

Fehlerbehebung: ACI-Richtlinienbasierte Umleitung

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Richtlinienbasierte Umleitung - Übersicht](#)

[Fehlerbehebung Service Graph Deployment](#)

[1. Konfigurationsschritte und Fehler prüfen](#)

[2. Überprüfen Sie die Bereitstellung von Servicediagrammen in der Benutzeroberfläche.](#)

[Fehlerbehebung: PBR-Weiterleitung](#)

[1. Überprüfen Sie, ob VLANs bereitgestellt und Endpunkte auf dem Leaf-Knoten gelernt wurden.](#)

[2. Überprüfen Sie die erwarteten Datenverkehrspfade](#)

[Wo werden die Richtlinien durchgesetzt?](#)

[3. Überprüfen Sie, ob der Datenverkehr zum Serviceknoten umgeleitet wird.](#)

[4. Überprüfen Sie die auf Leaf-Knoten programmierten Richtlinien.](#)

[Weitere Beispiele für den Datenfluss](#)

[1. Load Balancer ohne SNAT](#)

[Beispiel für Datenverkehrspfad](#)

[Die auf den Leaf-Knoten programmierten Richtlinien.](#)

[2. Beispiel für Datenverkehrsfluss - Firewall und Load Balancer ohne SNAT](#)

[Beispiel für Datenverkehrspfad](#)

[Die für die Leaf-Knoten programmierten Richtlinien](#)

[3. Shared Service \(Inter-VRF-Vertrag\)](#)

[Die für die Leaf-Knoten programmierten Richtlinien](#)

Einleitung

In diesem Dokument werden die Schritte zum Verständnis und zur Fehlerbehebung in einem ACI-PBR-Szenario (Policy-Based Redirect) beschrieben.

Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem Buch "[Troubleshooting Cisco Application Centric Infrastructure, Second Edition](#)" extrahiert, insbesondere aus dem Kapitel "Policy-Based Redirect - Overview", "Policy-Based Redirect - Service Graph Deployment", "Policy-Based Redirect" - "Forwarding" und "Policy-Based Redirect" - "Other traffic flow example" .

Richtlinienbasierte Umleitung - Übersicht

In diesem Kapitel wird die Fehlerbehebung im Servicediagramm für den nicht verwalteten Modus mit richtlinienbasierter Umleitung (Policy-Based Redirect, PBR) erläutert.

Im Folgenden sind typische Schritte zur Fehlerbehebung aufgeführt. In diesem Kapitel wird erläutert, wie Sie die PBR-spezifischen Schritte 2 und 3 überprüfen. Die Schritte 1 und 4 werden in den Kapiteln beschrieben: "Intra-Fabric Forwarding", "External Forwarding" und "Security Policies".

1. Prüfen Sie, ob der Datenverkehr ohne PBR-Servicediagramm funktioniert: Die Endgeräte von Verbrauchern und Anbietern werden erlernt. Die Kommunikation zwischen Endgeräten von Verbrauchern und Anbietern ist möglich.
2. Servicediagramm prüfen: Bereitgestellte Diagramminstanzen haben keinen Fehler. VLANs und Klassen-IDs für Service-Knoten werden bereitgestellt. Serviceknoten-Endpunkte werden erfasst.
3. Überprüfen Sie den Weiterleitungspfad: Die Prüfrichtlinie ist auf den Leaf-Knoten programmiert. Erfassen Sie den Datenverkehr auf dem Serviceknoten, um zu bestätigen, ob Datenverkehr umgeleitet wird. Erfassen Sie den Datenverkehr auf dem ACI-Leaf, um zu überprüfen, ob der Datenverkehr nach PBR zur ACI-Fabric zurückkehrt.
4. Überprüfen Sie, ob der Datenverkehr am Verbraucher- und Anbieterendpunkt ankommt und ob der Endpunkt den zurückkehrenden Datenverkehr generiert.

In diesem Dokument werden keine Design- oder Konfigurationsoptionen behandelt. Weitere Informationen finden Sie im "ACI PBR White Paper" unter Cisco.com

In diesem Kapitel implizieren Serviceknoten und Service-Leaf Folgendes:

- Serviceknoten - ein externer Knoten, zu dem der PBR den Datenverkehr umleitet, z. B. eine Firewall oder ein Load Balancer.
- Service-Leaf - Ein ACI-Leaf, der mit einem Service-Knoten verbunden ist.

Fehlerbehebung Service Graph Deployment

In diesem Kapitel wird ein Beispiel für die Fehlerbehebung erläutert, bei dem kein Servicediagramm bereitgestellt wird.

Nachdem eine Servicediagramm-Richtlinie definiert und auf einen Vertragsgegenstand angewendet wurde, sollte auf der ACI-GUI eine bereitgestellte Diagramminstanz angezeigt werden. Die folgende Abbildung zeigt ein Szenario zur Fehlerbehebung, bei dem das Servicediagramm nicht als bereitgestellt angezeigt wird.

Servicediagramm wird nicht als bereitgestellte Diagramminstanz angezeigt.

The screenshot shows the Cisco APIC interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Tenants' tab is active, and the breadcrumb trail is 'ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | Prod | PBR-Multinode | Symmetric-PBR'. The left sidebar shows a tree view under 'Prod' with folders for 'Application Profiles', 'Networking', 'Contracts', 'Policies', 'Services', and 'L4-L7'. The 'Services' and 'L4-L7' folders are highlighted with red boxes. The main content area shows a table titled 'Deployed Graph Instances' with columns for 'Service Graph', 'Contract', 'Contained By', 'State', and 'Description'. The table is currently empty, displaying 'No items have been found.'.

1. Konfigurationsschritte und Fehler prüfen

Der erste Schritt der Fehlerbehebung besteht darin, zu überprüfen, ob die erforderlichen Komponenten fehlerfrei konfiguriert wurden. Es wird davon ausgegangen, dass die folgenden allgemeinen Konfigurationen bereits vorgenommen wurden:

- VRF und BDs für Verbraucher-EPG, Provider-EPG und Service-Knoten
- Die Verbraucher- und Anbieter-EPG.
- Vertrag und Filter

Es sollte erwähnt werden, dass eine EPG für den Serviceknoten nicht manuell erstellt werden muss. Sie wird durch die Bereitstellung von Servicediagrammen erstellt.

Servicediagramm mit PBR-Konfigurationsschritten:

- Erstellen Sie das L4-L7-Gerät (logisches Gerät).
- Servicediagramm erstellen.
- Erstellen Sie die PBR-Richtlinie.
- Erstellen Sie die Richtlinie zur Geräteauswahl.
- Ordnen Sie das Servicediagramm dem Vertragsgegenstand zu.

2. Überprüfen Sie die Bereitstellung von Servicediagrammen in der Benutzeroberfläche.

Nachdem ein Servicediagramm dem Vertragssubjekt zugeordnet wurde, sollte für jeden Vertrag mit Servicediagramm eine bereitgestellte Diagramminstanz angezeigt werden (Abbildung unten).

Der Speicherort lautet "Tenant > Services > L4-L7 > Deployed Graph Instances".

Bereitgestellte Diagramminstanz

The screenshot shows the Cisco APIC interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrati'. The 'Tenants' tab is active, showing a search bar and filters for 'common', 'Prod', 'PBR-Multinode', and 'Symmetric-PBR'. The left sidebar is expanded to 'Prod' > 'Services' > 'L4-L7' > 'Deployed Graph Instances' > 'web-to-app-FW-Prod'. The main content area shows the 'L4-L7 Service Graph Instance - web-to-app-FW-Prod' with tabs for 'Topology', 'Policy', 'Faults', and 'History'. The 'Topology' tab is selected, displaying a diagram with a 'Consumer' EPG (Web) connected to a 'Provider' EPG (App) via a central node 'node1' (Prod-ASAv...). Below the diagram is a 'node1 Information' section with the following details: Contract: Prod/web-to-app, Graph: Prod/FW, Node: node1, Device Cluster: Prod-ASAv-VM1, Firewall: routed, Policy-Based: true, Redirect: true. A 'Show Usage' button is located at the bottom right.

Wenn eine bereitgestellte Diagramminstanz nicht angezeigt wird, stimmt etwas mit der Vertragskonfiguration nicht. Die wichtigsten Gründe hierfür sind:

- Der Vertrag hat keine Consumer- oder Provider-EPG.
- Der Vertragsgegenstand hat keinen Filter.
- Der Vertragsbereich umfasst VRF, obwohl es für die Kommunikation zwischen VRFs oder zwischen Tenants vorgesehen ist.

Wenn die Servicediagramm-Instanziierung fehlschlägt, werden Fehler in der bereitgestellten Diagramminstanz ausgelöst, was bedeutet, dass die Servicediagramm-Konfiguration fehlerhaft ist. Typische Fehler, die durch die Konfiguration verursacht werden:

F1690: Die Konfiguration ist aufgrund eines Fehlers bei der ID-Zuweisung ungültig.

Dieser Fehler zeigt an, dass das gekapselte VLAN für den Serviceknoten nicht verfügbar ist. So ist beispielsweise im VLAN-Pool, der mit der im logischen Gerät verwendeten VMM-Domäne verknüpft ist, kein dynamisches VLAN verfügbar.

Auflösung: Überprüfen Sie den VLAN-Pool in der Domäne, die für das logische Gerät verwendet wird. Überprüfen Sie das gekapselte VLAN in der Schnittstelle für logische Geräte, wenn es sich in einer physischen Domäne befindet. Die Standorte sind "Tenant > Services > L4-L7 > Devices and Fabric > Access Policies > Pools > VLAN".

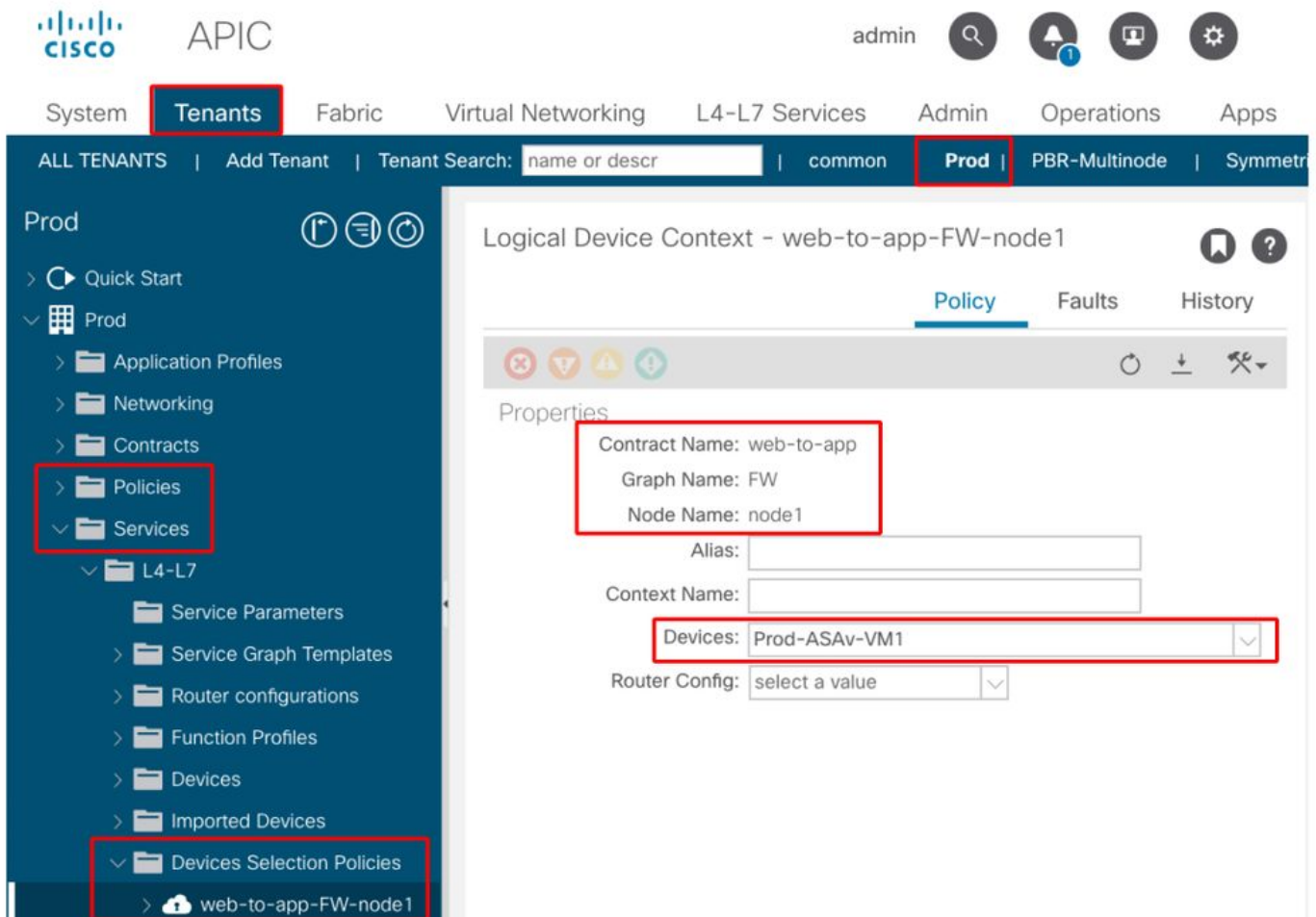
F1690: Konfiguration ist ungültig, da kein Gerätekontext für LDev gefunden wurde

Dieser Fehler weist darauf hin, dass das logische Gerät für das Servicediagramm-Rendering nicht gefunden werden kann. Es gibt beispielsweise keine mit dem Servicediagramm übereinstimmende

Richtlinie für die Geräteauswahl für den Vertrag.

Auflösung: Überprüfen Sie, ob die Richtlinie zur Geräteauswahl definiert ist. Die Richtlinie zur Geräteauswahl stellt ein Auswahlkriterium für ein Service-Gerät und dessen Anschlüsse bereit. Die Kriterien basieren auf einem Vertragsnamen, einem Servicediagrammenamen und einem Knotennamen im Servicediagramm. Der Standort lautet "Tenant > Services > L4-L7 > Device Selection Policy" (Tenant > Dienste > L4-L7 > Geräteauswahlrichtlinie).

Richtlinie zur Geräteauswahl überprüfen



F1690: Konfiguration ist ungültig, da keine Clusterschnittstelle gefunden wurde.

Dieser Fehler zeigt an, dass die Clusterschnittstelle für den Dienstknoten nicht gefunden wurde. Die Cluster-Schnittstelle ist beispielsweise in der Richtlinie zur Geräteauswahl nicht angegeben.

Auflösung: Überprüfen Sie, ob die Cluster-Schnittstelle in der Richtlinie für die Geräteauswahl angegeben ist und der Connector-Name richtig ist (Abbildung unten).

F1690: Konfiguration ist ungültig, da kein BD gefunden wurde

Dieser Fehler zeigt an, dass der BD für den Serviceknoten nicht gefunden wurde. Der BD ist beispielsweise in der Richtlinie zur Geräteauswahl nicht angegeben.

Auflösung: Prüfen Sie, ob BD in der Richtlinie für die Geräteauswahl angegeben ist, und der Connectorname ist richtig (Abbildung unten).

F1690: Die Konfiguration ist aufgrund einer ungültigen Richtlinie für die Dienstumleitung ungültig.

Dieser Fehler weist darauf hin, dass die PBR-Richtlinie nicht ausgewählt ist, obwohl die Umleitung für die Service-Funktion im Servicediagramm aktiviert ist.

Auflösung: Wählen Sie in der Richtlinie zur Geräteauswahl die Option PBR-Richtlinie aus (Abbildung unten).

Konfiguration der logischen Schnittstelle in der Richtlinie zur Geräteauswahl

The screenshot displays the Cisco APIC interface for configuring a Logical Interface Context. The left navigation pane shows the path: Prod > Services > L4-L7 > Devices Selection Policies > web-to-app-FW-node1 > consumer. The main configuration area is titled 'Logical Interface Context - consumer' and has tabs for Policy, Faults, and History. The Policy tab is active, showing a 'Properties' section with various configuration fields. A red box highlights the 'Connector Name: consumer', 'Cluster Interface: consumer', 'Associated Network: Bridge Domain', and 'Bridge Domain: Service-BD1'. Another red box highlights the 'L4-L7 Policy-Based Redirect: ASA-external' field. At the bottom, there are buttons for 'Show Usage', 'Reset', and 'Submit'.

Fehlerbehebung: PBR-Weiterleitung

In diesem Kapitel werden die Schritte zur Fehlerbehebung für den PBR-Weiterleitungspfad erläutert.

1. Überprüfen Sie, ob VLANs bereitgestellt und Endpunkte auf dem Leaf-Knoten gelernt wurden.

Sobald ein Servicediagramm fehlerfrei erfolgreich bereitgestellt wurde, werden EPGs und BDs für einen Serviceknoten erstellt. Die folgende Abbildung zeigt, wo Sie die gekapselten VLAN-IDs und Klassen-IDs der Service-Knoten-Schnittstellen (Service-EPGs) finden. In diesem Beispiel ist die Verbraucherseite einer Firewall die Klasse ID 16386 mit VLAN Encap 1000, und die Anbieterseite einer Firewall die Klasse ID 49157 mit VLAN Encap 1102.

Der Speicherort lautet "Tenant > Services > L4-L7 > Bereitgestellte Diagramminstanzen >

Funktionsknoten".

Serviceknoten

The screenshot shows the Cisco APIC interface for configuring a Function Node. The left sidebar has 'L4-L7' and 'Service Parameters' highlighted. The main content area shows the 'Function Node - node1' configuration page. The 'Function Connectors' table is highlighted with a red box, showing columns for Name, Encap, and Class ID.

Name	Encap	Class ID
consumer	vlan-1000	16386
provider	vlan-1102	49157

Serviceknoten-Schnittstellenklassen-ID

The screenshot shows the Cisco APIC interface for configuring a Function Node. The 'Function Connectors' table is highlighted with a red box, showing columns for Name, Encap, and Class ID.

Name	Encap	Class ID
consumer	vlan-1000	16386
provider	vlan-1102	49157

Diese VLANs werden an den Schnittstellen der Service-Leaf-Knoten bereitgestellt, mit denen die Service-Knoten verbunden sind. Die VLAN-Bereitstellung und der Endpunkt-Lernstatus können mithilfe von "show vlan extended" und "show endpoint" in der CLI des Service-Leaf-Knotens überprüft werden.

```
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
pol
Prod:VRF1   vlan-1000      192.168.101.100 LV
pol
59          vlan-1102      0050.56af.1c44 LV
pol
Prod:VRF1   vlan-1102      192.168.102.100 LV
pol
```

Wenn die Endpunkt-IPs der Serviceknoten nicht als Endpunkte in der ACI-Fabric erfasst werden, handelt es sich höchstwahrscheinlich um ein Verbindungs- oder Konfigurationsproblem zwischen dem Service-Leaf und dem Serviceknoten. Überprüfen Sie die folgenden Status:

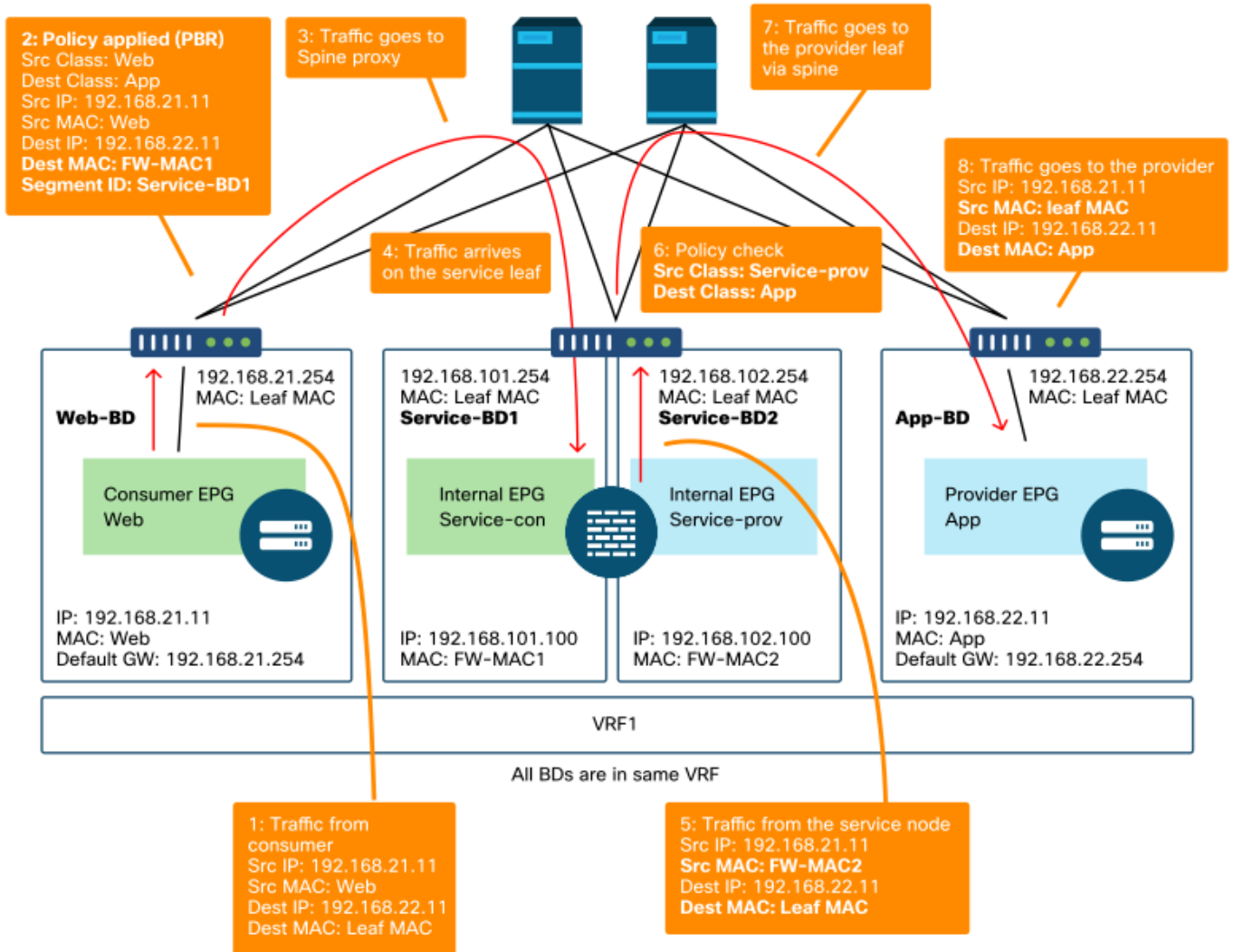
- Der Serviceknoten ist mit dem richtigen Leaf-Downlink-Port verbunden. Wenn sich der Serviceknoten in einer physischen Domäne befindet, muss das VLAN des statischen Endpfads des Leafs im logischen Gerät definiert werden. Wenn sich der Serviceknoten in einer VMM-Domäne befindet, überprüfen Sie, ob die VMM-Domäne funktioniert und ob die über Servicediagramm erstellte Portgruppe korrekt an den Serviceknoten VM angefügt ist.
- Der Leaf-Downlink-Port, der mit dem Serviceknoten oder Hypervisor verbunden ist, auf dem sich der Serviceknoten VM befindet, ist UP.
- Der Serviceknoten hat das richtige VLAN und die richtige IP-Adresse.
- Der Zwischen-Switch zwischen dem Service-Leaf und dem Service-Knoten verfügt über die richtige VLAN-Konfiguration.

2. Überprüfen Sie die erwarteten Datenverkehrspfade

Wenn der End-to-End-Datenverkehr nach Aktivierung von PBR nicht mehr funktioniert, obwohl die Serviceknoten-Endpunkte in der ACI-Fabric erfasst werden, besteht der nächste Schritt zur Fehlerbehebung darin, die erwarteten Datenverkehrspfade zu überprüfen.

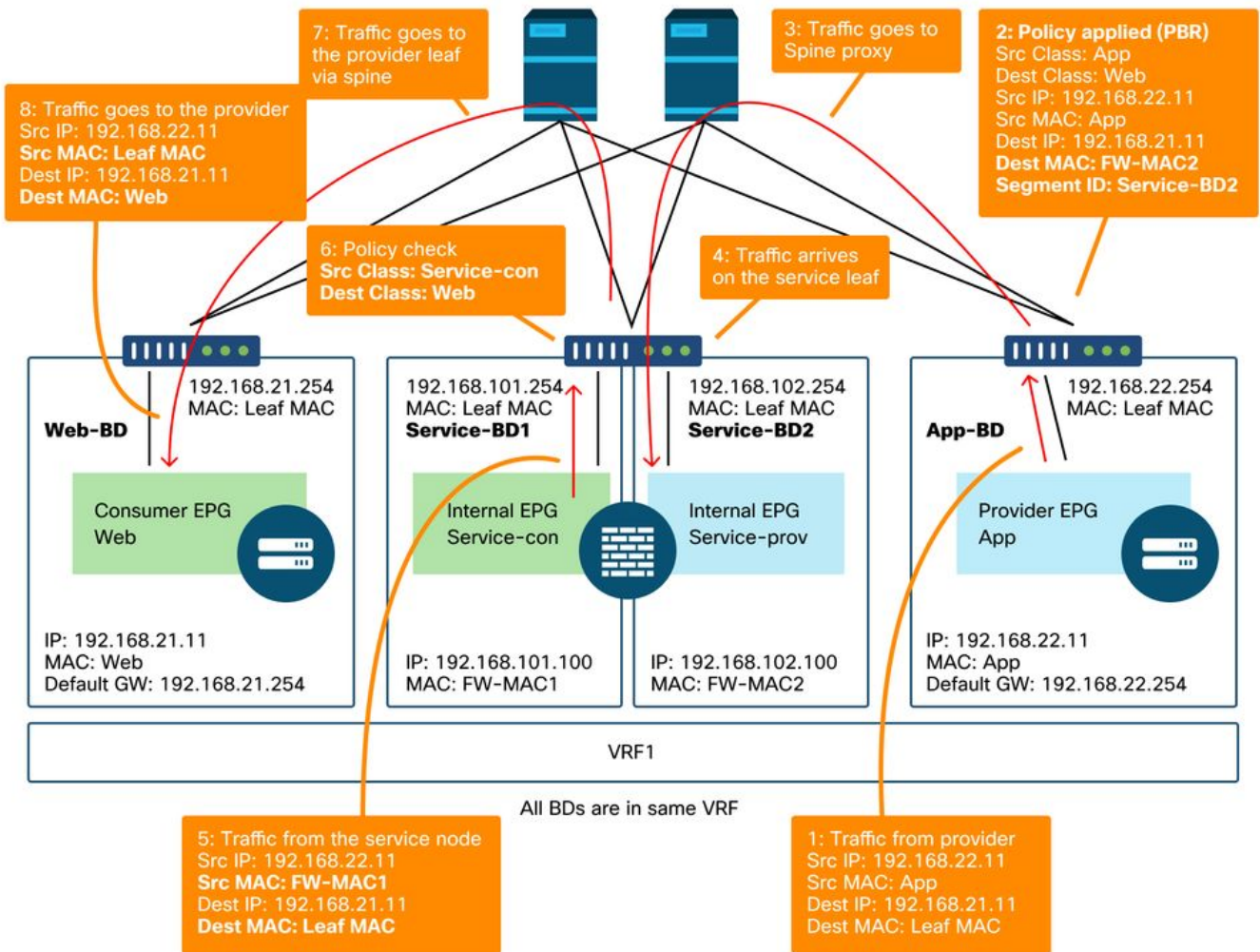
Die Abbildungen "PBR Forwarding Path Example - Consumer to Provider" und "PBR Forwarding Path Example - Provider to Consumer" veranschaulichen ein Beispiel für einen Weiterleitungspfad, bei dem eine Firewall mithilfe von PBR zwischen einem Consumerendpunkt und einem Anbieterendpunkt eingefügt wird. Es wird davon ausgegangen, dass die Endpunkte bereits auf Leaf-Knoten gelernt werden.

Beispiel für einen PBR-Weiterleitungspfad - Verbraucher an Anbieter



Hinweis: Da die Quell-MAC nicht in ACI-Leaf-MAC geändert wird, darf der PBR-Knoten keine Quell-MAC-basierte Weiterleitung verwenden, wenn Endpunkt und PBR-Knoten des Verbrauchers nicht im selben BD sind.

Beispiel für einen PBR-Weiterleitungspfad - Provider an Verbraucher



Anmerkung: Es sollte erwähnt werden, dass die PBR-Richtlinie entweder auf dem Consumer- oder auf dem Provider-Leaf durchgesetzt wird. ACI PBR bewirkt eine MAC-Zielumschreibung, wie in den Abbildungen "PBR Forwarding Path Example - Consumer to Provider" und "PBR Forwarding Path Example - Provider to Consumer" dargestellt. Beim Erreichen der PBR-Ziel-MAC-Adresse wird immer ein Spine-Proxy verwendet, selbst wenn sich der Quell-Endpunkt und die PBR-Ziel-MAC unter demselben Leaf befinden.

Obwohl die Abbildungen "PBR Forwarding Path Example - Consumer to Provider" und "PBR Forwarding Path Example - Provider to Consumer" ein Beispiel dafür zeigen, wo der Datenverkehr umgeleitet würde, hängt die Durchsetzung der Richtlinie von der Vertragskonfiguration und dem Endpunkt-Lernstatus ab. In der Tabelle "Where policy is enforced" (Wo wird die Richtlinie durchgesetzt) wird zusammengefasst, wo an einem einzelnen ACI-Standort die Richtlinie durchgesetzt wird. Bei der Durchsetzung von Richtlinien über mehrere Standorte gibt es Unterschiede.

Wo werden die Richtlinien durchgesetzt?

Szenario	VRF- Erzwingungsmodus	Verbraucher	Anbieter	Durchsetzung der Richtlinie am
Intra-VRF	Eingang/Ausgang	EPG	EPG	<ul style="list-style-type: none"> • Wenn der Zielpunkt erfasst wird: Eingangsblatt* • Wenn der Zielpunkt nicht erfasst

			wird: Ausgangsblatt	
Eingang	EPG	L3Out-EPG	Verbraucher-Leaf	
Eingang	L3Out-EPG	EPG	Provider-Leaf (ohne Border Leaf)	
Ausgehend	EPG	L3Out-EPG	Grenz-Leaf -> Nicht-Grenz-Leaf-Verkehr <ul style="list-style-type: none"> • Wenn der Zielendpunkt erfasst wird: Randblatt • Wenn der Zielendpunkt nicht erfasst wird: unbegrenztes Blatt 	
Ausgehend	L3Out-EPG	EPG	Nicht grenzübergreifender Leaf-> Grenz-Leaf-Datenverkehr <ul style="list-style-type: none"> • Grenz-Blatt 	
Eingang/Ausgang	L3Out-EPG	L3Out-EPG	Eingangs-Leaf*	
Eingang/Ausgang	EPG	EPG	Verbraucher-Leaf	
Eingang/Ausgang	EPG	L3Out-EPG	Verbraucher-Leaf	
Inter-VRF	Eingang/Ausgang	L3Out-EPG	EPG	Eingangs-Leaf*
	Eingang/Ausgang	L3Out-EPG	L3Out-EPG	Eingangs-Leaf*

* Die Richtliniendurchsetzung wird auf den ersten Leaf angewendet, der vom Paket betroffen ist.

Dies sind Beispiele:

- Wenn ein externer Endpunkt in der L3Out-EPG in VRF1 versucht, auf einen Endpunkt in der Web-EPG in VRF1 zuzugreifen, und VRF1 für den Durchsetzungseingangsmodus konfiguriert ist, wird der Datenverkehr unabhängig von der Vertragsrichtung über das Leaf umgeleitet, auf dem sich der Endpunkt in der Web-EPG befindet.
- Wenn ein Endpunkt in der Web-EPG eines Verbrauchers in VRF1 versucht, auf einen Endpunkt in der App-EPG des Anbieters in VRF1 zuzugreifen, und die Endpunkte auf Consumer- und Provider-Leaf-Knoten erfasst werden, wird der Datenverkehr vom Eingangs-Leaf umgeleitet.
- Wenn ein Endpunkt in der Web-EPG eines Verbrauchers in VRF1 versucht, auf einen Endpunkt in der App-EPG des Anbieters in VRF2 zuzugreifen, wird der Datenverkehr unabhängig vom VRF-Erzwingungsmodus vom Consumer-Leaf umgeleitet, auf dem sich der Consumerendpunkt befindet.

3. Überprüfen Sie, ob der Datenverkehr zum Serviceknoten umgeleitet wird.

Sobald der erwartete Weiterleitungspfad frei ist, kann mithilfe von ELAM überprüft werden, ob Datenverkehr an den Switch-Knoten eingeht, und die Weiterleitungsentscheidung kann an den Switch-Knoten überprüft werden. Anweisungen zur Verwendung von ELAM finden Sie im Abschnitt "Tools" im Kapitel "Intra-Fabric Forwarding".

Um beispielsweise den Datenverkehrsfluss in der Abbildung "PBR-Weiterleitungspfad Beispiel - Consumer zu Provider" nachzuverfolgen, können diese erfasst werden, um zu bestätigen, ob Datenverkehr von Consumer zu Provider umgeleitet wird.

- Downlink-Port auf Consumer-Leaf zu Check 1 und 2 (Datenverkehr kommt auf Consumer-Leaf an und PBR wird durchgesetzt).
- Fabric-Port an Spine-Knoten für Prüfung 3 (Datenverkehr geht an Spine-Proxy).
- Fabric-Port am Service-Leaf für Prüfung 4 (Datenverkehr kommt am Service-Leaf an).

Diese können dann erfasst werden, um zu bestätigen, ob der Datenverkehr, der vom Serviceknoten zurückkommt, an den Anbieter geht.

- Downlink-Port am Service-Leaf zu Prüfung 5 und 6 (Datenverkehr kommt vom Service-Knoten zurück und ist zulässig).
- Fabric-Port an Spine-Knoten für Prüfung 7 (Datenverkehr wird über Spine an Provider-Leaf weitergeleitet).
- Fabric-Port am Provider-Leaf für Prüfung von 8 (Datenverkehr kommt am Service-Leaf an und geht zum Provider-Endpunkt).

Anmerkung: Wenn sich Consumer- und Serviceknoten unter demselben Leaf befinden, geben Sie eine Schnittstelle oder Quell-MAC zusätzlich zur Quell-/Ziel-IP an, damit ELAM 1 oder 5 in der Abbildung 'Beispiel für PBR-Weiterleitungspfad - Consumer an Anbieter' überprüft, da beide dieselbe Quell-IP und Ziel-IP verwenden.

Wenn der Datenverkehr vom Verbraucher zum Anbieter zum Serviceknoten umgeleitet wird, aber nicht zum Service-Leaf zurückkehrt, überprüfen Sie die folgenden Punkte, da es sich um häufige Fehler handelt:

- Die Serviceknoten-Routingtabelle erreicht das Provider-Subnetz.
- Eine Sicherheitsrichtlinie für Serviceknoten wie die ACL lässt den Datenverkehr zu.

Wenn der Datenverkehr umgeleitet wird und beim Provider eingeht, überprüfen Sie den Pfad zum zurückkehrenden Datenverkehr vom Provider zum Verbraucher auf ähnliche Weise.

4. Überprüfen Sie die auf Leaf-Knoten programmierten Richtlinien.

Wenn der Datenverkehr nicht entsprechend weitergeleitet oder umgeleitet wird, besteht der nächste Fehlerbehebungsschritt darin, die auf den Leaf-Knoten programmierten Richtlinien zu überprüfen. In diesem Abschnitt werden Zoning-Rule und Contract_Parser als Beispiele dargestellt. Weitere Informationen zum Überprüfen von Zoning-Regeln finden Sie im Abschnitt "Tools" im Kapitel "Sicherheitsrichtlinien".

Anmerkung: Die Richtlinien werden basierend auf dem EPG-Bereitstellungsstatus auf dem Leaf programmiert. Bei der Ausgabe des Befehls show in diesem Abschnitt wird das Leaf verwendet, das über eine Consumer-EPG, eine Provider-EPG und EPGs für den Dienstknoten verfügt.

Verwenden des Befehls "show zoning-rule"

Die folgende Abbildung und die Ausgabe von "show zoning-rule" beschreiben die Zoning-Regeln vor der Bereitstellung von Service Graph.



Die VRF-Bereichs-ID finden Sie unter "Tenant > Networking > VRF".

```
Pod1-Leaf1# show zoning-rule scope 2752513
```

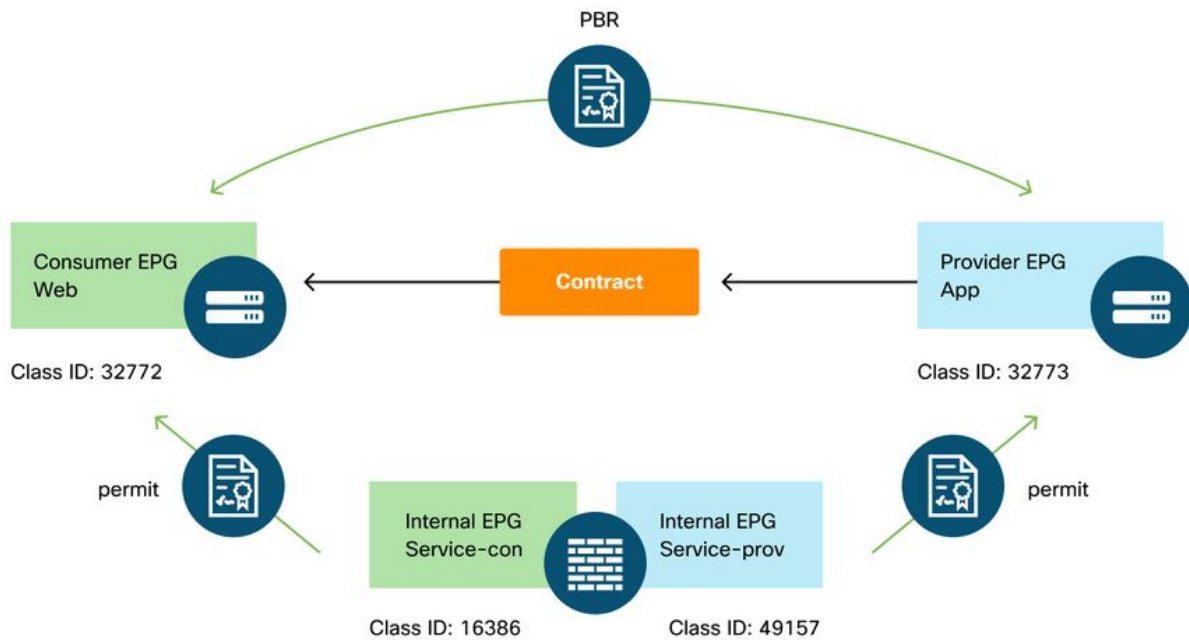
```

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

```

Nach der Bereitstellung des Servicediagramms werden EPGs für den Serviceknoten erstellt, und Richtlinien werden aktualisiert, um den Datenverkehr zwischen den Consumer- und den Provider-EPGs umzuleiten. Die folgende Abbildung und die Ausgabe von "show zoning-rule" beschreiben die Zoning-Regeln nach der Bereitstellung von Service Graph. In diesem Beispiel wird der Datenverkehr von pcTag 32772 (Web) zu pcTag 32773 (App) zu 'destgrp-27' (Consumerseite des Dienstknotens) umgeleitet, und der Datenverkehr von pcTag 32773 (App) zu pcTag 32772 (Web) wird zu 'destgrp-28' (Anbieterseite des Dienstknotens) umgeleitet.

Zoning-Regeln nach der Bereitstellung von Servicediagrammen



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

```

Die Zielinformationen der einzelnen Destgrp können mit dem Befehl "show service redir info" gefunden werden.

```
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
...

```

Wenn Zoning-Regeln entsprechend programmiert sind, der Datenverkehr jedoch nicht entsprechend umgeleitet oder weitergeleitet wird, überprüfen Sie bitte die folgenden Punkte, da es sich um häufige Fehler handelt:

- Überprüfen Sie, ob die Quell- oder Zielklassen-ID wie erwartet mithilfe von ELAM aufgelöst wird. Wenn nicht, überprüfen Sie die falsche Klassen-ID und die EPG-Ableitungskriterien wie Pfad und Encap-VLAN.
- Obwohl die Quell- und Zielklassen-IDs entsprechend aufgelöst werden und die PBR-Richtlinie angewendet wird, aber der Datenverkehr nicht am PBR-Knoten ankommt, überprüfen Sie die IP-, MAC- und VRF-Adresse des Destgrp in der Umleitungsaktion ("show service redir info").

Standardmäßig sind Zulassungsregeln für eine Consumerkennung zu einem Serviceknoten (Consumerseite) und eine Provider-EPG zu einem Serviceknoten (Anbieterseite) nicht programmiert, wenn PBR aktiviert ist. Daher kann ein Consumerendpunkt oder ein Anbieterendpunkt standardmäßig nicht direkt mit dem Dienstknoten kommunizieren. Um diesen Datenverkehr zuzulassen, muss die Option "Direct Connect" aktiviert sein. Der Anwendungsfall wird im Abschnitt "Beispiele für andere Datenverkehrsflüsse" **erläutert**.

Verwendung von contract_parser

Das contract_parser-Tool kann ebenfalls bei der Überprüfung der Richtlinien helfen. C-consumer ist die Consumerseite des Dienstknotens und C-provider die Anbieterseite des Dienstknotens.

```

Pod1-Leaf1# contract_parser.py --vrf Prod:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-14] dst-epg [dst-14]
[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-  
appl/epg-App(32773) [contract:uni/tn-Prod/brc-web-to-app] [hit=15]
```

...

Weitere Beispiele für den Datenfluss

In diesem Abschnitt werden weitere gängige Beispiele für den Datenverkehrsfluss behandelt, um die gewünschten Datenflüsse für die Fehlerbehebung zu identifizieren. Die Schritte zur Fehlerbehebung finden Sie im vorherigen Kapitel in diesem Abschnitt.

1. Load Balancer ohne SNAT: In diesem Beispiel haben Consumer-EPG-Web und Anbieter-EPG-App einen Vertrag mit einem Load Balancer-Servicediagramm. Endpunkte in der Anwendungs-EPG sind echte Server, die mit dem VIP auf dem Load Balancer verknüpft sind. PBR zum Load Balancer ist für die Datenverkehrsrichtung von Anbieter zu Verbraucher aktiviert.
2. Firewall und Load Balancer ohne SNAT: In diesem Beispiel haben Consumer-EPG-Web und Anbieter-EPG-App einen Vertrag mit einer Firewall und einem Load Balancer-Servicediagramm. Endpunkte in der Anwendungs-EPG sind echte Server, die mit dem VIP on load balancer verknüpft sind. PBR zur Firewall ist für beide Richtungen aktiviert. PBR zum Load Balancer ist für die Datenverkehrsrichtung von Anbieter zu Verbraucher aktiviert.
3. Shared Service (Inter-VRF-Vertrag): In diesem Beispiel haben Consumer-EPG-Web und Anbieter-EPG-App einen Vertrag mit einem Firewall-Servicediagramm. EPG Web und EPG App sind in verschiedenen VRFs. PBR zur Firewall ist für beide Richtungen aktiviert. Die Firewall befindet sich zwischen den VRFs.

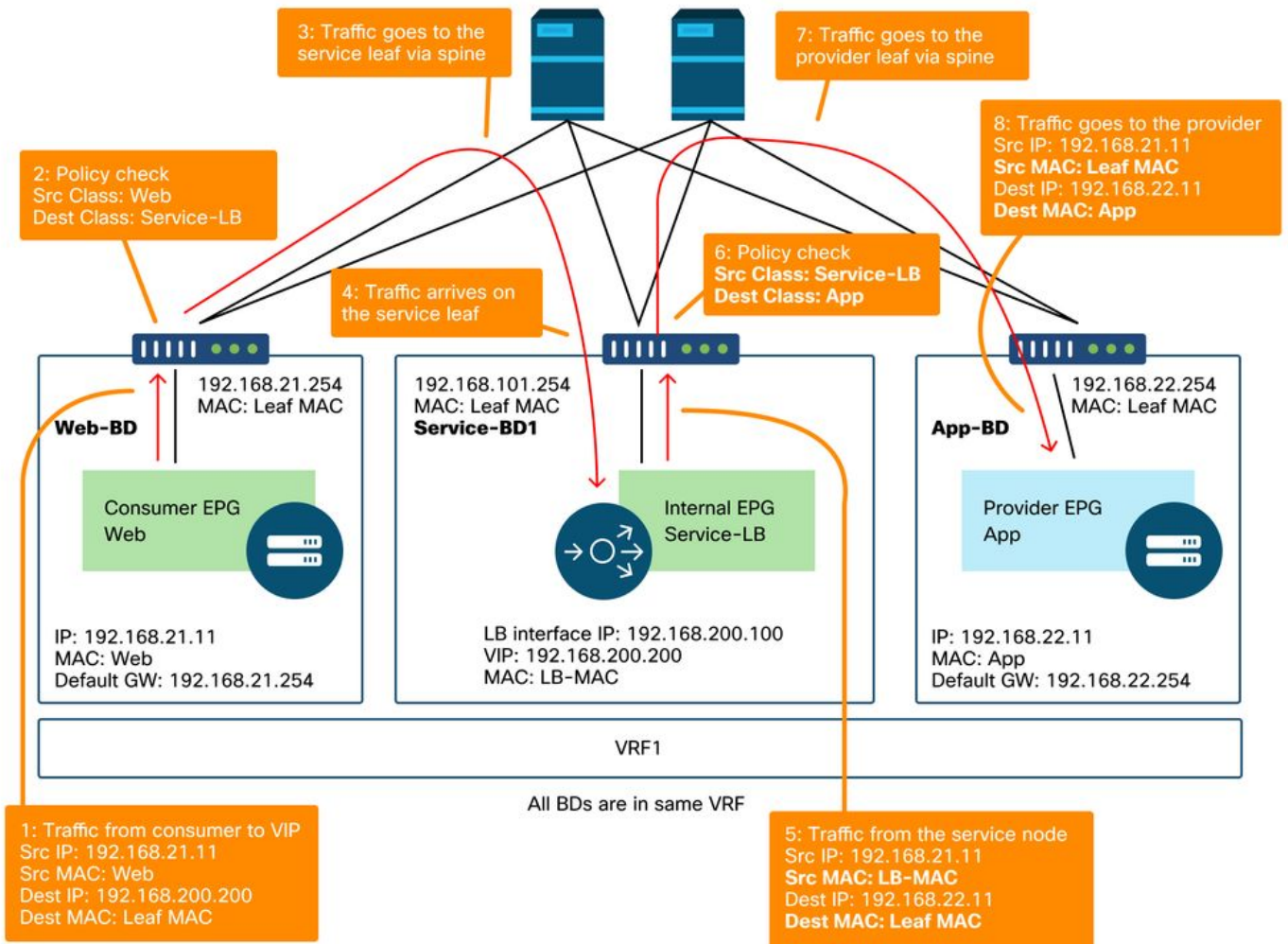
1. Load Balancer ohne SNAT

PBR kann als bidirektionaler PBR oder unidirektionaler PBR bereitgestellt werden. Ein Anwendungsfall für ein unidirektionales PBR ist die Load Balancer-Integration ohne Network Address Translation (NAT). Wenn der Load Balancer eine Quell-NAT durchführt, ist kein PBR erforderlich.

Beispiel für Datenverkehrspfad

Die folgende Abbildung zeigt ein Beispiel für einen eingehenden Datenverkehrsfluss von Consumer-EPG-Web zu Provider-EPG-App mit zwei Verbindungen: Der eine stammt von einem Endpunkt im Consumer-EPG-Web zum Load Balancer-VIP, der andere vom Load Balancer zum Endpunkt in der Anbieter-EPG-App. Da der eingehende Datenverkehr für die VIP bestimmt ist, wird der Datenverkehr ohne PBR an den Load Balancer weitergeleitet, sofern der VIP erreichbar ist. Der Load Balancer ändert die Ziel-IP in eines der Endpunkte in der EPG-Anwendung, die dem VIP zugeordnet ist, übersetzt jedoch nicht die Quell-IP. Dementsprechend wird der Datenverkehr an den Anbieterendpunkt weitergeleitet.

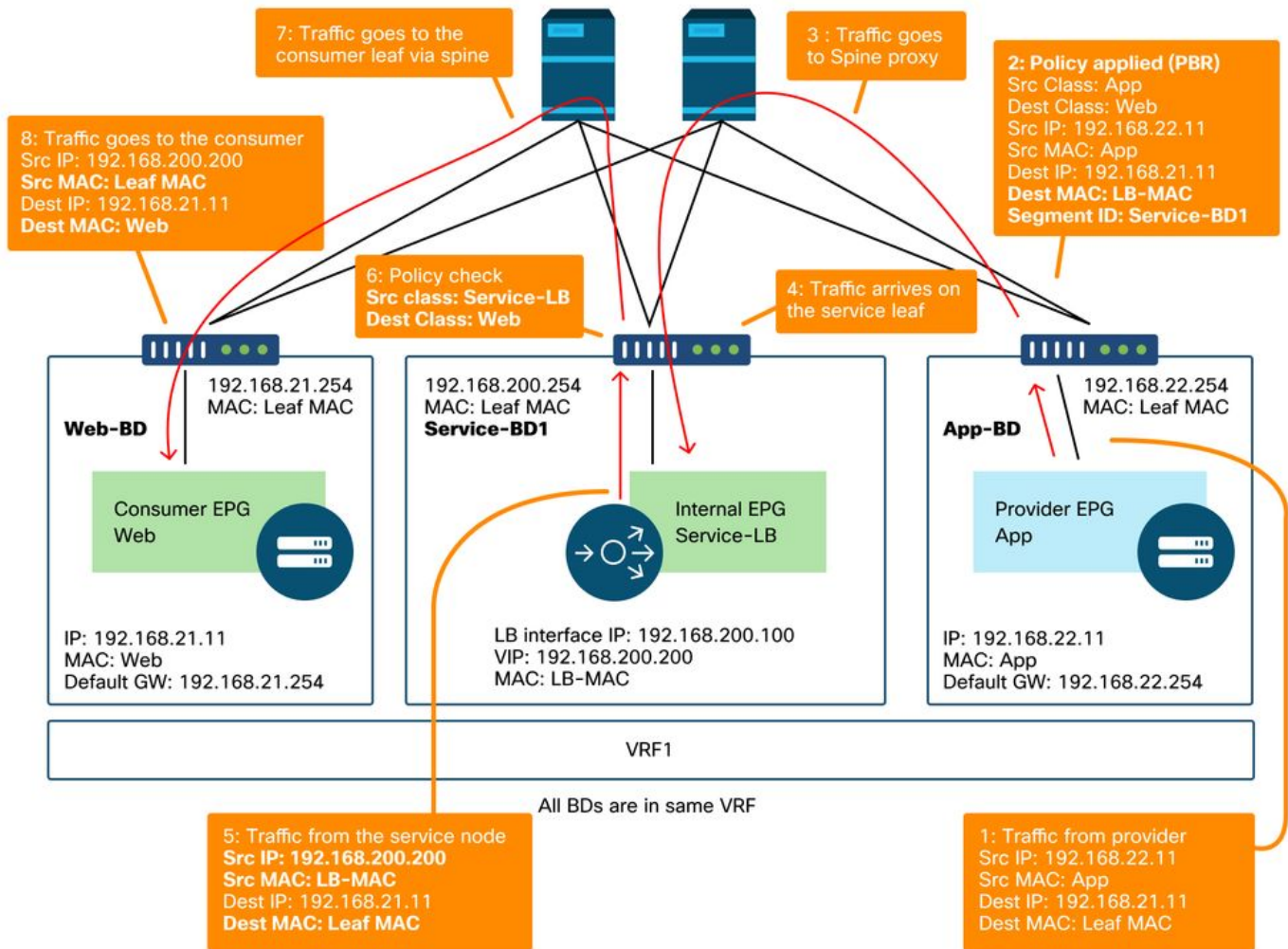
Load Balancer ohne SNAT-Weiterleitungspfad - Beispiel: Verbraucher an VIP und Load Balancer an Anbieter ohne PBR



In der folgenden Abbildung wird der Datenrückfluss von der Provider-EPG-App zum EPG-Web für Privatnutzer dargestellt. Da der zurückgeleitete Datenverkehr an die ursprüngliche Quell-IP gerichtet ist, muss PBR den zurückgeleiteten Datenverkehr zum Load Balancer zurückleiten. Andernfalls empfängt der Consumer-Endpoint den Datenverkehr, wobei die Quell-IP der Anbieter-Endpoint und nicht die VIP ist. Dieser Datenverkehr wird verworfen, da der Endpunkt des Verbrauchers keinen Datenverkehr zum Anbieter-Endpoint initiiert hat, selbst wenn das zwischengeschaltete Netzwerk wie die ACI-Fabric das Paket an den Endpunkt des Verbrauchers weiterleitet.

Nachdem der Datenverkehr vom Anbieter-Endpoint zum Verbraucher-Endpoint zum Load Balancer umgeleitet wurde, ändert der Load Balancer die Quell-IP in die VIP. Anschließend wird der Datenverkehr vom Load Balancer und zurück zum Endpunkt des Verbrauchers geleitet.

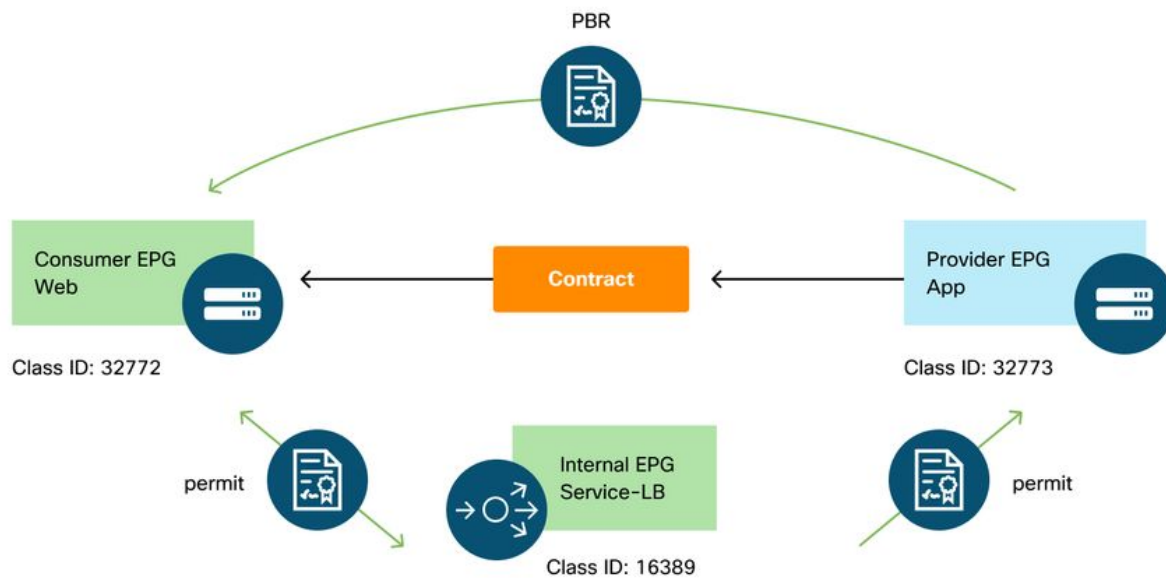
Load Balancer ohne SNAT-Weiterleitungspfad - Beispiel: Anbieter an Verbraucher mit PBR



Die auf den Leaf-Knoten programmierten Richtlinien.

Die folgende Abbildung und die Ausgabe von "show zoning-rule" beschreiben die Zoning-Regeln nach der Bereitstellung von Service Graph. In diesem Beispiel ist der Datenverkehr von pcTag 32772 (Web) zu pcTag 16389 (Service-LB) zulässig, der Datenverkehr von pcTag 16389 (Service-LB) zu pcTag 32773 (App) ist zulässig, und der Datenverkehr von pcTag 32773 (App) zu pcTag 32772 (Web) wird zu "destgrp-31" (Load Balancer) umgeleitet.

Zoning-Regeln nach Service Graph-Bereitstellung - Load Balancer ohne 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
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)					

Standardmäßig ist keine Zulässigkeitsregel für die Provider-EPG (pcTag 32773) zu Service-LB (pcTag 16389) programmiert. Um eine bidirektionale Kommunikation zwischen ihnen für Statusprüfungen vom Load Balancer zum Anbieterendpunkt zuzulassen, muss die Option "Direct Connect" für die Verbindung auf "True" festgelegt werden. Der Speicherort lautet "Tenant > L4-L7 > Servicediagramm-Vorlagen > Richtlinie". Der Standardwert ist False.

Direct Connect-Option festlegen

admin

System Tenants Fabric Virtual Networking L4-L7 Services Admin Operations Apps Integration

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | **Prod** | PBR-Multinode | Symmetric-PBR | L1-

Prod

- Quick Start
- Prod
 - Application Profiles
 - Networking
 - Contracts
 - Policies
 - Services**
 - L4-L7**
 - Service Parameters
 - Service Graph Templates**
 - FW
 - LB**
 - Router configurations

L4-L7 Service Graph Template - LB

Topology **Policy** Faults History

Properties

terminal nodes:

Name	Provider/Consumer	Description
T1	Consumer	
T2	Provider	

Connections:

Name	Connected Nodes	Direct Connect	Unicast Route	Adjacency Type	Description
C1	N1, T1	False	True	L3	
C2	N1, T2	True	True	L3	

C2 is the connection between provider EPG and provider side of service node

Es wird wie unten beschrieben eine Zulässigkeitsregel für die Provider-EPG(32773) zu Service-LB(16389) hinzugefügt.

```
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. Beispiel für Datenverkehrsfluss - Firewall und Load Balancer ohne SNAT

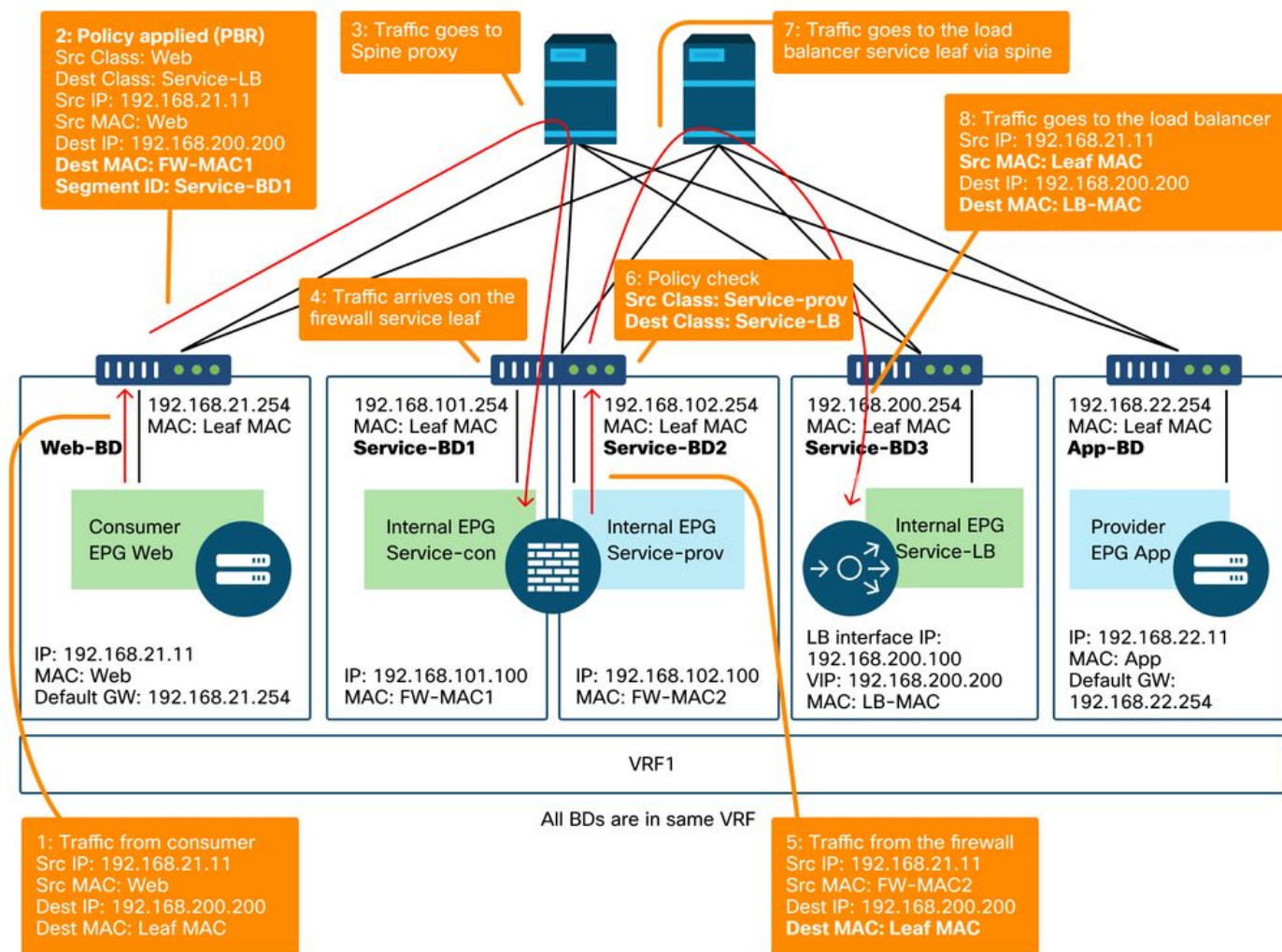
PBR kann mit mehreren Servicefunktionen in einem Servicediagramm bereitgestellt werden, z. B. Firewall als erster Knoten und Load Balancer als zweiter Knoten.

Beispiel für Datenverkehrspfad

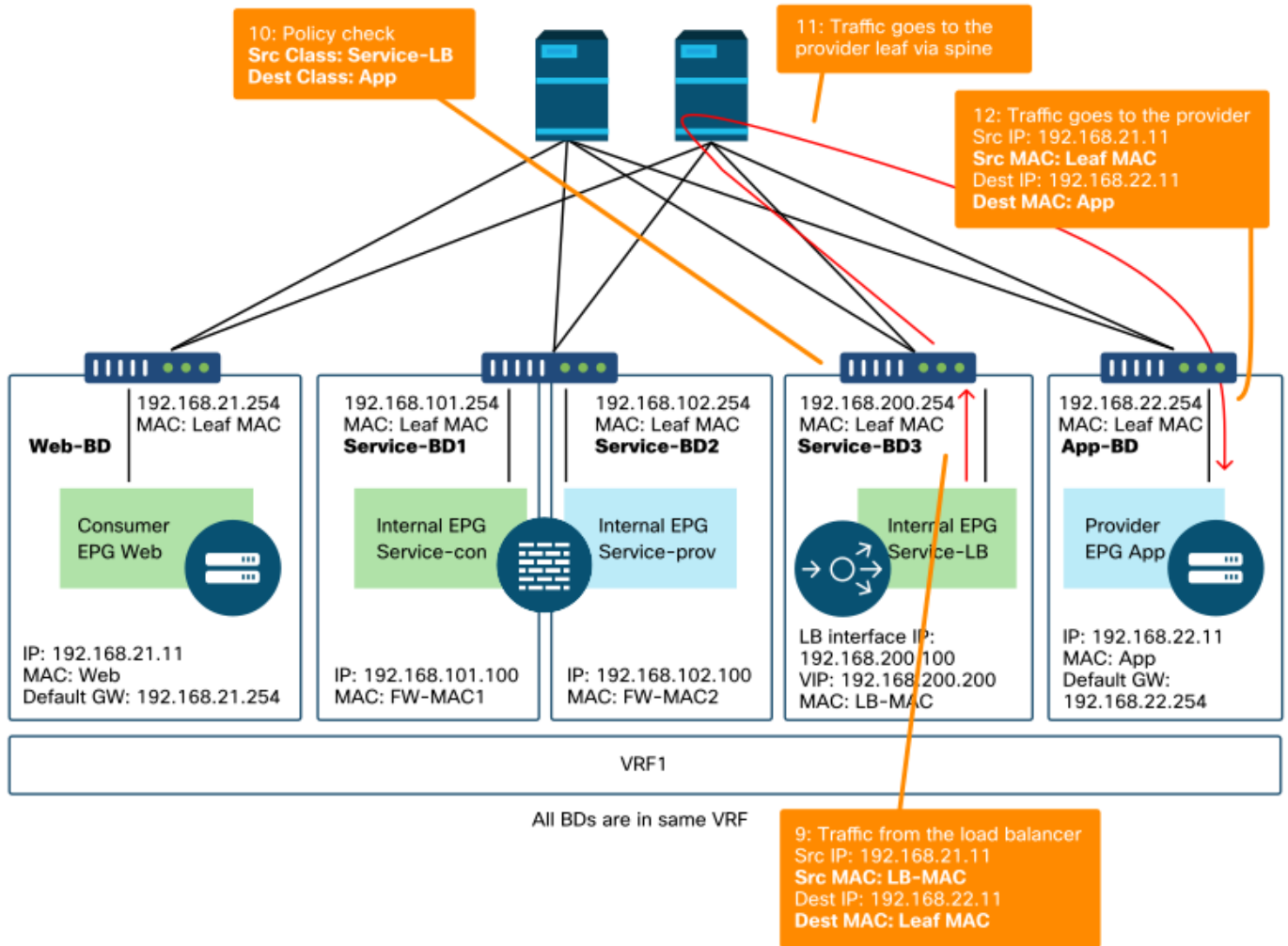
Die folgende Abbildung zeigt ein Beispiel für einen eingehenden Datenverkehrsfluss von Consumer-EPG-Web zu Provider-EPG-App mit zwei Verbindungen: Die eine wird von einem

Endpunkt im Consumer-EPG-Web an die Load Balancer-VIP über die Firewall übertragen, die andere vom Load Balancer an ein Endpunkt in der Provider-EPG-App. Der an das VIP gerichtete eingehende Datenverkehr wird zur Firewall umgeleitet und geht dann ohne PBR zum Load Balancer. Der Load Balancer ändert die Ziel-IP in eines der Endpunkte in der App-EPG, die dem VIP zugeordnet ist, übersetzt jedoch nicht die Quell-IP. Anschließend wird der Datenverkehr zum Anbieterendpunkt geleitet.

Firewall und Load Balancer ohne SNAT-Weiterleitungspfad - Beispiel: Verbraucher zu VIP und Load Balancer zu Anbieter



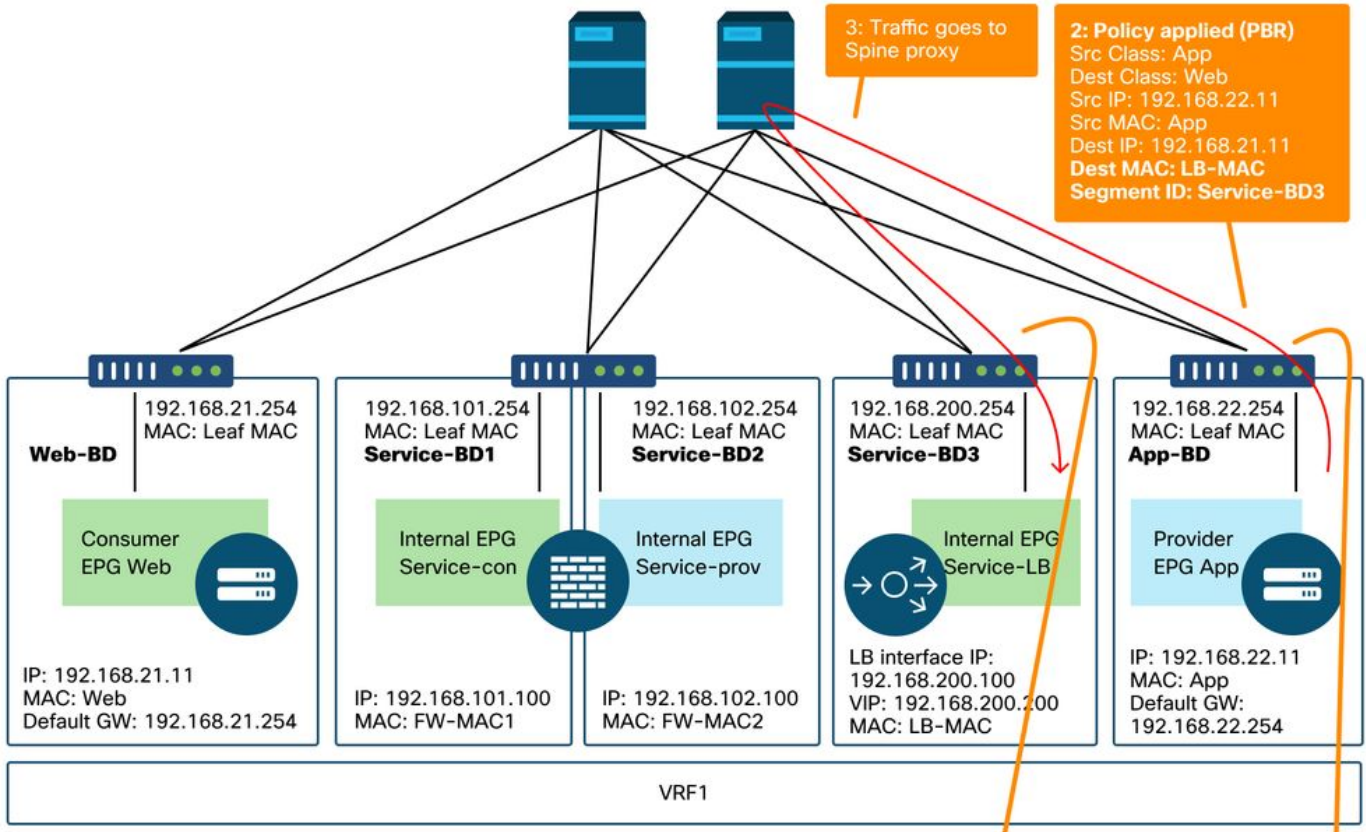
Firewall und Load Balancer ohne SNAT-Weiterleitungspfad - Beispiel für Verbraucher zu VIP und Load Balancer zu Anbieter (Fortsetzung)



In der folgenden Abbildung wird der Datenrückfluss von der Provider-EPG-App zum EPG-Web für Privatnutzer dargestellt. Da der zurückgeleitete Datenverkehr an die ursprüngliche Quell-IP gerichtet ist, ist PBR erforderlich, damit der zurückgeleitete Datenverkehr an den Load Balancer zurückgeleitet wird.

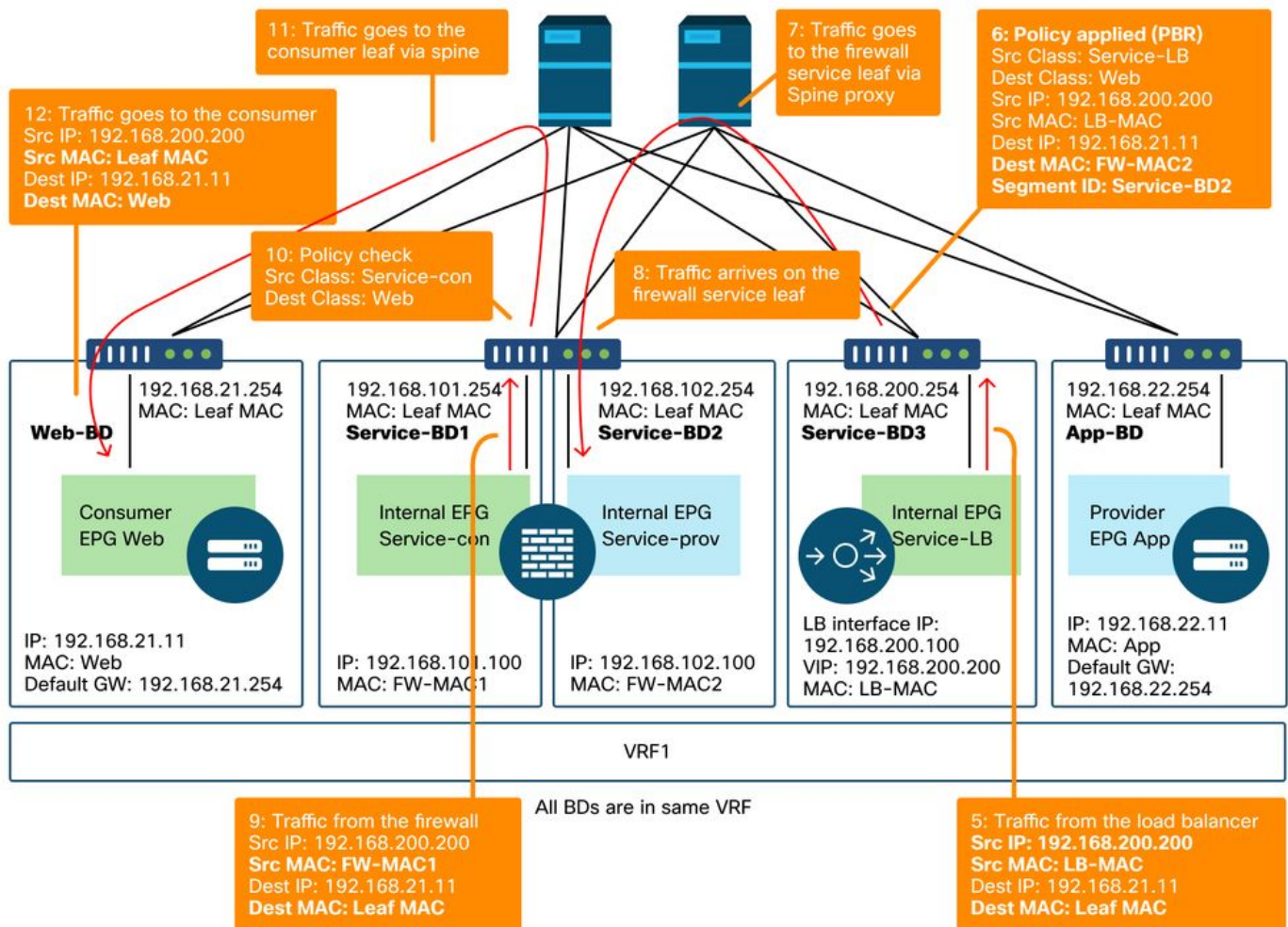
Nachdem der Datenverkehr vom Anbieterendpunkt zum Verbraucherendpunkt zum Load Balancer umgeleitet wurde, ändert der Load Balancer die Quell-IP in die VIP. Der Datenverkehr kommt vom Load Balancer zurück und wird zur Firewall umgeleitet. Anschließend wird der Datenverkehr von der Firewall zurück an den Endpunkt des Verbrauchers geleitet.

Firewall und Load Balancer ohne SNAT-Weiterleitungspfad - Beispiel: Anbieter an Verbraucher



All BDs are in same VRF

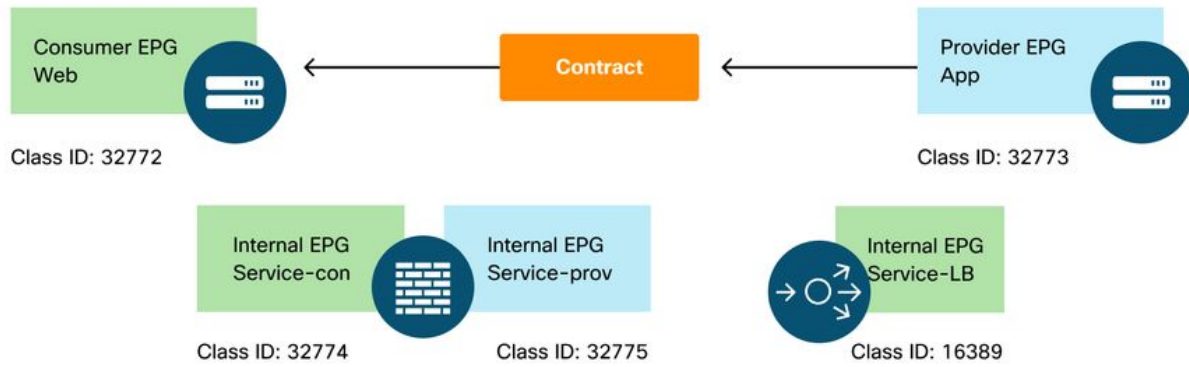
- 1: Traffic from the provider
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: Leaf MAC
- 2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
- 3: Traffic goes to Spine proxy
- 4: Traffic arrives on the load balancer service leaf



Die für die Leaf-Knoten programmierten Richtlinien

Die folgende Abbildung und die Ausgabe von "show zoning-rule" beschreiben die Zoning-Regeln nach der Bereitstellung von Service Graph. In diesem Beispiel wird der Datenverkehr von pcTag 32772 (Web) an pcTag 16389 (Service-LB) an 'destgrp-32' (Consumer-Seite der Firewall) umgeleitet, der Datenverkehr von pcTag 32773 (App) an pcTag 32772 (Web) an 'destgrp-33' (Load Balancer) und der Datenverkehr von pcTag 16389 (Service-LB)) auf pcTag 32772 (Web) wird auf 'destgrp-34' (Anbieterseite der Firewall) umgeleitet.

Zoning-Regeln nach der Service Graph-Bereitstellung - Firewall und Load Balancer ohne 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) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Im obigen Beispiel ist die Option Direct Connect für die Verbindung zwischen der Anbieterseite des Load Balancers und der Anbieter-EPG auf 'True' festgelegt. Sie muss für Statusprüfungen vom Load Balancer zu Anbieterendpunkten aktiviert sein. Der Speicherort ist "Tenant > L4-L7 > Service Graph Templates > Policy" (Tenant > L4-L7 > Servicediagrammvorlagen > Richtlinie).

Weitere Informationen finden Sie in der Abbildung 'Direkte Verbindungsoption festlegen'.

3. Shared Service (Inter-VRF-Vertrag)

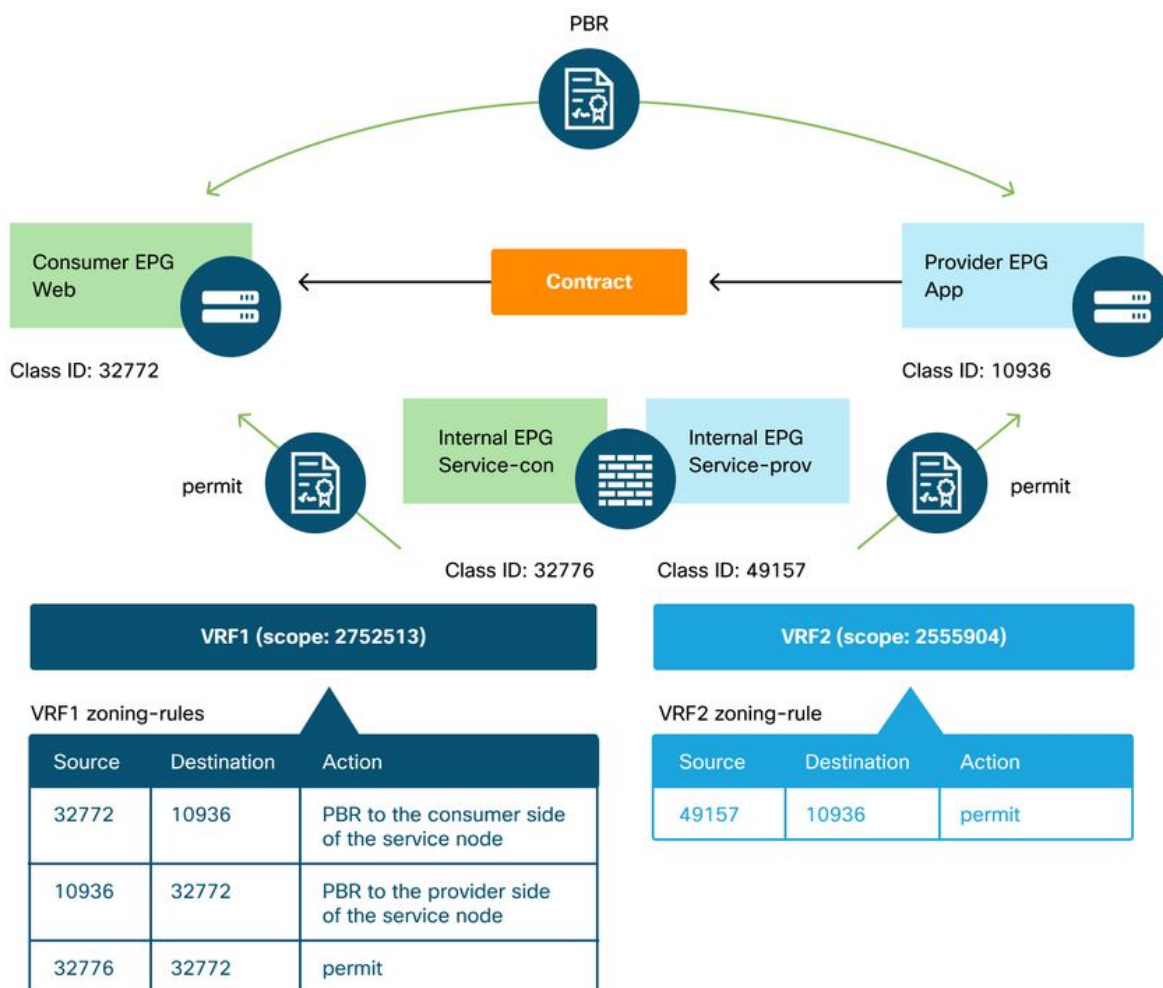
PBR kann in Inter-VRF-Verträgen aktiviert werden. In diesem Abschnitt wird erläutert, wie die Zoning-Regeln bei Inter-VRF-Verträgen zwischen EPG und EPG programmiert werden.

Die für die Leaf-Knoten programmierten Richtlinien

Bei Inter-VRF-Verträgen zwischen EPG und EPG wird die Richtlinie immer im Consumer-VRF durchgesetzt. Die Umleitung erfolgt also auf der VRF-Instanz des Verbrauchers. Weitere Kombinationen finden Sie in der Tabelle "Wo wird die Richtlinie angewendet?" im Abschnitt "Weiterleitung".

Die folgende Abbildung und die Ausgabe von "show zoning-rule" beschreiben die Zoning-Regeln nach der Bereitstellung von Service Graph. In diesem Beispiel wird der Datenverkehr von pcTag 32772 (Web) zu pcTag 10936 (App) zu 'destgrp-36' (Consumerseite des Dienstknotens) umgeleitet, und der Datenverkehr von pcTag 10936 (App) zu pcTag 32772 (Web) wird zu 'destgrp-35' (Anbieterseite des Dienstknotens) umgeleitet. Beide werden in VRF1 erzwungen, das Consumer-VRF. Der Datenverkehr von pcTag 32776 (Consumer-Seite der Firewall) zu pcTag 32772 (Web) ist in VRF1 zulässig.

Zoning-Regeln nach Bereitstellung des Servicediagramms - VRF-übergreifender Vertrag



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)

Der Datenverkehr vom pcTag 49157 (Anbieterseite der Firewall) zum pcTag 10936 (App) ist in VRF2 zulässig, da beide in VRF2 vorhanden sind.

Pod1-Leaf1# show zoning-rule scope 2555904

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action
4249	49157	10936	default	uni-dir	enabled	2555904		permit

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.