Cisco ACI의 L3outs에 겹치는 서브넷

목차

소개

Cisco의 ACI(Application Centric Infrastructure)는 L3outs(Layer 3 out)를 통해 내부 테넌트와 외부 라우팅 네트워크 간의 통신을 지원합니다. 이러한 L3outs는 하나 이상의 EPG(엔드포인트 그룹)를 포함하도록 구성할 수도 있습니다. ACI가 들어오는 트래픽을 L3out의 EPG로 분류하는 방법을 파악하려면 특정 플래그가 활성화된 명시적 서브넷을 정의해야 합니다.이 문서는 계약 기반 정책 애플리케이션의 맥락에서 L3out EPG의 하드웨어 구현에 대해 좀 더 자세히 설명하는 것을 목적으로 합니다.여기서는 '외부 EPG용 외부 서브넷' 플래그 및 겹치는 접두사를 별도의 EPG에서 '외부'로 선언하는 예기치 않은 결과를 구체적으로 살펴봅니다.

개념

엄지의 규칙은 다음과 같습니다.L3outs를 구축할 때 동일한 VRF(Virtual Routing and Forwarding) 인스턴스에 있는 별도의 EPG는 겹치는 서브넷을 '외부 EPG의 외부 서브넷'으로 표시해서는 안 됩니다. 이는 특정 서브넷에서 소싱된 트래픽이 서로 다른 EPG를 통해 유입되어서는 안 된다는 것을 의미합니다.이렇게 하면 상관없는 EPG에 대해 선언된 서브넷에 대해 가장 긴 접두사 일치를 기반으로 트래픽이 예기치 않게 분류될 수 있습니다.몇 가지 시나리오를 자세히 살펴보겠습니다.

사전 요구 사항

ACI에 대한 기본적인 이해:L3outs, 계약 및 정책 시행아래에 몇 가지 유용한 용어에 대해 간략하게 설명하며, 이에 대한 자세한 내용은 이 문서의 범위를 벗어납니다.

pcTag:ACI는 트래픽을 pcTags로 분류하며, 이는 EPG의 내부 표현입니다.기본적으로 이 값은 VRF 범위가 있습니다. 즉, VRF 내에서 고유하지만 VRF 전체에서 재사용될 수 있습니다.그러나 한 EPG가 다른 VRF/테넌트의 다른 EPG와 계약을 맺은 경우 pcTag 값은 전역 범위를 갖습니다. 즉, 동일한 pcTag를 사용하는 ACI에서 다른 EPG를 찾을 수 없습니다.

ELAM:Embedded Logic Analysis Module입니다.이 툴은 필터를 기반으로 ASIC에서 하나의 패킷을 캡처하고 패킷에 설정된 헤더/플래그를 확인하는 데 사용됩니다.이 툴은 하드웨어 기반 조회/로직을 파악하는 데도 도움이 됩니다.

sclass/dclass:트래픽이 leaf로 들어오는 경우 정책 시행 방향 및 로컬에서 사용 가능한 접두사 정보

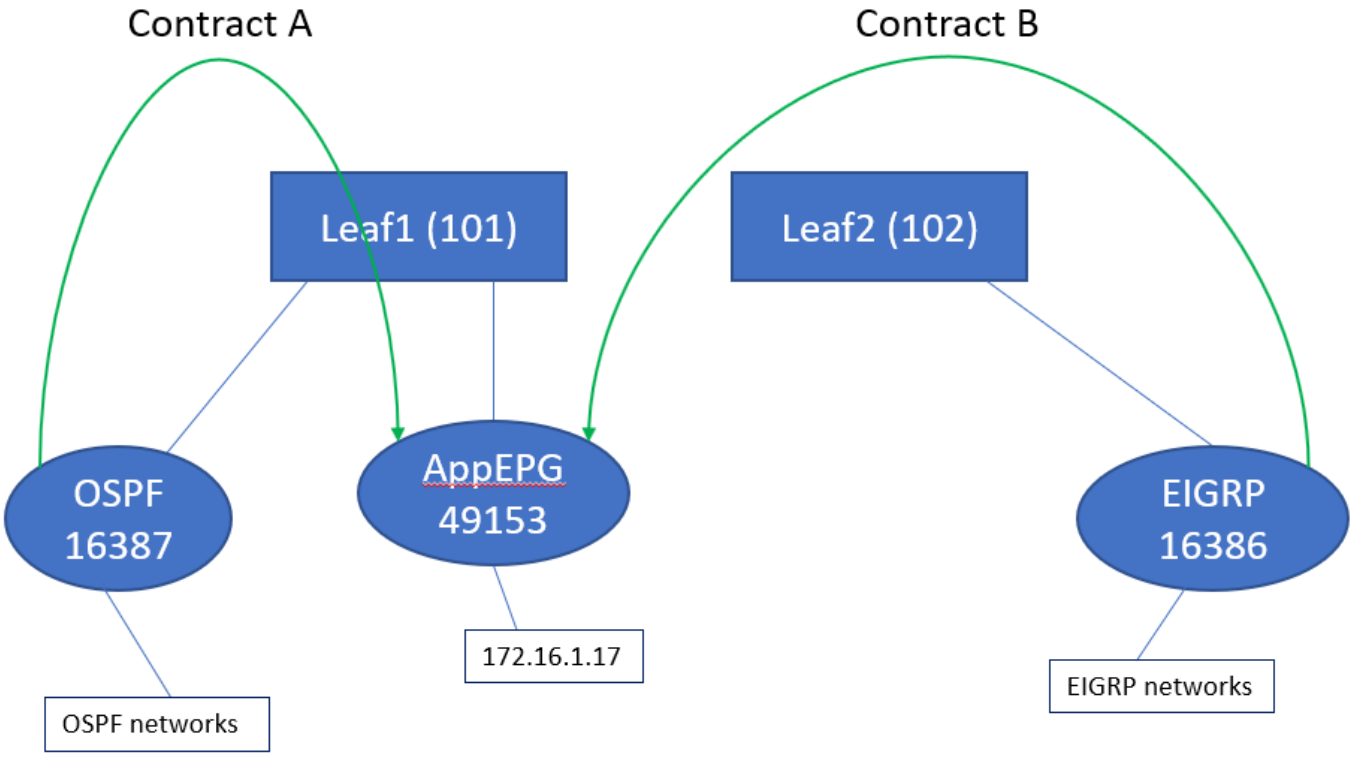
에 따라 leaf는 소스 및 대상 트래픽을 EPG로 표시합니다. ELAM에서는 이를 각각 sclass 및 dclass로 표시합니다.

zoning-rule: 계약에 대한 내부 표현이며 ACL의 행과 유사합니다.SrcEpg 및 DstEpg 값은 트래픽이 지정된 규칙에 도달하고 허용되도록 sclass/dclass와 일치해야 합니다.기본적으로 강제 적용된 vrf에서는 암시적 거부가 마지막 행으로 나타나므로, 특정 규칙에 대해 일치하지 않는 트래픽은 암시적 거부에 도달하여 삭제됩니다.

설정 및 토폴로지

2개의 리프 - 101 및 102, 모델: N9K-C93180YC-EX

- 버전 3.2(4e)
- VRF 1개 사용 - 정책 시행 환경 설정:적용정책 시행 방향:인그레스VRF VNID(VxLAN 네트워크 식별자): 2752513;pcTag: 32770
- Leaf1의 L3out(101) - 프로토콜:OSPF(Open Shortest Path First)L3 인터페이스 사용자 - eth1/22(10.27.48.1/24)외부 EPG pcTag:16387
- Leaf101의 애플리케이션 EPG 트렁크 - eth1/24 pcTag:49153IP 엔드포인트:172.16.1.17 게이트웨이:172.16.1.254/24 - 브리지 도메인에 구축(BD) BD에 pcTag 32771이 있음
- Leaf2의 L3out(202) - 프로토콜:EIGRP(Enhanced Interior Gateway Routing Protocol)경로 1/16 - vlan 2747(10.27.47.1/24)의 인접 디바이스에 사용되는 SVI외부 EPG pcTag:163869



시나리오

겹치는 서브넷에서 제공된 트래픽

이 시나리오에서는 트래픽이 겹치는 서브넷에서 소싱될 경우(ACI의 관점에서) 잠재적인 잘못된 분류가 있는지 살펴봅니다.

OSPF에서 광고하는 내용:

10.9.9.6/32

EIGRP가 광고하는 내용:

10.9.9.1/32

먼저 다이어그램 1의 토폴로지에서 시작하지만, 어떤 계약도 없습니다.OSPF의 EPG의 경우 서브넷 0.0.0.0/0을 '외부 EPG의 외부 서브넷'으로 정의하고, EIGRP의 EPG에 대해 동일한 플래그를 사용하여 10.9.9.0/24으로 정의합니다.Leaf1 및 2의 표는 다음과 같습니다.

리프1:

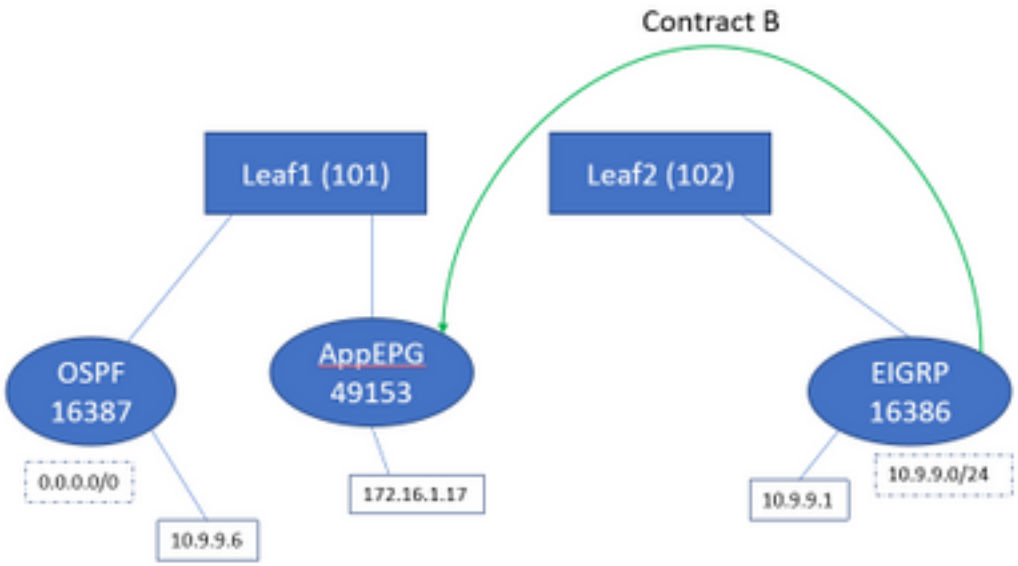
```
leaf101# show end int eth1/24
Legend:
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       L - local
+------------------------------------+--------------+-----------------+--------------+----------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

리프2:

```
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
```

계약 B를 추가하겠습니다(테넌트, 범위 vrf - filer: common:default).



계약 B를 추가하자마자 leaf1에 eigrp EPG 접두사가 추가된 것을 확인할 수 있습니다.

```
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
```

다른 정책을 살펴보겠습니다.

리프 1 계약:

```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)
4604 49153 16386 default enabled 2752513 permit src_dst_any(9) 4605 16386 49153 default enabled
2752513 permit src_dst_any(9)
```

Leaf 2 계약(변경되지 않음):

```
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)
```

이 시나리오에서는 ospf l3out에서 들어오는 트래픽으로, 이 트래픽은 16387은 대신 16386으로 태그됩니다.트래픽이 Leaf1의 새 접두사 엔트리에 도달하기 때문입니다.

10.9.9.6에서 엔드포인트 172.16.1.17으로 ping합니다.

```
# 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
```

Ping은 ospf epg와 app-epg 간의 계약 없이 작동합니다. 이는 eigrp-epg에 대한 정책에 대응하여 허용되기 때문입니다.

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
```

이 시나리오에서는 목적지와 계약이 있는 pcTag로 분류되어 트래픽이 작동하게 됩니다.그러나 예를 들어, 컴퓨팅 리프가 별도의 3rd leaf인 경우 트래픽이 실패합니다. 계약에 대한 항목이 세 번째 리프(인그레스 정책) 또는 leaf102(이그레스 정책)에만 있기 때문입니다.

겹치는 서브넷이 있는 패브릭이 별도의 외부 EPG에 외부로 선언됨

이 시나리오에서는 서로 다른 외부 EPG에 외부 서브넷으로 선언된 중복 또는 동일한 서브넷으로 인해 정책 충돌 및 잠재적인 잘못된 분류가 고려됩니다.

OSPF는 네트워크를 광고합니다.

10.9.1.0/24

EIGRP는 네트워크를 광고합니다.

10.9.2.0/24

먼저 다이어그램 1의 토폴로지에서 시작하지만, 어떤 계약도 없습니다.두 L3outs 모두에서 EPG에

대해 서브넷 10.9.0.0/16 as '외부 EPG에 대한 외부 서브넷'을 정의합니다.

Leaf1 및 2의 표는 다음과 같습니다.

리프 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
```

리프2:

```
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
```

이 상태에서는 계약이 없으면 EPG에 결함이 없습니다.접두사에 중복되는 부분이 아직 발견되지 않았습니다!

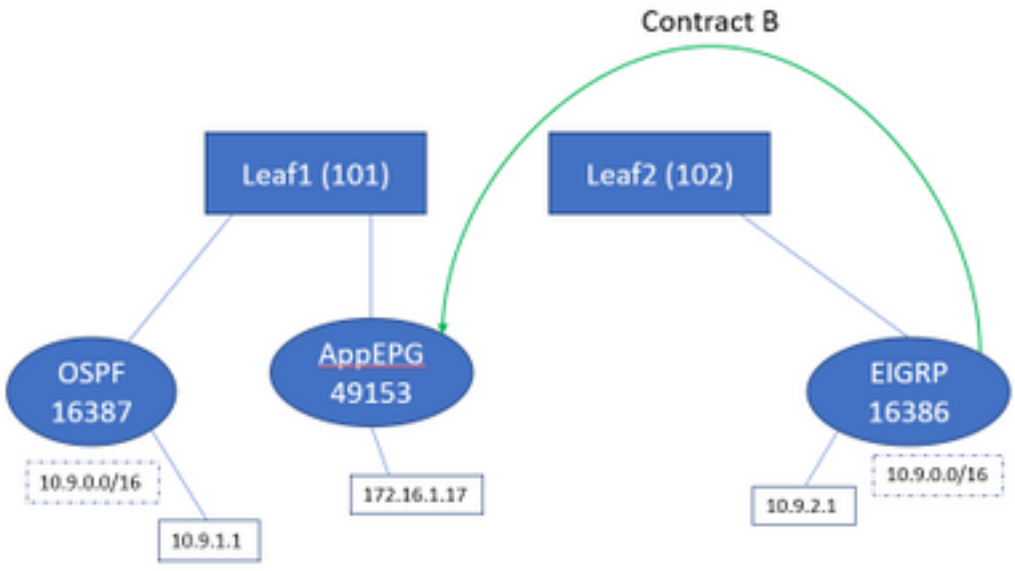
Contract B를 추가하면 app-EPG에 결함이 표시됩니다(Contract B 사용).

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

토폴로지:



이제 테이블의 변경 사항을 살펴보겠습니다.

```
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
```

Leaf2는 변경되지 않습니다.

계약 B에 해당하는 zoning-rule이 설치되어 있음을 보여줍니다.그러나 접두사는 이미 있으므로 추가할 수 없습니다. OSPF EPG에 대해 표시됩니다!

그리고 이것이 바로 fault가 경고하는 것입니다. "다른 EPG에서 이미 사용되는 접두사 입력" - 정책(zoning-rules)과 애플리케이션 간에 특정 leaf에 충돌이 있을 때만 결함이 제기됩니다.결함이 소비자 EPG에서 제기됩니다.

10.9.2.1에서 트래픽을 시작하면 정책 거부로 인해 Leaf101에서 삭제됩니다.

```
# 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
```

EP 172.16.1.17에서 10.9.2.1로의 회신이 삭제됩니다.그 이유는 다음과 같습니다.

- 패브릭에서 들어오는 10.9.2.1의 요청은 이미 클래스 16386으로 분류되어 있습니다. 이 요청은 규칙 ID 4604에 도달하여 허용됩니다.
- 172.16.1.17의 회신은 dclass 16387로 표시됩니다. 이는 policy-mgr 접두사 규칙에 따라 선택됩니다.16387에 해당하는 규칙이 없으며 거부됩니다.

이러한 상황에서 잘못 분류하면 올바른 컨피그레이션이 있는 것처럼 보이지만(결함이 무시된 경우) 트래픽이 삭제됩니다.

0.0.0.0/0 접두사가 있는 패브릭이 여러 외부 EPG에서 외부로 선언됨

이 시나리오에서는 다른 외부 EPG에 외부 서브넷으로 0.0.0.0/0 서브넷을 적용했기 때문에 잠재적인 잘못된 분류 및 예기치 않은 보안 위반을 살펴봅니다.

OSPF는 네트워크를 광고합니다.

10.7.7.0/24

EIGRP는 네트워크를 광고합니다.

10.8.8.0/24

먼저 다이어그램 1의 토폴로지에서 시작하지만, 어떤 계약도 없습니다.두 L3outs 모두에서 EPG에 대해 서브넷 0.0.0.0/0을 '외부 EPG의 외부 서브넷'으로 정의합니다.

Leaf1 및 2의 표는 다음과 같습니다.

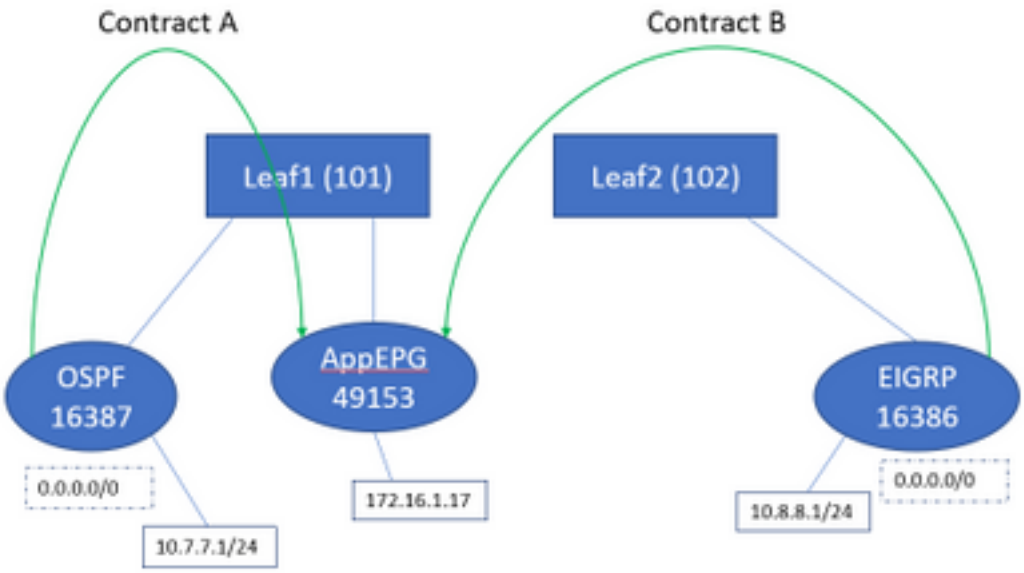
리프1:

```
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
```

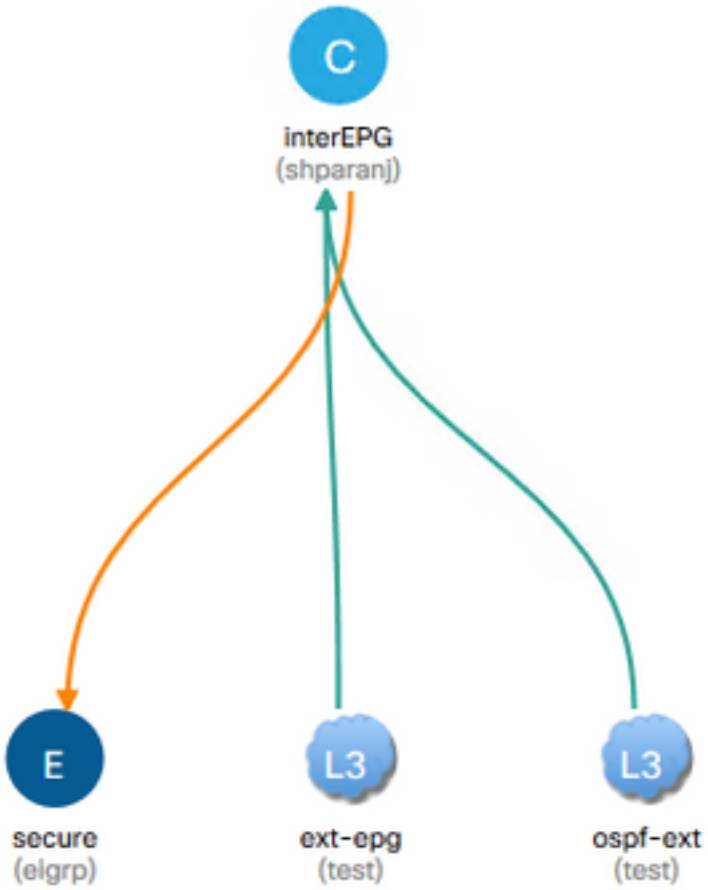
리프2:

```
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
```



계약 A와 B를 모두 추가해도 결함이 표시되지 않습니다.



Leaf의 표를 살펴보겠습니다.

리프1:

```
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
```

Leaf2의 테이블은 변경되지 않습니다.

각 잎의 관점에서는 정책 상충이 없기 때문에 우리는 어떤 결점도 보지 못합니다.**외부 EPG로 0.0.0.0/0을 사용할 때 추가된 규칙 ID는 특별합니다.**

- **각 EPG에서 경계 리프로 들어오는 트래픽은 클래스 32770으로 표시됩니다. 이는 VRF의 pcTag입니다.**
- 이 트래픽의 dclass는 app-EPG의 pcTag인 49153입니다.
- **app-EPG의 반환 트래픽은 클래스 15입니다.**

Leaf1의 ELAM:

```
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
```

계약 A를 제거하더라도 10.7.7.1은 172.16.1.17과 계속 통신할 수 있습니다.

계약 A를 제거해도 Leaf1의 zoning-rule이 변경되지 않기 때문입니다.

```
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)
```

또한 EPG는 여전히 0.0.0.0/0을 외부 서브넷으로 표시하므로 OSPF 외부 EPG에서 들어오는 트래

픽은 VRF pcTag로 계속 태그됩니다.

이로 인해 보안 정책(예: 강제 VRF에서 계약 없이 통신할 수 있는 EPG 2개)이 침해됩니다.

추가 읽기

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