자 대 공급자' 및 'PBR 전달 경로 예 - 공급자 대 소비자'는 소비자 엔드포인트와 공급자 엔드포인트 간에 PBR을 사용하여 방화벽을 삽입하는 전달 경로 예를 보여줍니다. 엔드포인트가 리프 노드에서 이미 학습된 것으로 가정합니다.

PBR 전달 경로 예 - 소비자-공급자



참고: 소스 MAC는 ACI 리프 MAC로 변경되지 않으므로 소비자 엔드포인트와 PBR 노드가 동일한 BD에 있지 않을 경우 PBR 노드는 소스 MAC 기반 전달을 사용하지 않아야 합니다

PBR 전달 경로 예 - 공급자 대 소비자



참고: PBR 정책은 소비자 또는 공급자 리프에서 시행되며 ACI PBR에서 수행하는 작업은 'PBR 전달 경로 예 - 소비자 대 공급자' 및 'PBR 전달 경로 예 - 공급자 대 소비자' 그림에 표시된 대로 대상 MAC 재작성입니다. 소스 엔드포인트와 PBR 대상 MAC가 동일한 leaf에 있는 경우에도 PBR 대상 MAC에 도달하면 항상 spine 프록시를 사용합니다.

'PBR 전달 경로 예 - 소비자 대 공급자' 및 'PBR 전달 경로 예 - 공급자 대 소비자'는 트래픽이 리디렉션되는 위치의 예를 보여주지만, 정책이 적용되는 위치는 계약 컨피그레이션 및 엔드포인트 학습 상태에 따라 다릅니다. '정책이 시행되는 위치' 테이블에는 단일 ACI 사이트에서 정책이 시행되는 위치가 요약되어 있습니다. 다중 사이트에서 정책이 적용되는 위치는 다릅니다.

정책이 적용되는 위치

시나리오	VRF 시행 모드	소비자	공급자	정책 적용 대상
VRF 내	인그레스/이그레스	이피지	이피지	·대상 엔드포인트를 학습한 경우: 인그레스 리프* ·대상 엔드포인트를 학습하지 않은 경우 : 이그레스 리프
	인그레스	이피지	L3Out EPG	소비자 리프(비경계 리프)
	인그레스	L3Out EPG	이피지	공급자 리프(비경계 리프)
	이그레스	이피지	L3Out EPG	경계 리프 -> 비경계 리프 트래픽 ·대상 엔드포인트를 학습한 경우: 보더

	이그레스	L3Out EPG	이피지	리프 ·대상 엔드포인트를 학습하지 않은 경우 : 비경계 리프 비경계 리프-> 경계 리프 트래픽 ·보더 리프
	인그레스/이그레스	L3Out EPG	L3Out EPG	인그레스 리프*
	인그레스/이그레스	이피지	이피지	소비자 리프
	인그레스/이그레스	이피지	L3Out EPG	소비자 리프(비경계 리프)
VRF 간	인그레스/이그레스	L3Out EPG	이피지	인그레스 리프*
	인그레스/이그레스	L3Out EPG	L3Out EPG	인그레스 리프*

*정책 시행은 패킷이 도달한 첫 번째 leaf에 적용됩니다.

예를 들면 다음과 같습니다.

- VRF1의 L3Out EPG에 있는 외부 엔드포인트가 VRF1의 웹 EPG에 있는 엔드포인트에 액세스하려고 시도하고 VRF1이 인그레스 시행 모드로 구성된 경우, 트래픽은 계약 방향과 상관없이 웹 EPG의 엔드포인트가 상주하는 leaf에 의해 리디렉션됩니다.
- VRF1의 소비자 웹 EPG에 있는 엔드포인트가 VRF1의 공급자 앱 EPG에 있는 엔드포인트에 액세스하려고 시도하고 소비자 및 공급자 리프 노드에서 엔드포인트를 학습하면 인그레스 리프에 의해 트래픽이 리디렉션됩니다.
- VRF1의 소비자 웹 EPG에 있는 엔드포인트가 VRF2의 공급자 앱 EPG에 있는 엔드포인트에 액세스하려고 시도하는 경우, VRF 시행 모드에 관계없이 소비자 엔드포인트가 상주하는 소비자 리프에 의해 트래픽이 리디렉션됩니다.

3. 트래픽이 서비스 노드로 리디렉션되는지 확인

예상 포워딩 경로가 명확해지면 ELAM을 사용하여 스위치 노드에 트래픽이 도착하는지 확인하고 스위치 노드에서 포워딩 결정을 확인할 수 있습니다. ELAM 사용 방법에 대한 지침은 "Intra-Fabric Forwarding" 장의 "Tools" 섹션을 참조하십시오.

예를 들어, 'PBR 전달 경로 예 - 소비자-공급자' 그림의 트래픽 흐름을 추적하기 위해 이들을 캡처하여 소비자-공급자 트래픽이 리디렉션되는지 확인할 수 있습니다.

- 1 및 2를 확인할 소비자 리프의 다운링크 포트(트래픽이 소비자 리프에 도착하고 PBR이 적용됨).
- 3(트래픽이 스파인 프록시로 이동)을 확인할 스파인 노드의 패브릭 포트.
- 4(트래픽이 서비스 리프에 도착함)를 확인할 서비스 리프의 패브릭 포트.

그런 다음 서비스 노드에서 다시 오는 트래픽이 공급자로 이동하는지 확인하기 위해 이러한 트래픽을 캡처할 수 있습니다.

- 5 및 6(트래픽은 서비스 노드에서 반환되며 허용됨)을 확인할 서비스 리프의 다운링크 포트입니다.
- 7을 확인할 스파인 노드의 패브릭 포트(스파인을 통해 사업자 리프로 트래픽 이동).
- 8을 확인할 공급자 리프의 패브릭 포트(트래픽이 서비스 리프에 도착하여 공급자 엔드포인트로 이동)

참고: 소비자 및 서비스 노드가 동일한 leaf에 있는 경우, 인터페이스 또는 소스 MAC를 지정하여 그림 'PBR 전달 경로 예 - 소비자 대 공급자'에서 ELAM이 1 또는 5를 확인하도록 합니다. 두 노드는 모두 동일한 소스 IP와 목적지 IP를 사용하기 때문입니다.

소비자-공급자 트래픽이 서비스 노드로 리디렉션되지만 서비스 leaf로 돌아오지 않는 경우, 일반적인 실수이므로 다음을 확인하십시오.

- 서비스 노드 라우팅 테이블이 공급자 서브넷에 도달합니다.
- ACL과 같은 서비스 노드 보안 정책은 트래픽을 허용합니다.

트래픽이 리디렉션되어 공급자에 도달하는 경우 유사한 방법으로 공급자에서 소비자로 돌아오는 트래픽 경로를 확인하십시오.

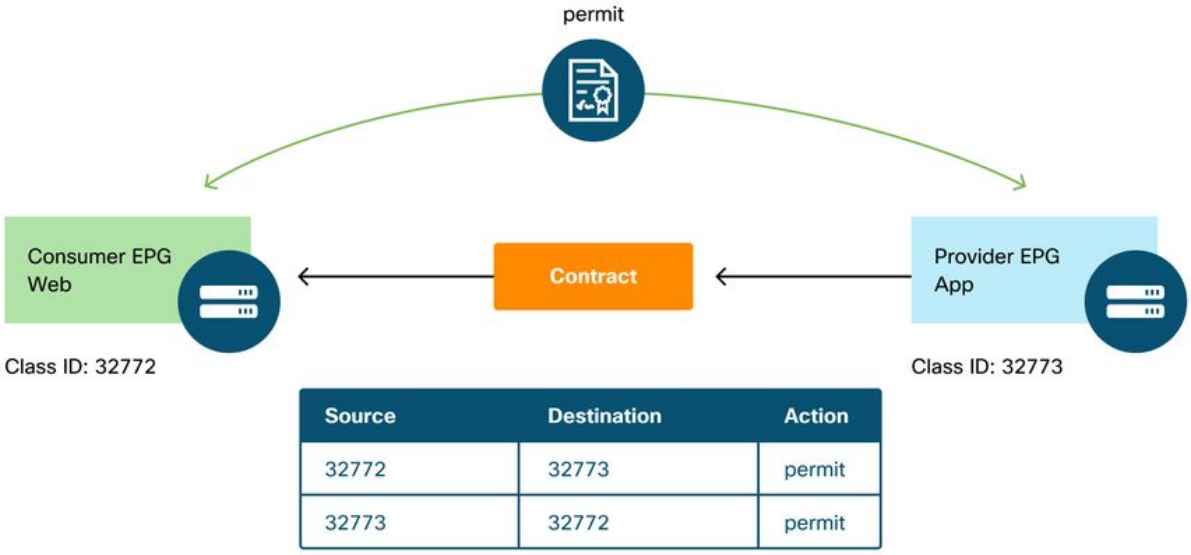
4. 리프 노드에 프로그래밍된 정책 확인

이에 따라 트래픽이 전달되거나 리디렉션되지 않으면 다음 트러블슈팅 단계는 리프 노드에 프로그래밍된 정책을 확인하는 것입니다. 이 섹션에서는 zoning-rule 및 contract_parser를 예로 보여 줍니다. zoning-rule을 확인하는 방법에 대한 자세한 내용은 "보안 정책" 장의 "툴" 섹션을 참조하십시오.

참고: 정책은 leaf의 EPG 구축 상태를 기반으로 프로그래밍됩니다. 이 섹션의 show 명령 출력에서는 소비자 EPG, 제공자 EPG 및 서비스 노드에 대한 EPG가 포함된 leaf를 사용합니다.

'show zoning-rule' 명령 사용

아래 그림과 'show zoning-rule' 출력은 서비스 그래프 구축 전의 zoning-rule에 대해 설명합니다.



Source	Destination	Action
32772	32773	permit
32773	32772	permit

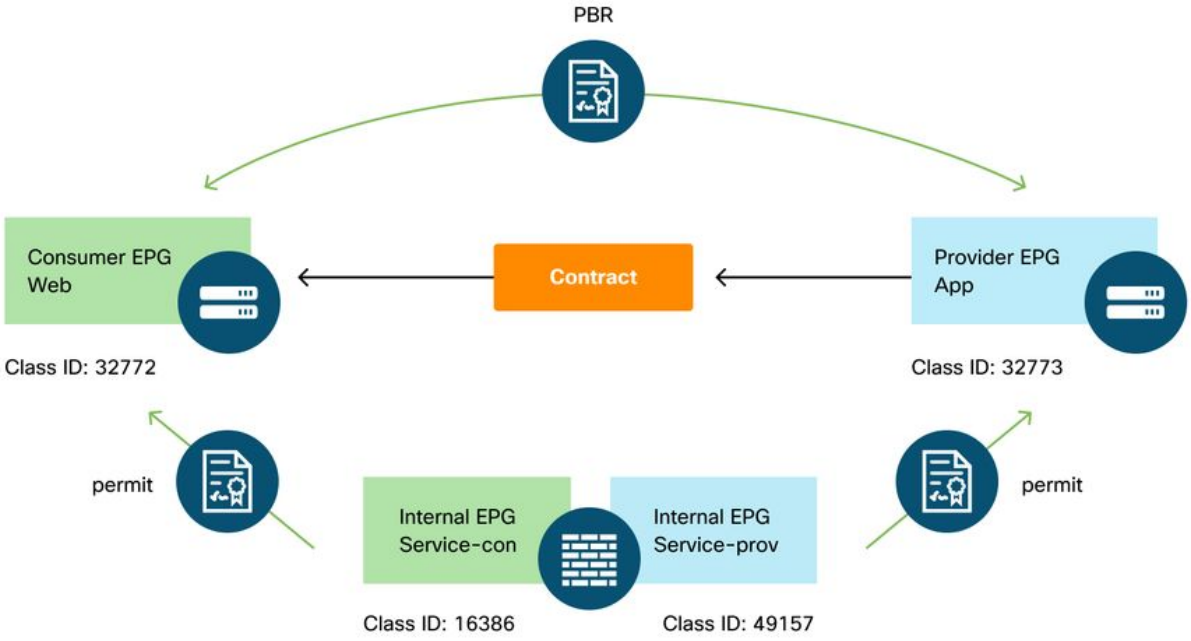
VRF 범위 ID는 'Tenant(테넌트) > Networking(네트워킹) > VRF'에서 확인할 수 있습니다.

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

서비스 그래프가 구축되면 서비스 노드에 대한 EPG가 생성되고 정책이 업데이트되어 소비자와 사업자 EPG 간의 트래픽이 리디렉션됩니다. 아래 그림과 'show zoning-rule' 출력은 서비스 그래프 구축 이후의 zoning-rule에 대해 설명합니다. 이 예에서는 pcTag 32772(웹)에서 pcTag 32773(앱)로의 트래픽이 'destgrp-27'(서비스 노드의 소비자 측)로 리디렉션되고 pcTag 32773(앱)에서 pcTag 32772(웹)로의 트래픽은 'destgrp-28'(서비스 노드의 공급자 측)로 리디렉션됩니다.

서비스 그래프 구축 후 조닝 규칙



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

각 destgrp의 목적지 정보는 'show service redir info' 명령을 사용하여 찾을 수 있습니다.

```
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
...
```

조닝 규칙이 그에 따라 프로그래밍되었지만 트래픽이 그에 따라 리디렉션되거나 전달되지 않는 경우, 일반적인 실수이므로 다음을 확인하십시오.

- ELAM을 사용하여 소스 또는 대상 클래스 ID가 예상대로 해결되었는지 확인합니다. 그렇지 않은 경우, 잘못된 클래스 ID가 무엇이고 EPG 유도 기준(예: 경로 및 캡슐화 VLAN)을 확인하십시오.
- 소스 및 대상 클래스 ID가 그에 따라 확인되고 PBR 정책이 적용되지만 트래픽이 PBR 노드에 도달하지 않더라도 redir 작업('show service redir info')에서 destgrp의 IP, MAC 및 VRF가 올바른지 확인하십시오.

기본적으로 PBR이 활성화된 경우 서비스 노드(소비자 측)에 대한 소비자 EPG 및 서비스 노드(공급자 측)에 대한 공급자 EPG에 대한 허용 규칙은 프로그래밍되지 않습니다. 따라서 소비자 또는 공급자 끝점이 기본적으로 서비스 노드와 직접 통신할 수 없습니다. 이 트래픽을 허용하려면 직접 연결 옵션을 활성화해야 합니다. 활용 사례는 "기타 트래픽 흐름 예**" 섹션**에서 설명합니다.

contract_parser 사용

contract_parser 도구를 사용하면 정책을 확인할 수도 있습니다. C-consumer는 서비스 노드의 소비자 측이고 C-provider는 서비스 노드의 공급자 측입니다.

```
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]
...
```

기타 트래픽 흐름의 예

이 섹션에서는 트러블슈팅을 위해 필요한 플로우를 식별하기 위해 다른 일반적인 트래픽 플로우 예를 고려합니다. 문제 해결 단계는 이 섹션의 이전 장을 참조하십시오.

1. SNAT가 없는 로드 밸런서: 이 예에서 소비자 EPG 웹 및 제공자 EPG 앱은 로드 밸런서 서비스 그래프와 계약을 맺습니다. 애플리케이션 EPG의 엔드포인트는 로드 밸런서의 VIP에 연결된 실제 서버입니다.공급자-소비자 트래픽 방향에 대해 PBR-로드 밸런서가 활성화됩니다.
2. SNAT가 없는 방화벽 및 로드 밸런서: 이 예에서 소비자 EPG 웹 및 사업자 EPG 앱은 방화벽 및 로드 밸런서 서비스 그래프와 계약을 맺습니다. 애플리케이션 EPG의 엔드포인트는 로드 밸런서의 VIP와 연결된 실제 서버입니다.PBR-to-firewall이 양방향으로 활성화되어 있습니다.공급자-소비자 트래픽 방향에 대해 PBR-로드 밸런서가 활성화됩니다.
3. 공유 서비스(VRF 간 계약): 이 예에서 소비자 EPG 웹 및 제공자 EPG 앱은 방화벽 서비스 그래프와 계약을 맺습니다. EPG 웹과 EPG 앱은 서로 다른 VRF에 있습니다.PBR-to-firewall이 양방향으로 활성화되어 있습니다.방화벽은 VRF 사이에 있습니다.

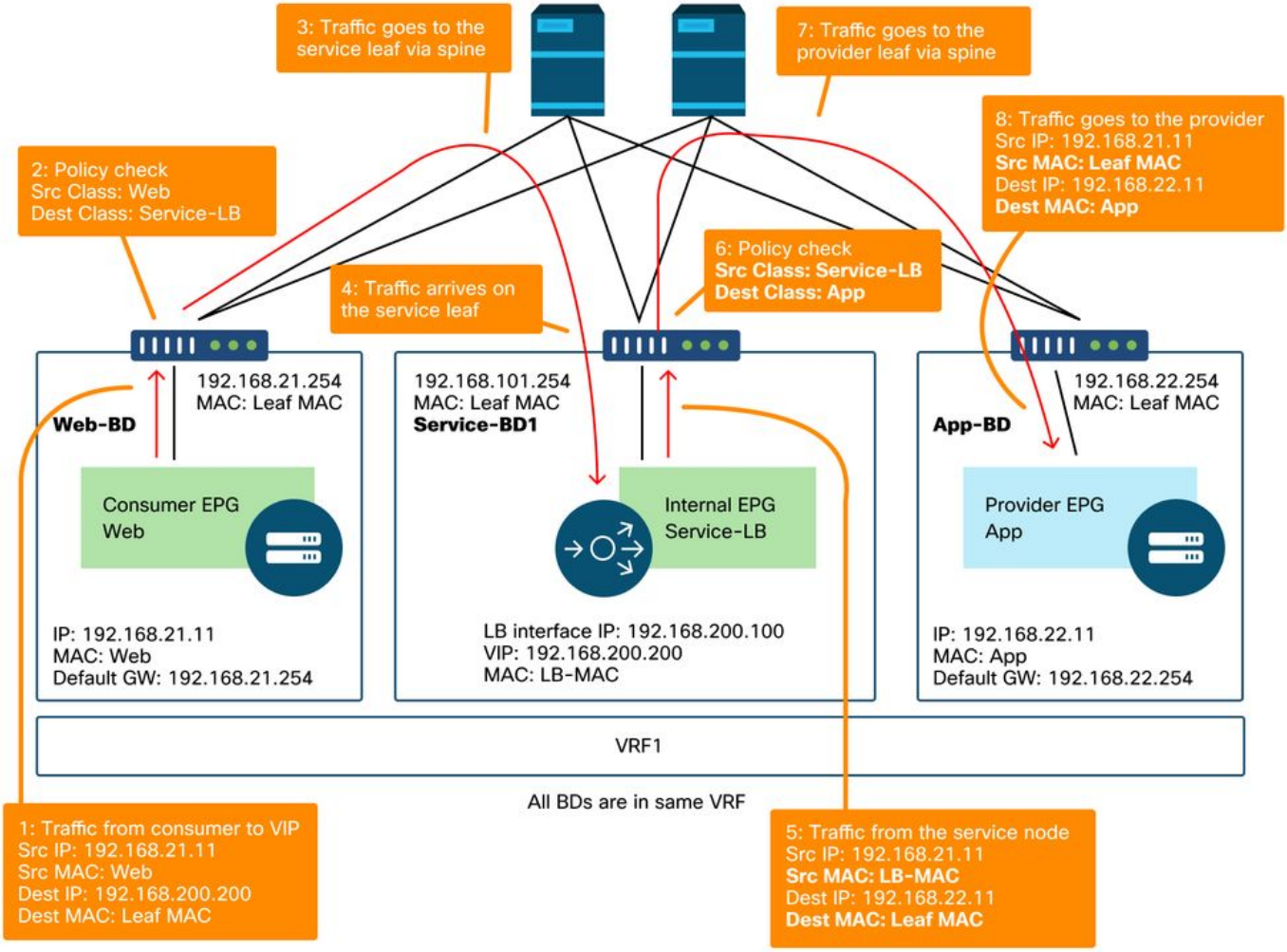
1. SNAT가 없는 로드 밸런서

PBR은 양방향 PBR 또는 단방향 PBR로 구축할 수 있습니다. 단방향 PBR의 활용 사례 중 하나는 소스 NAT(Network Address Translation)가 없는 로드 밸런서 통합입니다. 로드 밸런서가 소스 NAT를 수행하는 경우 PBR이 필요하지 않습니다.

트래픽 경로 예

아래 그림에는 두 개의 연결을 사용하여 소비자 EPG 웹에서 사업자 EPG 앱으로 들어오는 트래픽 흐름의 예가 나와 있습니다. 하나는 소비자 EPG 웹의 엔드포인트에서 로드 밸런서 VIP로, 다른 하나는 로드 밸런서에서 사업자 EPG 앱의 엔드포인트로 연결됩니다. 수신 트래픽은 VIP로 전달되므로 VIP에 연결할 수 있는 경우 트래픽이 PBR 없이 로드 밸런서에 도달합니다. 로드 밸런서는 대상 IP를 VIP와 연결된 EPG 앱의 엔드포인트 중 하나로 변경하지만 소스 IP를 변환하지는 않습니다. 따라서 트래픽은 사업자 엔드포인트로 이동합니다.

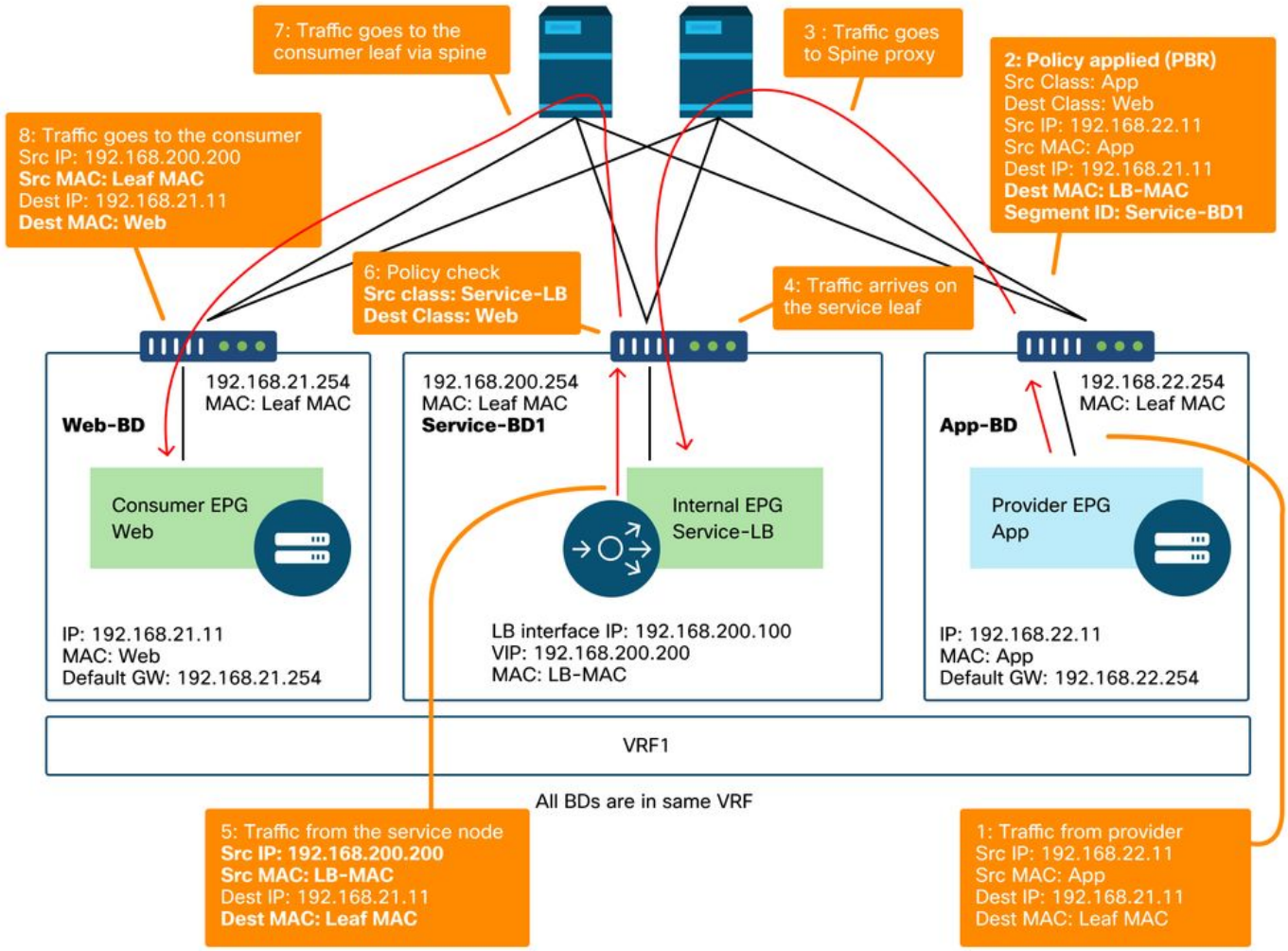
SNAT 포워딩 경로가 없는 로드 밸런서 예 — 소비자에서 VIP로, 로드 밸런서에서 공급자에서 PBR로



아래 그림에는 사업자 EPG 앱에서 소비자 EPG 웹으로의 반환 트래픽 흐름이 나와 있습니다. 반환 트래픽은 원래 소스 IP를 목적지로 하므로 반환 트래픽을 로드 밸런서로 되돌리려면 PBR이 필요합니다. 그렇지 않으면 소비자 엔드포인트는 소스 IP가 VIP가 아닌 제공자 엔드포인트인 트래픽을 수신합니다. ACI 패브릭과 같은 중간 네트워크가 패킷을 소비자 엔드포인트로 다시 전달하더라도 소비자 엔드포인트가 공급자 엔드포인트로 트래픽을 시작하지 않았으므로 이러한 트래픽이 삭제됩니다.

공급자 엔드포인트에서 소비자 엔드포인트로의 트래픽이 로드 밸런서로 리디렉션되면 로드 밸런서는 소스 IP를 VIP로 변경합니다. 그러면 트래픽이 로드 밸런서에서 다시 들어오고 소비자 엔드포인트로 다시 이동합니다.

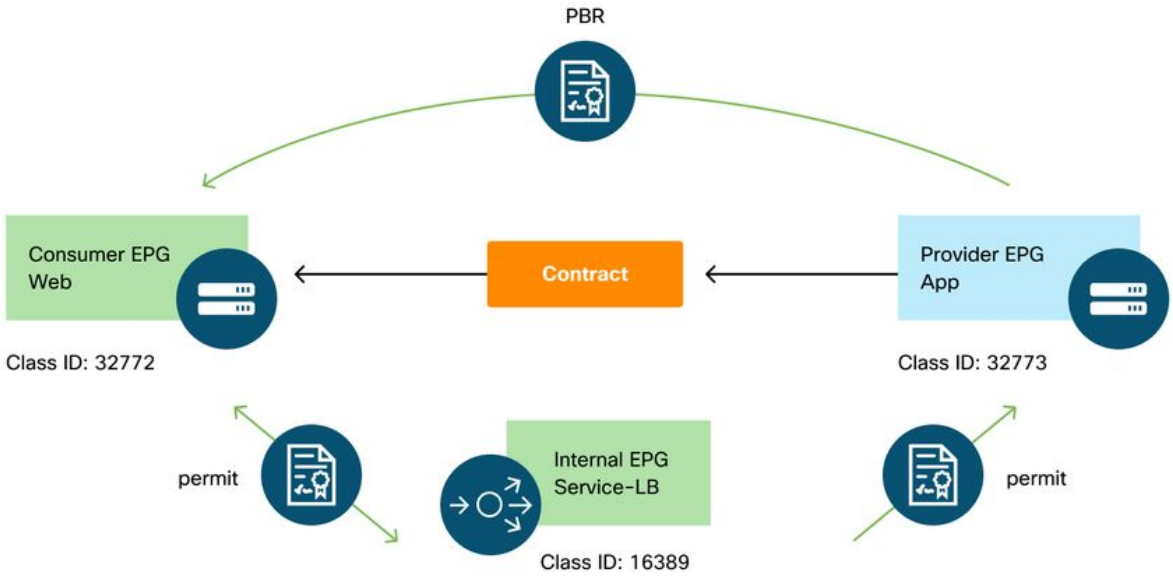
SNAT 포워딩 경로가 없는 로드 밸런서 예 - PBR이 있는 공급자-소비자



리프 노드에 프로그래밍된 정책.

아래 그림과 'show zoning-rule' 출력은 서비스 그래프 구축 이후의 zoning-rule에 대해 설명합니다. 이 예에서는 pcTag 32772(Web)에서 pcTag 16389(Service-LB)로의 트래픽이 허용되고, pcTag 16389(Service-LB)에서 pcTag 32773(App)로의 트래픽이 허용되며, pcTag 32773(App)에서 pcTag 32772(Web)로의 트래픽은 'destgrp-31'(로드 밸런서)로 리디렉션됩니다.

서비스 그래프 구축 후 조닝 규칙 - SNAT가 없는 로드 밸런서

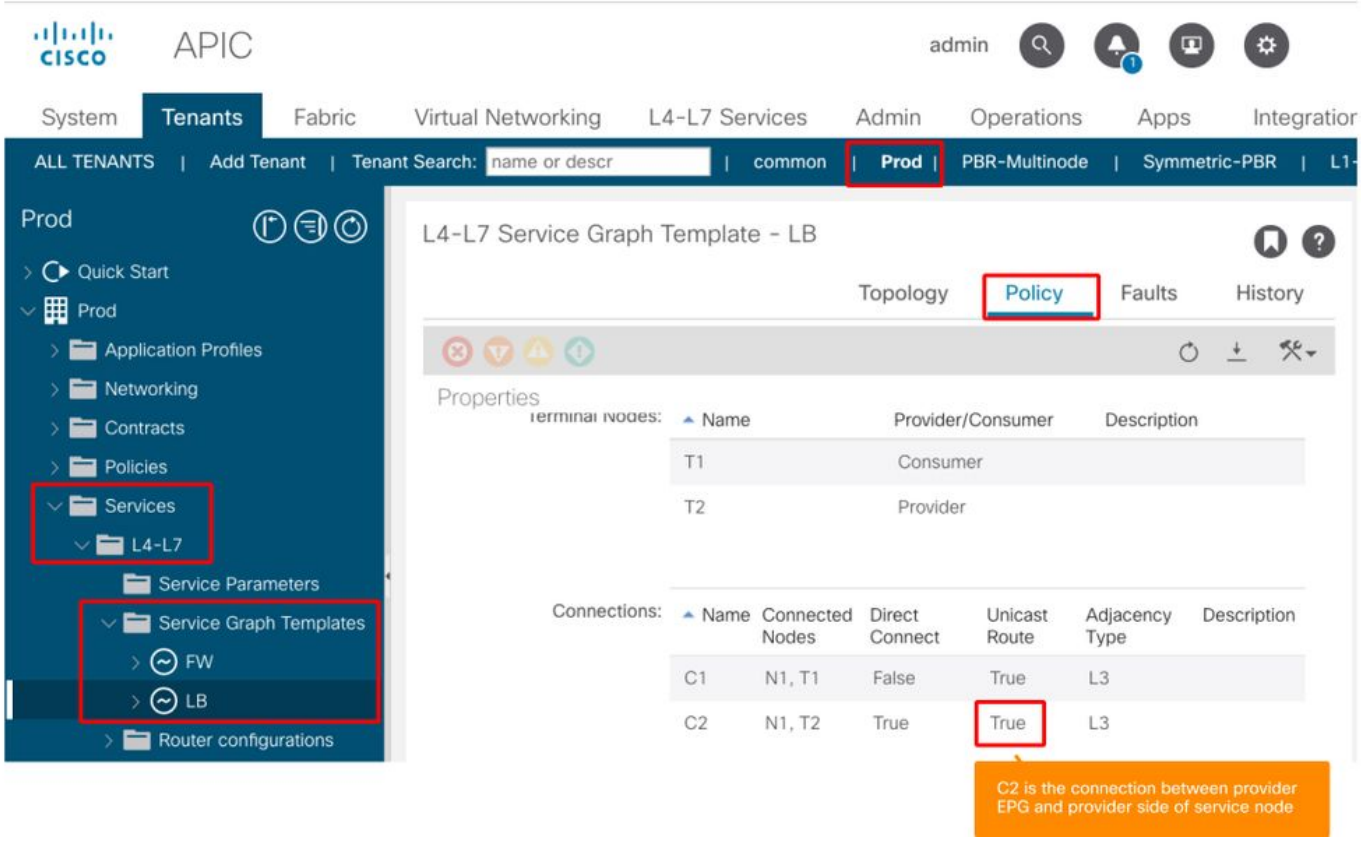


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
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)     |
...
```

기본적으로 사업자 EPG(pcTag 32773)에서 서비스 LB(pcTag 16389)로의 허용 규칙은 프로그래밍되지 않습니다. 부하 분산 장치에서 공급자 엔드포인트로의 상태 확인을 위해 두 장치 간의 양방향 통신을 허용하려면 연결에 대한 직접 연결 옵션을 True로 설정해야 합니다. 위치는 'Tenant(테넌트) > L4-L7 > Service Graph Templates(서비스 그래프 템플릿) > Policy(정책)'입니다. 기본값은 False입니다.

직접 연결 옵션 설정



아래와 같이 사업자 EPG(32773)에 대한 허용 규칙16389 Service-LB(Service-LB)에 추가합니다.

```
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. 트래픽 흐름의 예 - SNAT가 없는 방화벽 및 로드 밸런서

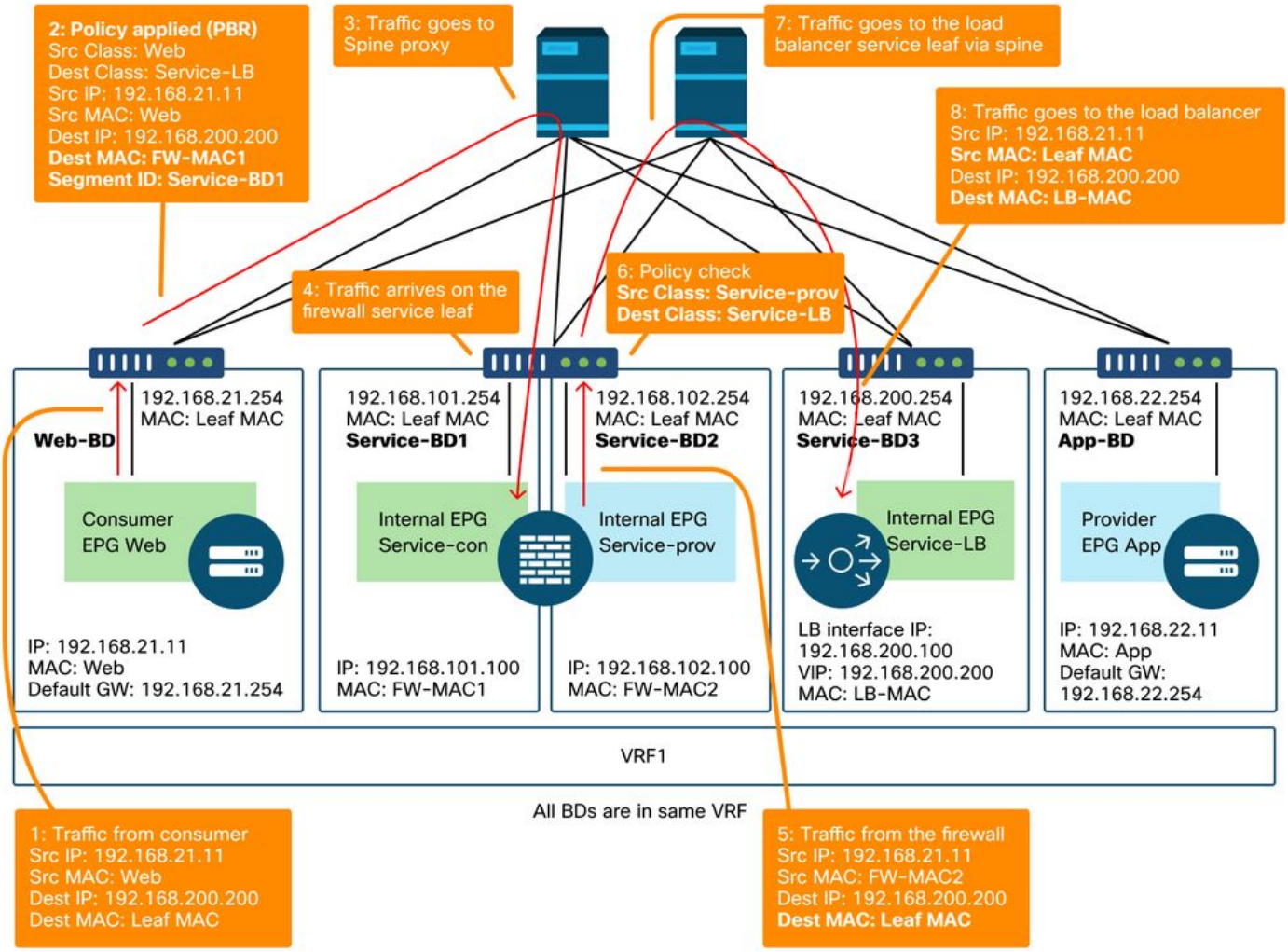
PBR은 서비스 그래프에서 여러 서비스 기능(예: 방화벽(1차 노드), 로드 밸런서(2차 노드))과 함께 구축할 수 있습니다.

트래픽 경로 예

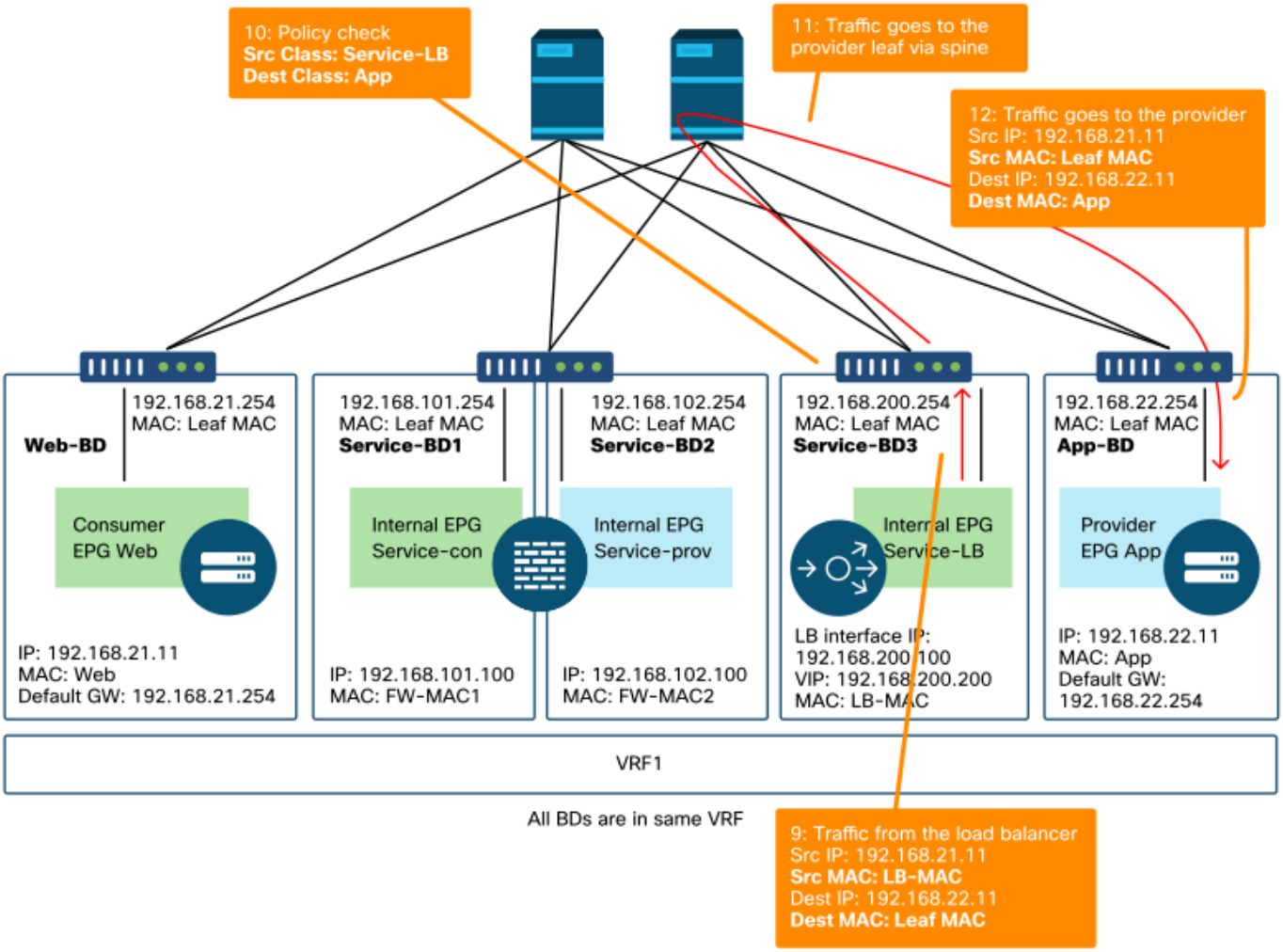
아래 그림에는 두 개의 연결을 사용하여 소비자 EPG 웹에서 사업자 EPG 앱으로 들어오는 트래픽 흐름의 예가 나와 있습니다. 하나는 소비자 EPG 웹의 엔드포인트에서 방화벽을 통해 로드 밸런서 VIP로, 다른 하나는 로드 밸런서에서 사업자 EPG 앱의 엔드포인트로 연결됩니다. VIP로 향하는 수

신 트래픽은 방화벽으로 리디렉션된 다음 PBR 없이 로드 밸런서로 이동합니다. 로드 밸런서는 대상 IP를 VIP와 연결된 앱 EPG의 엔드포인트 중 하나로 변경하지만 소스 IP를 변환하지는 않습니다. 그런 다음 트래픽이 공급자 엔드포인트로 이동합니다.

SNAT 포워딩 경로가 없는 방화벽 및 로드 밸런서 예 - consumer to VIP, load balancer to provider



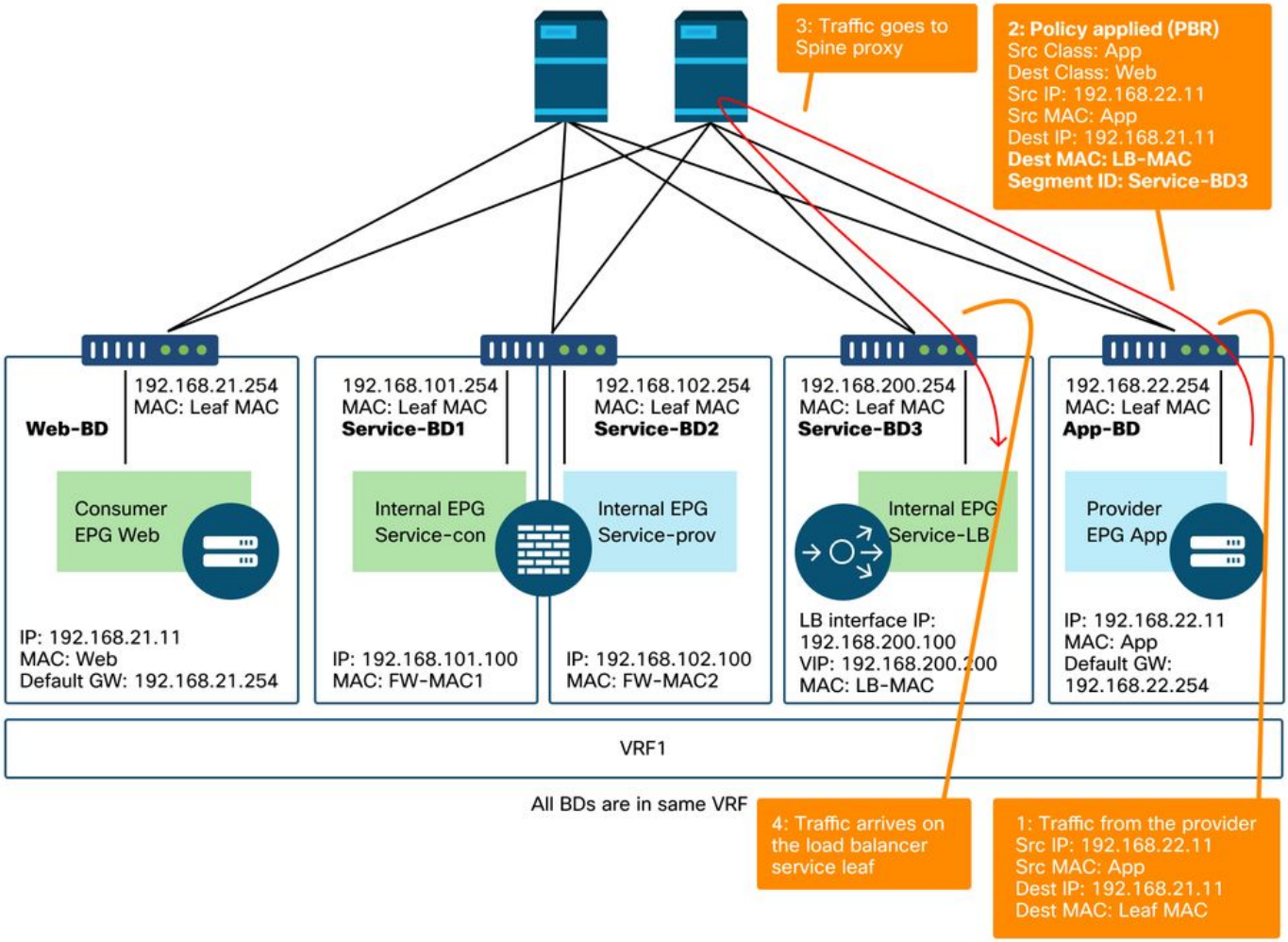
SNAT 포워딩 경로가 없는 방화벽 및 로드 밸런서 예 - consumer에서 VIP로, load balancer에서 provider로(계속)

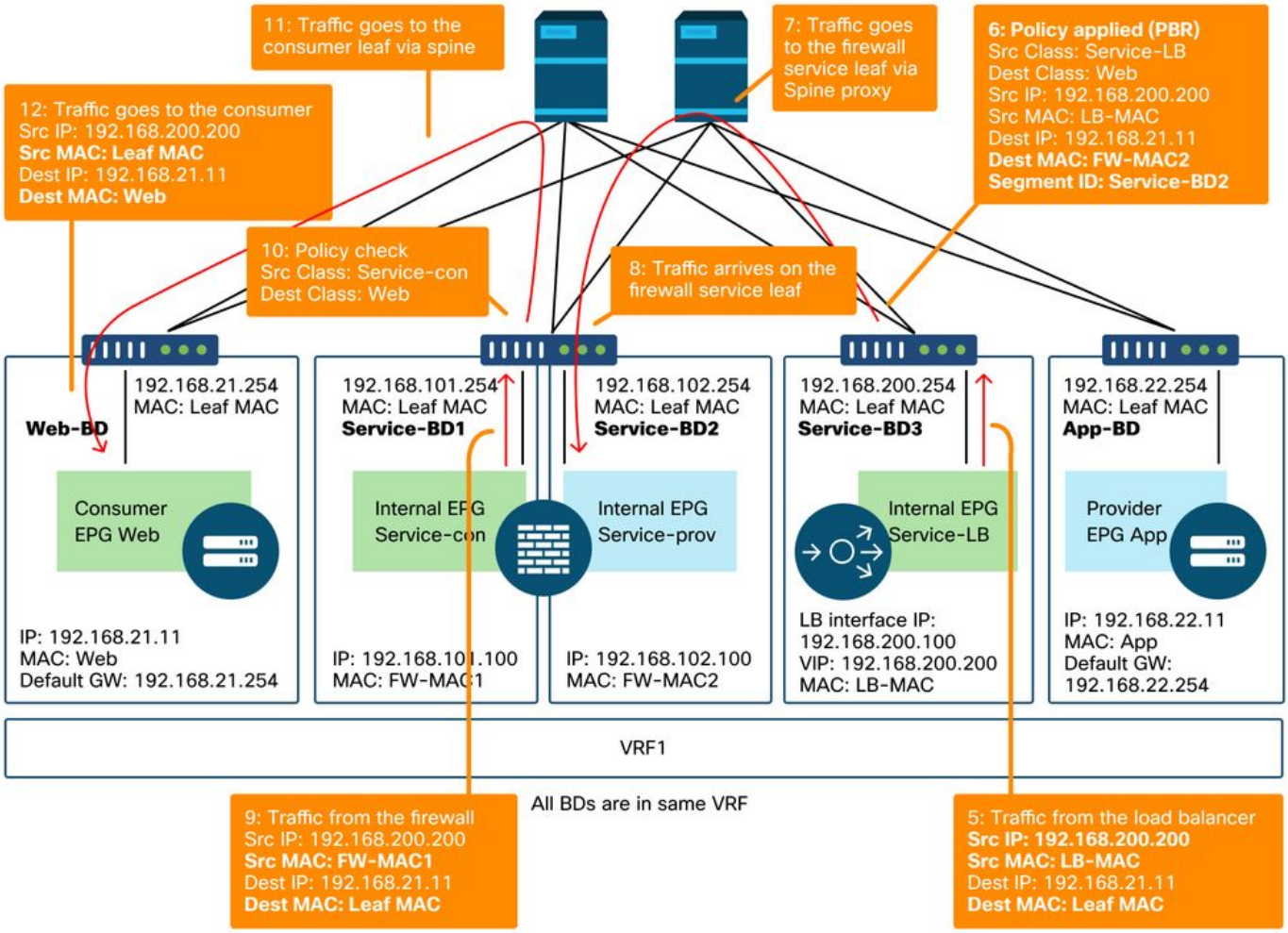


아래 그림에는 사업자 EPG 앱에서 소비자 EPG 웹으로의 반환 트래픽 흐름이 나와 있습니다. 반환 트래픽은 원래 소스 IP를 목적지로 하므로 반환 트래픽을 로드 밸런서로 되돌리려면 PBR이 필요합니다.

공급자 엔드포인트에서 소비자 엔드포인트로의 트래픽이 로드 밸런서로 리디렉션되면 로드 밸런서는 소스 IP를 VIP로 변경합니다. 트래픽은 로드 밸런서에서 돌아와 방화벽으로 리디렉션됩니다. 그런 다음 트래픽은 방화벽에서 다시 소비자 엔드포인트로 돌아갑니다.

SNAT 포워딩 경로가 없는 방화벽 및 로드 밸런서 예 - 공급자-소비자

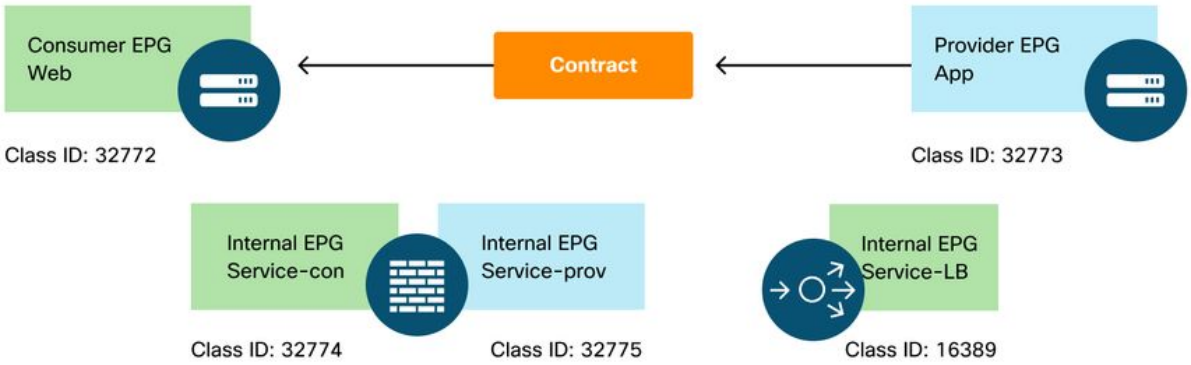

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254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



리프 노드에 프로그래밍된 정책

아래 그림과 아래에 표시된 'show zoning-rule' 출력은 서비스 그래프 구축 이후의 zoning-rule에 대해 설명합니다. 이 예에서 pcTag 32772(웹)에서 pcTag 16389(서비스-LB)로의 트래픽은 'destgrp-32'(방화벽의 소비자 측)로 리디렉션되고, pcTag 32773(앱)에서 pcTag 32772(웹)로의 트래픽은 'destgrp-33'(로드 밸런서)으로 리디렉션되며, pcTag 16389(서비스-LB)에서 pcTag 32772(웹)로의 트래픽은 'destgrp-34'(방화벽의 공급자 측)로 리디렉션됩니다.

서비스 그래프 구축 후 조닝 규칙 - SNAT가 없는 방화벽 및 로드 밸런서



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

위의 예에서 로드 밸런서의 공급자 측과 공급자 EPG 간의 연결에서 직접 연결 옵션은 'True'로 설정됩니다. 로드 밸런서에서 공급자 엔드포인트로의 상태 확인을 위해 활성화해야 합니다. 위치는 'Tenant(테넌트) > L4-L7 > Service Graph Templates(서비스 그래프 템플릿) > Policy(정책)'입니다. 그림 '직접 연결 옵션 설정'을 참조하십시오.

3. 공유 서비스(VRF 간 계약)

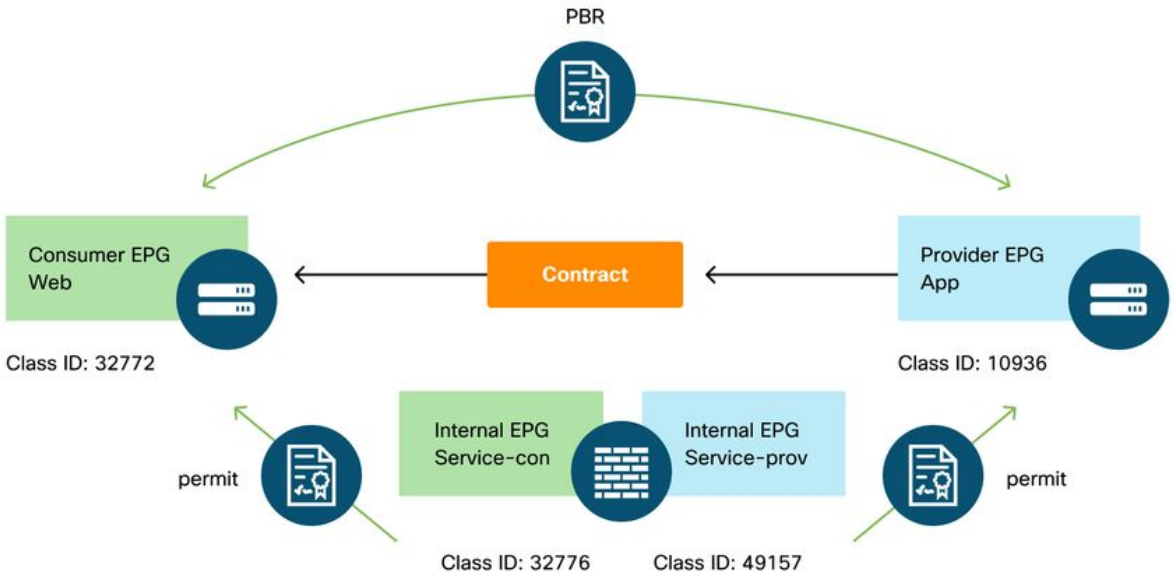
PBR은 VRF 간 계약에서 활성화할 수 있습니다. 이 섹션에서는 EPG와 EPG 간 VRF 계약의 경우 조닝 규칙이 어떻게 프로그래밍되는지 설명합니다.

리프 노드에 프로그래밍된 정책

EPG에서 EPG 간 VRF 계약인 경우, 정책은 항상 소비자 VRF에서 시행됩니다. 따라서 리디렉션은 소비자 VRF에서 수행됩니다. 다른 조합은 "정책이 적용되는 위치" 표를 참조하십시오. 섹션을 참조하십시오.

아래 그림과 'show zoning-rule' 출력은 서비스 그래프 구축 이후의 zoning-rule에 대해 설명합니다. 이 예에서는 pcTag 32772(웹)에서 pcTag 10936(앱)로의 트래픽이 'destgrp-36'(서비스 노드의 소비자 측)으로 리디렉션되고 pcTag 10936(앱)에서 pcTag 32772(웹)로의 트래픽은 'destgrp-35'(서비스 노드의 공급자 측)로 리디렉션됩니다. 둘 다 소비자 VRF인 VRF1에서 시행됩니다. pcTag 32776(방화벽의 소비자 측)에서 pcTag 32772(웹)로의 트래픽은 VRF1에서 허용됩니다.

서비스 그래프 구축 후 조닝 규칙 - VRF 간 계약



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

pcTag 49157(방화벽의 공급자 측)에서 pcTag 10936(App)로의 트래픽은 둘 다 VRF2에 있으므로 VRF2에서 허용됩니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.