排除ACI L3Out — 直连子网PcTag1故障

目录

简介

本文档介绍的场景是，来自直接连接的L3Out子网的流量在没有外部EPG下正确配置的情况下可能导致合同丢弃。

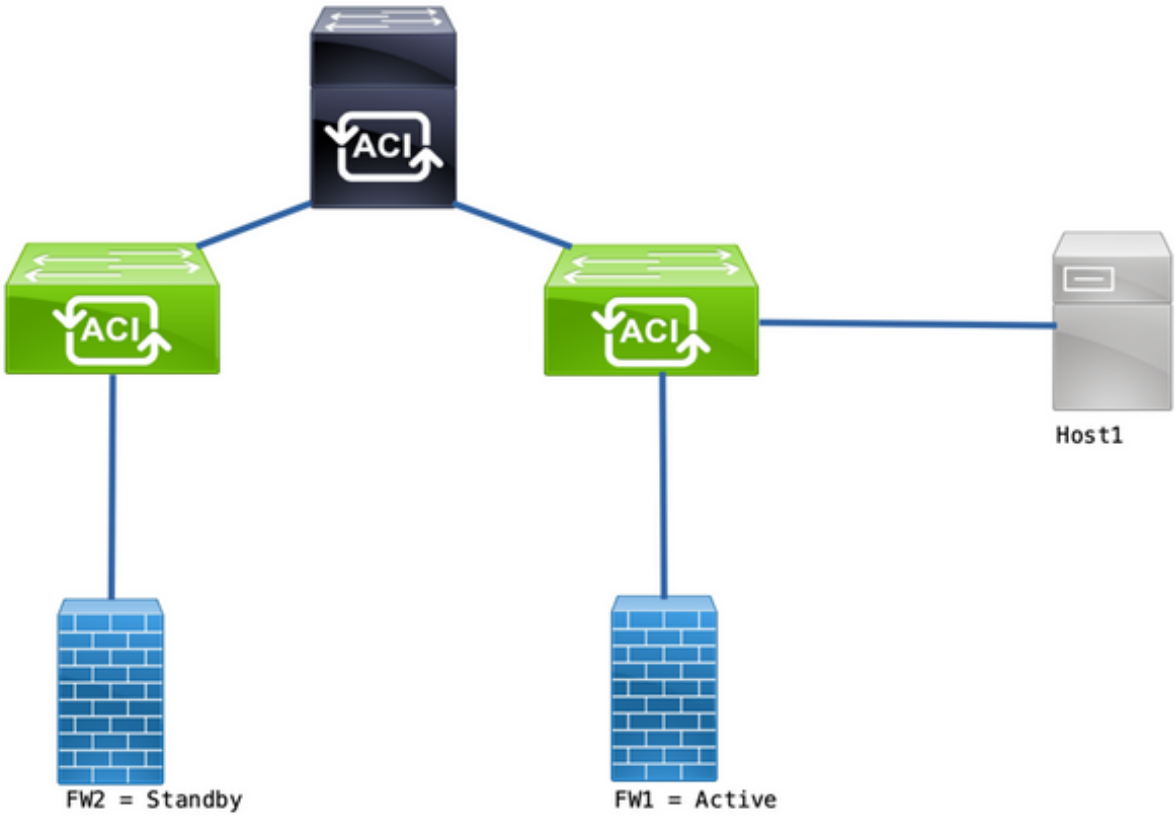
背景信息

ACI L3out白皮书中的“**0.0.0.0/0直连子网的例外”一节指出有关pcTag 1的以下行为：**

"...默认情况下，会为直接连接的子网分配pcTag 1，这是用于绕过合同的特殊pcTag。这是在拐角情况下隐式允许路由协议通信。但是……这会引发安全隐患。因此，可通过Cisco Bug ID CSCuz对此行为进行详细说明12913 ，还引入了应急配置："

场景

拓扑和配置



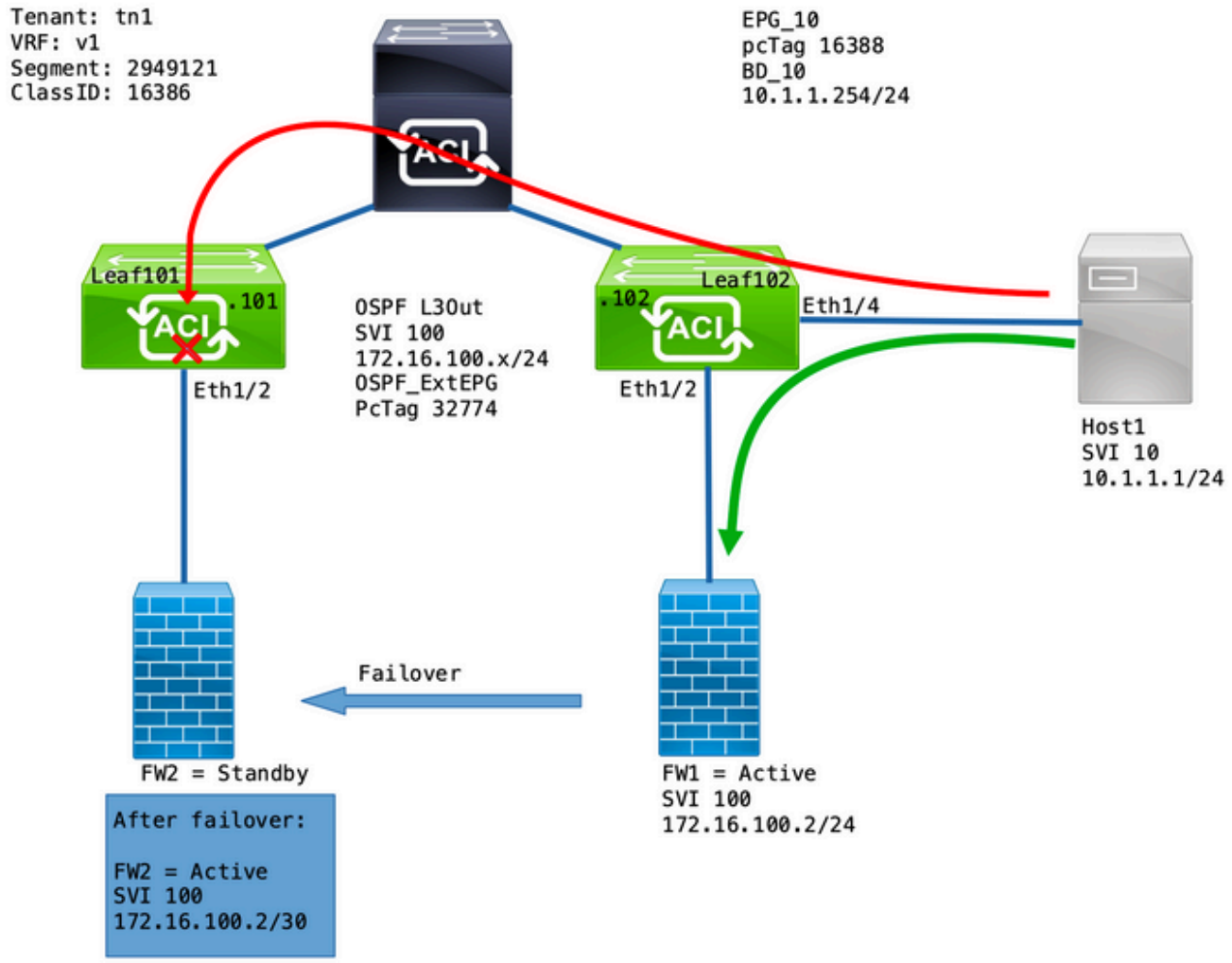
拓扑

- 防火墙(FW)配置了网络地址转换(NAT)。
- 发送到ACI交换矩阵的所有流量均来自与ACI形成OSPF邻接关系的FW的IP。
- 外部EPG有一个0.0.0.0/0网络，该网络配**置有外部EPG的外部子网**。
- 内部EPG和外部EPG之间已签订通信合同。

观察到的问题

使用FW1作为活动设备，流量可按预期工作。未观察到丢包。

在防火墙服务故障转移到FW2后，连接断开 — 10.1.1.1和172.16.100.2无法再通信。



问题深入探讨

Leaf101上的ELAM捕获允许我们验证从主机1到FW2的流量是否被丢弃。

使用以下ELAM选项：

```
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
```

在触发时，电子报告允许您查看查找结果：

```
<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" )
```

此报告显示流程为“已放弃合同”，同时显示以下详细信息：

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

接下来，验证VRF的分区规则：

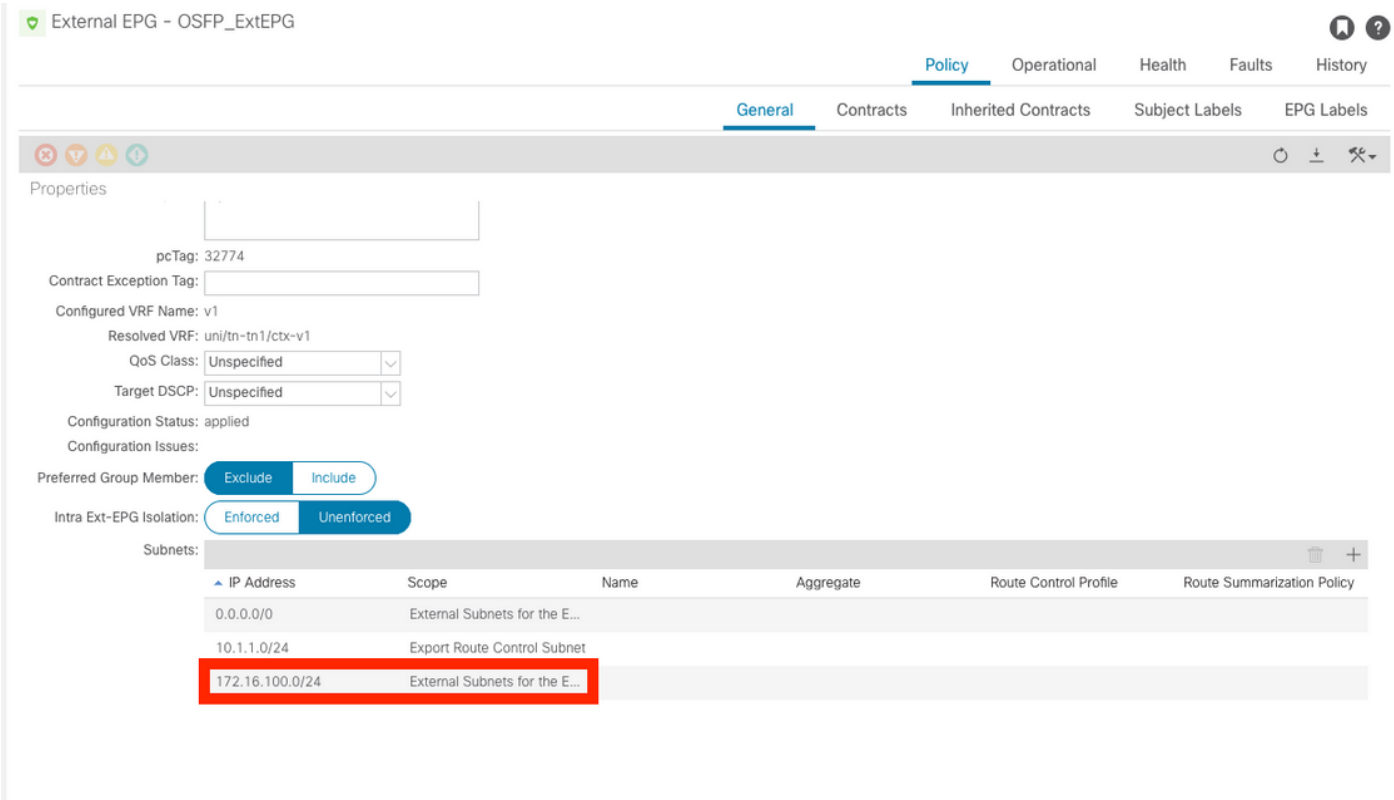
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name      |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+----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

存在从EPG_10(16388)到OSPF L3Out后的网络的通信合同(0.0.0.0/0 = 15)。 但是，来自172.16.100.2的流量在VRF v1的pcTag(16386)下标记。

解决方案

在OSPF Ext_EPG下添加L3Out的直连子网。



此添加有2个效果：

1. 来自直连子网的流量在OSPF_ExtEPG pcTag下标记(32774)
2. 添加规则以允许流入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)    |  <<<----
+---------+--------+--------+----------+---------------+---------+---------+-----------------
+----------+---------------------+
```

说明

当FW和主机连接到同一枝叶时（不添加L3Out子网），这样做的原因是直接连接的子网使用特殊的pcTag，即1，它会绕过所有合同。这是在拐角情况下隐式允许路由协议通信。

通过这些触发器，我们可以捕获从172.16.100.2到10.1.1.1的流量，而在枝叶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
```

此报告显示查找结果：

```
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
```

要验证退货流程，请执行以下操作：

```
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
```

返回流的查找结果：

```
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
```

下表总结了第2代交换机的预期行为：

场景	方向性	合同丢弃	无合同丢弃
跨越同一枝叶 VRF策略实施：两者	X到L3Out		X
	L3Out到X		X
跨2个枝叶节点 VRF策略实施：入口	X到L3Out	X	
	L3Out到X		X
跨2个枝叶节点 VRF策略实施：出口	X到L3Out		X
	L3Out到X		X

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。