Solución de problemas de ACI L3Out: subred conectada directamente PcTag1

Contenido

Introducción

Este documento describe un escenario donde el tráfico originado en una subred L3Out conectada directamente sin la configuración adecuada bajo el EPG externo puede conducir a caídas de contratos.

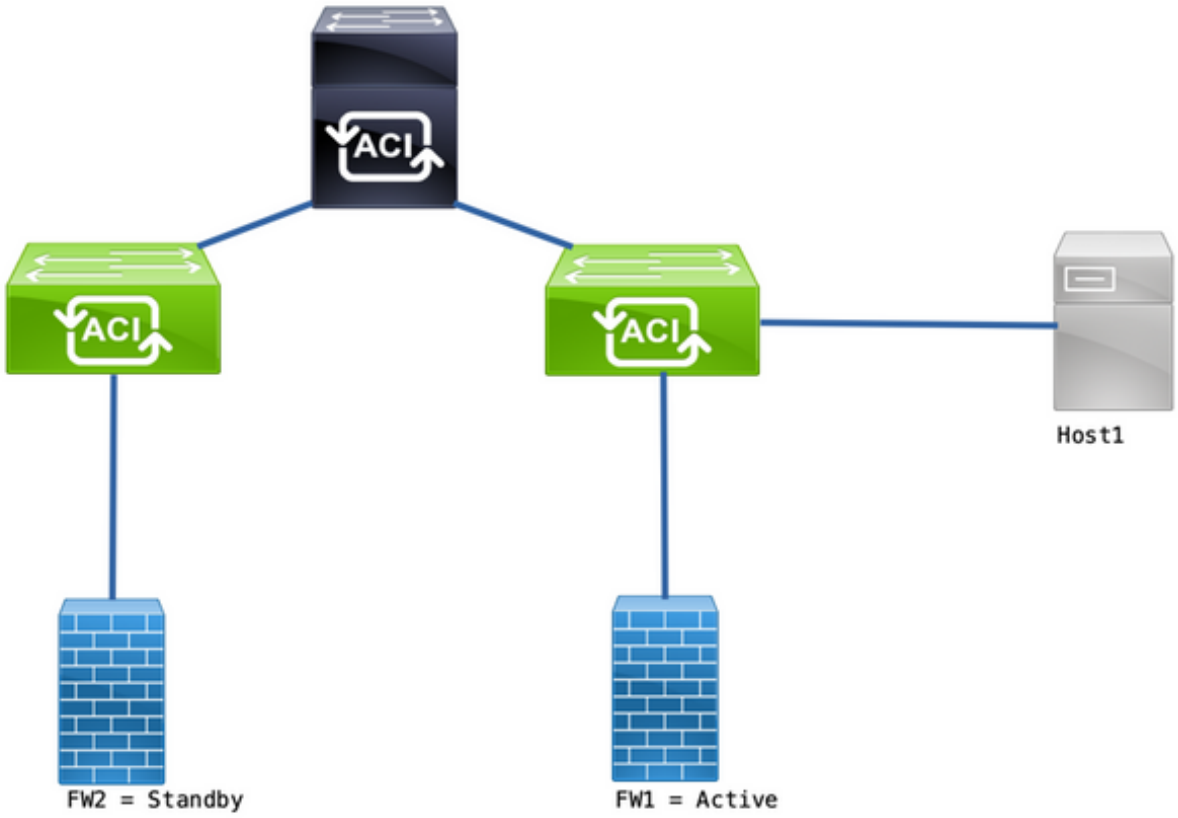
Antecedentes

La sección "**Una excepción para una subred conectada directamente con 0.0.0.0/0**" del Informe técnico de L3out de ACI señala este comportamiento con respecto a pcTag 1:

"...de forma predeterminada, a las subredes conectadas directamente se les asigna pcTag 1, que es un pcTag especial para saltarse un contrato. Esto es para permitir implícitamente las comunicaciones de protocolo de ruta en un escenario de casos de esquina. Sin embargo, esto puede causar problemas de seguridad. Por lo tanto, este comportamiento se explica en detalle a través del ID de bug de Cisco CSCuz12913 , que también introduce una configuración de solución alternativa:"

El escenario

Topología y configuración



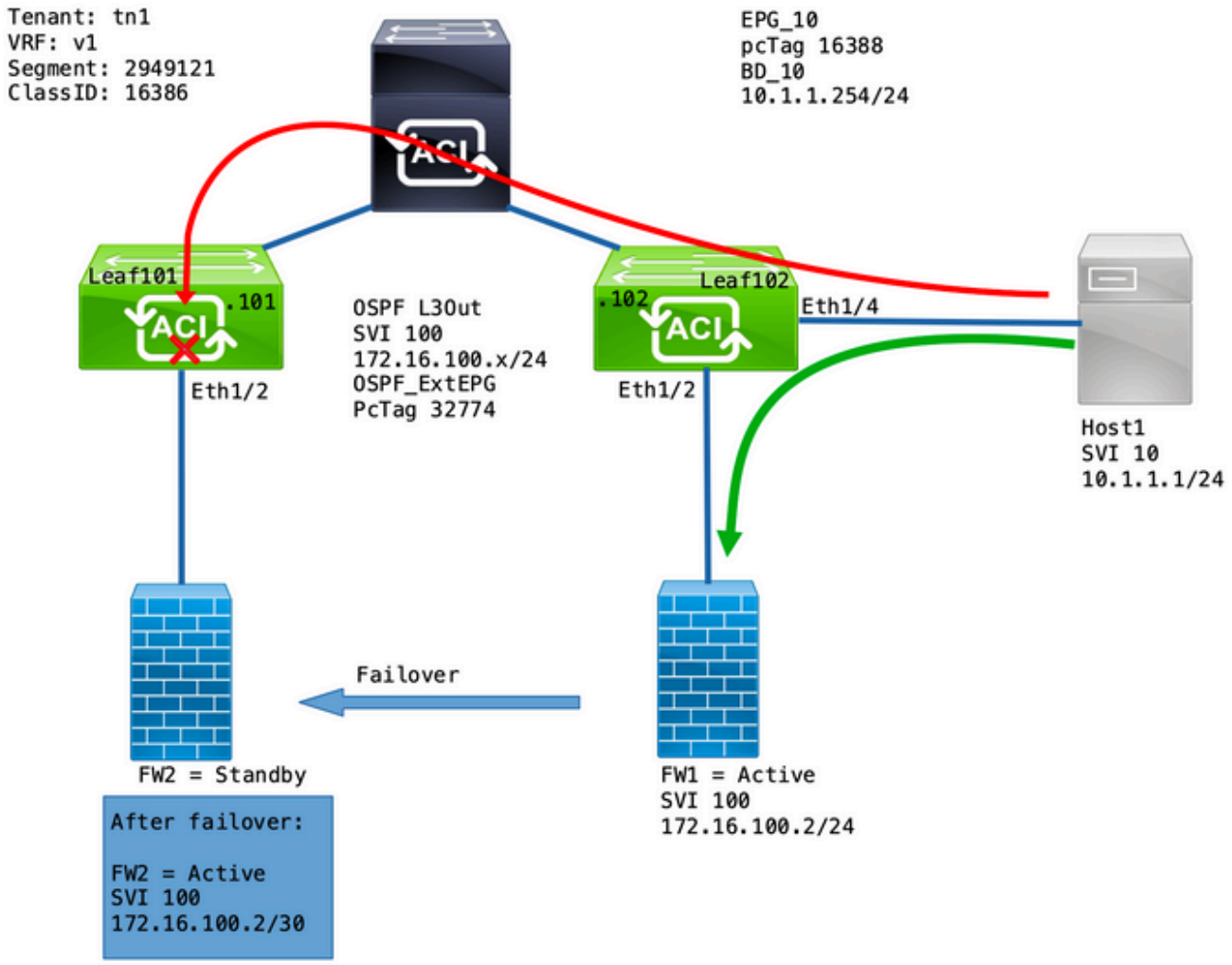
Topología

- Los firewalls (FW) se configuran con traducción de direcciones de red (NAT).
- Todo el tráfico enviado al fabric ACI se origina en la IP del firewall que forma la adyacencia OSPF con ACI.
- El EPG externo tiene una red 0.0.0.0/0 configurada con **subredes externas para el EPG externo**.
- Existe un contrato para la comunicación entre el EPG interno y el EPG externo.

Problema observado

Con FW1 como dispositivo activo, el tráfico funciona según lo esperado. No se han observado caídas.

Después de que los servicios de firewall conmuten por error a FW2, se pierde la conectividad: 10.1.1.1 y 172.16.100.2 ya no pueden comunicarse.



Problema en profundidad

Una captura ELAM en Leaf101 nos permite validar si el tráfico del Host1 al FW2 se descarta.

Se utilizaron estas opciones de ELAM:

```
leaf101# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 14 out-select 1
module-1(DBG-elam-insel14)# set inner ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel14)# start
module-1(DBG-elam-insel14)# status
```

Cuando se activa, el informe electrónico permite ver los resultados de la búsqueda:

```
<snip>
================================================================================================
================================================
Captured Packet
================================================================================================
================================================
<snip>
------------------------------------------------------------------------------------------------
```

```
------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------
------------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 254
IP Protocol Number : ICMP
Destination IP                  : 172.16.100.2   <<<----
Source IP                       : 10.1.1.1   <<<----
<snip>
================================================================================================
================================================
Contract Lookup ( FPC )
================================================================================================
================================================

------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------------
IP Protocol : ICMP( 0x1 )
L4 Src Port : 2048( 0x800 )
L4 Dst Port : 52579( 0xCD63 )
sclass (src pcTag)                      : 16388( 0x4004 )   <<<----
dclass (dst pcTag)                      : 16386( 0x4002 )   <<<----
<snip>

------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Drop                           : yes   <<<----
Contract Logging : yes
Contract Applied : no
Contract Hit : yes
Contract Aclqos Stats Index : 81824
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81824" )
```

Este informe muestra que el flujo es Contrato descartado junto con estos detalles:

- El valor de SCLASS es 16388, que es la pcTag de EPG_10.
- DCLASS es 16386, que es la pcTag del VRF v1.

A continuación, valide las reglas de zonificación para el VRF:

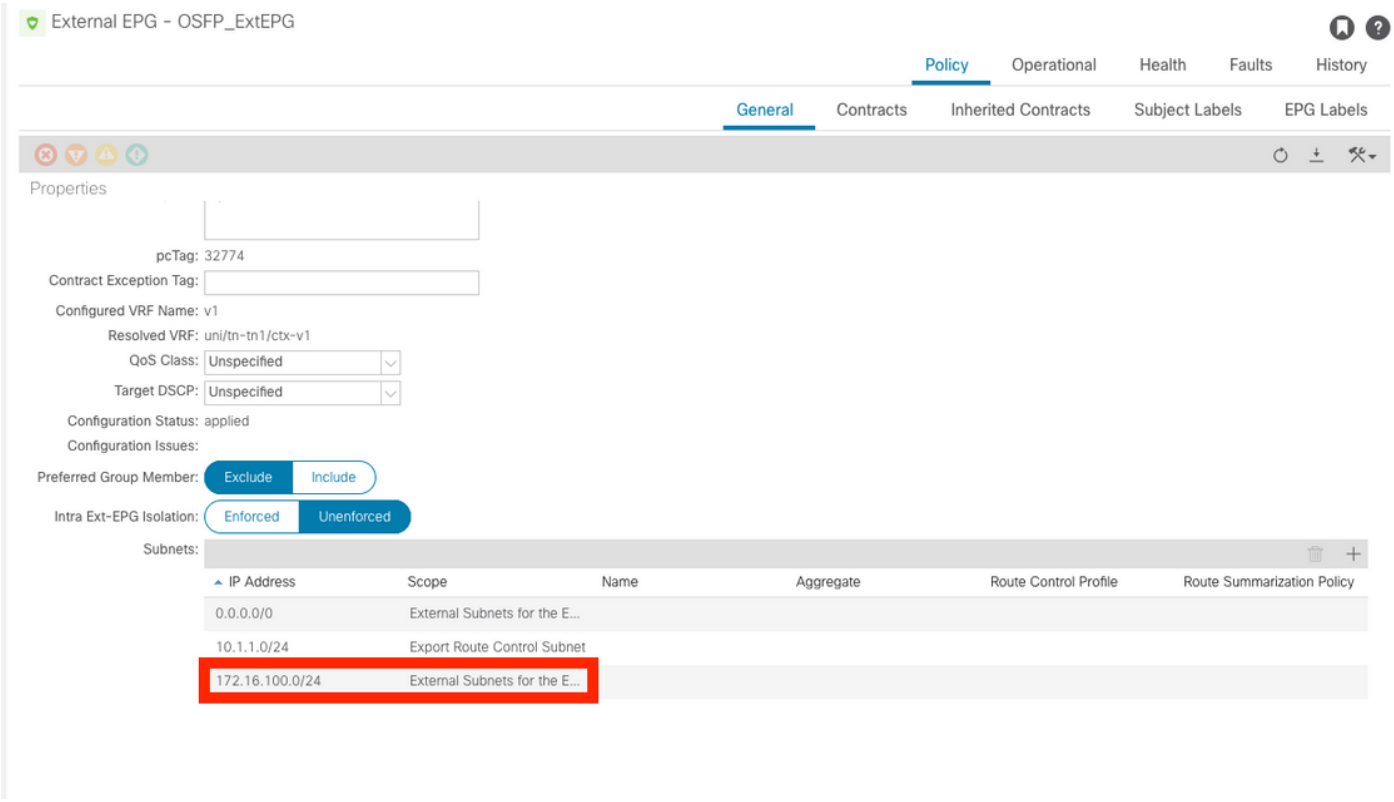
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4131  |   0    |   15   | implicit | uni-dir | enabled | 2949121 |                  |
deny,log | any_vrf_any_deny(22) |
|   4130  |   0    |   0    | implarp  | uni-dir | enabled | 2949121 |                  |
permit  |  any_any_filter(17)  |
|   4129  |   0    |   0    | implicit | uni-dir | enabled | 2949121 |                  |
deny,log |   any_any_any(21)    |
|   4132  |   0    | 49155  | implicit | uni-dir | enabled | 2949121 |                  |
```

```
permit  |   any_dest_any(16)    |
|   4112  | 16386  | 16388  | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)     |
|   4133  | 16388  |   15   | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)     |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+-----------------------+
```

Existe un contrato para la comunicación de EPG_10 (16388) a redes detrás de OSPF L3Out (0.0.0.0/0 = 15). Sin embargo, el tráfico de 172.16.100.2 está etiquetado bajo la pcTag de VRF v1 (16386).

Solución

Agregue la subred conectada directamente del L3Out bajo OSPF Ext_EPG.



Esta adición tiene 2 efectos:

1. El tráfico de la subred conectada directamente se etiqueta en OSPF_ExtEPG pcTag (32774)
2. Las reglas se agregan para permitir el flujo hacia y desde EPG_10 y OSPF_ExtEPG

```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+----------------+---------+---------+------------------
+----------+----------------------+ | Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt |
Scope | Name | Action | Priority | +---------+--------+--------+----------+----------------+----
-----+---------+------------------+----------+----------------------+ | 4131 | 0 | 15 | implicit
| uni-dir | enabled | 2949121 | | deny,log | any_vrf_any_deny(22) | | 4130 | 0 | 0 | implarp |
uni-dir | enabled | 2949121 | | permit | any_any_filter(17) | | 4129 | 0 | 0 | implicit | uni-
dir | enabled | 2949121 | | deny,log | any_any_any(21) | | 4132 | 0 | 49155 | implicit | uni-dir
| enabled | 2949121 | | permit | any_dest_any(16) | | 4112 | 16386 | 16388 | default | uni-dir |
enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | | 4133 | 16388 | 15 | default |
uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | | 4134 | 16388 |
32774 | default | bi-dir | enabled | 2949121 | tn1:EPG-to-L3Out | permit |
src_dst_any(9) | <<<----
```

```
|   4135  | 32774  | 16388  | default  | uni-dir-ignore | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |  <<<----
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Explicación

La razón por la que esto funciona cuando el FW y el Host están conectados a la misma hoja (sin la adición de subred L3Out) es porque las subredes conectadas directamente utilizan una pcTag especial de 1 que omite todos los contratos. Esto es para permitir implícitamente las comunicaciones de protocolo de ruta en un escenario de casos de esquina.

Con estos disparadores podemos capturar un flujo de tráfico de 172.16.100.2 a 10.1.1.1 mientras estamos en Leaf102:

```
leaf102# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 172.16.100.2 dst_ip 10.1.1.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
```

Este informe muestra los resultados de la búsqueda:

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================================
=====================================================
                                                                    Captured Packet
================================================================================================================
=====================================================

----------------------------------------------------------------------------------------------------------------
----------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------
L3 Type                       : IPv4
IP Version                    : 4
DSCP                          : 0
IP Packet Length              : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit            : not set
TTL                           : 255
IP Protocol Number            : ICMP
IP CheckSum                   : 32320( 0x7E40 )
Destination IP                : 10.1.1.1      <<<----
Source IP                     : 172.16.100.2  <<<----

================================================================================================================
=====================================================
```

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

----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 0( 0x0 )
L4 Dst Port                              : 19821( 0x4D6D )
sclass (src pcTag)                       : 1( 0x1 )           <<<----
dclass (dst pcTag)                       : 16388( 0x4004 )    <<<----
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
```

Para validar el flujo de retorno:

```
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
============
Asic 0 Slice 0 Status Triggered
```

Resultados de la búsqueda del flujo de retorno:

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================================
================================================
                                                                        Captured Packet
================================================================================================================
================================================
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
L3 Type                        : IPv4
IP Version                     : 4
DSCP                           : 0
IP Packet Length               : 84 ( = IP header(28 bytes) + IP payload )
```

```
Don't Fragment Bit            : not set
TTL                           : 255
IP Protocol Number            : ICMP
IP CheckSum                   : 32198( 0x7DC6 )
Destination IP                : 172.16.100.2  <<<----
Source IP                     : 10.1.1.1      <<<----

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

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 2048( 0x800 )
L4 Dst Port                           : 18134( 0x46D6 )
sclass (src pcTag)                    : 16388( 0x4004 ) <<<----
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
```

Esta tabla resume el comportamiento esperado en los switches Gen2:

Situación	Direccionalidad	Cancelación de contrato	Sin eliminación de co
En la misma hoja Aplicación de políticas VRF: Ambas	X a L3Out		X
	L3Out a X		X
En 2 nodos de hoja Aplicación de políticas VRF: Acceso	X a L3Out	X	
	L3Out a X		X
En 2 nodos de hoja Aplicación de políticas VRF: Egress	X a L3Out		X
	L3Out a X		X

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

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

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