Subnet sovrapposte su L3out in Cisco ACI

Sommario

Introduzione

L'ACI (Application Centric Infrastructure) di Cisco semplifica la comunicazione tra i tenant interni e le reti con routing esterno, tramite L3outs (layer 3 out). È inoltre possibile configurare gli output L3 in modo che dispongano di uno o più gruppi di endpoint (EPG, End Point Group). Affinché ACI sappia come classificare il traffico in entrata, come EPG di L3out, è necessario definire subnet esplicite con determinati flag abilitati. Questo articolo mira a fare luce sull'implementazione hardware di L3out EPG nel contesto dell'applicazione basata su contratto. In particolare, esamineremo il flag 'subnet esterne per EPG esterni' e le conseguenze inaspettate della dichiarazione di prefissi sovrapposti come 'esterni' su EPG separati.

Concetto

La regola pratica è: quando si distribuiscono l3out, gli EPG distinti nella stessa istanza VRF (Virtual Routing and Forwarding) non devono avere subnet sovrapposte contrassegnate come "subnet esterna per EPG esterni". Ciò significa anche che il traffico proveniente da una subnet specifica non deve arrivare attraverso EPG diversi. Ciò può causare una classificazione imprevista del traffico basata sulla corrispondenza del prefisso più lungo rispetto alle subnet dichiarate rispetto a EPG non correlati. Esaminiamo alcuni scenari per comprenderne i dettagli

Prerequisiti

Conoscenze base di ACI: L3out, contratti e applicazione delle policy. Di seguito vengono brevemente spiegati alcuni termini utili; informazioni più dettagliate al riguardo esulano dalle finalità del presente documento:

Tag PC: ACI classifica il traffico in pcTags e queste sono rappresentazioni interne di EPG. Per impostazione predefinita, questi valori hanno un ambito VRF, ovvero sono univoci all'interno di un VRF, ma possono essere riutilizzati tra VRF. Tuttavia, se un EPG ha un contratto con un altro EPG in un VRF/tenant diverso, il valore pcTag ha un ambito globale, ovvero non è possibile trovare altri EPG in ACI con lo stesso pcTag.

ELAM: Modulo Logic Analyzer incorporato. Questo strumento viene usato per acquisire un

pacchetto su ASIC in base ai filtri e per controllare le intestazioni/flag impostati sul pacchetto. Questo strumento consente inoltre di comprendere le ricerche e la logica eseguite da

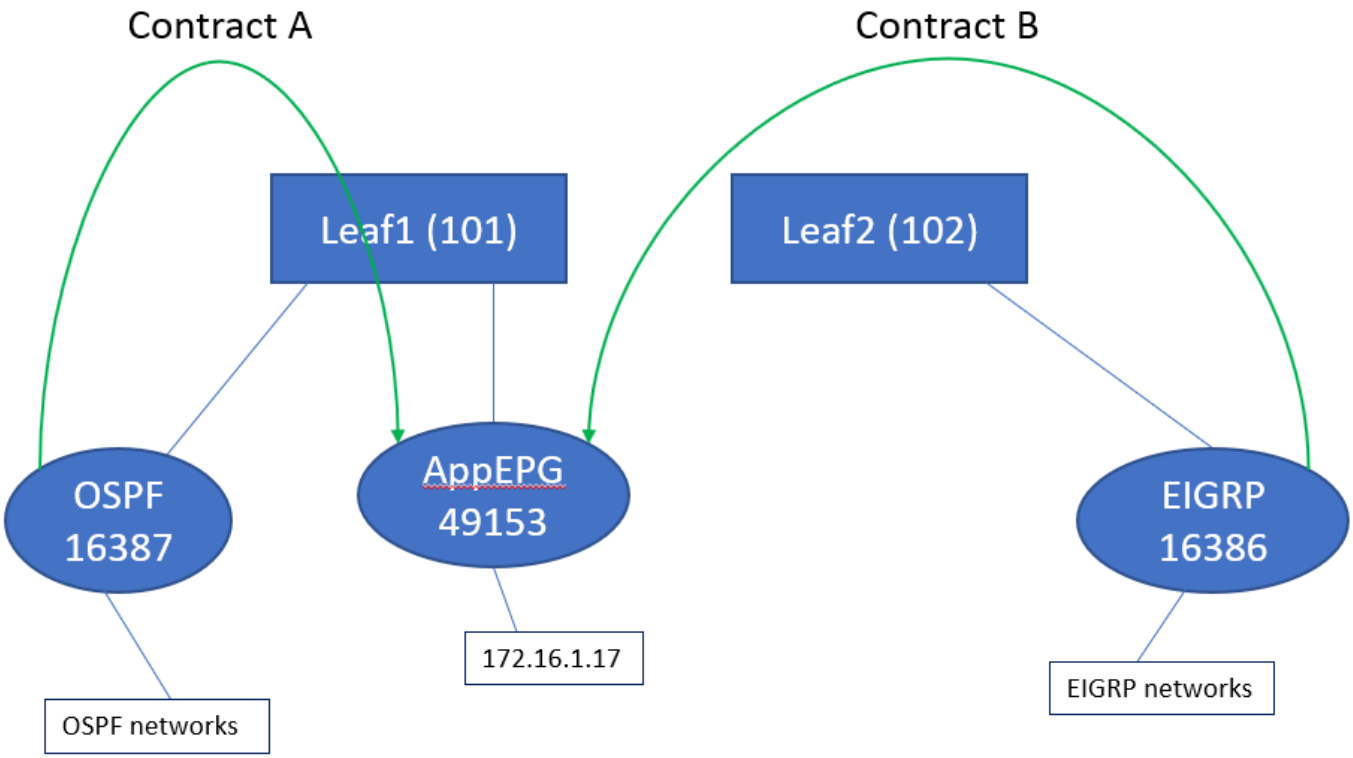
sclass/dclass: quando il traffico arriva a una foglia, in base alla direzione dell'applicazione delle policy e alla conoscenza del prefisso disponibile localmente, la foglia contrassegnerà il traffico di origine e di destinazione negli EPG - nelle acquisizioni ELAM questo sarà visto rispettivamente come classe e dclass

regola di zoning: queste sono rappresentazioni interne dei contratti e sono simili alle righe di un ACL. Affinché il traffico raggiunga una determinata regola ed sia consentito, i valori SrcEpg e DstEpg devono corrispondere a sclass/dclass. Per impostazione predefinita, in un file vrf imposto esiste un rifiuto implicito come ultima riga, quindi il traffico che non corrisponde a una determinata regola verrà rifiutato in modo implicito e verrà eliminato.

Impostazione e topologia

Two leafs - 101 e 102 , modello: N9K-C93180YC-EX

- Versione 3.2(4e)
- Un VRF utilizzato: Preferenza applicazione criterio: ApplicatoDirezione applicazione criteri: In ingresso.VRF VNID(VxLAN Network Identifier): 2752513 ; pcTag: 32770
- L3out in Foglia1 (101) - Protocollo: OSPF (Open Shortest Path First)Utente interfaccia L3 per relazioni - eth1/22 (10.27.48.1/24)pcTag EPG esterno: 16387
- Applicazione EPG su Leaf101 Trunk - eth1/24 Tag PC: 49153Endpoint IP: 172.16.1.17 Gateway: 172.16.1.254/24 - distribuito su Bridge Domain (BD) BD con pcTag 32771
- L3out su Leaf2 (202) - Protocollo: Protocollo EIGRP (Enhanced Interior Gateway Routing Protocol)SVI utilizzato per il collegamento con il percorso 1/16 - vlan 2747 (10.27.47.1/24)pcTag EPG esterno: 163869



Scenari

Traffico originato da subnet sovrapposte

In questo scenario viene presa in considerazione la potenziale mancata classificazione quando il traffico proviene da subnet sovrapposte (dal punto di vista di ACI)

OSPF annuncia:

10.9.9.6/32

EIGRP annuncia:

10.9.9.1/32

Si inizia con la topologia del Diagramma 1, ma senza alcun contratto. Per EPG su OSPF, la subnet 0.0.0.0/0 viene definita come 'subnet esterna per EPG esterni' e la subnet 10.9.9.0/24 viene definita come 'subnet esterna per EPG esterni'. Ecco come sono le tabelle di Foglia 1 e Foglia 2:

Foglia 1:

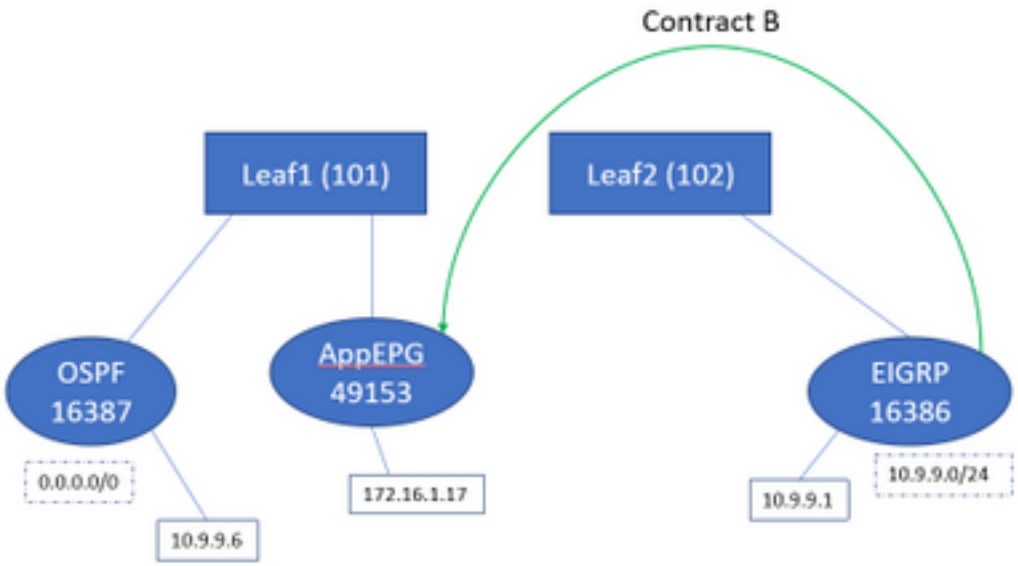
```
leaf101# show end int eth1/24
Legend:
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       L - local
+------------------------------------+--------------+-----------------+--------------+----------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

Foglia2:

```
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
```

Aggiungere il contratto B (contratto in tenant, ambito vrf - filtro: comune:predefinito)



Non appena si aggiunge il contratto B, sul foglio 1 viene aggiunto il prefisso EPG eigrp:

```
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
```

Esaminiamo altre politiche:

Contratti foglia 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)
```

Contratti foglia 2 (rimangono invariati):

```
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 questo scenario, il traffico proveniente da ospf l3out dovrebbe essere contrassegnato con 16387 viene invece etichettato con 16386. Infatti il traffico raggiunge il nuovo prefisso in Foglia1.

Eseguire il ping tra il punto 10.9.9.6 e il punto finale 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
```

Il ping funziona anche senza un contratto tra ospf epg e app-epg. Ciò perché viola i criteri per eigrp-epg e viene autorizzato.

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 questo scenario, il traffico finisce per funzionare a causa della classificazione in un pcTag che ha un contratto con la destinazione prevista. Tuttavia, se, ad esempio, la foglia di calcolo fosse una terza foglia separata, il nostro traffico fallirebbe, in quanto la voce per il contratto esisterebbe solo sulla terza foglia (politica in entrata) o su foglia102 (politica in uscita).

Fabric con subnet sovrapposte dichiarate come esterne su EPG esterni separati

In questo scenario vengono esaminati i conflitti di policy e le possibili classificazioni errate dovute alla sovrapposizione o alla presenza di subnet dichiarate esterne su diversi EPG esterni.

OSPF annuncia la rete:

10.9.1.0/24

EIGRP annuncia la rete:

10.9.2.0/24

Si inizia con la topologia del Diagramma 1, ma senza alcun contratto. La subnet 10.9.0.0/16 as 'subnet esterna per EPG esterni' viene definita per EPG su entrambi gli output L3out.

Ecco come sono le tabelle di Foglia 1 e Foglia 2:

Foglia 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
```

Foglia2:

```
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 questo stato, senza alcun contratto, non vediamo difetti né per gli EPG né per gli EPG. Non è stata ancora rilevata alcuna sovrapposizione nei prefissi.

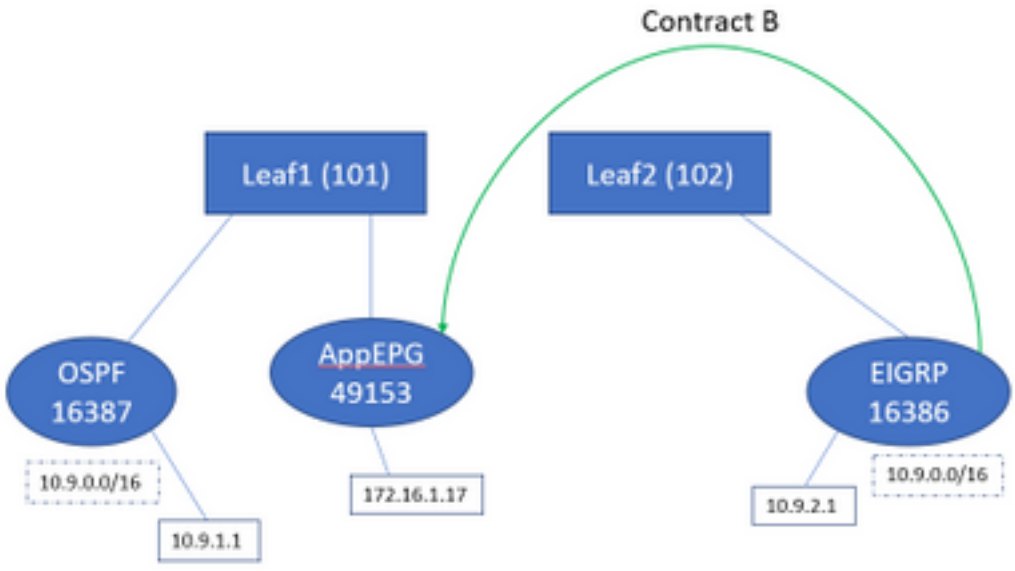
Se si aggiunge il contratto B, viene visualizzato un errore nell'app-EPG (che consuma il contratto B).

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

Topologia:



Di seguito vengono illustrate le modifiche apportate alle tabelle:

```
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 rimane invariato.

Ciò dimostra che è installata la regola di suddivisione in zone corrispondente al contratto B. Non è tuttavia possibile aggiungere il prefisso, poiché esiste già, contrassegnato con OSPF EPG.

E questo è esattamente ciò che la colpa ci avverte, "voce di prefisso già utilizzato in un altro EPG" - la colpa è sollevata solo quando c'è un conflitto su una particolare foglia tra la politica (zoning-rules) e la sua applicazione. Il difetto viene sollevato nei confronti del consumatore EPG.

Se iniziamo il traffico da 10.9.2.1 , esso viene scartato su Leaf101 a causa del rifiuto della policy:

```
# 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
```

Si constata che le risposte del PE da 172.16.1.17 a 10.9.2.1 sono state ritirate. Ciò è dovuto al fatto che:

- Le richieste da 10.9.2.1 provenienti dalla struttura sono già classificate con la classe 16386. Hanno raggiunto l'ID regola 4604 e sono consentite tramite
- Le risposte da 172.16.1.17 vengono contrassegnate con dclass 16387 - viene selezionato in base alle regole del prefisso di policy-mgr. Non c'è regola corrispondente a 16387 e queste sono negate.

In questa situazione, una classificazione errata causa la perdita del traffico anche se sembra che la configurazione sia corretta (se l'errore viene ignorato).

Fabric con prefisso 0.0.0.0/0 dichiarato esterno su più EPG esterni

In questo scenario vengono esaminate le possibili classificazioni errate e le violazioni impreviste della sicurezza dovute all'applicazione della subnet 0.0.0.0/0 come esterna su diversi EPG esterni.

OSPF annuncia la rete:

10.7.7.0/24

EIGRP annuncia la rete:

10.8.8.0/24

Si inizia con la topologia del Diagramma 1, ma senza alcun contratto. La subnet 0.0.0.0/0 viene

definita come 'subnet esterna per EPG esterni' per EPG su entrambi gli output L3out.

Ecco come sono le tabelle di Foglia 1 e Foglia 2:

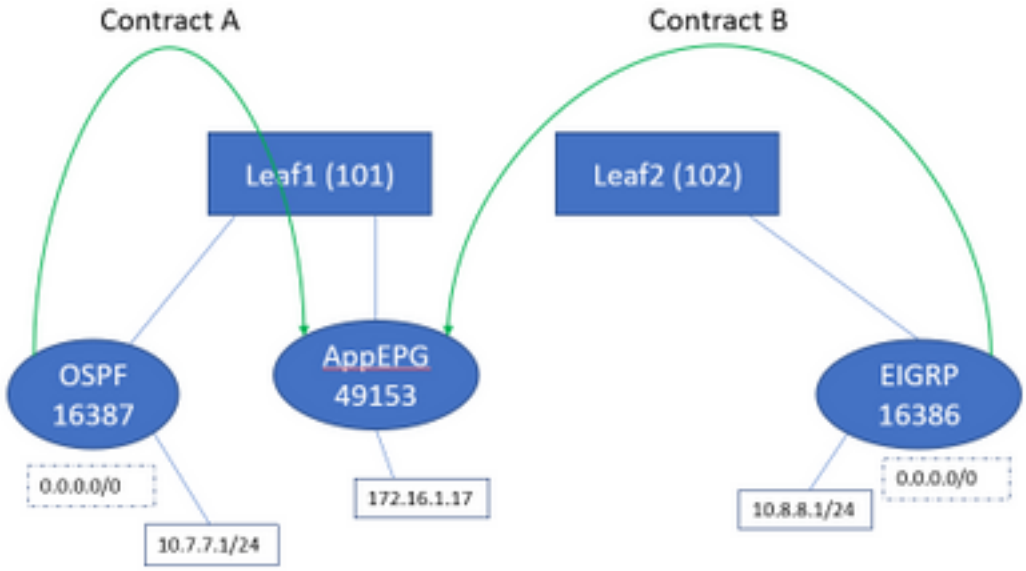
Foglia 1:

```
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)

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
```

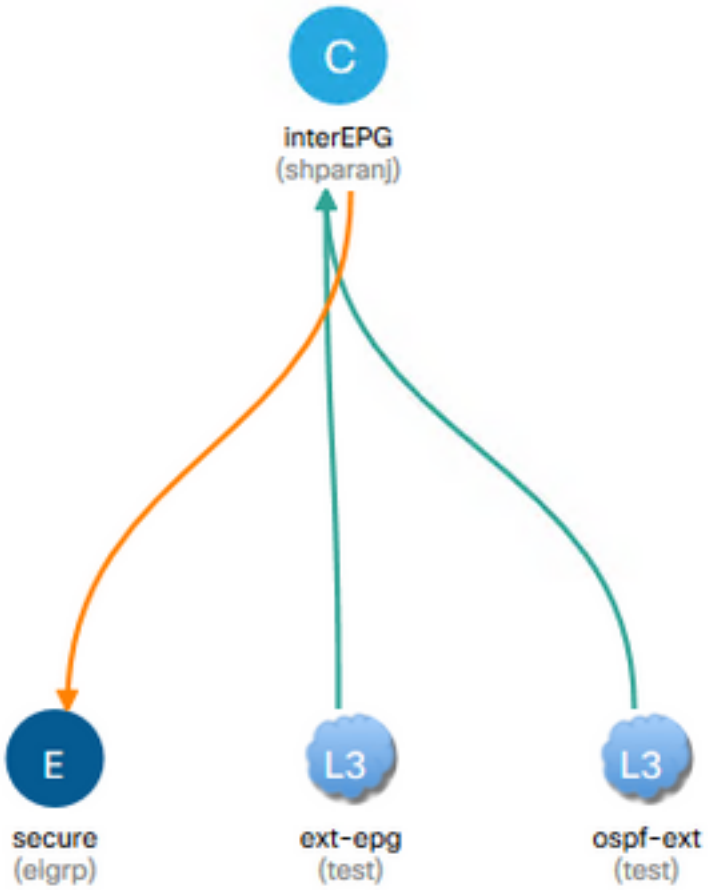
Foglia2:

```
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
```



Se aggiungiamo entrambi i contratti A e B, non vediamo ancora alcun difetto.



Diamo un'occhiata alle tabelle sulle foglie:

Foglia 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)
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
```

Le tabelle in Foglia2 rimangono invariate.

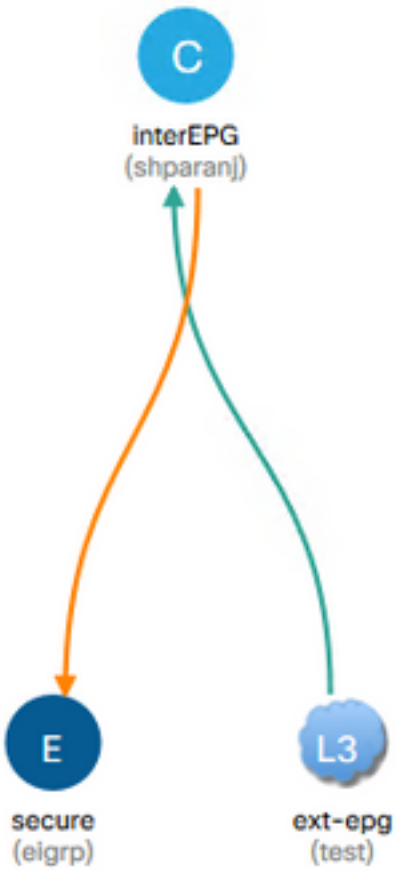
Non vediamo alcun difetto perché in realtà non c'è alcun conflitto politico dal punto di vista di ciascuna foglia. **Gli ID di regola aggiunti quando si utilizza 0.0.0.0/0 come EPG esterno sono speciali.**

- **Il traffico che arriva a una delle due foglie di confine dal rispettivo EPG è contrassegnato con la classe 32770 - questo è il pcTag VRF.**
- dclass su questo traffico è 49153 - l'app-EPG pcTag.
- **Il traffico di ritorno da app-EPG ha dclass di 15**

ELAM su 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
```

Anche se si rimuove il contratto A, la versione 10.7.7.1 può continuare a comunicare con la versione 172.16.1.17.



Ciò è dovuto al fatto che la rimozione del Contratto A non comporta alcuna modifica alle regole di zoning su Foglia1.

```
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)
```

Inoltre, il traffico in arrivo su EPG esterno OSPF continua ad essere contrassegnato con VRF pcTag, in quanto EPG ha ancora 0.0.0.0/0 contrassegnato come subnet esterna.

Ciò determina una violazione della politica di sicurezza, ossia due EPG in grado di comunicare senza un contratto in un VRF imposto.

Ulteriori letture

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