Cisco ACIのL3アウトでのサブネットのオーバーラップ

内容

概要

シスコのApplication Centric Infrastructure(ACI)は、内部テナントと外部ルーテッドネットワーク間の通信をL3out（レイヤ3アウト）経由で容易にします。 このようなL3outは、1つ以上のエンドポイントグループ(EPG)を持つように設定することもできます。 L3outのEPGとして着信するトラフィックを分類する方法をACIが知るためには、特定のフラグを有効にして明示的なサブネットを定義する必要があります。この記事では、契約ベースのポリシー適用に関連したL3out EPGのハードウェア実装について少し説明します。ここでは、フラグ「外部EPGの外部サブネット」と、重複するプレフィックスを別のEPGで「外部」として宣言することによる予期せぬ結果について具体的に説明します。

概念

経験則は次のとおりです。L3outを展開する場合、同じVirtual Routing and Forwarding(VRF)インスタンス内の別々のEPGには、「外部EPGの外部サブネット」としてマークされた重複するサブネットを設定しないでください。また、特定のサブネットから発信されたトラフィックはEPGを通過しません。これにより、無関係なEPGに対して宣言されたサブネットに対する最長プレフィクス照合に基づいて、トラフィックが予期せぬ分類される可能性があります。これを詳しく理解するためのシナリオをいくつか見てみましょう

前提条件

ACIの基本的な知識：L3アウト、契約、ポリシー適用有用な用語を次に簡単に説明します。これらの詳細な情報は、このドキュメントの範囲外です。

pcTag:ACIはトラフィックをpcTagsに分類し、これらはEPGの内部表現です。これらの値は、デフォルトでVRFの範囲を持ちます。つまり、VRF内で一意ですが、VRF間で再利用できます。ただし、あるEPGが異なるVRF/テナント(VRF/TENANT)内の別のEPGと契約している場合、pcTagの値にはグローバルスコープがあります。つまり、同じpcTagを持つACI内に他のEPGはありません。

ELAM: Embedded Logic Analyzer Module。このツールは、フィルタに基づいてASIC上の1つのパケットをキャプチャし、パケットに設定されているヘッダー/フラグを確認するために使用されます。このツールは、ハードウェアベースのルックアップ/ロジックの理解にも役立ちます

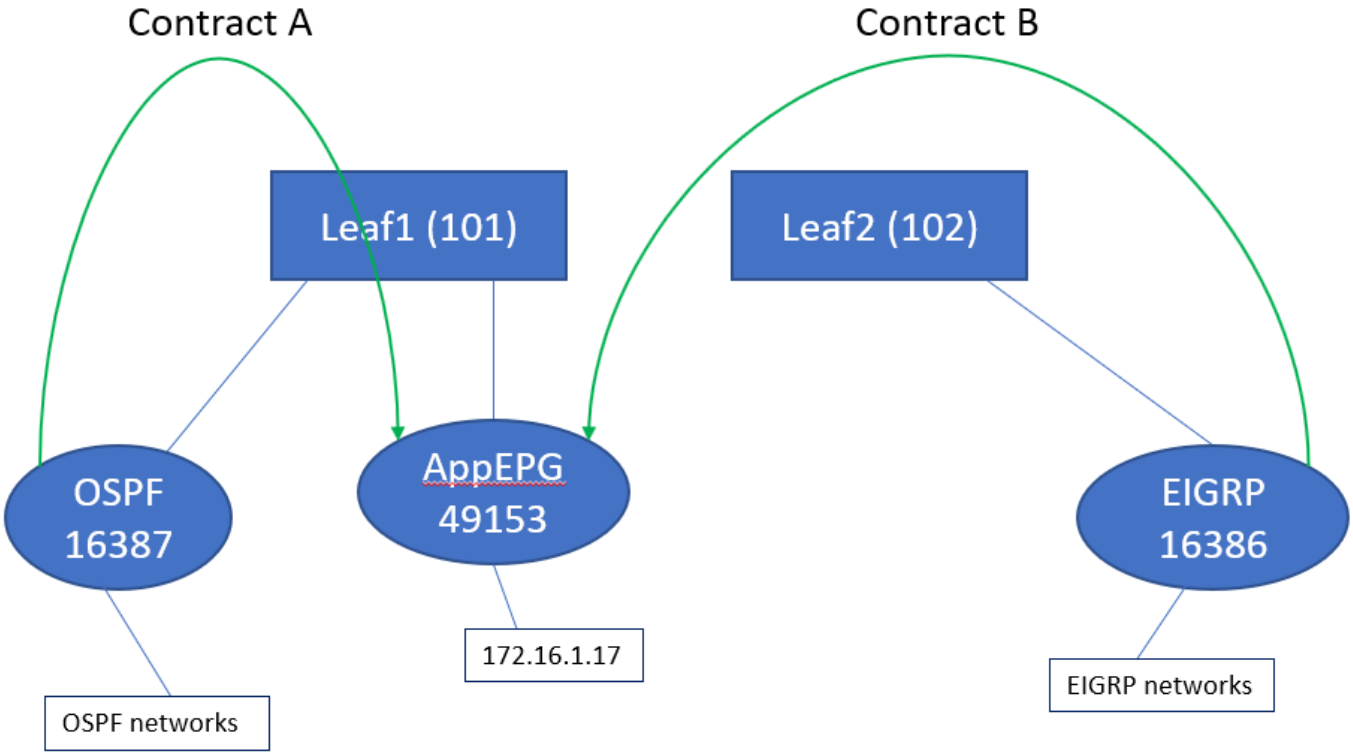
sclass/dclass:トラフィックがリーフに到着すると、ポリシーの適用の方向とローカルで使用可能なプレフィクス情報に基づいて、リーフがEPGに送信元トラフィックと宛先トラフィックをマークします。ELAMのキャプチャでは、それぞれsclassとdclassと見なされます

zoning-rule:これらはコントラクトの内部表現であり、ACLの行に似ています。SrcEpgおよびDstEpgの値は、トラフィックが特定のルールにヒットして許可されるように、sclass/dclassと一致する必要があります。強制的なvrfでは、デフォルトで最後の行として暗黙のdenyが存在するため、特定のルールに一致しないトラフィックは暗黙的なdenyにヒットし、廃棄されます。

セットアップとトポロジ

2つのリーフ – 101および102(N9K-C93180YC-EX)

- バージョン3.2(4e)
- 1つのVRFを使用： ポリシー適用のプリファレンス：実施ポリシー適用の方向：入力.VRF VNID（VxLANネットワーク識別子）:2752513、pcTag: 32770
- Leaf1のL3out(101) - プロトコル:Open Shortest Path First（OSPF）ネイバーシップのL3インターフェイスユーザ – eth1/22(10.27.48.1/24)外部EPG pcTag:16387
- Leaf101のアプリケーションEPG トランク：eth1/24 pcTag:49153IPエンドポイント：172.16.1.17 ゲートウェイ：172.16.1.254/24：ブリッジドメイン(BD)に導入 BDにはpcTag 32771があります。
- Leaf2のL3out(202) - プロトコル:Enhanced Interior Gateway Routing Protocol（EIGRP）パス1/16 - vlan 2747(10.27.47.1/24)のネイバーシップに使用されるSVI外部EPG pcTag:163869



シナリオ

重複するサブネットから送信されるトラフィック

このシナリオでは、トラフィックの送信元が重複するサブネットである場合の誤分類の可能性（ACIの観点から）について説明します

OSPFは次をアドバタイズします。

10.9.9.6/32

EIGRPは次をアドバタイズします。

10.9.9.1/32

図1のトポロジから始めますが、契約は必要ありません。OSPFのEPGでは、サブネット0.0.0.0/0を「外部EPGの外部サブネット」として定義し、EIGRPのEPGと同じフラグを持つ10.9.9.0/24を定義します。Leaf1と2のテーブルは次のようになります。

Leaf1:

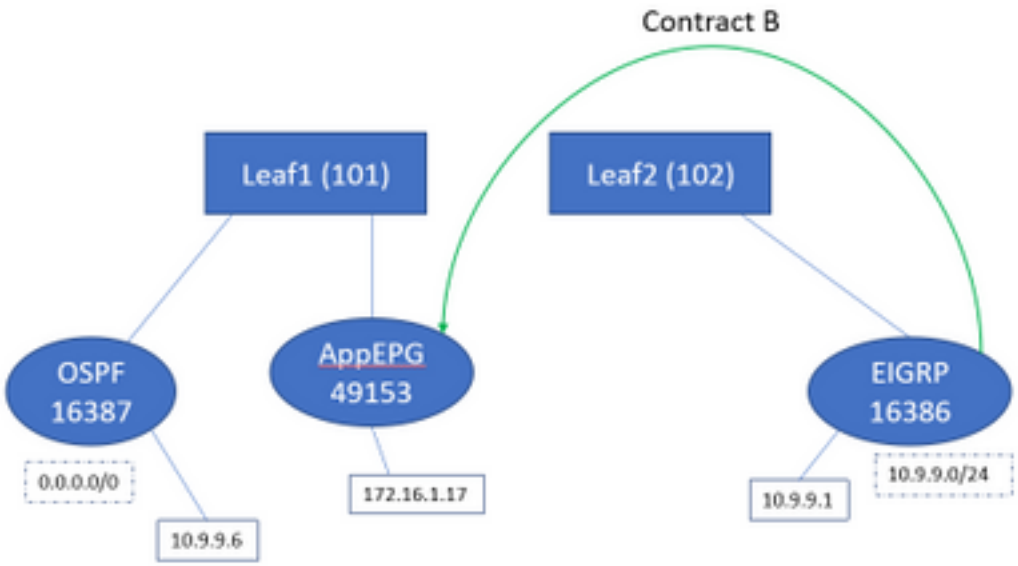
```
leaf101# show end int eth1/24
Legend:
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       L - local
+----------------------------------+---------------+-----------------+--------------+----------
---+
      VLAN/                           Encap           MAC Address       MAC Info/
Interface
      Domain                          VLAN            IP Address        IP Info
+----------------------------------+---------------+-----------------+--------------+----------
---+
48                                       vlan-2743    dcce.c15b.1e47 L
eth1/24
shparanj:eigrp-test                      vlan-2743       172.16.1.17 L
eth1/24

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

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

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


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

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

リーフ2:

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

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

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

コントラクトB (テナント内のコントラクト、scope vrf – ファイラ：common:default) を追加します。



コントラクトBを追加するとすぐに、leaf1に追加されたeigrp EPGプレフィクスが表示されます。

```
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
```

他のポリシーを見てみましょう。

リーフ1契約：

```
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)
```

リーフ2契約（変更なし）：

```
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)
```

このシナリオでは、ospf l3outから着信するトラフィックは次のようにタグ付けされます 代わりに16387に16386のタグが付けられます。これは、トラフィックがLeaf1の新しいプレフィックスエントリにヒットするためです。

10.9.9.6からエンドポイント172.16.1.17にpingします。

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

Pingは、ospf epgとapp-epgの間の契約がなくても動作します。これは、eigrp-epgのポリシーにヒットし、許可されるためです。

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
```

このシナリオでは、目的の宛先との契約があるpcTagへの分類が原因で、トラフィックが動作します。ただし、コンピュートリーフが別の3つ目のリーフである場合、トラフィックは失敗します。コントラクトのエントリは3つ目のリーフ（入力ポリシー）またはリーフ102（出力ポリシー）だけに存在するためです。

独立した外部EPGで外部として宣言された重複するサブネットを持つファブリック

このシナリオでは、異なる外部EPG上で外部として宣言されたサブネットが重複したり、同一のサブネットが宣言されたために、ポリシーの競合と潜在的な誤分類について説明します。

OSPFはネットワークをアドバタイズします。

10.9.1.0/24

EIGRPはネットワークをアドバタイズします。

10.9.2.0/24

図1のトポロジから始めますが、契約は必要ありません。サブネット10.9.0.0/16を、両方のL3outのEPGの「外部EPGの外部サブネット」として定義します。

Leaf1と2のテーブルは次のようになります。

リーフ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
```

リーフ2:

```
leaf102# show ip route vrf shparanj:eigrp-test
```

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

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

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

<<vsh>>

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

この状態では、契約がないと、どちらのEPGにも障害は発生しません。プレフィックスの重複は検出されていません。

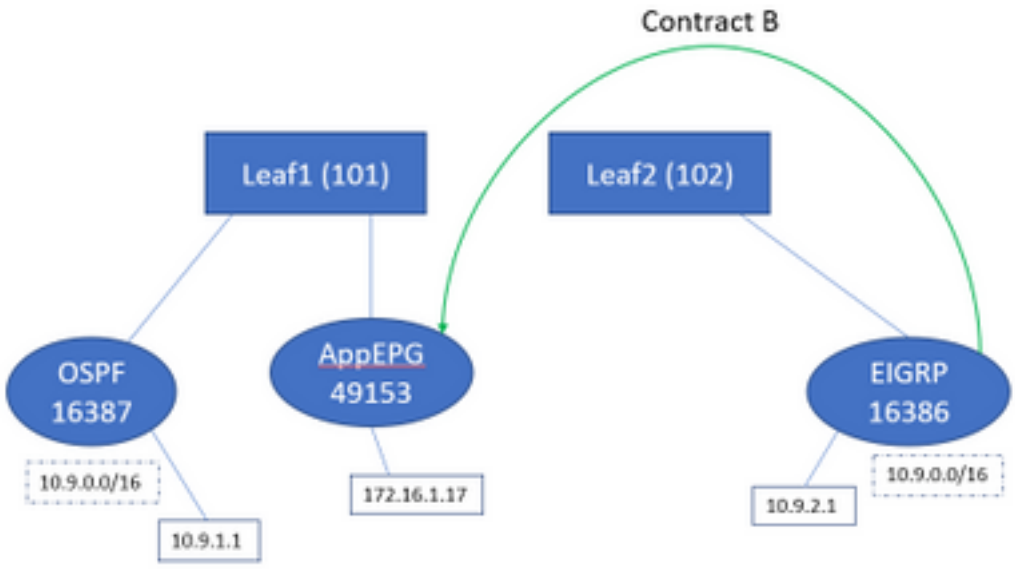
コントラクトBを追加すると、アプリケーションEPG (コントラクトBを消費する) にエラーが発生します。

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

トポロジ：



次に、テーブルの変更を示します。

```
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は変更されません。

これは、契約Bに対応するゾーニング・ルールがインストールされていることを示しています。ただし、プレフィックスは既に存在するため追加できません。OSPF EPGに対してマークされます。

この障害は、ポリシー（ゾーニング・ルール）とそのアプリケーションの間で特定のリーフに競合が発生した場合にのみ発生します。障害はコンシューマEPGで発生します。

10.9.2.1からのトラフィックを開始すると、ポリシー「deny:

```
# 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 172.16.1.17から10.9.2.1への応答がドロップされていることがわかります。これは、次の理由により発生します。

- ファブリックから着信する10.9.2.1からの要求は、すでにクラス16386で分類されています。これらはルールID 4604にヒットし、
- 172.16.1.17からの応答はdclass 16387でマークされます。これはpolicy-mgrプレフィックスルールに基づいてピックアップされます。16387に対応するルールはなく、これらは拒否されます。

この状況では、適切な設定が行われているように見えても（障害が無視された場合）、トラフィックがドロップされます。

0.0.0.0/0プレフィクスが複数の外部EPGで外部として宣言されたファブリック

このシナリオでは、異なる外部EPGに0.0.0.0/0サブネットを外部として適用することによる、誤分類の可能性と予期しないセキュリティ違反について説明します。

OSPFはネットワークをアドバタイズします。

10.7.7.0/24

EIGRPはネットワークをアドバタイズします。

10.8.8.0/24

図1のトポロジから始めますが、契約は必要ありません。サブネット0.0.0.0/0を、両方のL3outのEPGの「外部EPGの外部サブネット」として定義します。

Leaf1と2のテーブルは次のようになります。

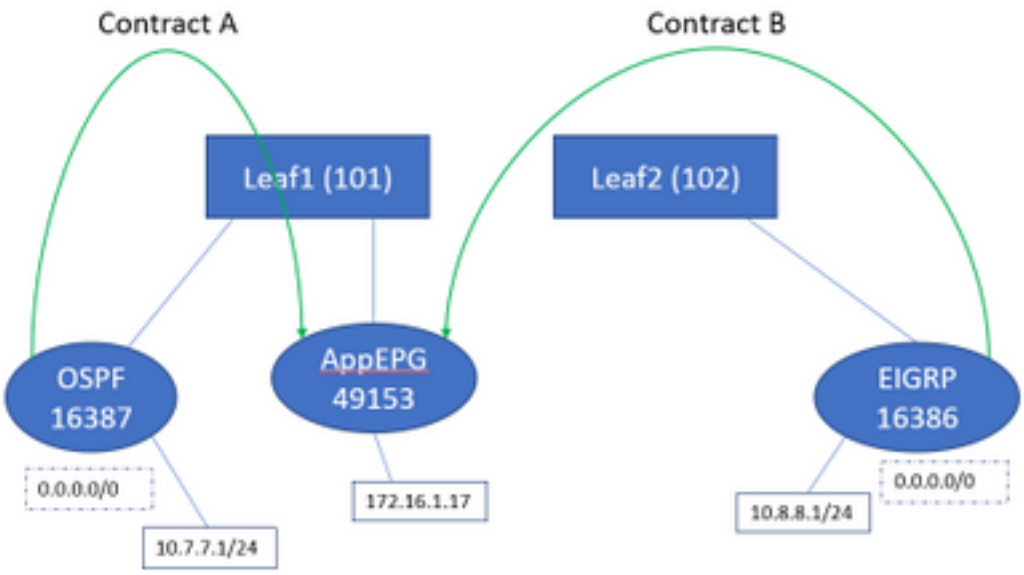
リーフ1:

```
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
```

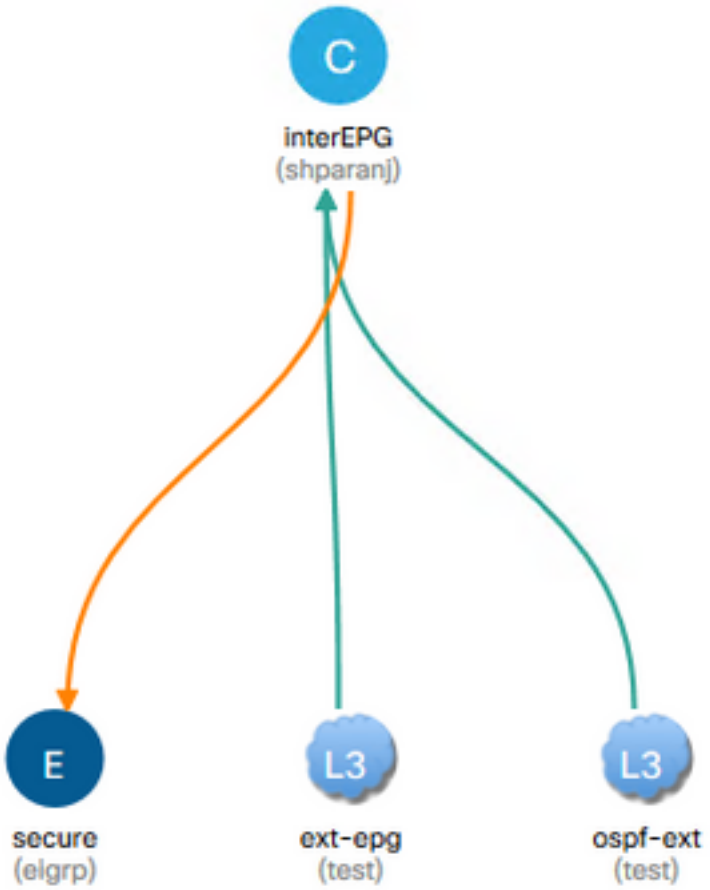
リーフ2:

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

10.7.7.0/24, ubest/mbest: 1/0
```

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


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

<<vsh>>

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



両方の契約AとBを追加しても、障害は発生しません。



Leasesの表を見てみましょう。

リーフ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
```

Leaf2のテーブルは変更されません。

各リーフの観点から見ると、ポリシーの競合は実際にはないため、障害は見られません。
0.0.0.0/0を外部EPGとして使用するときに追加されるルールIDは特別です。

- **それぞれのEPGからいずれかの境界リーフに着信するトラフィックは、クラス32770でマークされます。これはVRFのpcTagです。**
- このトラフィックのdclassは49153 (app-EPGのpcTag) です。
- **app-EPGからのリターントラフィックのクラスは15です**

リーフ1の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
```

コントラクトAを削除しても、10.7.7.1は172.16.1.17との通信を継続できます。

これは、コントラクトAを削除しても、Leaf1のゾーニングルールに変更が加わらないためです。

```
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)
```

さらに、OSPF外部EPGに着信するトラフィックは、VRF pcTagでタグ付けされ続けます。これ

は、EPGには引き続き0.0.0.0/0が外部サブネットとしてマークされているためです。

これにより、セキュリティポリシーが侵害されます。つまり、2つのEPGが強制的なVRFで契約なしで通信できます。

参考資料

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