ACI L3Out 문제 해결 - 서브넷 0.0.0.0/0 및 시스템 PcTag 15

목차

소개

이 문서에서는 L3Out EPG에 정의된 경우 0.0.0.0/0 서브넷의 PcTag 파생에 대해 설명합니다.

배경 정보

ACI Contract Guide의 **"L3Out EPG with 0.0.0.0/0 subnet" 섹션**은 0.0.0.0/0을 "External Subnets for the External EPG" 범위 트래픽 분류로 요약합니다.

- 구성된 0.0.0.0/0 서브넷과 일치하는 최장 접두사인 L3Out에서 시작된 트래픽에는 VRF PcTag의 소스 클래스 ID(sclass)가 할당됩니다.
- 구성된 0.0.0.0/0 서브넷과 일치하는 가장 긴 접두사인 L3Out EPG로 향하는 트래픽에는 목적지 클래스 ID(dclass)인 15가 할당됩니다(시스템 PcTag).

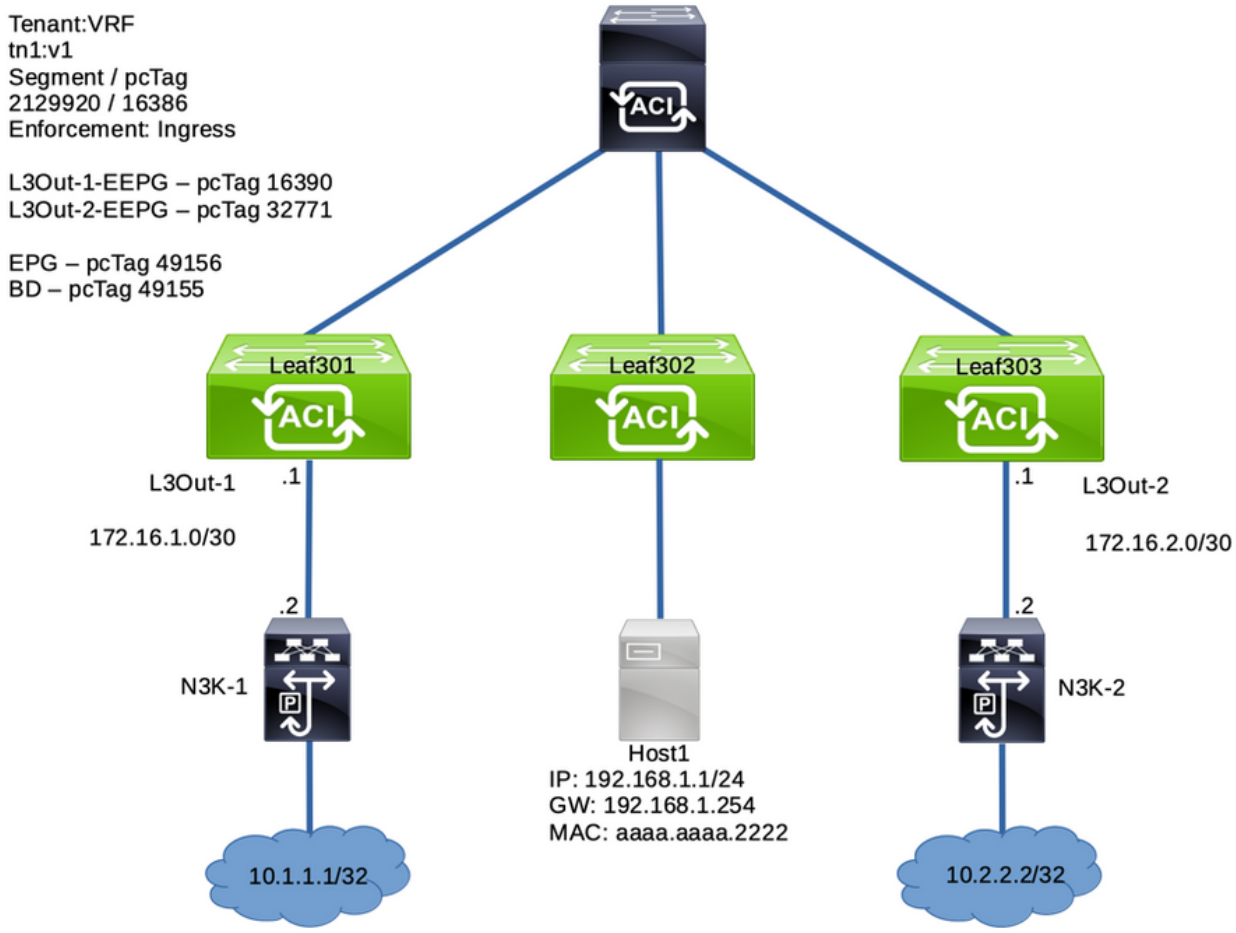
ACI L3Out **백서의 "외부 EPG를 위한 외부 서브넷이 있는 0.0.0.0/0의 예외**" 섹션에는 경고가 있습니다.

"...권장하지 않지만, 동일한 VRF에 있는 여러 L3Out EPG에서 '외부 EPG용 외부 서브넷'을 사용하여 0.0.0.0/0을 구성할 수 있습니다... 이 컨피그레이션이 허용되지만 의도하지 않은 계약 구축이 발생합니다..."

이 문서에서는 의도하지 않은 계약 구축에 대해 설명합니다.

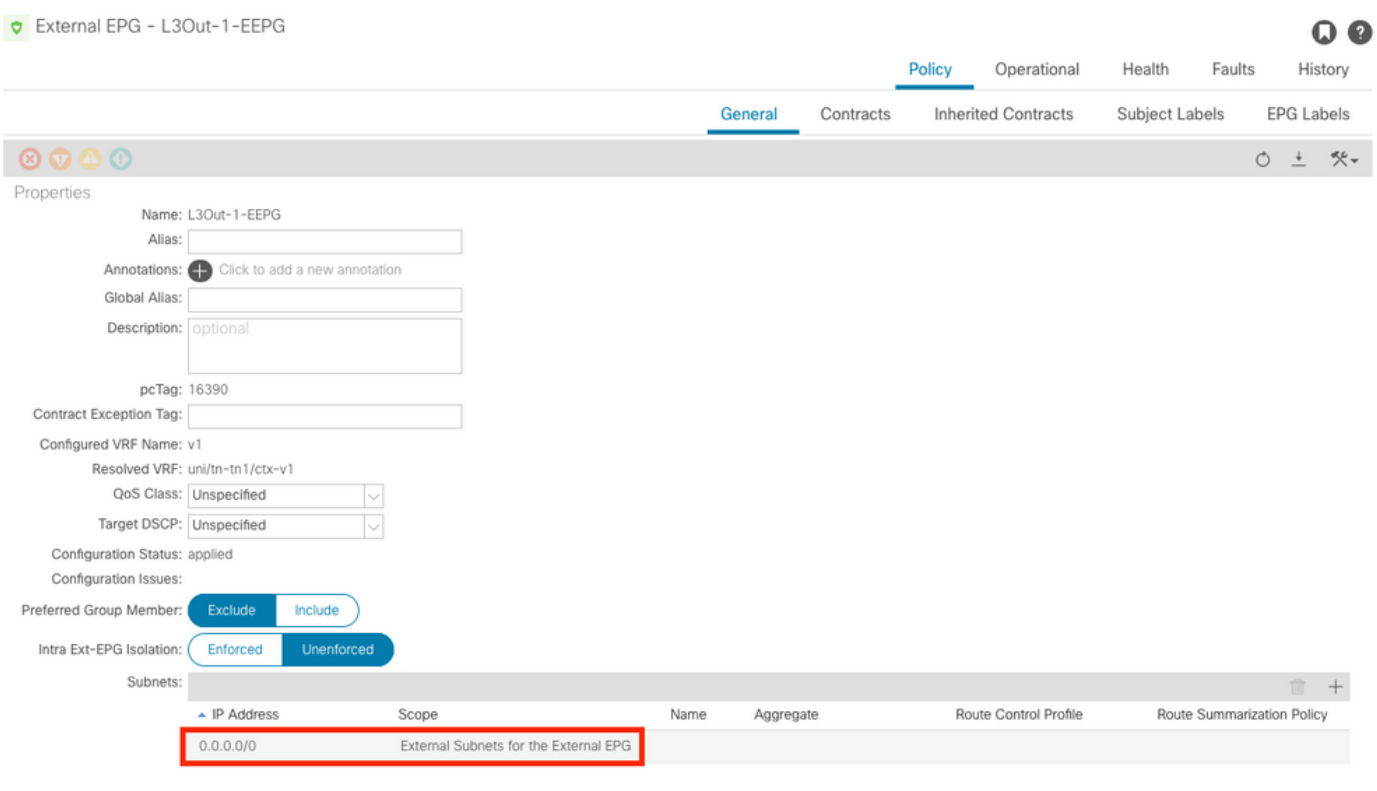
구성

토폴로지 다이어그램



구성 주요 내용

- 리프 노드(301, 303)는 경계 리프 노드이다
- 리프 노드(302)는 비경계 리프(Non-Border Leaf)이다
- 보더 리프 301의 L3Out-1-EPG에는 "외부 EPG용 외부 서브넷"이 포함된 0.0.0.0/0 서브넷이 있습니다.
- L3Out-1-EEPG는 계약을 제공합니다.
- Non-Border Leaf 302의 EPG는 동일한 계약을 소비합니다



다음을 확인합니다.

"인그레스(Ingress)" 정책 시행이 포함된 VRF

비경계 리프 영역 지정 규칙

Background Information(백그라운드 정보) 섹션에서 강조 표시된 것처럼, 구성된 0.0.0.0/0 서브넷에서 가장 긴 접두사가 일치하는 이 L3Out 뒤에 있는 네트워크로 향하는 트래픽은 목적지 클래스(pcTag)를 15로 가져옵니다.

다음은 VRF "v1"에 대한 Non-Border Leaf 302의 zoning-rules 테이블입니다(세그먼트 ID 2129920).

```
Leaf-302#  show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4107  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit | uni-dir | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
```

```
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
```

L3Out-1-EEPG와 EPG(49156) 간의 계약 결과로 설치되는 두 가지 규칙이 있습니다.

- 규칙(4112)은 EPG를 목적지로 하는 0.0.0.0/0 LPM을 사용하여 L3Out EPG에서 소싱된 외부 트래픽을 위한 것입니다. 트래픽 흐름은 VRF PcTag(16386) 및 dclass of EPG(49156)로 분류됩니다.
- 규칙 4111은 0.0.0.0/0 LPM을 사용하여 L3Out EPG로 향하는 EPG에서 발생하는 트래픽에 대한 것입니다. 트래픽 흐름은 EPG(49156) 및 System PcTag 15의 dclass로 분류됩니다

경계 리프 조닝 규칙

VRF 정책 시행이 '인그레스(Ingress)'(기본값)로 설정되었기 때문에 경계 리프 노드 301은 비경계 리프 노드 302와 동일한 조닝 규칙을 가지지 않습니다. 이러한 흐름 유형에 대한 정책은 비경계 리프 노드에 적용될 것으로 예상됩니다.

```
Leaf-301# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name |  Action  |
Priority       |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
|   4105  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |      |  permit  |
any_any_filter(17)  |
|   4107  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |      | deny,log |
any_any_any(21)     |
|   4106  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |      | deny,log |
any_vrf_any_deny(22) |
|   4108  |   0    | 16387  | implicit | uni-dir | enabled | 2129920 |      |  permit  |
any_dest_any(16)    |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+

*No entry for 16386 to 49156 , or 49156 to 15*
```

L3Out ELAM에 대한 EPG

EPG 엔드포인트 192.168.1.1에서 L3Out-1-EPG 뒤의 IP로 ping했습니다.

```
Host# ping 10.1.1.1 count 10000 int 1
PING 10.1.1.1 (10.1.1.1): 56 data bytes
64 bytes from 10.1.1.1: icmp_seq=0 ttl=252 time=1.063 ms
64 bytes from 10.1.1.1: icmp_seq=1 ttl=252 time=0.92 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=252 time=0.963 ms
```

Non-Border Leaf 302(EPG 게이트웨이)의 L3Out 트래픽에 대한 EPG의 ELAM은 다음을 확인합니다.

1. 패킷에 예상 소스 및 대상 IP가 있습니다. 소스 IP:192.168.1.1, 대상 IP: 10.1.1.1
2. 소스 클래스(sclass)는 EPG PcTag **49156**

3. 대상 클래스(dclass)는 System PcTag **15**입니다. 10.1.1.0/24 가장 긴 접두사가 L3Out-1-EEPG의 0.0.0.0/0 서브넷과 일치합니다
4. 비경계 리프 노드인 이 노드(302)에 정책이 적용되었습니다.

```
Leaf-302# ereport
================================================================================================================
=====================================================
                                                                    Captured Packet
================================================================================================================
=====================================================
...snip...
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Destination MAC               : 0022.BDF8.19FF
Source MAC                    : AAAA.AAAA.2222
802.1Q tag is valid           : yes( 0x1 )
CoS                           : 0( 0x0 )
Access Encap VLAN             : 192( 0xC0 )

----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
L3 Type                       : IPv4
...
IP Protocol Number            : ICMP
IP CheckSum                   : 63781( 0xF925 )
Destination IP                : 10.1.1.1
Source IP                     : 192.168.1.1
...
================================================================================================================
=====================================================
                                                                Contract Lookup ( FPC )
================================================================================================================
=====================================================

----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                             : ICMP( 0x1 )
L4 Src Port                             : 2048( 0x800 )
L4 Dst Port                             : 43014( 0xA806 )
sclass (src pcTag)                      : 49156( 0xC004 )
dclass (dst pcTag)                      : 15( 0xF )
src pcTag is from local table           : yes
...

----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Result
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Drop                           : no
Contract Logging                        : no
Contract Applied                        : yes
```

```
Contract Hit                            : yes
Contract Aclqos Stats Index             : 81875
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875" )
```

오류가 발생한 Zoning-Rule에 대한 추가 검증을 위해 ereport에서 제공하는 명령을 입력할 수 있습니다.

```
module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875"
========================================
Rule ID: 4111 Scope 6 Src EPG: 49156 Dst EPG: 15 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 46 | hw_index = 45 | stats_idx = 81875

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81875
```

EPG ELAM으로 L3Out

반환 흐름은 비경계 리프 노드 302에 적용되는 정책을 가져옵니다. 이는 VRF 정책 시행이 "인그레스"로 설정된 경우에 필요합니다.

```
Leaf-302# ereport
...
-------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Inner L3 Header
-------------------------------------------------------------------------------------------------------
-----------------------------------------------------
L3 Type                         : IPv4
DSCP                            : 0
Don't Fragment Bit              : 0x0
TTL                             : 254
IP Protocol Number              : ICMP
Destination IP                  : 192.168.1.1
Source IP                       : 10.1.1.1

=======================================================================================================
=====================================================
                                                                    Contract Lookup ( FPC )
=======================================================================================================
=====================================================

-------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
-------------------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                             : ICMP( 0x1 )
L4 Src Port                             : 0( 0x0 )
L4 Dst Port                             : 60691( 0xED13 )
sclass (src pcTag)                      : 16386( 0x4002 )
dclass (dst pcTag)                      : 49156( 0xC004 )
src pcTag is from local table           : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet          : no
```

```
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                          : no
Contract Logging                       : no
 Contract Applied                       : yes
 Contract Hit                           : yes
 Contract Aclqos Stats Index            : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
```

추가 검증:

```
module-1(DBG-elam-insel14)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874"
========================================
Rule ID: 4112 Scope 6 Src EPG: 16386 Dst EPG: 49156 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 47 | hw_index = 46 | stats_idx = 81874

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81874
module-1(DBG-elam-insel14)#
```

"이그레스(Egress)" 정책 시행을 사용하는 VRF

비경계 리프 영역 지정 규칙

VRF 정책 시행이 "이그레스(Egress)"로 설정된 경우 L3Out에 대한 계약 규칙이 경계 리프 노드와 비경계 리프 노드에 구축됩니다. 따라서 이 컨피그레이션은 "Ingress" 시행과 비교하여 추가 TCAM 공간을 사용합니다. 이 컨피그레이션은 기본값이 아니므로 사용하는 경우 신중하게 고려해야 합니다.

Non-Border Leaf Node(302)에는 2개의 Zoning-Rule이 있는데, 이는 플로우 방향성마다 하나씩 있습니다.

```
Leaf-302# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4107  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit | uni-dir | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
```

```
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
```

경계 리프 조닝 규칙

"이그레스(Egress)" 정책 시행을 통해 Border Leaf Node 301에는 두 개의 추가 영역 지정 규칙도 있습니다.

```
Leaf-301# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4105  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4107  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4106  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4108  |   0    | 16387  | implicit | uni-dir | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4109  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4110  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
```

L3Out ELAM에 대한 EPG

엔드포인트 192.168.1.1에서 L3Out을 지원하는 네트워크로 ping이 성공했습니다.

```
Host# ping 10.1.1.1 count 10000 int 1
PING 10.1.1.1 (10.1.1.1): 56 data bytes
64 bytes from 10.1.1.1: icmp_seq=0 ttl=252 time=1.319 ms
64 bytes from 10.1.1.1: icmp_seq=1 ttl=252 time=0.962 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=252 time=0.958 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=252 time=1.093 ms
```

비경계 리프 노드(302)의 ELAM은 정책이 **이 리프**에 **적용되지** 않았음을 나타낸다. 또한 **System** PcTag **1**의 dclass를 선택하여 플로우의 다음 리프 노드에 플로우를 히팅합니다.

```
Leaf-302# ereport
================================================================================================
=================================================
                                                                  Captured Packet

------------------------------------------------------------------------------------------------
-------------------------------------------------
Outer L3 Header
```

```
--------------------------------------------------------------------------------------------------
--------------------------------------------------
...
IP Protocol Number            : ICMP
IP CheckSum                   : 26943( 0x693F )
Destination IP                : 10.1.1.1
Source IP                     : 192.168.1.1

==================================================================================================
==================================================
                                                                    Contract Lookup ( FPC )
==================================================================================================
==================================================

--------------------------------------------------------------------------------------------------
--------------------------------------------------
Contract Lookup Key
--------------------------------------------------------------------------------------------------
--------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 2048( 0x800 )
L4 Dst Port                           : 27360( 0x6AE0 )
sclass (src pcTag)                    : 49156( 0xC004 )
dclass (dst pcTag)                    : 1( 0x1 )
...

--------------------------------------------------------------------------------------------------
--------------------------------------------------
Contract Result
--------------------------------------------------------------------------------------------------
--------------------------------------------------
Contract Drop                         : no
Contract Logging                      : no
Contract Applied                      : no
Contract Hit                          : yes
Contract Aclqos Stats Index           : 81903
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81903" )
```

보더 리프 노드(301)의 ELAM은 정책이 **이 노드에 적용되었음을** 나타낸다. 또한 **System PcTag 15**의 dclass를 가져왔습니다. 즉, 0.0.0.0/0 L3Out 서브넷 항목에서 Longest-Prefix가 일치합니다.

```
Leaf-301# ereport
==================================================================================================
==================================================
                                                                  Captured Packet
==================================================================================================
==================================================

--------------------------------------------------------------------------------------------------
--------------------------------------------------
Inner L3 Header
--------------------------------------------------------------------------------------------------
--------------------------------------------------
...
IP Protocol Number            : ICMP
Destination IP                : 10.1.1.1
Source IP                     : 192.168.1.1

==================================================================================================
==================================================
                                                                    Contract Lookup ( FPC )
```

```
================================================================================================
================================================

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 40498( 0x9E32 )
sclass (src pcTag)                       : 49156( 0xC004 )
dclass (dst pcTag)                       : 15( 0xF )
src pcTag is from local table            : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet           : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                            : no
Contract Logging                         : no
Contract Applied                         : yes
Contract Hit                             : yes
Contract Aclqos Stats Index              : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
...

module-1(DBG-elam-insel14)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874"
========================================
Rule ID: 4110 Scope 6 Src EPG: 49156 Dst EPG: 15 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 47 | hw_index = 46 | stats_idx = 81874

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81874
```

EPG ELAM으로 L3Out

이 설정에는 반환 플로우에 대한 주의 사항이 있습니다.

- Border Leaf Node 301에는 192.168.1.1에 대한 엔드포인트가 없습니다.

```
Leaf-301# show endpoint ip 192.168.1.1
Legend:
S - static s - arp L - local O - peer-attached
V - vpc-attached a - local-aged p - peer-aged M - span
B - bounce H - vtep R - peer-attached-rl D - bounce-to-proxy
E - shared-service m - svc-mgr
+-----------------------------------+---------------+-----------------+--------------+----------
---+
VLAN/ Encap MAC Address MAC Info/ Interface
Domain VLAN IP Address IP Info
+-----------------------------------+---------------+-----------------+--------------+----------
```

```
---+
...empty...
```

그 결과, 정책은 이 흐름에 대해 Border Leaf Node 301에 적용되지 않으며 다음 leaf에 도달하도록 암시적으로 허용되어야 합니다.

```
Leaf-301# ereport
================================================================================================================
================================================
                                                                    Captured Packet
================================================================================================================
================================================
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
...
IP Protocol Number            : ICMP
IP CheckSum                   : 25157( 0x6245 )
Destination IP                : 192.168.1.1
Source IP                     : 10.1.1.1

================================================================================================================
================================================
                                                                        Contract Lookup ( FPC )
================================================================================================================
================================================

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 0( 0x0 )
L4 Dst Port                           : 33570( 0x8322 )
sclass (src pcTag)                    : 16386( 0x4002 )
dclass (dst pcTag)                    : 1( 0x1 )
src pcTag is from local table         : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet        : no
If yes, Contract is not applied here because it is flooded

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                         : no
Contract Logging                      : no
Contract Applied                      : no
Contract Hit                          : yes
Contract Aclqos Stats Index           : 81903
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81903" )
```

그 대신, 정책은 비경계 리프 노드(302)에 적용된다:

```
Leaf-302# ereport
================================================================================================================
================================================
```

```
                                                                    Captured Packet
================================================================================================================
================================================

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Inner L3 Header
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
...
IP Protocol Number            : ICMP
Destination IP                : 192.168.1.1
Source IP                     : 10.1.1.1

================================================================================================================
================================================
                                                                          Contract Lookup ( FPC )
================================================================================================================
================================================

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                             : ICMP( 0x1 )
L4 Src Port                             : 0( 0x0 )
L4 Dst Port                             : 61057( 0xEE81 )
sclass (src pcTag)                      : 16386( 0x4002 )
dclass (dst pcTag)                      : 49156( 0xC004 )
src pcTag is from local table           : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet          : no
If yes, Contract is not applied here because it is flooded

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                           : no
Contract Logging                        : no
Contract Applied                        : yes
Contract Hit                            : yes
Contract Aclqos Stats Index             : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
...

module-1(DBG-elam-insel14)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874"
========================================
Rule ID: 4112 Scope 6 Src EPG: 16386 Dst EPG: 49156 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 47 | hw_index = 46 | stats_idx = 81874

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81874
```

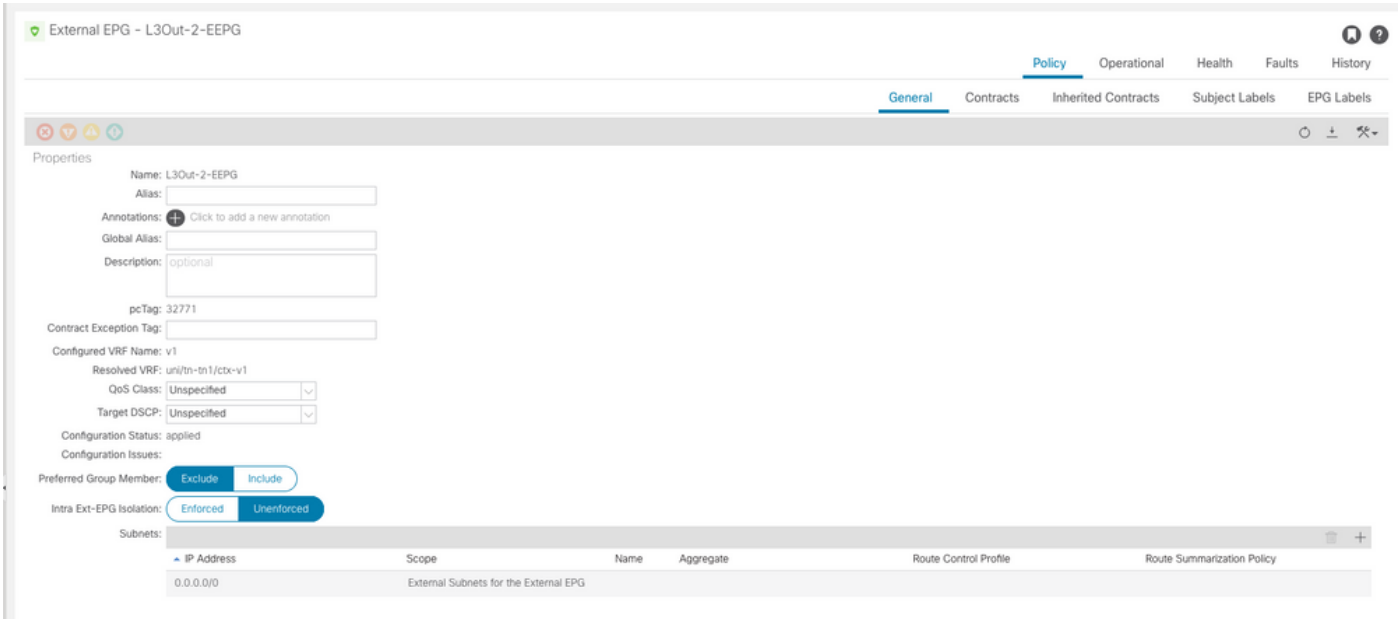
보더 리프 노드 301에 192.168.1.1을 학습하는 엔드포인트가 있는 경우 해당 노드에 정책이 적용되었을 것입니다.

문제 해결

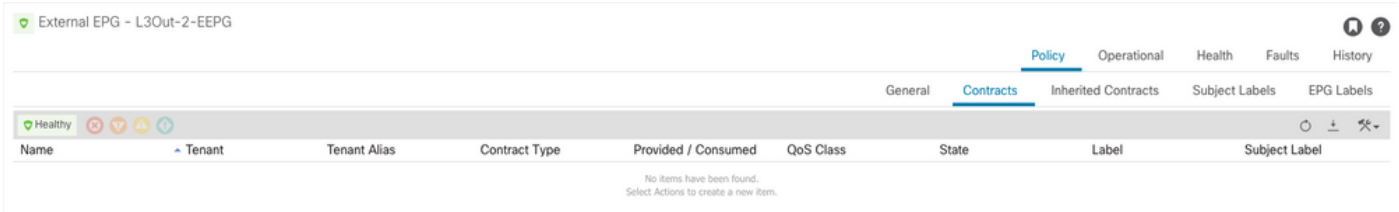
시나리오 - 의도하지 않은 허용

동일한 VRF에 L3Out이 여러 개 있는 구축에서 0.0.0.0/0 서브넷을 "외부 EPG용 외부 서브넷"으로 구성하면 트래픽이 예기치 않게 외부 대상으로 전달될 수 있습니다.

이를 유도하려면 L3Out-1-EEPG와 동일한 VRF에 있는 L3Out-2-EEPG 아래에 0.0.0.0/0 서브넷을 추가합니다.



L3Out-2-EEPG에는 계약이 없으므로 기본적으로 모든 트래픽이 삭제될 것으로 예상됩니다.



그러나 EPG 엔드포인트 192.168.1.1에서 L3Out-2-EPG 뒤의 대상 10.2.2.2로의 ping이 성공했습니다. 예상치 못한 일입니다!

```
Host# ping 10.2.2.2
PING 10.2.2.2 (10.2.2.2): 56 data bytes
64 bytes from 10.2.2.2: icmp_seq=0 ttl=252 time=0.881 ms
64 bytes from 10.2.2.2: icmp_seq=1 ttl=252 time=0.801 ms
64 bytes from 10.2.2.2: icmp_seq=2 ttl=252 time=0.877 ms
64 bytes from 10.2.2.2: icmp_seq=3 ttl=252 time=0.827 ms
```

전달 경로 및 policy-mgr 접두사는 모두 이 VRF에서 10.2.2.2로 향하는 트래픽에 시스템 PcTag 15가 할당됨을 보여줍니다

```
Leaf-302# vsh_lc -c "show forward route 10.2.2.2 platform vrf tn1:v1"
...
Policy Prefix 0.0.0.0/0
```

```
SDK Information:
vrf: 7(0x7), routed_if: 0x0 epc_class: 15(0xf)
...


Leaf-302# vsh -c "show system internal policy-mgr prefix"
Requested prefix data

Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                     Addr
Class Shared Remote Complete Svc_ena
======= ======  =========== =======  ============================
================================ ====== ====== ====== ======== ========
...
2129920 7      0x7           Up     tn1:v1
0.0.0.0/0   15      False  False  False    False
2129920 7      0x80000007    Up     tn1:v1
::/0   15      False  False  False    False

Leaf-302#
```

비경계 리프 노드(302) 상의 ELAM은 트래픽이 dclass of System PcTag 15로 분류되는지 검증한다.

```
Leaf-302# ereport
================================================================================================================
================================================== Captured Packet
================================================================================================================
================================================== ----------------------------------------
--------------------------------------------------------------------------------------------------------
------------- Outer L3 Header ------------------------------------------------------------------------
-------------------------------------------------------------------------------- ... IP
Protocol Number : ICMP IP CheckSum : 14444( 0x386C ) Destination IP                : 10.2.2.2
Source IP                      : 192.168.1.1

================================================================================================================
==================================================
                                                                  Contract Lookup ( FPC )
================================================================================================================
==================================================

--------------------------------------------------------------------------------------------------------
----------------------------------------------------
Contract Lookup Key
--------------------------------------------------------------------------------------------------------
----------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 2048( 0x800 )
L4 Dst Port                           : 33134( 0x816E )
sclass (src pcTag)                    : 49156( 0xC004 )
dclass (dst pcTag)                    : 15( 0xF )
src pcTag is from local table         : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet        : no
If yes, Contract is not applied here because it is flooded

--------------------------------------------------------------------------------------------------------
----------------------------------------------------
Contract Result
--------------------------------------------------------------------------------------------------------
----------------------------------------------------
```

```
Contract Drop                           : no
Contract Logging                        : no
Contract Applied                        : yes
Contract Hit                            : yes
Contract Aclqos Stats Index             : 81875
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875" )
...

module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875"
========================================
Rule ID: 4111 Scope 6 Src EPG: 49156 Dst EPG: 15 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 46 | hw_index = 45 | stats_idx = 81875

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81875
```

VRF "v1"에 대한 영역 지정 규칙은 EPG 및 L3Out-2에 대한 새 항목을 표시하지 않습니다.

```
Leaf-302# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4107  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit | uni-dir | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
Leaf-302#
```

L3Out-2-EEPG에는 0.0.0.0/0 서브넷만 구성되어 있으므로 목적지가 지정된 모든 트래픽은 dclass of System PcTag 15로 분류됩니다.

Zoning-Rules ID 4111 및 4112는 L3Out-1-EEPG가 0.0.0.0/0 서브넷을 모두 가지며 EPG에서 사용하는 계약을 제공하기 때문에 프로그래밍됩니다.

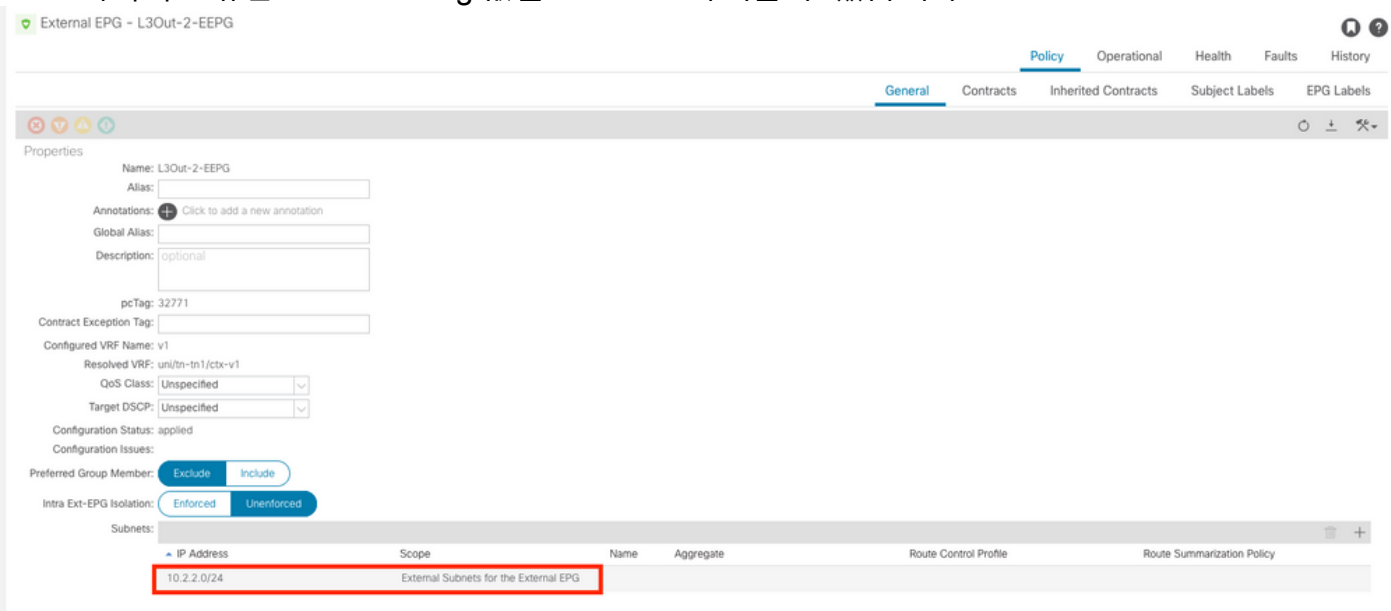
이 컨피그레이션으로 인해 L3Out-2-EEPG로의 흐름이 예기치 않게 허용됩니다.

솔루션 - 의도하지 않은 허용

이 동작을 방지하려면

1. VRF당 하나의 L3Out EPG에서만 0.0.0.0/0 서브넷을 사용하는 것이 좋습니다

2. 가능한 경우 동일한 VRF의 다른 L3Out에 대해 특정 서브넷을 사용합니다. 이렇게 하면 트래픽에서 고유한 L3Out PcTag 값을 dclass로 가져올 수 있습니다.



이러한 변경 사항을 적용하여 예기치 않은 허용 시간을 줄입니다.

1. L3Out-2-EEPG에서 0.0.0.0/0 서브넷을 10.2.2.0/24 서브넷으로 교체합니다
2. L3Out-2-EEPG에서 계약을 제공합니다.
3. EPG에서 동일한 계약을 사용합니다

완료되면, 비경계 리프 노드(302)에서 이러한 변화를 관찰한다.

- 10.2.2.0/24에 대한 더 구체적인 policy-mgr 접두사가 L3Out-2-EEPG PcTag 서버와 연결되어 32771
- Zoning-Rules ID 4109 항목이 있습니다. 이 항목은 EPG PcTag 서버에서 L3Out-2-EPG PcTag 49156으로의 흐름을 32771
- Zoning-Rules ID 4110 항목이 있습니다. 이 엔트리는 L3Out-2-EPG PcTag 스위치에서 EPG PcTag 32771으로 흐름을 49156

10.2.2.2에 L3Out-2-EEPG PgTag가 할당되었음을 나타내는 업데이트된 전달 경로 및 policy-mgr 32771:

```
Leaf-302# vsh_lc -c "show forward route 10.2.2.2 platform vrf tn1:v1"
...
Policy Prefix 10.2.2.0/24
...
SDK Information:
vrf: 7(0x7), routed_if: 0x0 epc_class: 32771(0x8003)
attributes: SUP_CP DST_POL_IC SRC_POL_IC

Leaf-302# vsh -c "show system internal policy-mgr prefix"
Requested prefix data

Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                        Addr
Class Shared Remote Complete Svc_ena
======= ======  ========== =======  ============================
================================ ====== ====== ====== ======== ========
...
2129920 7      0x7           Up     tn1:v1
0.0.0.0/0   15      False  False  False    False
2129920 7      0x80000007    Up     tn1:v1
```

```
::/0   15      False  False  False    False
2129920 7      0x7           Up     tn1:v1
10.2.2.0/24  32771   False  True   False    False
```

참고: L3Out-1-EEPG가 여전히 0.0.0.0/0 서브넷을 가지며 EPG와 계약 관계를 가지기 때문에 영역 지정 규칙 ID 4111 및 4112는 여전히 비경계 리프 노드 302에 존재합니다. 그러나 L3Out-2-EEPG 트래픽은 해당 트래픽이 시스템 PcTag 15가 아니라 L3Out PcTag로 분류되므로 더 이상 실수로 해당 규칙을 사용하지 않습니다.

```
Leaf-302# show zoning-rule scope 2129920
+---------+--------+--------+----------+----------------+---------+---------+------------------
+----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------------------
+----------+----------------------+
|   4107  |   0    |   0    | implarp  |    uni-dir     | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit |    uni-dir     | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit |    uni-dir     | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit |    uni-dir     | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  |    uni-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  |    uni-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4109  | 49156  | 32771  | default  |     bi-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4110  | 32771  | 49156  | default  | uni-dir-ignore | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------------------
+----------+----------------------+
```

EPG 호스트에서 L3Out-2-EEPG 뒤의 외부 대상으로 Ping했습니다.

```
Host# ping 10.2.2.2
PING 10.2.2.2 (10.2.2.2): 56 data bytes
64 bytes from 10.2.2.2: icmp_seq=0 ttl=252 time=0.854 ms
64 bytes from 10.2.2.2: icmp_seq=1 ttl=252 time=0.669 ms
64 bytes from 10.2.2.2: icmp_seq=2 ttl=252 time=0.716 ms
64 bytes from 10.2.2.2: icmp_seq=3 ttl=252 time=0.669 ms
64 bytes from 10.2.2.2: icmp_seq=4 ttl=252 time=0.666 ms
```

비경계 리프 노드(302)의 icmp 요청에 대한 ELAM은 dclass가 이제 32771(L3Out-2-EEPG의 PcTag)임을 나타냅니다.

```
Leaf-302# ereport
================================================================================================================
=====================================================
                                                                  Captured Packet
================================================================================================================
=====================================================
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Outer L3 Header
```

```
------------------------------------------------------------------------------------------------------
------------------------------------------------
...
IP Protocol Number : ICMP
IP CheckSum : 4095( 0xFFF )
Destination IP : 10.2.2.2
Source IP : 192.168.1.1

======================================================================================================
================================================
                                                                        Contract Lookup ( FPC )
======================================================================================================
================================================
------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 49837( 0xC2AD )
sclass (src pcTag)                       : 49156( 0xC004 )
dclass (dst pcTag)                       : 32771( 0x8003 )
src pcTag is from local table            : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet           : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                            : no
Contract Logging                         : no
Contract Applied                         : yes
Contract Hit                             : yes
Contract Aclqos Stats Index              : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
...
```

ereport provided aclqos 명령은 이 플로우가 새로운 Zoning-Rules 중 하나, 특히 Rule ID 4109에 도달함을 보여줍니다.

```
module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873"
========================================
Rule ID: 4109 Scope 6 Src EPG: 49156 Dst EPG: 32771 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 48 | hw_index = 47 | stats_idx = 81873

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81873
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.