ACI-beveiligingsbeleid voor probleemoplossing - contracten

Inhoud

Inleiding

Dit document beschrijft stappen om ACI-beveiligingsbeleid te begrijpen en problemen op te lossen, bekend als contracten.

Achtergrondinformatie

Het materiaal van dit document is afgeleid uit het boek Problemen oplossen van Cisco Application Centric Infrastructure, Second Edition, met name het Security Policies - Overzicht, Security Policies - Tools, **Security Policies - EPG naar EPG**, **Security Policies - Preferred group** en **Security Policies - vzAny naar EPG** hoofdstukken.

Overzicht

De fundamentele veiligheidsarchitectuur van de ACI-oplossing volgt een permitlist-model. Tenzij een VRF in **ongedwongen** modus is geconfigureerd, worden alle EPG naar EPG verkeersstromen impliciet verwijderd. Zoals wordt geïmpliceerd door het out-of-the-box permitlist model, is de standaard VRF-instelling in **afgedwongen** modus. Verkeersstromen kunnen worden toegestaan of expliciet worden ontkend door regels voor de indeling in zones op de knooppunten van de switch te implementeren. Deze zoning-regels kunnen in een verscheidenheid van verschillende configuraties afhankelijk van de gewenste communicatie stroom tussen eindpuntgroepen (EPG) en de methode worden geprogrammeerd worden gebruikt om hen te bepalen. Merk op dat de

zoning-regel ingangen niet stateful zijn en zullen typisch toestaan/ontkennen gebaseerd op haven/contactdoos gegeven twee EPGs zodra de regel is geprogrammeerd.

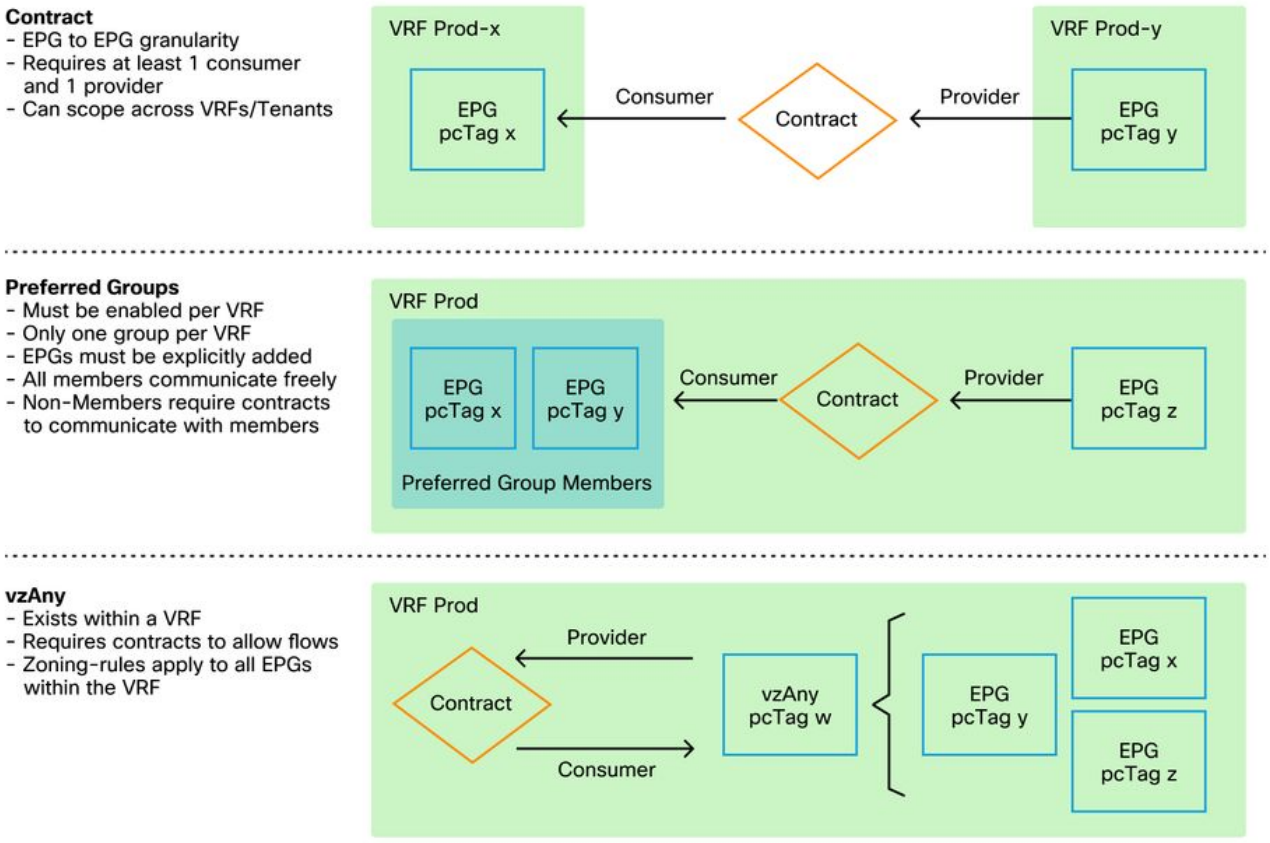
Methoden om de regels voor de indeling in zones te programmeren

De belangrijkste methoden om de regels voor de indeling in zones binnen de ACI te programmeren, zijn:

- **EPG-to-EPG contracten:** vereist doorgaans ten minste één consument en één provider om zoningregels te programmeren voor twee of meer verschillende endpointgroepen.
- **Voorkeursgroepen:** vereist groepering op VRF-niveau mogelijk te maken; per VRF kan slechts één groep bestaan. Alle leden van de groep kunnen vrij communiceren. Niet-leden verlangen contracten om stromen naar de voorkeursgroep toe te staan.
- **vzAny:** een 'EPG Collection' die is gedefinieerd onder een gegeven VRF. vzAny vertegenwoordigt alle EPG's in de VRF. Het gebruik van vzAny maakt stromen mogelijk tussen één EPG en alle EPG's binnen de VRF via één contractverbinding.

Het volgende diagram kan worden gebruikt om de granulariteit van de zoneringsregel aan te geven die elk van de bovenstaande methoden toestaat voor controle:

Vergelijking tussen de methoden met betrekking tot de zoneregels



Bij het gebruik van de contractmethode van de programmering van zoneregels, is er een optie voor het definiëren van de contractreikwijdte. Deze optie moet zorgvuldig worden overwogen als er een route lekt/gedeelde service ontwerp is vereist. Als de wens is om van de ene VRF naar de andere binnen de ACI-stof te komen, zijn contracten de methode om dit te doen.

De toepassingswaarden kunnen als volgt zijn:

- **Toepassing:** een contract-consument/aanbieder-relatie zal alleen programmaregels tussen EPG's programmeren die binnen hetzelfde toepassingsprofiel zijn gedefinieerd. Het hergebruiken van hetzelfde contract in andere Application Profile EPG's staat geen overspraak tussen deze contracten toe.
- **VRF (standaard):** een contract-consument/aanbieder-relatie programmeert regels tussen EPG's die binnen dezelfde VRF zijn gedefinieerd. Het hergebruiken van hetzelfde contract in andere Application Profile EPG's maakt overspraak tussen deze twee mogelijk. Zorg ervoor dat alleen de gewenste stromen zijn toegestaan, anders moet een nieuw contract worden gedefinieerd om onbedoelde overspraak te voorkomen.
- **huurder:** een contract-consument/aanbieder-relatie programmeert regels tussen EPG's die binnen dezelfde huurder zijn gedefinieerd. Als er EPG's zijn verbonden met meerdere VRF's binnen één huurder en zij verbruiken/leveren hetzelfde contract, kan dit bereik worden gebruikt om routelekkage te veroorzaken om interVRF-communicatie mogelijk te maken.
- **Wereldwijd:** een contract consument/leverancier relatie zal regels tussen EPG's over elke huurder binnen een ACI-stof programmeren. Dit is de grootst mogelijke reikwijdte van de definitie, en wanneer dit in eerder gedefinieerde contracten wordt toegestaan, moet grote voorzichtigheid worden betracht om onbedoelde lekkage te voorkomen.

Een regel voor zonering lezen

Zodra de zoneringsregel is geprogrammeerd, wordt deze op een blad als volgt weergegeven:

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

- **Regel-ID:** de ID van de regel. Geen echte betekenis, behalve dan als unieke identificator te fungeren.
- **Src EPG:** een unieke ID per VRF (pcTag) van de bronendpointgroep.
- **Dst EPG:** een unieke ID per VRF (pcTag) van de doelendpointgroep.
- **FilterID:** de ID van het filter waartegen de regel probeert aan te passen. Het filter bevat de protocolinformatie waartegen de regel zal overeenkomen.
- **Dir:** de richting van de regel van de zonering.
- **OperSt:** de operationele staat van de regel.
- **Toepassingsgebied:** een unieke ID van de VRF waartegen de regel zal overeenkomen.
- **Naam:** de naam van het contract dat heeft geleid tot de programmering van die vermelding.
- **Actie:** wat het blad zal doen als het overeenkomt met die ingang. Omvat: [Drop, Permit, Log, Redirect].
- **Prioriteit:** de volgorde waarin de zoneregels voor actie zullen worden gevalideerd, gegeven een bijpassende Scope, SrcEPG, DstEPG en Filter Vermeldingen.

Policy content-adresseerbaar geheugen (CAM)

Aangezien elke zoneringsregel geprogrammeerd wordt, zal een matrix van de zoneringsregel die tegen filteringangen in kaart wordt gebracht **Policy CAM** op de switches beginnen te verbruiken.

Bij het ontwerpen van toegestane stromen door een ACI-stof, moet speciale zorg worden genomen bij het hergebruiken van contracten, in plaats van het creëren van nieuwe, afhankelijk van het eindontwerp. Het toevallig hergebruiken van hetzelfde contract over meerdere EPG's zonder de resulterende zoning-regels te begrijpen kan snel in meerdere stromen worden gekaatst die onverwacht worden toegestaan. Tegelijkertijd zullen deze onbedoelde stromen beleidsCAM blijven consumeren. Wanneer Policy CAM volledig wordt, zal de zoning-regel programmering beginnen te mislukken wat kan resulteren in onverwacht en intermitterend verlies afhankelijk van configuratie en eindpunt gedrag.

VRF lekken, wereldwijde pcTags en beleidshandhaving directionaliteit van gedeelde L3Outs

Dit is een speciale callout voor de case voor het gebruik van de gedeelde diensten waarvoor contracten moeten worden geconfigureerd. Gedeelde services impliceren doorgaans interVRF-verkeer binnen een ACI-structuur die afhankelijk is van het gebruik van een 'huurder'- of 'wereldwijd'-toepassingscontract. Om dit volledig te begrijpen, moet men eerst het idee versterken dat de typische pcTag-waarde die aan EPG's wordt toegewezen niet wereldwijd uniek is. pcTags zijn scoped naar een VRF en dezelfde pcTag kan mogelijk worden hergebruikt binnen een andere VRF. Wanneer de discussie over weglekken opduikt, beginnen eisen op de ACI-stof af te dwingen, inclusief de behoefte aan wereldwijd unieke waarden, waaronder subnetten en pcTags.

Wat dit een bijzondere overweging maakt is het directionaliteitsaspect dat verbonden is aan een EPG als consument tegenover aanbieder. In een scenario met gedeelde services wordt van de provider verwacht dat hij een wereldwijde pcTag aanstuurt om een unieke waarde voor de stof te krijgen. Tegelijkertijd zal de consument zijn VRF-opgeruimde pcTag behouden, wat het in een speciale positie plaatst om nu het gebruik van de wereldwijde pcTag waarde te kunnen programmeren en begrijpen om beleid af te dwingen.

Ter referentie is de pcTag toewijzingsbereik als volgt:

- Gereserveerd systeem: 1-15.
- Wereldwijd bereik: 16-16384 voor gedeelde EPG’s van serviceproviders.
- Lokaal bereik: 16385-65535 voor EPG’s met VRF-scopie.

VRF-beleidscontrole, handhavingsrichting

In elke VRF is het mogelijk om de instelling van de afdwingingsrichting te definiëren.

- De standaardinstelling van de handhavingsrichting is Ingress.
- De andere optie voor handhavingsrichting is uitgaand.

Het begrip van waar het beleid wordt afgedwongen hangt van verscheidene verschillende variabelen af.

De onderstaande tabel helpt te begrijpen waar het beveiligingsbeleid op bladniveau wordt afgedwongen.

Waar wordt het beleid uitgevoerd?

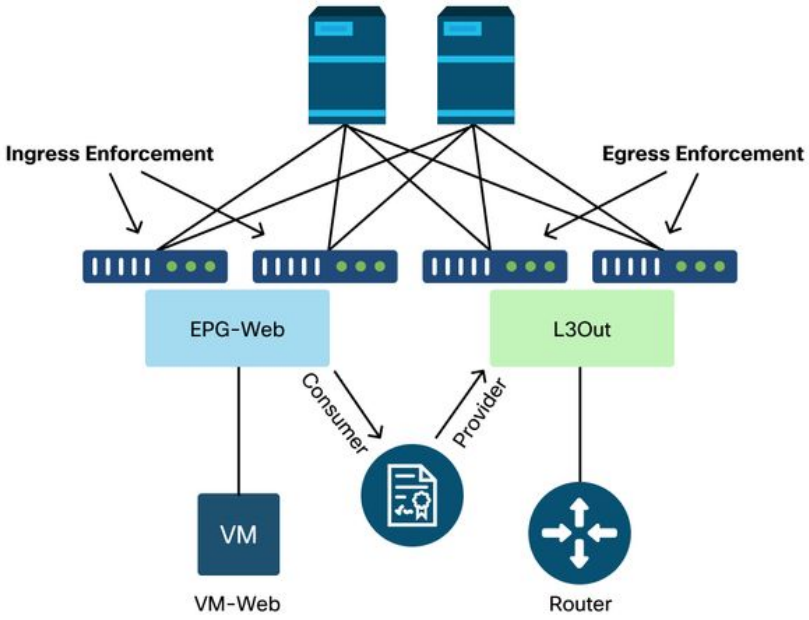
scenario	VRF-afdwingingsmodus	Consument	Provider	Gedwongen beleid
Intra-VRF	Ingang/uitgang	EPG	EPG	·Als eindpunt bestemming wordt

				aangeleerd: indringblad* ·Als eindpunt bestemming niet wordt geleerd: uitreisblad
	Ingress	EPG	L3Out-EPG	Consumentenblad (niet-grensblad)
	Ingress	L3Out-EPG	EPG	Dienstenblad (niet-grensblad)
	uitgang	EPG	L3Out-EPG	Grensblad -> niet-grensverkeer ·Als eindpunt bestemming wordt aangeleerd: grensblad
	uitgang	L3Out-EPG	EPG	·Als eindpunt bestemming niet wordt geleerd: niet-grensblad Buitengrensblad-> grensbladverkeer ·Grensblad
	Ingang/uitgang	L3Out-EPG	L3Out-EPG	Ingress leaf*
	Ingang/uitgang	EPG	EPG	Consumentenblad
	Ingang/uitgang	EPG	L3Out-EPG	Consumentenblad (niet-grensblad)
Inter-VRF	Ingang/uitgang	L3Out-EPG	EPG	Ingress leaf*
	Ingang/uitgang	L3Out-EPG	L3Out-EPG	Ingress leaf*

*Beleidshandhaving wordt toegepast op het eerste blad dat door het pakket wordt geraakt.

De onderstaande figuur illustreert een voorbeeld van contracthandhaving waar EPG-Web als consument en L3Out EPG als leverancier een intra-VRF contract hebben. Als VRF is ingesteld op Ingress-afdwingingsmodus, wordt het beleid afgedwongen door de bladknooppunten waar EPG-Web zich bevindt. Als de VRF is ingesteld op de uitgangshandhavingsmodus, wordt het beleid afgedwongen door de grensbladknooppunten waar L3Out zich bevindt als het VM-Web-eindpunt op het grensblad wordt geleerd.

Handhaving en uittreding uit de rechtshandhaving



Tools

Er zijn een verscheidenheid aan hulpmiddelen en opdrachten die kunnen worden gebruikt om te helpen bij de identificatie van een **beleidsdaling**. Een beleidsdruppel kan worden gedefinieerd als een pakketdruppel als gevolg van een contractconfiguratie of het ontbreken daarvan.

Validering van zones

De volgende tools en commando's kunnen worden gebruikt om de zoningregels die op switches geprogrammeerd zijn als gevolg van een afgewerkte contract-relatie tussen klant en aanbieder expliciet te valideren.

'regels inzake zonering weergeven'

Een opdracht op switch die alle zoneregels toont.

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

'zoneringsfilter tonen'

Een filter dat de sport/uitwijkinformatie bevat waarop de zoneringsregel werkt. De

filterprogrammering kan met deze opdracht worden geverifieerd.

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

"Toon systeem intern beleid-mgr stats"

Deze opdracht kan worden uitgevoerd om het aantal hits per zoning-rule te verifiëren. Dit is nuttig om te bepalen of een verwachte regel wordt geraakt in tegenstelling tot een andere, zoals een impliciete drop regel die een hogere prioriteit kan hebben.

```
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
```

'toon het registreren ip toegang-lijst intern pakketlogboek ontkennen'

Een opdracht op switch niveau die kan worden uitgevoerd op iBash-niveau en die ACL-gerelateerde (contract)dalingen en flow-gerelateerde informatie rapporteert, waaronder:

- VRF
- VLAN-ID
- MAC/Dest-broncode
- IP-bron/Dest IP
- Bronpoort/Dest-poort
- Broninterface

```
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
```

contract_parser

Een Python-script op het apparaat dat een uitvoer produceert die de zoningregels, filters en hit-statistieken correleert tijdens het uitvoeren van naamraadplegingen van ID's. Dit script is uitermate nuttig in die zin dat het een meerstappenproces neemt en het in één opdracht verandert die kan worden gefilterd naar specifieke EPG's/VRF's of op andere contractgerelateerde waarden.

```
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]
```

Validering van pakketclassificatie

ELAM

Een ASIC-rapport dat wordt gebruikt om te controleren of er gegevens worden doorgestuurd, wat bij een gedropt pakket de reden voor het uitzetten aangeeft. Relevant voor deze sectie, kan de reden een SECURITY_GROUP_DENY (contract policy drop) zijn.

fTriage

Een op Python gebaseerd hulpprogramma op de APIC die end-to-end pakketstroom met ELAM kan volgen.

ELAM Assistant-app

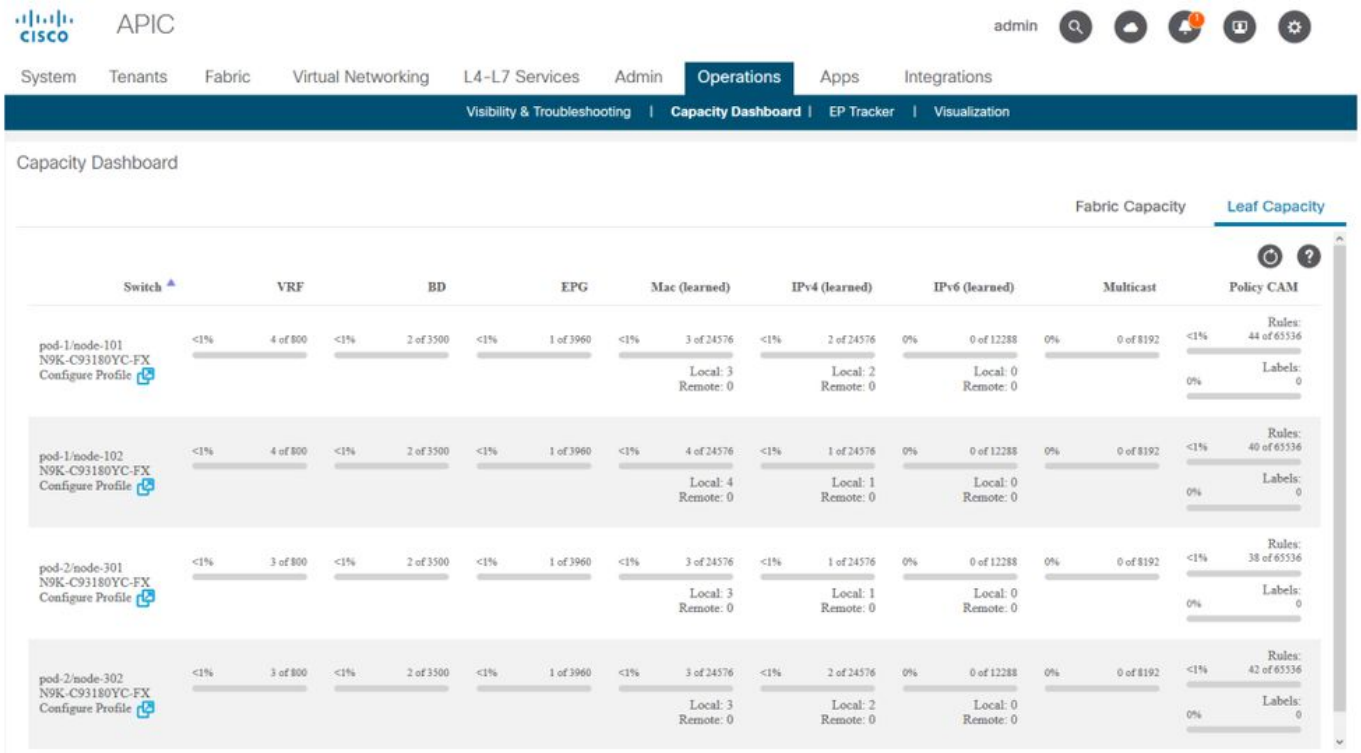
Een APIC-app die de complexiteit van verschillende ASIC's samenvat om het doorsturen van beslissingsinspectie veel handiger en gebruiksvriendelijker te maken.

Raadpleeg het gedeelte "Intra-Fabric Forwarding" voor meer informatie over de ELAM, fTriage en ELAM Assistant tools

Policy CAM-gebruik

Het gebruik van Policy CAM per blad is een belangrijke parameter om te monitoren om ervoor te zorgen dat de stof in een gezonde status is. De snelste manier om dat te controleren is door het 'Capacity Dashboard' te gebruiken binnen de GUI en expliciet de 'Policy Cam'-kolom te controleren.

De 'Leaf Capacity' weergave van Capacity Dashboard



"show platform interne hal gezondheid-stats"

Deze opdracht is handig voor het valideren van een verscheidenheid aan resourcegrenzen en gebruik, waaronder Policy CAM. Let op dat deze opdracht alleen uitgevoerd kan worden in vsh_lc, dus geef het door in de "-c" vlag als het vanaf iBash uitgevoerd wordt.

```
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 naar EPG

Algemene beleidsoverwegingen

Er zijn talrijke manieren om een connectiviteitskwestie tussen twee endpoints problemen op te lossen. De volgende methodologie biedt een goed uitgangspunt om snel en effectief te isoleren of het connectiviteitsprobleem het gevolg is van een **beleidsdaling** (geïnduceerd contract).

Enkele belangrijke vragen die het waard zijn om gesteld te worden voordat je binnenduikt:

- Zijn de eindpunten in dezelfde of een andere EPG? Het verkeer tussen twee eindpunten die in verschillende EPG's (inter-EPG) verblijven, wordt impliciet ontkend en vereist een contact om

communicatie toe te staan.Verkeer tussen twee eindpunten binnen hetzelfde EPG (intra-EPG) is impliciet toegestaan, tenzij intra-EPG isolatie in gebruik is.
- Wordt de VRF afgedwongen of niet afgedwongen? Wanneer een VRF in **afgedwongen** modus staat — binnen de VRF — moeten er contracten worden gesloten voor eindpunten in twee verschillende EPG's om te communiceren.Wanneer een VRF in **ongedwongen** modus staat — binnen de VRF — zou alle verkeer door de ACI-stof worden toegestaan over meerdere EPG's die tot de ongedwongen VRF behoren, ongeacht de ACI-contracten die worden toegepast.

Methodologie

Met de diverse beschikbare hulpmiddelen, zijn er sommige die geschikter en geschikter zijn om met dan anderen te beginnen, afhankelijk van het niveau van informatie reeds gekend over de beïnvloede stroom.

Is het volledige pad van het pakket in de ACI-stof bekend (indringblad, uitreisblad...)?

- Als het antwoord ja is, moet ELAM Assistant worden gebruikt om de reden van de val te identificeren op de bron of de switch van de bestemming.
- Als het antwoord neen is, zullen de Zichtbaarheid & het Oplossen van problemen, fTriage, contract_parser, het Operationele tabblad in de mening van de Huurder, en iBash bevelen helpen om de weg van het pakket te versmallen of meer zicht geven in de dalingsredenen.

Houd er rekening mee dat de tool fTriage niet in detail in deze sectie wordt besproken. Raadpleeg het hoofdstuk "Intra-Fabric Forwarding" voor meer informatie over het gebruik van deze tool.

Denk eraan dat, hoewel zichtbaarheid en probleemoplossing kunnen helpen om snel te visualiseren waar pakketten tussen twee eindpunten worden gelaten, fTriage meer diepgaande informatie toont voor verdere probleemoplossing. d.w.z. fTriage zal helpen interface, valreden, en andere lage details over de beïnvloede stroom identificeren

.

Dit voorbeeldscenario zal tonen hoe u een beleidsdaling tussen twee endpoints kunt oplossen: 192 168 21 11 en 192 168 23 11

Ervan uitgaande dat pakketdruppels tussen deze twee eindpunten worden ervaren, wordt de volgende workflow voor probleemoplossing gebruikt om de basisoorzaak van het probleem te identificeren:

Identificeer de src/dst-bladeren die bij de verkeersstroom betrokken zijn:

1. Gebruik **Zichtbaarheid en probleemoplossing** om de pakketstroom te traceren en vast te stellen welk apparaat het pakket laat vallen.
2. Voer de opdracht 'toon ip access-list van logboekregistratie interne pakketlogboekontkenning' uit op het geselecteerde apparaat. Als een pakket met een van de IP-adressen van belang wordt geweigerd en vastgelegd, wordt het **pakketlogboek** per hit afgedrukt met de relevante endpoint- en contractnaam.
3. Gebruik opdracht 'contract_parser.py —vrf <tenant>:<VRF>' op bron- en doelblad om hit count te observeren voor het geconfigureerde contract: Als een pakketpakket de switch van de bron of van de bestemming raakt, wordt de teller van het desbetreffende contract

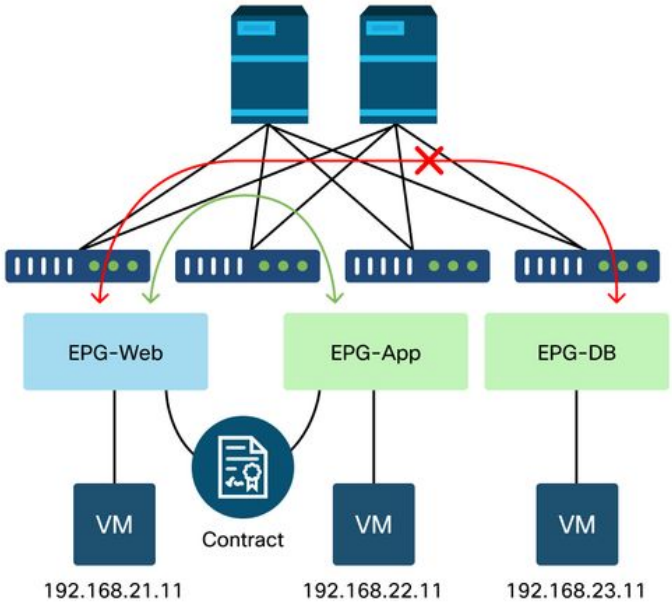
verhoogdDeze methode is minder granulair dan die van IP-toegangslijst intern pakketlogboek in situaties waarin veel stromen dezelfde regel zouden kunnen raken (veel endpoints/stromen tussen de twee EPG's die van belang zijn).

De bovenstaande stappen worden in de volgende paragraaf nader beschreven.

Voorbeeld van probleemoplossing scenario EPG naar EPG

Dit voorbeeldscenario zal tonen hoe u een beleidsdaling tussen twee endpoints kunt oplossen: 192.168.21.11 in EPG-Web en 192.168.23.11 in EPG-DB.

Topologie

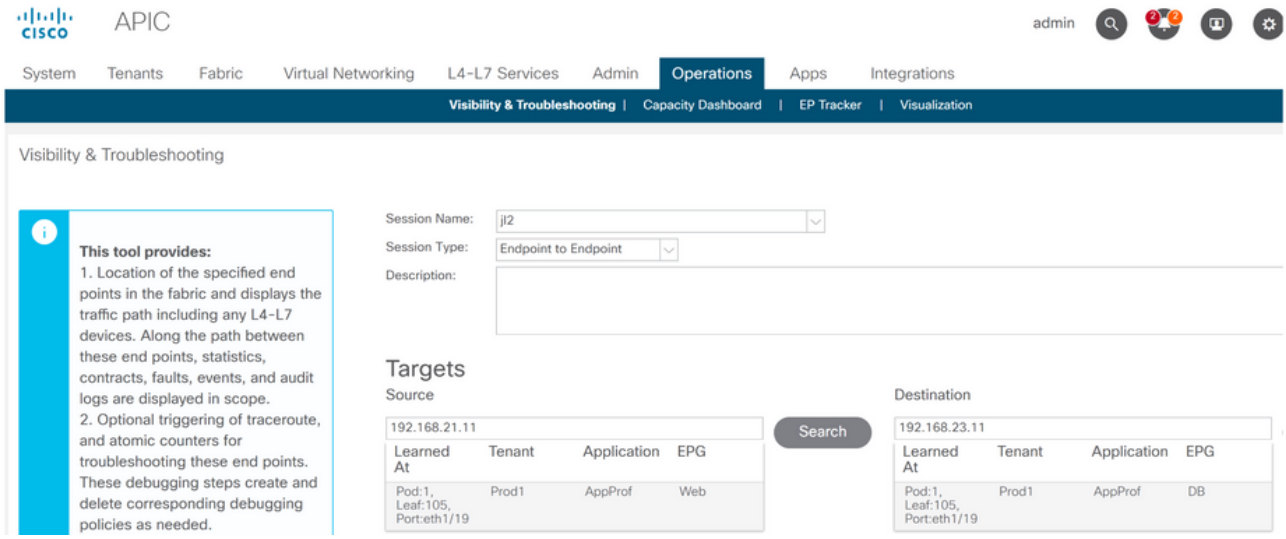


Identificeer de switches van het bron- en doelblad die bij de pakketdaling betrokken zijn

Zichtbaarheid en probleemoplossing

De tool Zichtbaarheid en probleemoplossing helpt de switch waar de pakketdaling heeft plaatsgevonden voor een specifieke EP-naar-EP-stroom te visualiseren en te identificeren waar pakketten mogelijk zijn gedropt.

Configuratie van zichtbaarheid en probleemoplossing

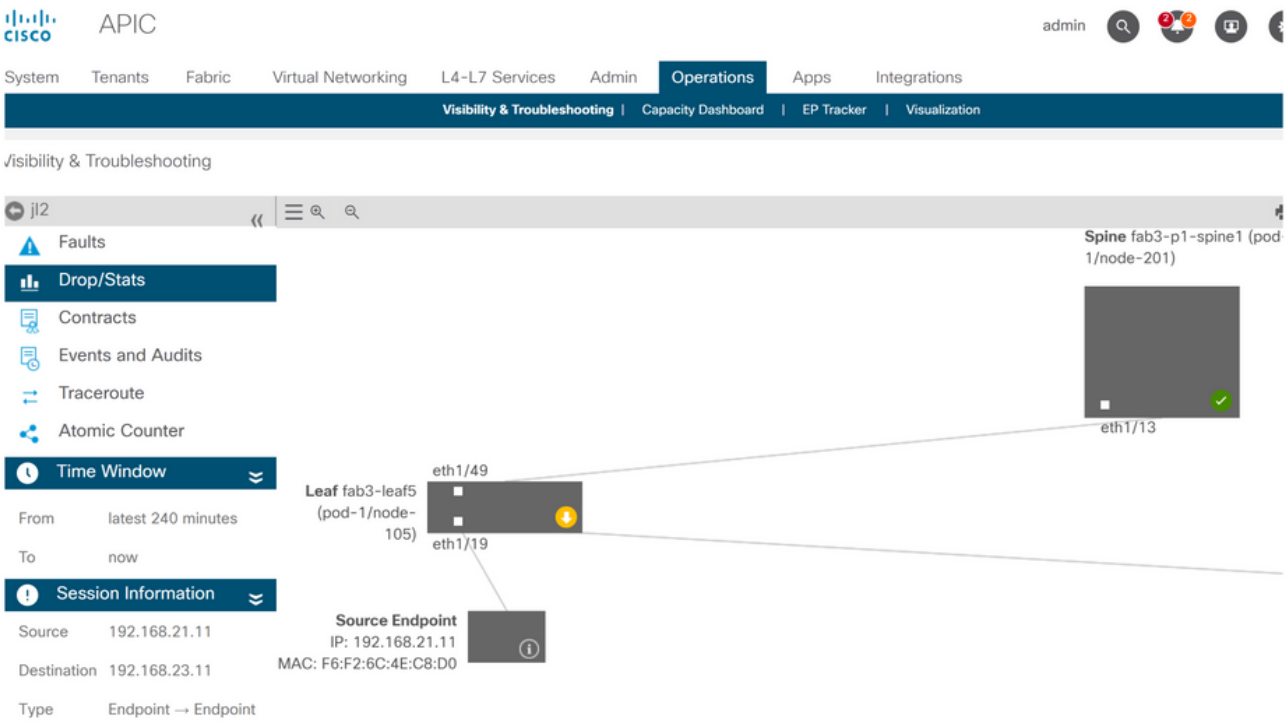


Configureer een sessienaam, bron en doeleindpunt. Klik vervolgens op 'Verzenden' of 'Rapport genereren'.

De tool zal automatisch de eindpunten in de stof vinden en informatie verstrekken over de huurder, het toepassingsprofiel en EPG die EP behoren tot.

In dit geval zal zij ontdekken dat de EP's behoren tot de huurder Prod1, zij behoren tot hetzelfde toepassingsprofiel 'AppProf' en worden toegewezen aan verschillende EPG's: 'Web' en 'DB'.

Identificatie van druppels

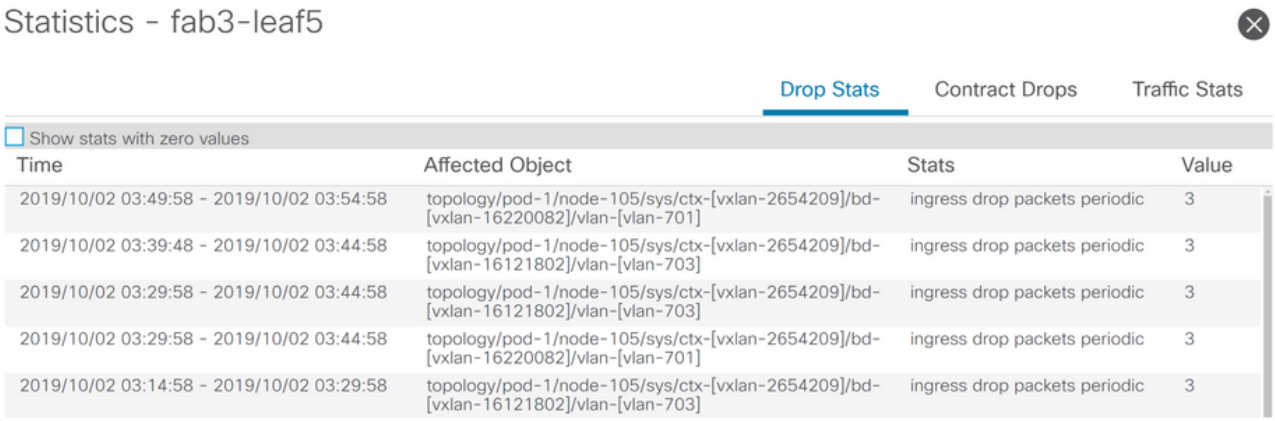


Het hulpmiddel zal automatisch de topologie van het het oplossen van probleemscenario visualiseren. In dit geval zijn de twee eindpunten toevallig verbonden met dezelfde switch.

Door naar het submenu Drop/Stats te navigeren, kan de gebruiker algemene druppels op het blad of de ruggengraat in kwestie bekijken. Raadpleeg de sectie "Interface Drops" in het hoofdstuk "Intra-Fabric Forwarding" van dit boek voor meer informatie over het begrijpen van welke druppels relevant zijn.

Veel van deze druppels zijn verwacht gedrag en kunnen worden genegeerd.

Drop details


Statistics - fab3-leaf5

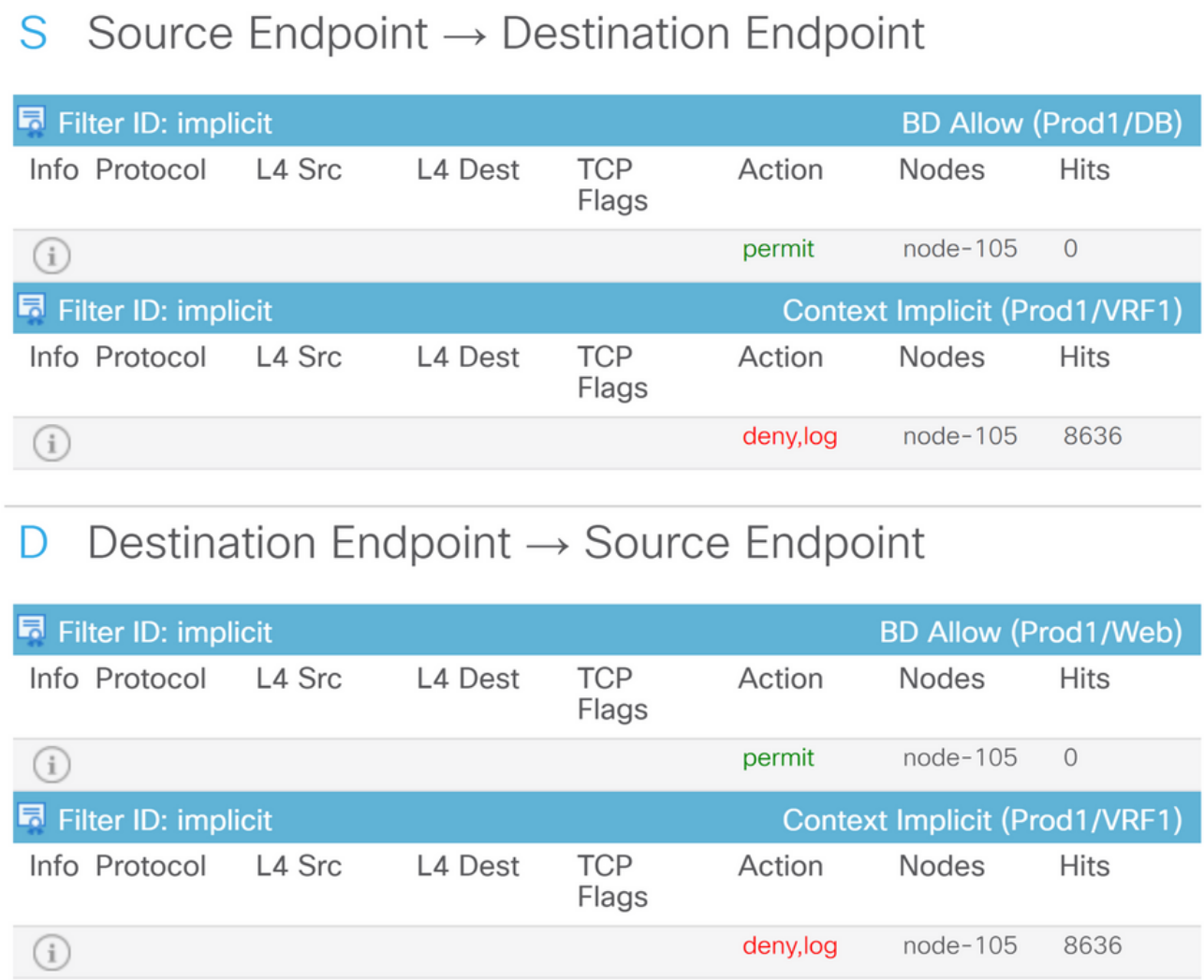
Drop Stats | Contract Drops | Traffic Stats

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

Door neer te boren om detail te laten vallen met behulp van de gele "Geknepen gevallen" knop in het switch diagram, kan de gebruiker details over de verloren stroom bekijken.

Contractgegevens


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

Door aan submenu Contracten te navigeren, kan de gebruiker identificeren welk contract beleidsvertraging tussen EPGs veroorzaakt. In het voorbeeld, is het impliciet om Prod1/VRF1 te ontkennen die sommige hits toont. Dit betekent niet noodzakelijkerwijs dat de gespecificeerde

stroom (192.168.21.11 en 192.168.23.11) deze impliciete ontkenning raakt. Als de Hits van Context Implicit ontkennen regel toeneemt, impliceert het dat er verkeer is tussen Prod1/DB en Prod1/Web die geen van de contracten raken, vandaar door Implicit ontkennen worden gelaten.

In de weergave van de topologie van het toepassingsprofiel bij huurder > selecteer de naam van het toepassingsprofiel links > Topologie, is het mogelijk om te verifiëren welke contracten worden toegepast op de DB EPG. In dat geval wordt aan de EPG geen contract toegewezen:

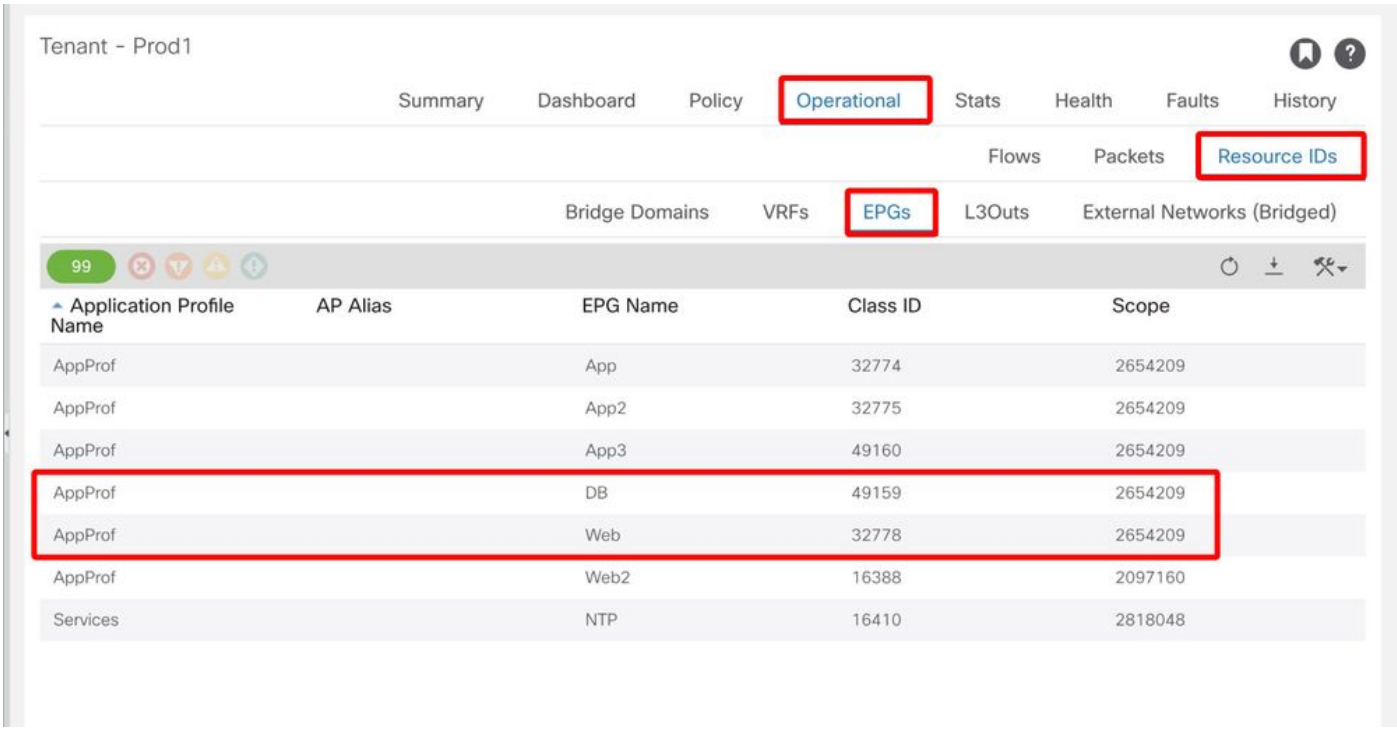
Contractvisualisatie

Nu de bron- en bestemming-EPG's bekend zijn, is het ook mogelijk andere relevante informatie te identificeren, zoals:

- De src/dst **EPG pcTag** van de betreffende endpoints. De pcTag is de klasse-ID die wordt gebruikt om een EPG te identificeren met een zoneringsregel.
- De src/dst **VRFNID,** ook wel **bereik** genoemd, van de betrokken eindpunten.

Klasse-ID en bereik kunnen gemakkelijk worden opgehaald uit de APIC GUI door de huurder te openen > selecteer de naam van de huurder links > Operationeel > Resource ID's > EPG's

Identificatie van de huurder om EPG pcTag en scope te vinden



In dit geval zijn de Klasse ID en Scopes:

- Web EPG pcTag 32778
- Web EPG-2654209
- DB EPG pcTag 49159
- DB EPG-2654209

Controleer of het beleid dat op de verkeersstroom is toegepast, problemen veroorzaakt

Bash

Een interessant hulpmiddel om het pakket te verifiëren dat op een ACI-blad wordt gelaten, is de iBash-opdrachtregel: 'toon het registreren ip toegang-lijst intern pakketlogboek ontkennen':

```
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
```

Op de switch van het blad zijn, net als bij de vorige uitgave, talrijke ICMP-pakjes uit EP 192.168.23.11 naar 192.168.21.11 weggelaten.

Het contract_parser hulpmiddel zal helpen om het daadwerkelijke beleid te verifiëren dat op VRF wordt toegepast waar de Endpoints met worden geassocieerd:

```
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]
```

Dit kan ook worden geverifieerd aan de hand van de zoneringsregel die in het blad is geprogrammeerd en het beleid dat door de switch wordt gehandhaafd.

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

Zoals reeds gezien door het hulpmiddel van het Zichtbaarheid & van het Problemen oplossen, het contract_parser hulpmiddel, en de zoneringsregels, bevestigt de output dat er geen contract tussen de bron en bestemming EPGs in het oplossen van problemen is. Het is gemakkelijk om te veronderstellen dat de gelaten vallen pakketten impliciet ontkennen regel 5155 aanpassen.

ELAM-opname

ELAM Capture levert een ASIC-rapport dat wordt gebruikt om te controleren of er gegevens worden doorgestuurd, wat in het geval van een gedropt pakket de reden voor het uitzetten aangeeft. Wanneer de reden van een daling een beleidsdaling is, zoals in dit scenario, zal de output van ELAM vangen als het volgende kijken.

Houd er rekening mee dat de details van het opzetten van een ELAM-opname niet in dit hoofdstuk worden besproken. Raadpleeg het hoofdstuk "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
```

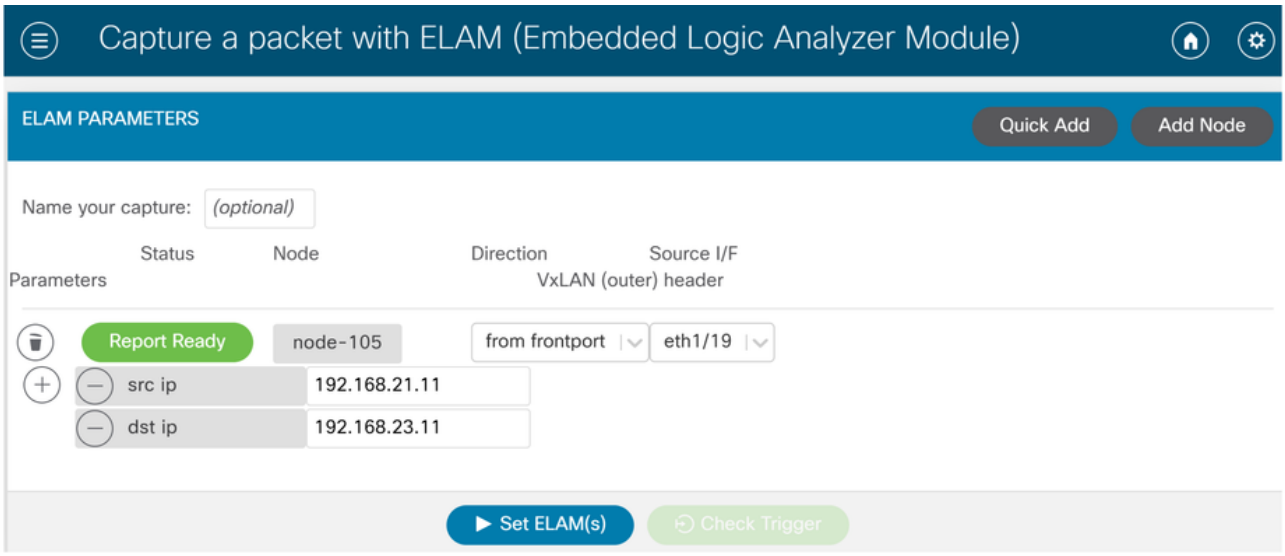
```
LU drop reason                          : SECURITY_GROUP_DENY
   pkt.lu_drop_reason: 0x2D
```

Uit het ELAM-rapport hierboven blijkt duidelijk dat het pakket is gevallen als gevolg van een beleidsdaling: 'SECURITY_GROUP_DENY'

ELAM Assistant:

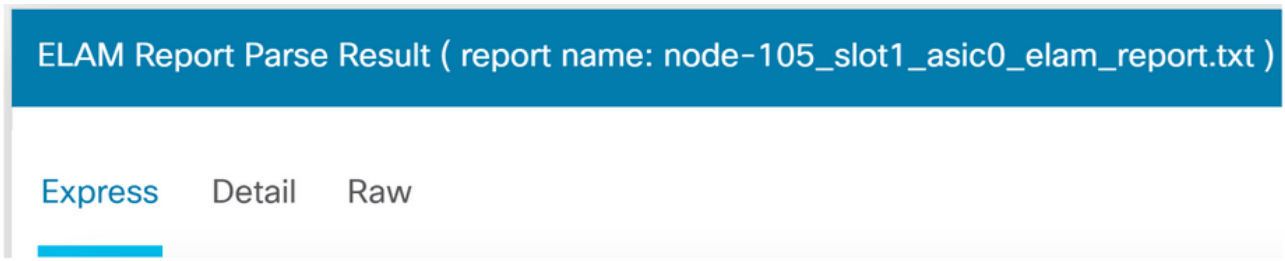
Hetzelfde resultaat van de ELAM-opname kan via de ELAM Assistant-app op de APIC GUI worden getoond.

Configuratie



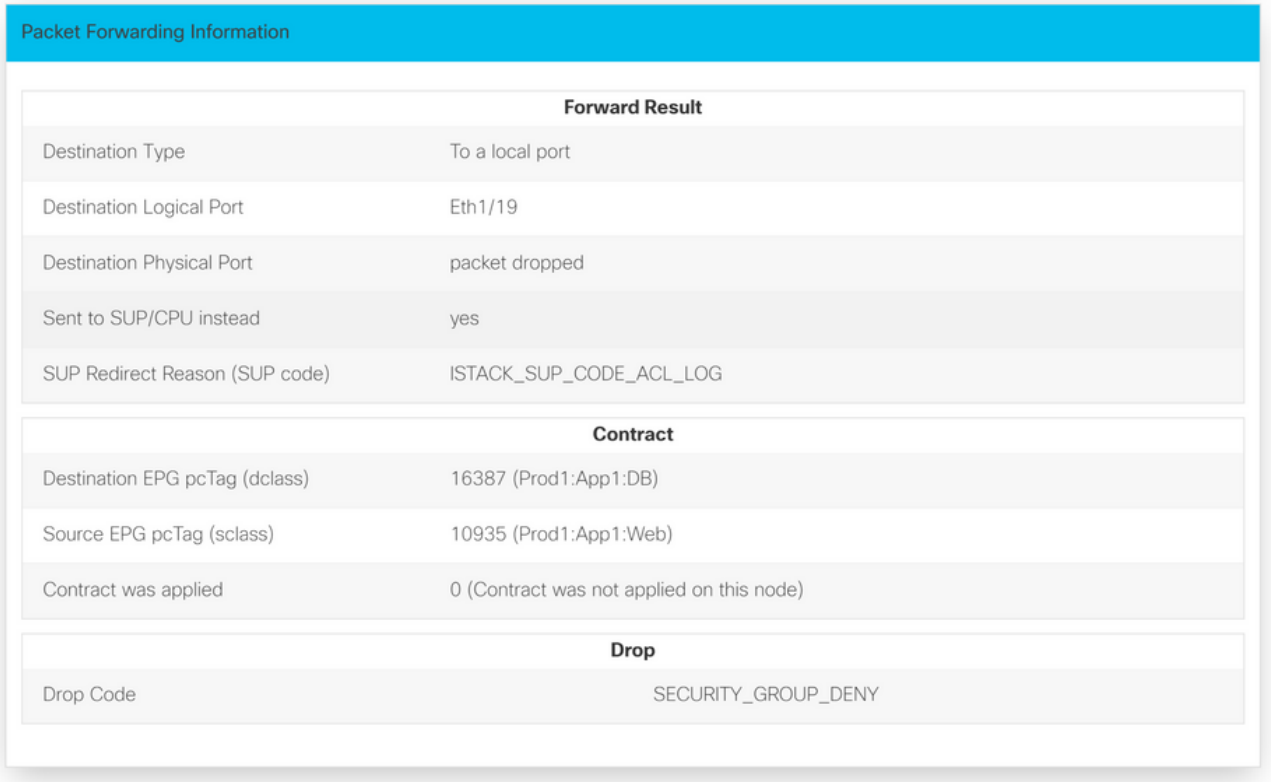
Typisch, zal de gebruiker zowel bron als bestemmingsdetails voor de stroom van belang vormen. In dit voorbeeld, wordt src IP gebruikt om verkeer naar eindpunt in bestemming EPG te vangen dat geen contractverhouding aan de bron EPG heeft.

Elam Assistant Express-rapport



Er zijn drie uitvoerniveaus die kunnen worden bekeken met ELAM Assistant. Dit zijn Express, Detail en Raw.

Elam Assistant Express rapport (vervolg)



Onder het Express Resultaat geeft de Drop Code reden SECURITY_GROUP_DENY aan dat de daling het gevolg was van een contracthit.

Voorkeursgroep

Over voorkeursgroepen van contracten

Er zijn twee soorten beleidshandhaving beschikbaar voor EPG's in een VRF met een voorkeursgroep voor een contract:

- Inbegrepen EPG's: EPG's kunnen vrij met elkaar communiceren zonder contracten, als ze lid zijn van een contractgeprefereerde groep. Dit is gebaseerd op de standaardregel source-any-bestemmings-any-license.
- Uitgesloten EPG's: EPG's die geen lid zijn van voorkeursgroepen, vereisen dat contracten met elkaar communiceren. Anders zijn de regels tussen de uitgesloten EPG en een EPG van toepassing.

De voorkeursgroepfunctie van het contract maakt een betere controle van de communicatie tussen EPG's in een VRF mogelijk. Als de meeste EPG's in de VRF open communicatie zouden moeten hebben, maar een paar slechts beperkte communicatie met de andere EPG's zouden moeten hebben, stel een combinatie van een contract voorkeursgroep en contracten met filters in om de communicatie tussen EPG's nauwkeuriger te controleren.

EPG's die van de voorkeursgroep zijn uitgesloten, kunnen alleen met andere EPG's communiceren als er een contract is om de standaardregel voor bron-willekeurige-bestemming-ontkennen te negeren.

Programmering met voorkeursgroep voor contracten

In wezen zijn voorkeursgroepen contracten een omgekeerde groep van reguliere contracten. Voor

reguliere contracten zijn expliciete regels voor de zonering van vergunningen geprogrammeerd met een impliciete ontkennen-regel met de VRF-scope. Voor voorkeursgroepen is een impliciete "PERMIT"-zoning-regel geprogrammeerd met de hoogste numerieke prioriteitswaarde en zijn specifieke "DENY" zoning-regels geprogrammeerd om verkeer van EPG's die geen voorkeursgroepleden zijn, te verbieden. Dientengevolge, ontkennen de regels eerst worden geëvalueerd en als de stroom niet door deze regels wordt aangepast, dan wordt de stroom impliciet toegestaan.

Er is altijd een paar expliciete ontkennen zoning-regels voor elke EPG buiten de voorkeursgroep:

- Een van de niet-geprefereerde leden van de groep naar een pcTag (waarde 0).
- Een andere van een pcTag (waarde 0) naar het niet-geprefereerde groepslid.

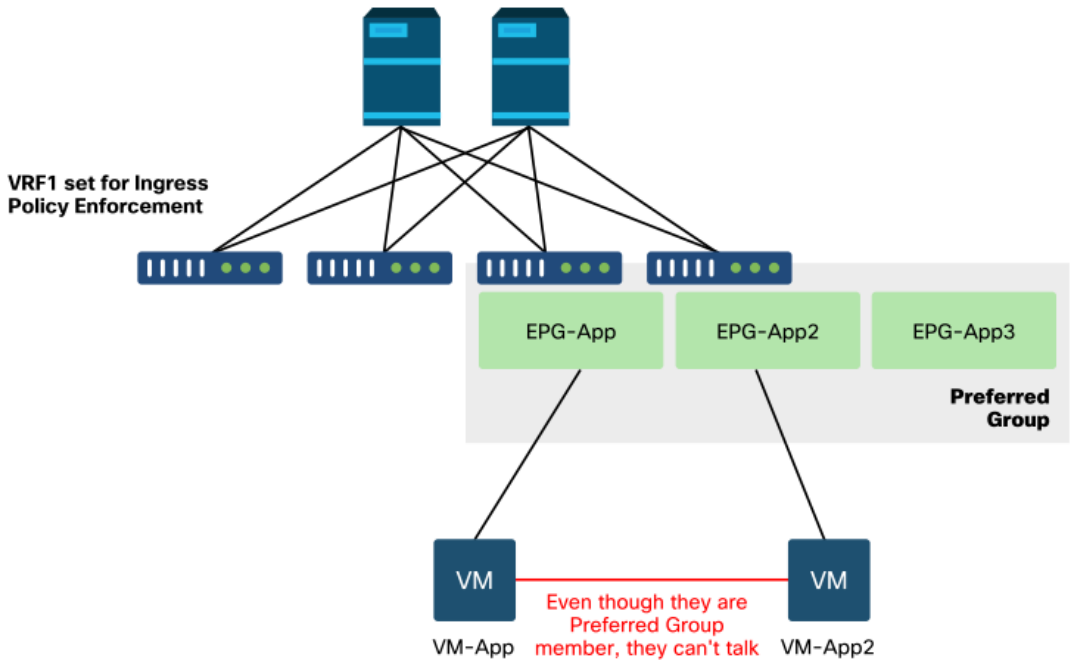
Scenario voor probleemoplossing bij voorkeursgroep

De onderstaande afbeelding toont een logische topologie waarin EPGs App, App2 en App3 allemaal zijn geconfigureerd als voorkeursgroep leden.

VM-App maakt deel uit van EPG-App en VM-App2 maakt deel uit van EPG-App2. Zowel App als App2 EPG moeten deel uitmaken van de voorkeursgroep en dus vrij communiceren.

VM-App initieert een verkeersstroom op TCP-poort 6000 naar VM-App2. Zowel EPG-App als EPG-App2 zijn voorkeursleden van de groep als onderdeel van VRF1. VM-App2 ontvangt nooit pakketten op TCP-poort 6000.

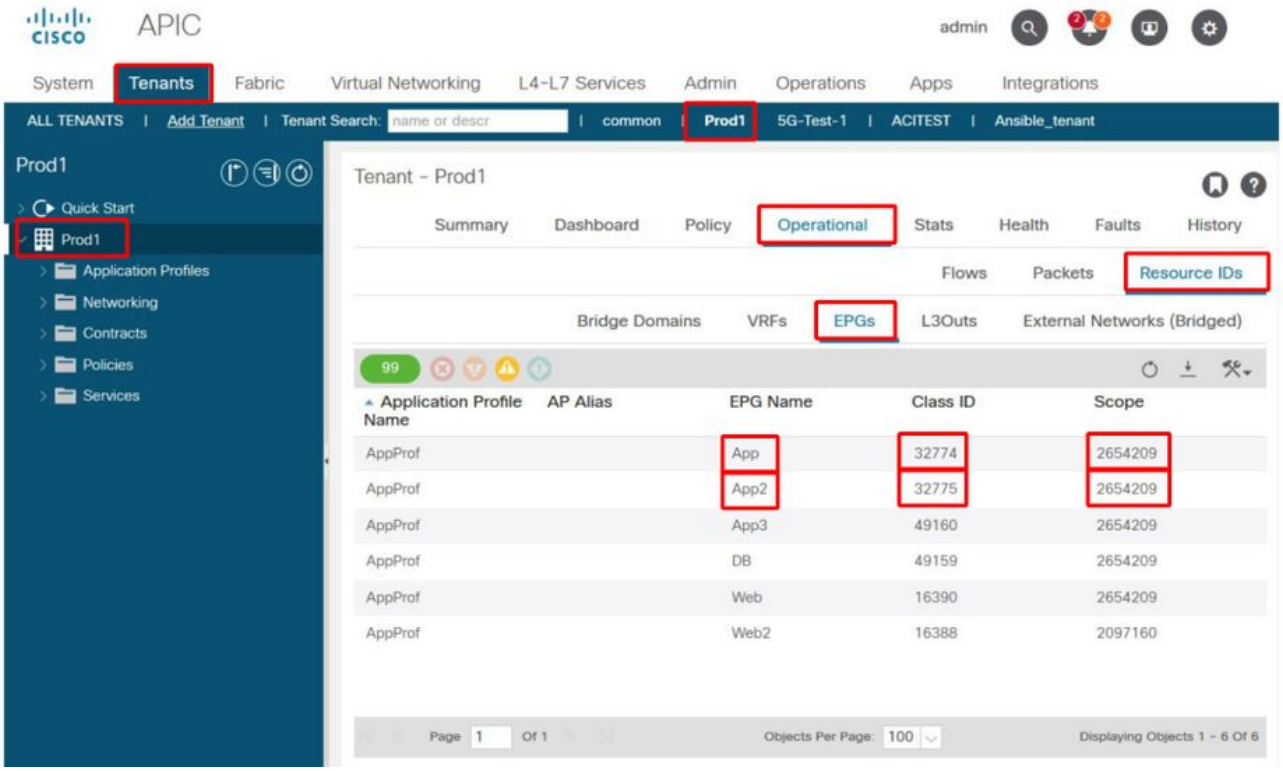
Topologie



werkstroom

1. Zoek de pcTag van EPG APP en zijn VRF VNID/Scope

EPG- en VRF-pc-tags



2. Controleer contractprogrammering met contract_parser.py op het toegangsblad

Gebruik contract_parser.py en/of de opdracht 'show zoning-rule' en specificeer de VRF

```
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]
```

Na onderzoek van de bovenstaande output wordt de impliciete vermelding van de vergunning — regelID 4165 — met de hoogste prioriteit van 20, in acht genomen. Deze impliciete vergunningsregel zal veroorzaken dat alle verkeersstromen worden toegestaan tenzij er een expliciete ontkennen regel met een lagere prioriteit is die de verkeersstroom verbiedt.

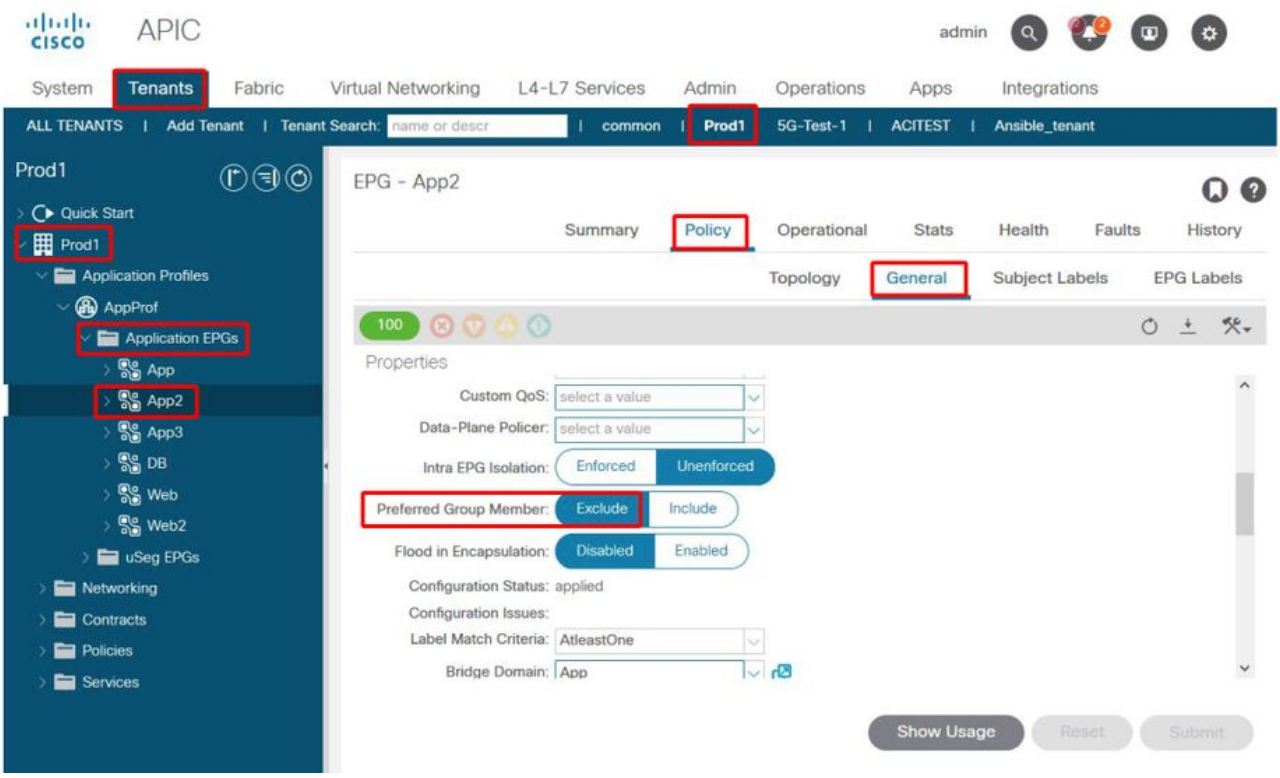
Daarnaast zijn er twee expliciete ontkenningsregels voor pcTag 32775, de pcTag van EPG App2. Deze twee expliciete ontkennen zoning-regels verkeer van elke EPG naar EPG App2, en vice versa. Deze regels hebben prioriteit 18 en 19, dus ze zullen voorrang hebben op de standaard-vergunningsregel.

De conclusie is dat EPG App2 geen voorkeurlid van de Groep is aangezien de expliciete ontkenningsregels worden nageleefd.

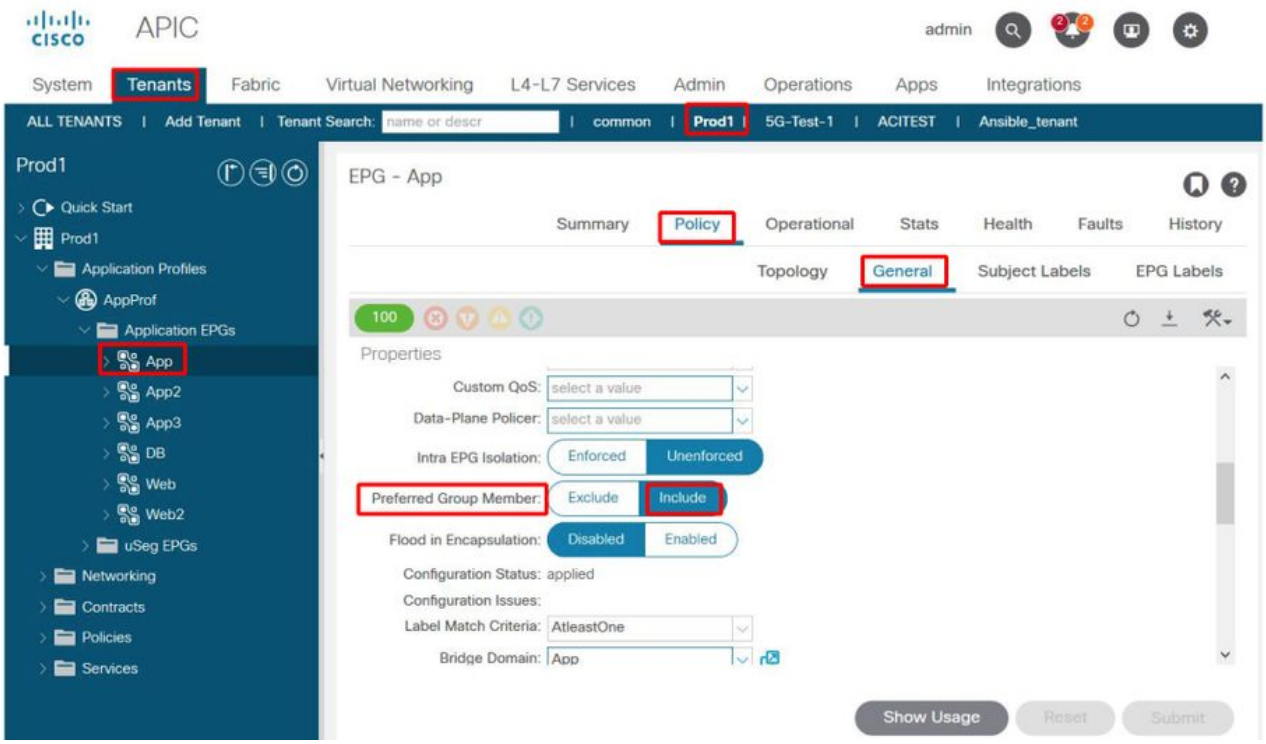
3. Controleer de configuratie van de voorkeursgroep van EPG-leden

Navigeer de APIC GUI en controleer de configuratie van de EPG App2 en de voorkeursgroep van de EPG App, In het volgende cijfer, zie EPG App2 niet als Voorkeursgroep Lid wordt gevormd.

EPG App2 — Uitgesloten instellingen voorkeursleden



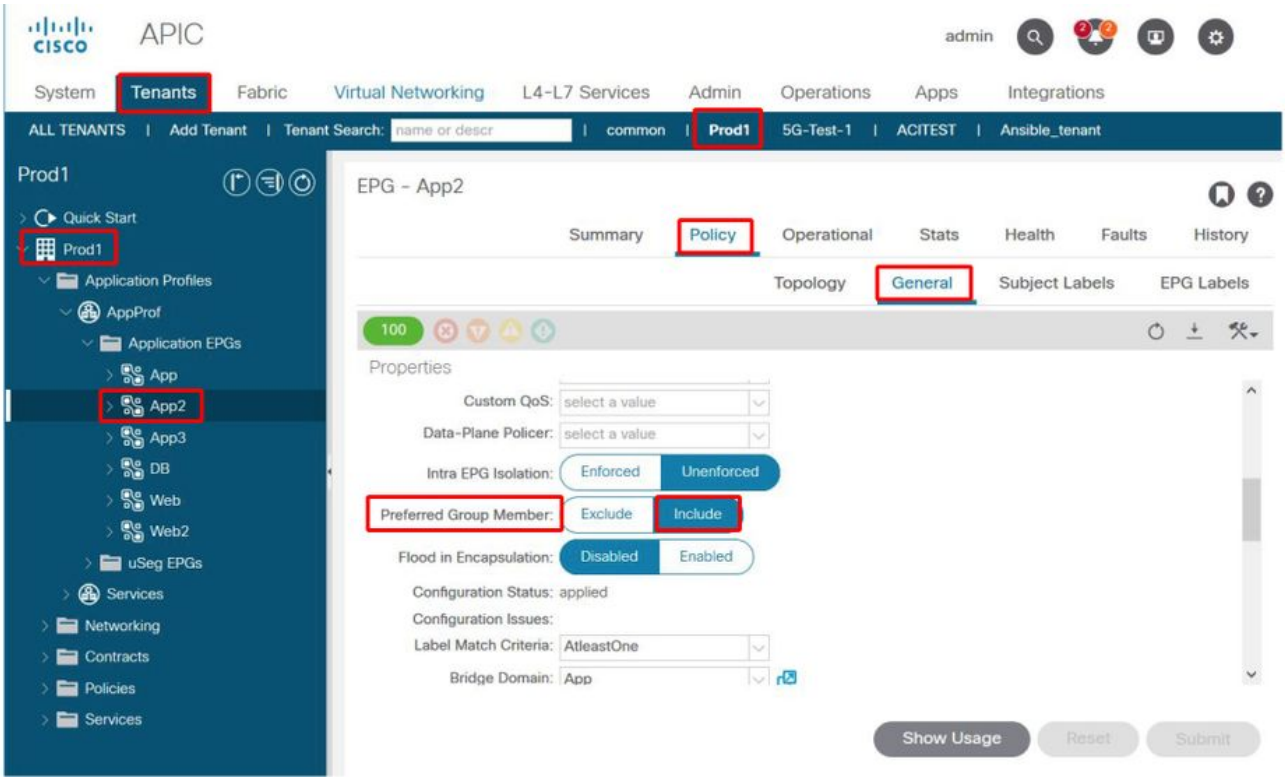
EPG App — voorkeursgroep Ledeninstelling inbegrepen



4. Stel EPG App2 in als voorkeurslid van de groep

Door de configuratie van App2 EPG te wijzigen kan de voorkeursgroep vrij communiceren als deel van de voorkeursgroep.

EPG App2 — Preferred Group Member setting inbegrepen



5. Controleer contractprogrammering opnieuw met behulp van contract_parser.py op het blad waar de src-EP zich bevindt

Gebruik contract_parser.py opnieuw en specificeer de VRF naam om te verifiëren of de expliciete ontkennen regels voor EPG App2 nu zijn verdwenen.

```
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]
```

De expliciete ontkenningsregels voor EPG App2 en zijn pcTag 32775 worden niet langer in de bovenstaande output waargenomen. Dit betekent dat het verkeer tussen EP's in EPG App en EPG App2 nu gelijk zal zijn aan de impliciete vergunningsregel — regelId 4165 — met de hoogste prioriteit van 20.

vzAny naar EPG

Over vzAny

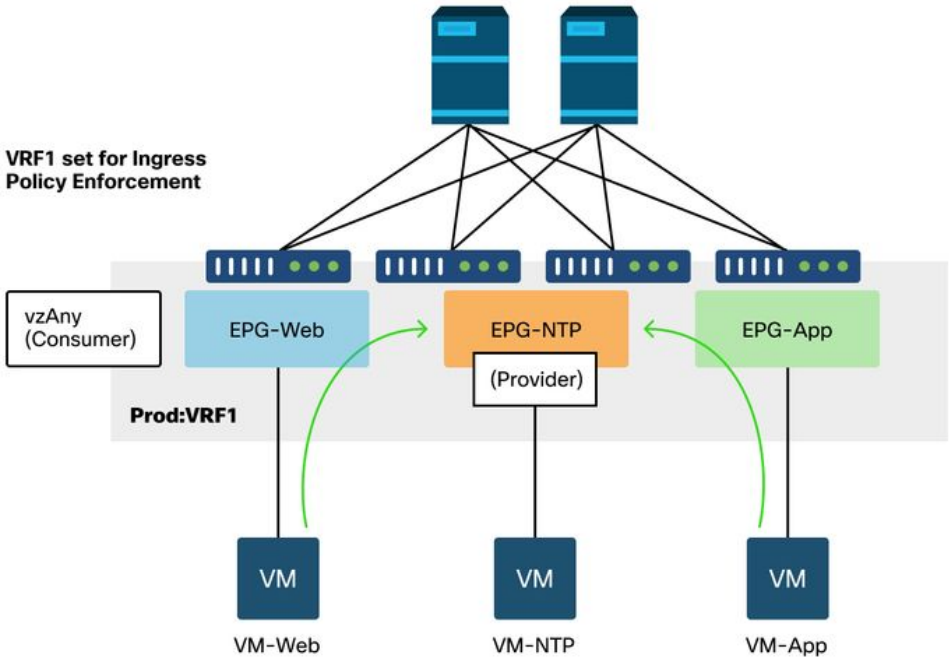
Bij het configureren van contracten tussen een of meerdere EPG’s kunnen contracten worden

geconfigureerd als een verbruikte of geleverde relatie. Wanneer het aantal EPG's groeit, kan dat ook de hoeveelheid contractuele relaties tussen hen. In sommige veel voorkomende gevallen moeten alle EPG's verkeersstromen uitwisselen met een andere specifieke EPG. Een dergelijk geval zou een EPG kunnen zijn met EP's die diensten verlenen die door alle andere EPG's binnen dezelfde VRF moeten worden verbruikt (bijvoorbeeld NTP of DNS). vzAny zorgt voor lagere operationele overheadkosten bij het configureren van contractrelaties tussen alle EPG's en specifieke EPG's die diensten leveren die door alle andere EPG's moeten worden verbruikt. Bovendien staat vzAny een veel efficiënter gebruik van de CAM van het Veiligheidsbeleid op bladregels toe aangezien slechts 2 zoning-switches voor elke vzAny contractverhouding worden toegevoegd.

Voorbeeld gebruikscase

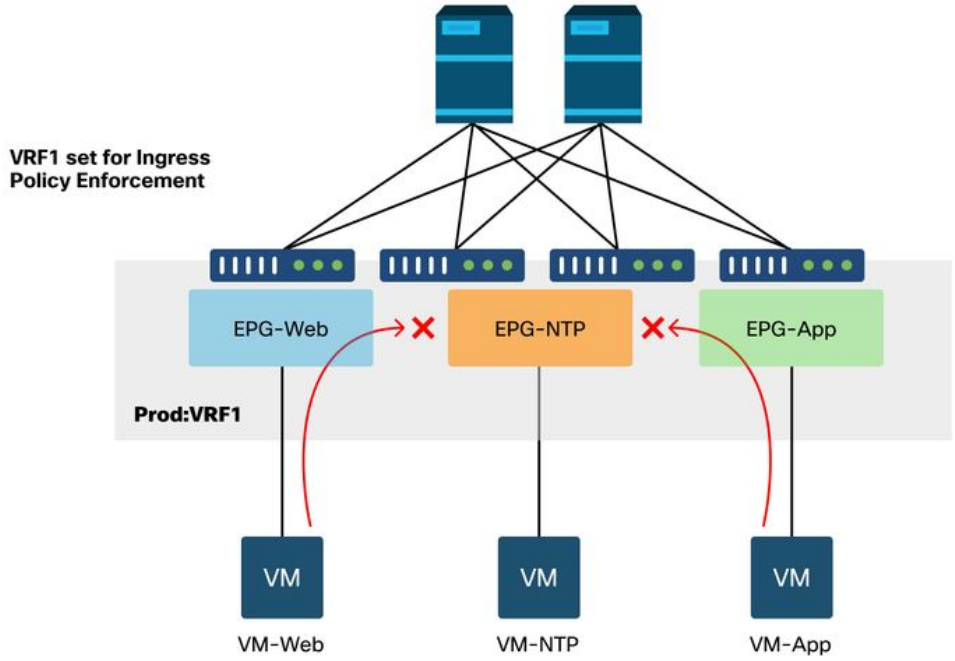
De onderstaande afbeelding beschrijft een dergelijke gebruikscase waarbij VM-Web en VM-App in EPGs Web en App respectievelijk NTP-services van VM-NTP in EPG-NTP moeten gebruiken. In plaats van het configureren van een geleverd contract op EPG NTP, en vervolgens het hebben van hetzelfde contract als een verbruikt contract op EPGs Web en App, staat vzAny elke EPG in VRF Prod toe:VRF1 om NTP-services te verbruiken van EPG NTP.

vzAny — Any EPG met VRF-proxy:VRF1 kan NTP-services van EPG NTP gebruiken



Overweeg een scenario waarin druppels worden waargenomen tussen EPG's die de NTP-diensten gebruiken wanneer er geen contract tussen hen is.

Scenario voor probleemoplossing - verkeer daalt als er geen contract is

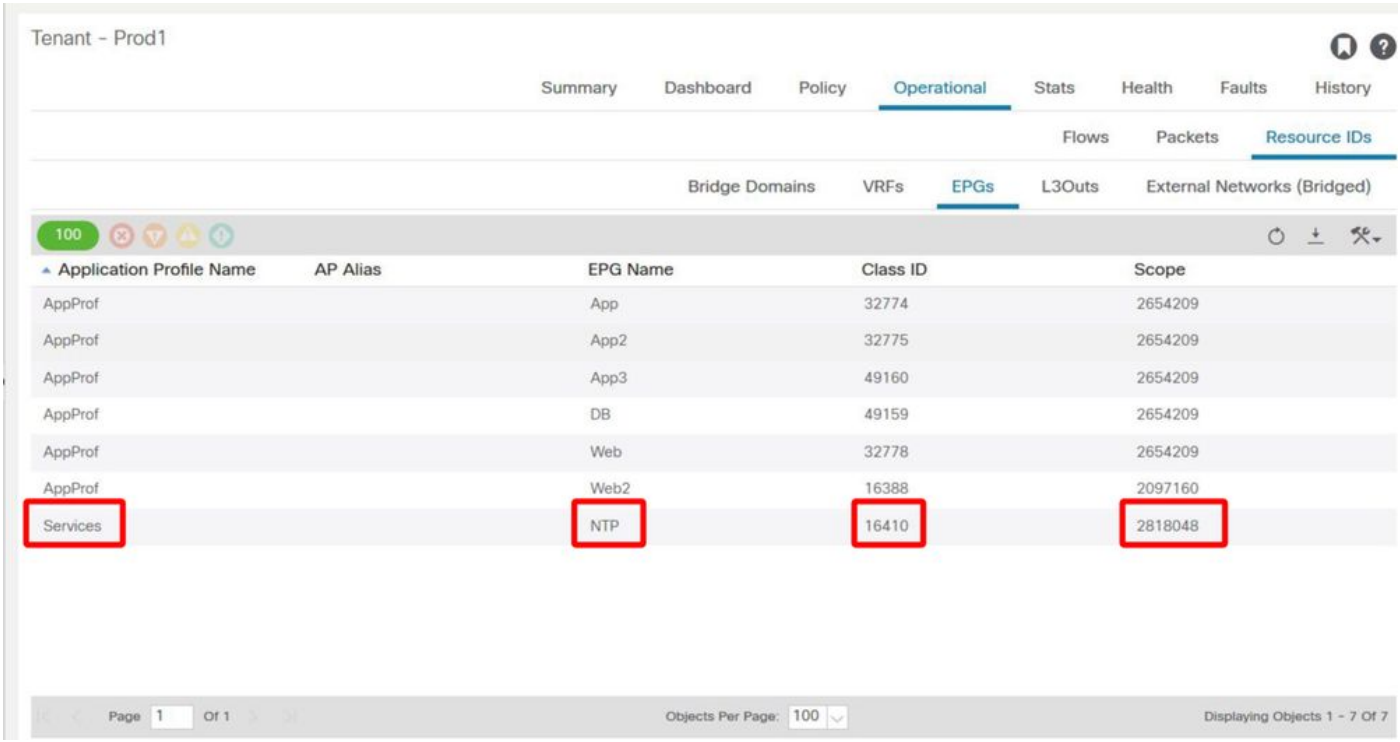


werkstroom

1. Zoek de pcTag van EPG NTP en zijn VRF VNID/Scope op

'huurder > Operationeel > Resource ID's > EPG's' maakt het mogelijk pcTag en scope te vinden

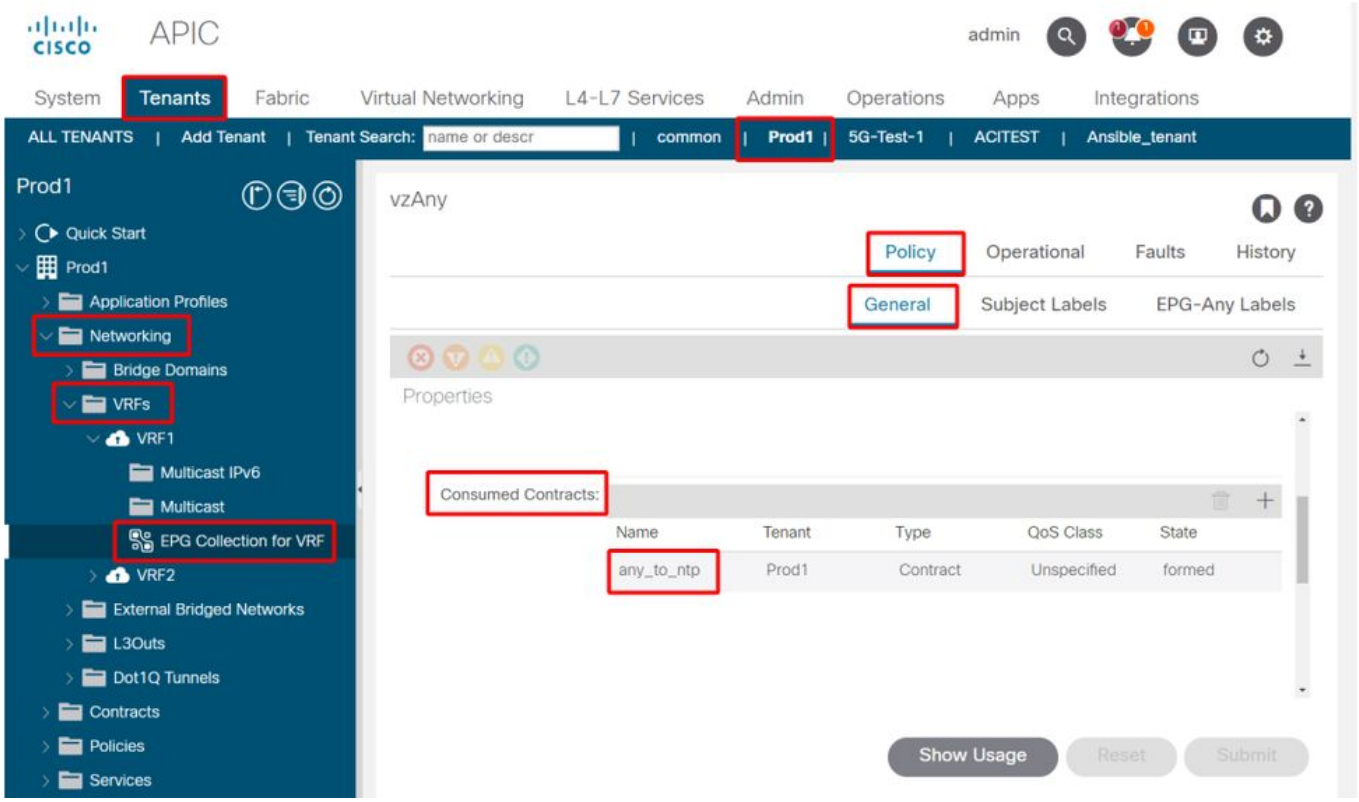
EPG NTP pcTag en de VRF-video/bereik ervan



2. Controleer of een contract is geconfigureerd als een vzAny verbruikt contract als onderdeel van de VRF

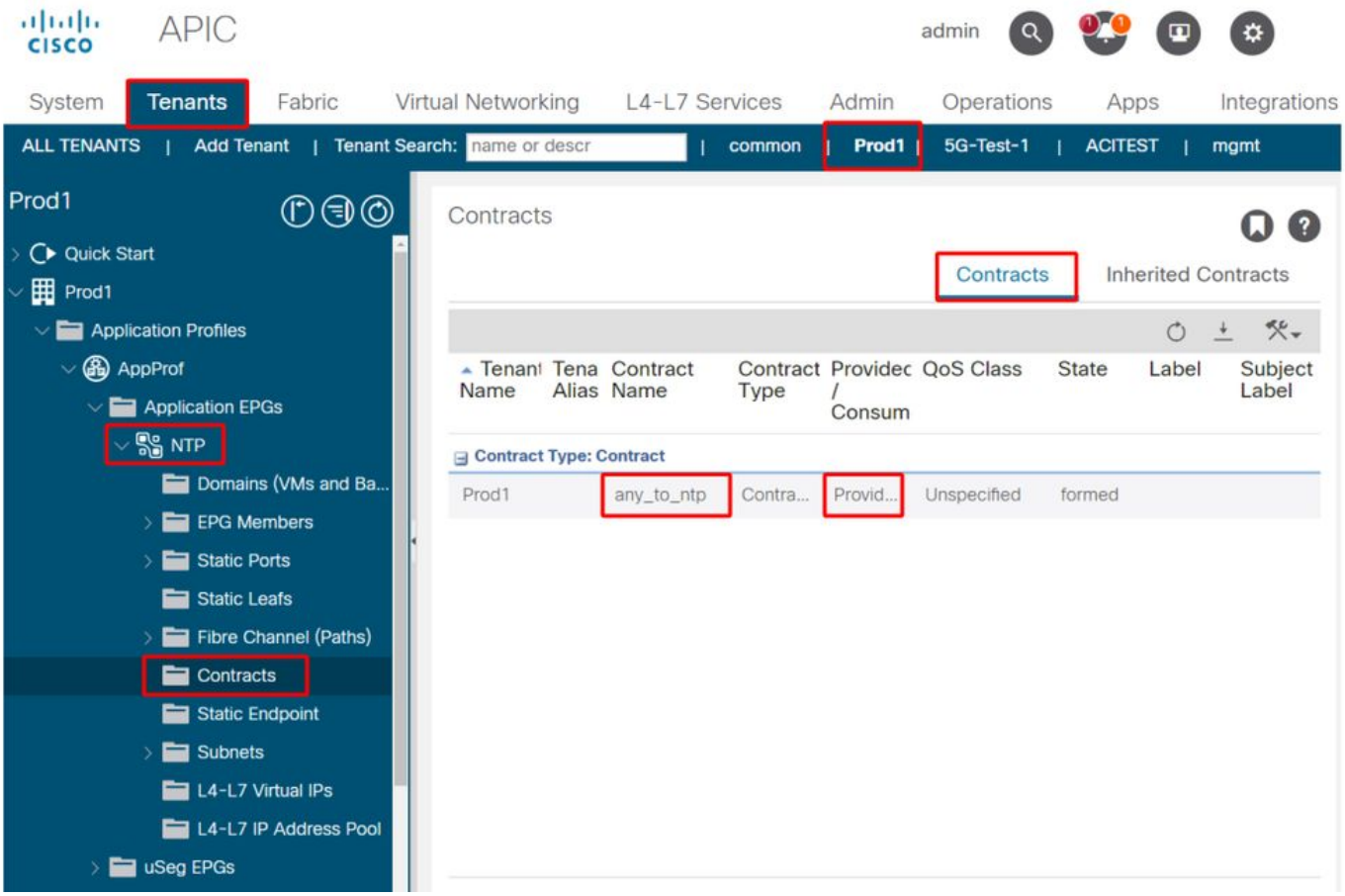
Navigeer naar de VRF en controleer of er een verbruikt contract is geconfigureerd als vzAny onder de 'EPG Collection for VRF'.

Contract geconfigureerd als een verbruikt vzAny contract op de VRF



3. Controleer of hetzelfde contract wordt toegepast als een geleverd contract op EPG NTP

Om een contractrelatie vast te stellen, moet hetzelfde contract worden toegepast als een verstrekt contract op EPG NTP dat NTP-diensten verleent aan de andere EPG's in zijn VRF.



4. Zones-regel verificatie op indringingsblad met contract_parser.py of 'toon zoning-regel'

Het toegangsblad moet 2 zoningregels hebben om bidirectionele verkeersstromen mogelijk te maken (als het contractonderwerp is ingesteld om beide richtingen toe te staan) tussen elke EPG en EPG NTP. 'Elke EPG' wordt aangeduid als pcTag 0 in zoning-rule programmeren.

Het gebruik van contract_parser.py of de 'show zoning-rule' commando's op het toegangsblad terwijl het specificeren van de VRF maakt het mogelijk om te verzekeren dat de zoning-regel geprogrammeerd is.

Zones-regels die verkeer naar/van EPG NTP van andere EPG's in de aanwezige VRF toestaan

Gebruik contract_parser.py en 'toon zoning-rule' om de aanwezigheid van de vzAny gebaseerde zoning-regels te controleren.

Hier zijn twee soorten regels duidelijk:

1. Regel 4156 en regel 4168 die Any naar NTP en vice versa toestaan. De prioriteiten 13 en 14 zijn: Zones-regel die verkeer toestaat stromen van elke EPG (pcTag 0) naar EPG NTP (pcTag 49161).Zones-regel die verkeer toestaat stromen van EPG NTP (pcTag 46161) naar een andere EPG (pcTag 0).
2. Regel 4165, wat de enige is om te ontkennen regel (standaard) met prioriteit 21.

Gezien het feit dat de laagste prioriteit voorrang heeft, zullen alle EPG's van de VRF toegang hebben tot 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)  |
+---------+--------+--------+----------+---------+---------+---------+------------+----------+--
--------------------+
```

Gedeeld L3Out naar EPG

Over gedeelde L3Out

Shared Layer 3 Out is een configuratie die het mogelijk maakt om een L3Out in één VRF te hebben die bepaalde diensten (externe toegang) biedt en één of meer andere VRF's verbruiken dit L3Out. Meer details over gedeelde L3Out kunnen worden gevonden in het hoofdstuk "Externe routing".

Bij het doen van gedeelde L3Out wordt aanbevolen om de aanbieder van het contract te hebben die de gedeelde L3Out en de EPG die de consument van het contract zijn. Dit scenario wordt in deze paragraaf toegelicht.

Het is niet aan te raden om het tegenovergestelde te doen, namelijk L3Out die een dienst van een EPG gebruikt. De reden hiervoor heeft te maken met schaalbaarheid, aangezien voor gedeelde diensten de zoneringsregels alleen op VRF voor consumenten worden geïnstalleerd. De beginselen van consumptie en aanbod geven aan waar verkeersstromen worden geïnitieerd. Bij de handhaving van het standaardtoegangsbeleid betekent dit dat de handhaving van het beleid zal worden toegepast aan de kant van de consument en meer specifiek op het indringblad (niet-grensblad). Voor het indringenblad om beleid af te dwingen vereist het de pcTag van de bestemming. In dit scenario is de bestemming de externe EPG pcTag. Het indringingsblad voert

dus de beleidshandhaving uit en stuurt de pakketten door naar het grensblad. Het grensblad ontvangt het pakket op zijn fabric link die een route lookup (LPM) uitvoert en het pakket doorstuurt naar de nabijheid voor de bestemming prefix.

Het grensblad voert echter GEEN beleidshandhaving uit bij het verzenden van verkeer naar de bestemming EP en doet dit ook niet op de terugstroom van verkeer naar de bron EP.

Als gevolg daarvan heeft alleen de Policy CAM van het indringende niet-BL-blad ingangen geïnstalleerd (in de VRF van de consument) en de Policy CAM van BL niet beïnvloed.

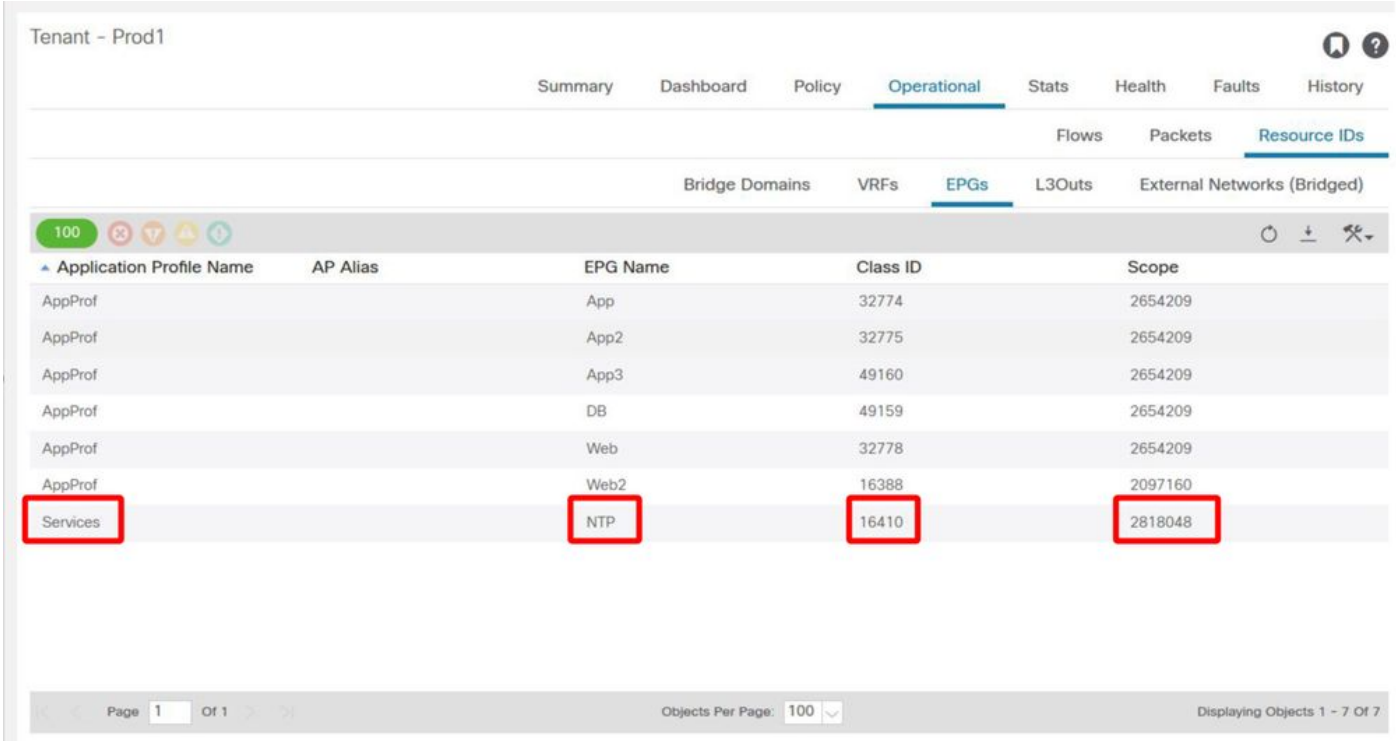
Gedeelde L3out probleemoplossing

werkstroom

1. Controleer EPG pcTag en VRF VNID/Scope voor de consument EPG

Met gedeelde L3Out, zijn de zoning-regels slechts geïnstalleerd in de consument VRF. De provider moet een wereldwijde pcTag (onder 16k) hebben waarmee deze pcTag kan worden gebruikt in alle VRF's voor consumenten. In ons scenario is de provider de externe EPG en heeft hij een wereldwijde pcTag. De consument EPG zal een lokale pcTag zoals gebruikelijk hebben.

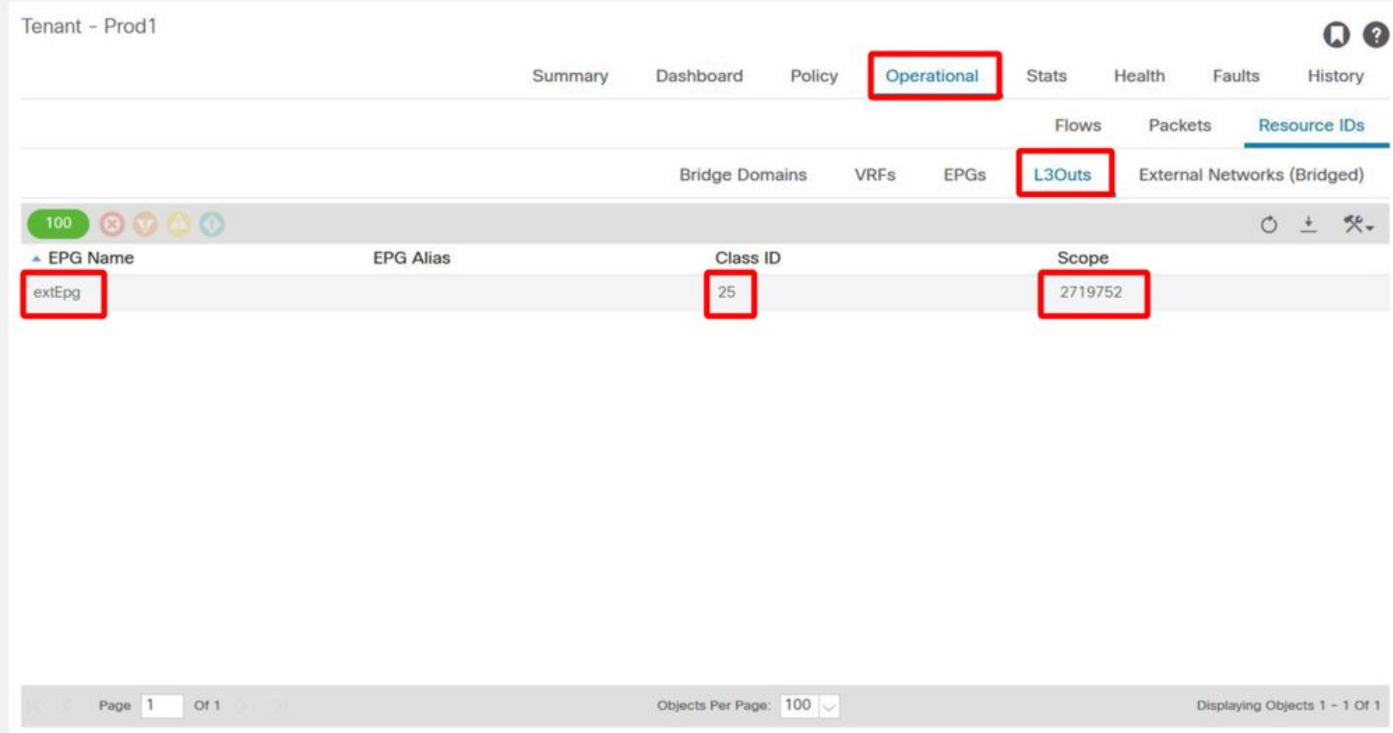
pcTag van de consument



2. Controleer pcTag en VRF VNID/Scope voor de provider L3Out EPG

Zoals opgemerkt in Stap 1, heeft de provider L3Out EPG een globale bereik pcTag als prefixes van L3Out die worden uitgelekt in de consument VRF. Als gevolg daarvan is de L3Out EPG pcTag vereist om niet te overlappen met pcTags in de VRF voor consumenten, en dus is het binnen het wereldwijde pcTag bereik.

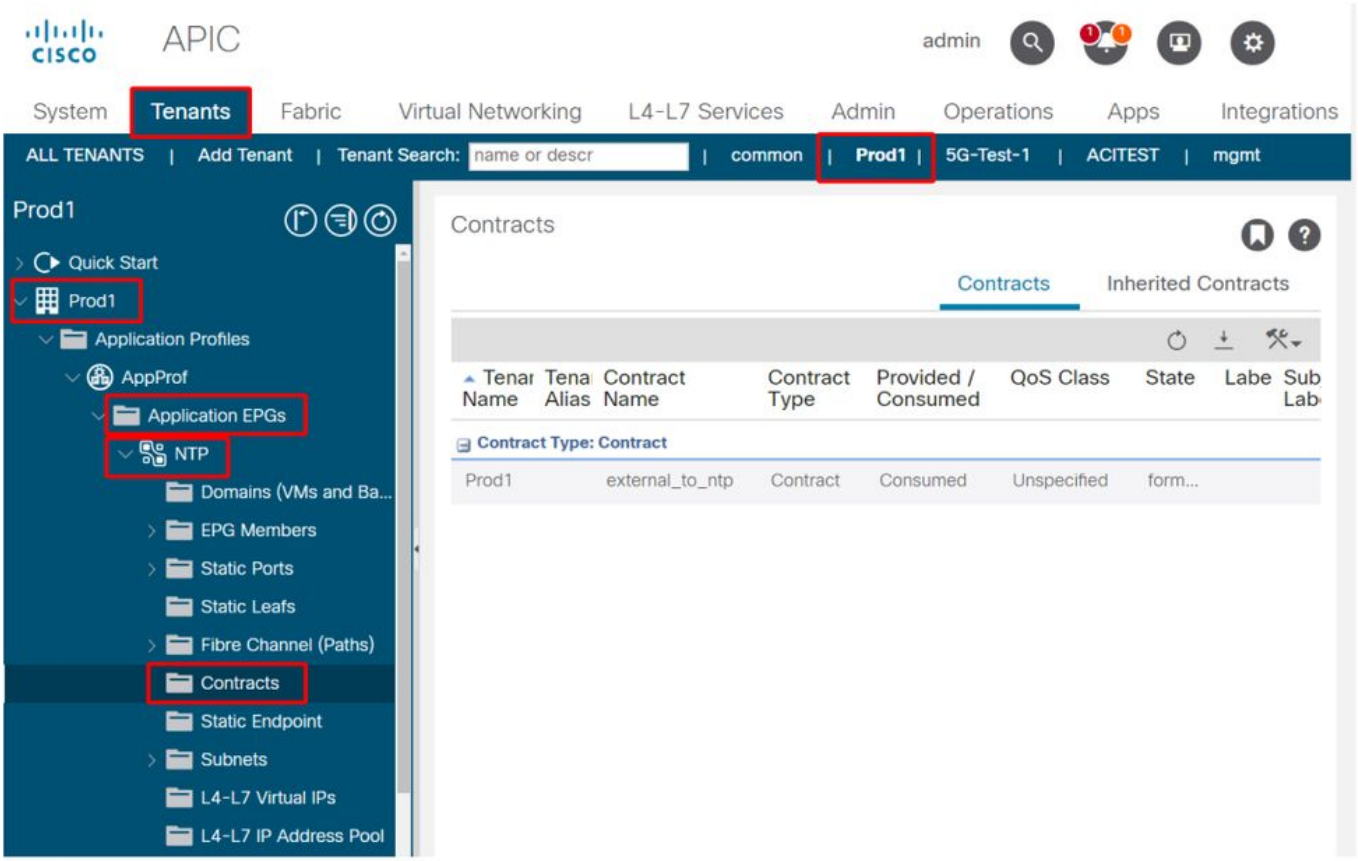
pcTag van externe EPG van de leverancier



3. Controleer of de EPG van de consument een geïmporteerd huurder-scoped contract of een wereldwijd contract heeft geconfigureerd

De consument EPG NTP met subnetverbinding gedefinieerd onder de EPG/BD verbruikt het 'huurder' of 'globaal' scoped contract

Door EPG verbruikte opdracht



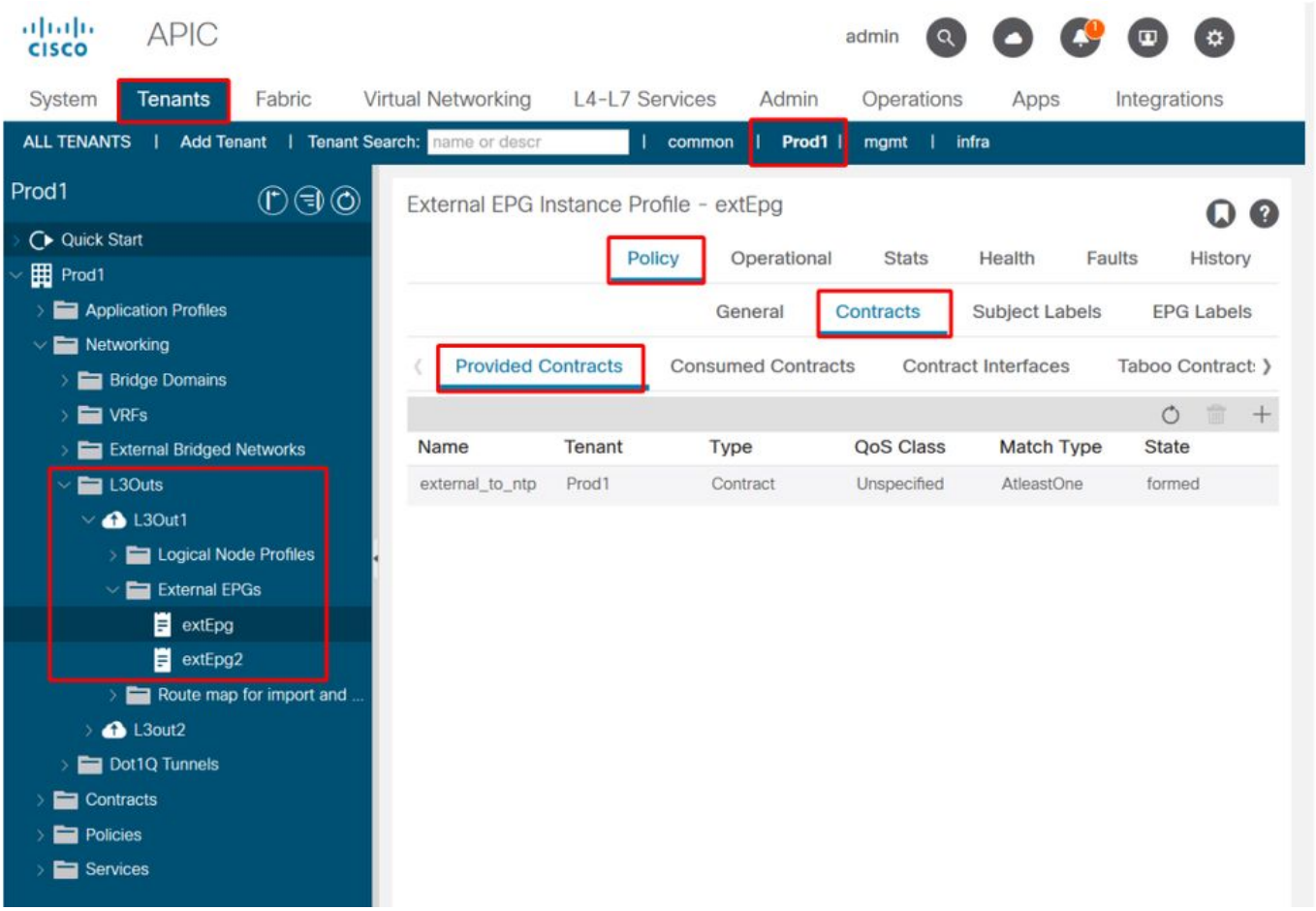
4. Controleer of de BD van de consument EPG een subnetverbinding heeft geconfigureerd met het bereik ingesteld op 'Gedeeld tussen VRF's'

Het subnet van de EPG wordt geconfigureerd onder het brugdomein, maar moet de 'gedeelde VRF'-vlag hebben (om routed leking toe te staan) en de 'geadverteerde extern' vlag (om te kunnen adverteren naar L3Out)

5. Controleer of de provider L3Out EPG een geïmporteerd huurder-scoped contract of een wereldwijd contract heeft geconfigureerd

De L3Out EPG moet een huurder-scoped contract of een globaal contract als een beschikbaar contract hebben.

Contract op provider L3Out



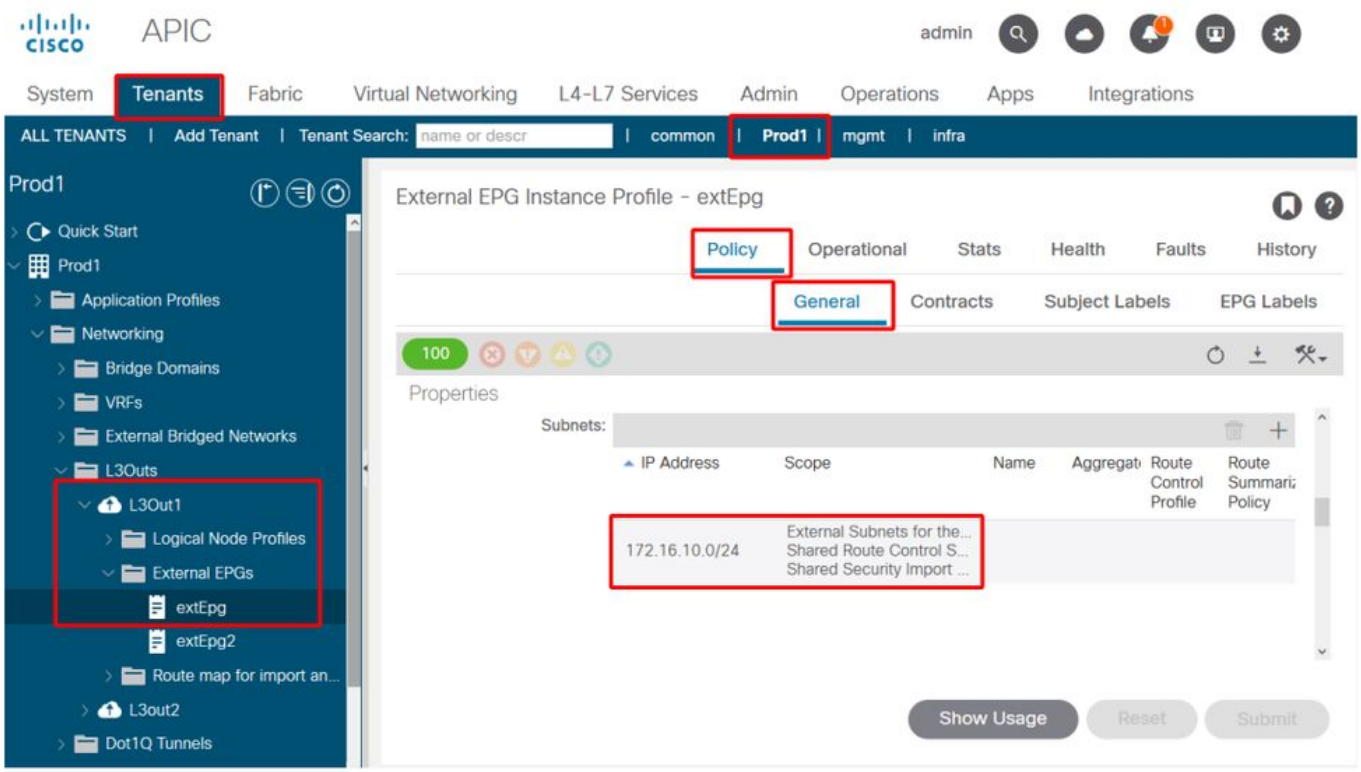
6. Controleer of de provider L3Out EPG een subnetverbinding heeft geconfigureerd met het benodigde bereik gecontroleerd

De provider L3Out EPG moet het te lekken prefix hebben geconfigureerd met de volgende scènes:

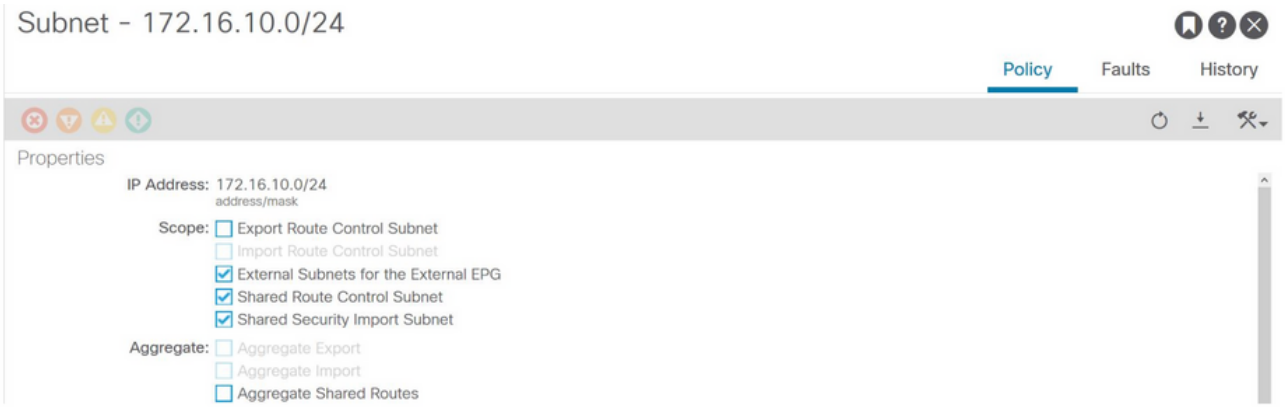
- Externe subnetten voor de externe EPG.
- Gedeelde routercontrolesubnet.
- Gedeelde security importsubnett.

Voor meer details over subnetvlag in L3Out EPG verwijzen naar het hoofdstuk "Extern doorsturen".

Externe EPG-subnetinstellingen



Externe EPG-subnetinstellingen uitgebreid



7. Controleer de pcTag van L3Out EPG-subnet op de niet-BL voor de VRF voor consumenten

Wanneer het verkeer dat bestemd is voor het externe EPG-subnettoegang de niet-BL ingaat, wordt een raadpleging uitgevoerd tegen het doelprefix om de pcTag te bepalen. Dit kan worden gecontroleerd met de volgende opdracht op de niet-BL.

Let op dat deze output valt onder het toepassingsgebied van de VNI 2818048, de VRF-VNID voor consumenten. Door te kijken naar de tabel kan de consument de pcTag van de bestemming vinden, ook al zit deze niet in dezelfde VRF.

```
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
```

De bovenstaande output laat de combinatie zien van het L3Out EPG-subnet en zijn wereldwijde pcTag 25.

8. Controleer de geprogrammeerde zoningregels op de niet-BL voor de VRF voor de consument

Gebruik 'contract_parser.py' of de 'show zoning-rule' opdracht en specificeer de VRF.

Onder commando outputs display twee zoning-regels zijn geïnstalleerd om verkeer van de consument EPG lokale pcTag 16410 naar de L3Out EPG globale pcTag 25 toe te staan. Dit is in het scope 2818048, dat is de scope van de consument VRF.

```
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. Controleer de geprogrammeerde zoningregels op de BL voor de VRF-aanbieder

Gebruik 'contract_parser.py' of de 'show zoning-rule' opdracht en specificeer de VRF. De volgende opdrachtoutput laat zien dat er **GEEN** specifieke zoningregels zijn in de provider VRF zoals

meerdere malen eerder geschetst.

Het is in het toepassingsgebied 2719752 dat de reikwijdte is van aanbieder 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]
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.