Chevauchement de sous-réseaux sur les couches 3 dans l'ACI Cisco

Contenu

Introduction

L'infrastructure axée sur les applications (ACI) de Cisco facilite la communication entre les locataires internes et les réseaux routés externes, via L3outs (couche 3 sortie). Ces sorties de couche 3 peuvent également être configurées pour avoir un ou plusieurs groupes de terminaux (EPG). Pour que l'ACI sache comment classer le trafic entrant, en tant qu'EPG de L3out, des sous-réseaux explicites doivent être définis avec certains indicateurs activés. Cet article vise à mettre en lumière la mise en oeuvre matérielle des EPG L3out dans le contexte de l'application de politique basée sur des contrats. Nous examinerons en particulier l'indicateur « sous-réseaux externes pour les groupes de terminaux externes » et les conséquences inattendues de la déclaration des préfixes chevauchants comme « externes » sur des groupes de terminaux distincts.

Concept

La règle générale est la suivante : lors du déploiement de couches 3, les groupes de terminaux distincts dans la même instance VRF (Virtual Routing and Forwarding) ne doivent pas avoir de sous-réseaux chevauchants marqués comme 'sous-réseau externe pour les groupes de terminaux externes'. Cela signifie également que le trafic provenant d'un sous-réseau spécifique ne doit pas être acheminé par des groupes de terminaux différents. Cela peut entraîner une classification inattendue du trafic basée sur la correspondance de préfixe la plus longue par rapport aux sous-réseaux déclarés contre les groupes de terminaux indépendants. Examinons quelques scénarios pour comprendre cela en détail

Conditions préalables

Compréhension de base de l'ACI : L3outs, contrats et application des politiques. Quelques termes utiles sont brièvement expliqués ci-dessous, des informations plus détaillées à ce sujet se trouvent au-delà de la portée de ce document :

pcTag : L'ACI classe le trafic dans pcTags et il s'agit de représentations internes des groupes de terminaux. Ces valeurs, par défaut, ont une portée VRF, c'est-à-dire qu'elles sont uniques dans un VRF, mais peuvent être réutilisées sur des VRF. Cependant, si un EPG a un contrat avec un autre EPG dans un VRF/locataire différent , alors la valeur pcTag a une portée globale - c'est-à-dire que vous ne trouverez aucun autre EPG dans ACI avec le même pcTag.

ELAM : Module d'analyse logique intégré. Cet outil est utilisé pour capturer un paquet sur ASIC en fonction de filtres et pour vérifier les en-têtes/indicateurs définis sur le paquet. Cet outil aide également à comprendre les recherches/logiques effectuées par le matériel

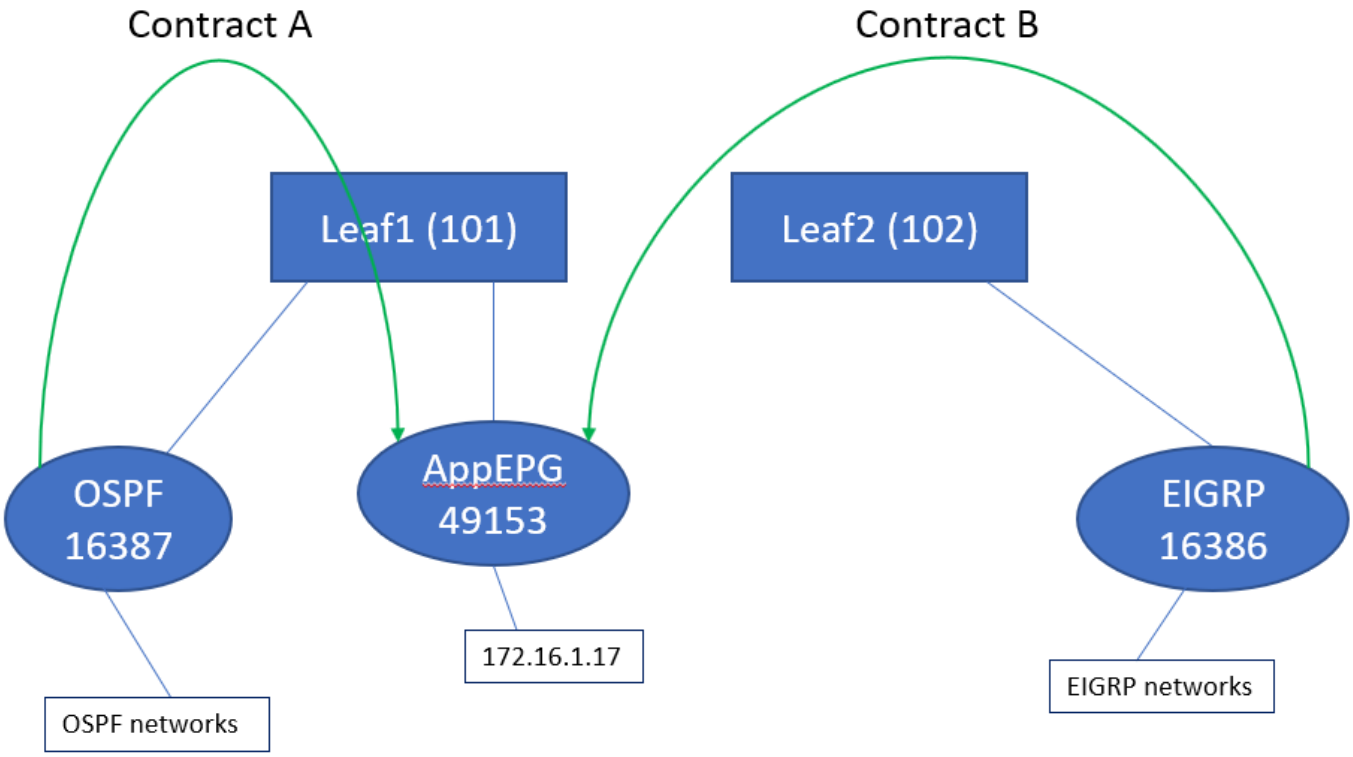
sclass/dclass : lorsque le trafic arrive sur une feuille, en fonction de la direction de l'application des politiques et des connaissances de préfixe disponibles localement, la feuille marque le trafic source et de destination dans les groupes de terminaux. dans les captures ELAM, cette valeur est considérée comme sclass et dclass respectivement

règle de zonage : il s'agit de représentations internes de contrats et sont similaires aux lignes d'une liste de contrôle d'accès. Les valeurs SrcEpg et DstEpg doivent correspondre à sclass/dclass pour que le trafic atteigne une règle donnée et soit autorisé. Par défaut dans un VRF appliqué, il y a un refus implicite comme dernière ligne , de sorte que tout trafic ne correspondant pas à une certaine règle frappera le refus implicite et sera abandonné.

Configuration et topologie

Deux feuilles - 101 et 102, modèle : N9K-C93180YC-EX

- Version 3.2(4e)
- Un VRF utilisé - Préférence d'application des politiques : AppliquéDirection de l'application des politiques : Entrée.VNID VRF (VxLAN Network Identifier) : 2752513 ; pcTag : 32770
- L3out dans Leaf1 (101) - Protocole : Protocole OSPF (Open Shortest Path First)Utilisateur de l'interface L3 pour le voisinage- eth1/22 (10.27.48.1/24)EPG pcTag externe : 16387
- EPG application sur Leaf101 Trunk - eth1/24 pcTag : 49153Point de terminaison IP : 172.16.1.17 Passerelle : 172.16.1.254/24 - déployé sur le domaine de pont (BD) BD a pcTag 32771
- L3out sur Leaf2 (202) - Protocole : Enhanced Interior Gateway Routing Protocol (EIGRP)SVI utilisé pour le voisinage avec Path 1/16 - vlan 2747 (10.27.47.1/24)EPG pcTag externe : 163869



Scénarios

Trafic provenant de sous-réseaux qui se chevauchent

Dans ce scénario, nous examinons les erreurs potentielles de classification lorsque le trafic provient de sous-réseaux qui se chevauchent (du point de vue de l'ACI)

Le protocole OSPF annonce :

10.9.9.6/32

EIGRP annonce :

10.9.9.1/32

Nous commençons par la topologie du schéma 1, mais sans aucun contrat. Pour EPG sur OSPF, nous définissons le sous-réseau 0.0.0.0/0 comme 'sous-réseau externe pour les EPG externes' et 10.9.9.0/24 avec le même indicateur pour l'EPG EIGRP. Voici à quoi ressemblent les tableaux des feuilles 1 et 2 :

Feuille1 :

```
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
+------------------------------------+---------------+-----------------+--------------+----------
---+
```

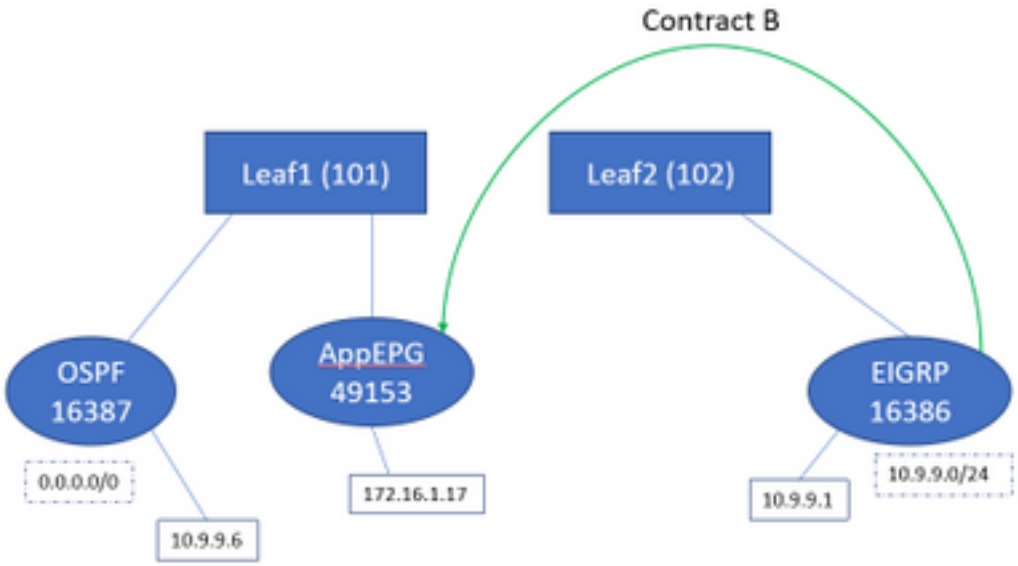
```
      VLAN/                            Encap           MAC Address       MAC Info/
Interface
      Domain                           VLAN            IP Address        IP Info
+----------------------------------+---------------+-----------------+--------------+----------
---+
48                                        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
```

Feuille 2 :

```
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
```

Ajoutons le contrat B (contrat dans le locataire, étendue vrf - filer : common:default)



Dès que nous ajoutons le contrat B, le préfixe EPG eigrp est ajouté sur leaf1 :

```
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
```

Examinons d'autres stratégies :

Contrats Leaf 1 :

```
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)
```

Contrats Leaf 2 (inchangés) :

```
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)
```

Dans ce scénario, le trafic entrant en provenance de ospf l3out , avec lequel nous prévoyons d'être balisé 16387 est marqué avec 16386 à la place. En effet, le trafic atteint la nouvelle entrée de préfixe sur Leaf1.

Envoyez une requête ping de 10.9.9.6 au point de terminaison 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
```

La commande ping fonctionne même sans contrat entre ospf epg et app-epg. Ceci est dû au fait qu'il s'oppose à la stratégie pour eigrp-epg et est autorisé.

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
```

Dans ce scénario, le trafic finit par fonctionner en raison d'une classification dans un pcTag qui a un contrat avec la destination prévue. Cependant, si, par exemple, la feuille de calcul était une 3ème feuille séparée, notre trafic échouerait - car l'entrée de contrat n'existerait que sur la troisième feuille (politique d'entrée) ou sur leaf102 (politique de sortie).

Fabric avec des sous-réseaux qui se chevauchent déclarés comme externes sur des groupes de terminaux externes distincts

Dans ce scénario, nous examinons les conflits de politiques et les erreurs potentielles de classification dues au chevauchement ou aux mêmes sous-réseaux déclarés comme externes sur différents groupes de terminaux externes.

OSPF annonce le réseau :

10.9.1.0/24

EIGRP annonce le réseau :

10.9.2.0/24

Nous commençons par la topologie du schéma 1, mais sans aucun contrat. Nous définissons le sous-réseau 10.9.0.0/16 as 'sous-réseau externe pour les groupes de terminaux externes' pour les groupes de terminaux sur les deux sorties L3.

Voici à quoi ressemblent les tableaux des feuilles 1 et 2 :

Feuille 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
```

Feuille 2 :

```
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
```

Dans cet état, sans aucun contrat, nous ne voyons aucune défaillance sur les deux groupes de terminaux. Aucun chevauchement de préfixes n'a encore été détecté !

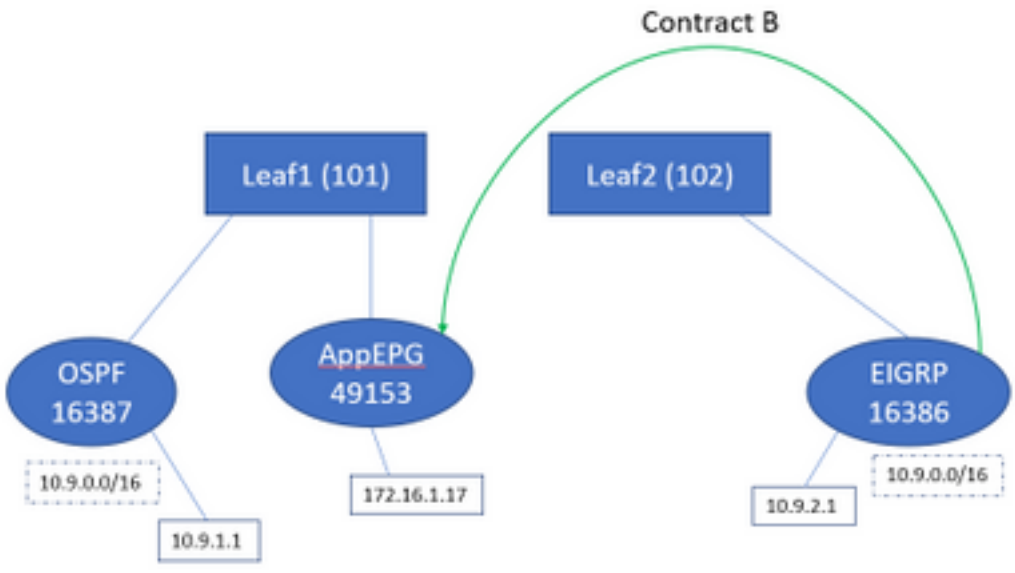
Si nous ajoutons le contrat B, nous voyons une erreur dans l'application-EPG (qui consomme le contrat B).

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:



Examinons le changement dans les tableaux :

```
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 reste inchangé.

Ceci nous montre que la règle de zonage correspondant au contrat B est installée. Cependant, le préfixe ne peut pas être ajouté, car il existe déjà - marqué par rapport à l'EPG OSPF !

Et c'est exactement ce que la faute nous avertit, « entrée de préfixe déjà utilisée dans un autre EPG » - la faute n'est soulevée que lorsqu'il y a un conflit sur une feuille particulière entre la politique (règles de zonage) et son application. La faute est soulevée sur l'EPG consommateur.

Si nous démarrons le trafic à partir de 10.9.2.1 , il est abandonné sur Leaf101 en raison du refus de stratégie :

```
# 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
```

Nous constatons que les réponses de EP 172.16.1.17 à 10.9.2.1 sont supprimées. En effet :

- Les demandes de 10.9.2.1 provenant du tissu sont déjà classées avec la classe 16386 - elles portent l'ID de règle 4604 et sont autorisées à passer
- Les réponses de 172.16.1.17 sont marquées avec la classe 16387 - cette valeur est récupérée en fonction des règles de préfixe de policy-mgr. Il n'y a pas de règle correspondant à 16387 et ceux-ci sont refusés.

Dans cette situation, une mauvaise classification entraîne l'abandon du trafic même si nous semblons avoir la bonne configuration en place (si l'erreur est ignorée).

Fabric avec préfixe 0.0.0.0/0 déclaré comme externe sur plusieurs groupes de terminaux externes

Dans ce scénario, nous examinons les erreurs potentielles de classification et les violations de sécurité inattendues dues dues à l'application du sous-réseau 0.0.0.0/0 comme externe sur différents groupes de terminaux externes.

OSPF annonce le réseau :

10.7.7.0/24

EIGRP annonce le réseau :

10.8.8.0/24

Nous commençons par la topologie du schéma 1, mais sans aucun contrat. Nous définissons le sous-réseau 0.0.0.0/0 comme 'sous-réseau externe pour les groupes de terminaux externes' pour les groupes de terminaux sur les deux sorties L3.

Voici à quoi ressemblent les tableaux des feuilles 1 et 2 :

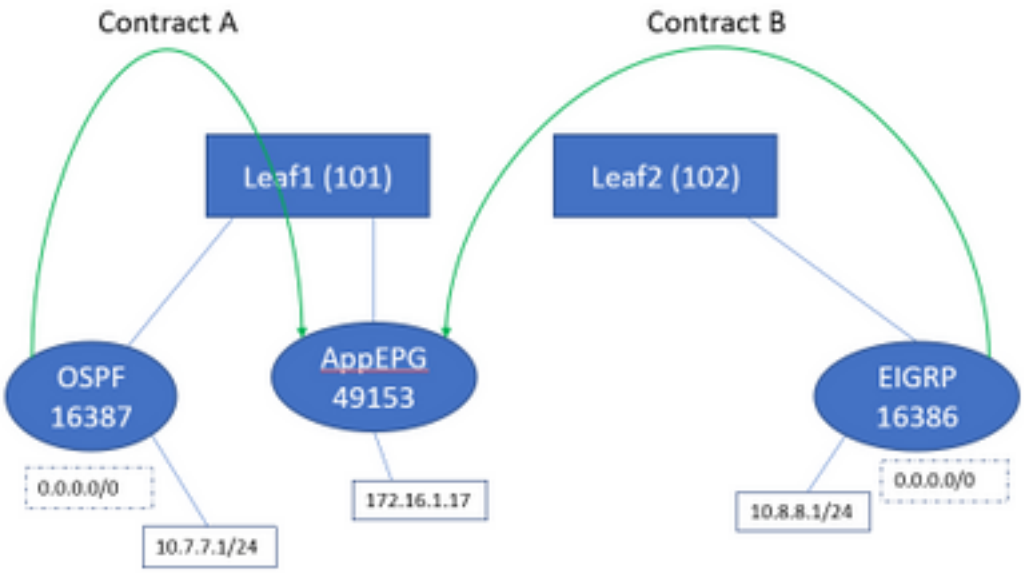
Feuille1 :

```
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
```

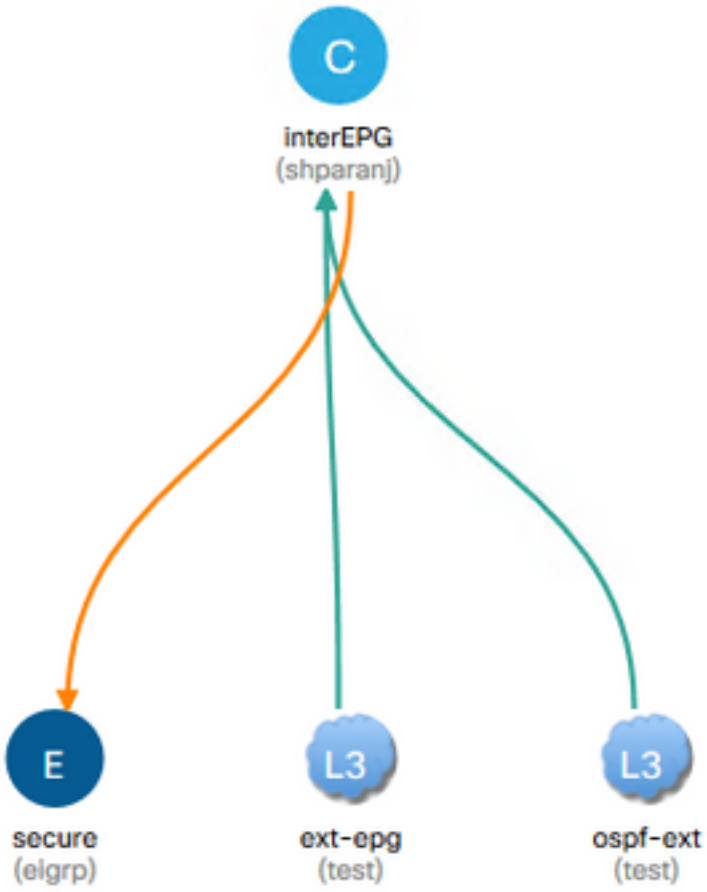
```
::/0   15      False  True   False
```

Feuille 2 :

```
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
```



Si nous ajoutons les deux contrats A et B, nous ne voyons toujours pas de défauts.



Regardons les tables des feuilles :

Feuille1 :

```
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
```

Les tableaux de Leaf2 restent inchangés.

Nous ne voyons aucun défaut, car il n'y a en fait aucun conflit de politique du point de vue de chaque feuille. **Les ID de règle ajoutés lors de l'utilisation de 0.0.0.0/0 comme EPG externe sont spéciaux.**

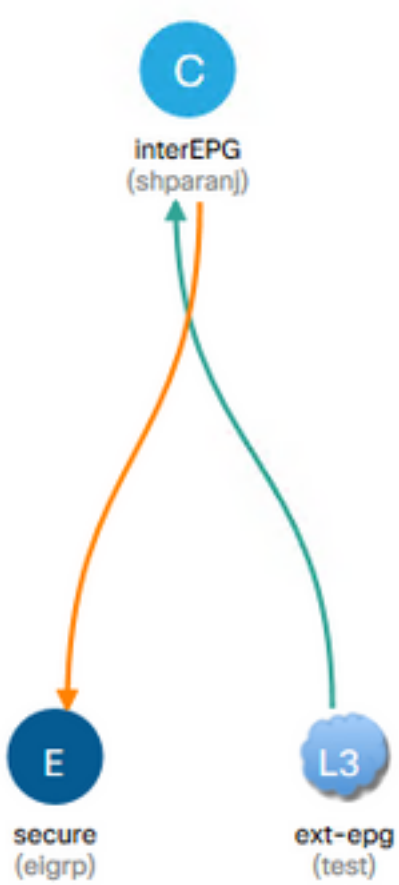
- **Le trafic entrant dans l'une ou l'autre des feuilles de périphérie de son EPG respectif est marqué avec la classe 32770 - il s'agit de l'pcTag du VRF.**
- dclass sur ce trafic est 49153 - le pcTag de l'app-EPG.
- **Le trafic de retour de app-EPG a la classe 15**

ELAM sur 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
```

Même si nous supprimons le contrat A, 10.7.7.1 peut continuer à communiquer avec 172.16.1.17.



En effet, la suppression du contrat A n'entraîne aucune modification des règles de zonage sur Leaf1.

```
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)
```

De plus, le trafic entrant sur le groupe de terminaux externe OSPF continue d'être étiqueté avec le pcTag VRF, car le groupe de terminaux a toujours 0.0.0.0/0 marqué comme sous-réseau externe.

Cela entraîne une violation de la stratégie de sécurité, c'est-à-dire deux groupes de terminaux capables de communiquer sans contrat dans un VRF forcé.

Lecture ultérieure

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