Sobreposição de sub-redes em L3outs na Cisco ACI

Contents

Introduction

A ACI (Application Centric Infrastructure, Infraestrutura Centrada em Aplicações) da Cisco facilita a comunicação entre usuários internos e redes roteadas externas, através de L3outs (saída da Camada 3). Tais L3outs também podem ser configurados para ter um ou mais EPGs (End Point Groups, grupos de pontos finais). Para que a ACI saiba como classificar o tráfego que chega, como um EPG da L3out, sub-redes explícitas precisam ser definidas com determinados flags ativados. Este artigo tem como objetivo esclarecer a implementação de hardware dos EPGs L3out no contexto da aplicação de política baseada em contrato. Exploraremos especificamente a bandeira 'sub-redes externas para EPGs externos' e as consequências inesperadas de declarar prefixos sobrepostos como 'externos' em EPGs separados.

Conceito

A regra geral é: ao implantar L3outs, EPGs separados na mesma instância de Virtual Routing and Forwarding (VRF) não devem ter sub-redes sobrepostas marcadas como 'sub-rede externa para EPGs externos'. Isso também significa que o tráfego originado de uma sub-rede específica não deve entrar através de EPGs diferentes. Isso pode causar classificação inesperada de tráfego com base na correspondência de prefixo mais longa em relação às sub-redes declaradas em relação aos EPGs não relacionados. Vejamos alguns cenários para entender isso em detalhes

Prerequisites

Compreensão básica da ACI: L3outs, contratos e aplicação de políticas. Alguns termos úteis são brevemente explicados abaixo, informações mais detalhadas sobre esses termos estão além do escopo deste documento:

pcTag: A ACI classifica o tráfego em pcTags e essas são representações internas de EPGs. Esses valores, por padrão, têm um escopo de VRF - ou seja, são únicos em um VRF, mas podem ser reutilizados em VRFs. No entanto, se um EPG tiver um contrato com outro EPG em um VRF/Espaço diferente , o valor de pcTag terá um escopo global - ou seja, você não encontrará

nenhum outro EPG na ACI com o mesmo pcTag.

ELAM: Embedded Logic Analyser Module (Módulo analisador de lógica incorporado). Essa ferramenta é usada para capturar um pacote no ASIC baseado em filtros e verificar os cabeçalhos/sinalizadores definidos no pacote. Essa ferramenta também ajuda a entender as pesquisas/lógicas feitas por hardware

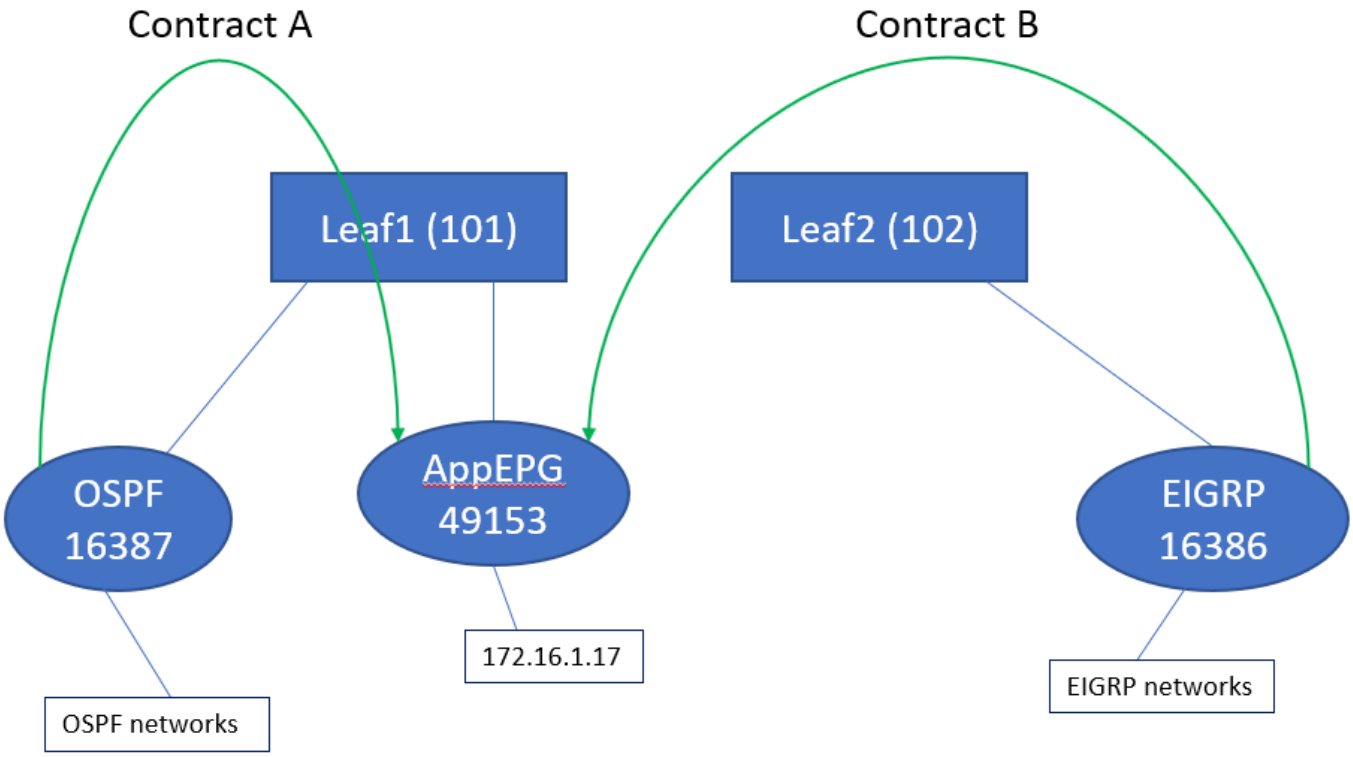
classe/classe: quando o tráfego entra em uma folha, com base na direção da aplicação de política e no conhecimento de prefixo disponível localmente, a folha marcará o tráfego de origem e destino em EPGs - nas capturas de ELAM, isso será visto como classe e classe, respectivamente

zoning-rule: essas são representações internas de contratos e são semelhantes às linhas de uma ACL. Os valores SrcEpg e DstEpg devem corresponder a sclass/dclass para que o tráfego atinja uma determinada regra e seja permitido. Por padrão, em um vrf imposto, há um deny implícito como a última linha , de modo que qualquer tráfego que não corresponda a uma determinada regra irá atingir o deny implícito e será descartado.

Configuração e Topologia

Duas folhas - 101 e 102, modelo: N9K-C93180YC-EX

- Versão 3.2(4e)
- Um VRF usado - Preferência de aplicação de política: ForçadoDireção de aplicação de política: Ingresso.VRF VNID(Identificador de Rede VxLAN): 2752513 ; pcTag: 32770
- L3out em folha1 (101) - Protocolo: Abra o protocolo OSPFUsuário da interface L3 para a vizinhança- eth1/22 (10.27.48.1/24)EPG pcTag externo: 16387
- Aplicativo EPG no Leaf101 Tronco - eth1/24 pcTag: 49153Ponto de extremidade IP: 172.16.1.17 Gateway: 172.16.1.254/24 - implantado no BD (Bridge Domain, Domínio de Bridge) BD tem pcTag 32771
- L3out on Leaf2 (202) - Protocolo: Protocolo de Roteamento IGRP Melhorado (EIGRP)SVI usado para a vizinhança com o Caminho 1/16 - vlan 2747 (10.27.47.1/24)EPG pcTag externo: 163869



Cenários

Tráfego originado de sub-redes sobrepostas

Neste cenário, observamos possíveis erros de classificação quando o tráfego é originado de sub-redes sobrepostas (da perspectiva da ACI)

O OSPF anuncia:

10.9.9.6/32

O EIGRP anuncia:

10.9.9.1/32

Começamos com a topologia no Figura 1, mas sem nenhum contrato. Para o EPG no OSPF, definimos a sub-rede 0.0.0.0/0 como 'sub-rede externa para EPGs externos' e 10.9.9.0/24 com o mesmo sinalizador para o EPG do EIGRP. Aqui está como as tabelas em Leaf1 e 2 se parecem:

Folha1:

```
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
```

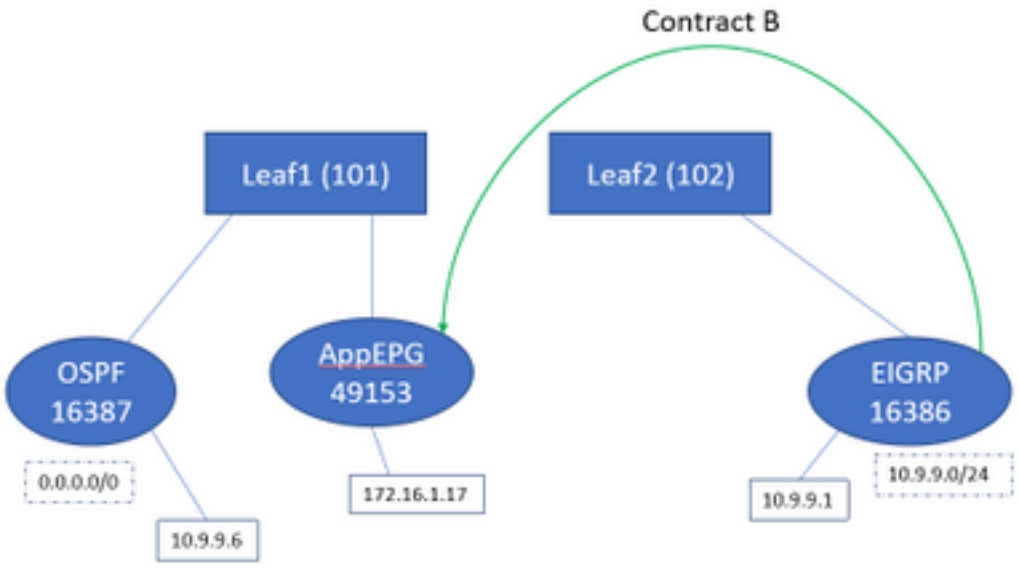
```
      Domain                            VLAN            IP Address        IP Info
+-----------------------------------+--------------+-----------------+--------------+----------
---+
48                                      vlan-2743    dcce.c15b.1e47 L
eth1/24
shparanj:eigrp-test                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

Folha2:

```
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
```

Vamos adicionar o contrato B (contrato no espaço , escopo vrf - arquivo: comum:padrão)



Assim que adicionamos o contrato B, vemos o prefixo EPG do eigrp adicionado no 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
```

Vejamos outras políticas:

Contratos de folha 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)
```

Contratos de folha 2 (manter-se inalterado):

```
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)
```

Neste cenário, o tráfego que entra do ospf l3out , com o qual esperamos ser marcados 16387 é marcado com 16386. Isso ocorre porque o tráfego atinge a entrada do novo prefixo em Leaf1.

Faça ping de 10.9.9.6 para o ponto final 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
```

O ping funciona mesmo sem um contrato entre o ospf epg e o app-epg. Isso porque ele atinge a política para eigrp-epg e é permitido.

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
```

Nesse cenário, o tráfego acaba funcionando devido à classificação em um pcTag que tem um contrato com o destino pretendido. No entanto, se, por exemplo, a folha de cálculo fosse uma terceira folha separada, então o nosso tráfego falharia - uma vez que a entrada para contrato existiria apenas na terceira folha (política de entrada) ou no leaf102 (política de saída).

Estrutura com sub-redes sobrepostas declaradas como externas em EPGs externos separados

Neste cenário, analisamos o conflito de políticas e a possível má classificação devido à sobreposição ou às mesmas sub-redes declaradas como externas em EPGs externos diferentes.

O OSPF anuncia a rede:

10.9.1.0/24

O EIGRP anuncia a rede:

10.9.2.0/24

Começamos com a topologia no Figura 1, mas sem nenhum contrato. Definimos a sub-rede 10.9.0.0/16 as 'sub-rede externa para EPGs externos' para EPG em ambos os L3outs.

Aqui está como as tabelas em Leaf1 e 2 se parecem:

Folha 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)
```

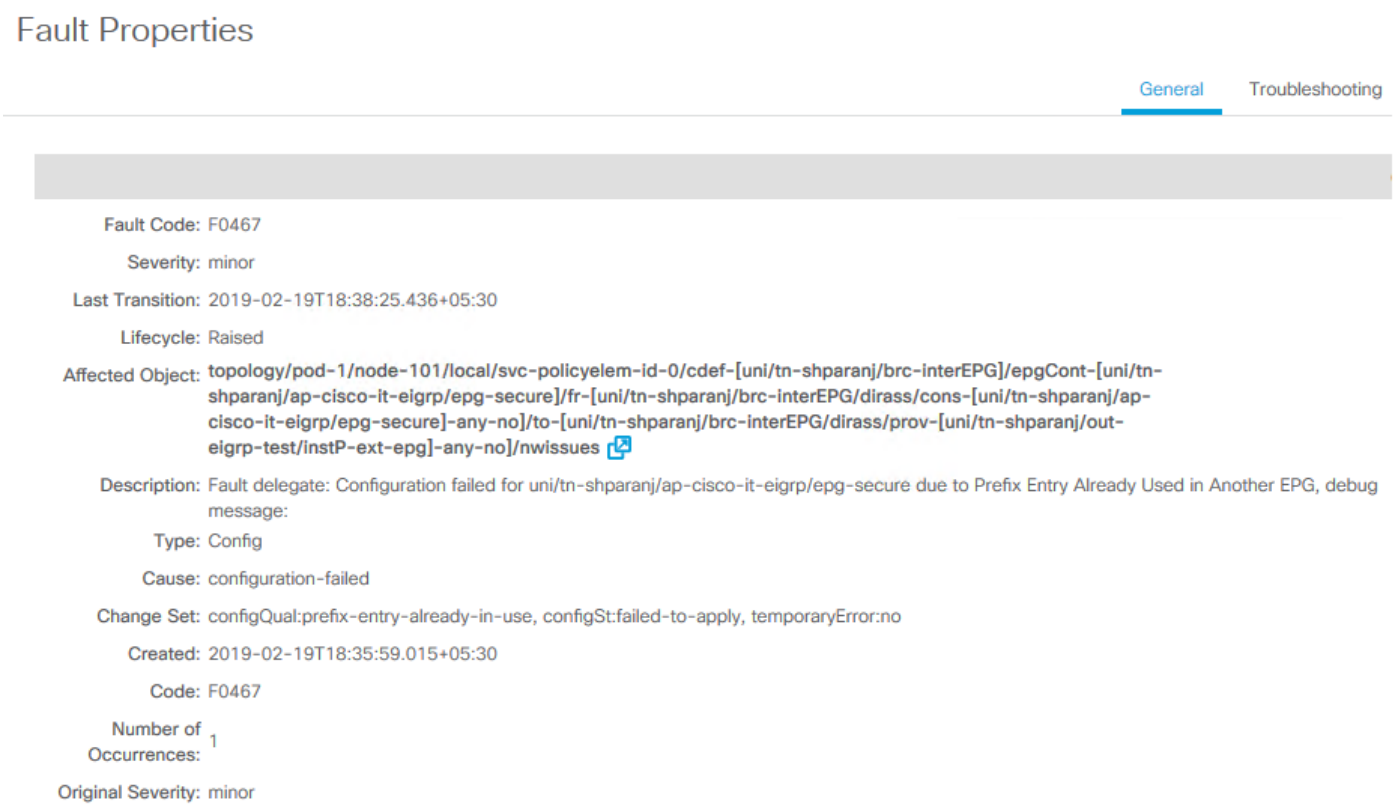
```
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207    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

Folha2:

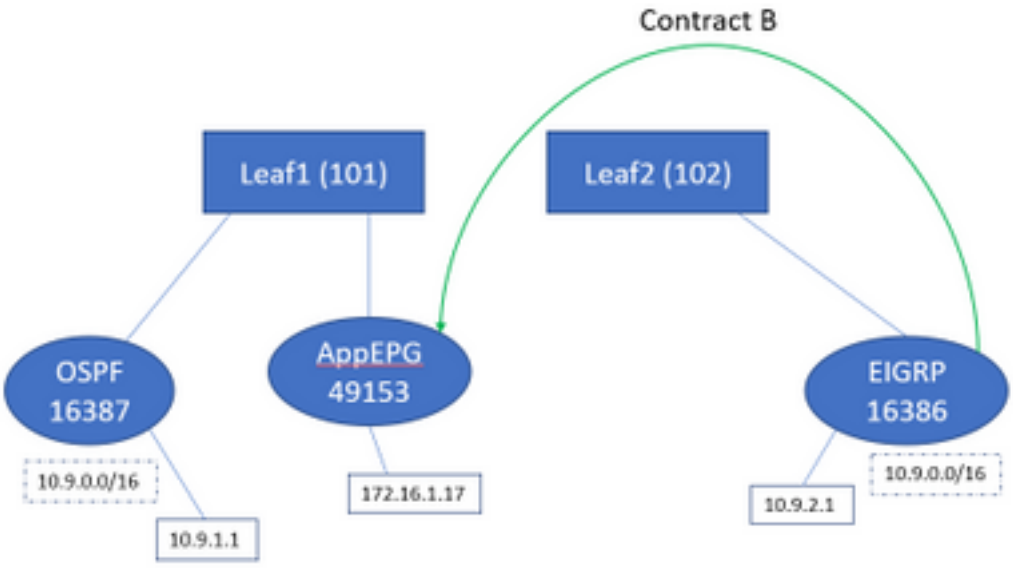
```
leaf102# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

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
```

Neste estado, sem nenhum contrato, não vemos falhas em nenhum dos EPG. Ainda não foi detectada nenhuma sobreposição nos prefixos!

Se adicionarmos o Contrato B, veremos uma falha no aplicativo-EPG (que consome o Contrato B).



Topologia:



Vamos ver a mudança nas tabelas:

```
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
```

A folha2 permanece inalterada.

Isso nos mostra que a regra de zoneamento correspondente ao Contrato B está instalada. No entanto, o prefixo não pode ser adicionado, pois já existe - marcado no OSPF EPG!

E é exatamente isso que a falha nos adverte, "entrada de prefixo já usada em outro EPG" - a falha só é levantada quando há um conflito em uma folha específica entre a política (regras de zoneamento) e sua aplicação. A falha é levantada no EPG do consumidor.

Se iniciarmos o tráfego de 10.9.2.1 , ele será descartado no Leaf101 devido à negação da política:

```
# 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
```

Verificamos que as respostas do PE 172.16.1.17 a 10.9.2.1 foram retiradas. Isso porque:

- As solicitações de 10.9.2.1 provenientes da estrutura já estão classificadas com a classe 16386 - elas atingem a ID da regra 4604 e são permitidas através
- As respostas de 172.16.1.17 são marcadas com a classe 16387 - são obtidas com base nas regras de prefixo do policy-mgr. Não existe uma regra correspondente a 16387, que é negada.

Nessa situação, a má classificação faz com que o tráfego seja descartado, mesmo que pareça que temos a configuração correta no lugar (se a falha for ignorada).

Estrutura com prefixo 0.0.0.0/0 declarado como externo em vários EPGs externos

Neste cenário, observamos possíveis erros de classificação e violações de segurança inesperadas devido à aplicação da sub-rede 0.0.0.0/0 como externa em EPGs externos diferentes.

O OSPF anuncia a rede:

10.7.7.0/24

O EIGRP anuncia a rede:

10.8.8.0/24

Começamos com a topologia no Figura 1, mas sem nenhum contrato. Definimos a sub-rede 0.0.0.0/0 como 'sub-rede externa para EPGs externos' para EPG em ambos os L3outs.

Aqui está como as tabelas em Leaf1 e 2 se parecem:

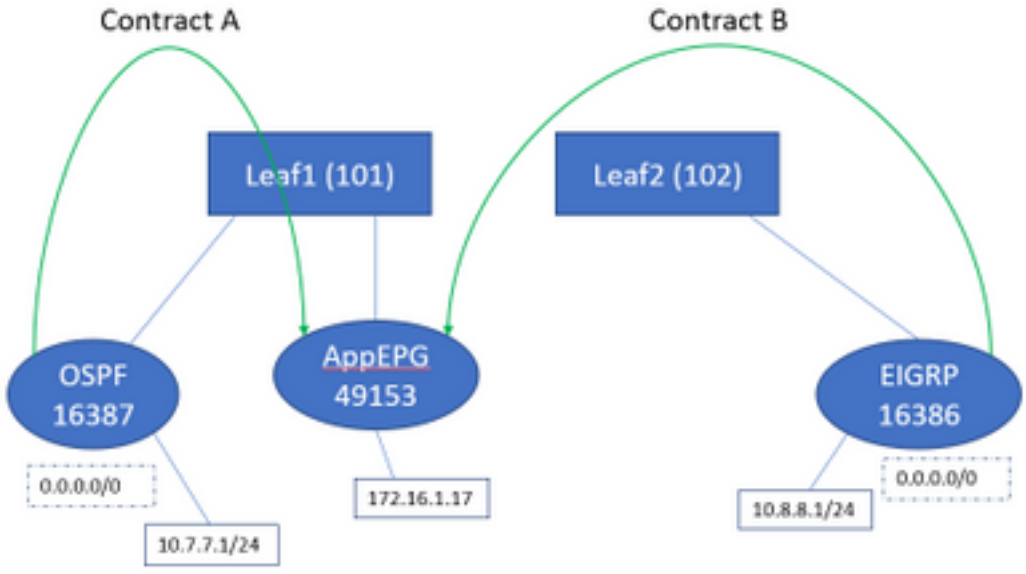
Folha1:

```
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
```

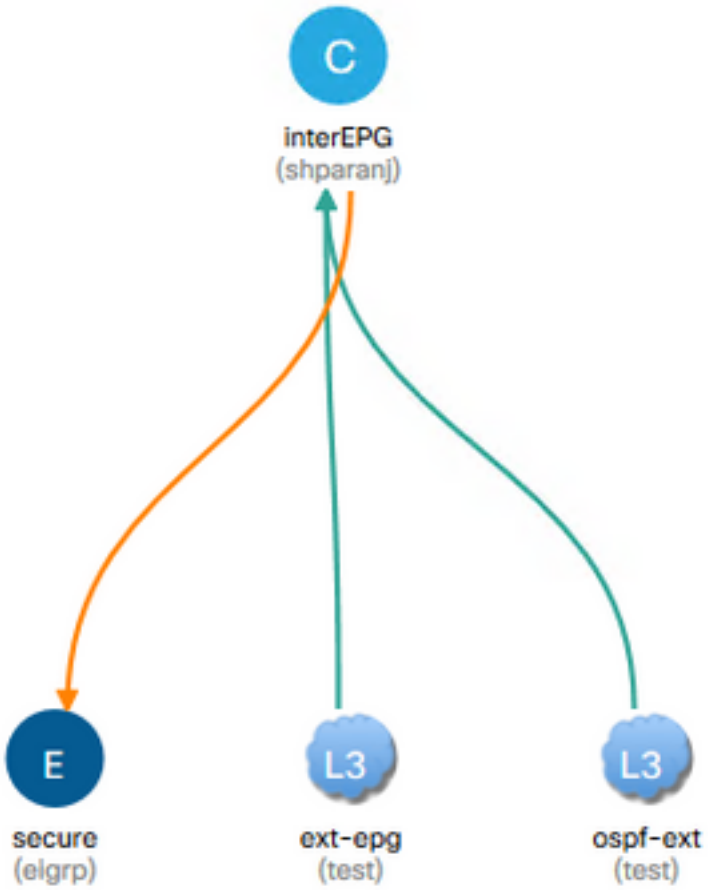
Folha2:

```
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 adicionarmos ambos os contratos A e B, ainda não veremos nenhuma falha.



Vamos ver as tabelas no Leafs:

Folha1:

```
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
```

As tabelas em Folha2 permanecem inalteradas.

Nós não vemos nenhuma falha, pois não há na verdade nenhum conflito de políticas da perspectiva de cada folha. **As IDs de regra adicionadas ao usar 0.0.0.0/0 como EPG externo são especiais.**

- **O tráfego que chega a qualquer folha de borda de seu respectivo EPG é marcado com classe 32770 - este é o pcTag do VRF.**
- dclass nesse tráfego é 49153 - o pcTag do app-EPG.
- **O tráfego de retorno do aplicativo-EPG tem classe de 15**

ELAM em Folha1:

```
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
```

Mesmo que removamos o Contrato A, 10.7.7.1 pode continuar a comunicação com 172.16.1.17.

Isso ocorre porque a remoção do Contrato A não resulta em nenhuma alteração nas regras de zoneamento do 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)
```

Além disso, o tráfego que entra no EPG externo do OSPF continua sendo marcado com VRF pcTag, já que o EPG ainda tem 0.0.0.0/0 marcado como sub-rede externa.

Isso gera uma violação na política de segurança, ou seja, dois EPGs capazes de se comunicar sem um contrato em um VRF imposto.

Leitura adicional

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