ACI L3Outのトラブルシューティング：直接接続されたサブネットPcTag1

内容

[概要](#)
[背景説明](#)
[シナリオ](#)
[トポロジと設定](#)
[確認済みの問題](#)
[問題の詳細](#)
[解決方法](#)
[説明](#)

概要

このドキュメントでは、外部EPGで適切に設定されていない直接接続されたL3Outサブネットから送信されたトラフィックがコントラクトのドロップにつながる可能性があるシナリオについて説明します。

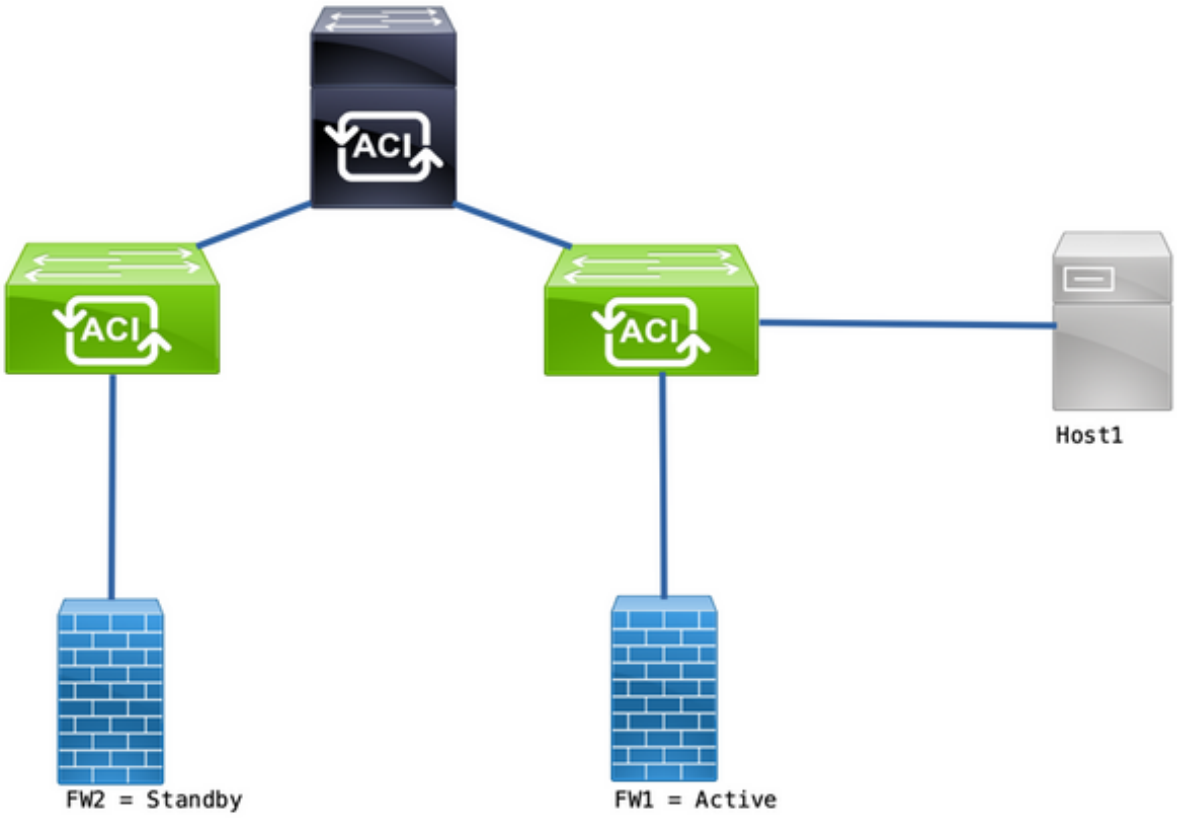
背景説明

『ACI L3out Whitepaper』の「**0.0.0.0/0で直接接続されたサブネットの例外**」セクションでは、pcTag 1に関して次の動作が示されています。

」...デフォルトでは、直接接続されたサブネットにはpcTag 1が割り当てられます。これは、契約をバイパスするための特別なpcTagです。これは、コーナーケースシナリオでルートプロトコル通信を暗黙的に許可するためです。しかし、これはセキュリティ上の問題を引き起こす可能性があります。したがって、この動作はCisco Bug ID CSCuz12913 また、回避策の設定も導入されています。

シナリオ

トポロジと設定



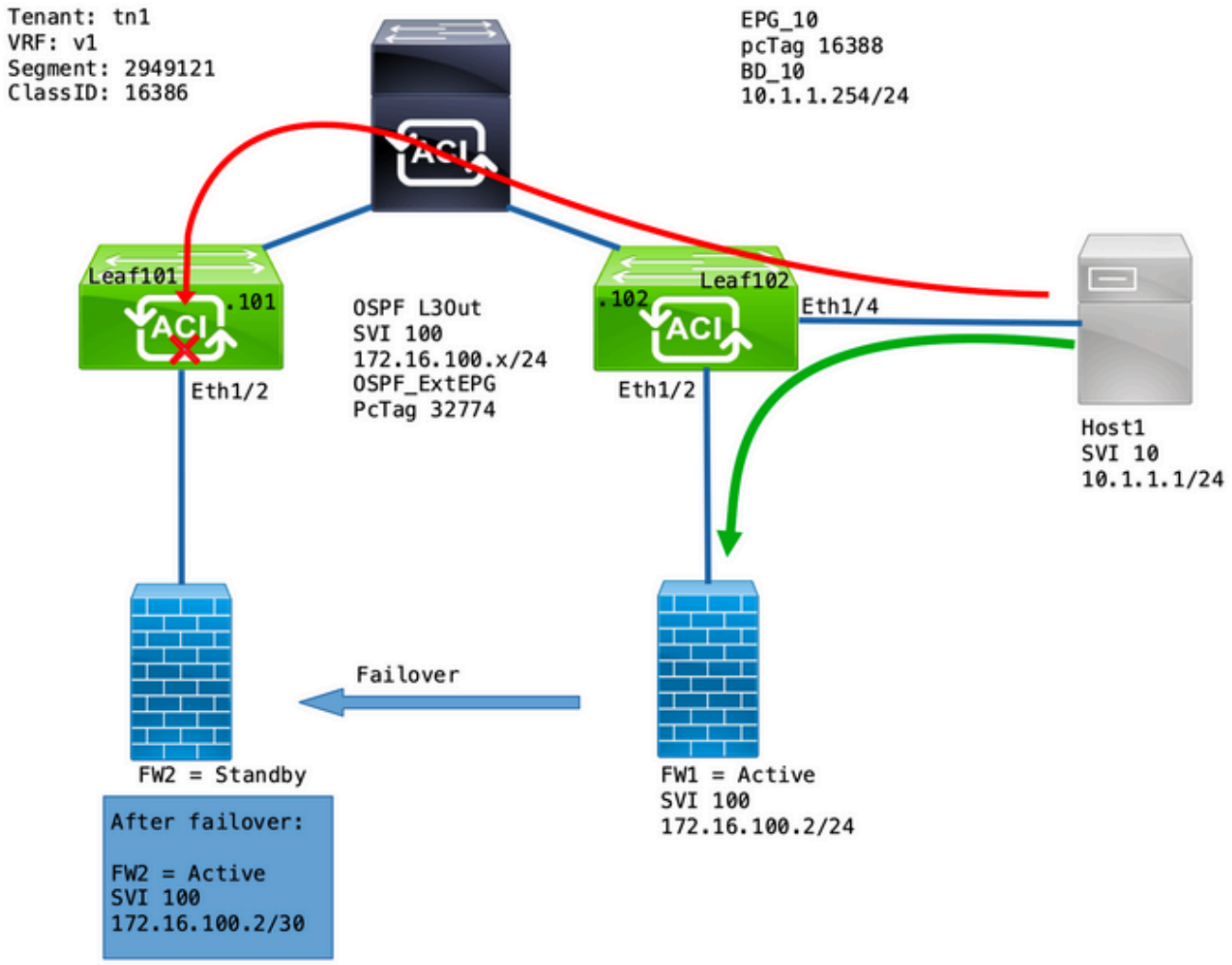
トポロジ

- ファイアウォール(FW)はネットワークアドレス変換(NAT)で設定されます。
- ACIファブリックに送信されるすべてのトラフィックは、ACIとのOSPF隣接関係を形成するFWのIPから送信されます。
- 外部EPGには、**外部EPGの外部サブネット**を使用して設定された0.0.0.0/0ネットワークがあります。
- 内部EPGと外部EPG間の通信に関する契約が締結されている。

確認済みの問題

FW1をアクティブデバイスとして使用すると、トラフィックは期待どおりに動作します。ドロップは観察されません。

ファイアウォールサービスがFW2にフェールオーバーすると、接続が失われ、10.1.1.1と172.16.100.2が通信できなくなります。



問題の詳細

Leaf101のELAMキャプチャを使用すると、Host1からFW2へのトラフィックがドロップされたかどうかを検証できます。

次のELAMオプションが使用されました。

```
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
```

また、電子レポートがトリガーされると、ルックアップ結果を表示できます。

```
<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" )
```

このレポートには、フローが次の詳細とともに契約破棄であることが示されます。

- SCLASSはEPG1638810のpcTagです。
- DCLASSは16386で、VRF v1のpcTagです。

次に、VRFのゾーン分割ルールを検証します。

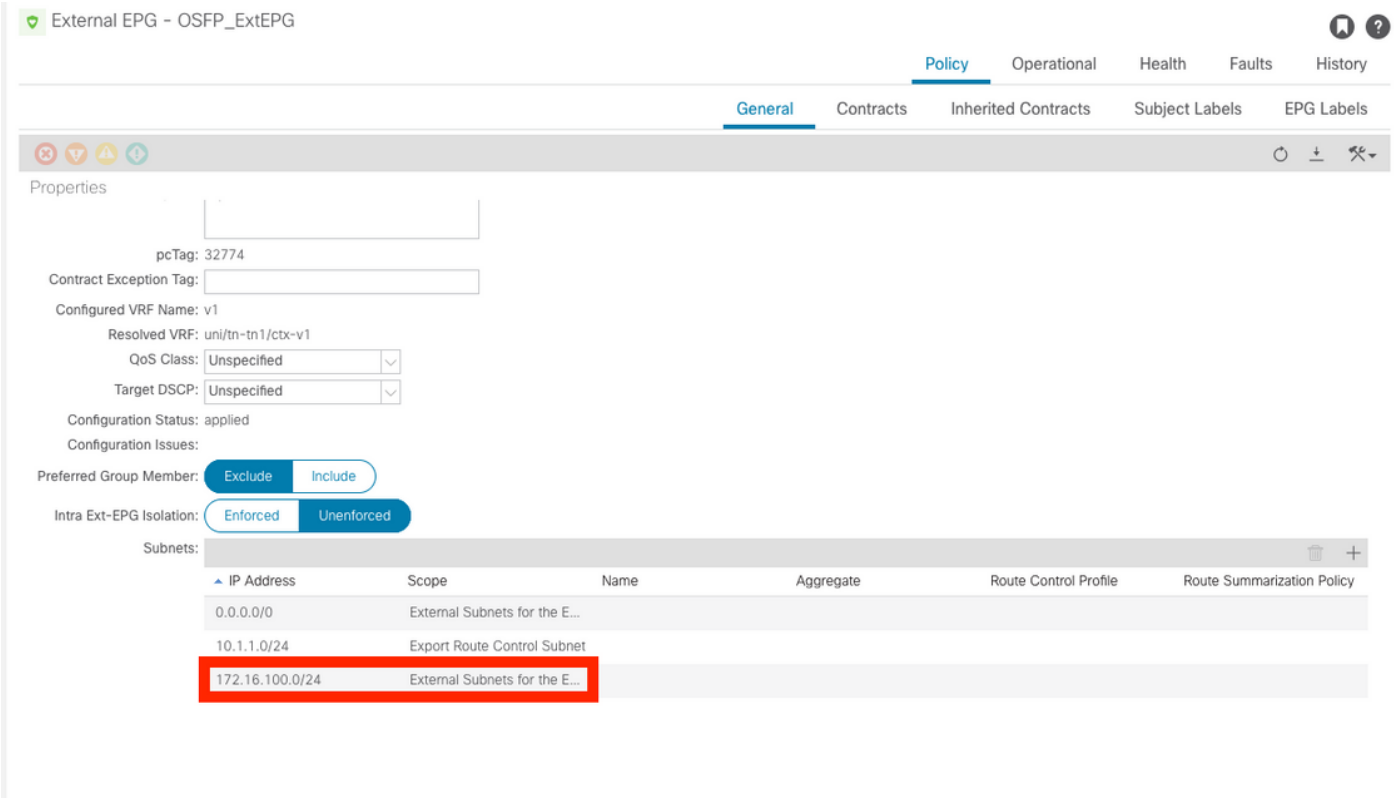
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+--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

EPG_10(16388)からOSPF L3Out(0.0.0.0/0 = 15)の背後にあるネットワークへの通信に関する契約が存在します。 ただし、172.16.100.2からのトラフィックは、VRF v1のpcTag(16386)でタグ付けされます。

解決方法

OSPF Ext_EPGの下にL3Outの直接接続されたサブネットを追加します。



この追加には2つの効果があります。

1. 直接接続されたサブネットからのトラフィックは、OSPF_ExtEPG pcTag(32774)でタグ付けされます
2. EPG_10とOSPF_ExtEPGとの間のフローを許可するルールが追加されます

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

説明

FWとHostが（L3Outサブネットの追加なしで）同じリーフに接続されている場合にこれが機能するのは、直接接続されたサブネットが、すべてのコントラクトをバイパスする1の特別なpcTagを使用するためです。これは、コーナーケースシナリオでルートプロトコル通信を暗黙的に許可するためです。

これらのトリガーを使用して、Leaf102で172.16.100.2から10.1.1.1へのトラフィックフローを捕捉できます。

```
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
```

このレポートには、ルックアップ結果が表示されます。

```
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
```

返品フローを検証する手順は、次のとおりです。

```
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
```

戻りフローの参照結果：

```
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
```

次の表に、Gen 2スイッチで予想される動作をまとめます。

シナリオ	方向性	契約破棄	契約破棄なし
同じリーフ上 VRFポリシーの適用：両方	XからL3Out		X
	L3OutからX		X
2つのリーフノード間 VRFポリシーの適用：入力	XからL3Out	X	
	L3OutからX		X
2つのリーフノード間 VRFポリシーの適用：出力	XからL3Out		X
	L3OutからX		X

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。