# Troubleshoot ACI L3Out - Subnet 0.0.0.0/0 and System PcTag 15

## Contents


Introduction
Background Information
Configure
Topology Diagram
Configuration Highlights
Verify
VRF with "Ingress" Policy Enforcement
Non-Border Leaf Zoning-Rules
Border Leaf Zoning-Rules
EPG to L3Out ELAM
L3Out to EPG ELAM
VRF with "Egress" Policy Enforcement
Non-Border Leaf Zoning-Rules
Border Leaf Zoning-Rules
EPG to L3Out ELAM
L3Out to EPG ELAM
Troubleshoot
Scenario - Unintended Allows
Solution - Unintended Allows


## Introduction

This document describes the PcTag derivation of the 0.0.0.0/0 subnet when defined in an L3Out EPG.

## Background Information

The **"L3Out EPG with 0.0.0.0/0 subnet"** section of the ACI Contract Guide summarizes 0.0.0.0/0 with "External Subnets for the External EPG" scope traffic classification as:

- Traffic sourced from an L3Out which is Longest Prefix Matched to a configured 0.0.0.0/0 subnet is assigned the source class ID (sclass) of the VRF PcTag.
- Traffic destined to an L3Out EPG which is Longest Prefix Matched to a configured 0.0.0.0/0 subnet is assigned the destination class ID (dclass) of 15, a System PcTag.

The **"An exception for 0.0.0.0/0 with External Subnets for the External EPG"** section of the ACI L3Out Whitepaper contains a warning:

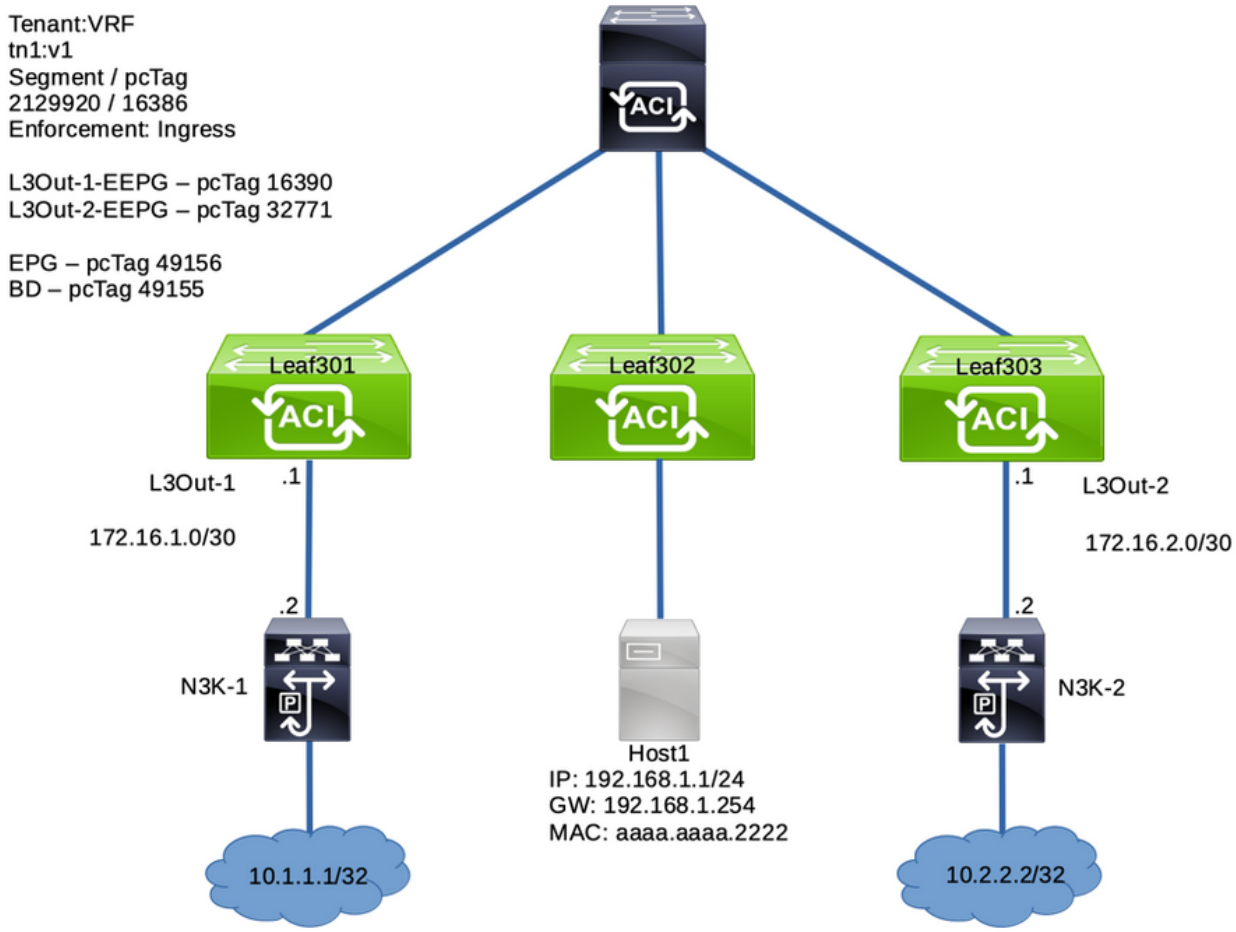
"...Although it is not recommended, you can configure 0.0.0.0/0 with 'External Subnets for the External EPG' in multiple L3Out EPGs in the same VRF... While this configuration is allowed, an

unintended contract deployment occurs..."

This article dives into that unintended contract deployment.

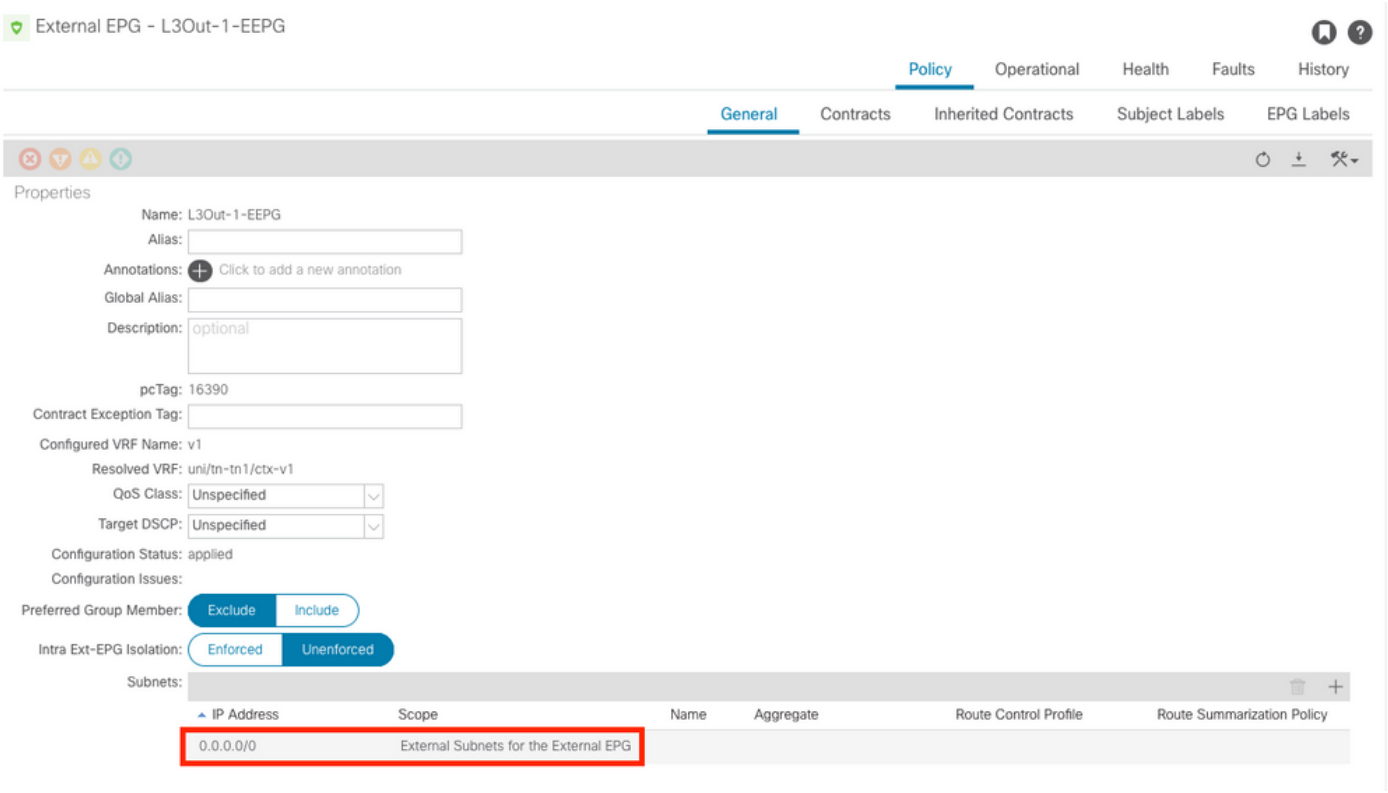
# Configure

## Topology Diagram




## Configuration Highlights

- Leaf Nodes 301 and 303 are Border Leaf Nodes
- Leaf Node 302 is a Non-Border Leaf
- L3Out-1-EEPG, on Border Leaf 301, has a 0.0.0.0/0 subnet with "External Subnets for the External EPG"
- L3Out-1-EEPG provides a contract
- EPG, on Non-Border Leaf 302, consumes the same contract




# Verify

## VRF with "Ingress" Policy Enforcement

### Non-Border Leaf Zoning-Rules

As highlighted in the Background Information section, traffic destined to networks behind this L3Out which Longest Prefix Match on the configured 0.0.0.0/0 subnet get a destination class (pcTag) of 15.

This is the zoning-rules table on Non-Border Leaf 302 for VRF "v1" (segment 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)     |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
```

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

There are two rules installed as a result of the contract between L3Out-1-EEPG and EPG (49156):

- Rule 4112 is for external traffic sourced from the L3Out EPG with 0.0.0.0/0 LPM destined to the EPG. The traffic flow is classified with the sclass of the VRF PcTag (16386) and dclass of EPG (49156) .
- Rule 4111 is for traffic sourced from the EPG destined to the L3Out EPG with 0.0.0.0/0 LPM. The traffic flow is classified with the sclass of EPG (49156) and the dclass of System PcTag 15

### Border Leaf Zoning-Rules

Border Leaf Node 301 does not have the same Zoning-Rules as Non-Border Leaf Node 302 due to VRF Policy Enforcement set to 'Ingress' (default value). Policy for these types of flows is expected to be applied on Non-Border Leaf Nodes.

```
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***

### EPG to L3Out ELAM

A ping from EPG endpoint 192.168.1.1 to the IP behind L3Out-1-EEPG is successful:

```
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
```

An ELAM for EPG to L3Out traffic on Non-Border Leaf 302 (EPG gateway) confirms:

1. The packet has the expected source and destination IPs: Source IP:192.168.1.1, Destination IP: 10.1.1.1
2. The source class (sclass) is the EPG PcTag **49156**

3. The destination class (dclass) is System PcTag **15**, as 10.1.1.0/24 Longest Prefix Matches the 0.0.0.0/0 Subnet on L3Out-1-EEPG
4. Policy was applied on this node 302, the Non-Border Leaf Node.

```
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" )
```

The command given by ereport can be entered for additional validation of the Zoning-Rule that was hit:

```
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
```

## L3Out to EPG ELAM

The return flow gets policy applied on the Non-Border Leaf Node 302. This is expected when VRF Policy Enforcement is set to "Ingress".

```
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" )
```

Further validation:

```
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)#
```

## VRF with "Egress" Policy Enforcement

### Non-Border Leaf Zoning-Rules

With VRF Policy Enforcement set to "Egress", contract rules for an L3Out are deployed on both Border Leaf and Non–Border Leaf Nodes. As a result, this configuration consumes additional TCAM space compared to "Ingress" Enforcement. This configuration is not the default value, and if used, must be carefully considered.

Non-Border Leaf Node 302 has two Zoning-Rules, one per flow directionality:

```
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)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
```

### Border Leaf Zoning-Rules

With "Egress" Policy Enforcement, Border Leaf Node 301 also has two additional Zoning-Rules:

```
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)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
```

### EPG to L3Out ELAM

A ping from the endpoint 192.168.1.1 to the network behind the L3Out is successful:

```
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
```

The ELAM on Non-Border Leaf Node 302 indicates that **policy was not applied** on this leaf. Additionally, it picked up a dclass of **System PcTag 1** to allow the flow to hit the next leaf node in the flow:

```
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" )
```

The ELAM on Border Leaf Node 301 indicates that **policy was applied on this node**. It also picked up a dclass of **System PcTag 15.** This means it Longest-Prefix Matched on the 0.0.0.0/0 L3Out Subnet entry:

```
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
```

## L3Out to EPG ELAM

There is a caveat with the return flow in this setup:

- Border Leaf Node 301 does not have an endpoint learn for 192.168.1.1.

```
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...
```

As a result, policy is not applied on Border Leaf Node 301 for this flow and it must be implicitly allowed to reach the next leaf:

```
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" )
```

Instead, policy is applied on Non-Border Leaf Node 302:

```
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
```

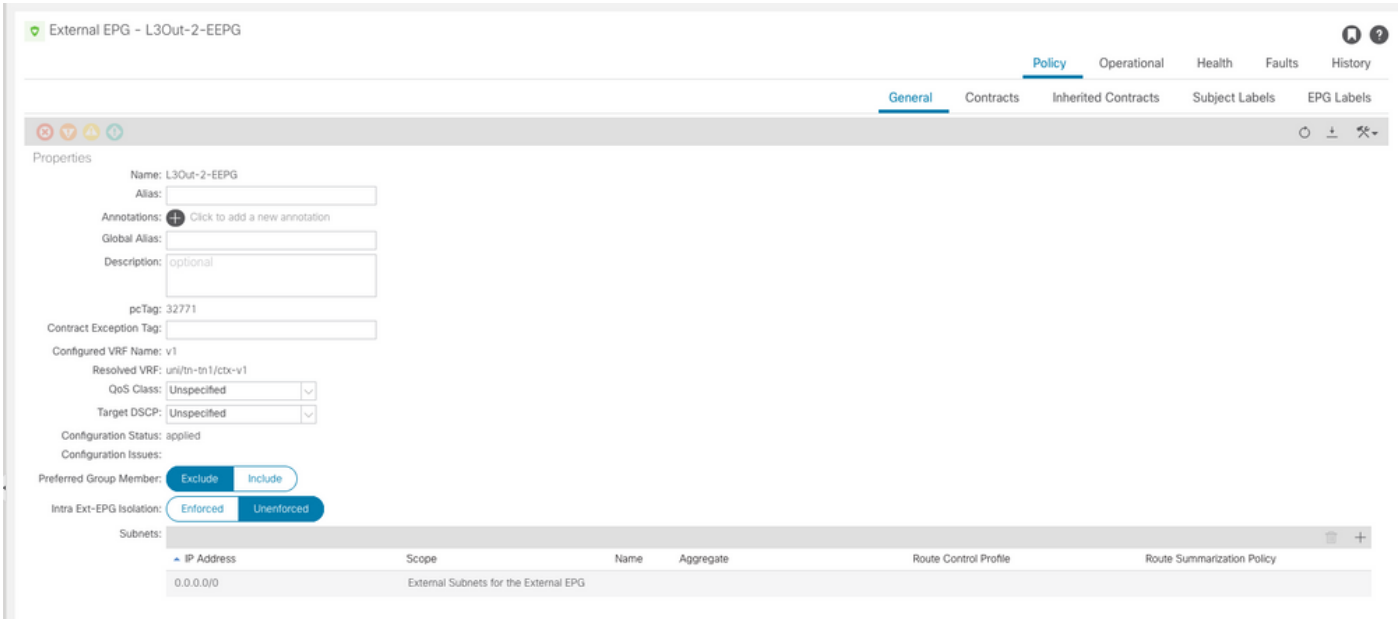
If Border Leaf Node 301 had an endpoint learn 192.168.1.1, policy would have been applied on that node.

# Troubleshoot

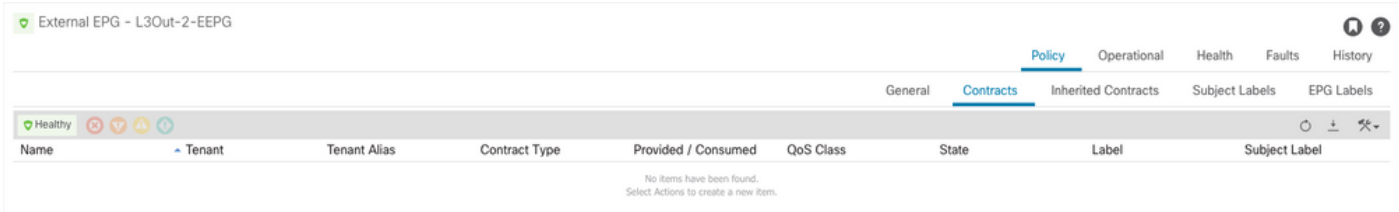
## Scenario - Unintended Allows

A deployment with multiple L3Outs in the same VRF configured with the 0.0.0.0/0 Subnet with “External Subnets for the External EPG” can allow traffic to pass to external destinations unexpectedly.

To induce this, add the 0.0.0.0/0 Subnet under L3Out-2-EEPG which is in the same VRF as L3Out-1-EEPG.




**There are no contracts on L3Out-2-EEPG, so we would expect all traffic to be dropped by default:**




However, a ping from EPG endpoint 192.168.1.1 to destination 10.2.2.2 behind L3Out-2-EEPG is successful. This is unexpected!

```
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
```

The forward route and policy-mgr prefix both show that traffic destined to 10.2.2.2 in this VRF is assigned System PcTag 15

```
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#
```

An ELAM on Non-Border Leaf Node 302 validates that traffic is classified with a dclass of System PcTag 15.

```
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
```

The Zoning-Rules for VRF "v1" do not show any new entries for EPG and L3Out-2:

```
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#
```

As L3Out-2-EEPG only has the 0.0.0.0/0 Subnet configured, all traffic destined to it is classified with dclass of System PcTag 15.

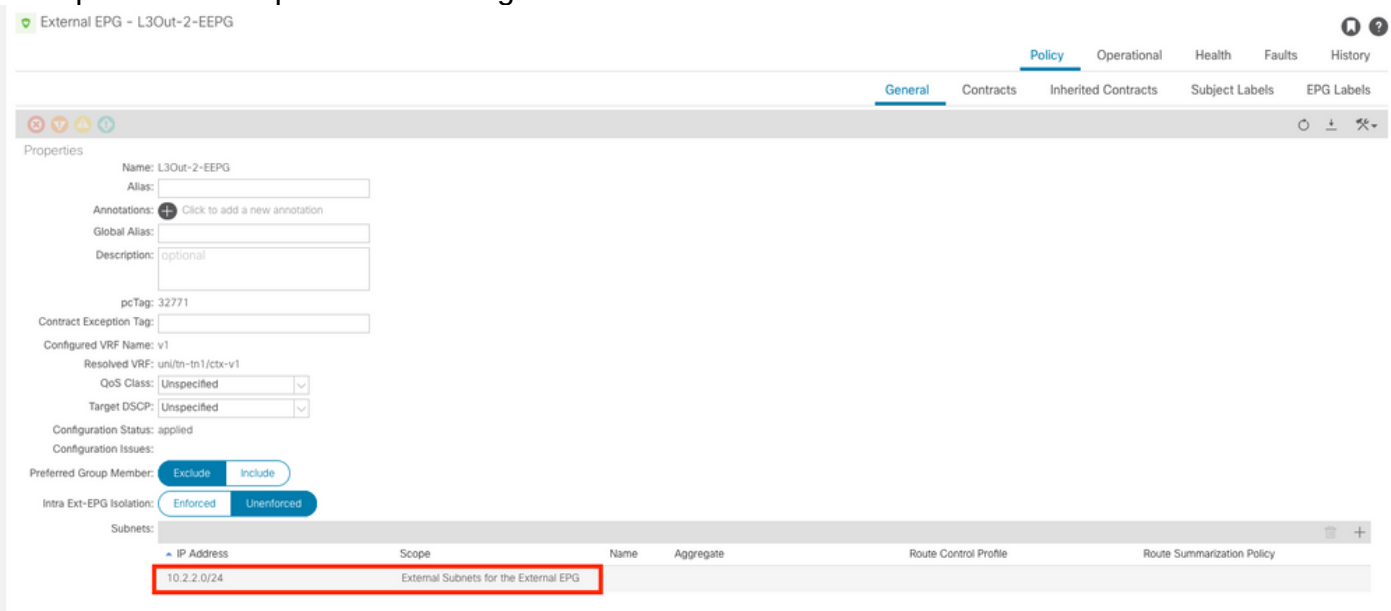
Zoning-Rules ID 4111 and 4112 are programmed as L3Out-1-EEPG has both the 0.0.0.0/0 Subnet and provides a contract that is consumed by EPG.

Flows to L3Out-2-EEPG are unexpectedly allowed due to this configuration!

## Solution - Unintended Allows

To prevent this behavior:

1. It is strongly recommended to only use the 0.0.0.0/0 Subnet on one L3Out EPG per VRF
2. Where possible, use specific subnets for other L3Outs in the same VRF. This allows traffic to pull in the unique L3Out PcTag values as their dclass.




Apply these changes to mitigate the unexpected allow:

1. On L3Out-2-EEPG, replace the 0.0.0.0/0 Subnet with a 10.2.2.0/24 Subnet
2. On L3Out-2-EEPG, provide a contract
3. On EPG, consume the same contract

Once completed, observe these changes on Non-Border Leaf Node 302:

- There is a more specific policy-mgr prefix for 10.2.2.0/24 tied to L3Out-2-EEPG PcTag 32771
- There is a Zoning-Rules ID 4109 entry This entry allows a flow from EPG PcTag 49156 to L3Out-2-EEPG PcTag 32771
- There is a Zoning-Rules ID 4110 entry This entry allows a flow from L3Out-2-EEPG PcTag 32771 to EPG PcTag 49156

The updated forward route and policy-mgr prefix which show that 10.2.2.2 is assigned the L3Out-2-EEPG PgTag of 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
```

**Note**: Zoning-Rules IDs 4111 and 4112 still exist on Non-Border Leaf Node 302 as L3Out-1-EEPG still has the 0.0.0.0/0 Subnet and also has a contract relationship with EPG. However, L3Out-2-EEPG traffic no longer inadvertently use those rules as its traffic is now be classified with the L3Out PcTag, and not System PcTag 15:

```
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)    |
+---------+--------+--------+----------+----------------+---------+---------+------------------
+----------+----------------------+
```

Ping from the EPG host to the external destination behind L3Out-2-EEPG is successful:

```
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
```

The ELAM for the icmp request on Non-Border Leaf Node 302 indicates the dclass is now 32771 - the PcTag of L3Out-2-EEPG.

```
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" )
...
```

The ereport provided aclqos command shows that this flow hits one of the new Zoning-Rules, specifically Rule ID 4109:

```
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
```