Solución de problemas de ACI L3Out: Subred 0.0.0.0/0 y System PcTag 15

Contenido

Introducción

Este documento describe la derivación PcTag de la subred 0.0.0.0/0 cuando se define en un EPG L3Out.

Antecedentes

La sección **"L3Out EPG with 0.0.0.0/0 subnet"** de la Guía de contratos de ACI resume 0.0.0.0/0 con la clasificación de tráfico de alcance "Subredes externas para el EPG externo" como:

- El tráfico originado en una L3Out con el prefijo más largo coincidente con una subred 0.0.0.0/0 configurada se asigna al ID de clase de origen (sclass) de la PcTag de VRF.
- El tráfico destinado a un EPG L3Out con el prefijo más largo coincidente con una subred 0.0.0.0/0 configurada se asigna al ID de clase de destino (dclass) de 15, System PcTag.

La sección **"Una excepción para 0.0.0.0/0 con subredes externas para el EPG externo"** del Informe técnico de L3Out de ACI contiene una advertencia:

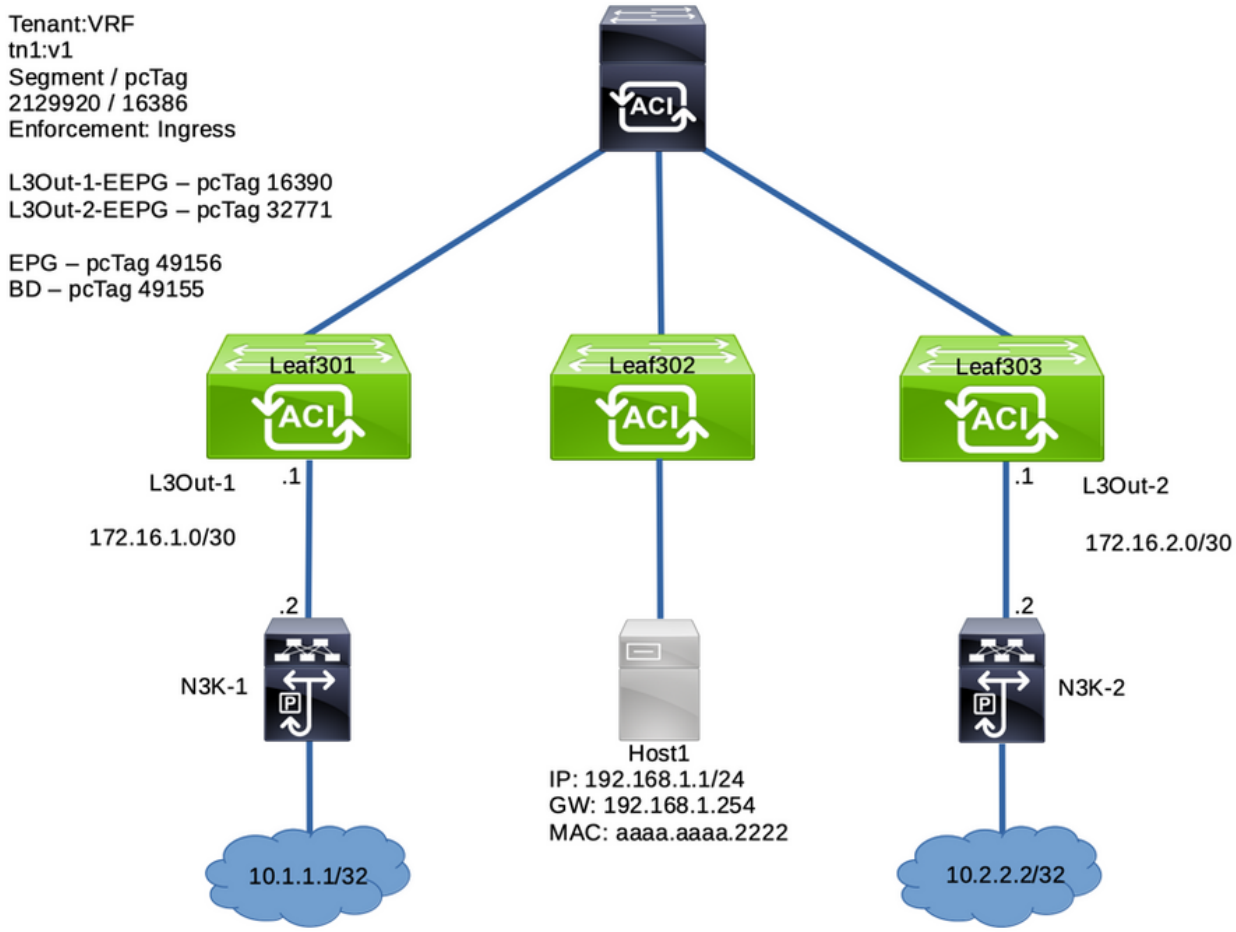
"...Aunque no se recomienda, puede configurar 0.0.0.0/0 con 'Subredes externas para el EPG externo' en varios EPG L3Out en el mismo VRF... Mientras se permite esta configuración, se

produce una implementación de contrato no intencionada..."

En este artículo se analiza el despliegue involuntario de contratos.

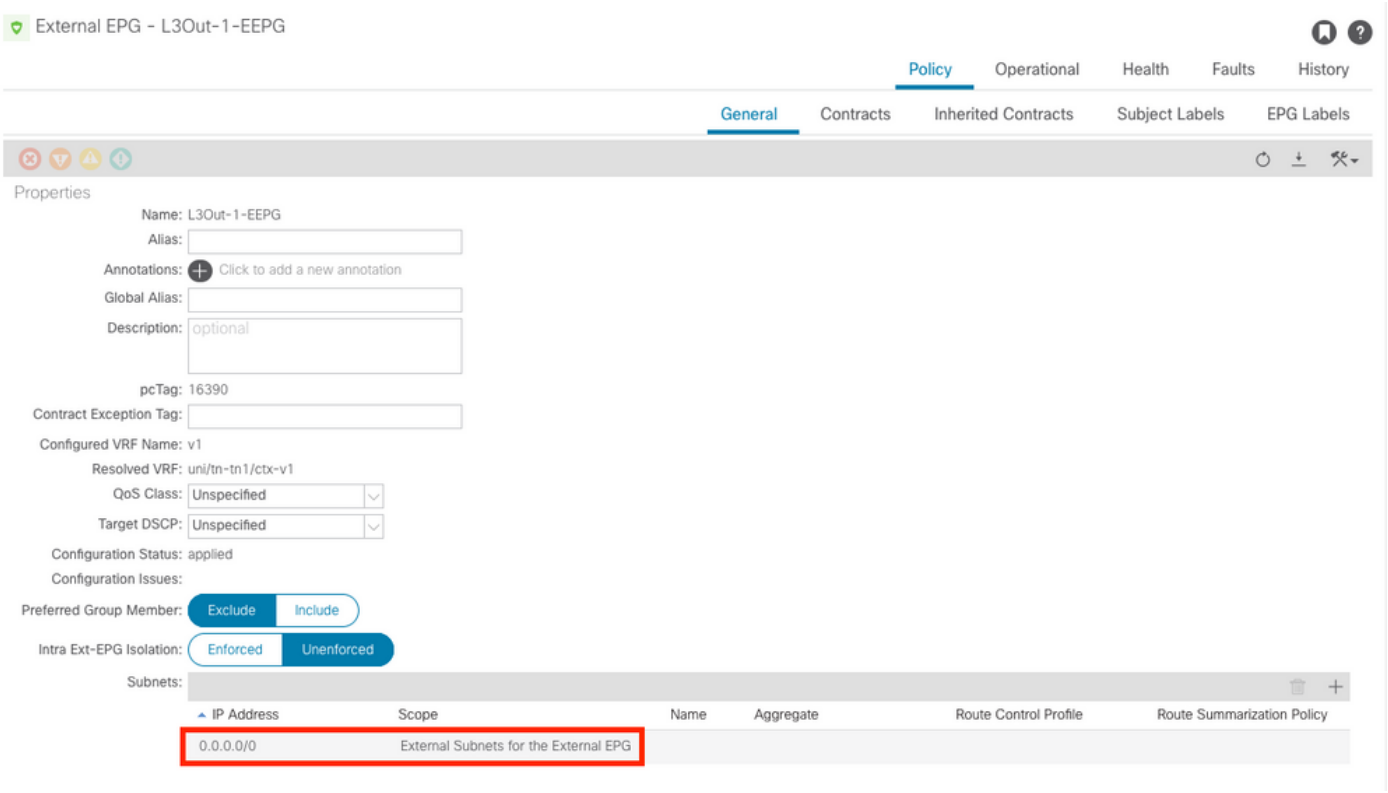
Configurar

Diagrama de topología



Aspectos destacados de configuración

- Los nodos de hoja 301 y 303 son nodos de hoja de borde
- El nodo de hoja 302 es una hoja no fronteriza
- L3Out-1-EEPG, en Border Leaf 301, tiene una subred 0.0.0.0/0 con "Subredes externas para el EPG externo"
- L3Out-1-EEPG proporciona un contrato
- EPG, en Non-Border Leaf 302, utiliza el mismo contrato



Verificación

VRF con aplicación de políticas de "entrada"

Non-Border Leaf Zoning-Rules

Como se resaltó en la sección Información en Segundo Plano, el tráfico destinado a las redes detrás de este L3Out cuyo prefijo más largo coincida en la subred 0.0.0.0/0 configurada obtiene una clase de destino (pcTag) de 15.

Esta es la tabla de reglas de zonificación en Non-Border Leaf 302 para VRF "v1" (ID de 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)    |
```

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

Hay dos reglas instaladas como resultado del contrato entre L3Out-1-EPG y EPG (49156):

- La regla 4112 es para el tráfico externo originado en el EPG L3Out con 0.0.0.0/0 LPM destinado al EPG. El flujo de tráfico se clasifica con la clase de VRF PcTag (16386) y dclass de EPG (49156) .
- La regla 4111 es para el tráfico originado en el EPG destinado al EPG L3Out con 0.0.0.0/0 LPM. El flujo de tráfico se clasifica con la clase EPG (49156) y la clase dclass de System PcTag 15

Reglas de zonificación de hojas de borde

El nodo de hoja de borde 301 no tiene las mismas reglas de zonificación que el nodo de hoja no de borde 302 debido a que la aplicación de políticas de VRF se estableció en 'Ingress' (valor predeterminado). Se espera que la política para estos tipos de flujos se aplique en los nodos de hoja no fronterizos.

```
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 a L3Out ELAM

Un ping del terminal EPG 192.168.1.1 a la IP detrás de L3Out-1-EEPG es exitoso:

```
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 para el tráfico de EPG a L3Out en Non-Border Leaf 302 (gateway EPG) confirma:

1. El paquete tiene las IP de origen y destino esperadas: IP de origen:192.168.1.1, IP de

destino: 10.1.1.1

2. La clase de origen (sclass) es EPG PcTag **49156**
3. La clase de destino (dclass) es System PcTag **15**, ya que el prefijo 10.1.1.0/24 más largo coincide con la subred 0.0.0.0/0 en L3Out-1-EEPG
4. La política se aplicó en este nodo 302, el nodo de hoja no fronterizo.

```
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" )
```

El comando dado por el informe se puede ingresar para la validación adicional de la regla de zonificación que fue alcanzada:

```
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 a EPG ELAM

El flujo de retorno obtiene la política aplicada en el nodo de hoja no fronterizo 302. Esto se espera cuando la aplicación de políticas VRF se establece en "Ingreso".

```
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" )
```

Validación adicional:

```
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 aplicación de políticas de "salida"

Non-Border Leaf Zoning-Rules

Con la aplicación de políticas de VRF establecida en "Egress" (Salida), las reglas de contrato para L3Out se implementan en los nodos de hoja de borde y no de hoja de borde. Como resultado, esta configuración consume espacio TCAM adicional en comparación con la aplicación de "entrada". Esta configuración no es el valor predeterminado y, si se utiliza, se debe considerar detenidamente.

El nodo de hoja no fronterizo 302 tiene dos reglas de zonificación, una por direccionalidad de flujo:

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

Reglas de zonificación de hojas de borde

Con la aplicación de políticas de "salida", el nodo de hoja de frontera 301 también tiene dos reglas de zonificación adicionales:

```
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 a L3Out ELAM

Un ping del terminal 192.168.1.1 a la red detrás de L3Out es exitoso:

```
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
```

El ELAM en el nodo de hoja no fronterizo 302 indica que la **política no se aplicó** en esta hoja. Además, tomó una clase de **System PcTag 1** para permitir que el flujo alcanzara el siguiente nodo de hoja en el flujo:

```
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" )
```

El ELAM en el nodo de hoja de borde 301 indica que **se aplicó la política en este nodo**. También recogió una clase de **System PcTag 15.** Esto significa que el prefijo más largo coincidió con la entrada de subred 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 a EPG ELAM

Hay una advertencia con el flujo de retorno en esta configuración:

- El nodo de hoja de borde 301 no tiene un aprendizaje de punto final para 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...
```

Como resultado, la política no se aplica en el nodo de hoja de borde 301 para este flujo y se debe permitir implícitamente que llegue a la siguiente hoja:

```
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" )
```

En su lugar, la política se aplica en el nodo de hoja no fronterizo 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
```

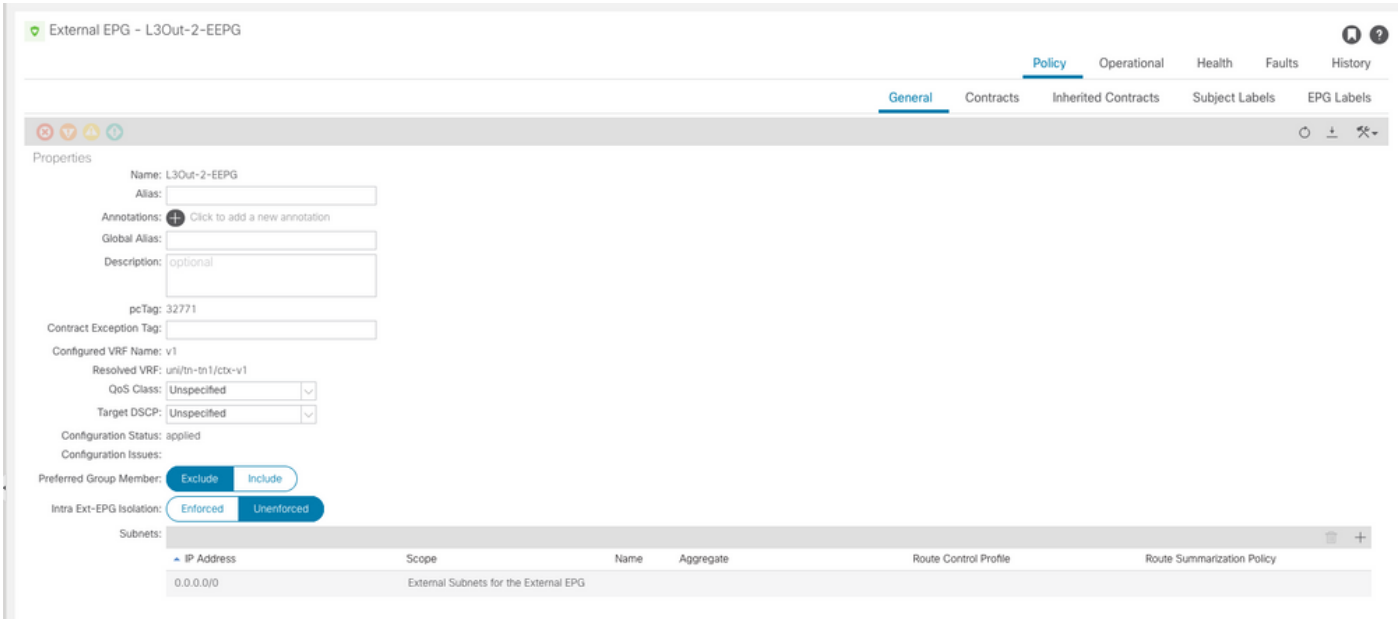
Si el nodo de hoja de borde 301 tuviera un aprendizaje de punto final 192.168.1.1, la política se habría aplicado en ese nodo.

Troubleshoot

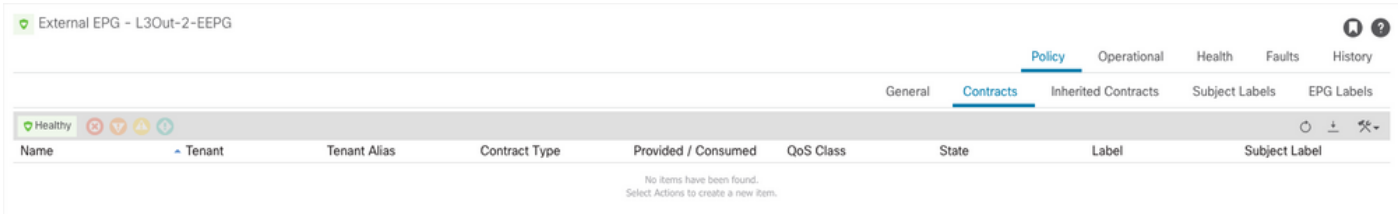
Escenario: permite el uso no intencionado

Una implementación con varias L3Outs en el mismo VRF configuradas con la subred 0.0.0.0/0 con "Subredes externas para el EPG externo" puede permitir que el tráfico pase a destinos externos inesperadamente.

Para inducir esto, agregue la subred 0.0.0.0/0 bajo L3Out-2-EEPG que está en el mismo VRF que L3Out-1-EEPG.



No hay contratos en L3Out-2-EEPG, por lo que cabría esperar que todo el tráfico se descarte de forma predeterminada:



Sin embargo, un ping del punto final EPG 192.168.1.1 al destino 10.2.2.2 detrás de L3Out-2-EPG es exitoso. ¡Esto es inesperado!

```
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
```

La ruta de reenvío y el prefijo de policy-mgr muestran que el tráfico destinado a 10.2.2.2 en este VRF tiene asignado 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#
```

Un ELAM en el nodo de hoja no fronterizo 302 valida que el tráfico se clasifica con una dclass de 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
```

Las reglas de zonificación para VRF "v1" no muestran ninguna entrada nueva para EPG y 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#
```

Como L3Out-2-EEPG sólo tiene configurada la subred 0.0.0.0/0, todo el tráfico destinado a ella se clasifica con dclass de System PcTag 15.

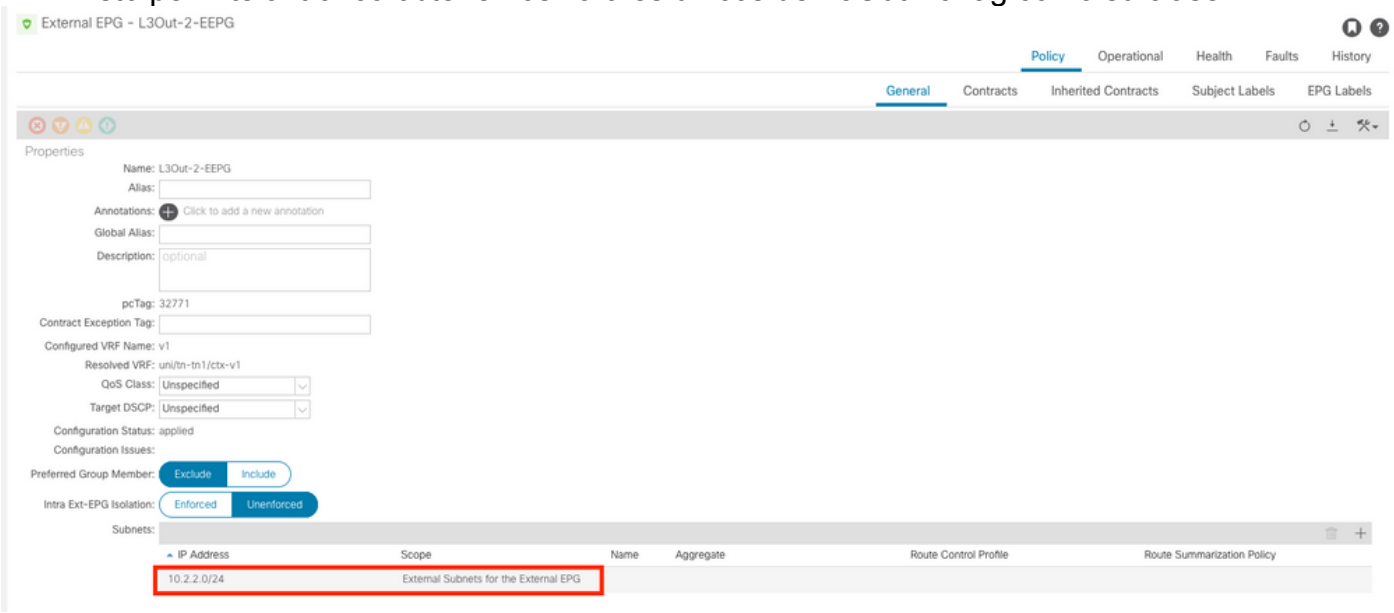
Las reglas de zonificación ID 4111 y 4112 se programan porque L3Out-1-EEPG tiene la subred 0.0.0.0/0 y proporciona un contrato que EPG consume.

¡Los flujos a L3Out-2-EPG se permiten inesperadamente debido a esta configuración!

Solución: permite el uso no intencionado

Para evitar este comportamiento:

1. Se recomienda encarecidamente utilizar solamente la subred 0.0.0.0/0 en un EPG L3Out por VRF
2. Siempre que sea posible, utilice subredes específicas para otras L3Outs en el mismo VRF. Esto permite al tráfico obtener los valores únicos de L3Out PcTag como su clase.



Aplique estos cambios para mitigar el permiso inesperado:

1. En L3Out-2-EPG, reemplace la subred 0.0.0.0/0 por una subred 10.2.2.0/24
2. En L3Out-2-EEPG, proporcione un contrato
3. En EPG, utilice el mismo contrato

Una vez completados, observe estos cambios en el nodo de hoja no fronterizo 302:

- Existe un prefijo de policy-mgr más específico para 10.2.2.0/24 vinculado a L3Out-2-EEPG PcTag 32771
- Hay una entrada Zoning-Rules ID 4109 Esta entrada permite un flujo de EPG PcTag 49156 a L3Out-2-EEPG PcTag 32771
- Hay una entrada Zoning-Rules ID 4110 Esta entrada permite un flujo de L3Out-2-EEPG PcTag 32771 a EPG PcTag 49156

La ruta de reenvío actualizada y el prefijo de policy-mgr que muestran que a 10.2.2.2 se le ha asignado la etiqueta de paginación L3Out-2-EEPG de 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: Los ID 4111 y 4112 de las reglas de zonificación siguen existiendo en el nodo de hoja no fronterizo 302, ya que L3Out-1-EEPG aún tiene la subred 0.0.0.0/0 y también tiene una relación de contrato con EPG. Sin embargo, el tráfico L3Out-2-EEPG ya no usa inadvertidamente esas reglas, ya que su tráfico ahora se clasifica con la PcTag L3Out, y no con la PcTag del sistema 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)    |
+---------+--------+--------+----------+----------------+---------+---------+------------------
+----------+----------------------+
```

El ping del host EPG al destino externo detrás de L3Out-2-EPG es exitoso:

```
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
```

El ELAM para la solicitud icmp en el nodo de hoja no fronterizo 302 indica que dclass es ahora

32771 - la PcTag de 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" )
...
```

El comando aclqos proporcionado por el informe muestra que este flujo llega a una de las nuevas Zoning-Rules, específicamente la Regla 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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).