Überschneidende Subnetze bei L3outs in der Cisco ACI

Inhalt

Einführung

Die Cisco Application Centric Infrastructure (ACI) ermöglicht die Kommunikation zwischen internen Tenants und externen gerouteten Netzwerken über L3outs (Layer 3 Out). Solche L3outs können auch für eine oder mehrere Endpunktgruppen (EPGs) konfiguriert werden. Damit die ACI wissen kann, wie der eingehende Datenverkehr als EPG eines L3out klassifiziert werden kann, müssen explizite Subnetze mit aktivierten Flaggen definiert werden. In diesem Artikel soll die Hardwareimplementierung von L3out-EPGs im Zusammenhang mit der vertraglich basierten Richtlinienanwendung näher erläutert werden. Wir werden speziell die Flag "externe Subnetze für externe EPGs" und die unerwarteten Folgen der Erklärung überlappender Präfixe als "extern" auf separaten EPGs untersuchen.

Konzept

Die Faustregel lautet: Bei der Bereitstellung von L3outs sollten separate EPGs in derselben VRF-Instanz (Virtual Routing and Forwarding) keine überlappenden Subnetze als "externes Subnetz für externe EPGs" markiert haben. Dies bedeutet auch, dass Datenverkehr, der von einem bestimmten Subnetz stammt, nicht über verschiedene EPGs eingehen darf. Dies kann zu einer unerwarteten Klassifizierung des Datenverkehrs führen, der auf der längsten Präfixübereinstimmung mit Subnetzen basiert, die gegenüber nicht verknüpften EPGs deklariert wurden. Schauen wir uns einige Szenarien an, um dies detailliert zu verstehen.

Voraussetzungen

Grundkenntnisse der ACI: L3outs, Verträge und Richtliniendurchsetzung. Einige nützliche Begriffe werden nachfolgend kurz erläutert. Ausführlichere Informationen zu diesen Begriffen finden Sie in diesem Dokument:

pcTag: Die ACI klassifiziert den Datenverkehr in PCTags. Dies sind interne Darstellungen von EPGs. Diese Werte haben standardmäßig einen VRF-Bereich, d. h. sie sind innerhalb einer VRF-

Instanz eindeutig, können jedoch in allen VRF-Instanzen wiederverwendet werden. Wenn jedoch eine EPG einen Vertrag mit einer anderen EPG in einem anderen VRF/Tenant hat, hat der pcTag-Wert einen globalen Gültigkeitsbereich, d.h. Sie finden keine andere EPG in der ACI mit demselben pcTag.

ELAM: Integriertes Logik-Analysemodul. Dieses Tool wird verwendet, um ein Paket auf der Basis von ASIC-Filtern zu erfassen und die Header/Flags auf dem Paket zu überprüfen. Dieses Tool hilft auch, Suchvorgänge/Logik zu verstehen, die von hardwarebasierten

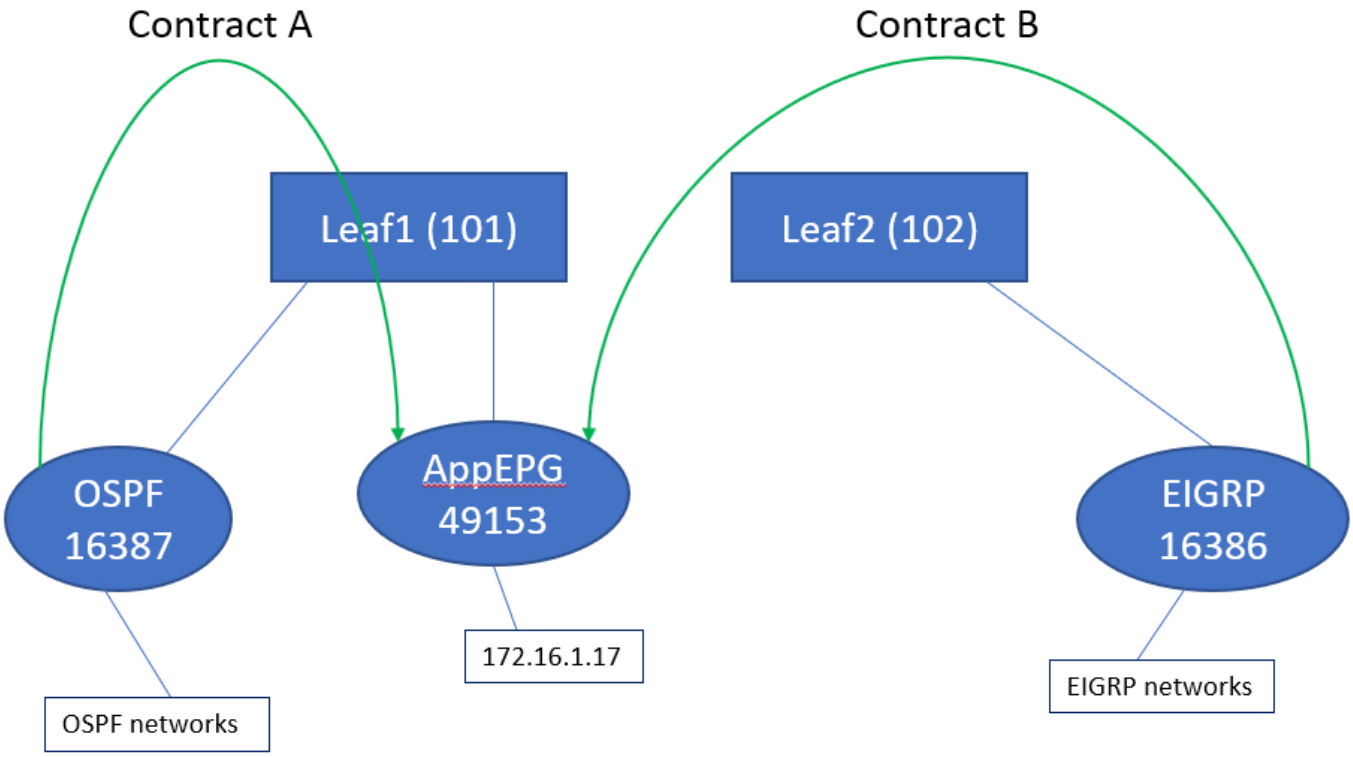
class/class: Wenn der Datenverkehr zu einem Leaf gelangt, wird der Quell-Datenverkehr anhand der Richtung der Richtliniendurchsetzung und der lokal verfügbaren Präfixinformationen als Quell- und Zieldatenverkehr in EPGs markiert. In ELAM wird dieser als Klasse bzw. Klasse erfasst.

Zoning-Regel: Dies sind interne Darstellungen von Verträgen und ähneln den Zeilen einer ACL. Die Werte SrcEpg und DstEpg sollten mit sclass/class übereinstimmen, damit Datenverkehr eine bestimmte Regel trifft und zugelassen wird. Standardmäßig gibt es in einem erzwungenen VRF eine implizite Verweigerung als letzte Zeile, sodass jeder Datenverkehr, der nicht mit einer bestimmten Regel übereinstimmt, die implizite Verweigerung trifft und verworfen wird.

Einrichtung und Topologie

Zwei Broschüren - 101 und 102, Modell: N9K-C93180YC-EX

- Version 3.2(4e)
- Verwendete eine VRF-Instanz - Bevorzugte Richtliniendurchsetzung: DurchgesetztRichtliniendurchsetzung: Eingang.VRF VNID(VxLAN Network Identifier): 2752513; PC-Tag: 32770
- L3out in Leaf1 (101) - Protokoll: Open Shortest Path First (OSPF)L3-Schnittstellenbenutzer für Nachbarschaft - eth1/22 (10.27.48.1/24)Externe EPG pcTag: 16387
- Anwendung EPG auf Leaf101 Trunk - eth1/24 PC-Tag: 49153IP-Endpunkt: 172,16,1,17 Gateway: 172.16.1.254/24 - bereitgestellt auf Bridge Domain (BD) BD hat pcTag 32771
- L3out auf Leaf2 (202) - Protokoll: Enhanced Interior Gateway Routing Protocol (EIGRP)SVI für Nachbarschaft verwendet mit Pfad 1/16 - VLAN 2747 (10.27.47.1/24)Externe EPG pcTag: 163.869



Szenarien

Datenverkehr, der von überlappenden Subnetzen stammt

In diesem Szenario wird die potenzielle Fehlklassifizierung untersucht, wenn der Datenverkehr aus überlappenden Subnetzen stammt (aus ACI-Sicht).

OSPF kündigt Folgendes an:

10.9.9.6/32

EIGRP kündigt Folgendes an:

10.9.9.1/32

Wir beginnen mit der Topologie in Abbildung 1, jedoch ohne Verträge. Für EPG auf OSPF definieren wir Subnetz 0.0.0.0/0 als "externes Subnetz für externe EPGs" und 10.9.9.0/24 mit derselben Markierung für EIGRPs EPG. So sehen die Tabellen auf Leaf1 und 2 aus:

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
```

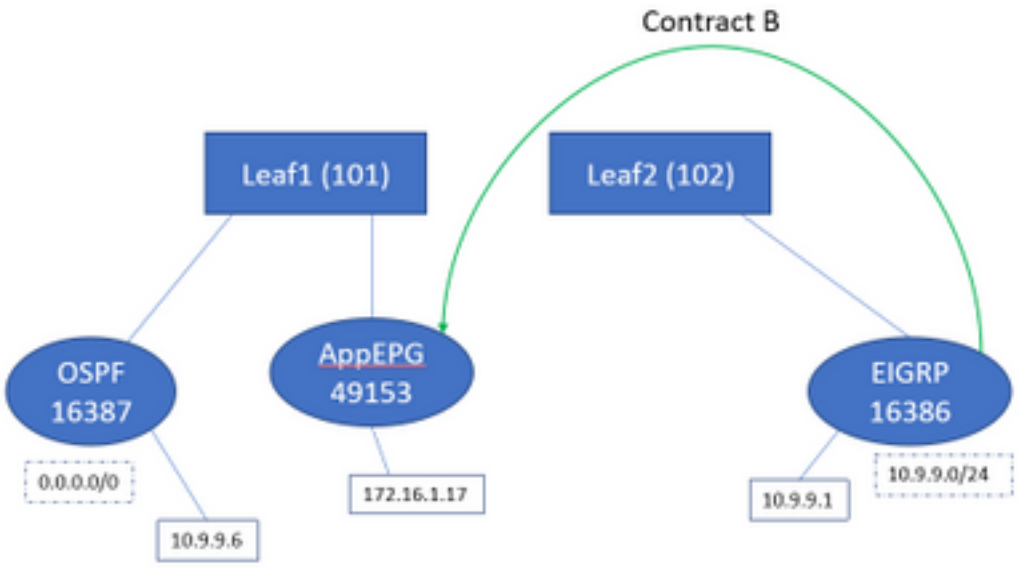
```
      Domain                            VLAN            IP Address        IP Info
+-----------------------------------+--------------+-----------------+--------------+----------
---+
48                                        vlan-2743    dcce.c15b.1e47 L
eth1/24
shparanj:eigrp-test              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

Leaf2:

```
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
```

Fügen wir Vertrag B hinzu (Vertrag im Tenant, Bereich vrf - filer: gängig:default)



Sobald Vertrag B hinzugefügt wurde, wird das eigrp-EPG-Präfix auf Leaf1 hinzugefügt:

```
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
```

Sehen wir uns andere Richtlinien an:

Leaf-1-Verträge:

```
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-Verträge (bleiben unverändert):

```
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 diesem Szenario kommt der Datenverkehr von ospf l3out , mit dem wir voraussichtlich markiert werden 16387 wird stattdessen mit 16386 getaggt. Der Grund hierfür ist, dass der Datenverkehr den neuen Präfixeintrag auf Leaf1 erreicht.

Ping von 10.9.9.6 bis Endpunkt 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
```

Ping funktioniert auch ohne Vertrag zwischen ospf epg und app-epg. Dies liegt daran, dass sie gegen die Richtlinie für eigrp-epg verstößt und zugelassen wird.

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 diesem Szenario funktioniert der Datenverkehr aufgrund der Klassifizierung in einen PC-Tag, der einen Vertrag mit dem beabsichtigten Ziel hat. Wäre das Computing-Leaf jedoch ein separates 3. Leaf, würde unser Datenverkehr scheitern - da der Eintrag für den Vertrag nur auf dem dritten Leaf (Ingress-Richtlinie) oder Leaf102 (Egress-Richtlinie) existieren würde.

Struktur mit überlappenden Subnetzen, die auf separaten externen EPGs als extern deklariert werden

In diesem Szenario betrachten wir Politikkonflikte und potenzielle Fehlklassifizierung aufgrund von sich überschneidenden oder denselben Subnetzen, die als externe Subnetze auf verschiedenen externen EPGs deklariert wurden.

OSPF kündigt Netzwerk an:

10.9.1.0/24

EIGRP kündigt Netzwerk an:

10.9.2.0/24

Wir beginnen mit der Topologie in Abbildung 1, jedoch ohne Verträge. Wir definieren Subnetz 10.9.0.0/16 as 'externes Subnetz für externe EPGs' für EPG auf beiden L3outs.

So sehen die Tabellen auf Leaf1 und 2 aus:

Leaf 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
```

Leaf2:

```
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 diesem Zustand, ohne Verträge, sehen wir keine Fehler auf beiden EPGs. Es wurde noch keine Überschneidung bei Präfixen erkannt!

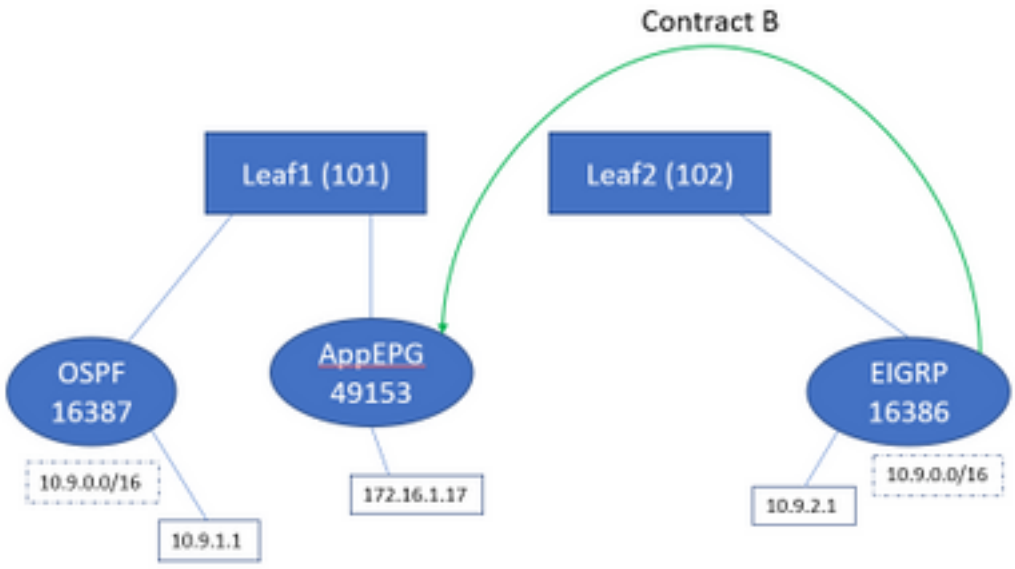
Beim Hinzufügen von Vertrag B tritt ein Fehler in der app-EPG auf (die Vertrag B belegt).

Fault Properties

General | Troubleshooting

Fault Code:	F0467
Severity:	minor
Last Transition:	2019-02-19T18:38:25.436+05:30
Lifecycle:	Raised
Affected Object:	topology/pod-1/node-101/local/svc-policyelem-id-0/cdef-[uni/tn-shparanj/brc-interEPG]/epgCont-[uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure]/fr-[uni/tn-shparanj/brc-interEPG/dirass/cons-[uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure]-any-no]/to-[uni/tn-shparanj/brc-interEPG/dirass/prov-[uni/tn-shparanj/out-eigrp-test/instP-ext-epg]-any-no]/nwissues
Description:	Fault delegate: Configuration failed for uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure due to Prefix Entry Already Used in Another EPG, debug message:
Type:	Config
Cause:	configuration-failed
Change Set:	configQual:prefix-entry-already-in-use, configSt:failed-to-apply, temporaryError:no
Created:	2019-02-19T18:35:59.015+05:30
Code:	F0467
Number of Occurrences:	1
Original Severity:	minor

Topologie:



Schauen wir uns die Änderungen in Tabellen an:

```
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 bleibt unverändert.

Dies zeigt, dass die Zoning-Regel für Vertrag B installiert ist. Das Präfix kann jedoch nicht hinzugefügt werden, da es bereits vorhanden ist - entsprechend der OSPF EPG markiert!

Und genau das warnt uns der Fehler: "Prefix entry already used in other EPG" - der Fehler wird nur ausgelöst, wenn auf einem bestimmten Leaf ein Konflikt zwischen Richtlinie (Zoning-Regeln) und ihrer Anwendung auftritt. Der Fehler wird auf der Consumer-EPG ausgelöst.

Wenn der Datenverkehr von 10.9.2.1 gestartet wird, wird er aufgrund der Richtlinienverweigerung auf Leaf101 fallen gelassen:

```
# 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
```

Wir sehen, dass Antworten von EP 172.16.1.17 auf 10.9.2.1 fallen gelassen werden. Grund:

- Anforderungen aus 10.9.2.1, die aus der Fabric eingehen, sind bereits der Klasse 16386 zugeordnet. Diese wurden mit der Regel-ID 4604 versehen und sind durch
- Antworten von 172.16.1.17 werden mit der Klasse 16387 markiert - diese wird basierend auf den Richtlinien-mgr-Präfixregeln abgerufen. Für 16387 gibt es keine Regel, und diese werden abgelehnt.

In dieser Situation führt eine falsche Klassifizierung dazu, dass der Datenverkehr verworfen wird, obwohl wir die richtige Konfiguration haben (wenn der Fehler ignoriert wird).

Fabric mit dem Präfix 0.0.0.0/0, das auf mehreren externen EPGs als extern deklariert wurde

In diesem Szenario betrachten wir mögliche Fehlklassifizierungen und unerwartete Sicherheitsverletzungen aufgrund der Anwendung von 0.0.0.0/0 als externes Subnetz auf verschiedenen externen EPGs.

OSPF kündigt Netzwerk an:

10.7.7.0/24

EIGRP kündigt Netzwerk an:

10.8.8.0/24

Wir beginnen mit der Topologie in Abbildung 1, jedoch ohne Verträge. Wir definieren Subnetz 0.0.0.0/0 als "externes Subnetz für externe EPGs" für EPG auf beiden L3outs.

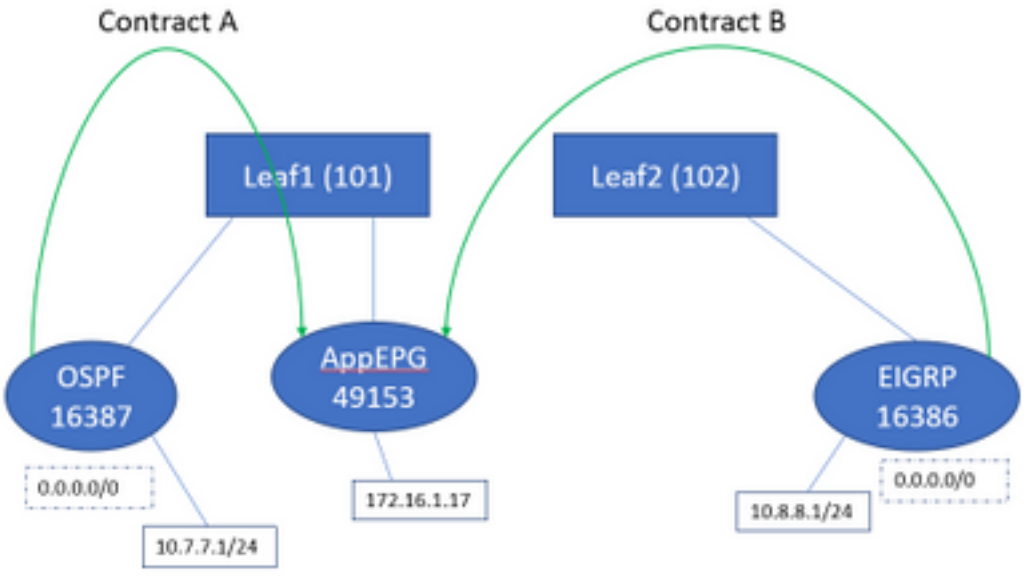
So sehen die Tabellen auf Leaf1 und 2 aus:

Leaf1:

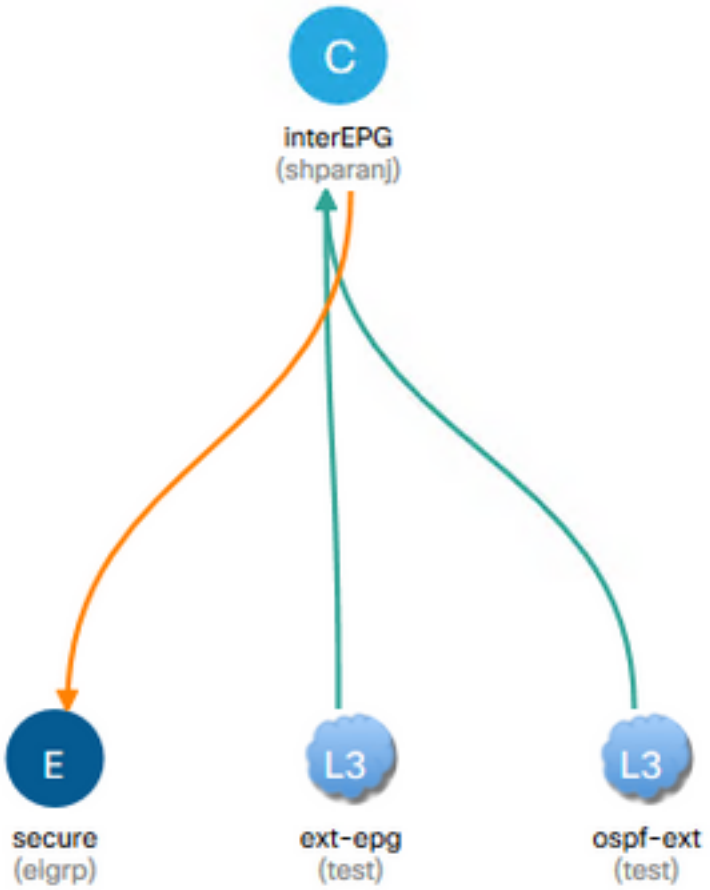
```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
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
```

Leaf2:

```
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
```



Wenn wir beide Verträge A und B hinzufügen, sehen wir immer noch keine Fehler.



Schauen wir uns die Tabellen zu Leafs an:

Leaf1:

```
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
```

Die Tabellen auf Leaf2 bleiben unverändert.

Wir sehen keine Fehler, da es aus der Perspektive der einzelnen Leaf eigentlich keine politischen Konflikte gibt. **Die bei Verwendung von 0.0.0.0/0 als externes EPG hinzugefügten Regel-IDs sind besonders.**

- **Datenverkehr, der von der jeweiligen EPG zu einem der beiden Grenz-Leaf eingeht, ist mit der Klasse 32770 gekennzeichnet - dies ist der pcTag der VRF-Instanz.**
- Die Klasse für diesen Datenverkehr lautet 49153 - das pcTag der app-EPG.
- **Rückverkehr von app-EPG hat 15 Klassen**

ELAM auf 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
```

Auch wenn wir Vertrag A entfernen, kann 10.7.7.1 die Kommunikation mit 172.16.1.17 fortsetzen.

Dies liegt daran, dass die Entfernung von Vertrag A keine Änderungen an den Zoning-Regeln für Leaf1 zur Folge hat.

```
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)
```

Darüber hinaus wird Datenverkehr, der über externe EPG von OSPF eingeht, weiterhin mit dem VRF pcTag markiert, da die EPG noch immer 0.0.0.0/0 als externes Subnetz markiert hat.

Dies führt zu einer Verletzung der Sicherheitsrichtlinien, d. h. zwei EPGs, die ohne Vertrag in einer durchgesetzten VRF-Instanz kommunizieren können.

Weitere Informationen

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