Problemen oplossen met L3Out-subnetclassificatie in ACI

Inhoud

Inleiding

Dit document beschrijft de classificatie van externe subnetten binnen Cisco ACI's L3Out EPG's,

Afkortingen

- BD: Bridge-domein
- EPG: Eindpuntgroep
- ExEPG: externe eindpuntgroep
- RIB: Routing Information Base
- VRF: Virtuele routering en doorsturen
- Klasse-ID: tag die een EPG identificeert

Externe EPG-classificatie

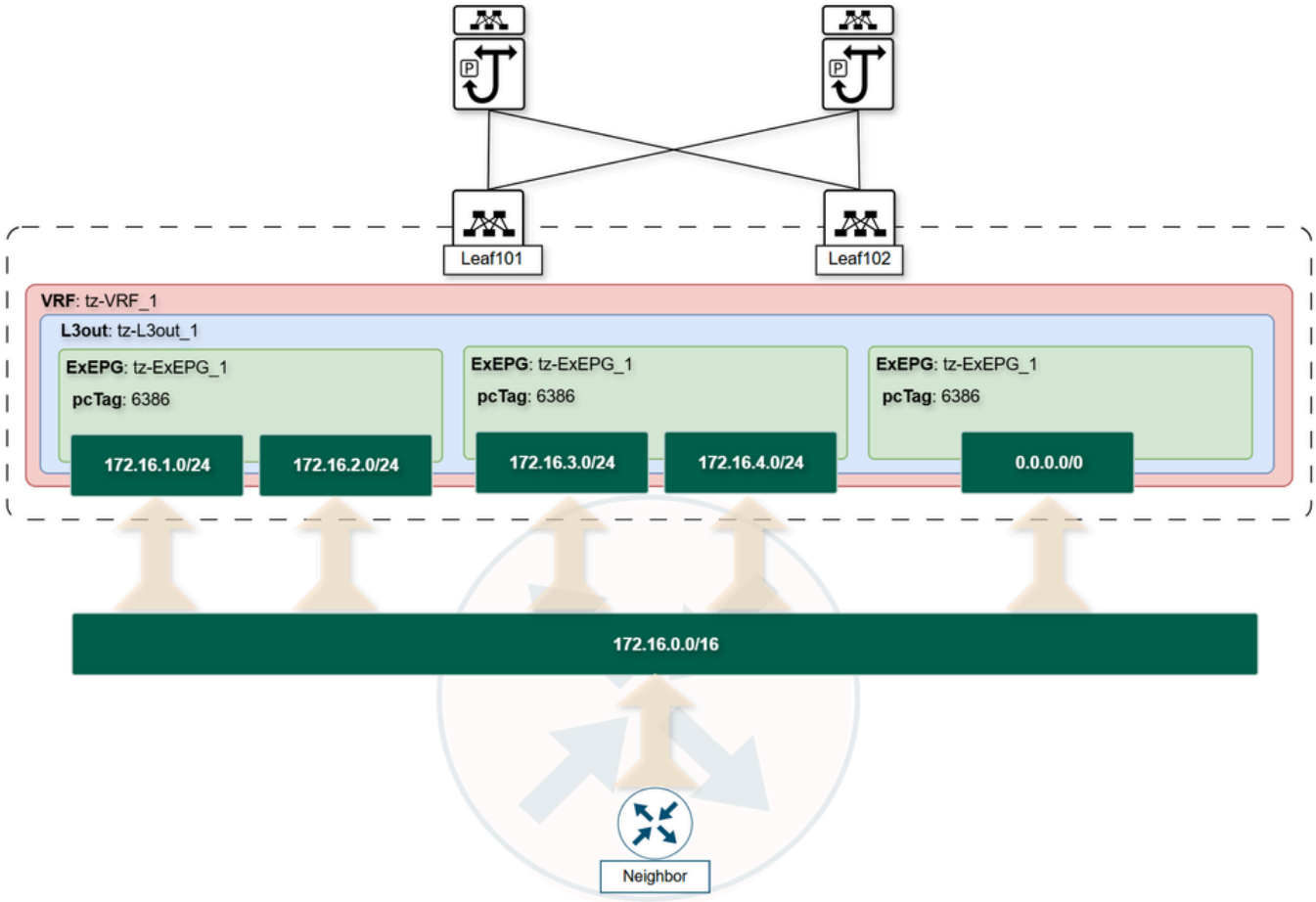
Een externe EPG in Cisco ACI vertegenwoordigt externe gerouteerde netwerken die zijn verbonden via L3Outs. Net als bij de classificatie van eindpunten door een reguliere EPG, classificeert een externe EPG externe subnetten per VRF-basis, wat betekent dat elk subnet uniek moet zijn binnen de VRF-context.

Een veel voorkomende misvatting is dat een extern EPG-subnet alleen voorvoegsels bevat die zijn geaccepteerd via het dynamische routeringsprotocol. Wanneer echter een L3Out wordt gemaakt, is er een standaard routekaart filtering inkomende advertenties; dus alle voorvoegsels

geadverteerd door de dynamische routering protocol worden standaard geaccepteerd. Het primaire doel van het definiëren van subnetten onder een ExEPG-classificatie is alleen om een unieke pcTag toe te wijzen aan subnetten die zijn ingesloten in de ExEPG voor contracthandhaving en beleidstoepassing.

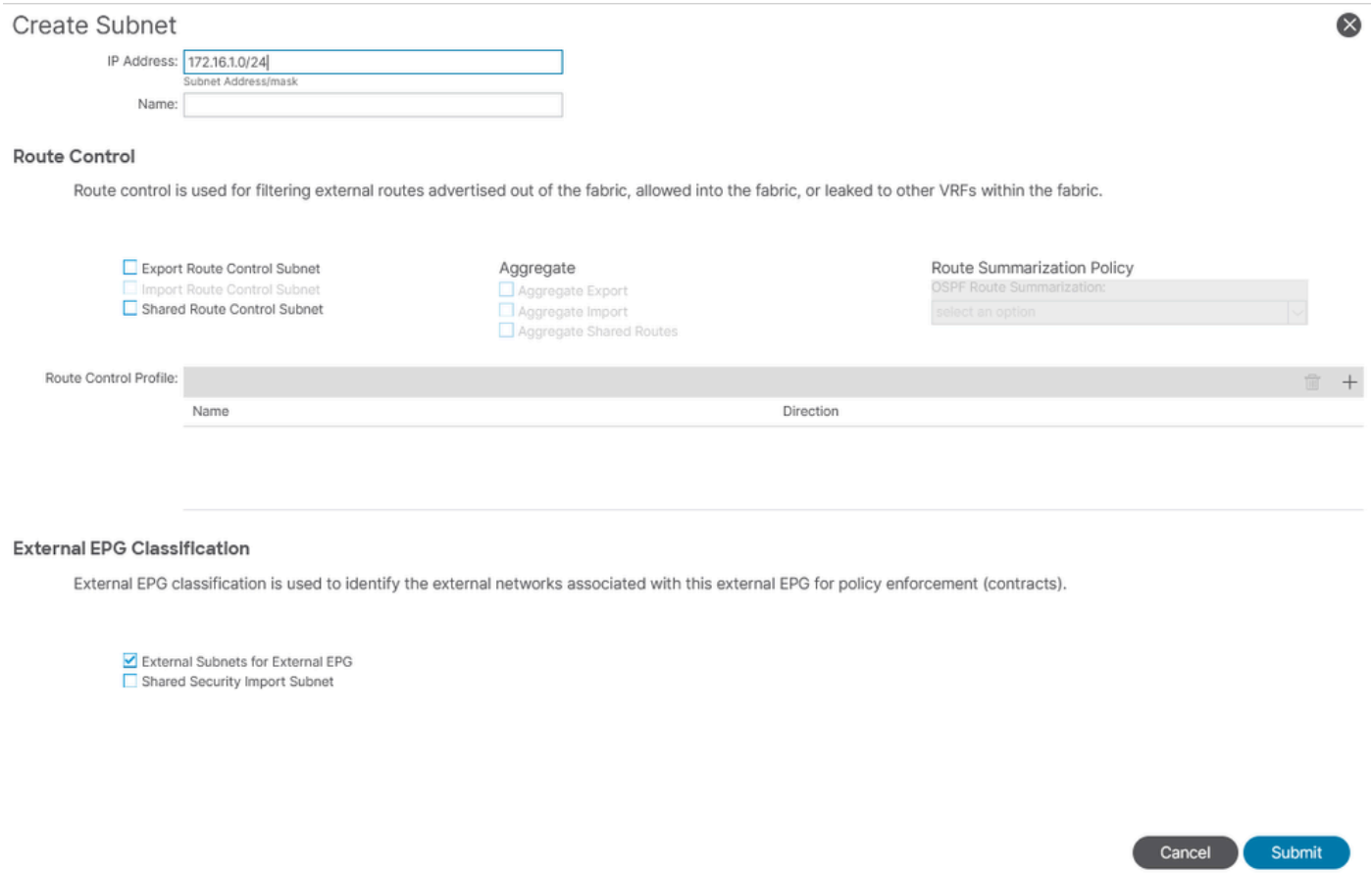
Deze classificatie maakt gedetailleerde beleidscontrole mogelijk. Een enkele externe buur kan bijvoorbeeld een supernet adverteren voor ACI, dat vervolgens kan worden gesegmenteerd in meerdere ExEPG's. Hierdoor kunnen verschillende contractacties worden toegepast op afzonderlijke subnetten, zoals het toestaan van specifieke interne EPG's om alleen te communiceren met aangewezen externe subnetten of het omleiden van verkeer dat bestemd is voor bepaalde voorvoegsels naar een PBR-node voordat het zijn eindbestemming bereikt.

Dit diagram illustreert hoe Cisco ACI externe subnetten classificeert op basis van externe EPG's, waardoor nauwkeurige verkeerssegmentatie en contracthandhaving mogelijk is.



Externe EPG-subnetten Vlaggen

Voor het classificeren en beheren van externe voorvoegsels binnen een ExEPG in ACI, worden specifieke subnetvlaggen geconfigureerd bij het maken van een subnetvoorvoegsel onder een ExEPG. In dit gedeelte wordt elke vlag en het beoogde gebruik ervan beschreven:



- Extern subnet voor externe EPG:
  Deze markering geeft aan dat het subnet zich buiten de ACI-structuur bevindt en niet is geconfigureerd binnen een Bridge Domain of EPG. Het mag alleen worden gebruikt wanneer het voorvoegsel wordt geadverteerd door een routerende buur of statisch in de RIB wordt geïnjecteerd. Deze vlag is standaard ingeschakeld.

- Exportroute controle subnet:
  Deze vlag geeft aan dat het subnet wordt geadverteerd van ACI naar de routerende buur via het dynamische routeringsprotocol. Het mag niet gelijktijdig worden ingeschakeld met de markering Extern subnet voor externe EPG, omdat dit Layer 3-routeringslussen kan veroorzaken. Aangezien ACI het subnet classificeert als extern en het ook terugadverteert, kan dit leiden tot routeringsinconsistenties, ondanks mechanismen voor lusvermijding in routeringsprotocollen.

- Subnet gedeelde routeregeling:
  Deze markering wordt ingesteld wanneer het subnetvoorvoegsel bedoeld is om te worden gedeeld over meerdere VRF's, waardoor er een route tussen de contexten kan lekken.

- Gedeeld subnet voor het importeren van beveiliging:
  Gebruikt in combinatie met de vlag van het subnet voor gedeelde routebesturing, maakt dit het delen van beveiligings-pcTags voor externe subnetten over verschillende VRF's mogelijk, waardoor consistente beleidshandhaving wordt vergemakkelijkt.

- Subnet voor controle van de invoerroute:
  Deze vlag maakt granulaire controle mogelijk over de voorvoegsels die worden ontvangen

van routerende buren. Standaard accepteert ACI alle binnenkomende routeadvertenties; voor het inschakelen van deze markering moet de handhaving van routebesturing worden geactiveerd om binnenkomende voorvoegsels te filteren.

- Geaggregeerde sectie:
  Dit deel is alleen van toepassing op het subnet quad-0 (0.0.0.0/0) en bevat een samenvatting van alle voorvoegsels in de RIB voor geaggregeerde export of import. Wanneer subnetten naar andere VRF's worden gelekt, worden ze samengevat als geaggregeerde gedeelde routes om routeringstabellen te optimaliseren.

Opdrachten voor verificatie en probleemoplossing

routering

Om te beginnen moet de route aanwezig zijn in de routetafel van de VRF op de Border Leaf-switches. Deze opdracht toont bijvoorbeeld een BGP-route in de VRF tz:tz-VRF_1:

<#root>

```
Leaf101#
show ip route bgp vrf tz:tz-VRF_1


IP Route Table for VRF "tz:tz-VRF_1"


'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>


172.16.1.0/24
, ubest/mbest: 1/0
*via 10.10.1.2
%tz:tz-VRF_1, [20/0], 00:00:04, bgp-65002, external, tag 65003
Leaf101#
```

Dit bevestigt dat de route is geïnstalleerd in de VRF-routeringstabel en beschikbaar is voor doorstuurbeslissingen.

Classificatie

Nadat de route in de routeringstabel aanwezig is, bepaalt de classificatie hoe het verkeer wordt afgehandeld op basis van het beleid. In ACI is classificatie gekoppeld aan de ExEPG en de bijbehorende subnetten.

Om subnetclassificatie onder een ExEPG te valideren, kan de APIC worden opgevraagd voor de klasse l3extInstP, die de externe EPG-instantie vertegenwoordigt. De onderliggende klasse l3extSubnet geeft de subnetten weer die onder die ExEPG zijn geconfigureerd. Voorbeeld:

<#root>

moquery -c l3extInstP -f 'l3ext.InstP.dn*"[tenant name].*[l3out name]"' -x rsp-subtree=children rsp-

<#root>

APIC#

moquery -c l3extInstP -f 'l3ext.InstP.dn*"tz.*l3out"' -x rsp-subtree=children rsp-subtree-class=l3extSub

Total Objects shown: 1

l3ext.InstP

name : tz-ExEPG_1

!-- cut for brevity --!
configSt : applied
descr :
dn : uni/tn-tz/out-l3out/instP-tz-ExEPG_1
!-- cut for brevity --!
floodOnEncap : disabled
isSharedSrvMsiteEPg : no
lcOwn : local
matchT : AtleastOne
mcast : no
modTs : 2025-09-10T00:36:49.239+00:00
monPolDn : uni/tn-common/monepg-default
nameAlias :
pcEnfPref : unenforced

pcTag : 32771

pcTagAllocSrc : idmanager
prefGrMemb : exclude
prio : unspecified
rn : instP-tz-ExEPG_1
scope : 3047430
status : modified
targetDscp : unspecified
triggerSt : triggerable
txId : 1152921504612318828
uid : 15374
userdom : :all:

l3ext.Subnet

ip : 172.16.1.0/24

!-- cut for brevity --!
dn : uni/tn-tz/out-l3out/instP-tz-ExEPG_1/extsubnet-[172.16.1.0/24]

```
extMngdBy :
lcOwn : local
modTs : 2025-09-10T01:05:13.249+00:00
monPolDn : uni/tn-common/monepg-default
!-- cut for brevity --!
rn : extsubnet-[172.16.1.0/24]

scope : import-security


status :
uid : 15374
userdom : :all:

APIC#
```

Als er geen uitvoer wordt geretourneerd voor de klasse l3extSubnet, geeft dit aan dat er geen subnetten zijn geconfigureerd onder de externe EPG. Zonder geconfigureerde subnetten kan ACI een pcTag niet koppelen aan het subnet voor inkomend verkeer, waardoor het verkeer wordt weggelaten ondanks de route die in de routeringstabel bestaat.

Een ander belangrijk aspect om op te merken, is de reikwijdte van het subnet, dit vertegenwoordigt de vlaggen die zijn ingesteld voor het subnet in kwestie:

- Invoerzekerheid

Het subnet is gemarkeerd met Extern subnet voor Externe EPG.

- export-rtctrl

Het subnet is gemarkeerd met Export Route Control.

- import-rtctrl

Het subnet is gemarkeerd met Import Route Control.

- met gedeeld effect

Het subnet is gemarkeerd met Shared Security Import Subnet.

- gedeeld-rtctrl

Het subnet is gemarkeerd met gedeelde routebesturing.

De routeringsprotocollen en controlevliegtuigprocessen werken de routeringstabellen bij bij het ontvangen van een prefix van een genoemde buur, die vervolgens worden geprogrammeerd in de HAL L3-forwardingtabellen. De HAL L3-routes vertegenwoordigen de werkelijke Layer 3-routes die zijn geprogrammeerd in de hardwaretafels (ASIC's) op de switches van het blad. Deze routes zijn afgeleid van de routeringsprotocollen en routeringstabel berekeningen en worden gebruikt voor het doorsturen van beslissingen.

<#root>

```
<-- When the prefix is not configured under the External EPG, a classification of 0xf is seen -->
Leaf101#
vsh_lc -c 'show platform internal hal l3 routes vrf tz:tz-VRF_1' | egrep "Prefix/Len|172.16.1.0" | cut -

VRF |   Prefix/Len  | RT|CLSS| Flags
4675| 172.16.1.0/ 24| UC| f|spi,dpi

Leaf101#
<-- When the prefix is configured under the External EPG, a classification of the pcTag in hexadecimal
Leaf101#
vsh_lc -c 'show platform internal hal l3 routes vrf tz:tz-VRF_1' | egrep "Prefix/Len|172.16.1.0" | cut -

VRF |   Prefix/Len  | RT|CLSS| Flags
4675| 172.16.1.0/ 24| UC|8003|spi,dpi

Leaf101#
Leaf101#
vsh_lc -c '
dec 0x8003'

32771
Leaf101#
```

Wanneer vervolgens een subnet is geconfigureerd met de markering Extern subnet voor externe EPG in een ExEPG, werkt een intern proces met de naam Beleidsmanager (policy-mgr) de toewijzingstabel prefix-naar-pcTag bij met dit subnetitem en de bijbehorende pcTag. De Policy Manager fungeert als de fabric-gecentraliseerde beleidsorchestratie-engine en vertaalt beleidsdefinities op hoog niveau naar uitvoerbare configuraties in de ACI-fabric. Dit zorgt voor consistente en veilige applicatieconnectiviteit en netwerkgedrag door de juiste pcTags af te dwingen voor verkeersclassificatie en doorstuurbeslissingen op basis van de geconfigureerde externe subnetten.

<#root>

```
Leaf101#
vsh -c 'show system internal policy-mgr prefix' | egrep "tz:tz-VRF_1"

3047430 36 0x80000024 Up tz:tz-VRF_1 ::/0 15 True True False False
3047430 36 0x24 Up tz:tz-VRF_1 0.0.0.0/0 15 True True False False
3047430 36 0x24 Up tz:tz-VRF_1 172.16.1.0/24 32771 True True False False

Leaf101#
```

Dit bevestigt het voorvoegsel 172.16.1.0/24 wordt geadverteerd door de buurman naar ACI border leaf switch, en ACI heeft het voorvoegsel hieronder pcTag 32771 geclassificeerd

Contracten

Een zoneringsregel is het onderliggende proces dat het contractbeleid tussen EPG's (inclusief ExEPG's) binnen de structuur afdwingt. De VRF VNID (scope) en de pcTag van de External EPG kunnen worden gebruikt om de communicatieregels die worden toegepast tussen bron- en bestemmings-EPG's te definiëren en te valideren. In wezen vertalen zoneregels contractrelaties op hoog niveau in specifieke, afdwingbare regels die zijn geprogrammeerd op de switches van bladeren.

Een belangrijk aspect om te overwegen is waar het contract in de stof is geïnstalleerd. Standaard is de VRF geconfigureerd met de optie Handhavingsrichting beleidsbesturing ingesteld op ingress. Met deze instelling wordt bepaald dat de bestemmingsregel voor een bepaald contract wordt ingesteld op de switch van het blad waar het broneindpunt zich bevindt.

Voor deze oefening komt het verkeer binnen van een L3Out, de bestemmingregel wordt geïnstalleerd op het grensblad dat verbinding maakt met dat L3Out, omdat dit blad fungeert als het bronblad voor het verkeer dat het weefsel binnenkomt.

<#root>

```
Leaf101#
```

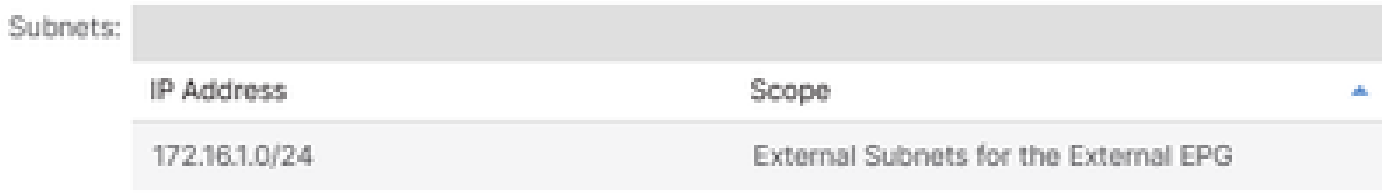
```
show zoning-rule scope 3047430 | egrep "Rule|---|32771"
```

```
+---------+--------+--------+----------+----------------+---------+---------+-------------------+------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       | operSt  |  Scope  |        Name       |
+---------+--------+--------+----------+----------------+---------+---------+-------------------+------
|  4441   | 49153  | 32771  |     5    |     bi-dir     | enabled | 3047430 |     tz:Contract   |
|  4500   | 32771  | 49153  |     5    | uni-dir-ignore | enabled | 3047430 |     tz:Contract   |
+---------+--------+--------+----------+----------------+---------+---------+-------------------+------
Leaf101#
```

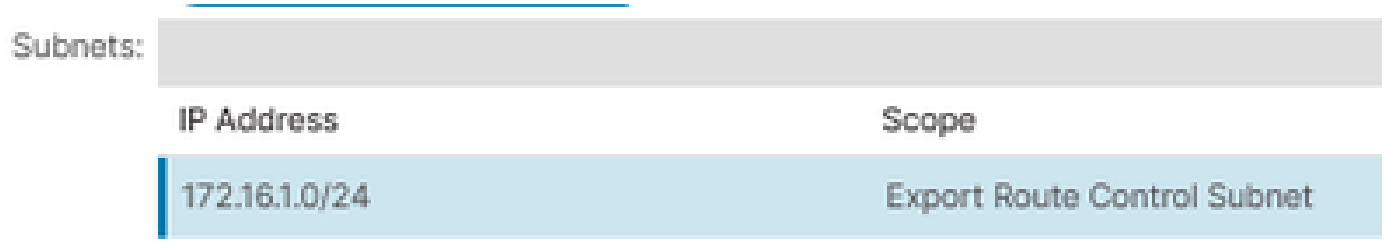
transitorouting

Transit routing stelt de stof in staat om als een doorvoernetwerk te fungeren door externe routes te

adverteren die van de ene L3Out naar de andere zijn geleerd. Voor een goede configuratie van de doorvoerroutering moet het binnenkomende subnet worden gemarkeerd met de markering Extern subnet voor externe EPG.



Tegelijkertijd moet de L3Out die dit subnet adverteert aan andere externe peers de vlag Export Route Control Subnet hebben ingeschakeld op het corresponderende subnet. Met deze vlag kan het subnet worden herverdeeld en geadverteerd uit de fabric via het routeringsprotocol dat op die L3Out is geconfigureerd.



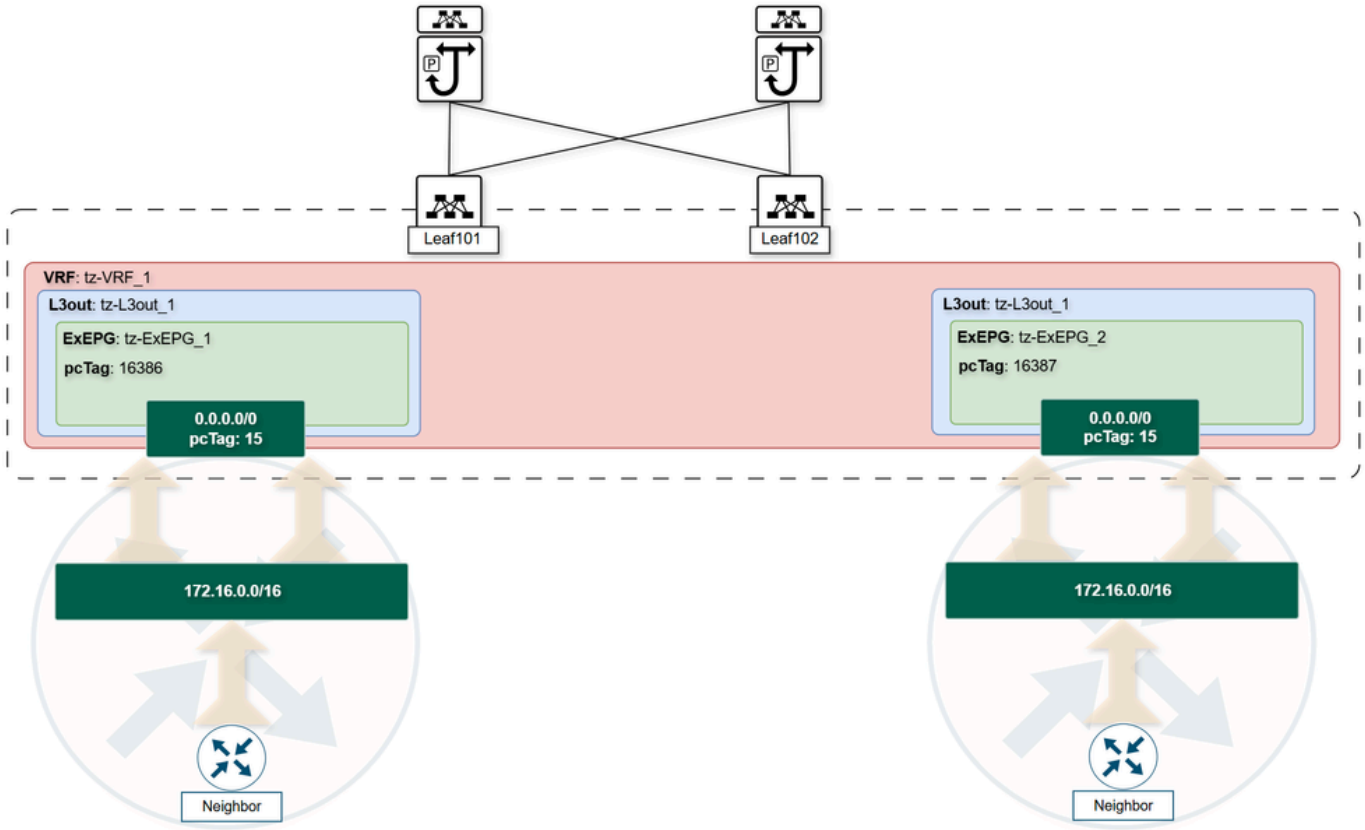
Ten slotte moet een contract tussen de ontvangen en de exporterende L3out worden geconfigureerd om het proces van het distribueren van de route te voltooien.

Veelvoorkomende problemen in de externe EPG-classificatie van het subnet

pcTag 15

Eerder werd in dit document vermeld dat het ExEPG-subnet u helpt om de subnetten in de juiste pcTag te classificeren om redenen van beleidshandhaving. Een belangrijke uitzondering op deze classificatie is het quad-0 subnet (0.0.0.0/0) wanneer geconfigureerd met de External Subnet for External EPG flag. Dit subnet krijgt altijd de gereserveerde pcTag 15 toegewezen, die effectief fungeert als een jokerteken voor al het externe verkeer binnen een VRF.

Dit diagram geeft het probleem weer bij het configureren van quad-0 met External Subnet for External EPG op meerdere ExEPG's binnen dezelfde VRF:



- Het quad-0-subnet wordt vaak verward met de standaardroute. Hoewel dit soms waar is, zoals wanneer een dynamische routeringsbuur alleen de standaardroute naar de ACI L3Out adverteert, is de rol van het quad-0-subnet in ACI breder als een catch-all-classificatie.
- Het is gebruikelijk om meerdere ExEPG's met het quad-0-subnet te configureren om alle voorvoegsels te accepteren die door een buurman worden geadverteerd. Hoewel dit het doel van brede acceptatie bereikt, kan dit leiden tot onverwachte asymmetrische routering wanneer meerdere ExEPG's met quad-0 worden geconfigureerd binnen dezelfde VRF. Wanneer meerdere ExEPG's binnen dezelfde VRF zijn geconfigureerd met quad-0 als een extern subnet, kan ACI niet deterministisch selecteren welke L3Out moet worden gebruikt voor een specifiek doelsubnet. In plaats daarvan selecteert het willekeurig een L3Out.
- Dit gedrag kan leiden tot asymmetrische routering, verkeersonderbrekingen of zelfs verkeersdalingen als de willekeurig geselecteerde L3Out niet over de nodige contracten beschikt om communicatie mogelijk te maken.

overlappende subnetten

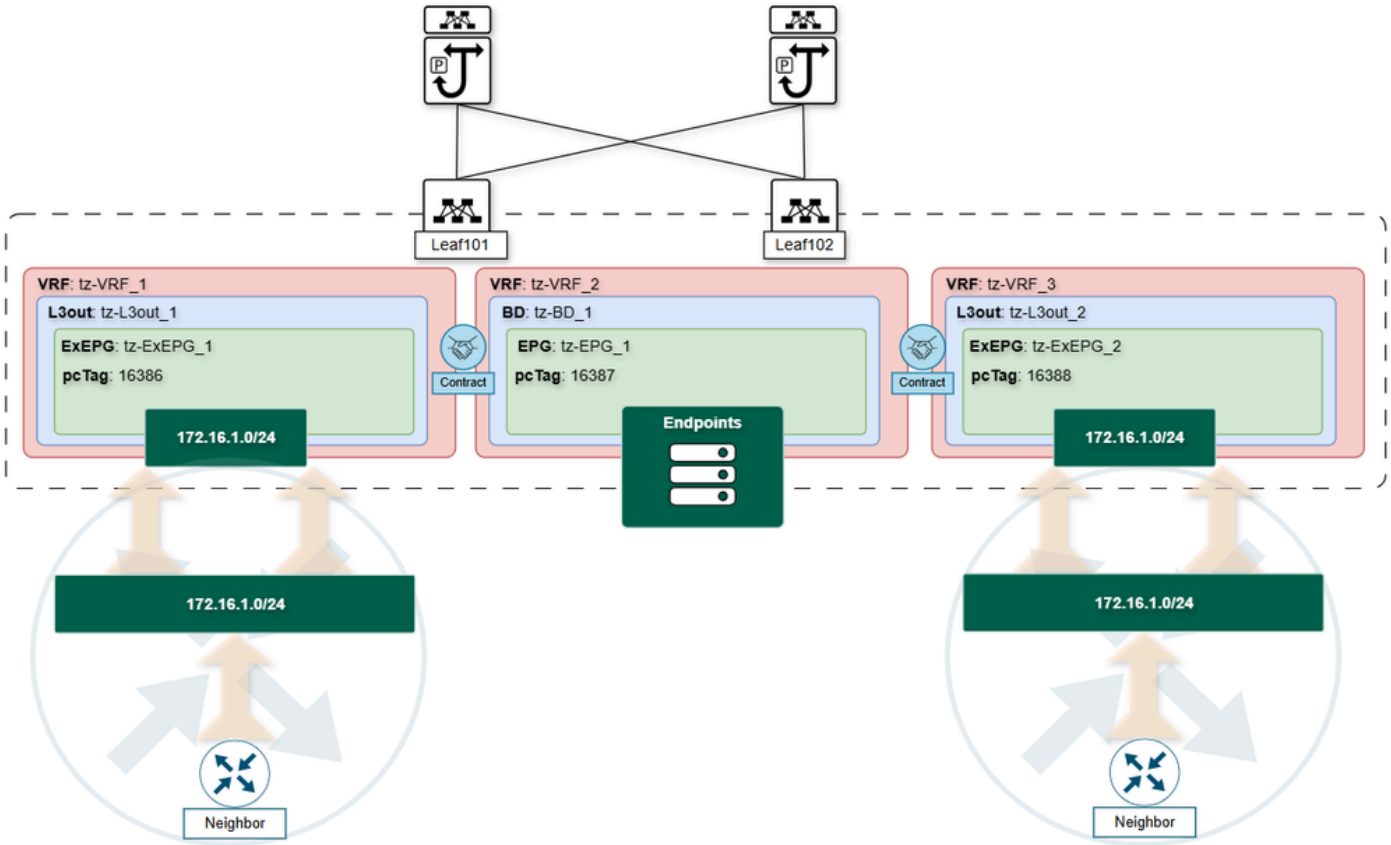
Configuratie van identieke subnetten voor verschillende ExEPG's is niet toegestaan. Als u dit probeert te doen, wordt fout "F0467: Prefix-item al gebruikt in een andere EPG" geactiveerd, waardoor subnetduplicatie binnen een VRF wordt voorkomen.

Er kunnen echter overlappende subnetten tussen verschillende VRF's bestaan, omdat elke VRF een onafhankelijke routeringtabelcontext behoudt. Door deze scheiding kan hetzelfde subnet worden geconfigureerd in ExEPG's die tot verschillende VRF's behoren. Desondanks is voorzichtigheid van cruciaal belang bij het uitvoeren van VRF-routelekken met betrekking tot deze overlappende subnetten, omdat dit kan leiden tot asymmetrische doorstuurbeslissingen vanwege

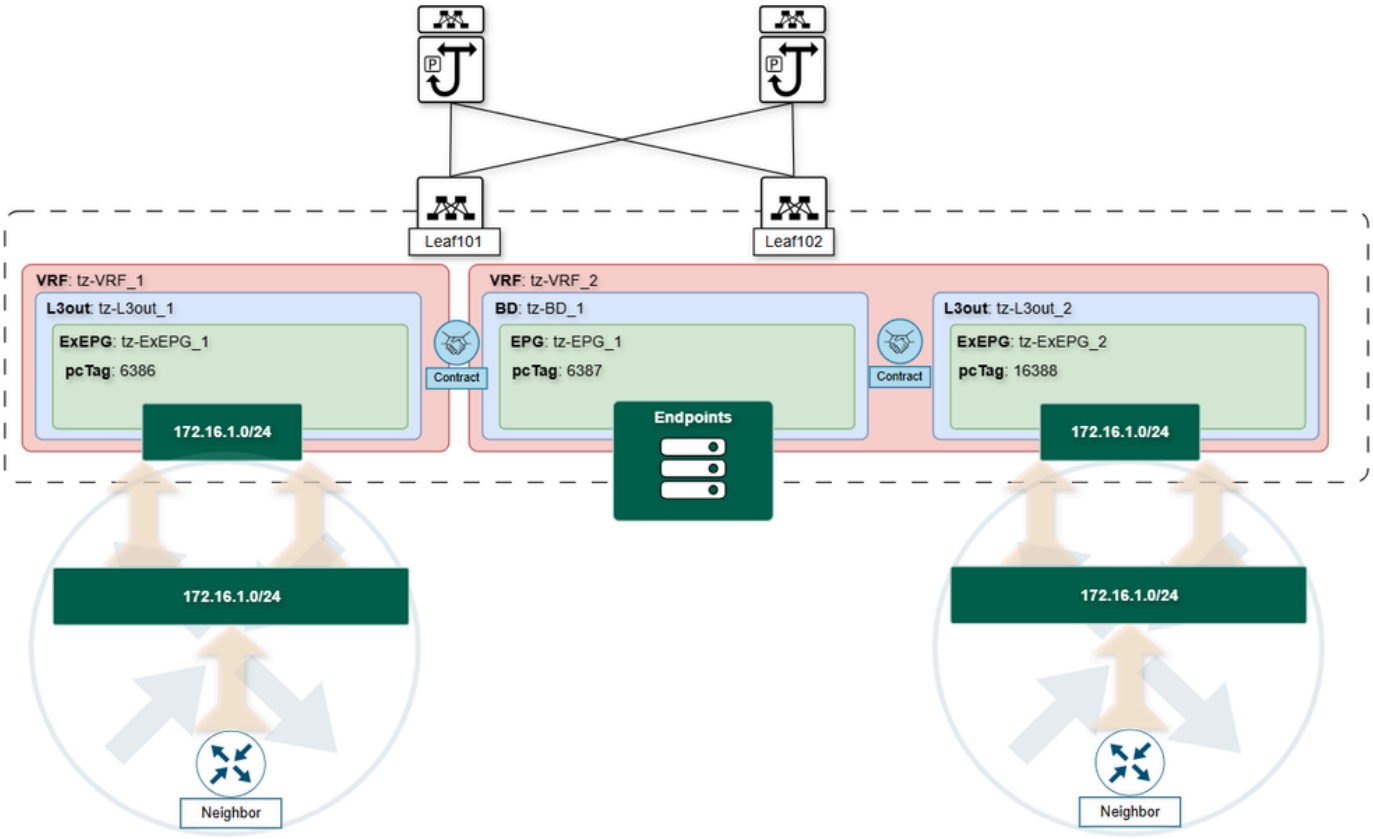
conflicten in subnetclassificatie (pcTag) versus routeringsinformatie (RIB).

Belangrijke scenario's zijn onder meer:

- Route lekken van twee VRF's naar een derde VRF:
  Wanneer twee VRF's hetzelfde subnet lekken in een derde VRF, installeert de ontvangende VRF het eerste subnet dat het ontvangt op basis van gedeeld beleid van de APIC. Als de switch die deze VRF afhandelt opnieuw opstart of de routeringsverkiezing wijzigt, kan de routeringstabel worden bijgewerkt naar een andere L3Out, waardoor inconsistent doorstuurgedrag ontstaat.



- Local-to-VRF L3Out ExEPG Overlapping met gelekte subnetten:
  In ontwerpen waar route lekken wordt gebruikt, als een lokale L3Out ExEPG is geconfigureerd met hetzelfde subnet als een gelekte subnet, de lokale routering vermelding altijd voorrang op de gelekte routes.



Deze situaties benadrukken dat de asymmetrische doorstuurproblemen voortkomen uit de classificatie- en doorstuurbeslissingslaag, niet uit de routeringstabel zelf. Terwijl subnetclassificatie een subnet associeert met een specifieke L3Out en ExEPG voor beleidshandhaving, kan de routeringstabel verwijzen naar een andere L3Out-bestemming. Deze mismatch kan ertoe leiden dat verkeer inconsistent wordt doorgestuurd, wat leidt tot potentiële connectiviteitsproblemen of lacunes in de handhaving van het beleid.

Standaardgedrag routebesturing importeren

ACI accepteert standaard alle binnenkomende routeadvertenties van buren. Om te bepalen welke voorvoegsels worden geaccepteerd, moet u Route Control Enforcement: inbound op het L3Out root-object inschakelen:

Navigeer naar Huurders > [naam huurder] > Netwerken > L3outs > [L3out name] .

Deze actie maakt een routekaart onder het geselecteerde routeringsprotocol.

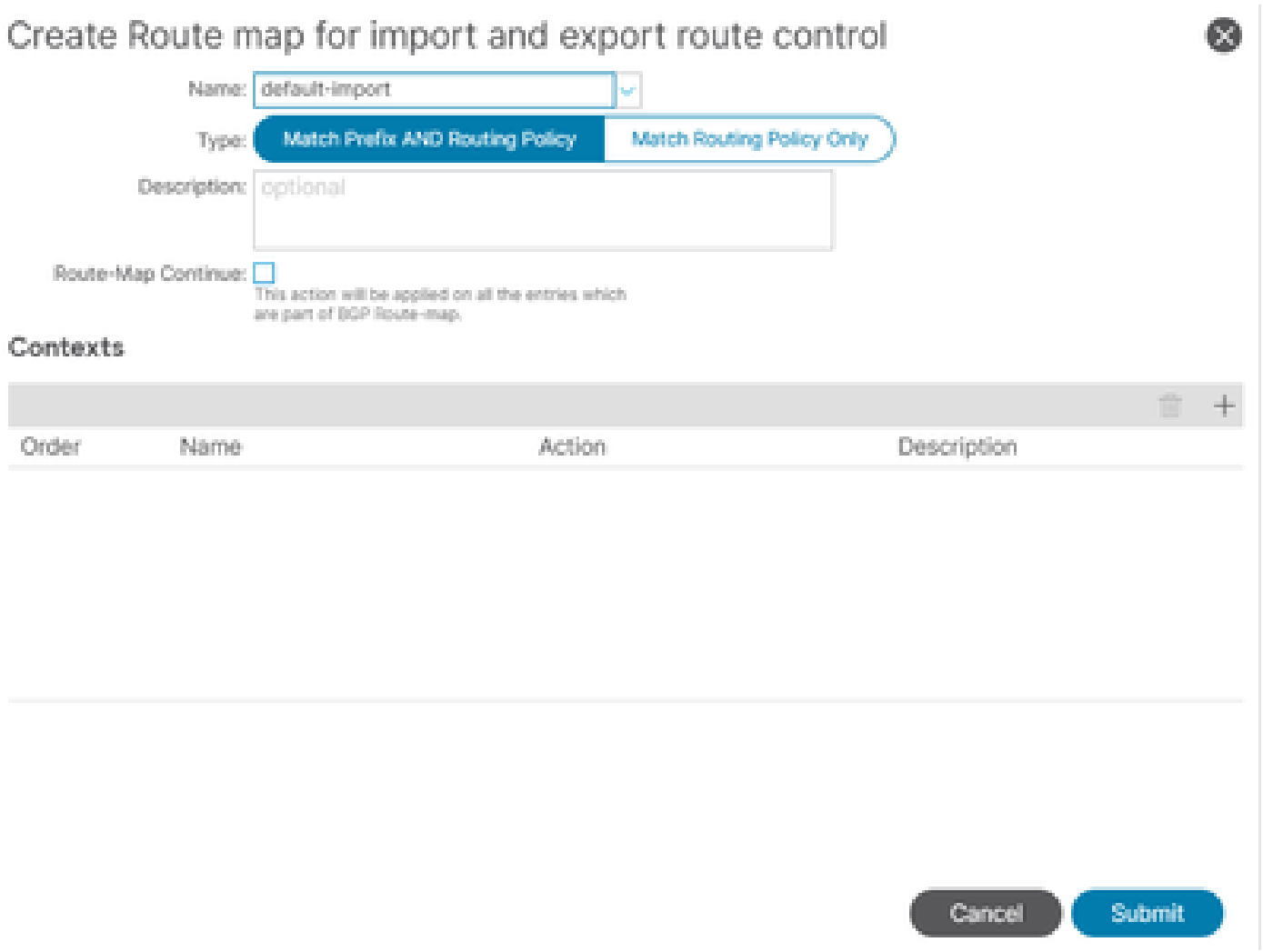
<#root>

```
Border Leaf#
show ip bgp neighbors vrf tz:tz-VRF1 | egrep route-map

Outbound route-map configured is exp-l3out-ExEPG-peer-2981888, handle obtained
Inbound route-map configured is imp-l3out-ExEPG-peer-2981888, handle obtained


Border Leaf#
show route-map imp-l3out-ExEPG-peer-2981888

route-map imp-l3out-ExEPG-peer-2981888,
permit
, sequence 15801
Match clauses:
ip address prefix-lists: IPv4-peer49155-2981888-exc-ext-inferred-import-dst

ipv6 address prefix-lists: IPv6-deny-all
Set clauses:

Border Leaf#
show ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst

ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst: 1 entries
seq 1 permit 172.16.1.0/24
Border Leaf#
```

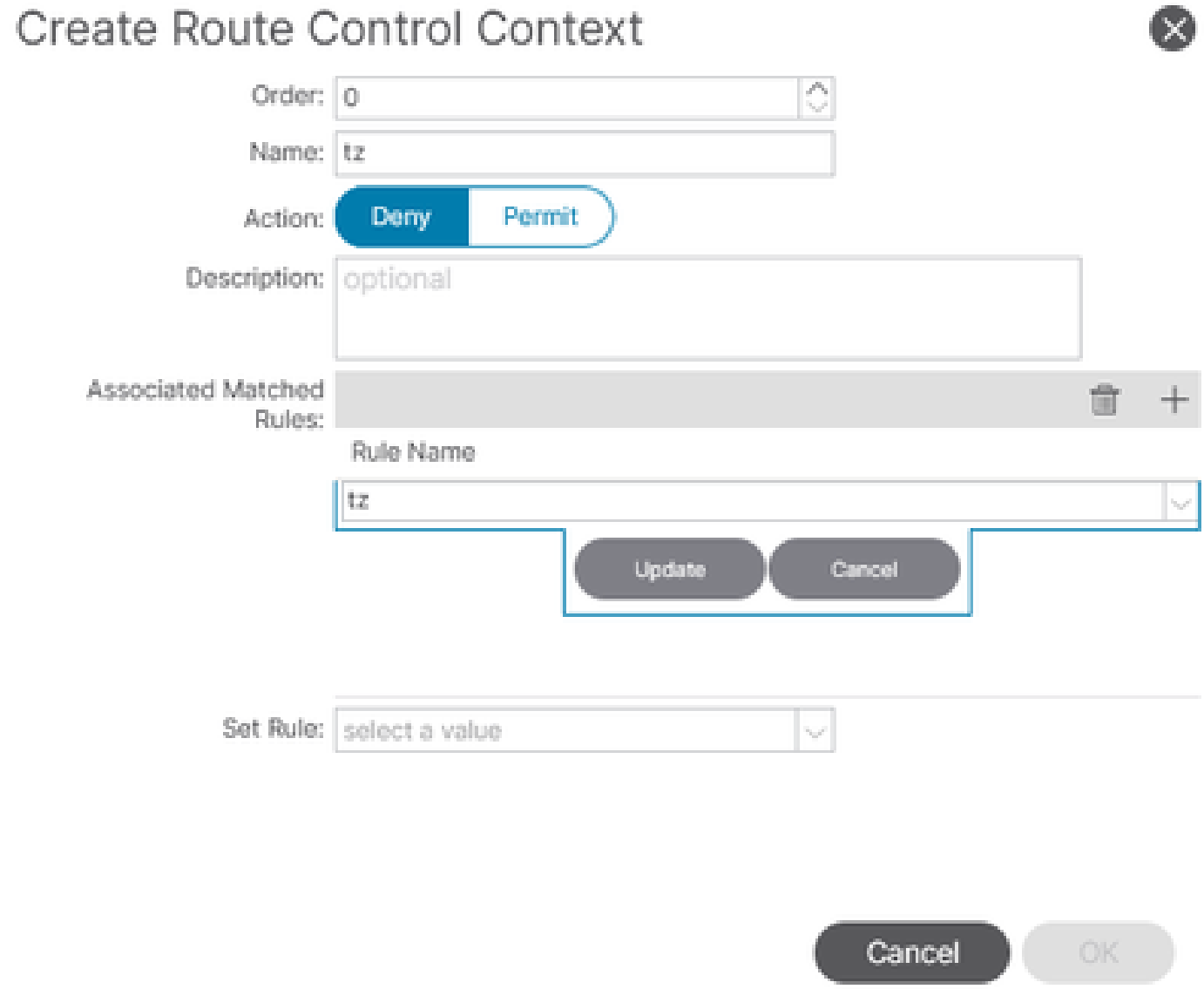
Standaard staat deze import route-map alle binnenkomende prefixes toe. U kunt dit gedrag als volgt wijzigen:

Navigeer naar Huurders > [naam huurder] > Netwerken > L3outs > [L3out name] > Routekaart voor import- en exportroutebeheer

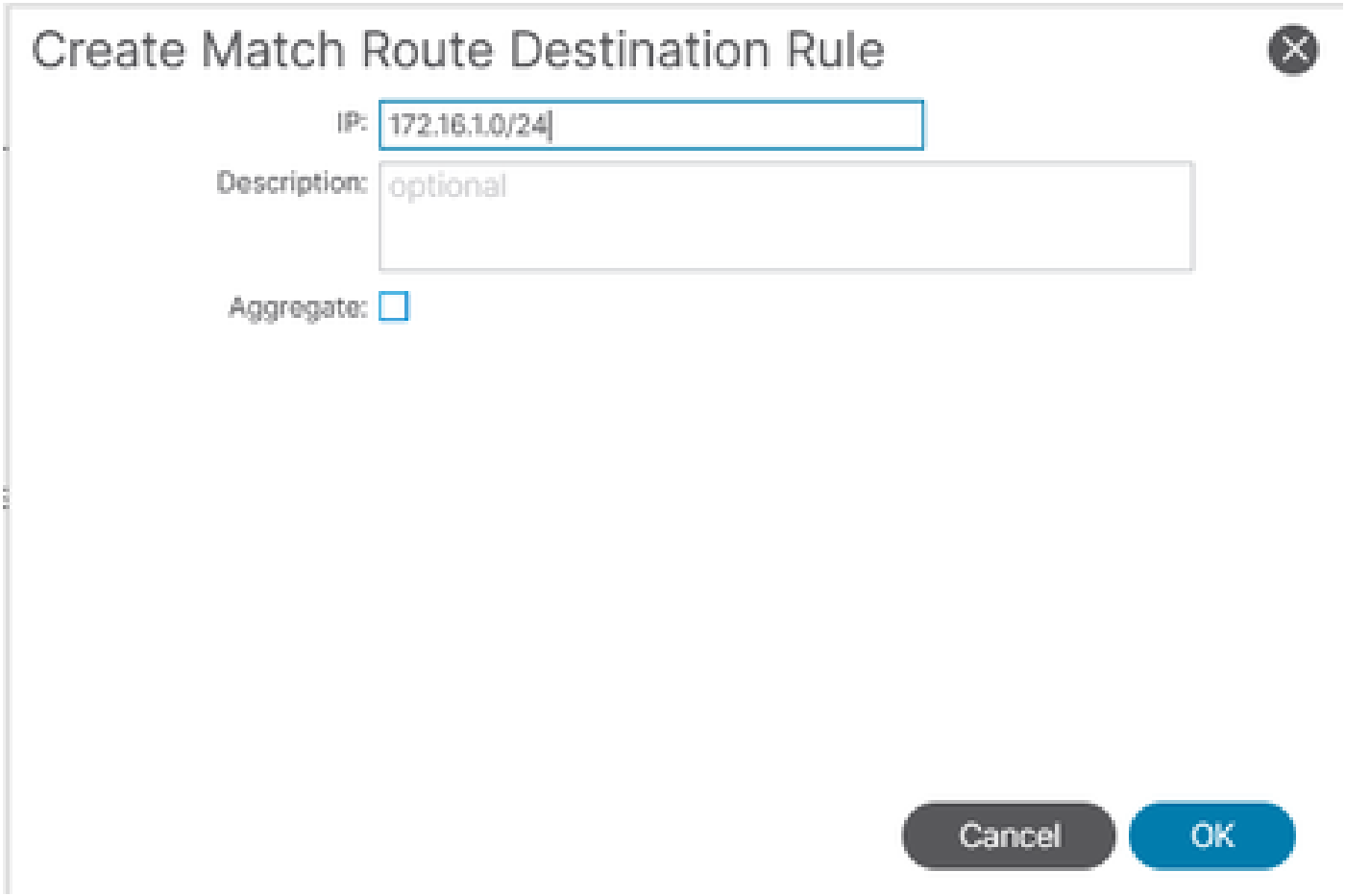
Selecteer de standaard routekaart importeren of maak een nieuwe met behulp van het tandwiel pictogram rechtsboven.



Maak in de sectie Context een nieuwe gekoppelde overeenkomende regel.



Blader in de sectie Regels afstemmen naar Voorvoegsel afstemmen en voeg de specifieke subnet(en) toe die u wilt beheren.



Na het indienen van het beleid verandert de actie voor het importeren van routekaarten dienovereenkomstig, waardoor de gewenste voorvoegselfiltering wordt afgedwongen.

<#root>

```
Border Leaf#
```

show route-map imp-l3out-ExEPG-peer-2981888

```
route-map imp-l3out-ExEPG-peer-2981888,
```

deny

```
, sequence 8001
Match clauses:
ip address prefix-lists: IPv4-peer49155-2981888-exc-ext-in-default-import2tz0tz-dst
ipv6 address prefix-lists: IPv6-deny-all
Set clauses:

Border Leaf#
```

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.