Solução de problemas da ACI L3Out - Subnet 0.0.0.0/0 e System PcTag 15

Contents

Introduction

Este documento descreve a derivação PcTag da sub-rede 0.0.0.0/0 quando definida em um EPG L3Out.

Informações de Apoio

A seção **"L3Out EPG with 0.0.0.0/0 subnet"** do Guia de Contrato da ACI resume 0.0.0.0/0 com a classificação de tráfego de escopo "Sub-redes Externas para o EPG Externo" como:

- O tráfego originado de uma L3Out, que é o maior prefixo correspondente a uma sub-rede 0.0.0.0/0 configurada, recebe o ID da classe de origem (class) do VRF PcTag.
- O tráfego destinado a um EPG de L3Out, que é o prefixo mais longo correspondente a uma sub-rede 0.0.0.0/0 configurada, recebe o ID de classe de destino (dclass) 15, um PcTag do sistema.

A seção **"An exception for 0.0.0.0/0 with External Subnets for the External EPG"** do Whitepaper L3Out da ACI contém um aviso:

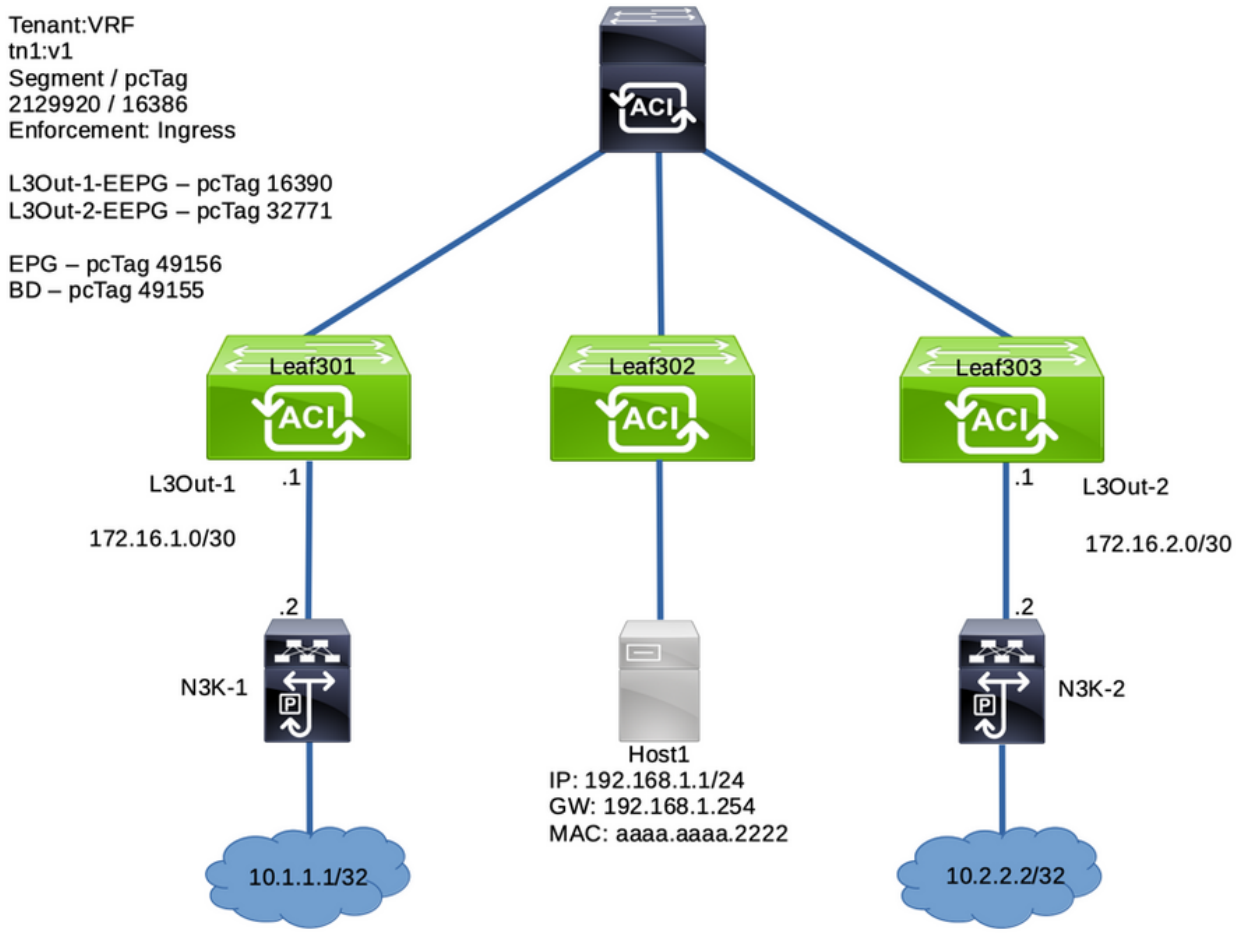
"...Embora não seja recomendado, você pode configurar 0.0.0.0/0 com 'Sub-redes Externas para

o EPG Externo' em vários EPGs L3Out no mesmo VRF... Embora essa configuração seja permitida, ocorre uma implantação de contrato não intencional..."

Este artigo se aprofunda nessa implantação de contrato não intencional.

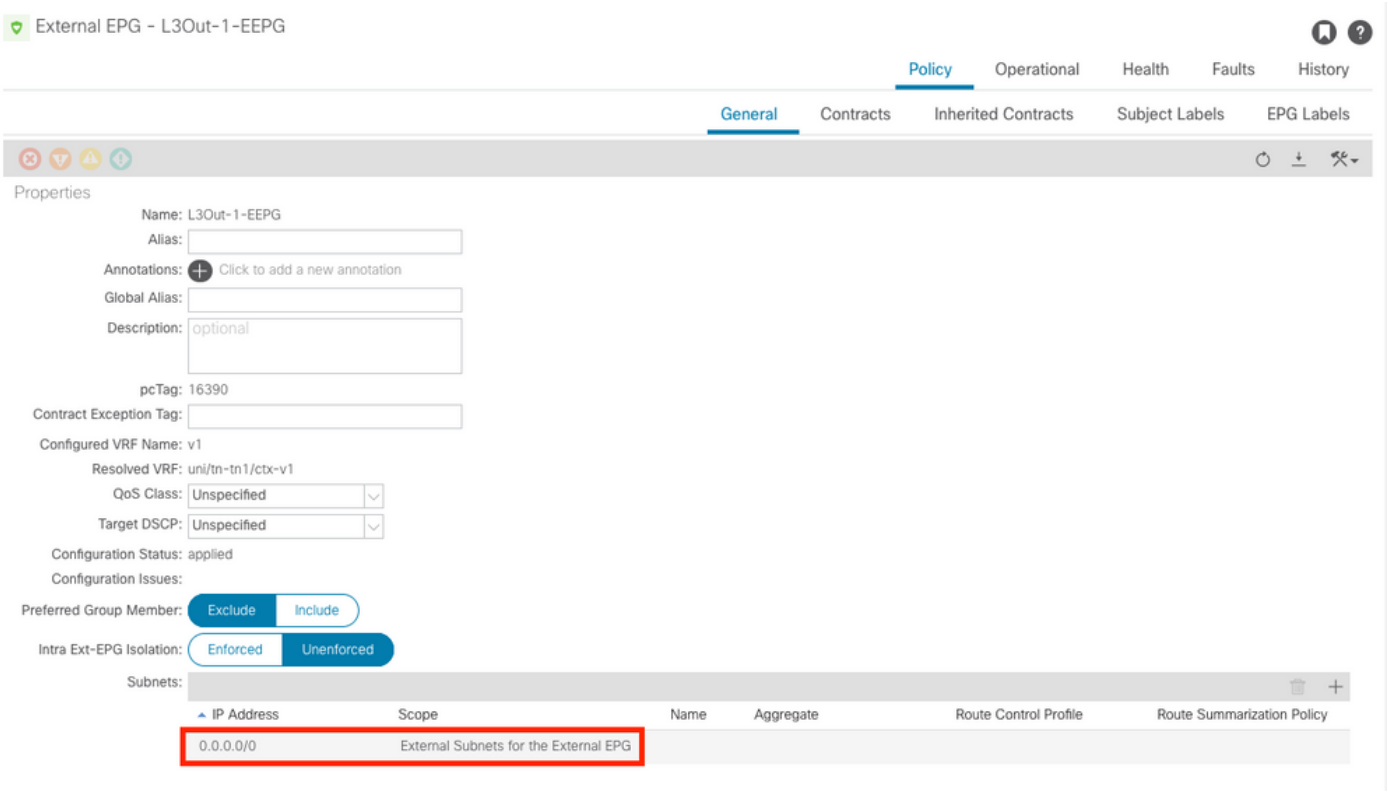
Configurar

Diagrama de topologia



Destaques da configuração

- Os nós folha 301 e 303 são nós folha de borda
- O Nó Folha 302 é uma Folha Sem Borda
- L3Out-1-EEPG, no Border Leaf 301, tem uma sub-rede 0.0.0.0/0 com "Sub-redes Externas para o EPG Externo"
- L3Out-1-EEPG fornece um contrato
- O EPG, no Non-Border Leaf 302, consome o mesmo contrato



Verificar

VRF com aplicação de política de "entrada"

Regras de zoneamento folha não fronteiriço

Como destacado na seção Informações de Segundo Plano, o tráfego destinado a redes por trás dessa L3Out que Maior Correspondência de Prefixo na sub-rede 0.0.0.0/0 configurada recebe uma classe de destino (pcTag) de 15.

Esta é a tabela de regras de zoneamento no 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)    |
```

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

Há duas regras instaladas como resultado do contrato entre L3Out-1-EEPG e EPG (49156):

- A regra 4112 é para o tráfego externo originado do EPG L3Out com 0.0.0.0/0 LPM destinado ao EPG. O fluxo de tráfego é classificado com a classe do VRF PcTag (16386) e a classe do EPG (49156) .
- A regra 4111 é para o tráfego originado do EPG destinado ao L3Out EPG com 0.0.0.0/0 LPM. O fluxo de tráfego é classificado com a classe de EPG (49156) e a classe de PcTag de sistema 15

Border Leaf Zoning-Rules

O Border Leaf Node 301 não tem as mesmas regras de zoneamento que o Non-Border Leaf Node 302 devido à Aplicação de Política de VRF definida como 'Ingress' (valor padrão). Espera-se que a política para esses tipos de fluxos seja aplicada em nós folha não borda.

```
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 para L3Out ELAM

Um ping do ponto final de EPG 192.168.1.1 para o IP atrás de L3Out-1-EEPG foi bem-sucedido:

```
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
```

Um ELAM para EPG para tráfego L3Out no Non-Border Leaf 302 (gateway EPG) confirma:

1. O pacote tem os IPs origem e destino esperados: IP origem:192.168.1.1, IP destino: 10.1.1.1
2. A classe de origem (class) é o **49156** EPG PcTag

3. A classe de destino (dclass) é System PcTag **15**, pois o prefixo mais longo 10.1.1.0/24 corresponde à sub-rede 0.0.0.0/0 em L3Out-1-EEPG
4. A política foi aplicada neste nó 302, o Nó Folha Sem Borda.

```
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" )
```

O comando fornecido pelo relatório pode ser inserido para validação adicional da regra de zoneamento que foi atingida:

```
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 para EPG ELAM

O fluxo de retorno obtém a política aplicada no nó folha não borda 302. Isso é esperado quando a aplicação da política de VRF é definida como "Ingress".

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

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

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

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

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

Validação 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 com aplicação de política de "saída"

Regras de zoneamento folha não fronteiriço

Com a aplicação da política de VRF definida como "Saída", as regras de contrato para uma L3Out são implantadas nos nós leaf de borda e não borda. Como resultado, essa configuração consome espaço de TCAM adicional em comparação com a aplicação de "entrada". Essa configuração não é o valor padrão e, se usada, deve ser cuidadosamente considerada.

O nó folha não borda 302 tem duas regras de zoneamento, uma por direcionalidade de fluxo:

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

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

Border Leaf Zoning-Rules

Com a aplicação da política de "saída", o Border Leaf Node 301 também tem duas regras de zoneamento adicionais:

```
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 para L3Out ELAM

Um ping do ponto final 192.168.1.1 para a rede atrás da L3Out foi bem-sucedido:

```
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
```

O ELAM no Nó Folha 302 Não Borda indica que a **política não foi aplicada** nesta folha. Além disso, ele pegou uma classe de **System PcTag 1** para permitir que o fluxo atinja o próximo nó folha no fluxo:

```
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" )
```

O ELAM no nó de folha de borda 301 indica que a **política foi aplicada neste nó**. Ele também selecionou uma classe de **System PcTag 15.** Isso significa que o prefixo mais longo correspondeu à entrada de sub-rede 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 para EPG ELAM

Há uma advertência com o fluxo de retorno nesta configuração:

- Border Leaf Node 301 não tem um endpoint learn 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, a política não é aplicada no Nó Folha de Borda 301 para esse fluxo e ele deve ter permissão implícita para acessar a próxima folha:

```
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" )
```

Em vez disso, a política é aplicada no nó folha não borda 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
```

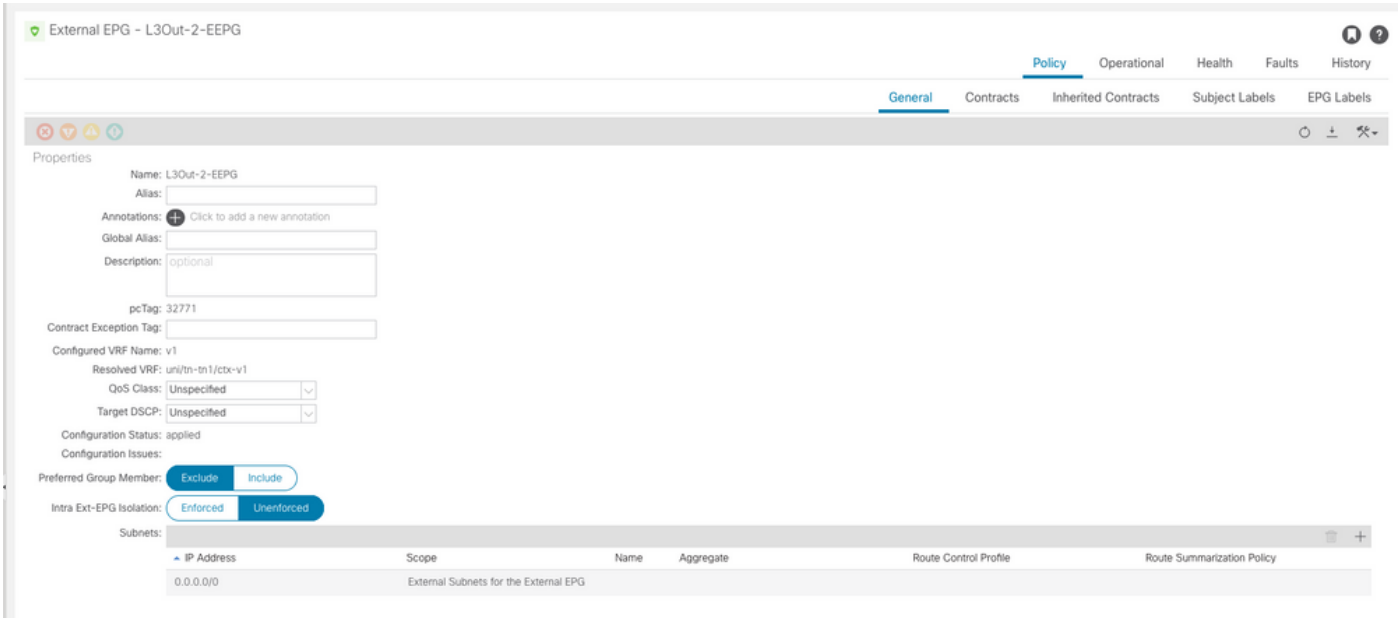
Se o nó de folha de borda 301 tivesse um ponto final aprendesse 192.168.1.1, a política teria sido aplicada nesse nó.

Troubleshoot

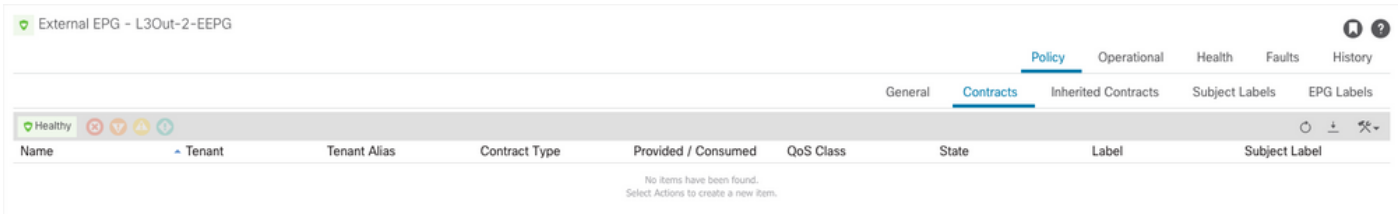
Cenário - Permite Não-Intencional

Uma implantação com várias L3Outs no mesmo VRF configurado com a sub-rede 0.0.0.0/0 com "Sub-redes externas para o EPG externo" pode permitir que o tráfego passe para destinos externos inesperadamente.

Para induzir isso, adicione a sub-rede 0.0.0.0/0 em L3Out-2-EEPG que está no mesmo VRF que L3Out-1-EEPG.



Não há contratos em L3Out-2-EEPG, portanto, esperamos que todo o tráfego seja descartado por padrão:



No entanto, um ping do ponto final do EPG 192.168.1.1 para o destino 10.2.2.2 atrás do L3Out-2-EEPG foi bem-sucedido. Isso é 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
```

A rota de encaminhamento e o prefixo do gerenciador de políticas mostram que o tráfego destinado a 10.2.2.2 neste VRF é atribuído 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#
```

Um ELAM no nó de folha não borda 302 valida que o tráfego é classificado com uma classe de sistema 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
```

As regras de zoneamento para VRF "v1" não mostram nenhuma entrada nova para 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#
```

Como L3Out-2-EEPG tem apenas a sub-rede 0.0.0.0/0 configurada, todo o tráfego destinado a ela é classificado com a classe do PcTag 15 do sistema.

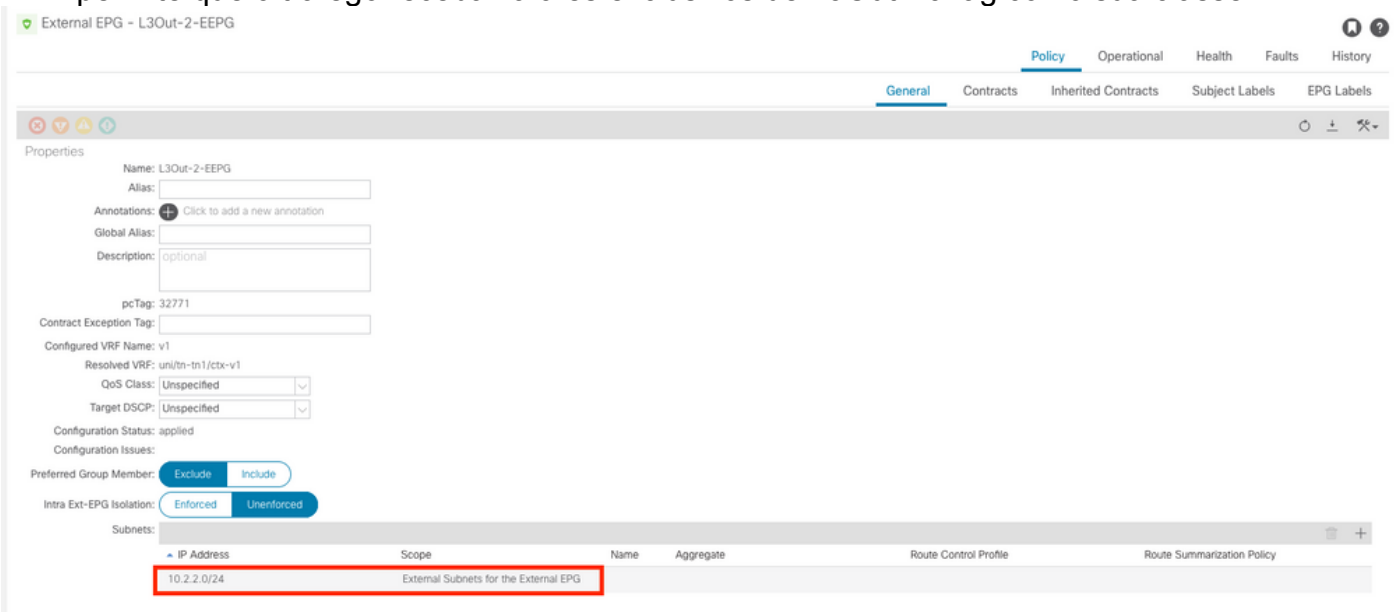
As regras de zoneamento ID 4111 e 4112 são programadas como L3Out-1-EEPG tem a sub-rede 0.0.0.0/0 e fornece um contrato que é consumido pelo EPG.

Fluxos para L3Out-2-EEPG são permitidos inesperadamente devido a esta configuração!

Solução - Permite involuntário

Para evitar esse comportamento:

1. Éaltamente recomendável usar apenas a sub-rede 0.0.0.0/0 em um EPG de L3Out por VRF
2. Quando possível, use sub-redes específicas para outras L3Outs no mesmo VRF. Isso permite que o tráfego receba valores exclusivos de L3Out PcTag como sua classe.



Aplique essas alterações para reduzir a permissão inesperada:

1. Em L3Out-2-EEPG, substitua a sub-rede 0.0.0.0/0 por uma sub-rede 10.2.2.0/24
2. No L3Out-2-EEPG, forneça um contrato
3. No EPG, consuma o mesmo contrato

Uma vez concluído, observe estas alterações no Nó Folha 302 Não-Borda:

- Há um prefixo de gerenciador de política mais específico para 10.2.2.0/24 vinculado à 32771 L3Out-2-EEPG PcTag
- Há uma entrada de ID 4109 de regras de zoneamento Esta entrada permite um fluxo de 49156 PcTag EPG para 32771 PcTag L3Out-2-EPG
- Há uma entrada de ID de regras de zoneamento 4110 Esta entrada permite um fluxo de 32771 PcTag L3Out-2-EEPG para 49156 PcTag EPG

A rota de encaminhamento atualizada e o prefixo do gerenciador de políticas que mostram que 10.2.2.2 recebeu a L3Out-2-EEPG PgTag 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
```

Note: As regras de zoneamento IDs 4111 e 4112 ainda existem no nó folha não borda 302, pois L3Out-1-EEPG ainda tem a sub-rede 0.0.0.0/0 e também tem um relacionamento de contrato com o EPG. Entretanto, o tráfego L3Out-2-EEPG não usa mais essas regras inadvertidamente, pois seu tráfego agora é classificado com o L3Out PcTag, e não com o 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)    |
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

O ping do host EPG para o destino externo atrás de L3Out-2-EEPG foi bem-sucedido:

```
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
```

O ELAM para a solicitação icmp no nó de folha não borda 302 indica que a classe agora está 32771 - o 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" )
...
```

O relatório fornecido pelo comando aclqos mostra que esse fluxo atinge uma das novas regras de zoneamento, especificamente o ID de regra 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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.