# Fehlerbehebung bei ACI-Sicherheitsrichtlinien - Verträgen

## Inhalt

# Einleitung

In diesem Dokument werden die Schritte zum Verständnis der ACI-Sicherheitsrichtlinien, die so genannten Verträge, und zur Fehlerbehebung beschrieben.

# Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem Buch Troubleshooting Cisco Application Centric Infrastructure, Second Edition, extrahiert, insbesondere die Security Policies - Overview, Security Policies - Tools, Security **Policies - EPG to EPG, Security Policies - Preferred group** und **Security Policies - vzAny to EPG, in den einzelnen** Kapiteln.

# Überblick

Die grundlegende Sicherheitsarchitektur der ACI-Lösung folgt einem Permitlistenmodell. Wenn eine VRF-Instanz nicht im **nicht erzwungenen** Modus konfiguriert wird, werden alle Datenflüsse zwischen EPGs implizit verworfen. Gemäß dem einsatzfertigen Permit-List-Modell befindet sich die Standard-VRF-Einstellung im **erzwungenen** Modus. Datenverkehrsflüsse können zugelassen oder explizit abgelehnt werden, indem Zoning-Regeln auf den Switch-Knoten implementiert werden. Diese Zoning-Regeln können in Abhängigkeit vom gewünschten Kommunikationsfluss zwischen Endpunktgruppen (EPG) und der zu ihrer Definition verwendeten Methode in

verschiedenen Konfigurationen programmiert werden. Beachten Sie, dass Zoning-Regeleinträge nicht statusbehaftet sind und nach dem Programmieren der Regel bei zwei EPGs in der Regel Port/Socket zulassen/verweigern.

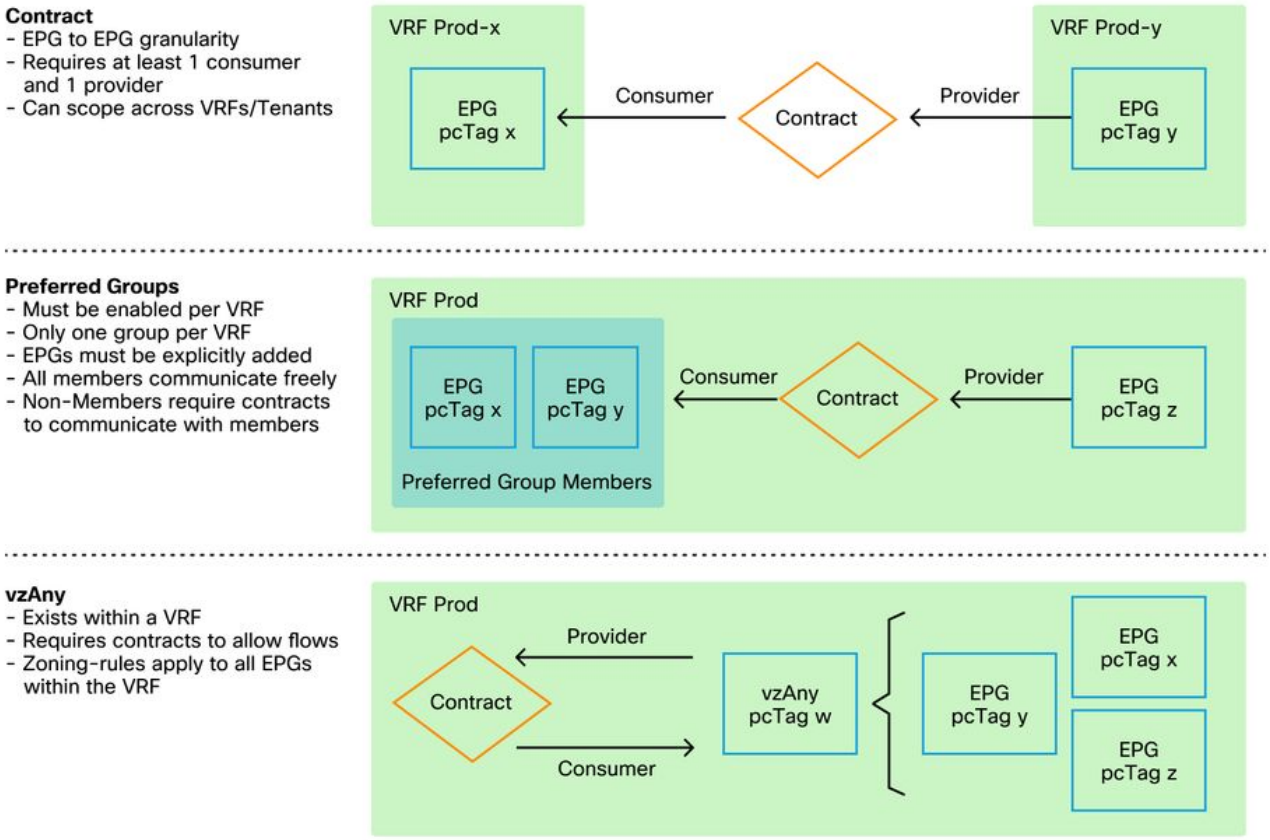
## Methoden zur Programmierung von Zoning-Regeln

Die wichtigsten Methoden zur Programmierung von Zoning-Regeln in der ACI sind:

- **EPG-zu-EPG-Verträge:** In der Regel muss mindestens ein Verbraucher und ein Anbieter Zoning-Regeln für zwei oder mehr unterschiedliche Endpunktgruppen programmieren.
- **Bevorzugte Gruppen:** Erfordert die Aktivierung der Gruppierung auf VRF-Ebene; Pro VRF kann nur eine Gruppe existieren. Alle Mitglieder der Gruppe können frei miteinander kommunizieren. Nicht-Mitglieder benötigen Verträge, um Datenflüsse an die bevorzugte Gruppe zu ermöglichen.
- **vzAny:** Eine "EPG-Sammlung", die unter einer bestimmten VRF-Instanz definiert ist. vzAny stellt alle EPGs in der VRF-Instanz dar. Die Verwendung von vzAny ermöglicht Datenflüsse zwischen einer EPG und allen EPGs innerhalb der VRF-Instanz über eine Vertragsverbindung.

Das folgende Diagramm kann verwendet werden, um auf die Granularität von Zoning-Regeln zu verweisen, die jede der oben genannten Methoden für die Steuerung ermöglicht:

## Vergleich zwischen Zoning-Regelmethoden




Bei Verwendung der Vertragsmethode zum Programmieren von Zoning-Regeln gibt es eine Option zum Definieren des Vertragsbereichs. Diese Option muss sorgfältig geprüft werden, wenn ein Design für Route Leaking/Shared Services erforderlich ist. Wenn innerhalb der ACI-Fabric

VRFs übertragen werden sollen, können Verträge abgeschlossen werden.

Folgende Bereichswerte sind möglich:

- **Anwendung: In** einer Vertragsbeziehung zwischen Verbrauchern und Anbietern werden nur Regeln zwischen EPGs programmiert, die im gleichen Anwendungsprofil definiert sind. Bei der Wiederverwendung desselben Vertrags in anderen Anwendungsprofil-EPGs ist kein Übersprechen zwischen diesen möglich.
- **VRF (Standard):** Eine Contract Consumer/Provider-Beziehung programmiert Regeln zwischen EPGs, die innerhalb derselben VRF-Instanz definiert sind. Die Wiederverwendung desselben Vertrags in anderen Anwendungsprofil-EPGs ermöglicht ein Übersprechen zwischen diesen EPGs. Achten Sie darauf, dass nur gewünschte Datenströme zugelassen werden. Andernfalls sollte ein neuer Vertrag definiert werden, um unbeabsichtigtes Übersprechen zu vermeiden.
- **Tenant:** Eine Vertragsbeziehung zwischen Verbrauchern und Anbietern programmiert Regeln zwischen EPGs, die im gleichen Tenant definiert sind. Wenn EPGs mit mehreren VRFs innerhalb eines Tenants verknüpft sind und denselben Vertrag nutzen/bereitstellen, kann dieser Bereich verwendet werden, um ein Route Leaking zu bewirken, das eine VRF-übergreifende Kommunikation ermöglicht.
- **Global:** Eine Vertragsbeziehung zwischen Verbrauchern und Anbietern programmiert Regeln zwischen EPGs für jeden Tenant innerhalb einer ACI-Fabric. Dies ist der höchstmögliche Umfang der Definition, und bei zuvor definierten Verträgen sollte mit großer Sorgfalt vorgegangen werden, um unbeabsichtigte Leckströme zu verhindern.

## Zoning-Regeleintrag wird gelesen

Sobald die Zoning-Regel programmiert wurde, wird sie auf einem Leaf wie folgt angezeigt:

```
+---------+--------+--------+----------+----------------+---------+---------+----------------+-
---------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |       Name     |
Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+----------------+-
---------+----------------------+
```

- **Regel-ID**: Die ID des Regeleintrags. Keine wirkliche Bedeutung außer als eindeutiger Identifikator zu fungieren.
- **Src EPG:** eine eindeutige ID pro VRF (pcTag) der Quellendpunktgruppe.
- **Ziel-EPG:** eine eindeutige ID pro VRF (pcTag) der Zielendpunktgruppe.
- **FilterID:** Die ID des Filters, dem die Regel zugeordnet werden soll. Der Filter enthält die Protokollinformationen, mit denen die Regel übereinstimmt.
- **Dir:** die Richtung der Zoning-Regel.
- **OperSt:** der Betriebszustand der Regel.
- **Scope:** eine eindeutige ID der VRF-Instanz, mit der die Regel übereinstimmt.
- **Name:** der Name des Vertrags, der zur Programmierung dieses Eintrags geführt hat.
- **Action (Aktion**): Die Aktion, die das Leaf ausführt, wenn es mit dem Eintrag übereinstimmt. Umfasst: [Löschen, Zulassen, Protokollieren, Umleiten].
- **Priorität:** die Reihenfolge, in der die Zoning-Regeln bei übereinstimmenden Einträgen für Scope, SrcEPG, DstEPG und Filter für die Aktion validiert werden.

## Richtlinien-Content-Addressable Memory (CAM)

Wenn jede Zoning-Regel programmiert wird, verwendet eine Matrix des Zoning-Regeleintrags, der Filtereinträgen zugeordnet ist, den **Richtlinien-CAM** auf den Switches. Beim Design der zulässigen Datenflüsse durch eine ACI-Fabric ist bei der Wiederverwendung von Verträgen besondere Vorsicht geboten, anstatt neue Verträge zu erstellen, je nach Enddesign. Wenn ein Vertrag über mehrere EPGs hinweg ohne Verständnis der daraus resultierenden Zonenregeln wiederverwendet wird, kann dies schnell dazu führen, dass mehrere Datenflüsse unerwartet zugelassen werden. Gleichzeitig nutzen diese unbeabsichtigten Flows weiterhin den Richtlinien-CAM. Wenn der Richtlinien-CAM voll ist, schlägt die Zoning-Regel fehl, was je nach Konfiguration und Endpunktverhalten zu unerwarteten und zeitweiligen Verlusten führen kann.

## VRF-Leaking, globale PC-Tags und Richtlinienerzwingung bei gemeinsam genutzten L3Outs

Dies ist eine spezielle Klausel für den Anwendungsfall der Shared Services, für die Verträge konfiguriert werden müssen. Gemeinsam genutzte Services implizieren in der Regel Inter-VRF-Datenverkehr innerhalb einer ACI-Fabric, der auf der Nutzung eines Vertrags mit Tenant- oder globalem Umfang beruht. Um dies vollständig zu verstehen, muss man zunächst die Vorstellung bekräftigen, dass der typische, EPGs zugewiesene pcTag-Wert nicht global eindeutig ist. pcTags gelten für eine VRF-Instanz, und dasselbe pcTag kann in einer anderen VRF-Instanz verwendet werden. Sobald die Diskussion über Route Leaking aufkommt, beginnen Sie damit, Anforderungen an die ACI-Fabric durchzusetzen, einschließlich der Notwendigkeit global eindeutiger Werte, einschließlich Subnets und pcTags.

Besonders wichtig ist dabei der Aspekt der Richtwirkung, der damit verknüpft ist, dass eine EPG ein Verbraucher und kein Anbieter ist. In einem Shared-Services-Szenario wird vom Anbieter in der Regel erwartet, dass er ein globales pcTag fördert, um einen eindeutigen Wert für die Fabric zu erhalten. Gleichzeitig behält der Verbraucher sein VRF-fähiges pcTag bei, wodurch er in eine besondere Position versetzt wird, um jetzt die Verwendung des globalen pcTag-Werts programmieren und verstehen zu können, um Richtlinien durchzusetzen.

Der Zuweisungsbereich von pcTag ist wie folgt:

- System reserviert: 1-15.
- Weltweiter Umfang: 16-16384 für Shared Services Provider-EPGs.
- Lokaler Bereich: 16385-65535 für VRF-EPGs.

## Durchsetzungsrichtung für VRF-Richtlinienkontrolle

In jeder VRF-Instanz kann die Einstellung der Durchsetzungsrichtung definiert werden.

- Die Standardeinstellung für die Durchsetzungsrichtung ist "Ingress" (Eingang).
- Die andere Option für die Durchsetzungsrichtung ist "Egress".

Um zu verstehen, wo die Richtlinie durchgesetzt wird, müssen verschiedene Variablen verwendet werden.

Die nachfolgende Tabelle hilft zu verstehen, wo die Sicherheitsrichtlinien auf Leaf-Ebene durchgesetzt werden.

## Wo werden die Richtlinien durchgesetzt?

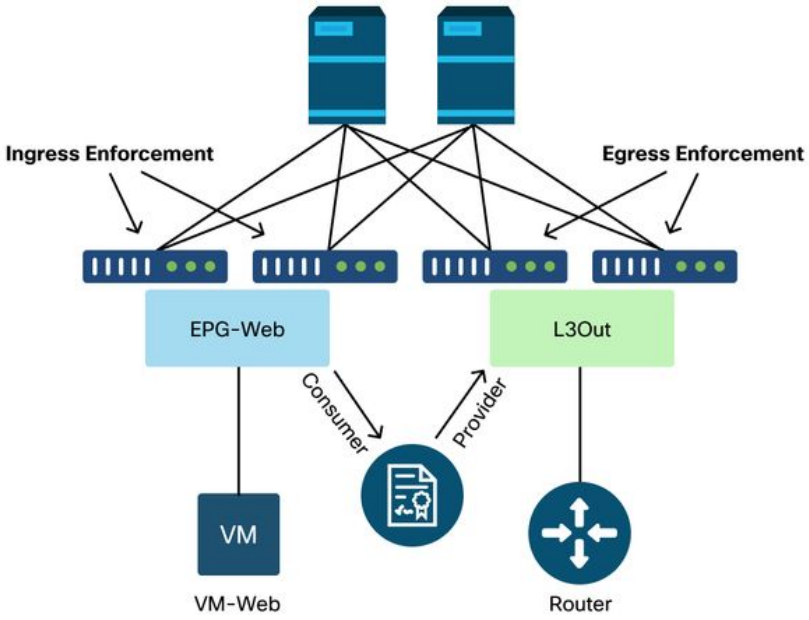
| Szenario | VRF- | Verbrauch | Anbieter | Durchsetzung der Richtlinie am |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | Erzwingungsmodus | er | | |
| Intra-VRF | Eingang/Ausgang | EPG | EPG | • Wenn der Zielendpunkt erfasst wird: Eingangsblatt*<br>• Wenn der Zielendpunkt 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 |
| | Ausgehend | L3Out-EPG | EPG | • Wenn der Zielendpunkt erfasst wird: Randblatt<br>• Wenn der Zielendpunkt nicht erfasst wird: unbegrenztes Blatt<br>Nicht grenzübergreifender Leaf-> Grenz-Leaf-Datenverkehr |
| Inter-VRF | Eingang/Ausgang | L3Out-EPG | L3Out-EPG | • Grenz-Blatt<br>Eingangs-Leaf* |
| | Eingang/Ausgang | EPG | EPG | Verbraucher-Leaf |
| | Eingang/Ausgang | EPG | L3Out-EPG | Verbraucher-Leaf |
| | 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.

Die folgende Abbildung zeigt ein Beispiel für die Vertragsdurchsetzung, bei der EPG-Web als Consumer und L3Out EPG als Provider über einen Intra-VRF-Vertrag verfügen. Wenn VRF auf den Ingress-Erzwingungsmodus festgelegt ist, wird die Richtlinie von den Leaf-Knoten durchgesetzt, auf denen EPG-Web gespeichert ist. Wenn VRF auf den Egress-Erzwingungsmodus festgelegt ist, wird die Richtlinie von den Grenz-Leaf-Knoten durchgesetzt, auf denen sich L3Out befindet, wenn der VM-Web-Endpunkt auf dem Grenz-Leaf erfasst wird.

## Durchsetzung bei Eingang und Ausgang




# Tools

Es stehen eine Reihe von Tools und Befehlen zur Verfügung, die bei der Identifizierung einer **Richtlinienaufgabe** helfen können. Ein Richtlinienverlust kann als Paketverlust definiert werden, wenn er auf eine Vertragskonfiguration zurückzuführen ist oder nicht vorhanden ist.

## Validierung von Zoning-Regeln

Die folgenden Tools und Befehle können verwendet werden, um die Zoning-Regeln explizit zu validieren, die auf Leaf-Switches als Ergebnis abgeschlossener Verbraucher-/Provider-Vertragsbeziehungen programmiert sind.

### 'show zoning-rules'

Ein Befehl auf Switch-Ebene, der alle vorhandenen Zoning-Regeln anzeigt.

```
leaf# show zoning-rule
+---------+--------+--------+----------+----------------+---------+----------+----------------
+----------+----------------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope   |       Name
|  Action  |          Priority          |
+---------+--------+--------+----------+----------------+---------+----------+----------------
+----------+----------------------------+
|   4156  |   25   | 16410  |   425    | uni-dir-ignore | enabled | 2818048  | external_to_ntp
|  permit  |       fully_qual(7)        |
|   4131  | 16410  |   25   |   424    |     bi-dir     | enabled | 2818048  | external_to_ntp
|  permit  |       fully_qual(7)        |
+---------+--------+--------+----------+----------------+---------+----------+----------------
+----------+----------------------------+
```

### 'show zoning-filter'

Ein Filter, der die Sport-/Portinformationen enthält, auf die die Zoning-Regel wirkt. Die

Filterprogrammierung kann mit diesem Befehl überprüft werden.

```
leaf# show zoning-filter
+----------+----------+------------+------------+------------+----------+------------+------
-------+------------+------------+----------+
| FilterId |   Name   |    EtherT  |     Prot    | ApplyToFrag | Stateful |  SFromPort  |
SToPort   |  DFromPort  |   DToPort   |   Prio   |
+----------+----------+------------+------------+------------+----------+------------+------
-------+------------+------------+----------+
| implarp  | implarp  |     arp     | unspecified |      no     |    no    | unspecified |
unspecified | unspecified | unspecified |  dport   |
| implicit | implicit | unspecified | unspecified |      no     |    no    | unspecified |
unspecified | unspecified | unspecified | implicit |
|   425    |  425_0   |      ip     |     tcp     |      no     |    no    |     123     |
123     | unspecified | unspecified |  sport   |
|   424    |  424_0   |      ip     |     tcp     |      no     |    no    | unspecified |
unspecified |     123     |     123     |  dport   |
+----------+----------+------------+------------+------------+----------+------------+------
-------+------------+------------+----------+
```

### 'show system internal policy-mgr stats'

Mit diesem Befehl kann die Anzahl der Treffer pro Zoning-Regel überprüft werden. Dies ist nützlich, um zu bestimmen, ob eine erwartete Regel getroffen wird, im Gegensatz zu einer anderen, z. B. einer impliziten Ablagerungsregel, die eine höhere Priorität haben kann.

```
leaf# show system internal policy-mgr stats
Requested Rule Statistics
Rule (4131) DN (sys/actrl/scope-2818048/rule-2818048-s-16410-d-25-f-424) Ingress: 0, Egress: 0,
Pkts: 0  RevPkts: 0
Rule (4156) DN (sys/actrl/scope-2818048/rule-2818048-s-25-d-16410-f-425) Ingress: 0, Egress: 0,
Pkts: 0  RevPkts: 0
```

### 'show logging ip access-list internal packet-log deny'

Ein Befehl auf Switch-Ebene, der auf iBash-Ebene ausgeführt werden kann und Zugriffskontrolllisten (Contract)-bezogene Auslassungen und Informationen zum Datenfluss meldet, darunter:

- VRF
- VLAN-ID
- Quell-MAC/Ziel-MAC
- Quell-IP/Ziel-IP
- Quellport/Zielport
- Quellschnittstelle

```
leaf# show logging ip access-list internal packet-log deny
[ Tue Oct  1 10:34:37 2019 377572 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: Unknown,
Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.11,
SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98
[ Tue Oct  1 10:34:36 2019 377731 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: Unknown,
Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.11,
SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98
```

### Vertrags-Parser

Ein geräteinternes Python-Skript, das eine Ausgabe erzeugt, die die Zoning-Regeln, Filter und Trefferstatistiken während der Namenssuche von IDs korreliert. Dieses Skript ist äußerst nützlich, da es einen mehrstufigen Prozess ausführt und in einen einzigen Befehl umwandelt, der auf bestimmte EPGs/VRFs oder andere vertragsbezogene Werte gefiltert werden kann.

```
leaf# contract_parser.py
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]

[7:4131] [vrf:common:default] permit ip tcp tn-Prod1/ap-Services/epg-NTP(16410) tn-Prod1/l3out-
L3Out1/instP-extEpg(25) eq 123  [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[7:4156] [vrf:common:default] permit ip tcp tn-Prod1/l3out-L3Out1/instP-extEpg(25) eq 123 tn-
Prod1/ap-Services/epg-NTP(16410)  [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[12:4169] [vrf:common:default] deny,log any tn-Prod1/l3out-L3Out1/instP-extEpg(25) epg:any
[contract:implicit] [hit=0]
[16:4167] [vrf:common:default] permit any epg:any tn-Prod1/bd-Services(32789)
[contract:implicit] [hit=0]
```

## Validierung der Paketklassifizierung

### ELAM

Ein Bericht auf ASIC-Ebene zur Überprüfung der Weiterleitungsdetails, der im Fall eines verworfenen Pakets den Grund für die Verwerfung angibt. Für diesen Abschnitt relevant, kann der Grund ein SECURITY_GROUP_DENY (Verwerfen der Vertragsrichtlinie) sein.

### fTriage

Ein Python-basiertes Dienstprogramm auf dem APIC, das den Paketfluss mit ELAM nachverfolgen kann.

### ELAM Assistant-Anwendung

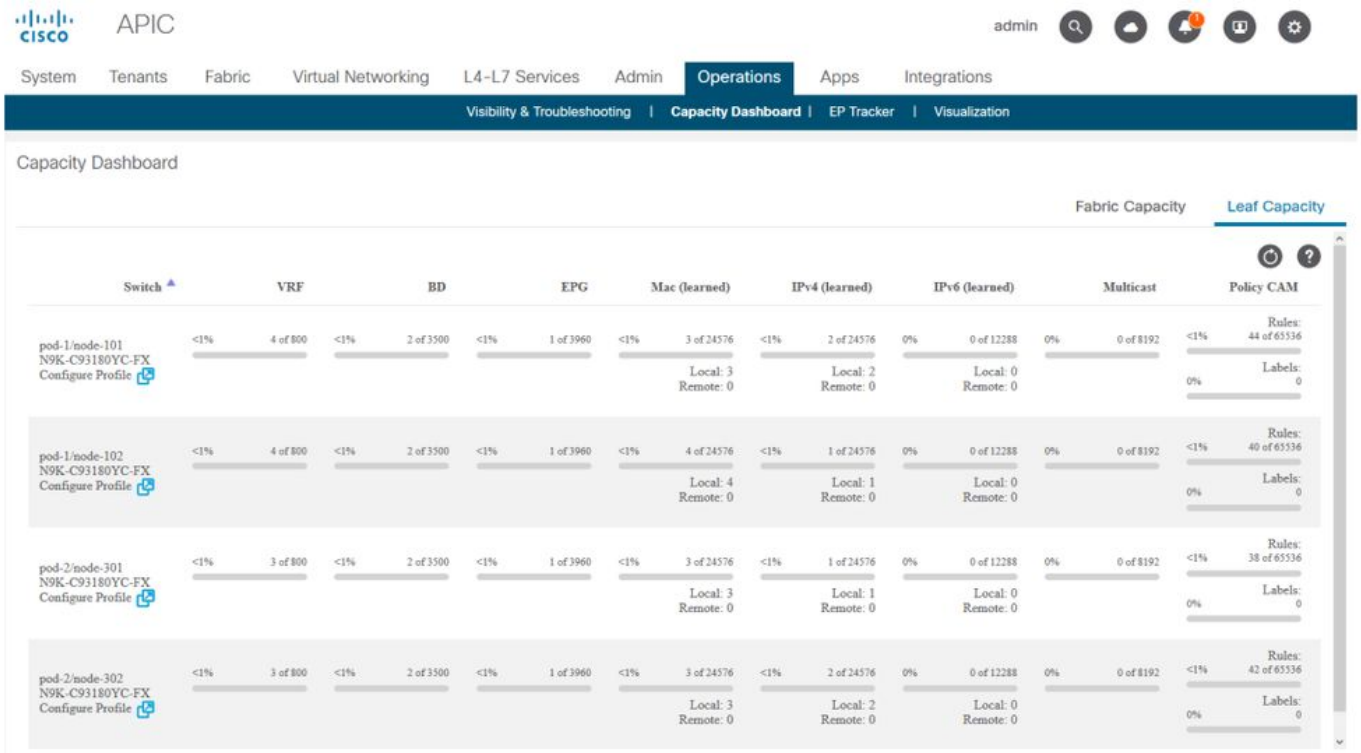
Diese APIC-Anwendung abstrahiert die Komplexität verschiedener ASICs, um die Weiterleitungsentscheidungsprüfung wesentlich bequemer und benutzerfreundlicher zu gestalten.

Im Abschnitt "Intra-Fabric Forwarding" finden Sie weitere Informationen zu den ELAM-, fTriage- und ELAM Assistant-Tools.

## Nutzung von Richtlinien-CAM

Die CAM-Verwendung der Richtlinien auf Leaf-Basis ist ein wichtiger Parameter, der überwacht werden muss, um sicherzustellen, dass sich die Fabric in einem fehlerfreien Zustand befindet. Die schnellste Möglichkeit, dies zu überwachen, besteht darin, das 'Capacity Dashboard' in der GUI zu verwenden und die Spalte 'Policy Cam' explizit zu überprüfen.

## Die Ansicht "Leaf-Kapazität" des Kapazitäts-Dashboards




**'show platform internal hal health-stats'**

Mit diesem Befehl können Sie verschiedene Ressourcenbeschränkungen und die Ressourcennutzung überprüfen, einschließlich des Richtlinien-CAM. Beachten Sie, dass dieser Befehl nur in vsh_lc ausgeführt werden kann, übergeben Sie ihn also mit dem Flag '-c', wenn er von iBash ausgeführt wird.

```
leaf8# vsh_lc -c "show platform internal hal health-stats"
|Sandbox_ID: 0  Asic Bitmap: 0x0
|-----------------------------------
 ...
Policy stats:
=============
policy_count                  : 96
max_policy_count              : 65536
policy_otcam_count            : 175
max_policy_otcam_count            : 8192
policy_label_count                : 0
max_policy_label_count            : 0
=============
```

# EPG zu EPG

## Allgemeine Überlegungen zum Löschen von Richtlinien

Es gibt zahlreiche Möglichkeiten, ein Verbindungsproblem zwischen zwei Endpunkten zu beheben. Die folgende Methodik bietet einen guten Ausgangspunkt, um schnell und effektiv zu isolieren, ob das Verbindungsproblem das Ergebnis eines **Policy Drop** (durch einen Vertrag verursacht) ist.

Vor dem Eintauchen sollten Sie einige wichtige Fragen stellen:

- Befinden sich die Endpunkte in derselben oder in einer anderen EPG? Der Datenverkehr zwischen zwei Endpunkten in unterschiedlichen EPGs (Inter-EPGs) wird implizit abgelehnt und erfordert einen Kontakt, der die Kommunikation ermöglicht.Datenverkehr zwischen zwei Endpunkten innerhalb derselben EPG (intra-EPG) ist implizit zulässig, es sei denn, es wird eine intra-EPG-Isolierung verwendet.
- Wird die VRF-Instanz erzwungen oder nicht? Befindet sich eine VRF-Instanz im **erzwungenen** Modus, sind für die Kommunikation von Endpunkten in zwei verschiedenen EPGs innerhalb der VRF-Instanz Verträge erforderlich.Befindet sich eine VRF-Instanz im **nicht erzwungenen** Modus, wird innerhalb der VRF-Instanz - unabhängig von den angewendeten ACI-Verträgen - der gesamte Datenverkehr über mehrere EPGs, die zur nicht erzwungenen VRF-Instanz gehören, durch die ACI-Fabric zugelassen.

## Methodik

Mit den verschiedenen verfügbaren Tools gibt es einige, die besser geeignet und bequemer als andere zu beginnen sind, abhängig von der Ebene der bereits bekannten Informationen über den betroffenen Fluss.

Ist der vollständige Pfad des Pakets in der ACI-Fabric bekannt (Eingangs-Leaf, Ausgangs-Leaf usw.)?

- Wenn die Antwort "Ja" lautet, muss der ELAM-Assistent verwendet werden, um den Grund für das Verwerfen auf dem Quell- oder Zielswitch zu ermitteln.
- Wenn die Antwort nein lautet, können Sie mithilfe der Befehle Visibility & Troubleshooting, fTriage, contract_parser, Operational in der Tenant-Ansicht und iBash den Pfad des Pakets eingrenzen und die Ursachen für das Verwerfen besser anzeigen.

Bitte beachten Sie, dass das fTriage-Tool in diesem Abschnitt nicht im Detail behandelt wird. Weitere Informationen zur Verwendung dieses Tools finden Sie im Kapitel "Intra-Fabric Forwarding".

Zwar können Transparenz und Fehlerbehebung helfen, schnell zu erkennen, wo Pakete zwischen zwei Endpunkten verloren gehen, fTriage bietet jedoch detailliertere Informationen für die weitere Fehlerbehebung. d. h. fTriage hilft bei der Identifizierung von Schnittstelle, Verwerfungsgrund und anderen grundlegenden Details zum betroffenen Datenfluss.

.

In diesem Beispielszenario wird die Fehlerbehebung bei einem Richtlinienverlust zwischen zwei Endpunkten veranschaulicht: 192.168.21.11 und 192.168.23.11

Wenn zwischen diesen beiden Endpunkten Paketverluste auftreten, wird der folgende Workflow zur Fehlerbehebung verwendet, um die Ursache des Problems zu identifizieren:

Identifizieren Sie die am Datenverkehrsfluss beteiligten src/dst-Leaf(s):

1. Verwenden Sie **Transparenz und Fehlerbehebung**, um den Paketfluss zu verfolgen und zu identifizieren, welches Gerät das Paket verwirft.
2. Führen Sie den Befehl "show logging ip access-list internal packet-log deny" auf dem ausgewählten Gerät aus. Wenn ein Paket mit einer der relevanten IP-Adressen abgelehnt und protokolliert wird, wird im **Paketprotokoll** der entsprechende Endpunkt- und

Vertragsname nach Treffern ausgegeben.

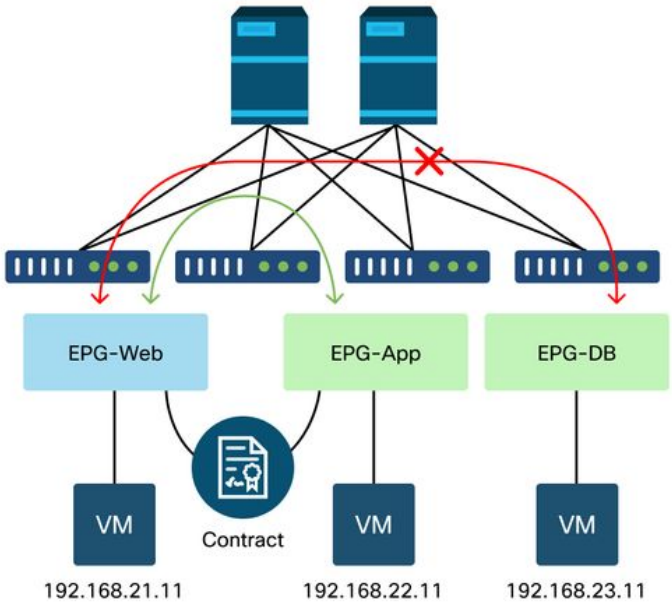
3. Verwenden Sie den Befehl "contract_parser.py —vrf <tenant>:<VRF>" auf dem Quell- und Ziel-Leaf, um die Trefferanzahl für den konfigurierten Vertrag zu beobachten: Wenn ein Paket den Vertrag auf dem Quell- oder Ziel-Switch erreicht, erhöht sich der Zähler des entsprechenden VertragsDiese Methode ist in Situationen, in denen viele Datenflüsse dieselbe Regel erfüllen (viele Endpunkte/Datenflüsse zwischen den beiden relevanten EPGs), weniger detailliert als die Methode der internen Paketprotokollierung der IP-Zugriffsliste.

Die obigen Schritte werden im nächsten Absatz näher beschrieben.

## Beispiel für ein Fehlerbehebungsszenario zwischen EPG und EPG

In diesem Beispielszenario wird die Fehlerbehebung bei einem Richtlinienverlust zwischen zwei Endpunkten veranschaulicht: 192.168.21.11 in EPG-Web und 192.168.23.11 in EPG-DB.

## Topologie

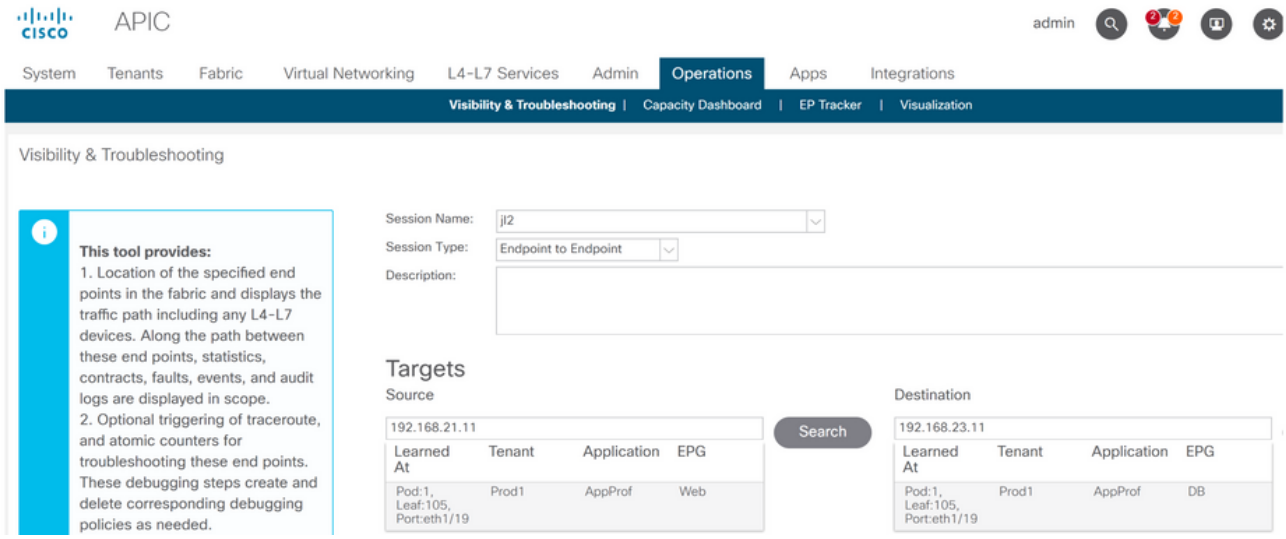



## Identifizieren der am Paketverlust beteiligten Quell- und Ziel-Leaf-Switches

### Transparenz und Fehlerbehebung

Das Tool für Transparenz und Fehlerbehebung hilft dabei, den Switch, an dem der Paketverlust aufgetreten ist, für einen bestimmten EP-to-EP-Datenstrom darzustellen und zu identifizieren, wo möglicherweise Pakete verloren gegangen sind.

## Konfiguration von Transparenz und Fehlerbehebung

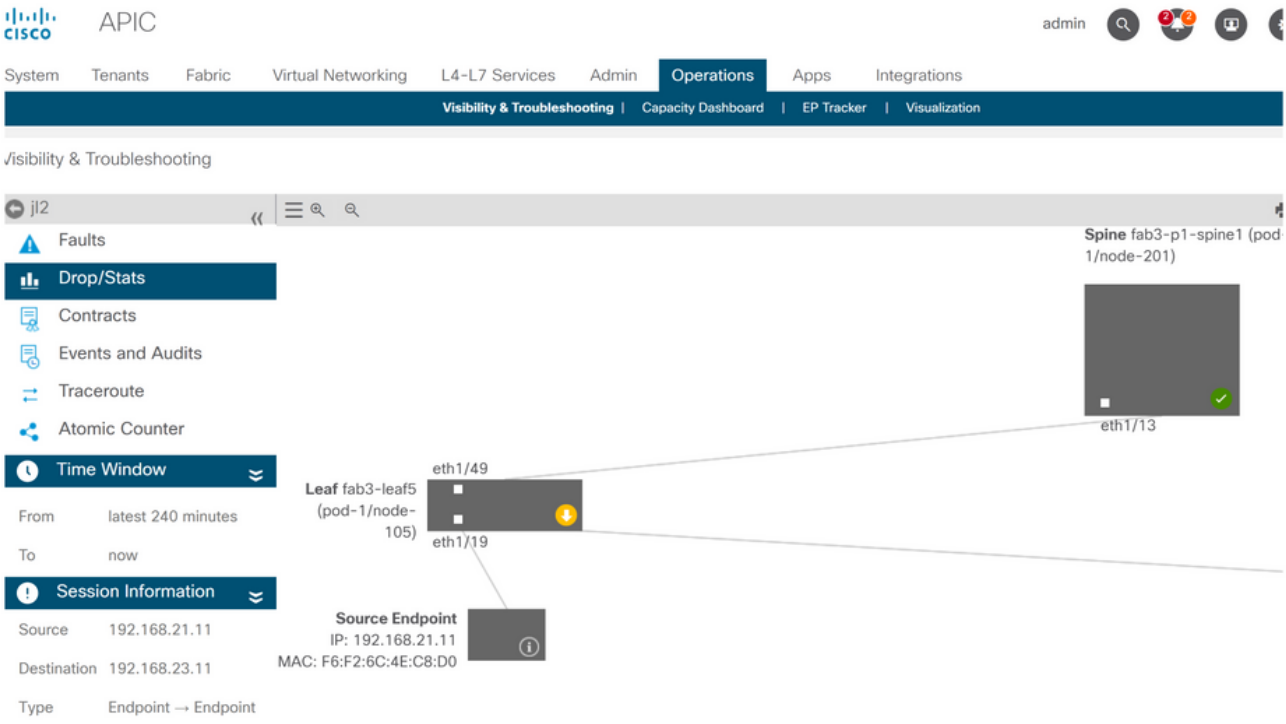



Konfigurieren eines Sitzungsnamens, einer Quelle und eines Zielendpunkts Klicken Sie dann auf "Senden" oder "Bericht erstellen".

Das Tool sucht automatisch nach den Endpunkten in der Fabric und stellt Informationen über den Tenant, das Anwendungsprofil und die EPG bereit, zu denen diese EP gehören.

In diesem Fall wird festgestellt, dass die EPs zum Tenant Prod1 gehören, dem gleichen Anwendungsprofil "AppProf" angehören und verschiedenen EPGs zugewiesen sind: 'Web' und 'DB'.

## Kennung verwerfen

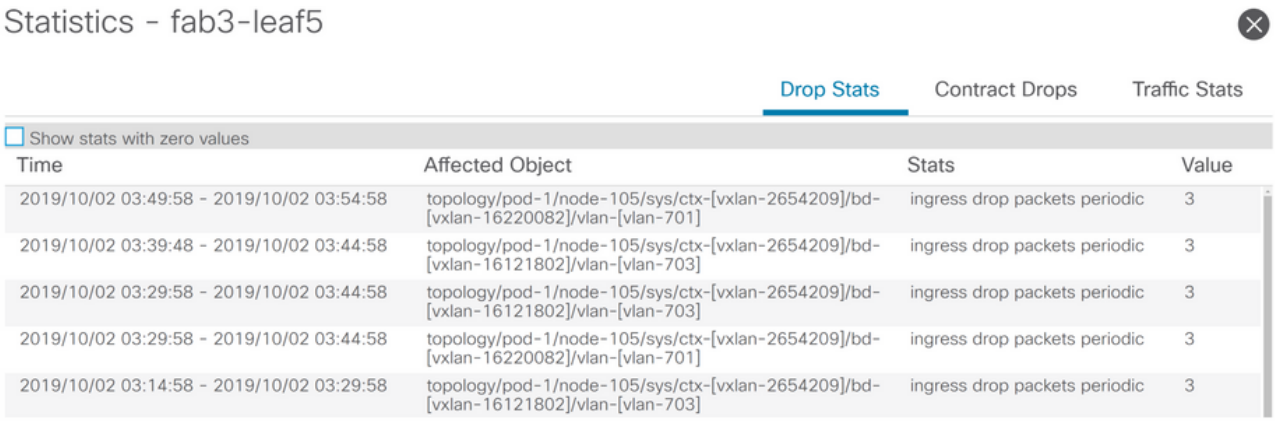



Das Tool visualisiert automatisch die Topologie des Fehlerbehebungsszenarios. In diesem Fall sind die beiden Endpunkte zufällig mit demselben Leaf-Switch verbunden.

Durch Navigieren zum Untermenü Drop/Stats kann der Benutzer allgemeine Drops auf dem jeweiligen Leaf oder Spine anzeigen. Im Abschnitt "Interface Drops" im Kapitel "Intra-Fabric Forwarding" dieses Buchs finden Sie weitere Informationen darüber, welche Drops relevant sind.

Viele dieser Einbrüche werden als Verhalten erwartet und können ignoriert werden.

## Details löschen


Statistics - fab3-leaf5

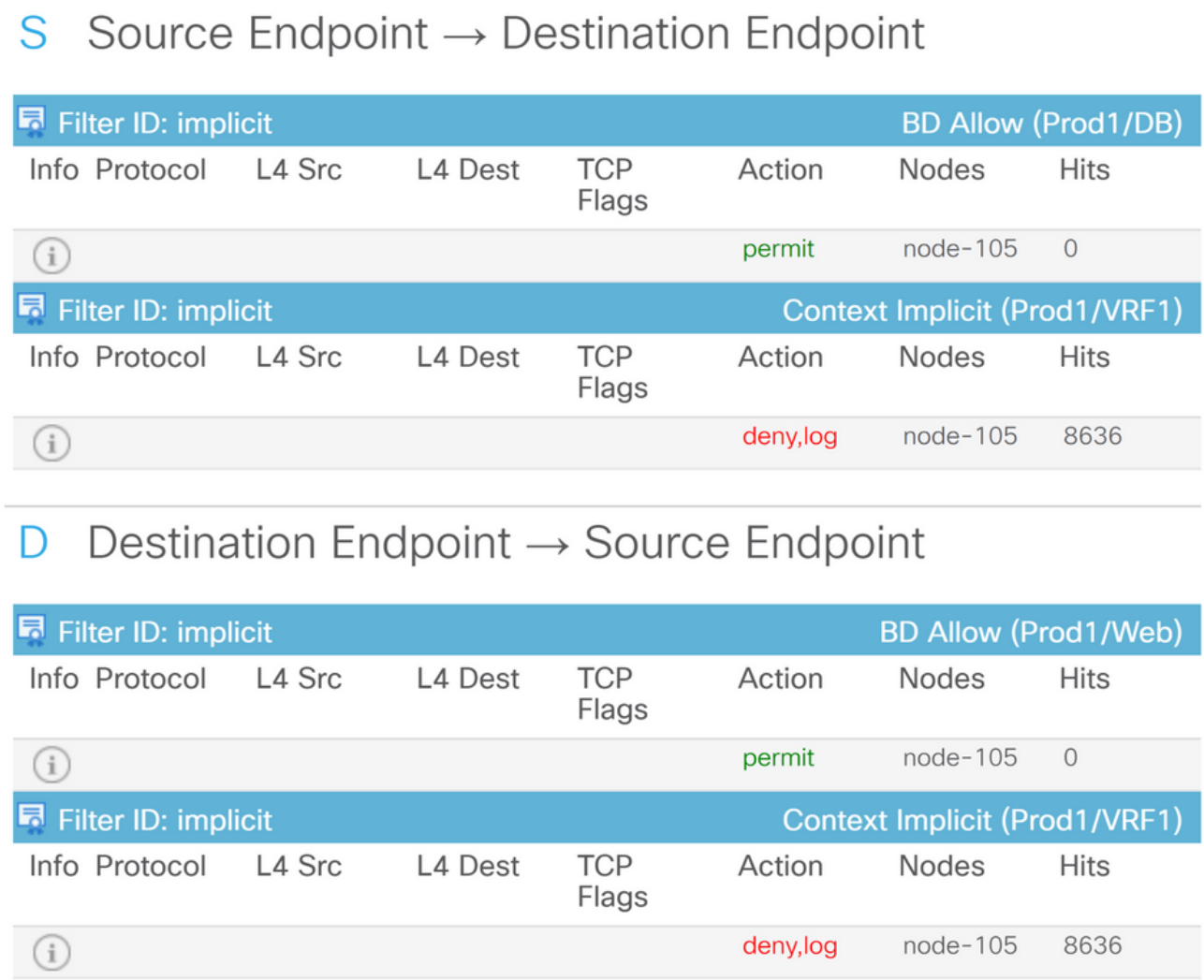
Drop Stats | Contract Drops | Traffic Stats

Show stats with zero values

| Time | Affected Object | Stats | Value |
|---|---|---|---|
| 2019/10/02 03:49:58 - 2019/10/02 03:54:58 | topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16220082]/vlan-[vlan-701] | ingress drop packets periodic | 3 |
| 2019/10/02 03:39:48 - 2019/10/02 03:44:58 | topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16121802]/vlan-[vlan-703] | ingress drop packets periodic | 3 |
| 2019/10/02 03:29:58 - 2019/10/02 03:44:58 | topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16121802]/vlan-[vlan-703] | ingress drop packets periodic | 3 |
| 2019/10/02 03:29:58 - 2019/10/02 03:44:58 | topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16220082]/vlan-[vlan-701] | ingress drop packets periodic | 3 |
| 2019/10/02 03:14:58 - 2019/10/02 03:29:58 | topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16121802]/vlan-[vlan-703] | ingress drop packets periodic | 3 |

Wenn Sie im Switch-Diagramm über die gelbe Schaltfläche "Verworfene Pakete" detaillierte Angaben zum Dropdown-Menü anzeigen, können Sie Details zum verworfenen Fluss anzeigen.

## Vertragsdetails


S Source Endpoint → Destination Endpoint

Filter ID: implicit — BD Allow (Prod1/DB)

| Info | Protocol | L4 Src | L4 Dest | TCP Flags | Action | Nodes | Hits |
|---|---|---|---|---|---|---|---|
| | | | | | permit | node-105 | 0 |

Filter ID: implicit — Context Implicit (Prod1/VRF1)

| Info | Protocol | L4 Src | L4 Dest | TCP Flags | Action | Nodes | Hits |
|---|---|---|---|---|---|---|---|
| | | | | | deny,log | node-105 | 8636 |

D Destination Endpoint → Source Endpoint

Filter ID: implicit — BD Allow (Prod1/Web)

| Info | Protocol | L4 Src | L4 Dest | TCP Flags | Action | Nodes | Hits |
|---|---|---|---|---|---|---|---|
| | | | | | permit | node-105 | 0 |

Filter ID: implicit — Context Implicit (Prod1/VRF1)

| Info | Protocol | L4 Src | L4 Dest | TCP Flags | Action | Nodes | Hits |
|---|---|---|---|---|---|---|---|
| | | | | | deny,log | node-105 | 8636 |

Durch Navigieren zum Untermenü "Contracts" (Verträge) kann der Benutzer erkennen, welcher Vertrag zu einem Verwerfen von Richtlinien zwischen den EPGs führt. Im Beispiel ist es Implicit to Deny Prod1/VRF1, das einige Treffer anzeigt. Dies bedeutet nicht unbedingt, dass der

angegebene Fluss (192.168.21.11 und 192.168.23.11) diese implizite Verweigerung trifft. Wenn die Regel "Hits of Context Implicit Deny" ansteigt, impliziert dies, dass es Datenverkehr zwischen Prod1/DB und Prod1/Web gibt, der keinen der Verträge betrifft und daher von der Implicit Deny verworfen wird.

Wählen Sie in der Ansicht "Anwendungsprofil-Topologie" unter Tenant > links den Namen des Anwendungsprofils aus > Topologie, um zu überprüfen, welche Verträge auf die DB-EPG angewendet werden. In diesem Fall wird der EPG kein Vertrag zugewiesen:

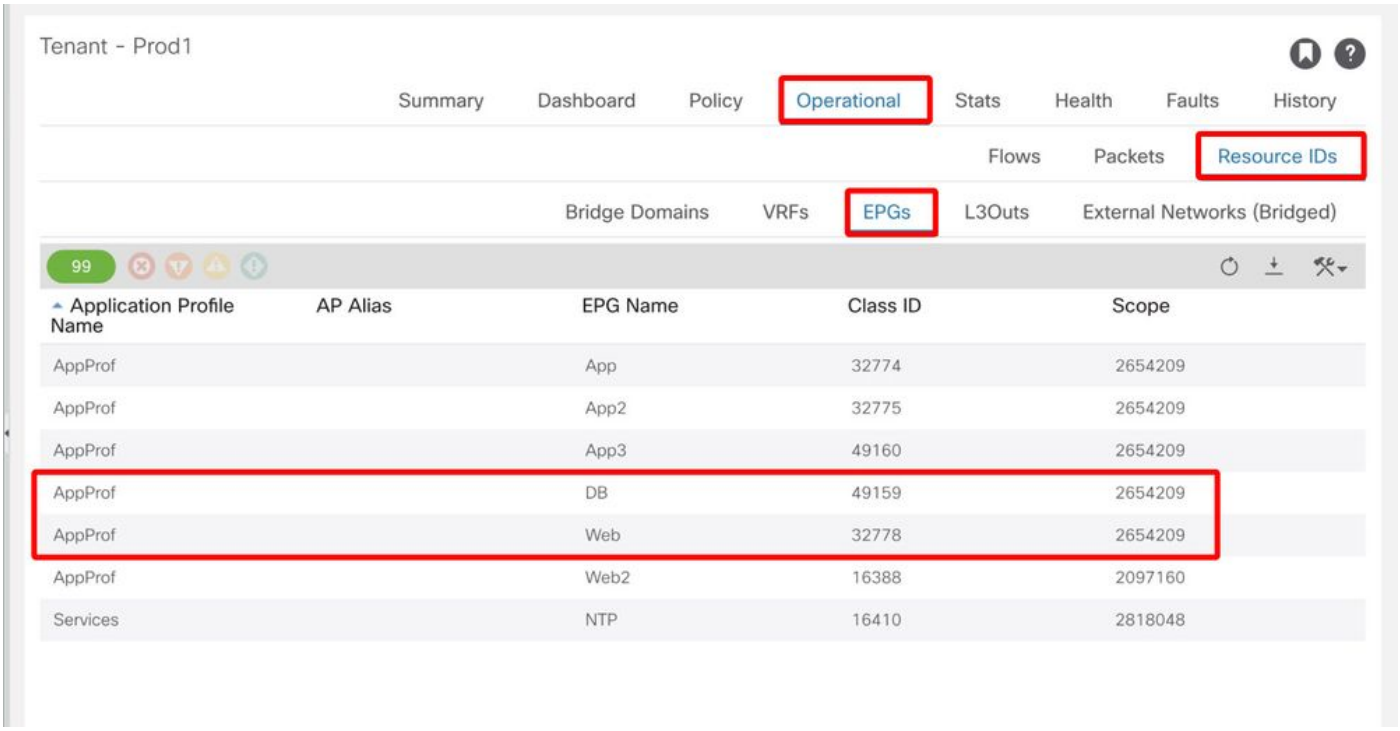
## Vertragsvisualisierung


Nachdem die Quell- und Ziel-EPGs bekannt sind, können weitere relevante Informationen wie die folgenden identifiziert werden:

- Das src/dst **EPG pcTag** der betroffenen Endpunkte. Das pcTag ist die Klassen-ID, die zur Identifizierung einer EPG mit einer Zoning-Regel verwendet wird.
- Die src/dst **VRFVNID,** auch **Scope** genannt, der betroffenen Endpunkte.

Die Klassen-ID und der Umfang können auf einfache Weise über die APIC-GUI abgerufen werden. Öffnen Sie dazu Tenant > wählen Sie links den Tenant-Namen aus > Betrieb > Ressourcen-IDs > EPGs.

## Tenant-Ressourcen-ID zum Suchen von EPG-PCtag und -Bereich




In diesem Fall lauten die Klassen-ID und die Bereiche:

- Web-EPG pcTag 32778
- Umfang der Web-EPG 2654209
- DB EPG pcTag 49159
- DB EPG Geltungsbereich 2654209

## Überprüfen der auf den zu behebenden Datenverkehrsfluss angewendeten Richtlinie

### iBash

Ein interessantes Tool zum Überprüfen der auf einem ACI-Leaf blockierten Pakete ist die iBash-Befehlszeile: 'show logging ip access-list internal packet-log deny':

```
leaf5# show logging ip access-list internal packet-log deny | grep 192.168.21.11
[2019-10-01T14:25:44.746528000+09:00]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: FD_VLAN,
Vlan-Id: 114, SMac: 0xf6f26c4ec8d0, DMac:0x0022bdf819ff, SIP: 192.168.21.11, DIP: 192.168.23.11,
SPort: 0, DPort: 0, Src Intf: Ethernet1/19, Proto: 1, PktLen: 126
[2019-10-01T14:25:44.288653000+09:00]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: FD_VLAN,
Vlan-Id: 116, SMac: 0x3e2593f0eded, DMac:0x0022bdf819ff, SIP: 192.168.23.11, DIP: 192.168.21.11,
SPort: 0, DPort: 0, Src Intf: Ethernet1/19, Proto: 1, PktLen: 126
```

Wie aus der vorherigen Ausgabe ersichtlich, wurden auf dem Leaf-Switch zahlreiche ICMP-Pakete verworfen, die von der EP 192.168.23.11 in Richtung 192.168.21.11 bezogen wurden.

Das contract_parser-Tool hilft bei der Überprüfung der tatsächlichen Richtlinien für die VRF-Instanz, mit der die Endgeräte verknüpft sind:

```
leaf5# contract_parser.py --vrf Prod1:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
```

```
[7:5159] [vrf:Prod1:VRF1] permit ip tcp tn-Prod1/ap-App1/epg-App(32771) eq 5000 tn-Prod1/ap-
App1/epg-Web(32772)  [contract:uni/tn-Prod1/brc-web_to_app] [hit=0]
[7:5156] [vrf:Prod1:VRF1] permit ip tcp tn-Prod1/ap-App1/epg-Web(32772) tn-Prod1/ap-App1/epg-
App(32771) eq 5000  [contract:uni/tn-Prod1/brc-web_to_app] [hit=0]
[16:5152] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-Web(49154) [contract:implicit] [hit=0]
[16:5154] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]
[21:5155] [vrf:Prod1:VRF1] deny,log any epg:any epg:any [contract:implicit] [hit=38,+10]
[22:5153] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
```

Dies kann auch mithilfe der Zoning-Regel überprüft werden, die im Leaf der vom Switch durchgesetzten Richtlinien programmiert ist.

```
leaf5# show zoning-rule scope 2654209
+---------+--------+--------+----------+----------------+---------+----------+------------+-----
-----+-------------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope   |    Name    |
Action  |         Priority        |
+---------+--------+--------+----------+----------------+---------+----------+------------+-----
-----+-------------------------+
|   5155  |   0    |   0    | implicit |    uni-dir     | enabled | 2654209  |            |
deny,log |     any_any_any(21)     |
|   5159  | 32771  | 32772  |   411    | uni-dir-ignore | enabled | 2654209  | web_to_app |
permit  |      fully_qual(7)      |
|   5156  | 32772  | 32771  |   410    |     bi-dir     | enabled | 2654209  | web_to_app |
permit  |      fully_qual(7)      |
+---------+--------+--------+----------+----------------+---------+----------+------------+-----
-----+-------------------------+
```

Wie bereits vom Visibility & Troubleshooting Tool, vom contract_parser Tool und den Zoning-Regeln festgestellt, wird bei der Ausgabe bestätigt, dass es bei der Fehlerbehebung keinen Vertrag zwischen der Quell- und der Ziel-EPGs gibt. Es kann leicht davon ausgegangen werden, dass die verworfenen Pakete mit der impliziten Ablehnungsregel 5155 übereinstimmen.

## ELAM-Erfassung

Die ELAM-Erfassung bietet einen Bericht auf ASIC-Ebene, mit dem die Weiterleitungsdetails geprüft werden. Dieser Bericht gibt bei einem verworfenen Paket den Grund für die Verwerfung an. Wenn der Grund für das Verwerfen ein Verwerfen von Richtlinien ist (wie in diesem Szenario), sieht die Ausgabe der ELAM-Erfassung wie folgt aus.

Bitte beachten Sie, dass Details zur Einrichtung einer ELAM-Erfassung in diesem Kapitel nicht behandelt werden. Weitere Informationen finden Sie im Kapitel "Intra-Fabric Forwarding".

```
leaf5# vsh_lc
module-1# debug platform internal tah elam asic 0
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 192.168.21.11 dst_ip 192.168.23.11
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status

ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
Asic 0 Slice 1 Status Armed

module-1(DBG-elam-insel6)# ereport | grep reason
RW drop reason                          : SECURITY_GROUP_DENY
```

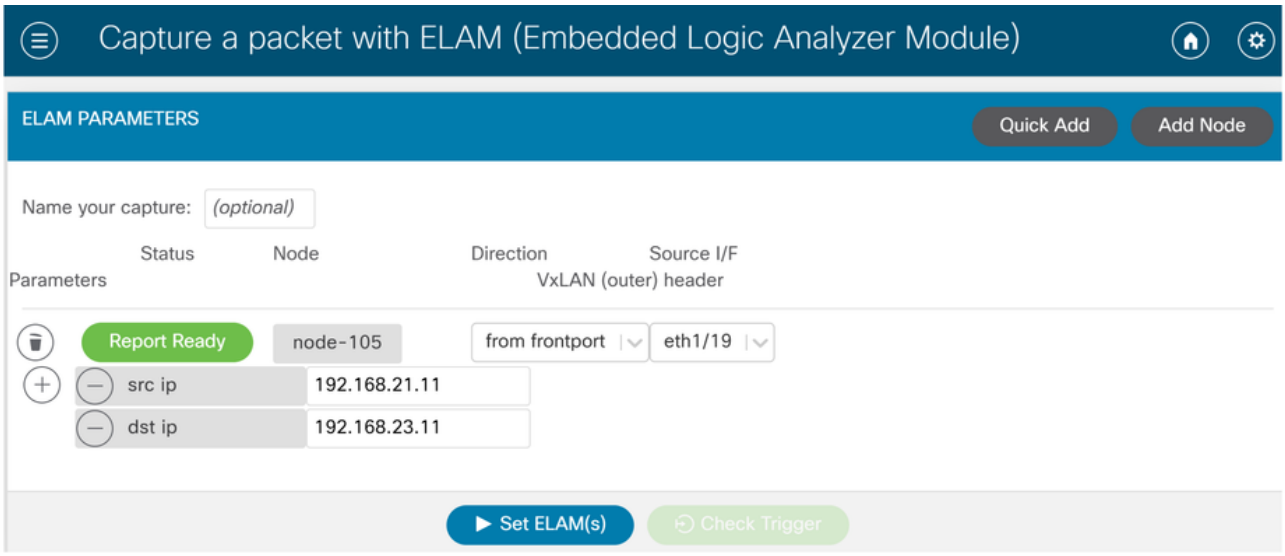
```
LU drop reason                          : SECURITY_GROUP_DENY
   pkt.lu_drop_reason: 0x2D
```

Der oben gezeigte ELAM-Bericht zeigt deutlich, dass das Paket aufgrund einer Richtlinienlöschung verworfen wurde: 'SECURITY_GROUP_DENY'

### ELAM-Assistent:

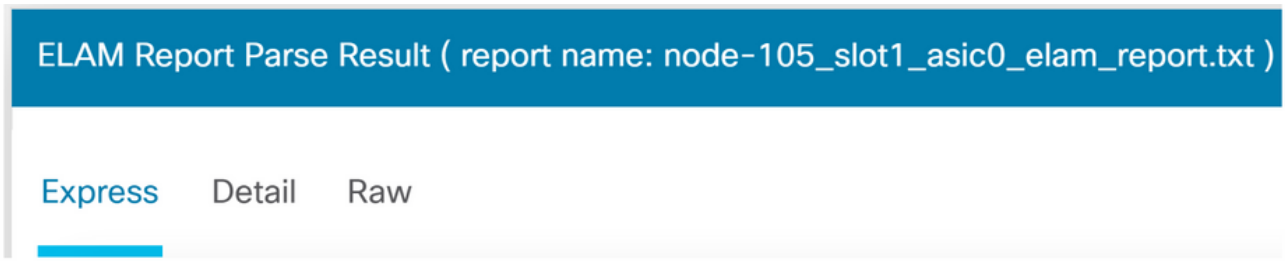
Das gleiche Ergebnis der ELAM-Erfassung kann über die ELAM Assistant-App auf der APIC-GUI angezeigt werden.

## Konfiguration



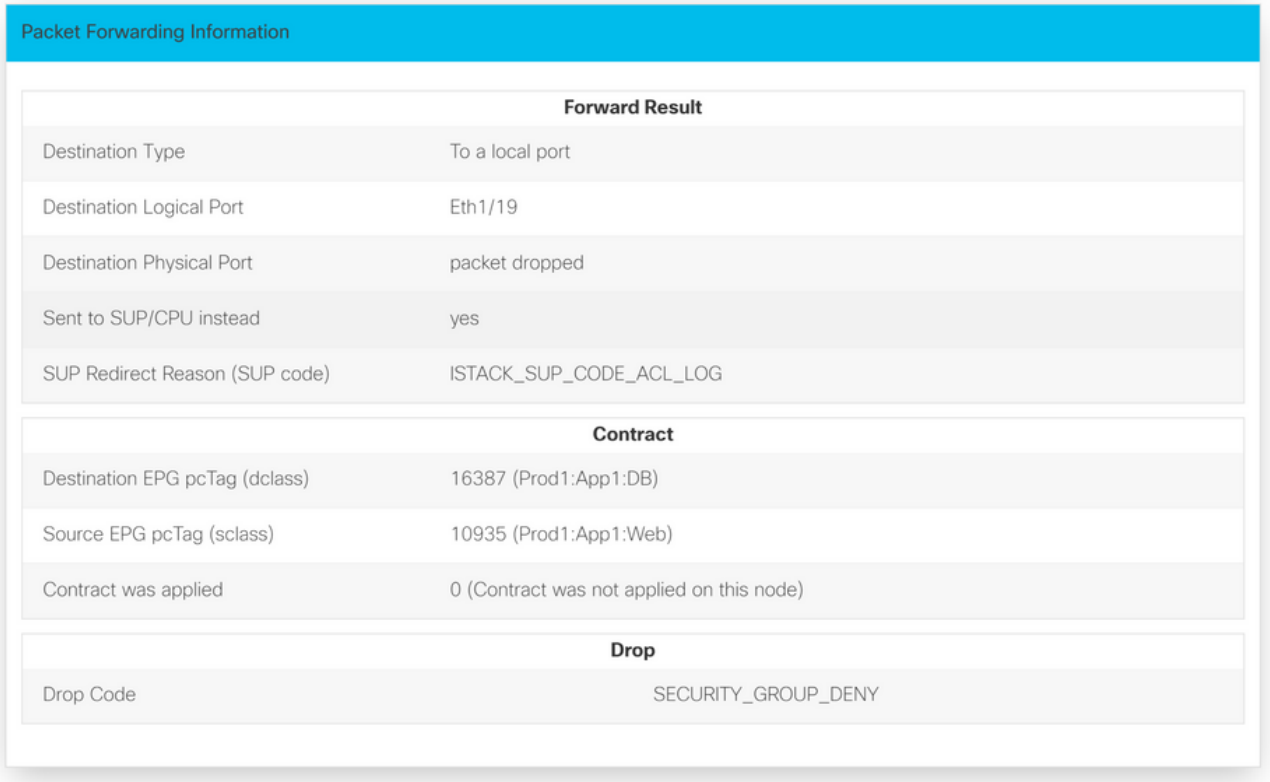

In der Regel konfiguriert der Benutzer sowohl Quell- als auch Zieldetails für den gewünschten Fluss. In diesem Beispiel wird "src IP" verwendet, um den Datenverkehr zum Endpunkt in der Ziel-EPG zu erfassen, der keine Vertragsbeziehung zur Quell-EPG hat.

## Elam Assistant Express-Bericht




Es gibt drei Ausgabeebenen, die mit dem ELAM-Assistenten angezeigt werden können. Dies sind Express, Detail und Raw.

## Elam Assistant Express-Bericht (Forts.)




Unter dem Express-Ergebnis gibt der Drop-Code-Grund SECURITY_GROUP_DENY an, dass der Verlust das Ergebnis eines Vertrags war.

# Bevorzugte Gruppe

## Informationen zu bevorzugten Vertragsgruppen

Es gibt zwei Arten von Richtliniendurchsetzung für EPGs in einer VRF-Instanz, für die eine vom Vertrag bevorzugte Gruppe konfiguriert ist:

- Enthaltene EPGs: EPGs können ohne Vertrag frei miteinander kommunizieren, wenn sie Mitglied einer von einem Vertrag bevorzugten Gruppe sind. Dies basiert auf der Standardregel source-any-destination-any-permit.
- Ausgeschlossene EPGs: EPGs, die nicht Mitglied einer bevorzugten Gruppe sind, erfordern Verträge für die Kommunikation untereinander. Andernfalls gelten die Ablehnungsregeln zwischen der ausgeschlossenen EPG und jeder EPG.

Die Funktion der vom Vertrag bevorzugten Gruppe ermöglicht eine bessere Steuerung der Kommunikation zwischen EPGs in einer VRF-Instanz. Wenn die meisten EPGs in der VRF-Instanz über eine offene Kommunikation verfügen sollten, einige jedoch nur über eine eingeschränkte Kommunikation mit den anderen EPGs verfügen sollten, konfigurieren Sie eine Kombination aus einer vom Vertrag bevorzugten Gruppe und Verträgen mit Filtern, um die Kommunikation zwischen EPGs genauer zu steuern.

EPGs, die aus der bevorzugten Gruppe ausgeschlossen sind, können nur mit anderen EPGs kommunizieren, wenn ein Vertrag besteht, der die Standardregel source-any-destination-any-deny außer Kraft setzt.

## Programmierung der bevorzugten Vertragsgruppe

Im Wesentlichen handelt es sich bei den bevorzugten Vertragsgruppen um eine Kehrseite aus regulären Verträgen. Bei regulären Verträgen werden explizite Zulassen-Zoning-Regeln mit einer impliziten Deny-Zoning-Regel für den VRF-Bereich programmiert. Für bevorzugte Gruppen wird eine implizite PERMIT-Zoning-Regel mit dem höchsten numerischen Prioritätswert programmiert, und spezifische DENY-Zoning-Regeln werden programmiert, um Datenverkehr von EPGs, die keine Mitglieder einer bevorzugten Gruppe sind, zu verbieten. Daher werden die Verweigerungsregeln zuerst ausgewertet. Wenn der Fluss nicht mit diesen Regeln übereinstimmt, wird der Fluss implizit zugelassen.

Für jede EPG außerhalb der bevorzugten Gruppe gibt es immer ein Paar expliziter Deny Zoning-Regeln:

- Einer vom Mitglied der nicht bevorzugten Gruppe zu einem beliebigen pcTag (Wert 0).
- Ein weiteres Element von einem pcTag (Wert 0) zum nicht bevorzugten Gruppenmitglied.

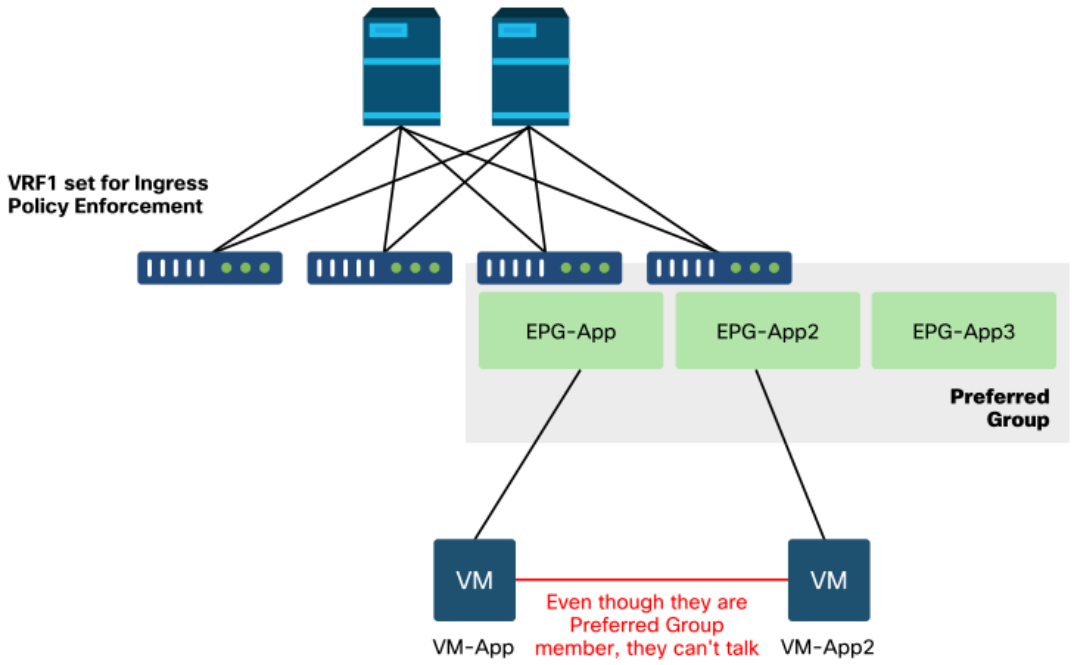
## Fehlerbehebung für bevorzugte Gruppen

Die folgende Abbildung zeigt eine logische Topologie, in der die EPGs App, App2 und App3 alle als Mitglieder einer bevorzugten Gruppe konfiguriert sind.

VM-App ist Teil von EPG-App und VM-App2 ist Teil von EPG-App2. Sowohl App als auch App2 EPG sollten Teil der bevorzugten sein und somit frei kommunizieren.

VM-App initiiert einen Datenverkehrsfluss auf dem TCP-Port 6000 zu VM-App2. Sowohl EPG-App als auch EPG-App2 sind Preferred Group Members als Teil von VRF1. VM-App2 empfängt keine Pakete auf dem TCP-Port 6000.

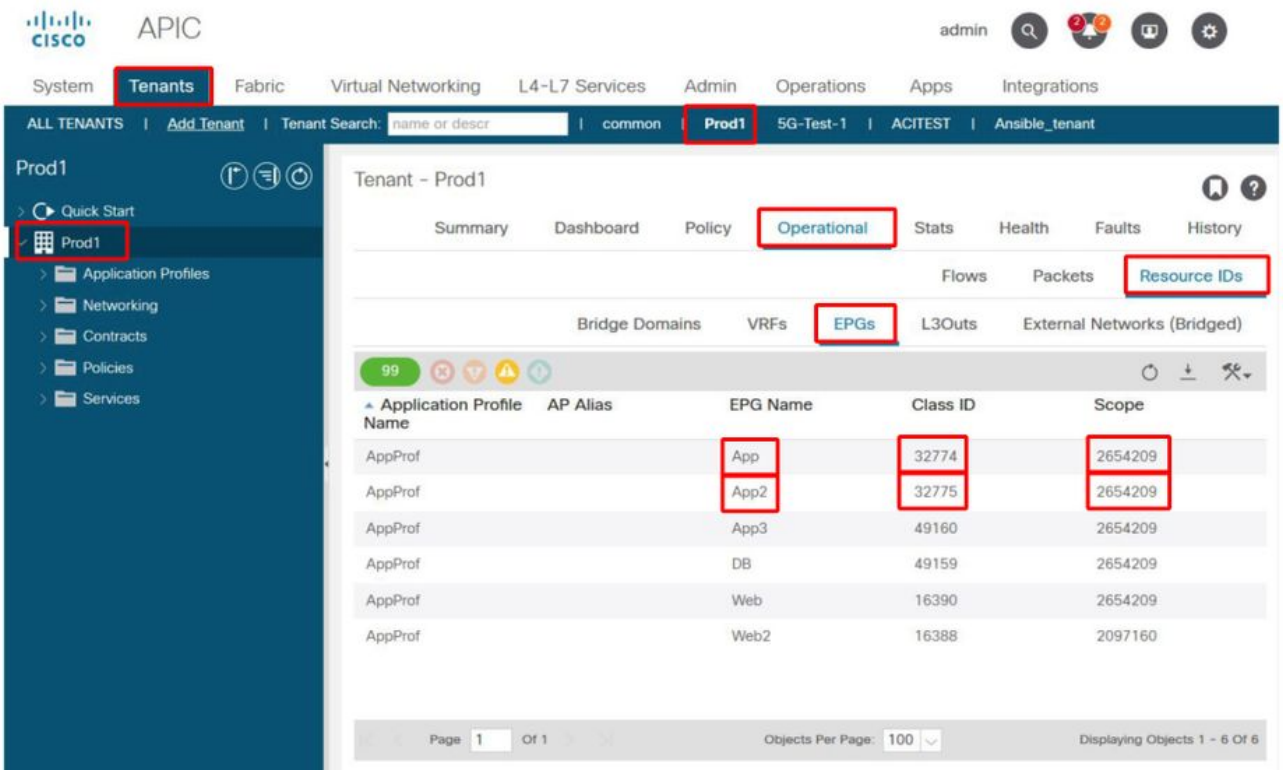
### Topologie




### Workflow

## 1. Das pcTag der EPG-APP und ihre VRF-VNID/ihren VNID/Scope nachschlagen

### EPG- und VRF-PC-Tags




## 2. Überprüfen Sie die Vertragsprogrammierung mit contract_parser.py auf dem Eingangs-Leaf.

Verwenden Sie contract_parser.py und/oder den Befehl "show zoning rule", und geben Sie die VRF-Instanz an.

```
fab3-leaf8# show zoning-rule scope 2654209
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name |  Action
|          Priority          |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------------+
|   4165  |   0    |   0    | implicit | uni-dir | enabled | 2654209 |      |  permit  |
grp_any_any_any_permit(20) |
|   4160  |   0    |   0    | implarp  | uni-dir | enabled | 2654209 |      |  permit  |
any_any_filter(17)     |
|   4164  |   0    |   15   | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_any_dest_any_deny(19)  |
|   4176  |   0    | 16386  | implicit | uni-dir | enabled | 2654209 |      |  permit  |
any_dest_any(16)       |
|   4130  | 32770  |   0    | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_src_any_any_deny(18)   |
|   4175  | 49159  |   0    | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_src_any_any_deny(18)   |
|   4129  |   0    | 49159  | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_any_dest_any_deny(19)  |
|   4177  | 32778  |   0    | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_src_any_any_deny(18)   |
|   4128  |   0    | 32778  | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_any_dest_any_deny(19)  |
|   4178  | 32775  |   0    | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_src_any_any_deny(18)   |
```

```
|   4179  |   0    | 32775  | implicit | uni-dir | enabled | 2654209 |      | deny,log |
grp_any_dest_any_deny(19)  |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------------+

fab3-leaf8# contract_parser.py --vrf Prod1:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
[16:4176] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-App(16386) [contract:implicit] [hit=0]
[16:4160] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]
[18:4130] [vrf:Prod1:VRF1] deny,log any tn-Prod1/vrf-VRF1(32770) epg:any [contract:implicit]
[hit=?]
[18:4178] [vrf:Prod1:VRF1] deny,log any epg:32775 epg:any [contract:implicit] [hit=?]
[18:4177] [vrf:Prod1:VRF1] deny,log any epg:32778 epg:any [contract:implicit] [hit=?]
[18:4175] [vrf:Prod1:VRF1] deny,log any epg:49159 epg:any [contract:implicit] [hit=?]
[19:4164] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
[19:4179] [vrf:Prod1:VRF1] deny,log any epg:any epg:32775 [contract:implicit] [hit=?]
[19:4128] [vrf:Prod1:VRF1] deny,log any epg:any epg:32778 [contract:implicit] [hit=?]
[19:4129] [vrf:Prod1:VRF1] deny,log any epg:any epg:49159 [contract:implicit] [hit=?]
[20:4165] [vrf:Prod1:VRF1] permit any epg:any epg:any [contract:implicit] [hit=65]
```

Bei der Untersuchung der obigen Ausgabe wird die implizite Zulassungseingabe — ruleId 4165 — mit der höchsten Priorität von 20 beobachtet. Diese implizite Zulässigkeitsregel bewirkt, dass alle Datenverkehrsflüsse zugelassen werden, es sei denn, es gibt eine explizite Ablehnungsregel mit einer niedrigeren Priorität, die den Datenverkehrsfluss nicht zulässt.

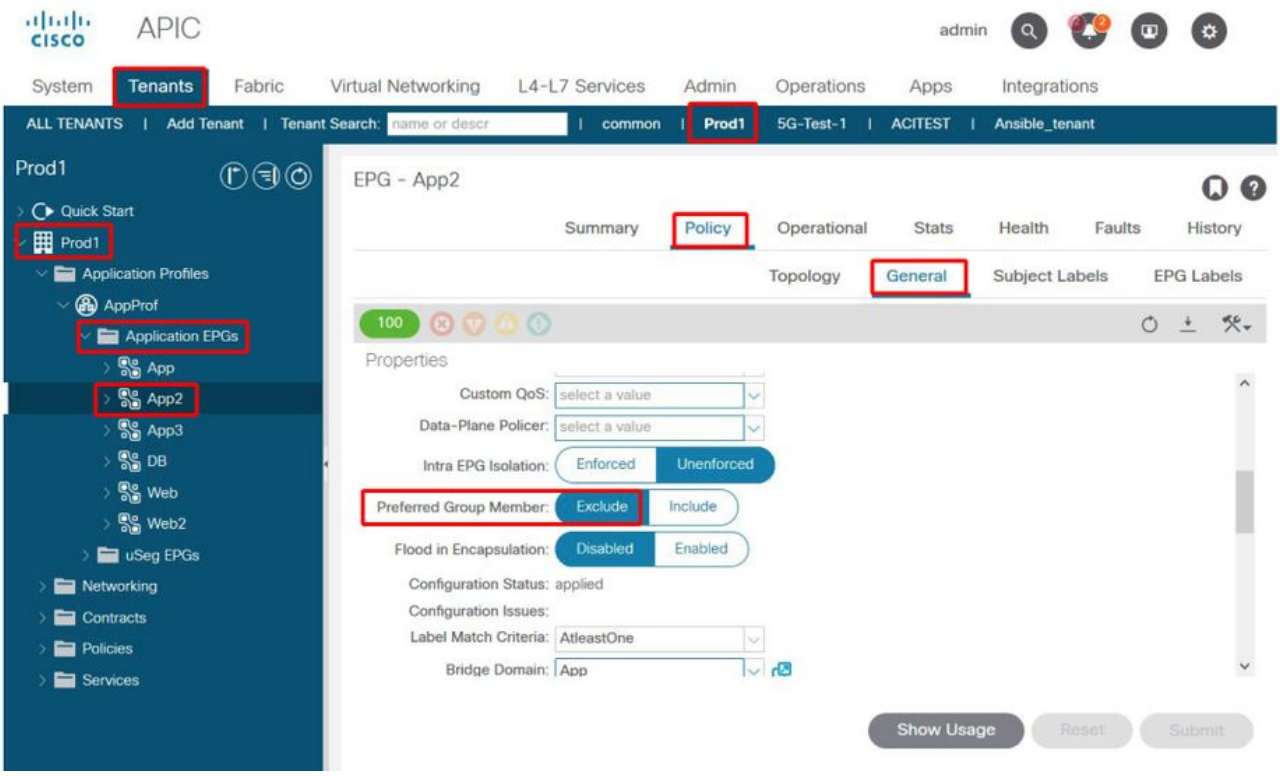
Darüber hinaus wurden zwei explizite Deny-Regeln für den pcTag 32775 beobachtet, der das pcTag von EPG App2 ist. Diese beiden expliziten Deny-Zoning-Regeln verbieten den Datenverkehr von einer EPG zu EPG App2 und umgekehrt. Diese Regeln haben die Priorität 18 und 19, daher haben sie Vorrang vor der Standard-Zulassungsregel.

Die Schlussfolgerung lautet, dass EPG App2 kein Preferred Group-Mitglied ist, da die expliziten Deny-Regeln eingehalten werden.

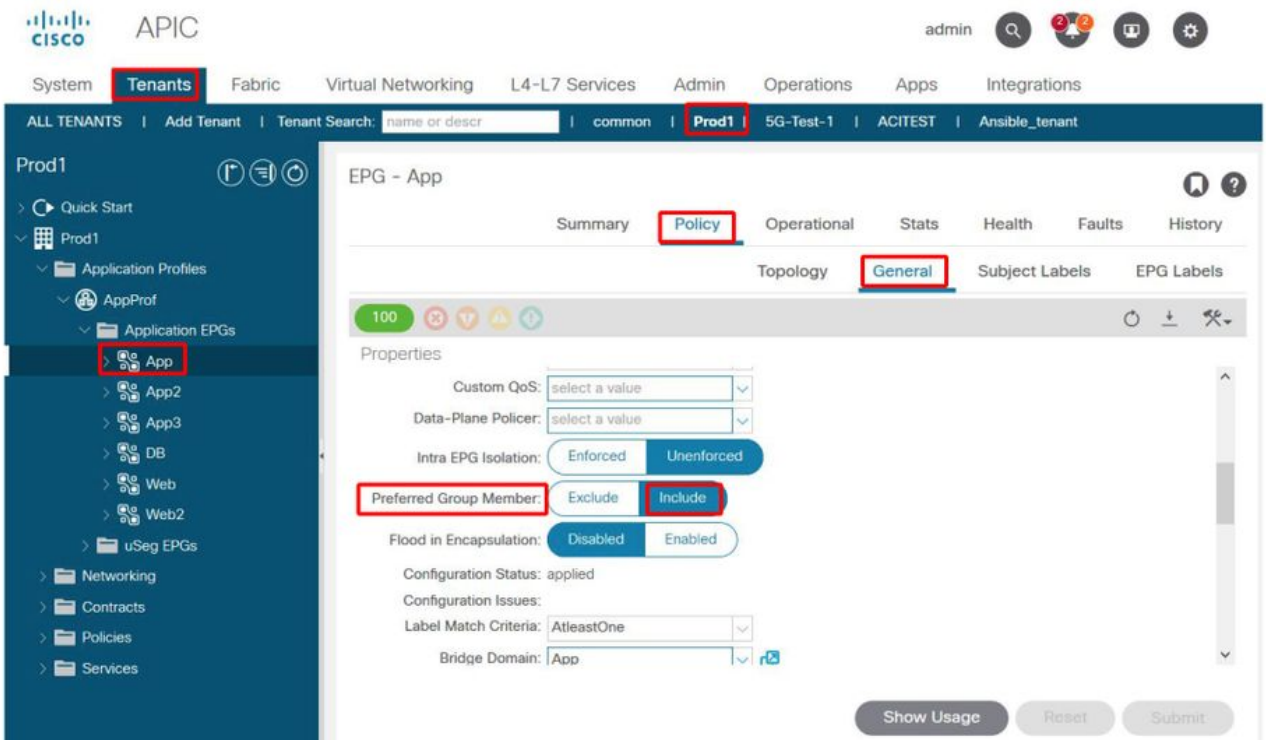
### 3. Konfiguration der bevorzugten Gruppenmitglieder für die EPG überprüfen

Navigieren Sie in der APIC-GUI, und überprüfen Sie die Konfiguration der bevorzugten Gruppenmitglieder für EPG App2 und EPG App Preferred Group. In der folgenden Abbildung ist EPG App2 nicht als bevorzugtes Gruppenmitglied konfiguriert.

### EPG App2 — Bevorzugte Gruppenmitgliedschaft ausgeschlossen



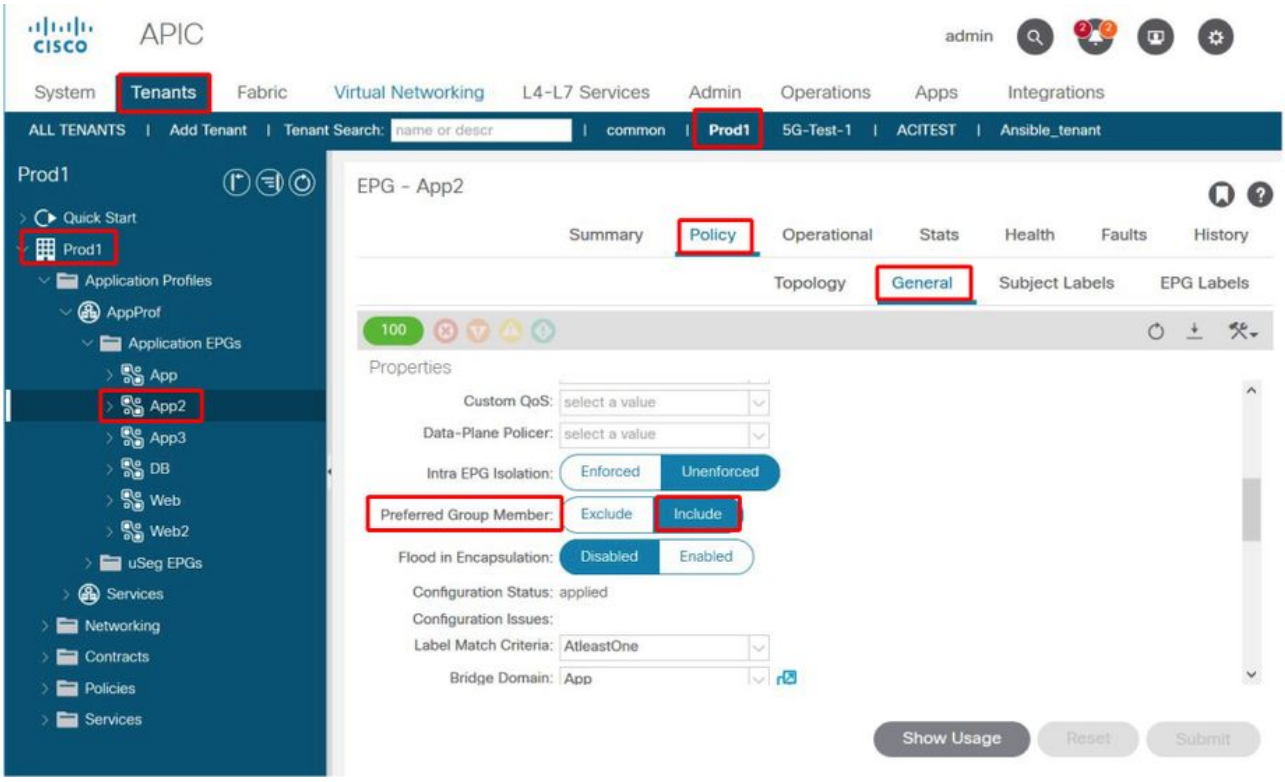

EPG-Anwendung - Einstellungen für bevorzugte Gruppenmitglieder enthalten




## 4. Setzen Sie EPG App2 als bevorzugtes Gruppenmitglied

Durch Ändern der Konfiguration der App2 EPG kann die bevorzugte Gruppe frei als Teil der bevorzugten Gruppe kommunizieren.

EPG App2 — Einstellungen für bevorzugte Gruppenmitglieder enthalten




**5. Überprüfen Sie die Vertragsprogrammierung mit contract_parser.py auf dem Leaf, auf dem sich das src-EP befindet.**

Verwenden Sie contract_parser.py erneut, und geben Sie den VRF-Namen an, um zu überprüfen, ob die expliziten Verweigerungsregeln für EPG App2 jetzt entfernt sind.

```
fab3-leaf8# contract_parser.py --vrf Prod1:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
[16:4176] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-App(16386) [contract:implicit] [hit=0]
[16:4160] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]
[18:4175] [vrf:Prod1:VRF1] deny,log any epg:16390 epg:any [contract:implicit] [hit=0]
[18:4167] [vrf:Prod1:VRF1] deny,log any epg:23 epg:any [contract:implicit] [hit=0]
[18:4156] [vrf:Prod1:VRF1] deny,log any tn-Prod1/vrf-VRF1(32770) epg:any [contract:implicit]
[hit=0]
[18:4168] [vrf:Prod1:VRF1] deny,log any epg:49159 epg:any [contract:implicit] [hit=0]
[19:4164] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
[19:4169] [vrf:Prod1:VRF1] deny,log any epg:any epg:16390 [contract:implicit] [hit=0]
[19:4159] [vrf:Prod1:VRF1] deny,log any epg:any epg:23 [contract:implicit] [hit=0]
[19:4174] [vrf:Prod1:VRF1] deny,log any epg:any epg:49159 [contract:implicit] [hit=0]
[20:4165] [vrf:Prod1:VRF1] permit any epg:any epg:any [contract:implicit] [hit=65]
```

Die expliziten Deny-Regeln für EPG App2 und sein pcTag 32775 werden in der obigen Ausgabe nicht mehr beachtet. Das bedeutet, dass der Datenverkehr zwischen EPs in EPG App und EPG App2 nun mit der impliziten Zulässigkeitsregel RuleId 4165 mit der höchsten Priorität von 20 übereinstimmt.

# vzAny zu EPG

## Info über vzAny

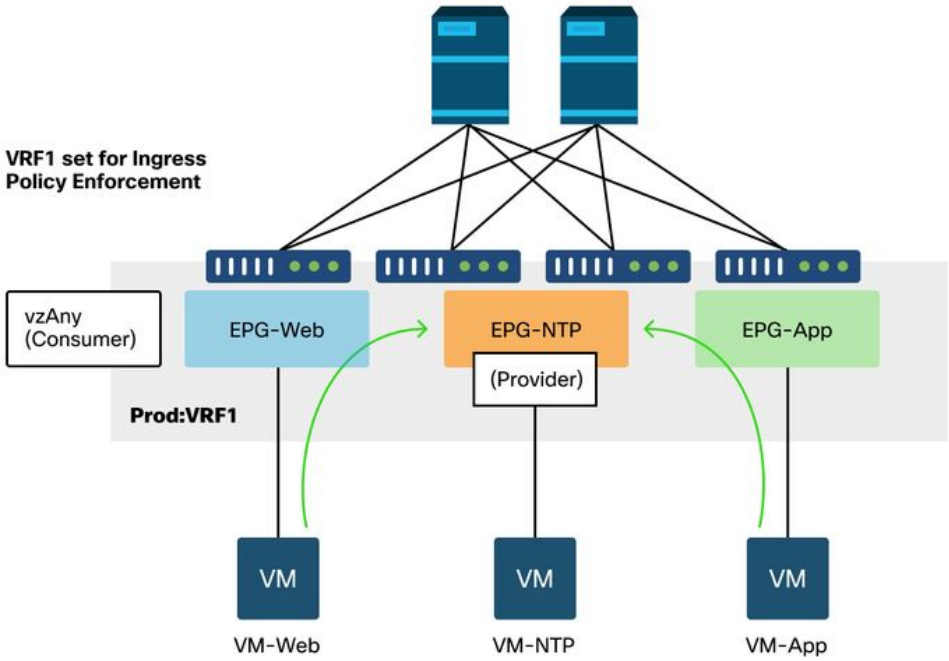
Beim Konfigurieren von Verträgen zwischen einer oder mehreren EPGs können Verträge

entweder als verwendete oder bereitgestellte Beziehung konfiguriert werden. Mit steigender Anzahl EPGs kann auch die Anzahl der Vertragsbeziehungen zwischen ihnen zunehmen. In einigen gängigen Anwendungsfällen müssen alle EPGs Datenverkehrsflüsse mit einer anderen spezifischen EPG austauschen. Ein solcher Anwendungsfall könnte eine EPG mit EPs sein, die Dienste bereitstellen, die von allen anderen EPGs innerhalb derselben VRF-Instanz genutzt werden müssen (z. B. NTP oder DNS). vzAny ermöglicht einen geringeren betrieblichen Aufwand bei der Konfiguration der Vertragsbeziehungen zwischen allen EPGs und bestimmten EPGs, die Services bereitstellen, die von allen anderen EPGs genutzt werden. Darüber hinaus ermöglicht vzAny eine wesentlich effizientere Nutzung von Sicherheitsrichtlinien-CAMs auf Leaf-Switches, da für jede vzAny-Vertragsbeziehung nur 2 Zoning-Regeln hinzugefügt werden.

## Anwendungsbeispiel

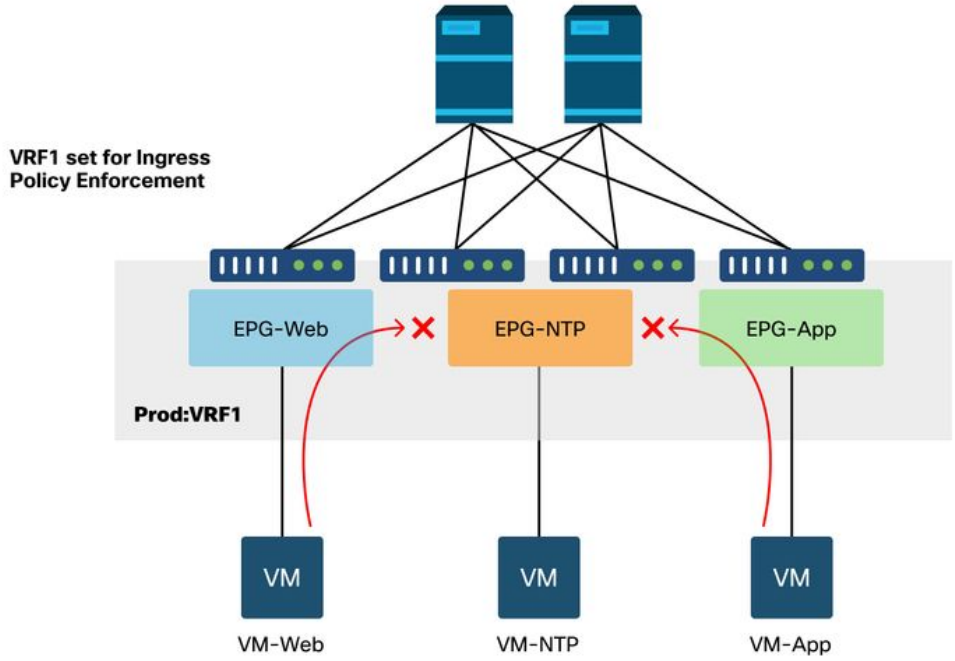
Die folgende Abbildung beschreibt einen solchen Anwendungsfall, bei dem VM-Web und VM-App in EPGs Web bzw. App NTP-Services von VM-NTP in EPG-NTP nutzen müssen. Anstatt einen bereitgestellten Vertrag für das EPG-NTP zu konfigurieren und anschließend denselben Vertrag wie einen genutzten Vertrag für das EPG-Web und die EPG-App zu haben, ermöglicht vzAny jeder EPG in VRF Prod:VRF1 die Nutzung von NTP-Services vom EPG-NTP.

**vzAny - Jede EPG in VRF Prod:VRF1 kann NTP-Services von EPG NTP nutzen**




Stellen Sie sich ein Szenario vor, in dem Verwerfungen zwischen EPGs beobachtet werden, die die NTP-Services nutzen, wenn es keinen Vertrag zwischen diesen gibt.

## Fehlerbehebungsszenario - Datenverkehr wird verworfen, wenn kein Vertrag besteht

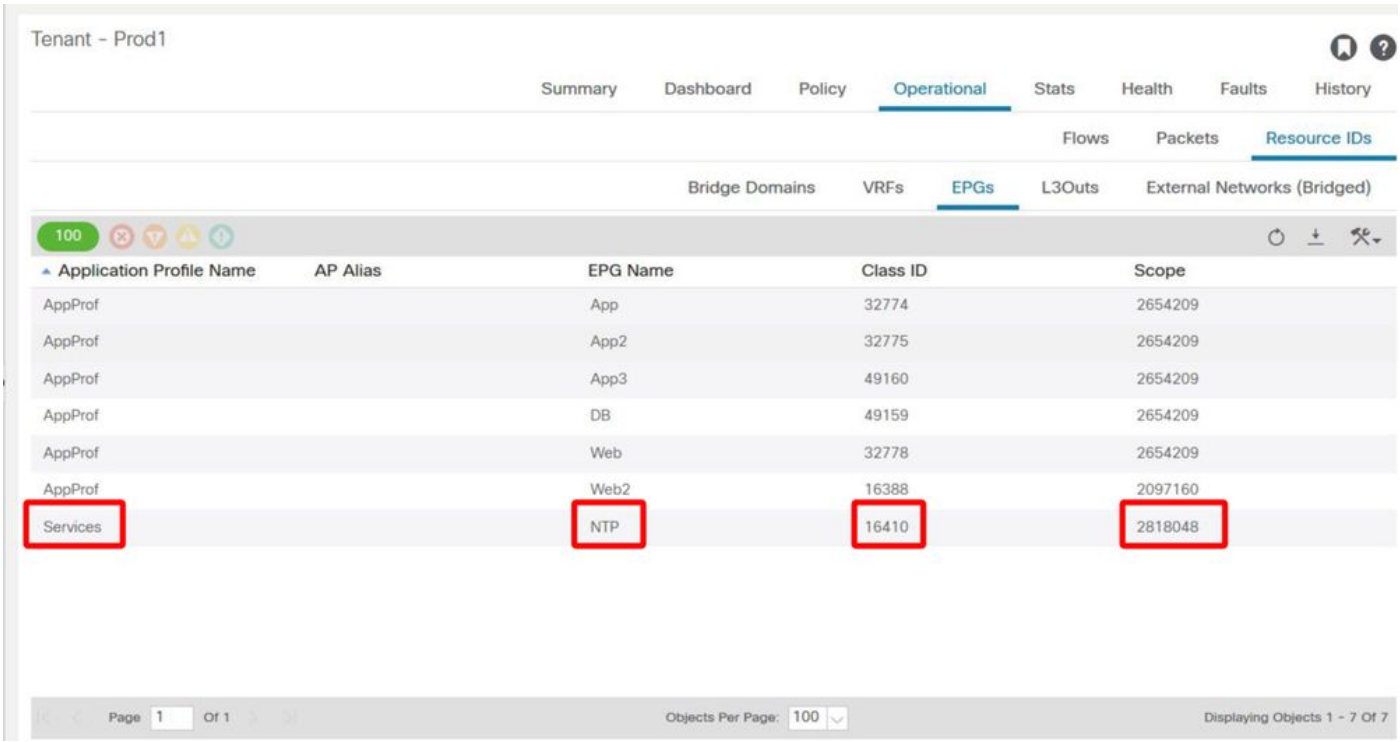



## Workflow

### 1. Das pcTag des EPG NTP und seine VRF VNID/Scope nachschlagen

'Tenant > Operational > Resource IDs > EPGs' ermöglicht das Finden des pcTag und des Geltungsbereichs

### EPG NTP pcTag und VRF-VNID/Scope

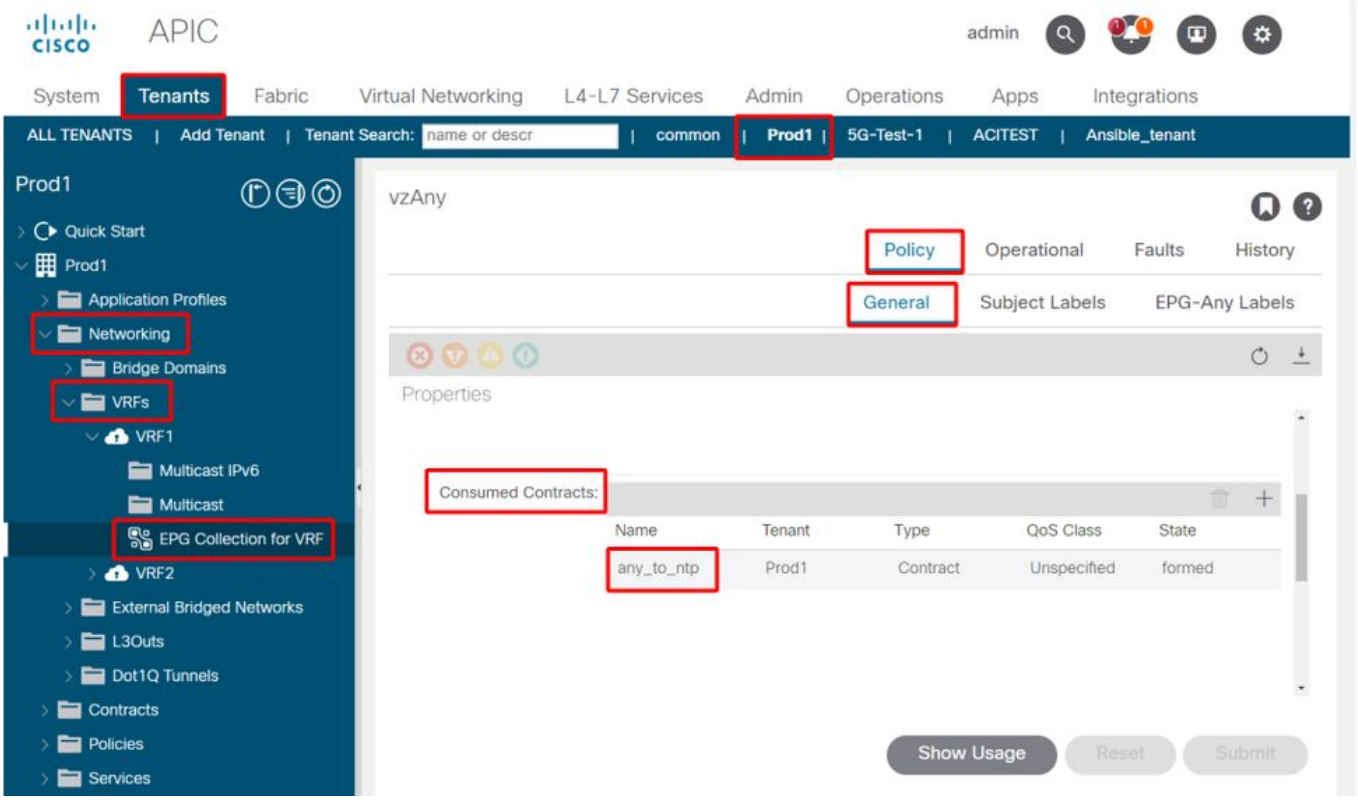



### 2. Überprüfen Sie, ob ein Vertrag als vzAny-Vertrag konfiguriert ist, der als Teil der VRF-Instanz

**genutzt wird.**

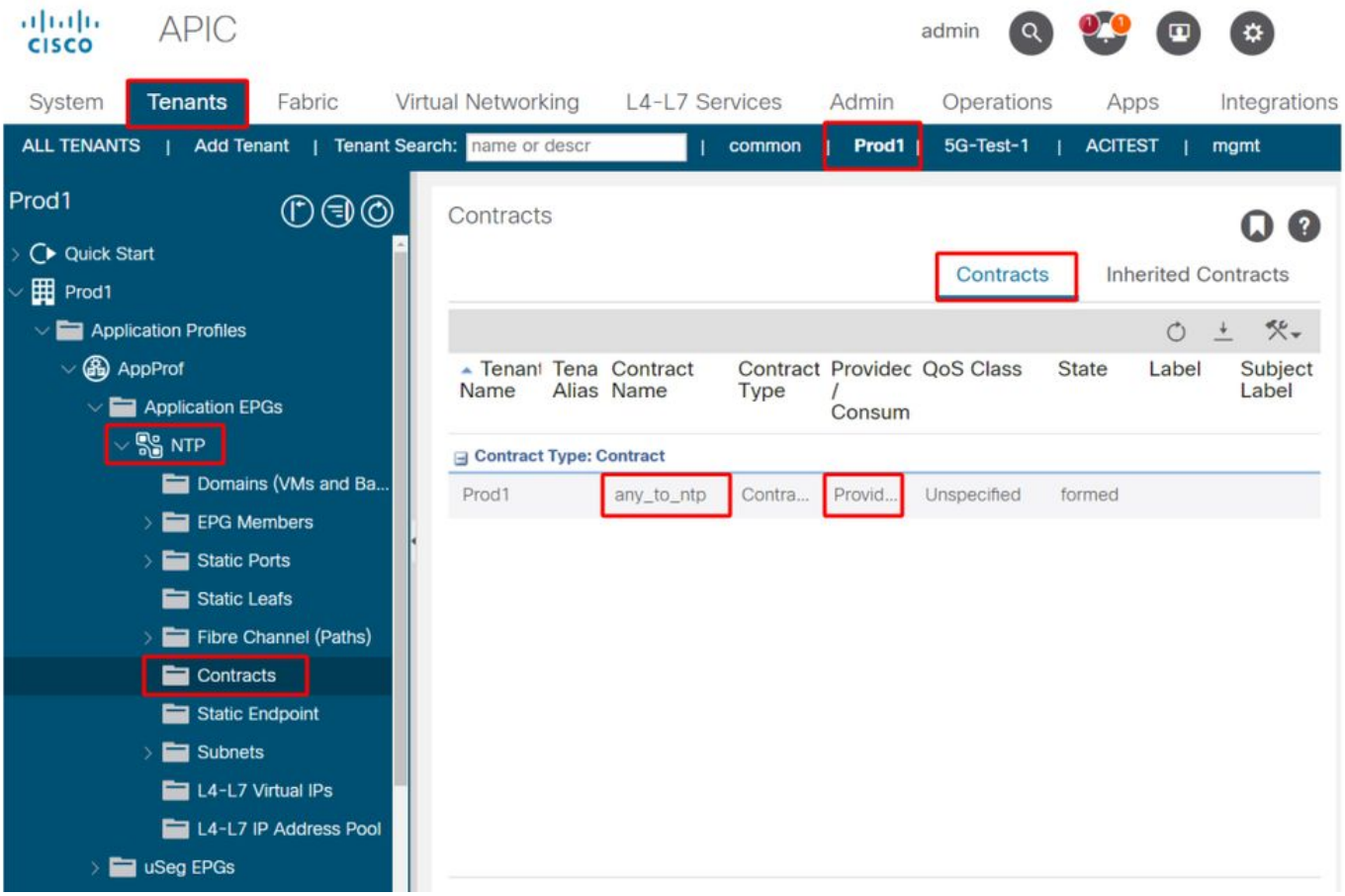
Navigieren Sie zur VRF-Instanz, und überprüfen Sie, ob unter "EPG Collection for VRF" ein als vzAny konfigurierter Consumed-Vertrag vorhanden ist.

**Vertrag als genutzter vz konfiguriertJeder Vertrag auf der VRF-Instanz**




**3. Überprüfen Sie, ob derselbe Vertrag wie ein bereitgestellter Vertrag auf das EPG NTP angewendet wird.**

Um eine Vertragsbeziehung herzustellen, muss derselbe Vertrag wie ein bereitgestellter Vertrag auf EPG NTP angewendet werden, das NTP-Services für die anderen EPGs in seiner VRF-Instanz bereitstellt.




### 4. Überprüfung der Zoning-Regel auf dem Eingangs-Leaf mit contract_parser.py oder 'show zoning-rule'

Der Eingangs-Leaf sollte über 2 Zoning-Regeln verfügen, um bidirektionale Datenverkehrsflüsse zwischen EPG und EPG-NTP zu ermöglichen (wenn der Vertragssubjekt so festgelegt ist, dass beide Richtungen zulässig sind). "Any EPG" wird in der Zoning-Regel-Programmierung als pcTag 0 bezeichnet.

Durch die Verwendung der Befehle contract_parser.py oder "show zoning-rule" auf dem Eingangs-Leaf und die Angabe der VRF-Instanz wird sichergestellt, dass die Zoning-Regel programmiert wird.

### Zoning-Regeln für den Datenverkehr zu/von EPG-NTP von anderen EPGs in der vorhandenen VRF-Instanz

Verwenden Sie contract_parser.py und 'show zoning-rule', um das Vorhandensein der vzAny-basierten Zoning-Regeln zu überprüfen.

Hier werden zwei Arten von Regeln deutlich:

1. Regel 4156 und Regel 4168, die Any (Alle) zum NTP zulassen und umgekehrt. Sie haben die Prioritäten 13 und 14: Zoning-Regel, die Datenverkehrsflüsse von jeder EPG (pcTag 0) zu EPG NTP (pcTag 49161) zulässt.Zoning-Regel, die Datenverkehrsflüsse von EPG NTP (pcTag 46161) zu einer anderen EPG (pcTag 0) zulässt.
2. Regel 4165, die die Any-to-Any-Verweigerungsregel (Standard) mit Priorität 21 ist.

Da die niedrigste Priorität Vorrang hat, haben alle EPGs der VRF-Instanz Zugriff auf die NTP-EPG.

```
fab3-leaf8# contract_parser.py --vrf Prod1:VRF
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]

[13:4156] [vrf:Prod1:VRF1] permit ip tcp tn-Prod1/ap-Services/epg-NTP(49161) eq 123 epg:any
[contract:uni/tn-Prod1/brc-any_to_ntp] [hit=0]
[14:4168] [vrf:Prod1:VRF1] permit ip tcp epg:any tn-Prod1/ap-Services/epg-NTP(49161) eq 123
[contract:uni/tn-Prod1/brc-any_to_ntp] [hit=0]
[16:4176] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-App(16386) [contract:implicit] [hit=0]
[16:4174] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-Services(32776) [contract:implicit]
[hit=0]
[16:4160] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]
[21:4165] [vrf:Prod1:VRF1] deny,log any epg:any epg:any [contract:implicit] [hit=65]
[22:4164] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]

fab3-leaf8# show zoning-rule scope 2654209
+---------+--------+--------+----------+---------+---------+---------+------------+----------+--
--------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |    Name    |  Action
|       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------+----------+--
--------------------+
|   4165  |   0    |   0    | implicit | uni-dir | enabled | 2654209 |            | deny,log |
any_any_any(21)    |
|   4160  |   0    |   0    | implarp  | uni-dir | enabled | 2654209 |            |  permit  |
any_any_filter(17)  |
|   4164  |   0    |   15   | implicit | uni-dir | enabled | 2654209 |            | deny,log |
any_vrf_any_deny(22) |
|   4176  |   0    | 16386  | implicit | uni-dir | enabled | 2654209 |            |  permit  |
any_dest_any(16)   |
|   4174  |   0    | 32776  | implicit | uni-dir | enabled | 2654209 |            |  permit  |
any_dest_any(16)   |
|   4168  |   0    | 49161  |   424    | uni-dir | enabled | 2654209 | any_to_ntp |  permit  |
any_dest_filter(14)  |
|   4156  | 49161  |   0    |   425    | uni-dir | enabled | 2654209 | any_to_ntp |  permit  |
src_any_filter(13)  |
+---------+--------+--------+----------+---------+---------+---------+------------+----------+--
--------------------+
```

# L3Out für EPG freigegeben

## Info über gemeinsam genutztes L3Out

Shared Layer 3 Out ist eine Konfiguration, die ein L3Out in einer VRF-Instanz zulässt, das einige Dienste bereitstellt (externer Zugriff), und eine oder mehrere andere VRFs nutzen dieses L3Out. Weitere Informationen zu gemeinsam genutztem L3Out finden Sie im Kapitel "Externes Routing".

Wenn Sie gemeinsam genutztes L3Out verwenden, wird empfohlen, dass der Anbieter des Vertrags das gemeinsam genutzte L3Out ist und die EPG der Verbraucher des Vertrags ist. Dieses Szenario wird in diesem Abschnitt veranschaulicht.

Es wird nicht empfohlen, das Gegenteil zu tun, d. h. L3Out nutzt einen Service, der von einer EPG bereitgestellt wird. Der Grund dafür liegt in der Skalierbarkeit, da bei Shared Services die Zoning-Regeln nur auf der VRF-Instanz des Verbrauchers installiert werden. Die Prinzipien von Consuming und Provisioning bezeichnen, wo Datenverkehrsflüsse initiiert werden. Bei der standardmäßigen Durchsetzung von Zugangsrichtlinien bedeutet dies, dass die Durchsetzung von Richtlinien auf der Verbraucherseite und insbesondere auf dem Eingangs-Leaf (nicht

grenzüberschreitend) erfolgt. Damit der Eingangs-Leaf die Richtlinie erzwingen kann, benötigt er das pcTag des Ziels. In diesem Szenario ist das externe EPG pcTag das Ziel. Der Eingangs-Leaf führt somit die Richtliniendurchsetzung durch und leitet die Pakete an den Grenz-Leaf weiter. Der Grenz-Leaf empfängt das Paket über seine Fabric-Verbindung, die eine Route Lookup (LPM) durchführt, und leitet das Paket an die Adjacency für das Zielpräfix weiter.

Der Grenz-Leaf führt jedoch KEINE Richtliniendurchsetzung durch, wenn Datenverkehr an das Ziel-EP gesendet wird, und tut dies auch nicht, wenn der zurückkehrende Datenverkehr an das Quell-EP zurückfließt.

Daher sind nur auf dem Richtlinien-CAM des Eingangs-Nicht-BL-Leaf Einträge installiert (im Verbraucher-VRF), und der Richtlinien-CAM des BL ist davon nicht betroffen.

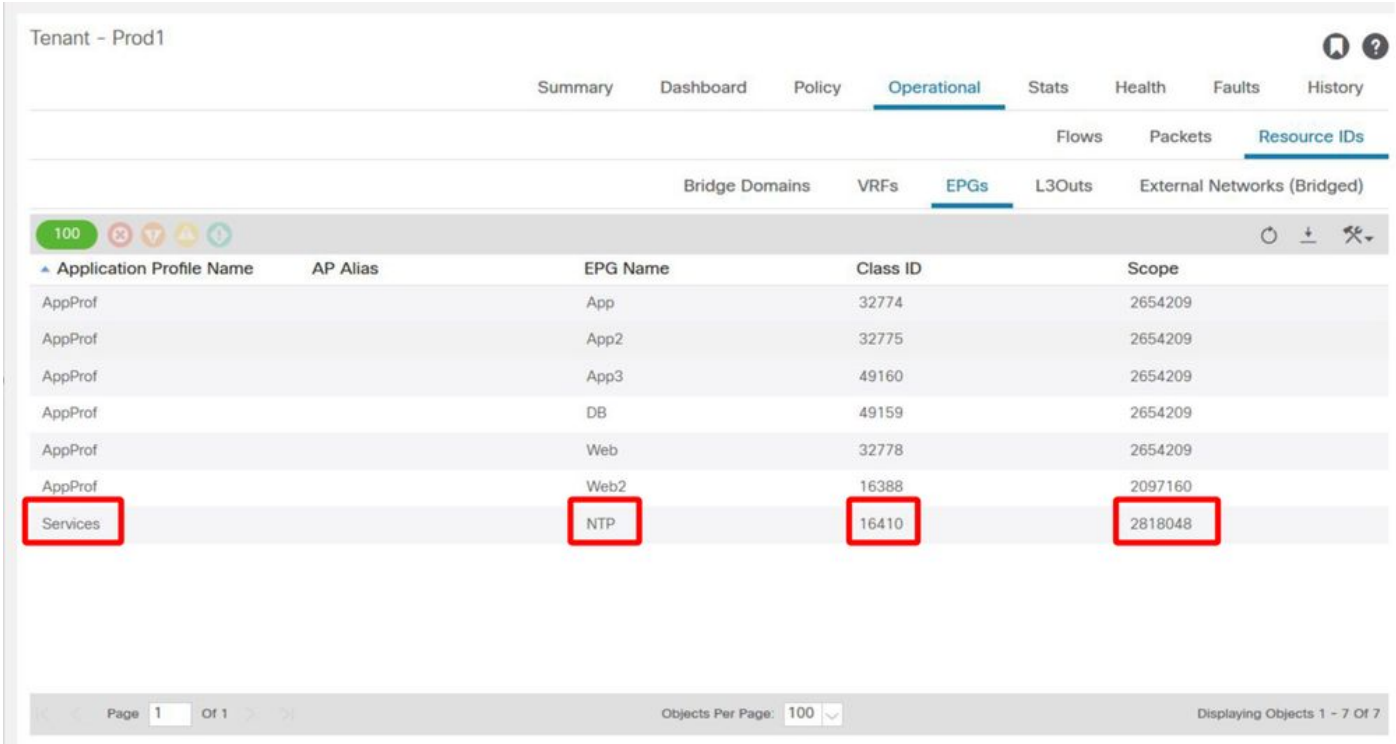
## Fehlerbehebung bei einem gemeinsam genutzten L3out

### Workflow

### 1. Überprüfen Sie EPG pcTag und VRF VNID/Scope für die Verbraucher-EPG

Bei gemeinsam genutztem L3Out werden die Zoning-Regeln nur im Verbraucher-VRF installiert. Der Anbieter muss über ein globales pcTag (unter 16k) verfügen, das die Verwendung dieses pcTags in allen Consumer-VRFs ermöglicht. In unserem Szenario ist der Anbieter die externe EPG und verfügt über ein globales pcTag. Die Verbraucher-EPG verfügt wie gewohnt über ein lokales pcTag.

### pcTag der Verbraucher-EPG

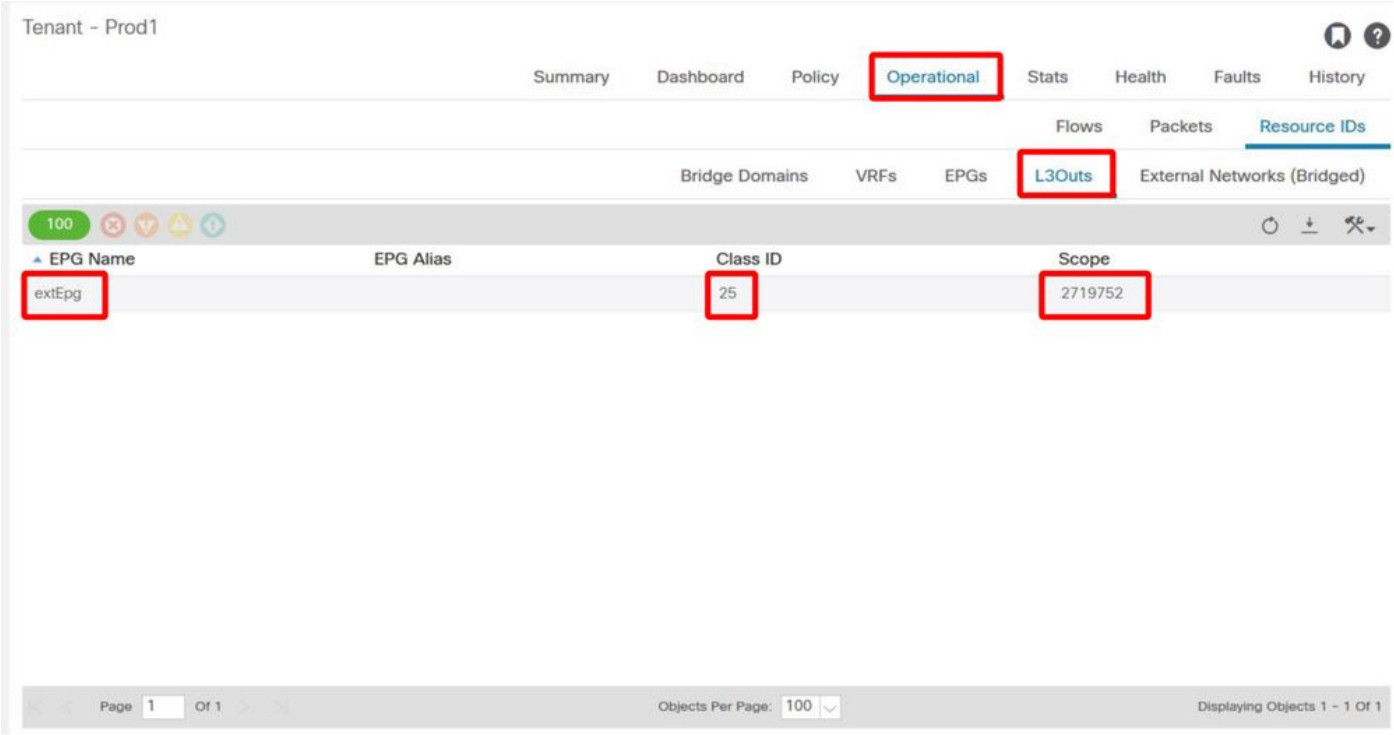



### 2. Überprüfen Sie das pcTag und VRF VNID/Scope für die Provider L3Out EPG.

Wie in Schritt 1 angegeben, verfügt die L3Out-EPG des Anbieters über einen globalen Bereich für pcTag als Präfixe von L3Out, die in die VRF-Instanz des Verbrauchers gelangen. Daher muss sich das L3Out EPG pcTag nicht mit pcTags im Consumer-VRF überschneiden und liegt somit im

globalen pcTag-Bereich.

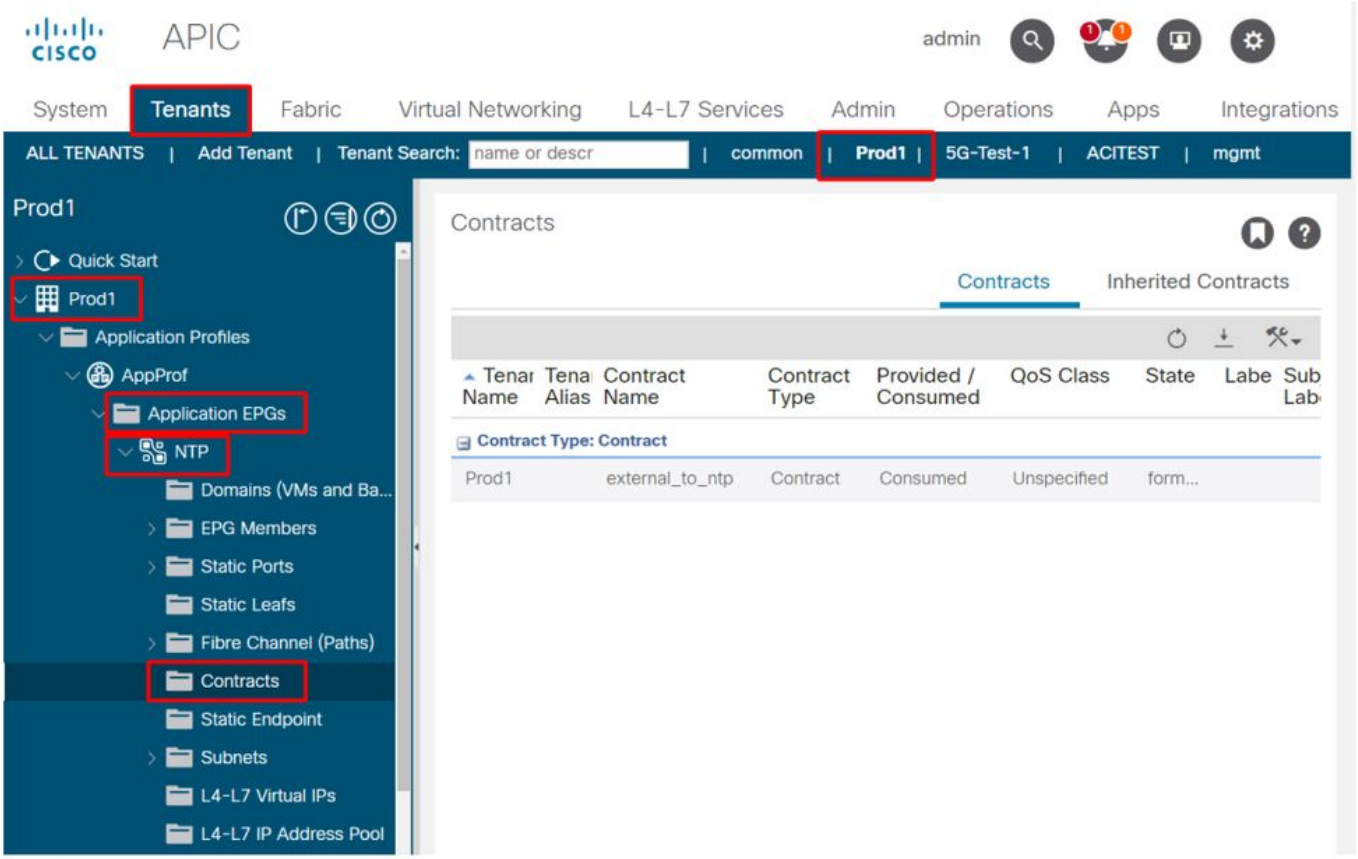
### pcTag des Anbieters externe EPG




### 3. Vergewissern Sie sich, dass für die Consumer-EPG entweder ein importierter Tenant-Vertrag oder ein globaler Vertrag konfiguriert ist.

Das EPG-NTP des Privatnutzers mit dem in der EPG/BD definierten Subnetz nutzt den Vertrag mit dem Gültigkeitsbereich "Tenant" oder "global".

### Von EPG genutzter Vertrag



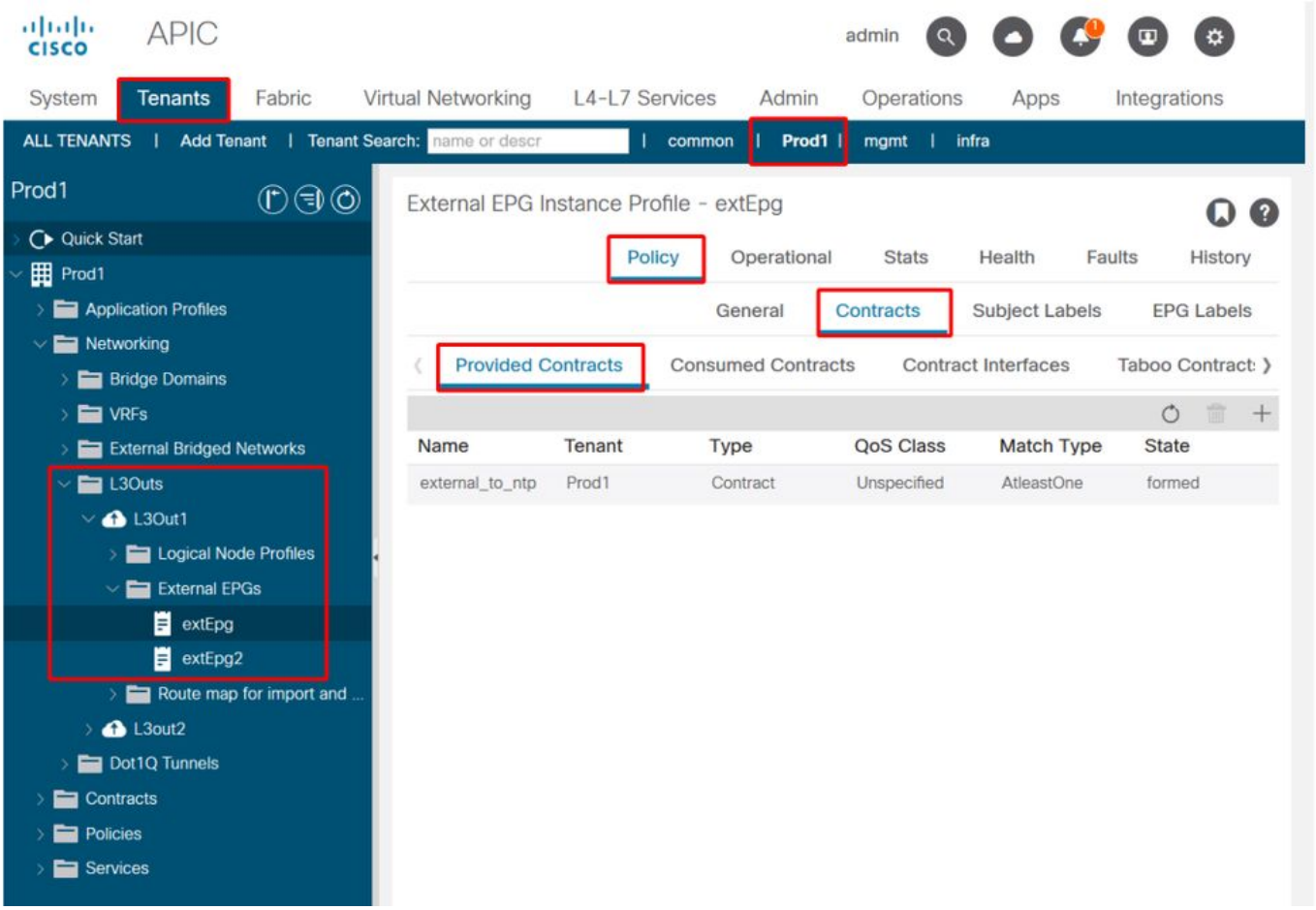

**4. Überprüfen Sie, ob für den BD der Consumer-EPG ein Subnetz konfiguriert ist, dessen Bereich auf "Shared between VRFs" (Gemeinsam genutzte VRFs) festgelegt ist.**

Das Subnetz der EPG wird unter der Bridge-Domäne konfiguriert, muss jedoch das Flag "shared between VRF" (für das Routing von Lecks) und das Flag "advertised external" (für das Ankündigen von L3Out) aufweisen.

**5. Überprüfen Sie, ob für die L3Out-EPG des Anbieters entweder ein importierter Vertrag mit Tenant-Gültigkeitsbereich oder ein globaler Vertrag konfiguriert ist.**

Für die L3Out-EPG muss entweder ein Vertrag mit Tenant-Umfang oder ein globaler Vertrag als bereitgestellter Vertrag konfiguriert sein.

**Vertrag bei Anbieter L3Out**



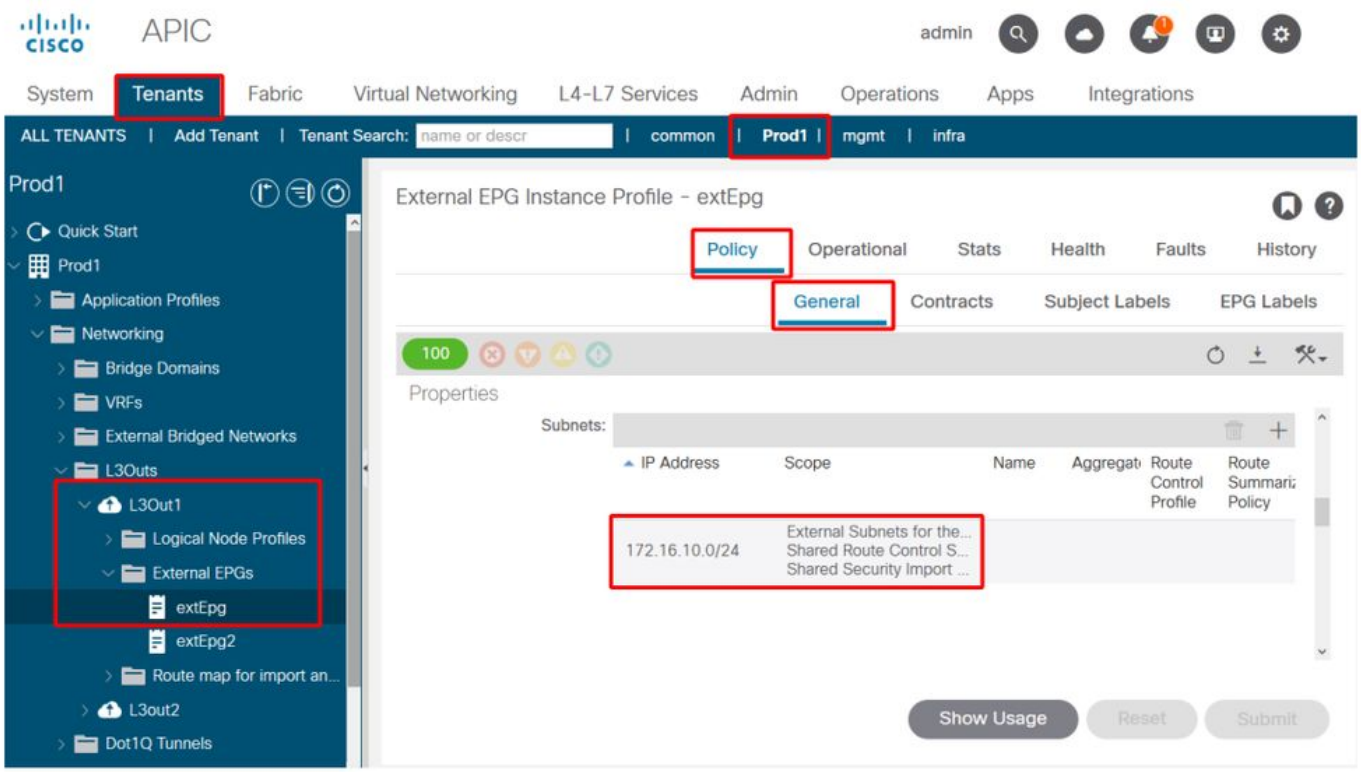

**6. Überprüfen Sie, ob für die L3Out-EPG des Anbieters ein Subnetz konfiguriert ist, das die erforderlichen Bereiche aktiviert hat.**

Für die Provider-L3Out-EPG sollte das zu durchsickernde Präfix mit den folgenden Bereichen konfiguriert sein:

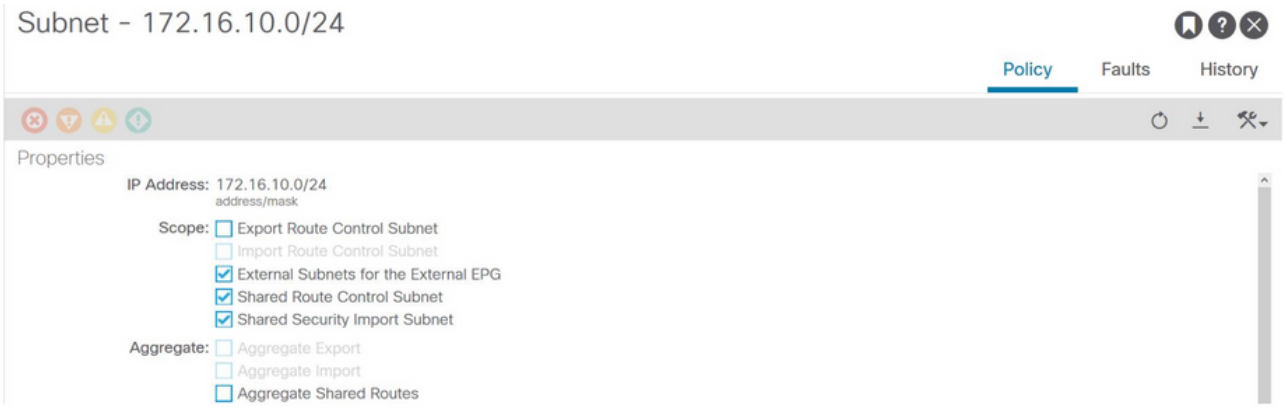
- Externe Subnetze für die externe EPG.
- Gemeinsam genutztes Subnetz für die Routenkontrolle
- Subnetz für gemeinsamen Sicherheitsimport.

Weitere Informationen zur Subnetzflagge in der L3Out-EPG finden Sie im Kapitel "Externe Weiterleitung".

**Externe EPG-Subnetzeinstellungen**




### Erweiterte externe EPG-Subnetzeinstellungen




### 7. Überprüfen Sie das pcTag des L3Out-EPG-Subnetzes auf dem Nicht-BL für die VRF-Instanz des Verbrauchers.

Wenn Datenverkehr, der an das externe EPG-Subnetz gerichtet ist, die Nicht-BL-Domäne erreicht, wird anhand des Zielpräfix eine Suche durchgeführt, um das pcTag zu ermitteln. Dies kann mit dem folgenden Befehl auf der anderen Seite überprüft werden.

Diese Ausgabe erfolgt im Rahmen des VNI 2818048, der VRF-VNID des Verbrauchers. In der Tabelle kann der Verbraucher das pcTag des Ziels finden, auch wenn es sich nicht im gleichen VRF befindet.

```
fab3-leaf8# vsh -c 'show system internal policy-mgr prefix' | egrep 'Vrf-Vni|==|common:default'
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name
Addr                                Class Shared Remote Complete
======= ======  ========== =======  ============================
================================= ====== ====== ====== ========
2818048 19     0x13          Up     common:default
0.0.0.0/0   15      False  False  False
```

```
2818048 19     0x80000013    Up     common:default
::/0   15      False  False  False
2818048 19     0x13          Up     common:default
172.16.10.0/24  25      True   True   False
```

Die obige Ausgabe zeigt die Kombination des L3Out EPG-Subnetzes und seines globalen pcTag 25.

### 8. Überprüfen Sie die programmierten Zoning-Regeln auf dem Nicht-BL für das Verbraucher-VRF.

Verwenden Sie entweder den Befehl "contract_parser.py" oder den Befehl "show zoning-rule", und geben Sie die VRF-Instanz an.

Im Folgenden werden zwei Zoning-Regeln angezeigt, die den Datenverkehr vom lokalen pcTag 16410 der Consumer-EPG zum globalen pcTag 25 der L3Out-EPG zulassen. Dies ist im Bereich 2818048, dem Bereich der Consumer-VRF-Instanz.

```
fab3-leaf8# show zoning-rule scope 2818048
+---------+--------+--------+----------+----------------+---------+---------+----------------+-
---------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |       Name      |
Action  |        Priority       |
+---------+--------+--------+----------+----------------+---------+---------+----------------+-
---------+----------------------+
|   4174  |   0    |   0    | implarp  |    uni-dir     | enabled | 2818048 |                 |
permit  |   any_any_filter(17)  |
|   4168  |   0    |   15   | implicit |    uni-dir     | enabled | 2818048 |                 |
deny,log |  any_vrf_any_deny(22) |
|   4167  |   0    | 32789  | implicit |    uni-dir     | enabled | 2818048 |                 |
permit  |    any_dest_any(16)   |
|   4159  |   0    |   0    | implicit |    uni-dir     | enabled | 2818048 |                 |
deny,log |    any_any_any(21)    |
|   4169  |   25   |   0    | implicit |    uni-dir     | enabled | 2818048 |                 |
deny,log | shsrc_any_any_deny(12)|
|   4156  |   25   | 16410  |   425    | uni-dir-ignore | enabled | 2818048 | external_to_ntp |
permit  |     fully_qual(7)     |
|   4131  | 16410  |   25   |   424    |     bi-dir     | enabled | 2818048 | external_to_ntp |
permit  |     fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+----------------+-
---------+----------------------+

fab3-leaf8# contract_parser.py  --vrf common:default
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]

[7:4131] [vrf:common:default] permit ip tcp tn-Prod1/ap-Services/epg-NTP(16410) tn-Prod1/l3out-
L3Out1/instP-extEpg(25) eq 123  [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[7:4156] [vrf:common:default] permit ip tcp tn-Prod1/l3out-L3Out1/instP-extEpg(25) eq 123 tn-
Prod1/ap-Services/epg-NTP(16410)  [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[12:4169] [vrf:common:default] deny,log any tn-Prod1/l3out-L3Out1/instP-extEpg(25) epg:any
[contract:implicit] [hit=0]
[16:4167] [vrf:common:default] permit any epg:any tn-Prod1/bd-Services(32789)
[contract:implicit] [hit=0]
[16:4174] [vrf:common:default] permit arp epg:any epg:any [contract:implicit] [hit=0]
[21:4159] [vrf:common:default] deny,log any epg:any epg:any [contract:implicit] [hit=0]
[22:4168] [vrf:common:default] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit]
[hit=0]
```

### 9. Überprüfen Sie die programmierten Zoning-Regeln auf dem BL für das Provider-VRF.

Verwenden Sie entweder den Befehl "contract_parser.py" oder den Befehl "show zoning-rule", und geben Sie die VRF-Instanz an. Die folgenden Befehlsausgaben zeigen, dass es **KEINE** spezifischen Zoning-Regeln in der Provider-VRF-Instanz gibt, wie zuvor mehrmals beschrieben.

Der Bereich 2719752 gehört zum Bereich von Provider-VRF.

```
border-leaf# show zoning-rule scope 2719752
+---------+--------+--------+----------+----------------+---------+---------+-------------+----
------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |     Name    |
Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+-------------+----
------+----------------------+
|   4134  | 10937  |   24   | default  | uni-dir-ignore | enabled | 2719752 | vrf1_to_vrf2 |
permit  |    src_dst_any(9)    |
|   4135  |   24   | 10937  | default  |     bi-dir     | enabled | 2719752 | vrf1_to_vrf2 |
permit  |    src_dst_any(9)    |
|   4131  |   0    |   0    | implicit |    uni-dir     | enabled | 2719752 |              |
deny,log |   any_any_any(21)    |
|   4130  |   0    |   0    | implarp  |    uni-dir     | enabled | 2719752 |              |
permit  |  any_any_filter(17)  |
|   4132  |   0    |   15   | implicit |    uni-dir     | enabled | 2719752 |              |
deny,log | any_vrf_any_deny(22) |
+---------+--------+--------+----------+----------------+---------+---------+-------------+----
------+----------------------+

border-leaf# contract_parser.py --vrf Prod1:VRF3
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]

[9:4134] [vrf:Prod1:VRF3] permit any tn-Prod1/l3out-L3Out1/instP-extEpg2(10937) tn-Prod1/l3out-
L3Out2/instP-extEpg2(24) [contract:uni/tn-Prod1/brc-vrf1_to_vrf2] [hit=0]
[9:4135] [vrf:Prod1:VRF3] permit any tn-Prod1/l3out-L3Out2/instP-extEpg2(24) tn-Prod1/l3out-
L3Out1/instP-extEpg2(10937) [contract:uni/tn-Prod1/brc-vrf1_to_vrf2] [hit=0]
[16:4130] [vrf:Prod1:VRF3] permit arp epg:any epg:any [contract:implicit] [hit=0]
[21:4131] [vrf:Prod1:VRF3] deny,log any epg:any epg:any [contract:implicit] [hit=0]
[22:4132] [vrf:Prod1:VRF3] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
```

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.