Solução de problemas da ACI L3Out - PcTag1 de sub-rede diretamente conectada

Contents

Introduction

Este documento descreve um cenário em que o tráfego originado de uma sub-rede L3Out diretamente conectada sem a configuração adequada no EPG externo pode levar a quedas de contrato.

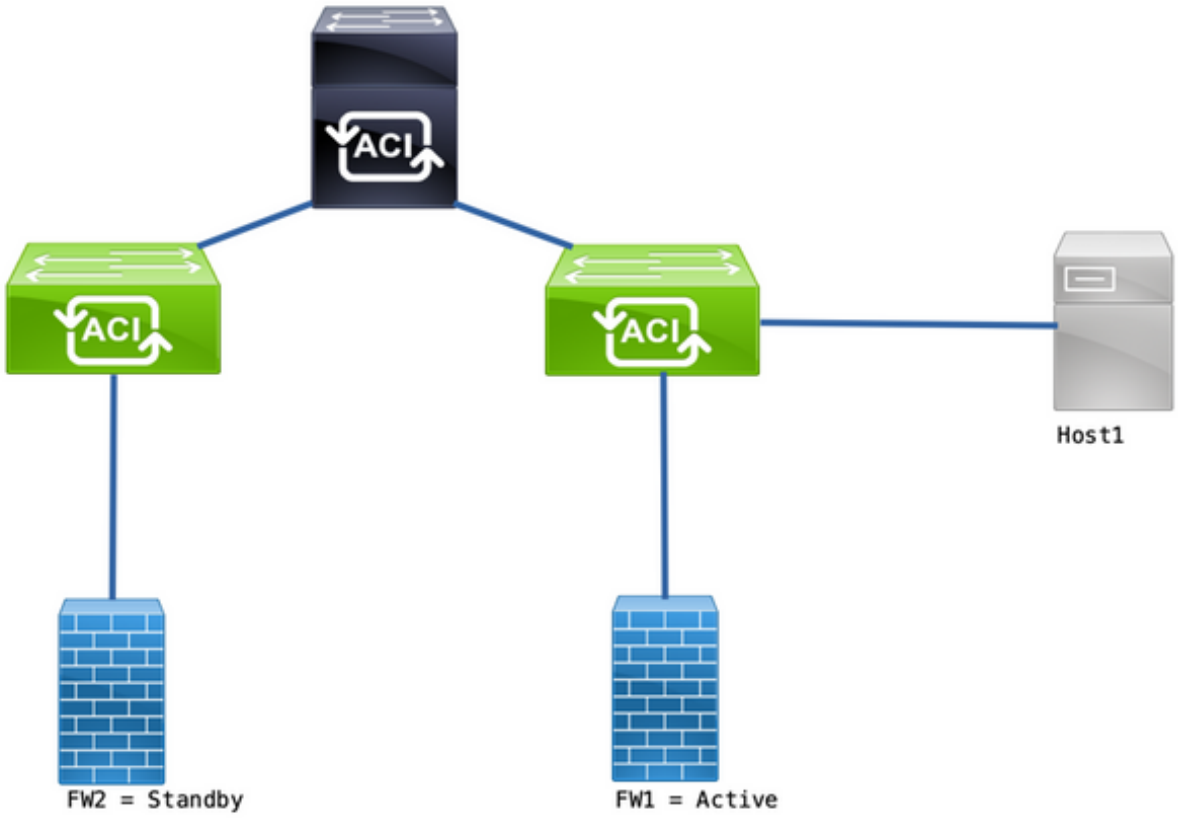
Informações de Apoio

A seção "**Uma exceção para uma sub-rede diretamente conectada com 0.0.0.0/0**" do Whitepaper L3out da ACI chama esse comportamento em relação ao pcTag 1:

"...por padrão, as sub-redes conectadas diretamente recebem o pcTag 1, que é um pcTag especial para ignorar um contrato. Isso permite implicitamente comunicações de protocolo de rota em um cenário de caso de canto. No entanto... isso pode causar uma preocupação de segurança. Portanto, esse comportamento é explicado em detalhes através da ID de bug da Cisco CSCuz12913 , que também apresenta uma configuração alternativa:"

O cenário

Topologia e configuração



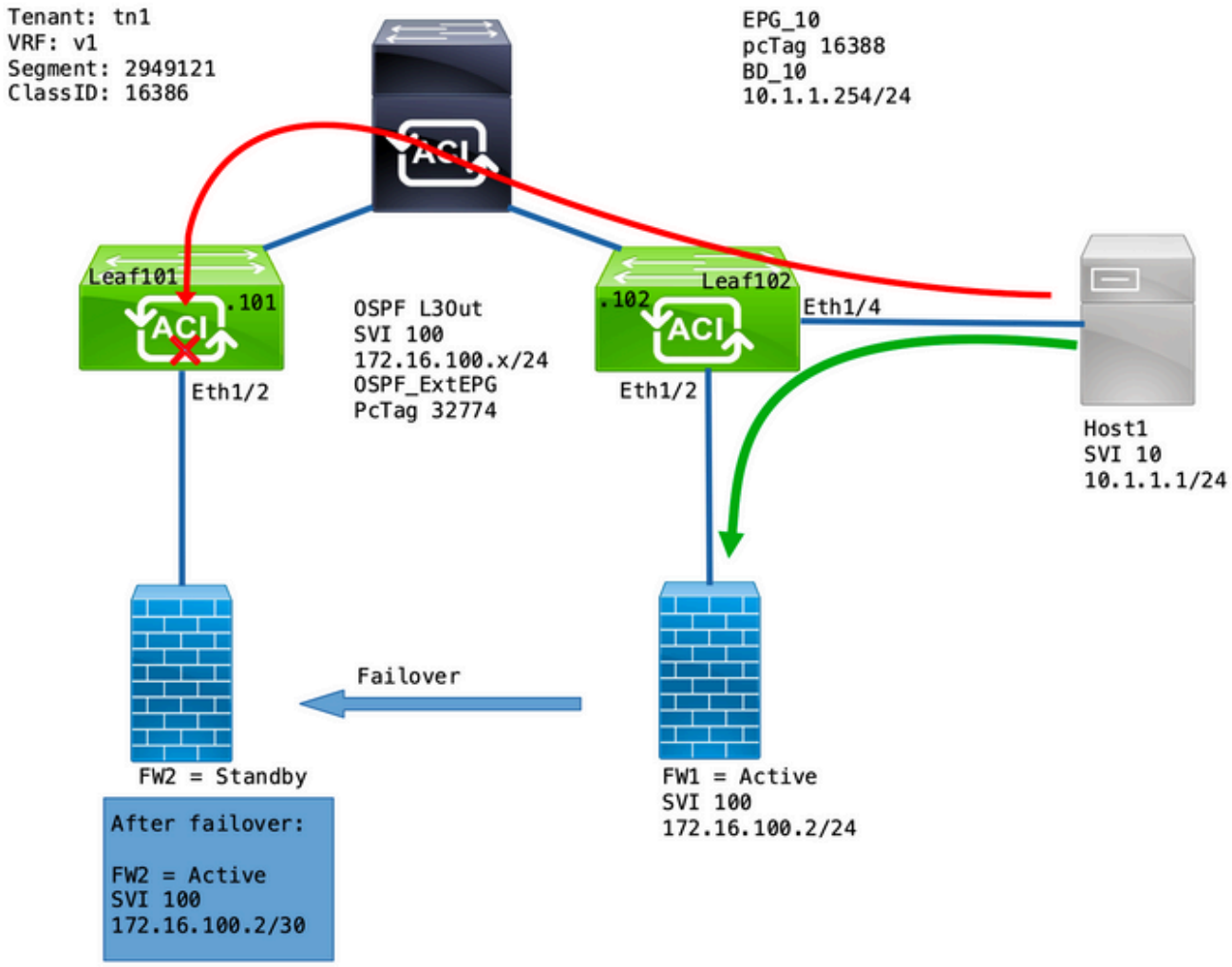
Topologia

- Os Firewalls (FW) são configurados com a Network Address Translation (NAT).
- Todo o tráfego enviado para a estrutura da ACI é originado do IP do FW que forma a adjacência OSPF com a ACI.
- O EPG externo tem uma rede 0.0.0.0/0 configurada com **Sub-redes Externas para o EPG Externo**.
- Um contrato está em vigor para a comunicação entre o EPG interno e o EPG externo.

Problema observado

Com o FW1 como o dispositivo ativo, o tráfego funciona como esperado. Não foram observadas gotas.

Após o failover dos serviços de firewall para o FW2, a conectividade é perdida - 10.1.1.1 e 172.16.100.2 não podem mais se comunicar.



Mergulho profundo no problema

Uma captura ELAM no Leaf101 nos permite validar se o tráfego do Host1 para o FW2 é descartado.

Estas opções de ELAM foram usadas:

```
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
```

E quando acionado, o relatório eletrônico permite exibir os resultados da pesquisa:

```
<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 relatório mostra que o fluxo é Contrato descartado junto com estes detalhes:

- O SCLASS é 16388, que é o pcTag de EPG_10.
- O DCLASS é 16386, que é o pcTag do VRF v1.

Em seguida, valide as regras de zoneamento para o VRF:

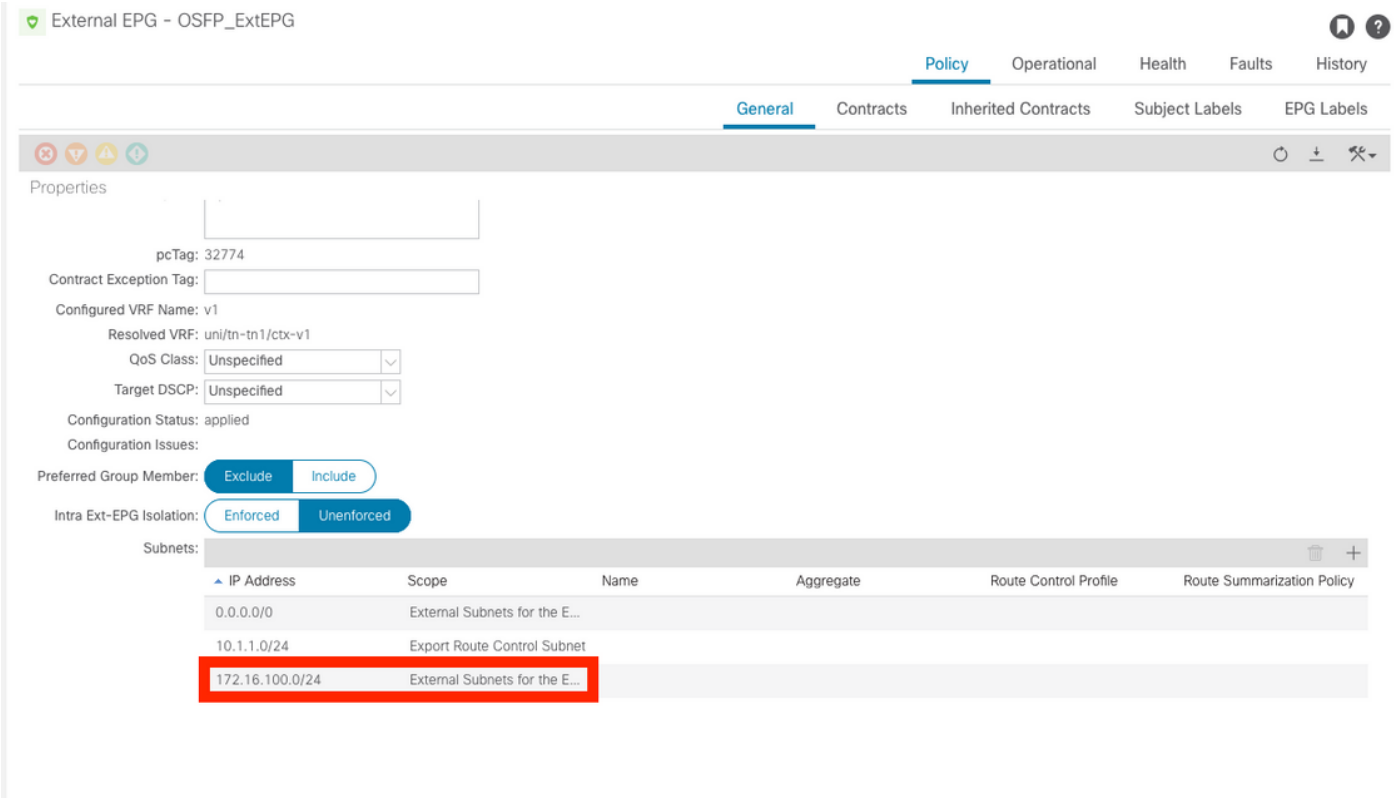
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+--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

Há um contrato em vigor para a comunicação do EPG_10 (16388) com as redes por trás da L3Out do OSPF (0.0.0.0/0 = 15). No entanto, o tráfego de 172.16.100.2 é marcado sob o pcTag do VRF v1 (16386).

Solução

Adicione a sub-rede diretamente conectada da L3Out no OSPF Ext_EPG.



Esta adição tem 2 efeitos:

1. O tráfego da sub-rede diretamente conectada é marcado sob o comando OSPF_ExtEPG pcTag (32774)
2. São adicionadas regras para permitir o fluxo de e para EPG_10 e 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)    |  <<<----
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Explicação

O motivo disso funcionar quando o FW e o Host estão conectados à mesma folha (sem a adição de sub-rede L3Out) é porque as sub-redes diretamente conectadas usam um pcTag especial de 1 que ignora todos os contratos. Isso permite implicitamente comunicações de protocolo de rota em um cenário de caso de canto.

Com esses disparadores, podemos capturar um fluxo de tráfego de 172.16.100.2 para 10.1.1.1 enquanto no 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 relatório mostra os resultados da pesquisa:

```
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 o fluxo de devolução:

```
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
```

Os resultados da pesquisa do fluxo 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 tabela resume o comportamento esperado em switches Gen2:

Cenário	Direcionalidade	Queda de contrato	Sem perda de cont
Na mesma folha Aplicação da política VRF: Ambos	X para L3Saída		X
	L3Saída para X		X
Em 2 nós folha Aplicação da política VRF: Ingresso	X para L3Saída	X	
	L3Saída para X		X
Em 2 nós folha Aplicação da política VRF: Saída	X para L3Saída		X
	L3Saída para X		X

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.