Fehlerbehebung bei ACI L3Out - Subnetz 0.0.0.0/0 und System PcTag 15

Inhalt

Einleitung

In diesem Dokument wird die PcTag-Ableitung des Subnetzes 0.0.0.0/0 bei Definition in einer L3Out-EPG beschrieben.

Hintergrundinformationen

Im Abschnitt **"L3Out EPG with 0.0.0.0/0 subnet"** des ACI-Vertragsleitfadens wird 0.0.0.0/0 mit der Klassifizierung des Datenverkehrs im Bereich "Externe Subnetze für die externe EPG" wie folgt zusammengefasst:

- Datenverkehr, der von einem L3Out stammt, bei dem es sich um das längste Präfix handelt, das mit einem konfigurierten Subnetz von 0.0.0.0/0 abgeglichen wurde, wird der Quellklassenkennung (Klasse) des VRF PcTag zugewiesen.
- Datenverkehr, der an eine L3Out-EPG mit dem längsten Präfix gerichtet ist, das mit einem konfigurierten Subnetz mit der Adresse 0.0.0.0/0 abgeglichen wird, wird die Zielklassen-ID (dclass) von 15 zugewiesen, ein System-PcTag.

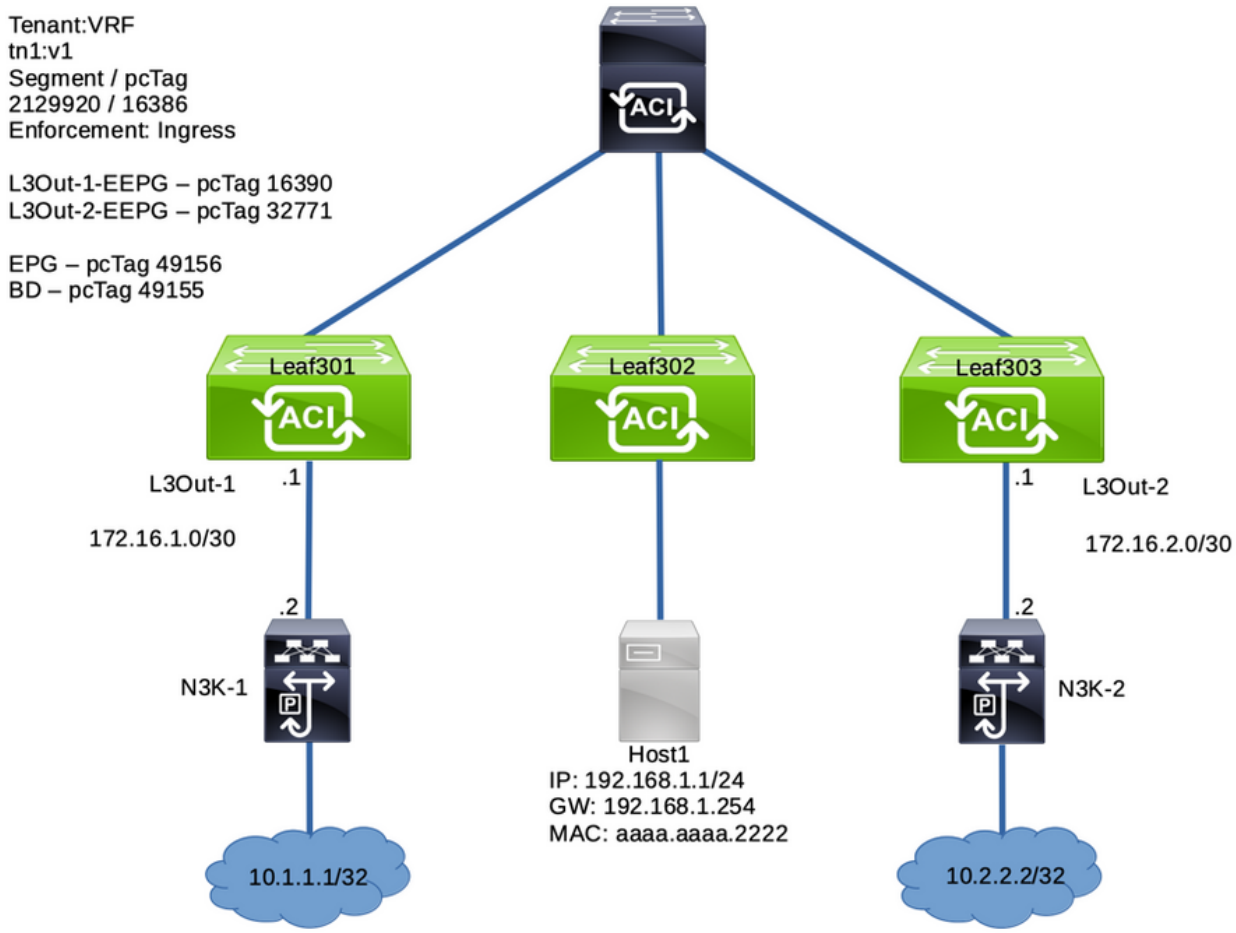
Der Abschnitt **"Eine Ausnahme für 0.0.0.0/0 mit externen Subnetzen für die externe EPG"** des ACI L3Out-Whitepapers enthält eine Warnung:

"...Obwohl es nicht empfohlen wird, können Sie 0.0.0.0/0 mit "Externen Subnetzen für die externe EPG" in mehreren L3Out-EPGs in derselben VRF-Instanz konfigurieren... Diese Konfiguration ist zulässig, es erfolgt jedoch eine unbeabsichtigte Vertragsbereitstellung ..."

In diesem Artikel wird näher auf die unbeabsichtigte Vertragsbereitstellung eingegangen.

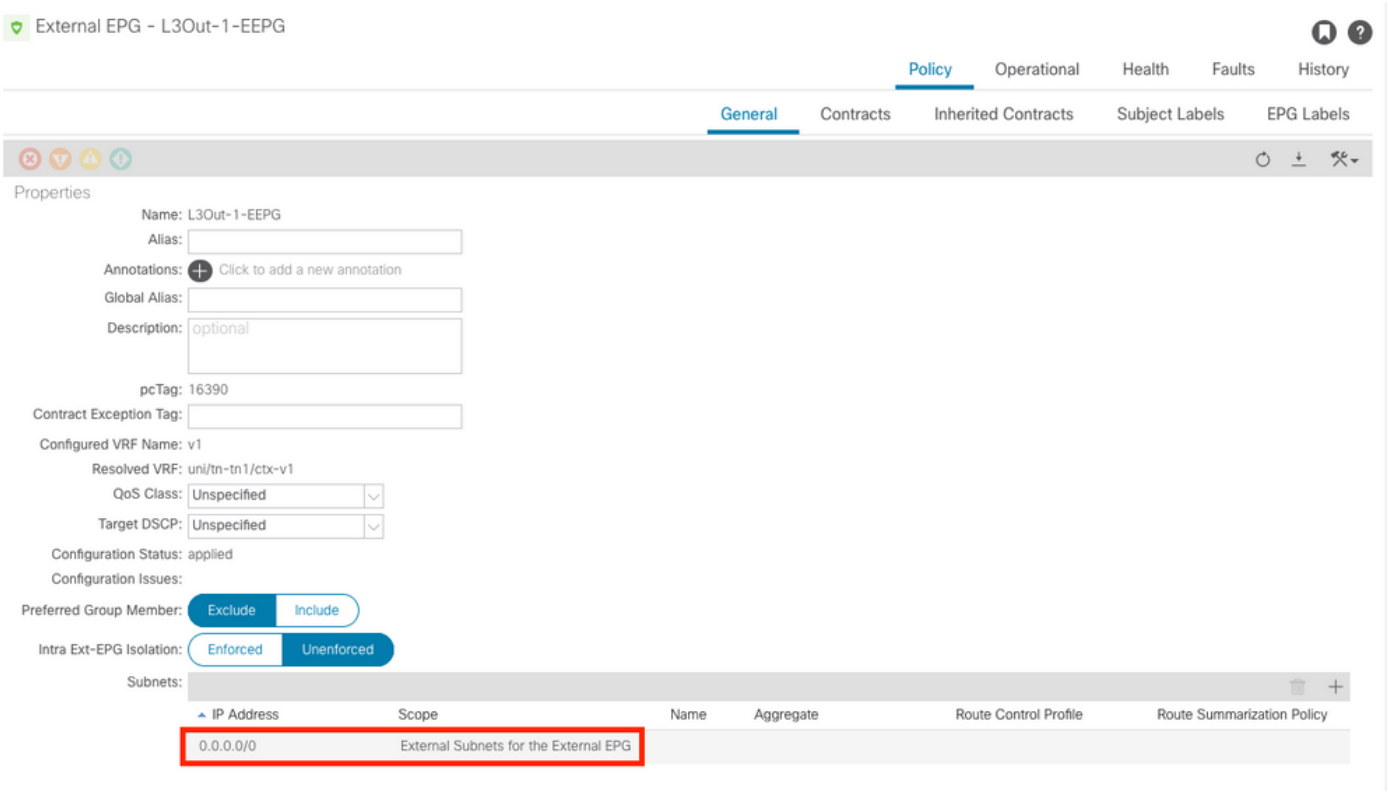
Konfigurieren

Topologiediagramm



Highlights der Konfiguration

- Die Leaf-Knoten 301 und 303 sind Border Leaf-Knoten.
- Leaf Node 302 ist ein Non-Border Leaf
- L3Out-1-EEPG auf Border Leaf 301 verfügt über ein 0.0.0.0/0-Subnetz mit "externen Subnetzen für die externe EPG"
- L3Out-1-EEPG bietet einen Vertrag
- Die EPG nutzt auf dem Non-Border Leaf 302 denselben Vertrag



Überprüfung

VRF mit Richtliniendurchsetzung bei Eingang

Nicht-Grenzblatt-Zoning-Regeln

Wie im Abschnitt "Hintergrundinformationen" hervorgehoben, erhält Datenverkehr, der für Netzwerke hinter diesem L3Out bestimmt ist, für die das längste Präfix auf dem konfigurierten Subnetz 0.0.0.0/0 gilt, die Zielklasse (pcTag) 15.

Dies ist die Tabelle mit den Zonenregeln für den Non-Border Leaf 302 für 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)    |
```

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

Aufgrund des Vertrags zwischen L3Out-1-EEPG und EPG (49156) wurden zwei Regeln installiert:

- Regel 4112 gilt für externen Datenverkehr, der von der L3Out-EPG mit 0.0.0.0/0 LPM stammt und für die EPG bestimmt ist. Der Datenverkehrsfluss wird mit der Klasse des VRF PcTag (16386) und der Klasse der EPG (49156) klassifiziert.
- Regel 4111 gilt für Datenverkehr, der von der EPG stammt und für die L3Out-EPG mit 0.0.0.0/0 LPM bestimmt ist. Der Datenverkehrsfluss wird anhand der EPG-Klasse (49156) und der System-PcTag-Klasse 15 klassifiziert.

Zoning-Regeln für Grenzblätter

Der Border Leaf Node 301 verfügt aufgrund der VRF-Richtliniendurchsetzung auf "Ingress" (Standardwert) nicht über dieselben Zoning-Regeln wie der Non-Border Leaf Node 302. Richtlinien für diese Arten von Datenflüssen sollen auf Nicht-Grenzblätterknoten angewendet werden.

```
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 zu L3Out ELAM

Ein Ping von EPG-Endpunkt 192.168.1.1 an die IP-Adresse hinter L3Out-1-EEPG ist erfolgreich:

```
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
```

Ein ELAM für Datenverkehr vom Typ "EPG zu L3Out" auf Non-Border Leaf 302 (EPG-Gateway) bestätigt Folgendes:

1. Das Paket hat die erwarteten Quell- und Ziel-IPs: Quell-IP:192.168.1.1, Ziel-IP: 10.1.1.1
2. Die Quellklasse (Klasse) ist das EPG PcTag **49156**
3. Die Zielklasse (dclass) ist System PcTag **15,** da das längste Präfix 10.1.1.0/24 mit dem Subnetz 0.0.0.0/0 auf L3Out-1-EEPG übereinstimmt.
4. Die Richtlinie wurde auf diesen Node 302, den Non-Border Leaf Node, angewendet.

```
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" )
```

Der Befehl von report kann zur zusätzlichen Validierung der Zoning-Regel eingegeben werden, die getroffen wurde:

```
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
```

L3Aus zu EPG ELAM

Der Rücklauf wird auf den Non-Border Leaf Node 302 angewendet. Dies wird erwartet, wenn die VRF-Richtliniendurchsetzung auf "Ingress" (Eingehend) festgelegt ist.

```
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" )
```

Weitere Validierung:

```
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 mit Durchsetzung von "Egress"-Richtlinien

Nicht-Grenzblatt-Zoning-Regeln

Wenn die VRF-Richtliniendurchsetzung auf "Egress" (Ausgehend) gesetzt ist, werden Vertragsregeln für einen L3Out sowohl auf Grenz-Leaf- als auch auf Nicht-Grenz-Leaf-Knoten bereitgestellt. Dadurch belegt diese Konfiguration im Vergleich zur Durchsetzung der Eingangsregeln zusätzlichen TCAM-Speicherplatz. Diese Konfiguration ist nicht der Standardwert und muss bei Verwendung sorgfältig geprüft werden.

Non-Border Leaf Node 302 verfügt über zwei Zoning-Regeln, eine pro Flussrichtung:

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

Zoning-Regeln für Grenzblätter

Mit der Durchsetzung von Richtlinien für den "Ausgang" verfügt Border Leaf Node 301 außerdem über zwei zusätzliche Zoning-Regeln:

```
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 zu L3Out ELAM

Ein Ping vom Endpunkt 192.168.1.1 zum Netzwerk hinter dem L3Out ist erfolgreich:

```
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
```

Der ELAM für Non-Border Leaf Node 302 gibt an, dass auf diesem Leaf **keine Richtlinie angewendet wurde**. Darüber hinaus wurde eine Klasse von **System-PCtag 1** aufgenommen, damit der Fluss auf den nächsten Leaf-Knoten im Fluss treffen kann:

```
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" )
```

Der ELAM-Knoten 301 für Grenz-Leaf gibt an, dass **die Richtlinie auf diesen Knoten angewendet wurde**. Es wurde auch eine Klasse des **System-PcTag 15** erkannt. Dies bedeutet, dass das Präfix am längsten mit dem L3Out-Subnetzeintrag 0.0.0.0/0 übereinstimmt:

```
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
```

L3Aus zu EPG ELAM

In dieser Konfiguration besteht ein Problem mit dem Rücklauf:

- Border Leaf Node 301 verfügt nicht über einen Endpunkt, der für 192.168.1.1 gelernt wurde.

```
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...
```

Daher wird die Richtlinie für diesen Fluss auf Border Leaf Node 301 nicht angewendet und es muss implizit zugelassen werden, dass er das nächste Leaf erreicht:

```
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" )
```

Stattdessen wird die Richtlinie auf den Non-Border Leaf Node 302 angewendet:

```
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
```

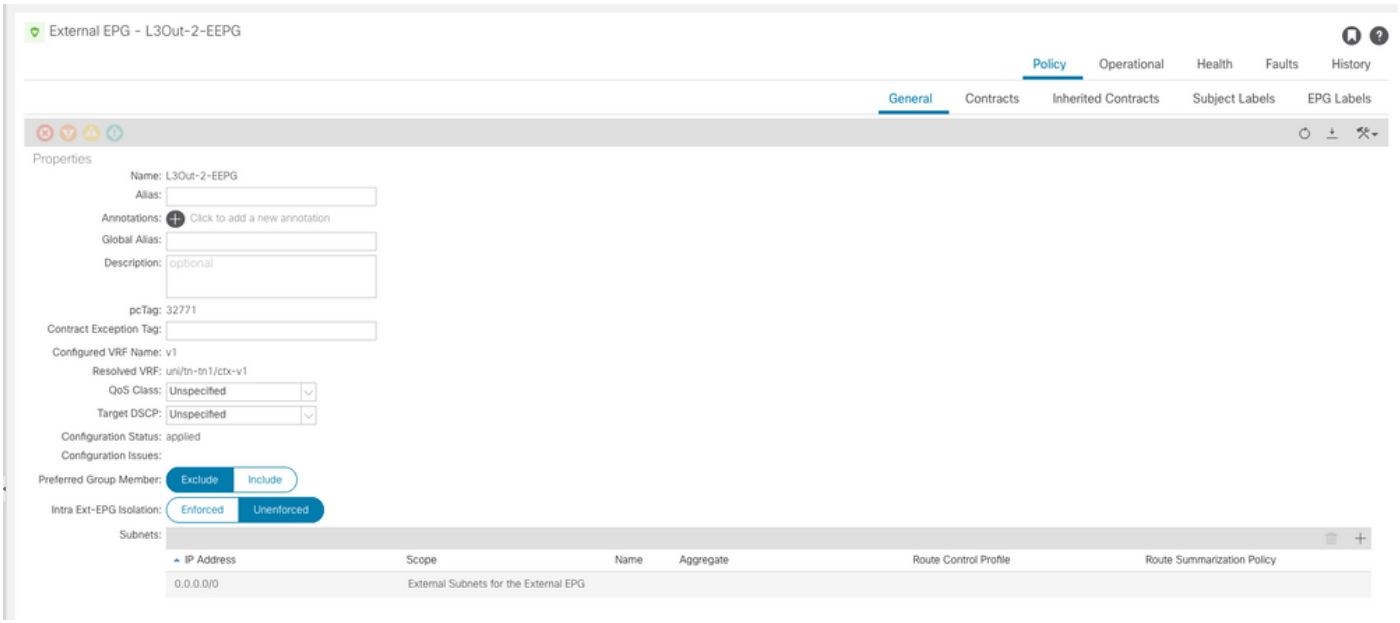
Hätte Border Leaf Node 301 den Endpunkt 192.168.1.1, wäre die Richtlinie auf diesen Knoten angewendet worden.

Fehlerbehebung

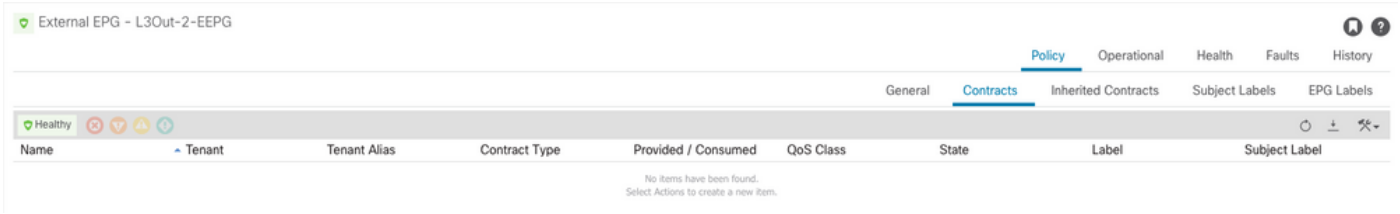
Szenario - Unbeabsichtigt erlaubt

Bei einer Bereitstellung mit mehreren L3Outs in derselben VRF-Instanz, die mit dem Subnetz 0.0.0.0/0 mit "Externen Subnetzen für die externe EPG" konfiguriert wurde, kann der Datenverkehr unerwartet an externe Ziele weitergeleitet werden.

Fügen Sie dazu das Subnetz 0.0.0.0/0 unter L3Out-2-EEPG hinzu, das sich in derselben VRF-Instanz wie L3Out-1-EEPG befindet.



Es gibt keine Verträge für L3Out-2-EEPG, daher gehen wir davon aus, dass standardmäßig der gesamte Datenverkehr verworfen wird:



Ein Ping von EPG-Endpunkt 192.168.1.1 an Ziel 10.2.2.2 hinter L3Out-2-EEPG ist jedoch erfolgreich. Das ist unerwartet!

```
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
```

Die Weiterleitung und das Policy-Mgr-Präfix zeigen an, dass der an 10.2.2.2 in dieser VRF-Instanz gerichtete Datenverkehr dem System-PCtag 15 zugewiesen ist.

```
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#
```

Ein ELAM auf Non-Border Leaf Node 302 validiert, dass der Datenverkehr mit einer Klasse des System-PCtag 15 klassifiziert wird.

```
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
```

Die Zoning-Regeln für VRF "v1" enthalten keine neuen Einträge für EPG und 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#
```

Da für L3Out-2-EEPG nur das Subnetz 0.0.0.0/0 konfiguriert ist, wird der gesamte an dieses Subnetz gerichtete Datenverkehr mit der Klasse System PcTag 15 klassifiziert.

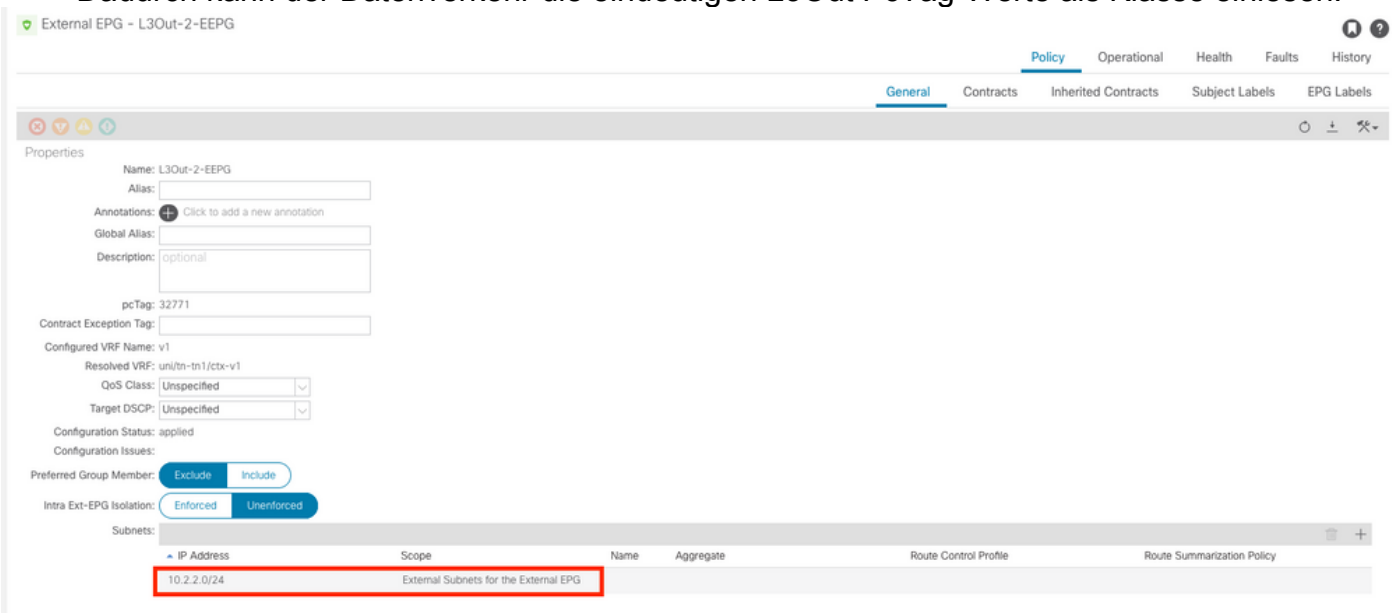
Die Zoning-Rules ID 4111 und 4112 sind so programmiert, dass L3Out-1-EEPG sowohl das Subnetz 0.0.0.0/0 als auch einen Vertrag bereitstellt, der von EPG genutzt wird.

Datenflüsse nach L3Out-2-EEPG sind aufgrund dieser Konfiguration unerwartet zulässig!

Lösung - unbeabsichtigt erlaubt

So verhindern Sie dieses Verhalten:

1. Es wird dringend empfohlen, das Subnetz 0.0.0.0/0 nur auf einer L3Out-EPG pro VRF zu verwenden.
2. Verwenden Sie nach Möglichkeit spezifische Subnetze für andere L3Outs im gleichen VRF. Dadurch kann der Datenverkehr die eindeutigen L3Out PcTag-Werte als Klasse einlesen.



Wenden Sie diese Änderungen an, um die unerwartete Erlaubnis einzuschränken:

1. Ersetzen Sie auf L3Out-2-EEPG das Subnetz 0.0.0.0/0 durch ein Subnetz 10.2.2.0/24.
2. Auf L3Out-2-EEPG einen Vertrag abschließen
3. Verwenden Sie für eine EPG denselben Vertrag

Beachten Sie nach Abschluss dieses Vorgangs die folgenden Änderungen bei Non-Border Leaf Node 302:

- Es gibt ein spezifischeres policy-mgr-Präfix für 10.2.2.0/24 in Verbindung mit L3Out-2-EEPG PcTag 32771.
- Es gibt einen Eintrag für Zoning-Rules ID 4109. Dieser Eintrag ermöglicht einen Fluss von EPG PcTag 49156 zu L3Out-2-EEPG PcTag 32771
- Es gibt einen Eintrag für die Zoning-Rules ID 4110. Dieser Eintrag ermöglicht einen Fluss von L3Out-2-EEPG PcTag 32771 zu EPG PcTag 49156

Das aktualisierte Forward-Routing- und Policy-Mgr-Präfix, das angibt, dass 10.2.2.2 das L3Out-2-EEPG PgTag von 32771 zugewiesen ist:

```
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
```

Anmerkung: Die Zoning-Rules-IDs 4111 und 4112 sind auf dem Non-Border Leaf Node 302 weiterhin vorhanden, da L3Out-1-EEPG noch das Subnetz 0.0.0.0/0 hat und außerdem eine Vertragsbeziehung mit der EPG hat. Der L3Out-2-EEPG-Datenverkehr verwendet diese Regeln jedoch nicht mehr versehentlich, da sein Datenverkehr jetzt mit dem L3Out-PcTag klassifiziert wird, und nicht dem System-PcTag 15:

```
Leaf-302# show zoning-rule scope 2129920
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
|   4107  |   0    |   0    | implarp  |    uni-dir     | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit |    uni-dir     | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit |    uni-dir     | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit |    uni-dir     | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  |    uni-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  |    uni-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4109  | 49156  | 32771  | default  |     bi-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4110  | 32771  | 49156  | default  | uni-dir-ignore | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Ping vom EPG-Host zum externen Ziel hinter L3Out-2-EEPG ist erfolgreich:

```
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
```

Die ELAM für die ICMP-Anforderung auf dem Non-Border Leaf Node 302 gibt an, dass die Klasse jetzt 32771 ist - das PcTag von 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" )
...
```

Der angegebene aclqos-Befehl zeigt, dass dieser Fluss eine der neuen Zoning-Regeln erreicht, insbesondere 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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.