Dépannage de l'ACI L3Out - Direct-Connected Subnet PcTag1

Contenu

Introduction

Ce document décrit un scénario où le trafic provenant d'un sous-réseau L3Out directement connecté sans la configuration appropriée sous l'EPG externe peut conduire à des pertes de contrat.

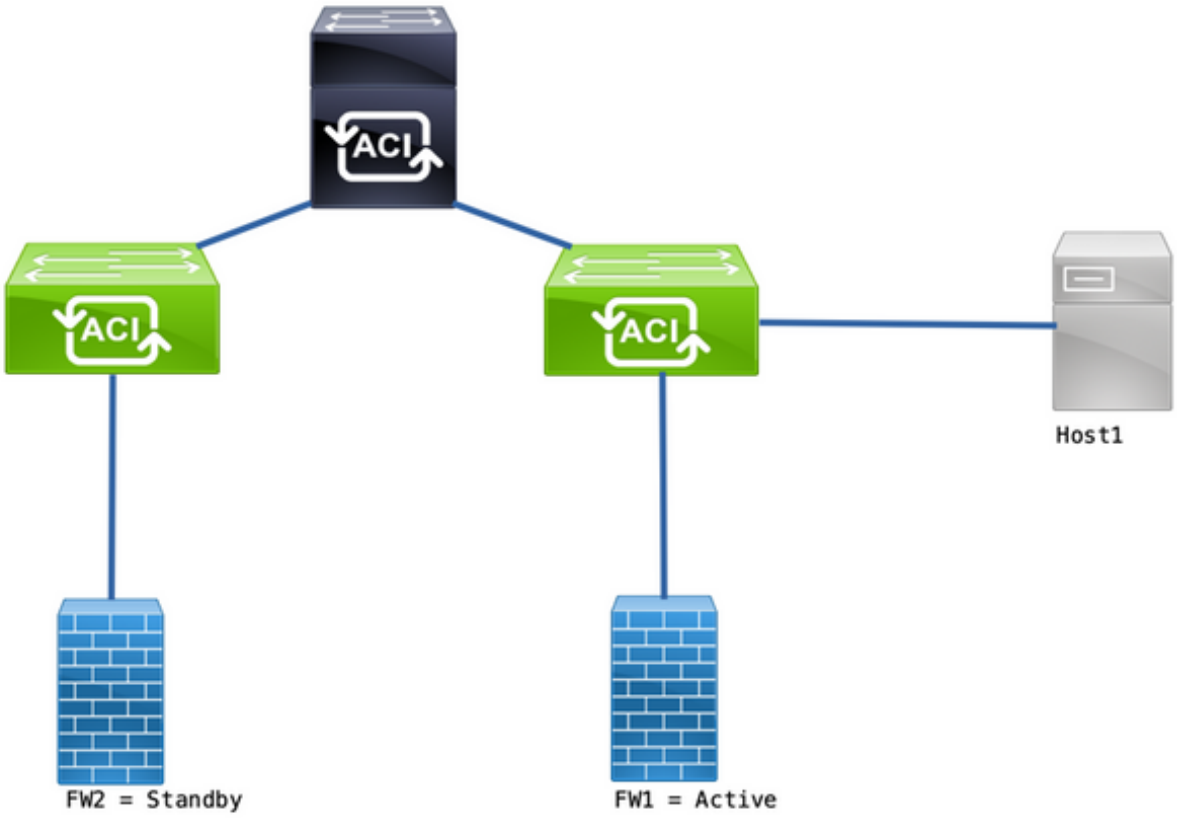
Informations générales

La section « **Une exception pour un sous-réseau connecté directement avec 0.0.0.0/0** » du livre blanc ACI L3out appelle ce comportement en ce qui concerne pcTag 1 :

"...par défaut, les sous-réseaux connectés directement se voient attribuer pcTag 1, un pcTag spécial pour contourner un contrat. Ceci permet implicitement les communications de protocole de routage dans un scénario de cas de coin. Cependant... cela peut causer un problème de sécurité à la place. Par conséquent, ce comportement est expliqué en détail via l'ID de bogue Cisco CSCuz12913 , qui introduit également une configuration de contournement :"

Le scénario

Topologie et configuration



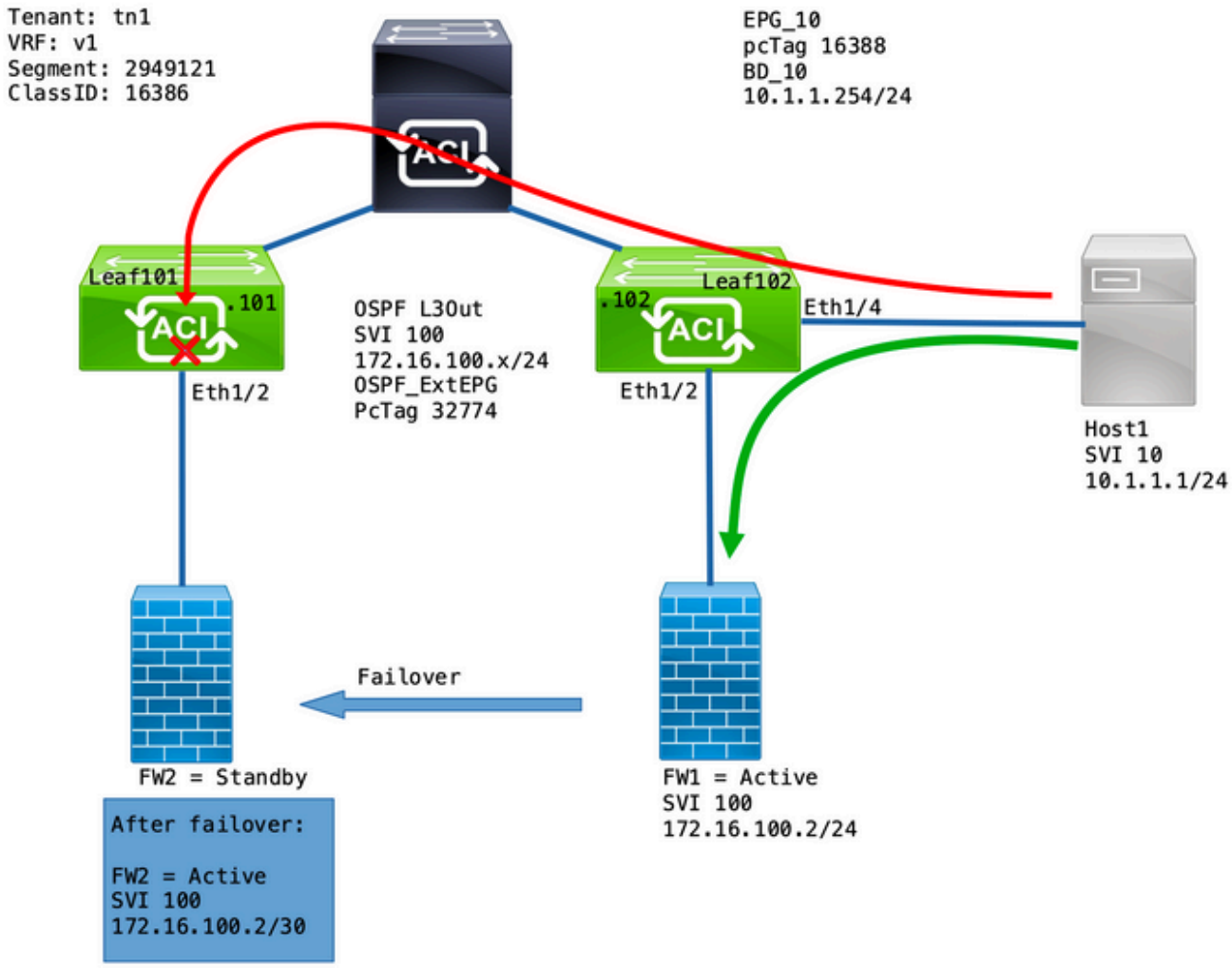
Topologie

- Les pare-feu (FW) sont configurés avec la traduction d'adresses réseau (NAT).
- Tout le trafic envoyé dans le fabric ACI provient de l'adresse IP du pare-feu qui forme la contiguïté OSPF avec l'ACI.
- L'EPG externe a un réseau 0.0.0.0/0 configuré avec des **sous-réseaux externes pour l'EPG externe**.
- Un contrat est en place pour la communication entre l'EPG interne et l'EPG externe.

Problème observé

Avec FW1 comme périphérique actif, le trafic fonctionne comme prévu. Aucune baisse n'est observée.

Après le basculement des services de pare-feu sur FW2, la connectivité est perdue : 10.1.1.1 et 172.16.100.2 ne peuvent plus communiquer.



Émission Deep-Dive

Une capture ELAM sur Leaf101 nous permet de valider si le trafic de l'hôte 1 vers FW2 est abandonné.

Les options ELAM suivantes ont été utilisées :

```
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
```

Et lorsqu'il est déclenché, le rapport électronique vous permet d'afficher les résultats de la recherche :

```
<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" )
```

Ce rapport indique que le flux est Abandonné sous contrat, ainsi que les détails suivants :

- La valeur SCLASS est 16388, qui correspond au pcTag de EPG_10.
- Le DCLASS est 16386, qui est le pcTag du VRF v1.

Ensuite, validez les règles de zonage pour le VRF :

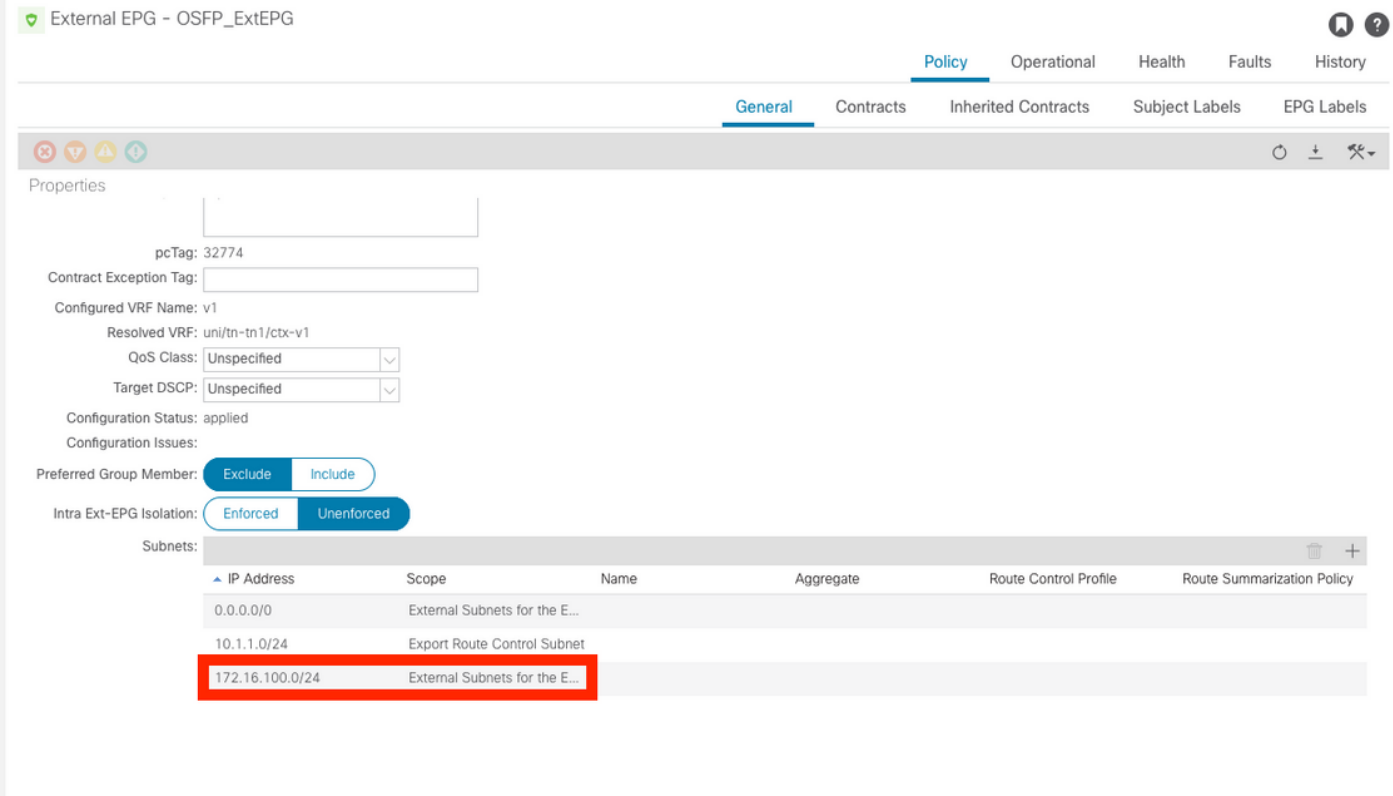
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+--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

Un contrat est en place pour la communication entre EPG_10 (16388) et les réseaux derrière l'OSPF L3Out (0.0.0.0/0 = 15). Cependant, le trafic provenant de 172.16.100.2 est étiqueté sous pcTag (16386) du VRF v1.

Solution

Ajoutez le sous-réseau connecté directement de L3Out sous le Ext_EPG OSPF.



Cet ajout a 2 effets :

1. Le trafic provenant du sous-réseau directement connecté est étiqueté sous OSPF_ExtEPG pcTag (32774)
2. Des règles sont ajoutées pour autoriser le flux vers et depuis EPG_10 et 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)    |  <<<----
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Explication

Cela fonctionne lorsque le pare-feu et l'hôte sont connectés au même noeud leaf (sans l'ajout de sous-réseau L3Out) parce que les sous-réseaux connectés directement utilisent un pcTag spécial de 1 qui contourne tous les contrats. Ceci permet implicitement les communications de protocole de routage dans un scénario de cas de coin.

Avec ces déclencheurs, nous pouvons intercepter un flux de trafic de 172.16.100.2 à 10.1.1.1 sur 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
```

Ce rapport affiche les résultats de la recherche :

```
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
```

Pour valider le flux de retour :

```
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
```

Résultats de la recherche du flux de retour :

```
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
```

Ce tableau résume le comportement attendu sur les commutateurs Gen2 :

Scénario	Direction	Abandon du contrat	Aucun abandon de c
Sur la même feuille Application des politiques VRF : Les deux	X à L3Sortant		X
	L3Sortie vers X		X
Sur 2 noeuds leaf Application des politiques VRF : Entrée	X à L3Sortant	X	
	L3Sortie vers X		X
Sur 2 noeuds leaf Application des politiques VRF : Sortie	X à L3Sortant		X
	L3Sortie vers X		X

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.