Overlappende subnetten op L3outs in Cisco ACI

Inhoud

Inleiding

Cisco's Application Centric Infrastructure (ACI) vergemakkelijkt de communicatie tussen interne huurders en externe routed netwerken, via L3outs (Layer 3). Zulke L3outs kunnen ook worden geconfigureerd om één of meer End Point Group (EPG's) te hebben. Om ACI te weten te komen hoe het inkomende verkeer te classificeren als een L3out's EPG, moeten expliciete subnetten worden gedefinieerd met bepaalde vlaggen die worden geactiveerd. Dit artikel beoogt een licht te werpen op de hardwareimplementatie van L3out EPG's in de context van op contracten gebaseerde beleidsapplicatie. We zullen specifiek de vlag "externe subnetten voor externe EPG's" verkennen en de onverwachte gevolgen van het verklaren van overlappende prefixes als "extern" op afzonderlijke EPG's.

concept

De vuistregel is: Bij het implementeren van L3outs moeten afzonderlijke EPG's in dezelfde Virtual Routing and Forwarding (VRF)-instantie geen overlappende subnetten hebben die gemarkeerd zijn als "externe subnetten voor externe EPG's". Dit betekent ook dat verkeer dat afkomstig is van een specifiek subnet niet door verschillende EPG's moet worden ingevoerd. Dit kan een onverwachte classificatie van het verkeer op basis van de langste prefixwedstrijd veroorzaken ten opzichte van subnetten die zijn gedeclareerd voor niet-verbonden EPG's. Laten we een paar scenario's bekijken om dit in detail te begrijpen

Voorwaarden

Basisbegrip van ACI: L3outs, contracten en handhaving van het beleid. Enkele nuttige termen worden hieronder kort uitgelegd, meer gedetailleerde informatie hierover valt buiten het toepassingsgebied van dit document:

pcTag: ACI classificeert verkeer in pcTags en dit zijn interne representaties van EPG's. Deze waarden hebben standaard een bereik van VRF, d.w.z. ze zijn uniek binnen een VRF, maar kunnen opnieuw gebruikt worden bij VRF's. Als de ene EPG echter een contract heeft met een andere EPG in een andere VRF / Tenant, heeft de waarde van de pcTag een mondiaal bereik, d.w.z. dat u geen andere EPG in ACI met dezelfde pcTag vindt.

ELAM: Embedded Logic-netwerkmodule. Dit gereedschap wordt gebruikt om één pakje op ASIC in te voeren op basis van filters en om de kopregels/vlaggen te controleren die op het pakje zijn ingesteld. Dit hulpmiddel helpt ook het begrijpen van lookups / logica die is gemaakt door op hardware gebaseerde oplossingen

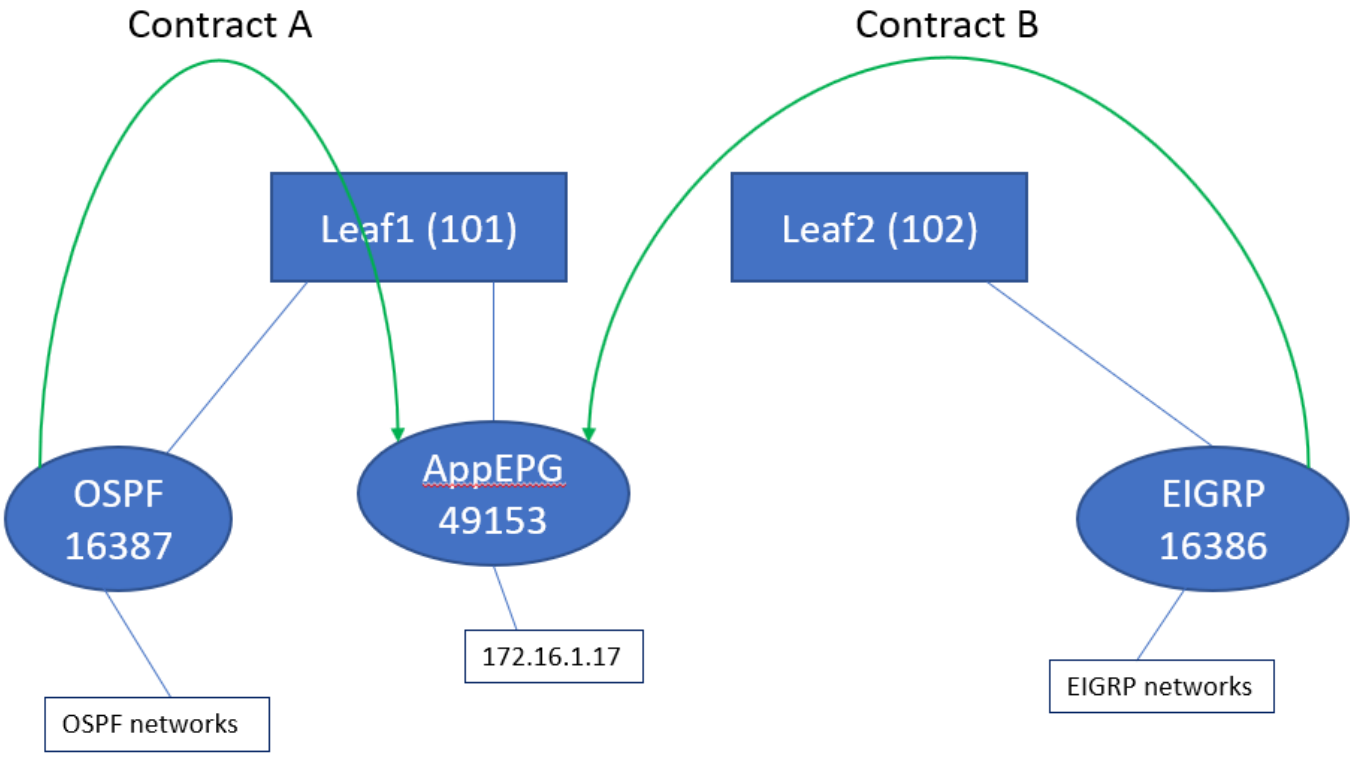
klasse/klasse: wanneer het verkeer binnenkomt in een blad, op basis van de richting van beleidshandhaving en de ter plaatse beschikbare voorvoegselkennis, zal het blad bron- en doelverkeer in EPG's markeren - in ELAM-opnamen zal dit respectievelijk als klasse en klasse worden gezien

zoning-regel: Dit zijn interne representaties van contracten en zijn vergelijkbaar met lijnen van een ACL. De waarden SrcEpg en DstEpg zouden met klasse/klasse voor verkeer moeten overeenkomen om een bepaalde regel te bereiken en moeten worden toegestaan. Standaard in een afgedwongen vrf wordt de laatste regel impliciet ontkend , zodat elk verkeer dat niet aansluit tegen een bepaalde regel , het impliciete ontkennen geraakt en wordt ingetrokken.

Instellen en topologie

Twee bladzijden - 101 en 102 , model: N9K-C93180YC-EX

- Versie 3.2(4)e
- Eén VRF gebruikt - Beleidshandhaving voorkeur : gedwongenHandhaving van het beleid: Ingoers.VRF VPN(VxLAN-netwerkidentificatie): 2752513; pcTag: 3270
- L3out in Leaf1 (101) - Protocol: Open kortste pad eerst (OSPF)L3 interfacegebruiker voor wijk - eth1/22 (10.27.48.1/24)externe EPG pcTag: 16387
- Toepassing EPG op Leaf101 Trunk - eth1/24 pcTag: 49153IP-eindpunt: 172.16.1.17 Gateway: 172.16.1.254/24 - ingezet op Bridge Domain (BD) BD heeft pcTag 3271
- L3out op Leaf2 (202) - Protocol: Enhanced Interior Gateway Routing Protocol (NGEW)SVI gebruikt voor buren met pad 1/16 - VLAN 2747 (10.27.47.1/24)externe EPG pcTag: 163869



Scenarios

Verkeersbronnen uit overlappende subnetten

In dit scenario kijken we naar mogelijke verkeerde classificatie als het verkeer afkomstig is van overlappende subnetten (vanuit het perspectief van ACI)

OSPF-advertenties:

10.9.9.6/32

DHCP-advertenties:

10.9.9.1/32

We beginnen met de topologie in Figuur 1, maar zonder contracten. Voor EPG op OSPF definiëren wij Subnet 0.0.0.0/0 als "extern Subnet voor externe EPGs" en 10.9.9.0/24 met de zelfde vlag voor de EPG van Ecu. Zo zien de tabellen op Leaf1 en 2 eruit:

Leaf1:

```
leaf101# show end int eth1/24
Legend:
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       L - local
+------------------------------------+--------------+-----------------+--------------+----------
---+
      VLAN/                           Encap           MAC Address       MAC Info/
Interface
```

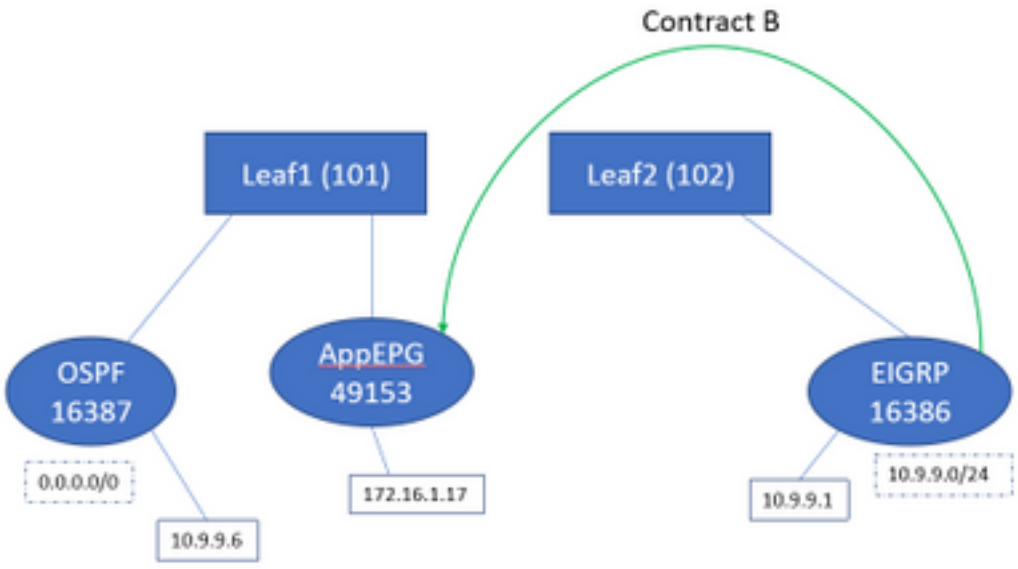
```
      Domain                            VLAN            IP Address        IP Info
+-----------------------------------+--------------+-----------------+--------------+----------
---+
48                                        vlan-2743    dcce.c15b.1e47 L
eth1/24
shparanj:eigrp-test                       vlan-2743       172.16.1.17 L
eth1/24

leaf101# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.9.9.1/32, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/128576], 05:31:49, bgp-65003, internal, tag 65003
10.9.9.6/32, ubest/mbest: 1/0
    *via 10.27.48.2, eth1/22, [110/5], 05:09:51, ospf-default, intra
10.27.47.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/0], 05:31:49, bgp-65003, internal, tag 65003
10.27.48.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.48.1, eth1/22, [1/0], 05:31:46, direct
10.27.48.1/32, ubest/mbest: 1/0, attached
    *via 10.27.48.1, eth1/22, [1/0], 05:31:46, local, local
172.16.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.34%overlay-1, [1/0], 05:27:43, static
172.16.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 172.16.1.254, vlan47, [1/0], 05:31:52, local, local



leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)


<<vsh>>  (to go into vsh propmt , type: #vsh )

leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
```

Leaf2:

```
leaf102# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
```

```
'%<string>' in via output denotes VRF <string>

10.9.9.1/32, ubest/mbest: 1/0
    *via 10.27.47.10, vlan78, [90/128576], 06:13:41, eigrp-default, internal
10.9.9.6/32, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/5], 05:20:27, bgp-65003, internal, tag 65003
10.27.47.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.47.2, vlan78, [1/0], 3d21h, direct
10.27.47.2/32, ubest/mbest: 1/0, attached
    *via 10.27.47.2, vlan78, [1/0], 3d21h, local, local
10.27.48.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/0], 05:35:06, bgp-65003, internal, tag 65003

leaf102# show zoning-rule scope 2752513 Rule ID SrcEPG DstEPG FilterID operSt Scope Action
Priority ======= ====== ====== ======== ====== ===== ====== ======== 4472 0 0 implicit enabled
2752513 deny,log any_any_any(21) 4471 0 0 implarp enabled 2752513 permit any_any_filter(17) 4470
0 15 implicit enabled 2752513 deny,log any_vrf_any_deny(22) <<vsh>> leaf102# show system
internal policy-mgr prefix | grep shparanj:eigrp-test 2752513 37 0x80000025 Up shparanj:eigrp-
test ::/0 15 False True False 2752513 37 0x25 Up shparanj:eigrp-test 0.0.0.0/0 15 False True
False 2752513 37 0x25 Up shparanj:eigrp-test 10.9.9.0/24 16386 False True False
```

Laten we contract B (huurcontract, scope vrf - filer: common:default) toevoegen



Zodra we contract B toevoegen zien we het nummer EPG voorvoegsel op blad 1 toegevoegd:

```
leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26 0x1a Up shparanj:eigrp-test 10.9.9.0/24 16386 False True False 2752513 26 0x1a Up
shparanj:eigrp-test 0.0.0.0/0 15 False True False 2752513 26 0x8000001a Up shparanj:eigrp-test
::/0 15 False True False
```

Laten we andere politiemensen bekijken:

1 contracten:

```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
```

```
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)
4604 49153 16386 default enabled 2752513 permit src_dst_any(9) 4605 16386 49153 default enabled
2752513 permit src_dst_any(9)
```

Leaf 2-contracten (blijven ongewijzigd):

```
leaf102# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4472            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4471            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4470            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
```

In dit scenario komt het verkeer binnen van ospf l3out, dat we verwachten te worden getagd met 16387 wordt getagd met 16386. Dit komt doordat het verkeer de nieuwe prefix ingang op Leaf1 bereikt.

Van 10.9.9.6 t/m punt 172.16.1.17:

```
# ping 172.16.1.17 vrf shp-ospf source 10.9.9.6 count 1000 interval 1
PING 172.16.1.17 (172.16.1.17) from 10.9.9.6: 56 data bytes
64 bytes from 172.16.1.17: icmp_seq=0 ttl=253 time=2.207 ms
64 bytes from 172.16.1.17: icmp_seq=1 ttl=253 time=1.443 ms
64 bytes from 172.16.1.17: icmp_seq=2 ttl=253 time=1.312 ms
```

Ping werkt zelfs zonder contract tussen ospf epg en app-epg. Dit komt doordat het beleid tegen eigrp-epg indruist en toegelaten wordt.

ELAM:

```
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.9.9.6
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered
module-1(DBG-elam-insel6)# report | grep sclass
      sug_lurw_vec.info.nsh_special.sclass: 0x4002
      sug_lurw_vec.info.ifabric_spine.sclass: 0x4002
      sug_lurw_vec.info.ifabric_leaf.sclass: 0x4002
#dec 0x4002
```

16386

In dit scenario werkt het verkeer uiteindelijk dankzij classificatie in een pcTag die een contract heeft met de beoogde bestemming. Als bijvoorbeeld het computerblad een apart derde blad zou zijn, dan zou ons verkeer mislukken, omdat de vermelding voor een contract alleen op het derde blad (INGress policy) of op bladzijde 102 (egress policy) zou staan.

Fabric met overlappende subnetten gedeclareerd als extern op afzonderlijke externe EPG's

In dit scenario kijken we naar beleidsconflicten en mogelijke onjuiste classificatie door overlappende of dezelfde subnetten die als extern zijn verklaard op verschillende externe EPG's.

OSPF-advertentienetwerk:

10.9.1.0/24

DHCP adverteert netwerk:

10.9.2.0/24

We beginnen met de topologie in Figuur 1, maar zonder contracten. We definiëren net 10.9.0.0/16 as 'extern Subnet voor externe EPG's' voor EPG op beide L3outs.

Zo zien de tabellen op Leaf1 en 2 eruit:

1:

```
leaf101# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.9.1.0/24, ubest/mbest: 1/0
    *via 10.27.48.2, eth1/22, [110/5], 00:01:50, ospf-default, intra
10.9.2.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/128576], 00:00:32, bgp-65003, internal, tag 65003
10.27.47.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/0], 01:54:45, bgp-65003, internal, tag 65003
10.27.48.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.48.1, eth1/22, [1/0], 1d09h, direct
10.27.48.1/32, ubest/mbest: 1/0, attached
    *via 10.27.48.1, eth1/22, [1/0], 1d09h, local, local
172.16.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.34%overlay-1, [1/0], 1d09h, static
172.16.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 172.16.1.254, vlan47, [1/0], 1d09h, local, local


leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
```

```
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)

<<vsh>>

leaf101#  show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
10.9.0.0/16  16387   False  True   False
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
```

Leaf2:

```
leaf102# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.9.1.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/5], 00:05:29, bgp-65003, internal, tag 65003
10.9.2.0/24, ubest/mbest: 1/0
    *via 10.27.47.10, vlan80, [90/128576], 00:04:10, eigrp-default, internal
10.27.47.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.47.2, vlan80, [1/0], 01:58:24, direct
10.27.47.2/32, ubest/mbest: 1/0, attached
    *via 10.27.47.2, vlan80, [1/0], 01:58:24, local, local
10.27.48.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/0], 1d09h, bgp-65003, internal, tag 65003

leaf102# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4472            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4471            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4470            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)

<<vsh>>

leaf102# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 37     0x80000025    Up     shparanj:eigrp-test
::/0   15      False  True   False
2752513 37     0x25          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 37     0x25          Up     shparanj:eigrp-test
10.9.0.0/16  16386   False  True   False
```

In deze staat, zonder contracten, zien we geen fouten op beide EPG's. Er is nog geen overlapping

in prefixes vastgesteld!

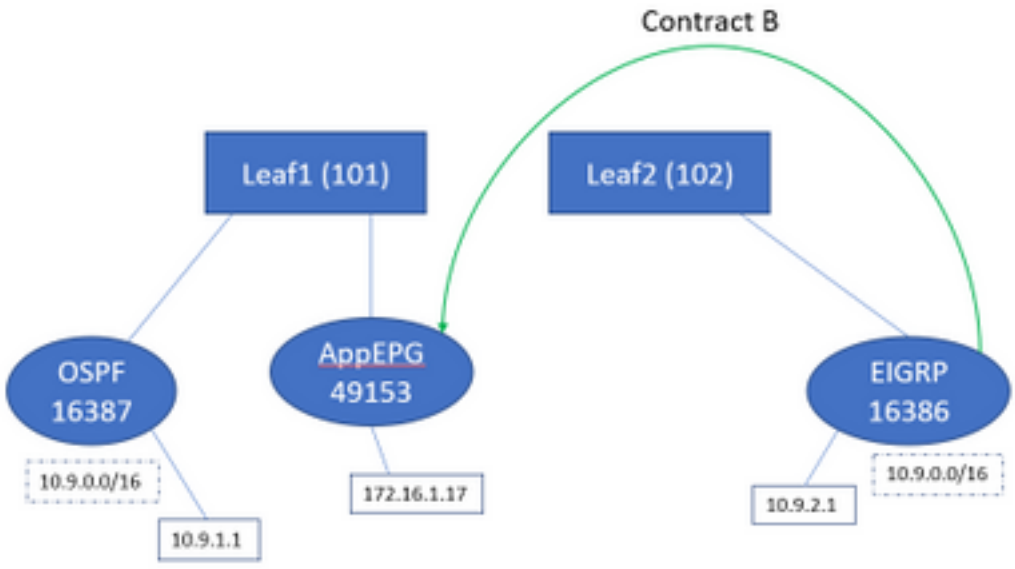
Als we contract B toevoegen zien we een fout in de app-EPG (die contract B verwerkt).

Fault Properties

General | Troubleshooting

Fault Code:	F0467
Severity:	minor
Last Transition:	2019-02-19T18:38:25.436+05:30
Lifecycle:	Raised
Affected Object:	topology/pod-1/node-101/local/svc-policyelem-id-0/cdef-[uni/tn-shparanj/brc-interEPG]/epgCont-[uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure]/fr-[uni/tn-shparanj/brc-interEPG/dirass/cons-[uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure]-any-no]/to-[uni/tn-shparanj/brc-interEPG/dirass/prov-[uni/tn-shparanj/out-eigrp-test/instP-ext-epg]-any-no]/nwissues
Description:	Fault delegate: Configuration failed for uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure due to Prefix Entry Already Used in Another EPG, debug message:
Type:	Config
Cause:	configuration-failed
Change Set:	configQual:prefix-entry-already-in-use, configSt:failed-to-apply, temporaryError:no
Created:	2019-02-19T18:35:59.015+05:30
Code:	F0467
Number of Occurrences:	1
Original Severity:	minor

Topologie:



Laten we naar de verandering in tabellen kijken:

```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
```

```
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)
4605 49153 16386 default enabled 2752513 permit src_dst_any(9) 4604 16386 49153 default enabled
2752513 permit src_dst_any(9) <<vsh>> leaf101# show system internal policy-mgr prefix | grep
shparanj:eigrp-test 2752513 26 0x1a Up shparanj:eigrp-test 10.9.0.0/16 16387 False True False
2752513 26 0x1a Up shparanj:eigrp-test 0.0.0.0/0 15 False True False 2752513 26 0x8000001a Up
shparanj:eigrp-test ::/0 15 False True False
```

Leaf2 blijft ongewijzigd.

Dit toont aan dat de zoning-regel die overeenkomt met contract B is geïnstalleerd. Maar het voorvoegsel kan niet worden toegevoegd, aangezien het reeds bestaat - gemarkeerd met OSPF EPG!

En dat is precies wat de fout ons waarschuwt, "prefix entry" dat al gebruikt wordt in een andere EPG"; de fout wordt alleen gemaakt als er een conflict is op een bepaald blad tussen beleid (zoning-regels) en de toepassing ervan. De fout wordt opgeworpen bij de consument EPG.

Als we vanaf 10.9.2.1 het verkeer starten, valt het op Leaf101 vanwege beleidsontkenning:

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

[ Tue Feb 19 19:31:33 2019 234270 usecs]: CName: shparanj:eigrp-test(VXLAN: 2752513), VlanType:
FD_VLAN, Vlan-Id: 48, SMac: 0xdccec15b1e47, DMac:0x0022bdf819ff, SIP: 172.16.1.17, DIP:
10.9.2.1, SPort: 0, DPort: 0, Src Intf: Ethernet1/24, Proto: 1, PktLen: 98 [ Tue Feb 19 19:31:31
2019 234310 usecs]: CName: shparanj:eigrp-test(VXLAN: 2752513), VlanType: FD_VLAN, Vlan-Id: 48,
SMac: 0xdccec15b1e47, DMac:0x0022bdf819ff, SIP: 172.16.1.17, DIP: 10.9.2.1, SPort: 0, DPort: 0,
Src Intf: Ethernet1/24, Proto: 1, PktLen: 98
```

Wij zien dat de antwoorden van het EP 172.16.1.17 t/m 10.9.2.1 worden geschrapt. Dit komt doordat:

- Verzoeken van 10.9.2.1 die afkomstig zijn van stoffen zijn al ingedeeld bij klasse 16386 - deze vallen onder regel ID 4604 en zijn toegestaan door
- Antwoorden van 172.16.1.17 worden gemarkeerd met klasse 16387 - dit wordt opgepikt op basis van beleidsmakers. Er is geen regel die overeenkomt met 16387 en deze wordt ontkend.

In deze situatie leidt een verkeerde classificatie ertoe dat het verkeer wordt teruggebracht, ook al lijken we de juiste configuratie te hebben (als de fout wordt genegeerd).

Fabric met 0.0.0.0/0 voorvoegsel verklaard als extern op meerdere externe EPG's

In dit scenario kijken we naar mogelijke verkeerde classificatie en onverwachte veiligheidsschendingen door de toepassing van 0.0.0.0/0-net als extern op verschillende externe EPG's.

OSPF-advertentienetwerk:

10.7.7.0/24

DHCP adverteert netwerk:

10.8.8.0/24

We beginnen met de topologie in Figuur 1, maar zonder contracten. We definiëren net 0.0.0.0/0 als 'extern netwerk voor externe EPG's' voor EPG op beide L3outs.

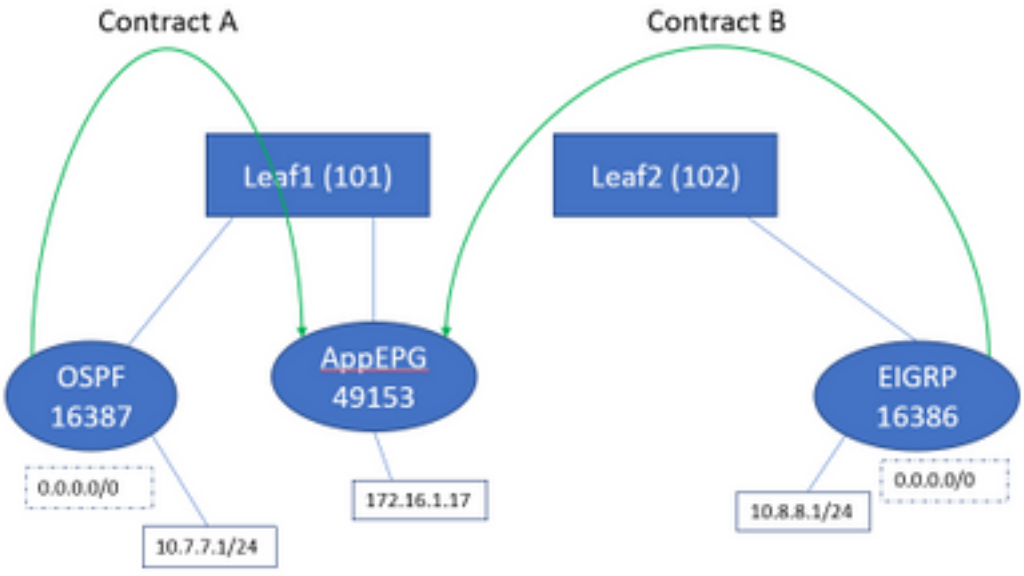
Zo zien de tabellen op Leaf1 en 2 eruit:

Leaf1:

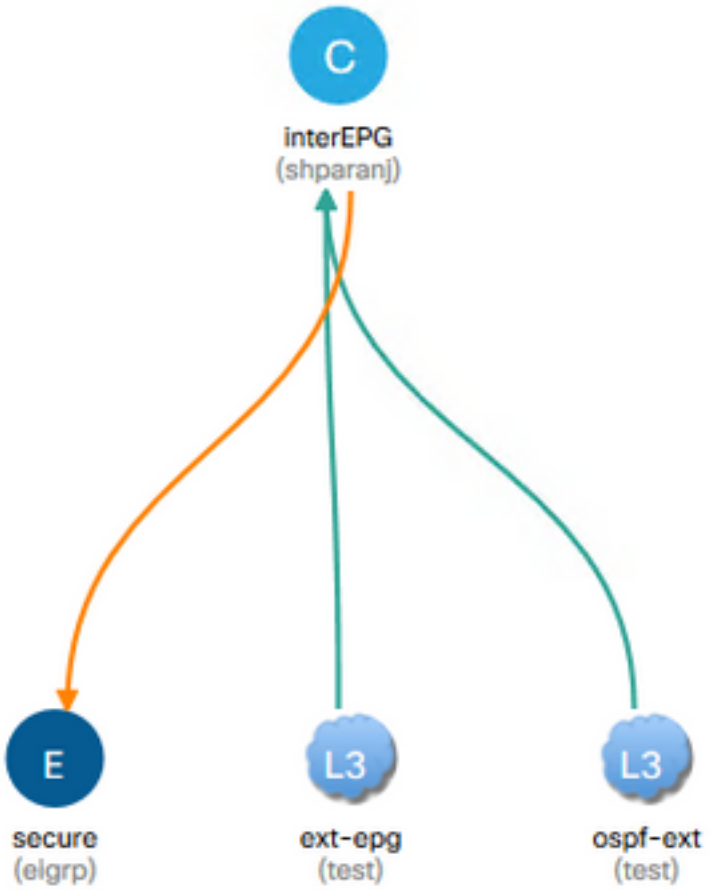
```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)

leaf101# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.7.7.0/24, ubest/mbest: 1/0
    *via 10.27.48.2, eth1/22, [110/5], 00:23:29, ospf-default, intra
10.8.8.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/128576], 00:02:30, bgp-65003, internal, tag 65003
10.27.47.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/0], 00:02:33, bgp-65003, internal, tag 65003
10.27.48.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.48.1, eth1/22, [1/0], 1d07h, direct
10.27.48.1/32, ubest/mbest: 1/0, attached
    *via 10.27.48.1, eth1/22, [1/0], 1d07h, local, local
172.16.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.34%overlay-1, [1/0], 1d07h, static
172.16.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 172.16.1.254, vlan47, [1/0], 1d07h, local, local


<<vsh>>

leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
```

Leaf2:

```
leaf102# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.7.7.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/5], 00:26:07, bgp-65003, internal, tag 65003
10.8.8.0/24, ubest/mbest: 1/0
    *via 10.27.47.10, vlan80, [90/128576], 00:05:08, eigrp-default, internal
10.27.47.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.47.2, vlan80, [1/0], 00:05:11, direct
10.27.47.2/32, ubest/mbest: 1/0, attached
    *via 10.27.47.2, vlan80, [1/0], 00:05:11, local, local
10.27.48.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/0], 1d07h, bgp-65003, internal, tag 65003


leaf102#  show zoning-rule scope 2752513
Rule ID          SrcEPG           DstEPG           FilterID         operSt           Scope
Action                                Priority
=======          ======           ======           ========         ======           =====
======                                ========
4472             0                0                implicit         enabled          2752513
deny,log                              any_any_any(21)
4471             0                0                implarp          enabled          2752513
permit                                any_any_filter(17)
4470             0                15               implicit         enabled          2752513
deny,log                              any_vrf_any_deny(22)

<<vsh>>

leaf102# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 37     0x80000025    Up     shparanj:eigrp-test
::/0   15      False  True   False
2752513 37     0x25          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
```



Als we beide contracten A & B toevoegen, zien we nog steeds geen fouten.



Laten we eens kijken naar de ranglijsten op Leafs:

Leaf1:

```
leaf101# show zoning-rule scope 2752513
Rule ID          SrcEPG           DstEPG           FilterID         operSt           Scope
Action                                Priority
=======          ======           ======           ========         ======           =====
======                                ========
4173             0                0                implicit         enabled          2752513
deny,log                              any_any_any(21)
4174             0                0                implarp          enabled          2752513
permit                                any_any_filter(17)
4175             0                15               implicit         enabled          2752513
deny,log                              any_vrf_any_deny(22)
4207             0                32771            implicit         enabled          2752513
permit                                any_dest_any(16)
4616             49153            15               default          enabled          2752513
permit                                src_dst_any(9)
4617             32770            49153            default          enabled          2752513
permit                                src_dst_any(9)

<<vsh>>
leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test 2752513 26 0x1a Up
shparanj:eigrp-test 0.0.0.0/0 15 False True False 2752513 26 0x8000001a Up shparanj:eigrp-test
::/0 15 False True False
```

Tabellen op Leaf2 blijven ongewijzigd.

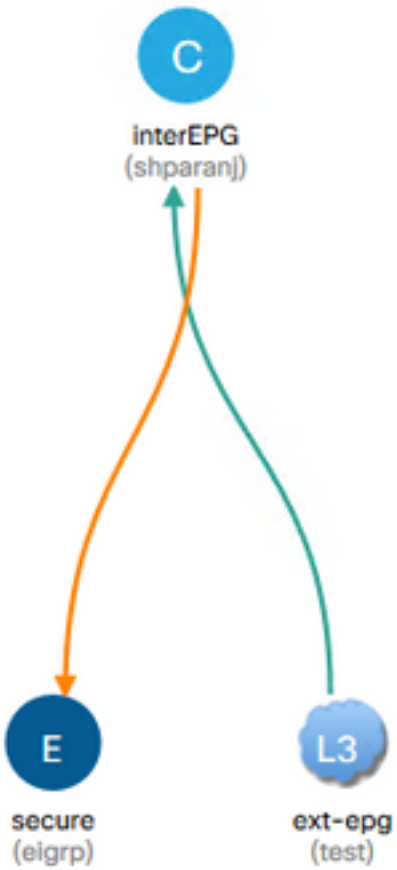
We zien geen fouten omdat er geen beleidsconflict is vanuit het perspectief van elk blad. **De regel-ID's die worden toegevoegd bij gebruik van 0.0.0.0/0 als externe EPG zijn speciaal.**

- **Het verkeer dat vanuit zijn respectievelijke EPG naar een van beide grenzen leaf komt, is gemarkeerd met sclass 32770 - dit is de pcTag van VRF.**
- Studie op dit verkeer is 49153 - de pcTag van de app-EPG.
- **Het retourverkeer van app-EPG heeft een klasse van 15**

ELAM op Leaf1:

```
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.7.7.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered

module-1(DBG-elam-insel6)# report | grep sclass
      sug_lurw_vec.info.nsh_special.sclass: 0x8002
      sug_lurw_vec.info.ifabric_spine.sclass: 0x8002
      sug_lurw_vec.info.ifabric_leaf.sclass: 0x8002
module-1(DBG-elam-insel6)# dec 0x8002
32770

module-1(DBG-elam-insel6)# reset
module-1(DBG-elam-insel6)# set outer ipv4 dst_ip 10.7.7.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Armed

module-1(DBG-elam-insel6)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered

module-1(DBG-elam-insel6)# report | grep dclass
      sug_lurw_vec.info.nsh_special.dclass: 0xF
      sug_lurw_vec.info.ifabric_leaf.dclass: 0xF
```

Zelfs als we contract A schrappen, kan 10.7.7.1 de communicatie met 172.16.1.17 voortzetten.



Dit komt doordat de schrapping van contract A geen wijzigingen van de zoning-regels op Leaf1 tot gevolg heeft.

```
leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
leaf101# exit
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)
4616            49153           15              default         enabled         2752513
permit                              src_dst_any(9)
4617            32770           49153           default         enabled         2752513
permit                              src_dst_any(9)
```

Verder blijft het verkeer dat binnenkomt op OSPF externe EPG gelabeld zijn met VRF pcTag, aangezien de EPG nog steeds 0.0.0.0/0 als extern net gemarkeerd heeft.

Dit leidt tot een schending van het veiligheidsbeleid, d.w.z. twee EPG's die zonder contract in een gedwongen VRF kunnen communiceren.

Meer informatie

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/ACI_Best_Practices/b_ACI_Best_Practices/b_ACI_Best_Practices_chapter_010010.html