# Risoluzione dei problemi ACI L3Out - Subnet 0.0.0.0/0 e System PcTag 15

## Sommario



## Introduzione

Questo documento descrive la derivazione PcTag della subnet 0.0.0.0/0 quando definita in un EPG L3Out.

## Premesse

La sezione **"L3Out EPG with 0.0.0.0/0 subnet"** della ACI Contract Guide riassume 0.0.0.0/0 con "External Subnet for the External EPG" nella classificazione del traffico dell'ambito come:

- Al traffico originato da un'uscita L3 con prefisso più lungo corrispondente a una subnet 0.0.0.0/0 configurata viene assegnato l'ID classe origine (classe) del tag PcTag VRF.
- Al traffico destinato a un EPG L3Out con il prefisso più lungo corrispondente a una subnet 0.0.0.0/0 configurata viene assegnato l'ID della classe di destinazione (dclass) di 15, un PcTag di sistema.

La sezione **"Eccezione per 0.0.0.0/0 con subnet esterne per EPG esterno"** del white paper ACI L3Out contiene un avviso:

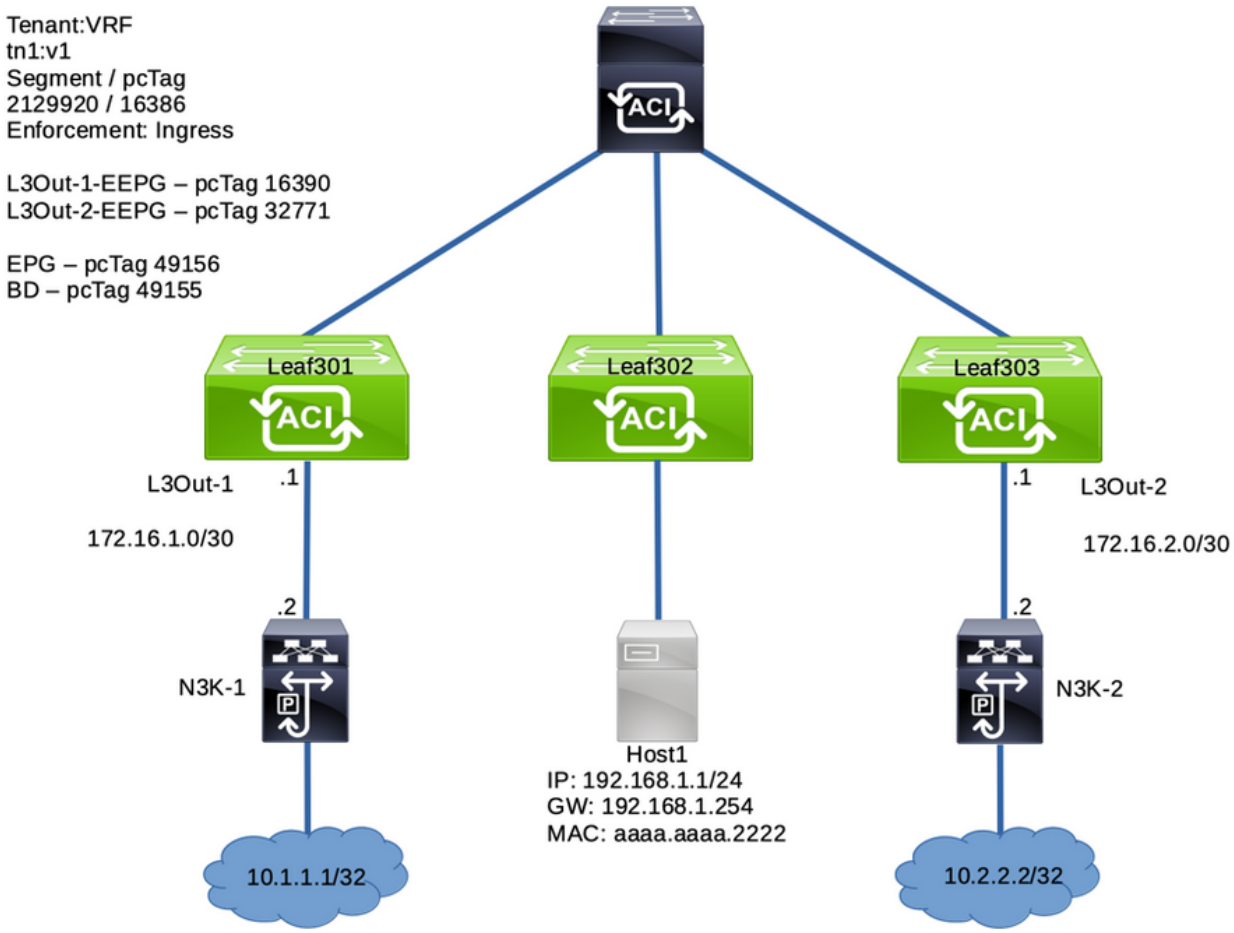
"...Sebbene non sia consigliato, è possibile configurare 0.0.0.0/0 con 'Subnet esterne per EPG

esterno' in più EPG L3Out nello stesso VRF... Anche se questa configurazione è consentita, si verifica una distribuzione non intenzionale del contratto..."

In questo articolo viene illustrata la distribuzione non intenzionale del contratto.

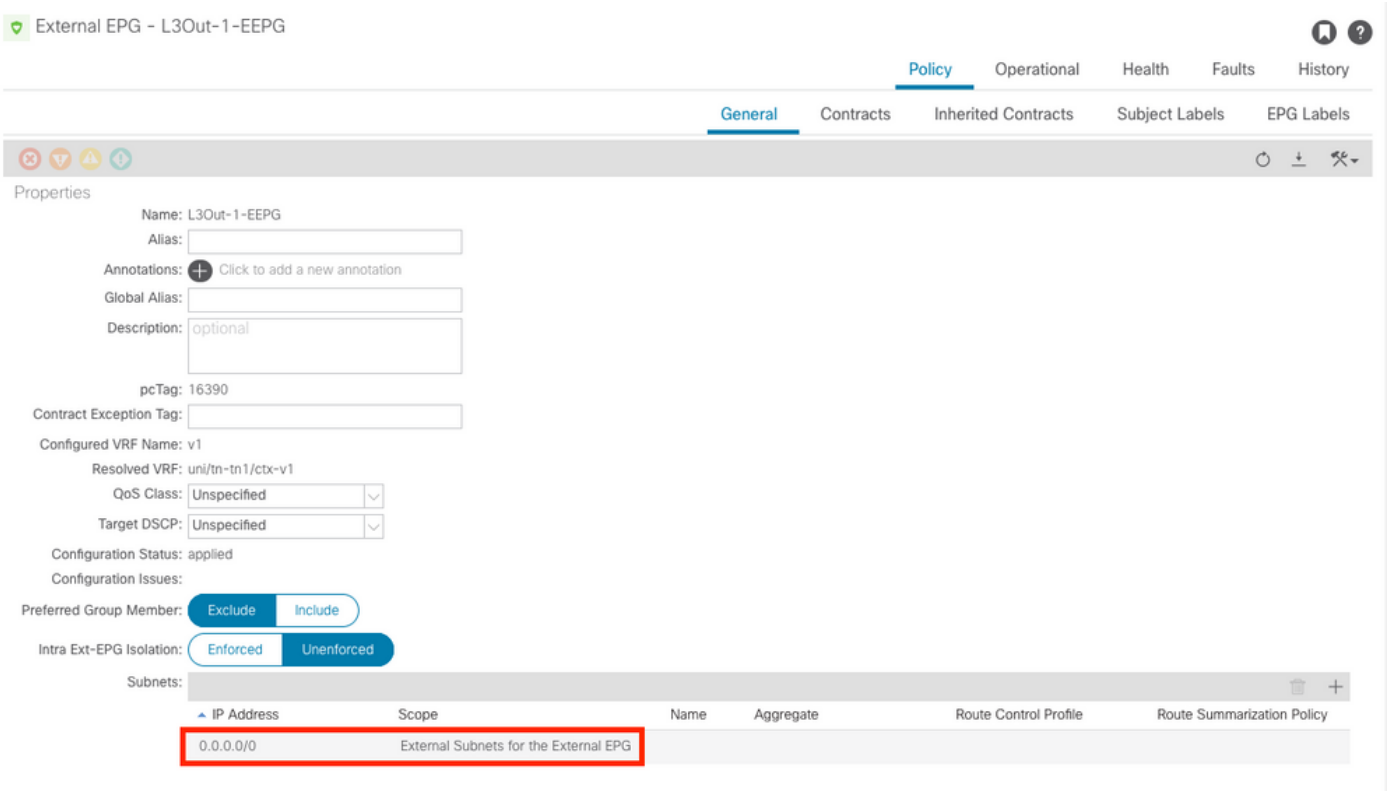
# Configurazione

## Diagramma topologico




## Caratteristiche principali della configurazione

- I nodi foglia 301 e 303 sono nodi foglia di bordo
- Il nodo foglia 302 è una foglia non di bordo
- L3Out-1-EEPG, su Border Leaf 301, ha una subnet 0.0.0.0/0 con "Subnet esterne per EPG esterno"
- L3Out-1-EEPG fornisce un contratto
- EPG, su Foglia 302 non frontaliera, consuma lo stesso contratto




# Verifica

## VRF con applicazione delle policy "in entrata"

### Regole di zonizzazione foglia non-bordo

Come evidenziato nella sezione Background Information (Informazioni in background), il traffico destinato alle reti dietro questo L3Out che corrispondono al prefisso più lungo nella subnet 0.0.0.0/0 configurata ottiene una classe di destinazione (pcTag) di 15.

Questa è la tabella delle regole di zoning su Foglia non-bordo 302 per VRF "v1" (ID segmento 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)    |
```

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

Il contratto tra L3Out-1-EEPG e EPG (49156) prevede l'installazione di due regole:

- La regola 4112 si applica al traffico esterno originato dall'EPG L3Out con 0.0.0.0/0 LPM destinato all'EPG. Il flusso del traffico è classificato con la classe del VRF PcTag (16386) e con la classe di EPG (49156).
- La regola 4111 si applica al traffico proveniente dall'EPG destinato all'EPG L3Out con 0.0.0.0/0 LPM. Il flusso del traffico è classificato con la classe EPG (49156) e la classe System PcTag 15

### Regole di zoning per le foglie del bordo

Il nodo foglia del bordo 301 non ha le stesse regole di zoning del nodo foglia non del bordo 302 a causa dell'applicazione dei criteri VRF impostati su 'In entrata' (valore predefinito). I criteri per questi tipi di flussi dovrebbero essere applicati ai nodi foglia non frontalieri.

```
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 su L3Out ELAM

Il ping tra l'endpoint EPG 192.168.1.1 e l'indirizzo IP dietro L3Out-1-EEPG ha esito positivo:

```
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
```

Un ELAM per EPG a L3Out traffic on Non-Border Leaf 302 (EPG gateway) conferma:

1. Il pacchetto ha gli IP di origine e di destinazione previsti: Origine IP:192.168.1.1, IP destinazione: 10.1.1.1

2. La classe di origine (sclass) è EPG PcTag **49156**
3. La classe di destinazione (dclass) è System PcTag **15**, in quanto il prefisso più lungo 10.1.1.0/24 corrisponde alla subnet 0.0.0.0/0 su L3Out-1-EPG
4. Il criterio è stato applicato al nodo 302, il nodo foglia non di bordo.

```
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" )
```

Il comando fornito da report può essere immesso per un'ulteriore convalida della regola di zoning trovata:

```
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 per EPG ELAM

Il flusso di ritorno ottiene i criteri applicati al nodo foglia non frontaliero 302. Ciò è previsto quando l'applicazione dei criteri VRF è impostata su "In ingresso".

```
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" )
```

Ulteriore convalida:

```
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 con applicazione delle policy "in uscita"

### Regole di zonizzazione foglia non-bordo

Se l'opzione di applicazione delle policy VRF è impostata su "Esci", le regole del contratto per un'uscita L3 vengono distribuite sia sui nodi foglia del bordo che sui nodi foglia non del bordo. Di conseguenza, questa configurazione consuma ulteriore spazio TCAM rispetto all'applicazione "in ingresso". Questa configurazione non è il valore predefinito e, se utilizzata, deve essere considerata con attenzione.

Il nodo foglia non di confine 302 ha due regole di zoning, una per direzionalità di flusso:

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

## Regole di zoning per le foglie del bordo

Con l'applicazione della policy "Egress", Border Leaf Node 301 ha anche due ulteriori regole di zoning:

```
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 su L3Out ELAM

Il ping tra l'endpoint 192.168.1.1 e la rete dietro l3Out è riuscito:

```
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
```

Il messaggio ELAM sul nodo foglia non frontaliero 302 indica che la **politica non è stata applicata** a questa foglia. Inoltre, ha scelto una classe di **System PcTag 1** per consentire al flusso di raggiungere il nodo foglia successivo nel flusso:

```
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" )
```

L'ELAM sul nodo foglia del bordo 301 indica che **su questo nodo è stata applicata la policy**. Ha inoltre scelto una classe di **System PcTag 15.** Ciò significa che il prefisso più lungo corrisponde alla voce della subnet 0.0.0.0/0 L3Out:

```
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 per EPG ELAM

In questa impostazione, è presente un avvertimento per il flusso di ritorno:

- Il nodo foglia del bordo 301 non dispone di un endpoint per imparare a 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...
```

Di conseguenza, la policy non viene applicata al Border Leaf Node 301 per questo flusso e deve essere implicitamente consentita per raggiungere il successivo foglia:

```
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" )
```

Al contrario, la policy viene applicata al nodo foglia non-frontiera 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
```

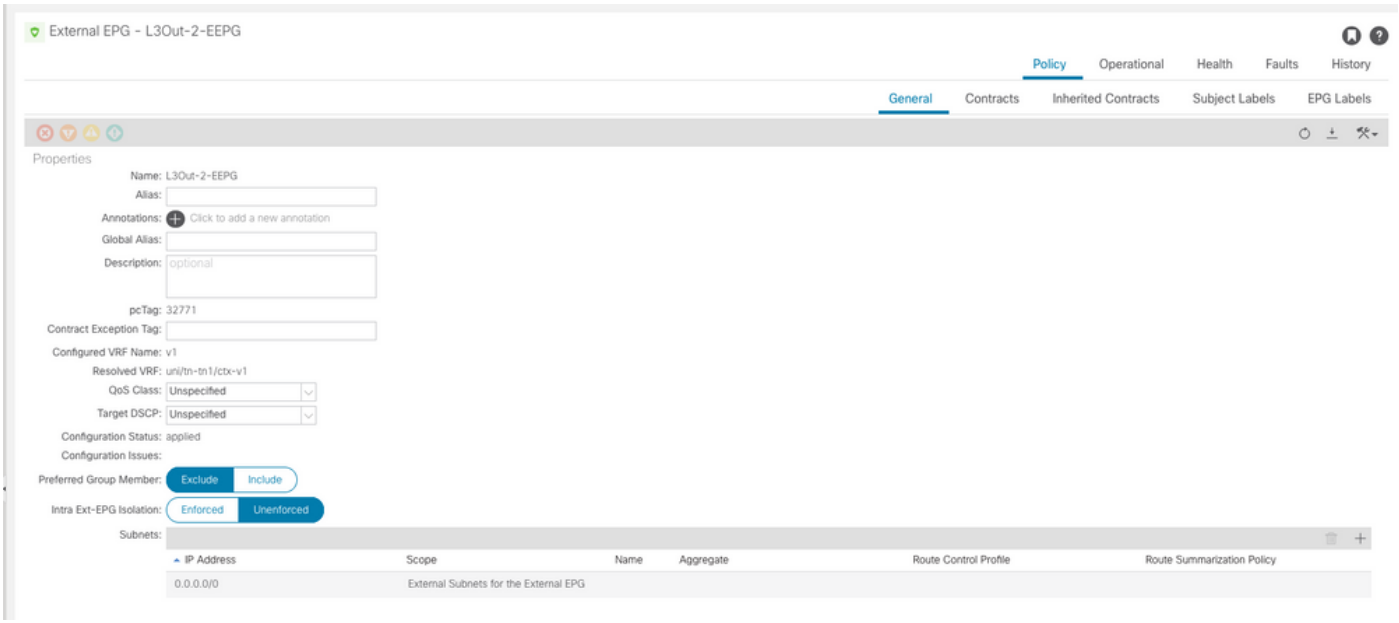
Se il nodo foglia del bordo 301 disponesse di un endpoint con informazioni 192.168.1.1, la policy sarebbe stata applicata a tale nodo.

# Risoluzione dei problemi

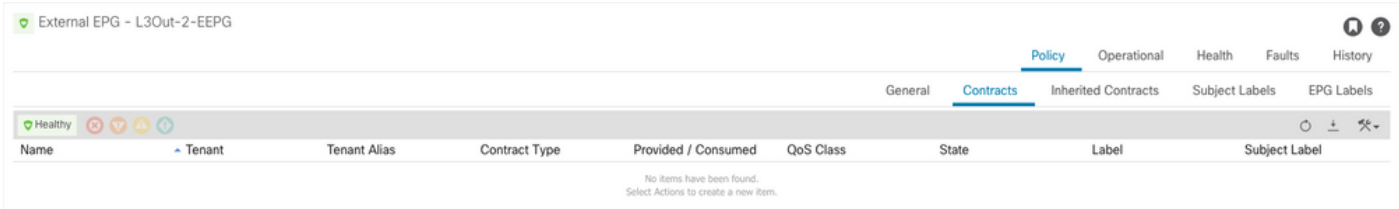
## Scenario - Consente

Una distribuzione con più L3Out nello stesso VRF configurato con la subnet 0.0.0.0/0 con "Subnet esterne per EPG esterno" può consentire il passaggio del traffico a destinazioni esterne in modo imprevisto.

Per ottenere questo risultato, aggiungere la subnet 0.0.0.0/0 in L3Out-2-EEPG che si trova nello stesso VRF di L3Out-1-EEPG.




**Non ci sono contratti su L3Out-2-EEPG, quindi ci aspettiamo che tutto il traffico venga scartato per impostazione predefinita:**




Tuttavia, il ping tra l'endpoint EPG 192.168.1.1 e la destinazione 10.2.2.2 dietro L3Out-2-EEPG ha esito positivo. Questo è inaspettato!

```
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
```

Il prefisso forward route e policy-mgr indicano entrambi che al traffico destinato alla versione

10.2.2.2 di questo VRF viene assegnato il codice di matricola del sistema 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#
```

Un ELAM su non-Border Leaf Node 302 convalida che il traffico sia classificato con una dclass di 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
```

Le regole di zoning per VRF "v1" non mostrano nuove voci per EPG e 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#
```

Poiché per L3Out-2-EEPG è configurata solo la subnet 0.0.0.0/0, tutto il traffico a essa destinato è classificato con la dclass di System PcTag 15.

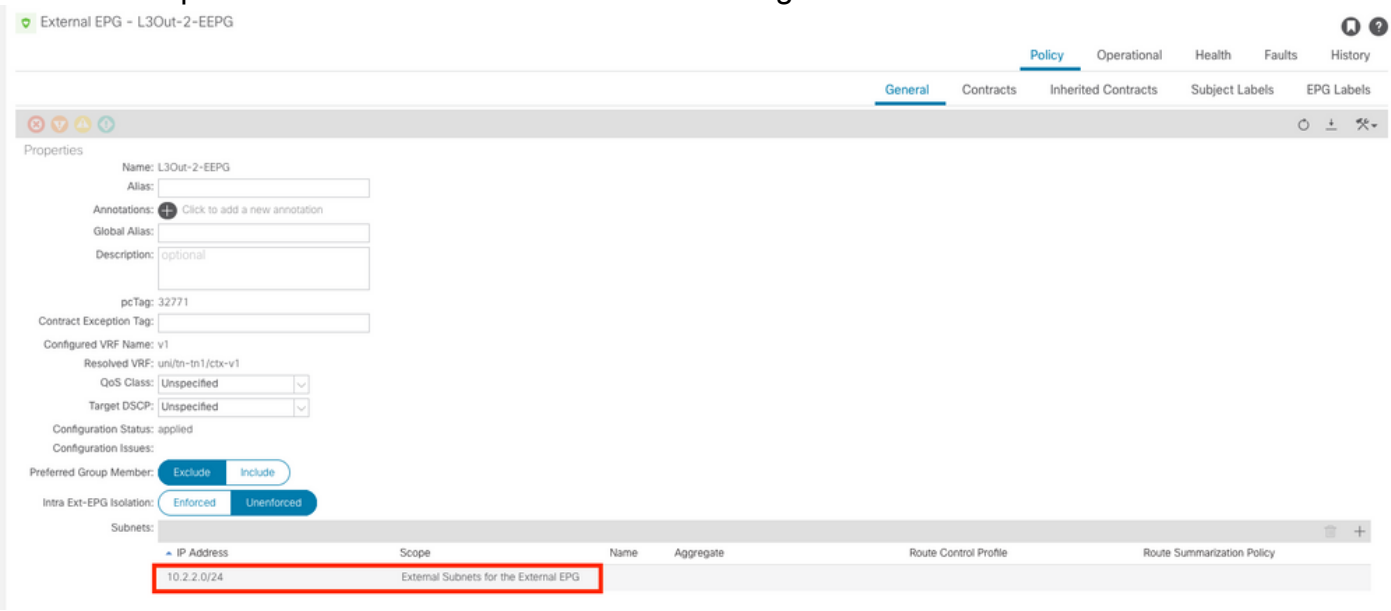
Le regole di zoning con ID 4111 e 4112 vengono programmate in quanto L3Out-1-EEPG dispone della subnet 0.0.0.0/0 e fornisce un contratto utilizzato da EPG.

I flussi a L3Out-2-EEPG sono consentiti in modo imprevisto a causa di questa configurazione.

## Soluzione - Consente

Per evitare questo comportamento:

1. Si consiglia di utilizzare solo la subnet 0.0.0.0/0 su un EPG L3Out per VRF
2. Se possibile, utilizzare subnet specifiche per altri L3Out nello stesso VRF. In questo modo, il traffico può estrarre i valori univoci di L3Out PcTag come dclass.




Applicare queste modifiche per ridurre l'autorizzazione imprevista:

1. In L3Out-2-EEPG, sostituire la subnet 0.0.0.0/0 con una subnet 10.2.2.0/24
2. Su L3Out-2-EEPG, fornire un contratto
3. In EPG, utilizzare lo stesso contratto

Al termine, osservare le seguenti modifiche sul nodo foglia non bordo 302:

- Èdisponibile un prefisso policy-mgr più specifico per 10.2.2.0/24 associato a L3Out-2-EEPG PcTag 32771
- Esiste una voce Zoning-Rules ID 4109 Questa voce consente il passaggio da EPG PcTag 49156 a L3Out-2-EEPG PcTag 32771
- Esiste una voce Zoning-Rules ID 4110 Questa voce consente il passaggio da L3Out-2-EEPG PcTag 32771 a EPG PcTag 49156

La route di inoltro aggiornata e il prefisso policy-mgr indicano che alla porta 10.2.2.2 è assegnato il tag IP L3Out-2-EEPG di 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
```

**Nota:** Gli ID 4111 e 4112 delle regole di zoning sono ancora presenti sul nodo foglia non-frontaliero 302 poiché L3Out-1-EEPG ha ancora la subnet 0.0.0.0/0 e ha anche una relazione contrattuale con EPG. Tuttavia, il traffico L3Out-2-EEPG non utilizza più inavvertitamente queste regole, in quanto il suo traffico è ora classificato con l'L3Out PcTag e non con l'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)    |
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Il ping tra l'host EPG e la destinazione esterna dietro L3Out-2-EEPG ha esito positivo:

```
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
```

L'ELAM per la richiesta icmp sul Non-Border Leaf Node 302 indica che la classe è ora 32771 - il PcTag di 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" )
...
```

Il comando aclqos del report indica che il flusso raggiunge una delle nuove regole di zoning, in particolare l'ID regola 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).