Probleemoplossing ACI L3Out - Subnet 0.0.0.0/0 en System PCTag 15

Inhoud

Inleiding

Dit document beschrijft de PcTag-afleiding van het 0.0.0.0/0-subnetnummer wanneer dit in een L3Out EPG is gedefinieerd.

Achtergrondinformatie

De sectie **"L3Out EPG with 0.0.0.0/0 subnet"** van de ACI-contractgids vat 0.0.0.0/0 samen met "Externe subnetten voor de Externe EPG" verkeersclassificatie als volgt:

- Verkeer dat afkomstig is van een L3Out die de langste prefix is die aan een geconfigureerd 0.0.0.0/0-subnetnummer is toegewezen, krijgt de bronklasse-ID (klasse) van de VRF-pc-tag toegewezen.
- Verkeer dat bestemd is voor een L3Out EPG die de langste prefix is die aan een geconfigureerd 0.0.0.0/0-subnetnummer is toegewezen, krijgt de doelklasse-ID (klasse) van 15, een System PcTag toegewezen.

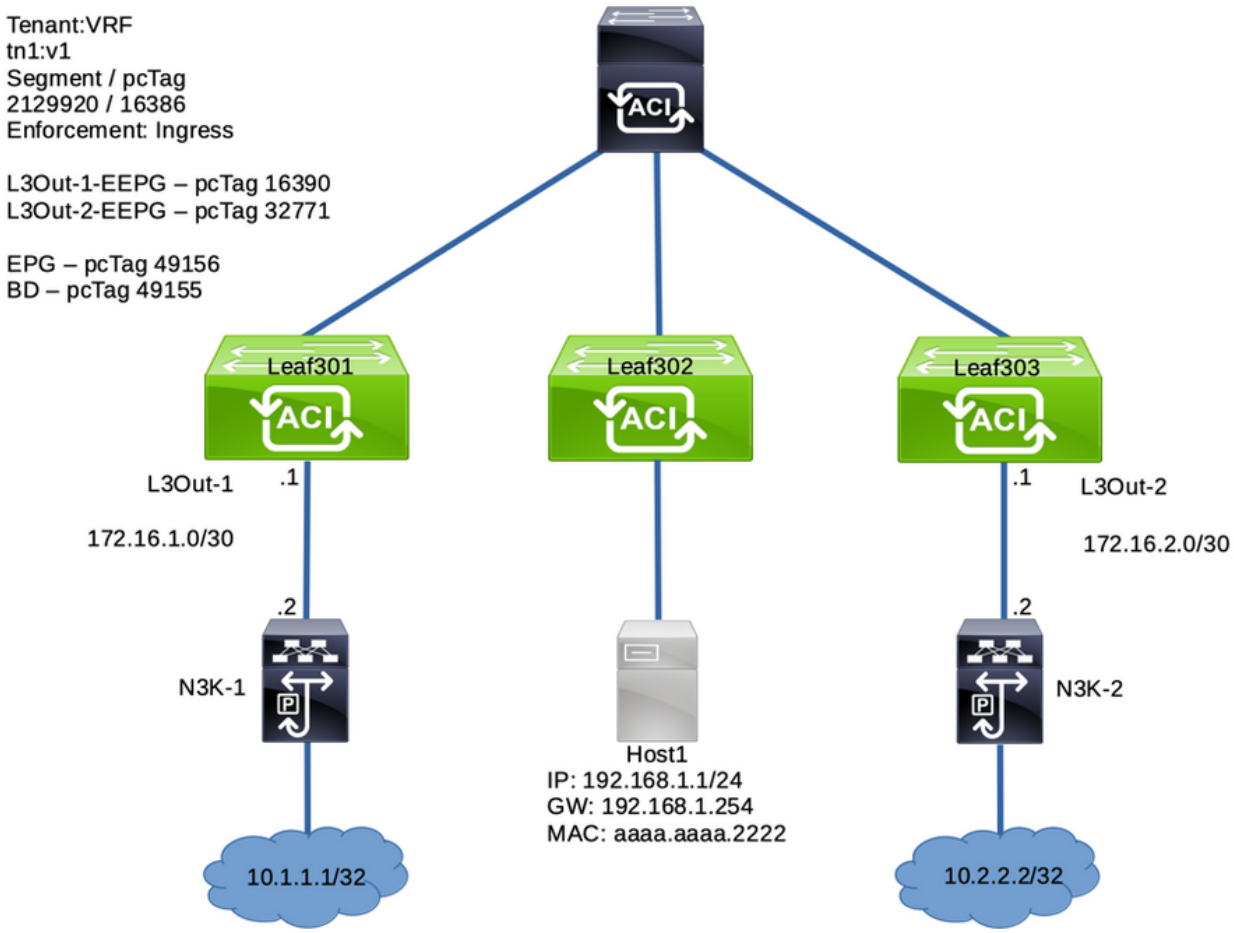
De sectie **"Een uitzondering voor 0.0.0.0/0 met externe subnetten voor de externe EPG"** van het ACI L3Out Whitepaper bevat een waarschuwing:

"...Hoewel het niet wordt aanbevolen, kunt u 0.0.0.0/0 configureren met 'Externe subnetten voor de Externe EPG' in meerdere L3Out EPG's in dezelfde VRF... Terwijl deze configuratie is toegestaan, vindt een onbedoelde implementatie van een contract plaats..."

Dit artikel duikt in die onbedoelde contractplaatsing.

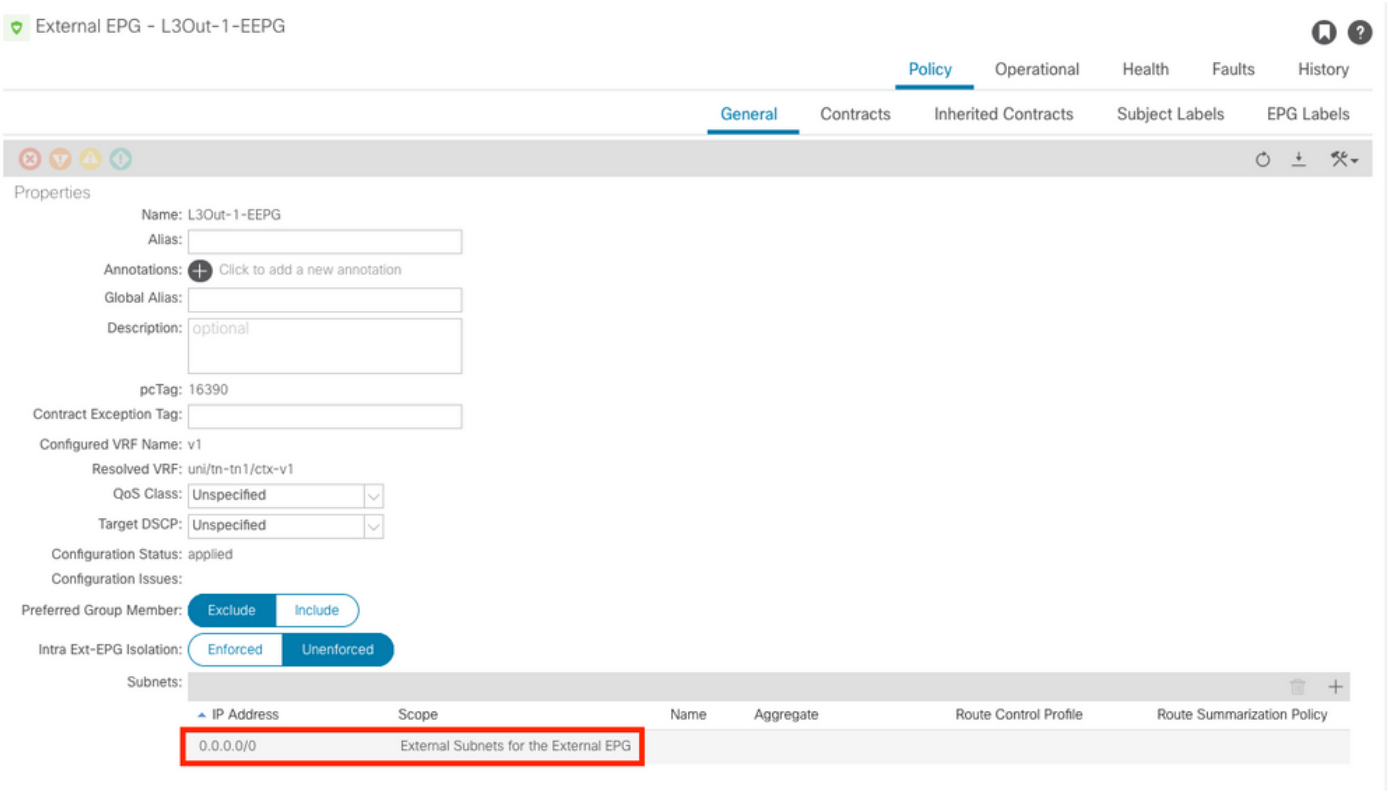
Configureren

Topologiediagram



Configuratiekenmerken

- Bladknooppunten 301 en 303 zijn grensbladknooppunten
- Leaf Node 302 is een niet-grens blad
- L3Out-1-EEPG, op Border Leaf 301, heeft een 0.0.0.0/0-subnet met "Externe Subnets voor Externe EPG"
- L3Out-1-EEPG biedt een contract
- EPG, op niet-grensblad 302, neemt hetzelfde contract



Verifiëren

VRF-beleidsuitvoering met "Ingress"

Regels voor het zones van bladeren buiten de grens

Zoals benadrukt in de sectie Achtergrondinformatie, verkeer dat aan netwerken achter dit L3Out wordt bestemd die Langste prefixgelijke op gevormde 0.0.0.0/0 subnetto krijgt een bestemmingsklasse (pcTag) van 15.

Dit is de tabel met zoningregels op niet-grensblad 302 voor VRF "v1" (segment-ID 2129920):

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

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

Als gevolg van het contract tussen L3Out-1-EEPG en EPG (49156) zijn twee regels opgesteld:

- Regel 4112 is voor extern verkeer afkomstig van de L3Out EPG met 0.0.0.0/0 LPM bestemd voor de EPG. De verkeersstroom is geclassificeerd met de klasse van de VRF PcTag (16386) en de klasse van EPG (49156) .
- Regel 411 is voor verkeer dat afkomstig is van de EPG die bestemd is voor de L3Out EPG met 0.0.0.0/0 LPM. De verkeersstroom is geclassificeerd met de klasse van EPG (49156) en de klasse van System PcTag 15

Zones voor grensbladeren

Border Leaf Node 301 heeft niet dezelfde Zones-Rules als Non-Border Leaf Node 302 vanwege de VRF-beleidsafdwingbaarheid ingesteld op 'Ingress' (standaardwaarde). Het beleid voor dit soort stromen zal naar verwachting worden toegepast op niet-grens bladknooppunten.

```
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 naar L3Out ELAM

Pingel van EPG-eindpunt 192.168.1.1 aan IP achter L3Out-1-EEPG is succesvol:

```
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
```

Een ELAM voor EPG naar L3Out-verkeer op niet-grensblad 302 (EPG-gateway) bevestigt:

1. Het pakket heeft de verwachte bron en bestemming IPs: Bron IP:192.168.1.1, IP-bestemming: 10.1.1.1
2. De bronklasse is de EPG PcTag **49156**

3. De doelklasse (klasse) is System PCTag **15**, aangezien 10.1.1.0/24 Langste prefix overeenkomt met 0.0.0.0/0 Subnet op L3Out-1-EPG
4. Het beleid werd toegepast op dit knooppunt 302, het niet-grens bladknooppunt.

```
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" )
```

Het commando per rapport kan worden ingevoerd voor aanvullende validatie van de Zones-Rule die is ingesteld:

```
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 naar EPG ELAM

De return flow krijgt het beleid toegepast op het niet-grens bladknooppunt 302. Dit wordt verwacht wanneer VRF-beleidshandhaving is ingesteld op "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" )
```

Verdere validatie:

```
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-beleid met "uitgaand" beheer

Regels voor het zones van bladeren buiten de grens

Met VRF Policy Enforcement ingesteld op "Uitgang" worden contractregels voor een L3Out ingezet op zowel Border Leaf als Non-Border Leaf Nodes. Hierdoor neemt deze configuratie extra TCAM-ruimte in vergelijking met "Ingress" Enforcement. Deze configuratie is niet de standaardwaarde en moet, indien gebruikt, zorgvuldig worden overwogen.

Non-Border Leaf Node 302 heeft twee Zones-Rules, één per flow directionality:

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

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

Zones voor grensbladeren

Met "uitgaande" beleidshandhaving heeft Border Leaf Node 301 ook twee extra Zones-regels:

```
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 naar L3Out ELAM

Pingel van het eindpunt 192.168.1.1 aan het netwerk achter L3Out is succesvol:

```
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
```

De ELAM op niet-grens bladknooppunt 302 geeft aan dat **het beleid niet** op dit blad **werd toegepast**. Bovendien, nam het een klasse van **System PcTag 1** om de stroom toe te staan om het volgende bladknooppunt in de stroom te raken:

```
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" )
```

De ELAM op Border Leaf Node 301 geeft aan dat **het beleid op dit knooppunt is toegepast**. Het heeft ook een klasse van **System PcTag 15** opgepikt**.** Dit betekent het langst-prefix afgestemd op de 0.0.0.0/0 L3Out Subnet ingang:

```
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 naar EPG ELAM

In deze instelling is er een waarschuwing met betrekking tot de retourstroom:

- Border Leaf Node 301 heeft geen eindpunt leren voor 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...
```

Als gevolg hiervan wordt het beleid niet toegepast op Border Leaf Node 301 voor deze stroom en moet het impliciet worden toegestaan om het volgende blad te bereiken:

```
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" )
```

In plaats daarvan wordt beleid toegepast op niet-grens bladknooppunt 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
```

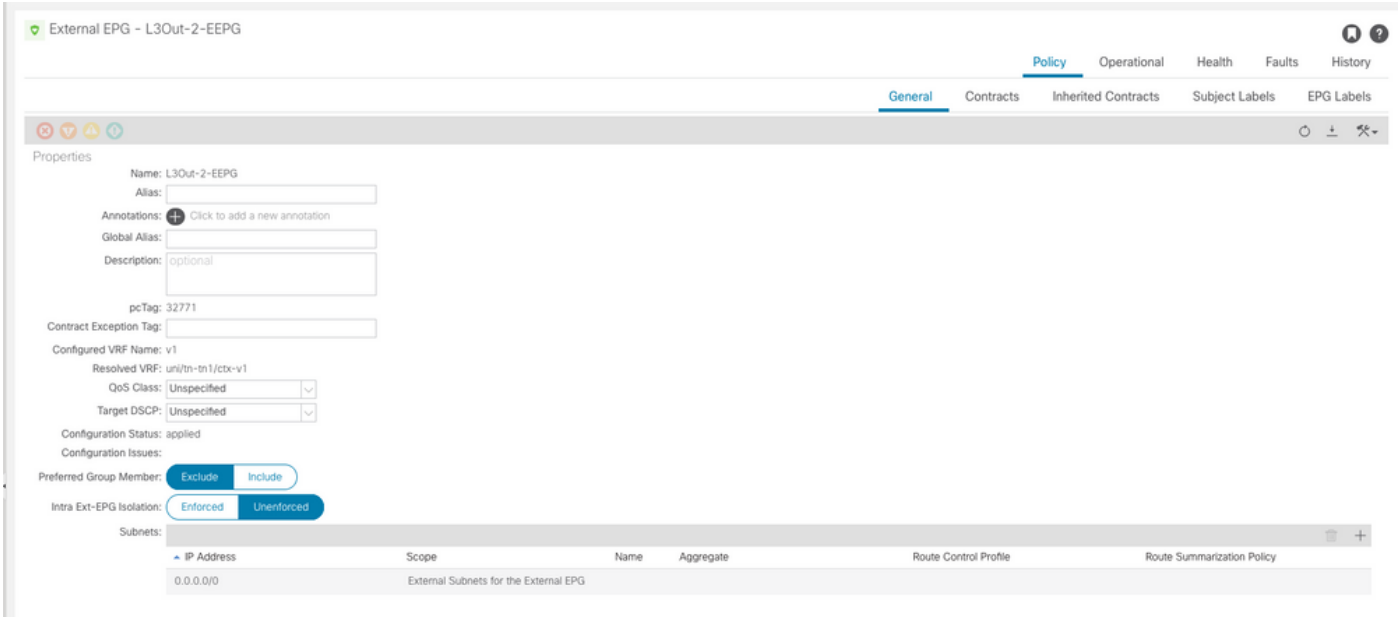
Als Border Leaf Node 301 een eindpunt had leren 192.168.1.1, zou het beleid op dat knooppunt zijn toegepast.

Problemen oplossen

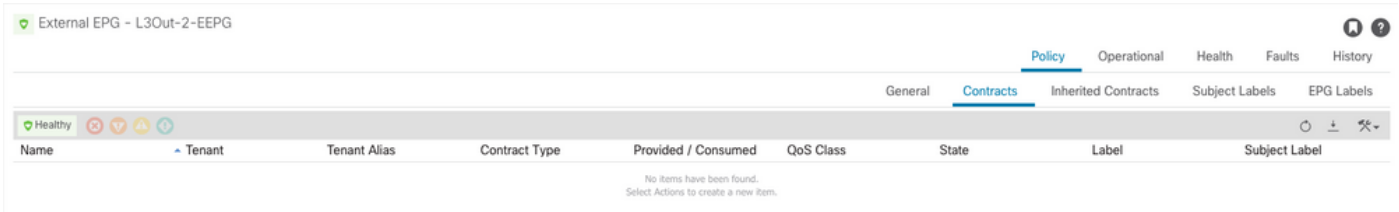
Scenario - onbedoelde rechten

Een uitrol met meerdere L3Outs in dezelfde VRF geconfigureerd met de 0.0.0.0/0 Subnet met "Externe Subnetten voor de Externe EPG" kan verkeer onverwacht laten overgaan naar externe bestemmingen.

Om dit te induceren, voegt u het 0.0.0.0/0 subnet toe onder L3Out-2-EEPG dat zich in dezelfde VRF bevindt als L3Out-1-EEPG.



Er zijn geen contracten op L3Out-2-EEPG, dus we verwachten dat al het verkeer standaard wordt geannuleerd:



Echter, een ping van EPG-eindpunt 192.168.1.1 naar bestemming 10.2.2.2 achter L3Out-2-EEPG is succesvol. Dit is onverwacht!

```
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
```

De voorwaartse route en het beleid-mgr prefix tonen allebei aan dat het verkeer dat aan 10.2.2.2 in dit VRF wordt bestemd Systeem PcTag 15 wordt toegewezen

```
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#
```

Een ELAM op niet-grens bladknooppunt 302 bevestigt dat verkeer is geclassificeerd met een klasse van 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
```

De Zones-Rules voor VRF "v1" geven geen nieuwe waarden voor EPG en L3Out-2 weer:

```
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#
```

Aangezien L3Out-2-EEPG alleen het 0.0.0.0/0-subnet geconfigureerd heeft, is al het verkeer dat ervoor bestemd is geclassificeerd met klasse van System PcTag 15.

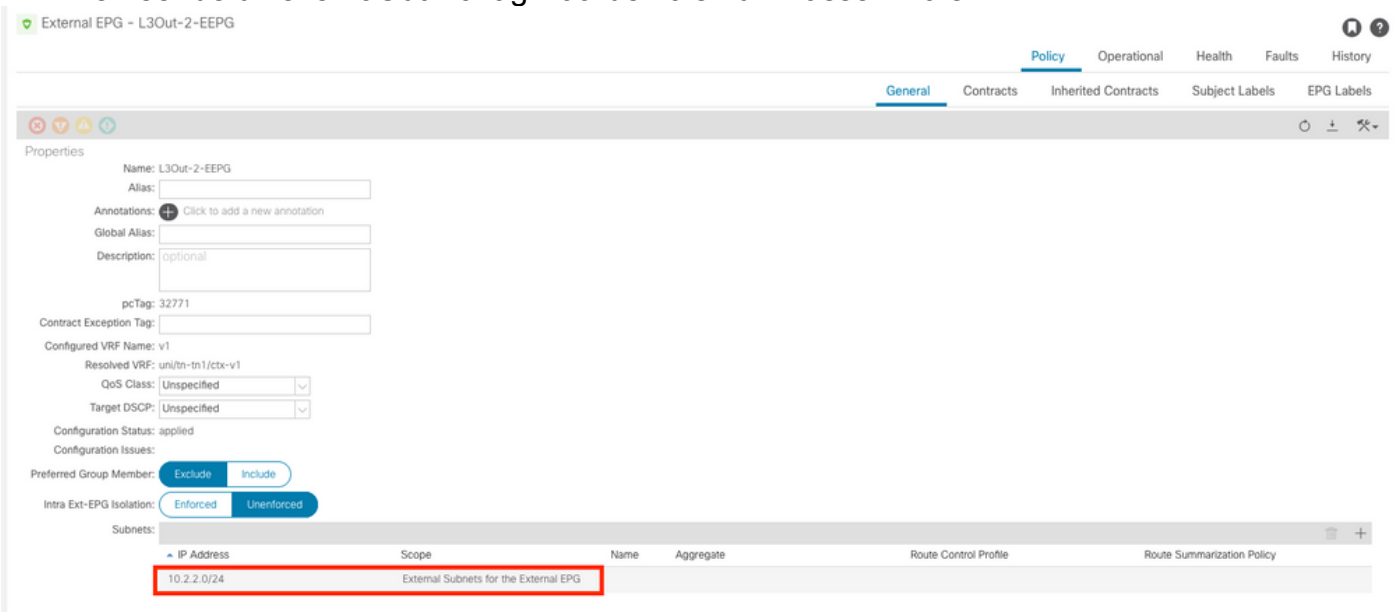
Zones-Rules ID 4111 en 4112 zijn geprogrammeerd als L3Out-1-EEPG heeft zowel het 0.0.0.0/0 Subnet als biedt een contract dat wordt verbruikt door EPG.

Stromen naar L3Out-2-EEPG zijn onverwacht toegestaan vanwege deze configuratie!

Oplossing - onbedoelde toestemmingen

Zo voorkomt u dat:

1. Het is sterk aanbevolen om slechts 0.0.0.0/0 Subnet te gebruiken op één L3Out EPG per VRF
2. Gebruik zo mogelijk specifieke subnetten voor andere L3Outs in dezelfde VRF. Hierdoor kan verkeer de unieke L3Out PcTag waarden als hun klasse inhalen.



Pas deze veranderingen toe om het onverwachte te verzachten toestaan:

1. Vervang op L3Out-2-EPG de subnetpagina 0.0.0.0/0 door een subnetknooppunt 10.2.2.0/24
2. Typ op L3Out-2-EEPG een contract
3. Voer op EPG hetzelfde contract in

Nadat u dit hebt voltooid, kunt u deze wijzigingen bekijken op knooppunt 302 voor niet-grensbladen:

- Er is een meer specifieke policy-mgr prefix voor 10.2.2.0/24 gekoppeld aan L3Out-2-EEPG PcTag 32771
- Er is een Zones-Rules ID 4109 ingang Dit artikel maakt een stroom mogelijk van EPG PcTag 49156 naar L3Out-2-EEPG PcTag 32771
- Er is een ingang voor Zones-Rules ID 4110 Dit artikel maakt een stroom mogelijk van L3Out-2-EEPG PcTag 32771 naar EPG PcTag 49156

De bijgewerkte voorwaartse route en policy-mgr prefix die aantonen dat 10.2.2.2 is toegewezen de L3Out-2-EEPG PgTag van 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
```

Opmerking: Zones-Rules IDs 4111 en 4112 bestaan nog steeds op Non-Border Leaf Node 302, aangezien L3Out-1-EEPG nog steeds 0.0.0.0/0 Subnet heeft en ook een contractrelatie heeft met EPG. Echter, L3Out-2-EEPG verkeer niet meer onbedoeld gebruik van die regels, aangezien zijn verkeer nu wordt geclassificeerd met de L3Out PcTag, en niet systeem 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)    |
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Pingen van de EPG-host naar de externe bestemming achter L3Out-2-EEPG is succesvol:

```
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
```

De ELAM voor het ICMP-verzoek op Non-Border Leaf Node 302 geeft aan dat de klasse nu 32771 is - de PcTag van 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" )
...
```

Het opgegeven rapport geeft aan dat deze stroom een van de nieuwe Zones-regels raakt, met name Regel-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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.