ACI L3Out — 直連子網PcTag1故障排除

目錄

簡介

本檔案將說明以下情況：源自直接連線的L3Out子網且在外部EPG下沒有正確組態的流量，可能會導致合約捨棄。

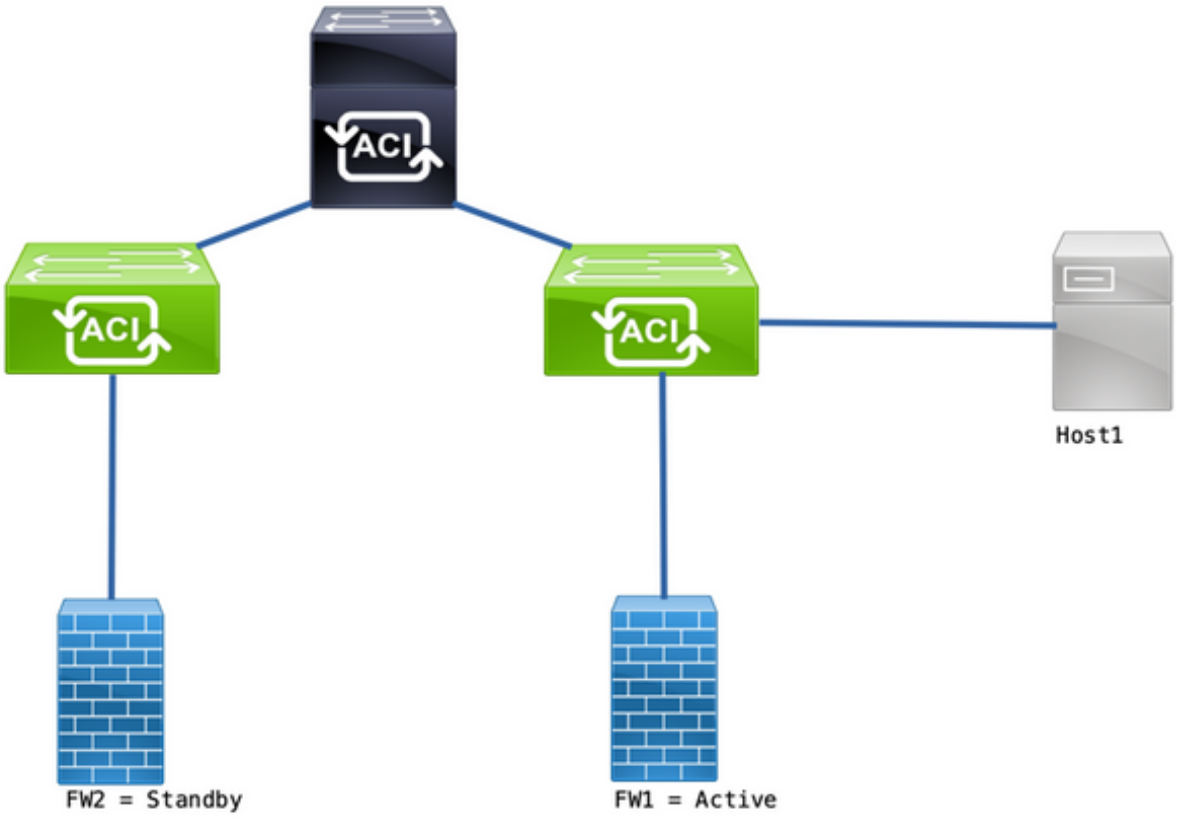
背景資訊

ACI L3out白皮書的「An exception for a directly connected subnet with 0.0.0.0/0」一節將針對pcTag 1的此行為稱為：

「……預設情況下，會為直接連線的子網分配pcTag 1，這是繞過合約的特殊的pcTag。這是在拐角情況下隱式允許路由協定通訊。但是……這會引起安全隱患。因此，此行為將通過思科錯誤ID CSCuz12913加以詳細解釋 ，其中還引入了解決方法配置："

案例

拓撲和配置



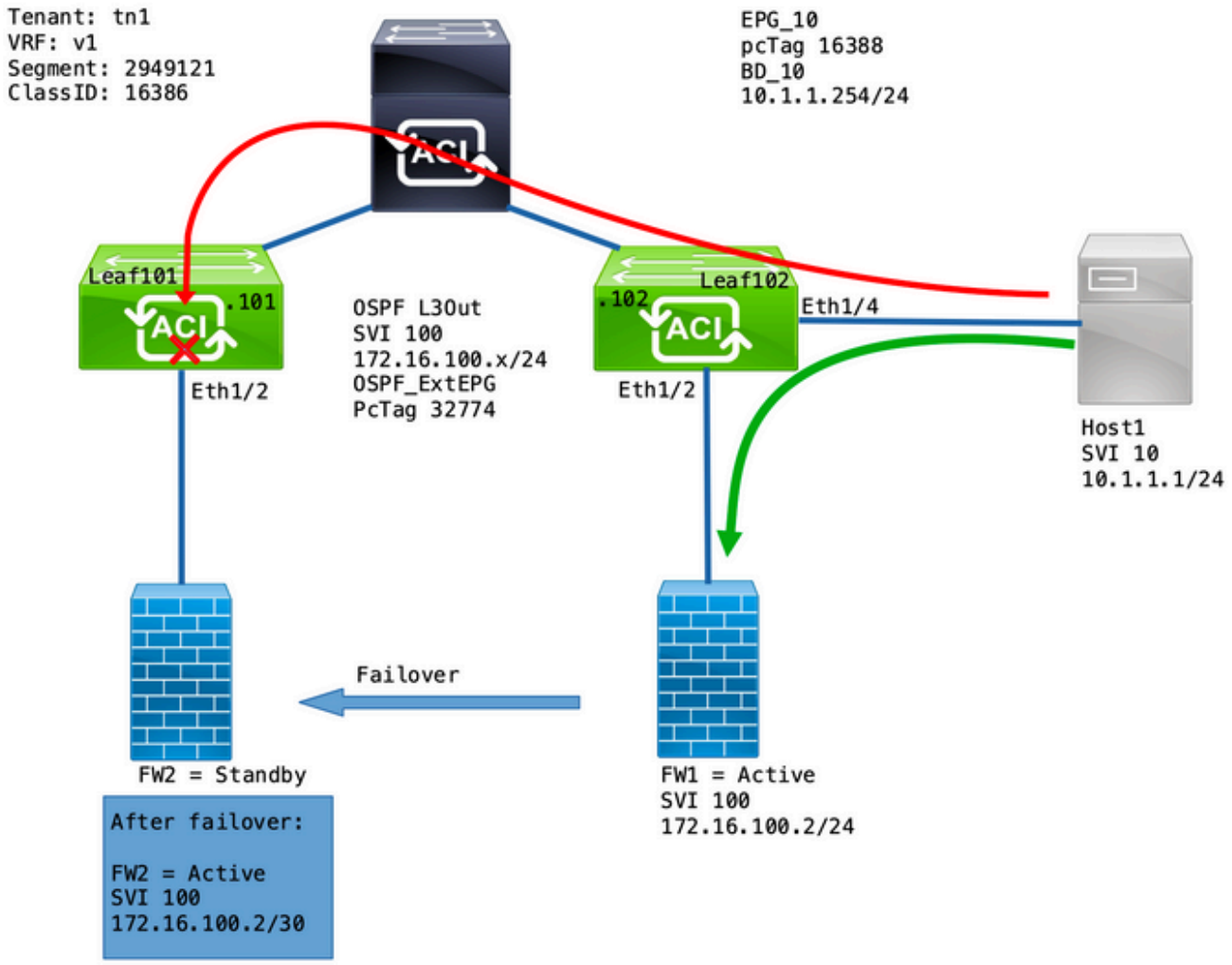
拓撲

- 防火牆(FW)配置了網路地址轉換(NAT)。
- 傳送到ACI交換矩陣的所有流量均來自與ACI形成OSPF鄰接關係的FW的IP。
- 外部EPG有一個0.0.0.0/0網路，該網路配**置了外部EPG的外部子網**。
- 內部EPG和外部EPG之間的通訊已有合約。

觀察的問題

使用FW1作為活動裝置，流量可按預期工作。沒有觀察到丟包。

在防火牆服務故障轉移到FW2後，連線斷開 — 10.1.1.1和172.16.100.2無法再通訊。



問題深入分析

通過Leaf101上的ELAM捕獲，我們可以驗證從Host1到FW2的流量是否被丟棄。

使用了以下ELAM選項：

```
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
```

在觸發時，電子報告允許您檢視查詢結果：

```
<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" )
```

此報表顯示流程為「已丟棄合約」以及以下詳細資訊：

- SCLASS為16388，即EPG_10的pcTag。
- DCLASS為16386，即VRF v1的pcTag。

接下來，驗證VRF的分割槽規則：

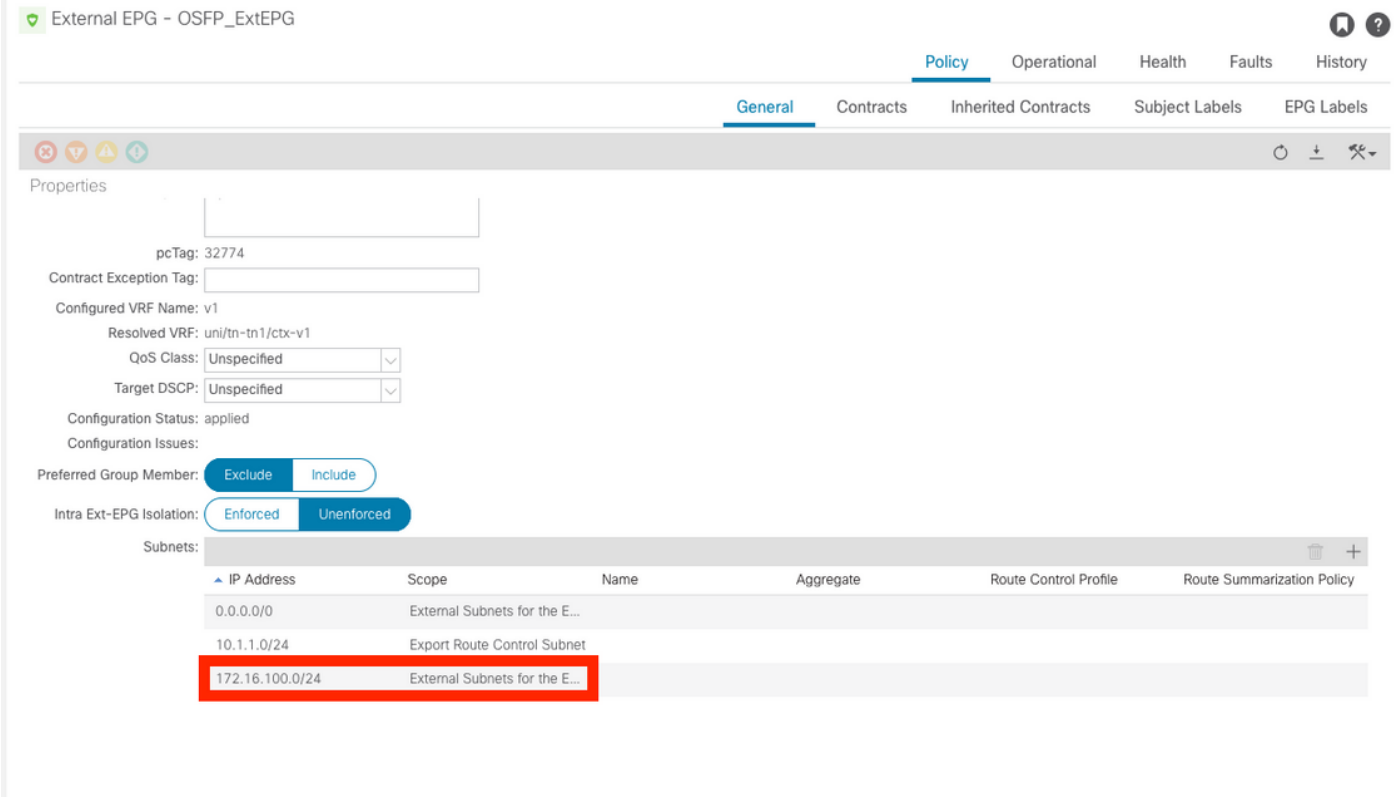
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   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)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
```

存在從EPG_10(16388)到OSPF L3Out背後的網路的通訊協定(0.0.0.0/0 = 15)。 但是，來自172.16.100.2的流量在VRF v1的pcTag(16386)下標籤。

解決方案

在OSPF Ext_EPG下新增L3Out的直連子網。



此增加有兩個效果：

1. 來自直連子網的流量在OSPF_ExtEPG pcTag(32774)下標籤
2. 新增規則以允許流入EPG_10和OSPF_ExtEPG和流出

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

說明

當FW和主機連線到同一枝葉時（不新增L3Out子網），這樣做的原因是直接連線的子網使用特殊的pcTag 1，它繞過所有合約。這是在拐角情況下隱式允許路由協定通訊。

透過這些觸發器，我們可以捕獲從172.16.100.2到10.1.1.1的流量，而在枝葉102上：

```
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
```

此報表顯示查詢結果：

```
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
```

要驗證退貨流程，請執行以下操作：

```
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
```

返回流的查詢結果：

```
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
```

下表總結了第2代交換機的預期行為：

案例	方向性	合約丟棄	無合約丟棄
跨同一枝葉 VRF策略實施：兩者	X到L3Out		X
	L3Out到X		X
跨2個枝葉節點 VRF策略實施：輸入	X到L3Out	X	
	L3Out到X		X
跨2個枝葉節點 VRF策略實施：輸出	X到L3Out		X
	L3Out到X		X

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。