Fehlerbehebung bei ACI L3Out - direkt verbundenes Subnetz PCtag1

Inhalt

Einleitung

In diesem Dokument wird ein Szenario beschrieben, in dem Datenverkehr, der von einem direkt verbundenen L3Out-Subnetz ohne die richtige Konfiguration unter der externen EPG stammt, zum Verwerfen von Verträgen führen kann.

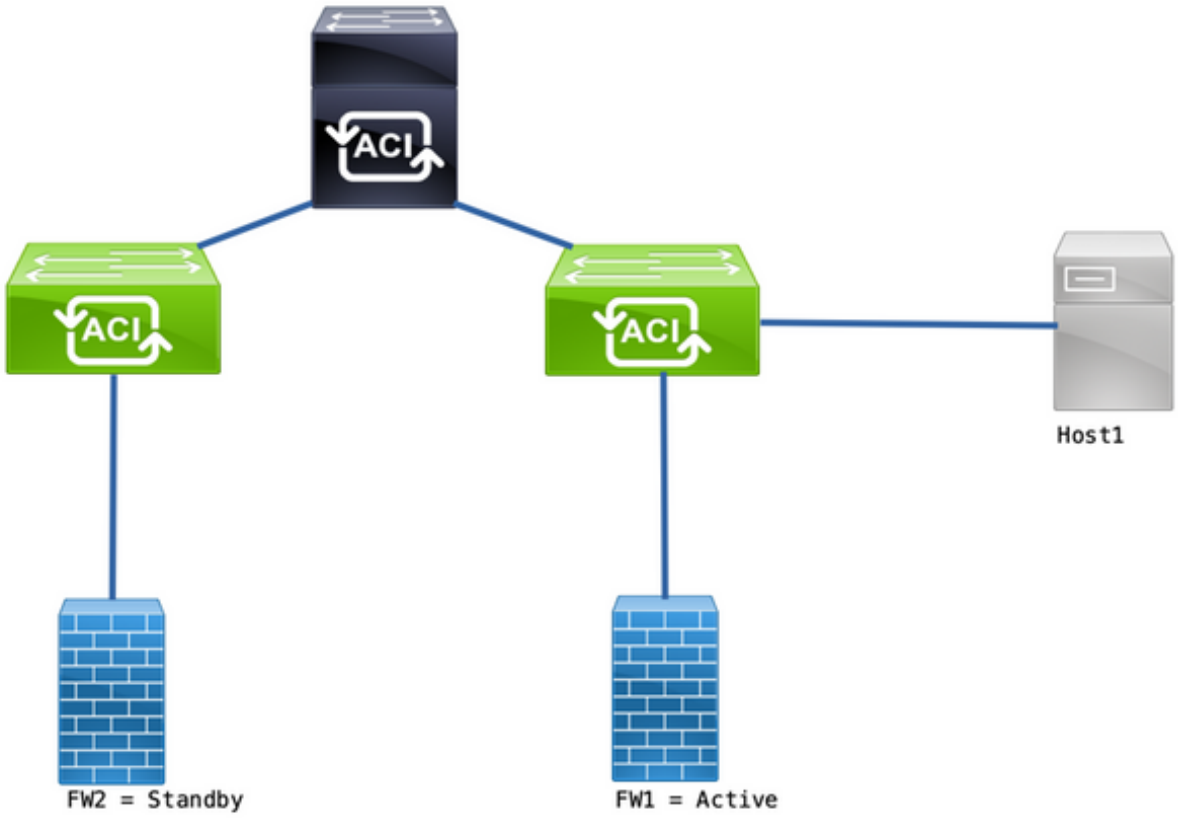
Hintergrundinformationen

Im Abschnitt **"Eine Ausnahme für ein direkt verbundenes Subnetz mit 0.0.0.0/0"** des ACI L3out-Whitepapers wird dieses Verhalten in Bezug auf den pcTag 1 aufgezeigt:

"...standardmäßig werden direkt verbundenen Subnetzen pcTag 1 zugewiesen, ein spezielles pcTag, um einen Vertrag zu umgehen. Damit wird implizit eine Routing-Protokoll-Kommunikation in einem Eck-Case-Szenario zugelassen. Dies kann jedoch zu Sicherheitsproblemen führen. Dieses Verhalten wird daher detailliert mit der Cisco Bug-ID CSCuz12913 erklärt. , die auch eine Workaround-Konfiguration einführt:"

Das Szenario

Topologie und Konfiguration



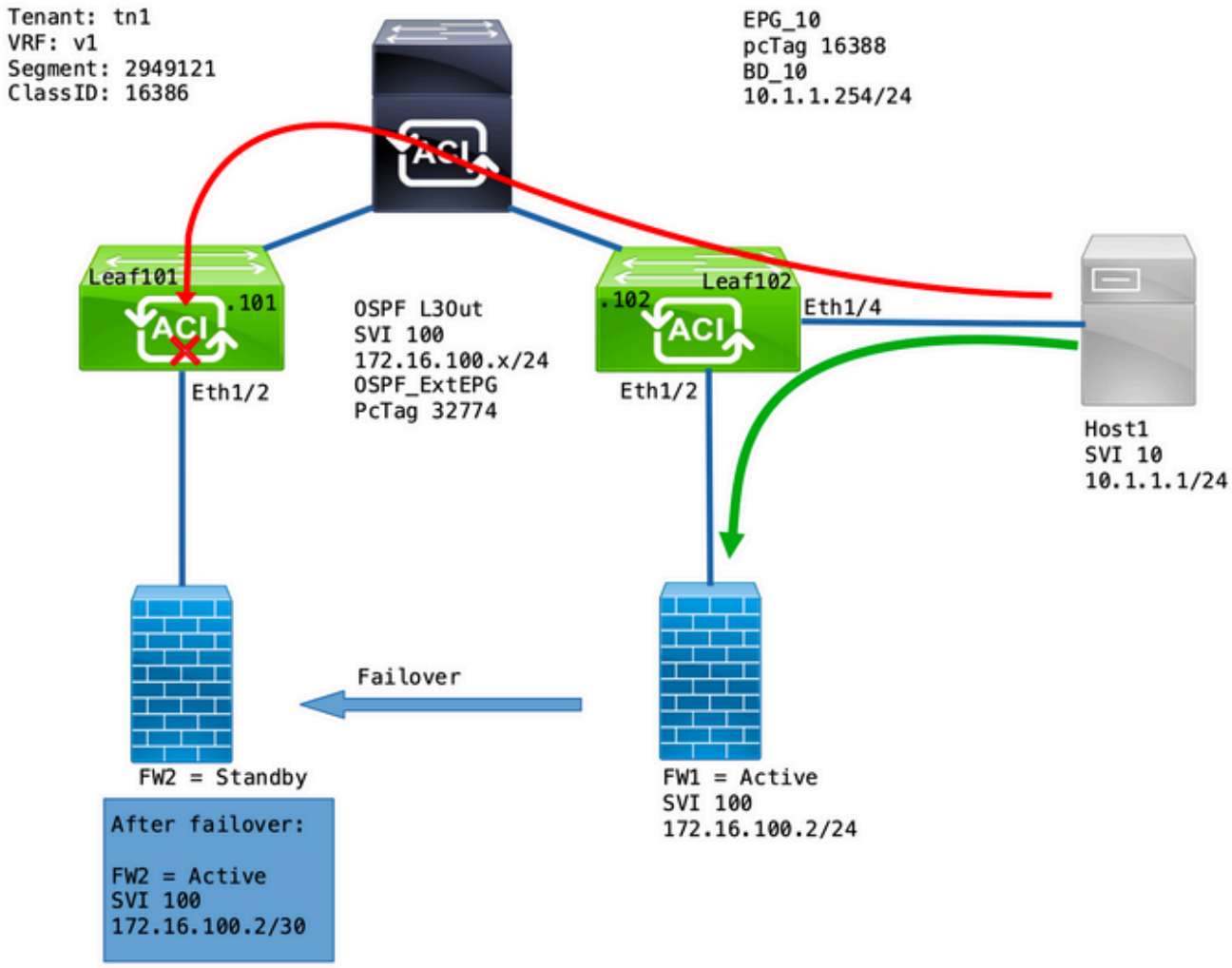
Topologie

- Die Firewalls (FW) werden mit Network Address Translation (NAT) konfiguriert.
- Der gesamte an die ACI-Fabric gesendete Datenverkehr stammt aus der IP-Adresse der FW, die die OSPF-Adjacency mit der ACI bildet.
- Die externe EPG verfügt über ein Netzwerk mit der Adresse 0.0.0.0/0, das mit **externen Subnetzen für die externe EPG** konfiguriert ist.
- Zwischen der internen und der externen EPG besteht ein Kommunikationsvertrag.

Beobachtetes Problem

Mit FW1 als aktivem Gerät funktioniert der Datenverkehr wie erwartet. Es wurden keine Tropfen beobachtet.

Nach dem Failover der Firewall-Services auf FW2 geht die Verbindung verloren - 10.1.1.1 und 172.16.100.2 können nicht mehr kommunizieren.



Details zum Problem

Mithilfe einer ELAM-Erfassung auf Leaf101 können wir überprüfen, ob der Datenverkehr von Host1 zu FW2 verworfen wird.

Folgende ELAM-Optionen wurden verwendet:

```
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
```

Wenn der E-Report ausgelöst wird, können Sie die Suchergebnisse anzeigen:

```
<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" )
```

Dieser Bericht zeigt, dass es sich bei dem Datenfluss um Contract Dropped mit folgenden Details handelt:

- Die SCLASS ist 16388, das ist das pcTag von EPG_10.
- DCLASS ist 16386 und damit das pcTag der VRF-Instanz v1.

Validieren Sie anschließend die Zoning-Regeln für die VRF-Instanz:

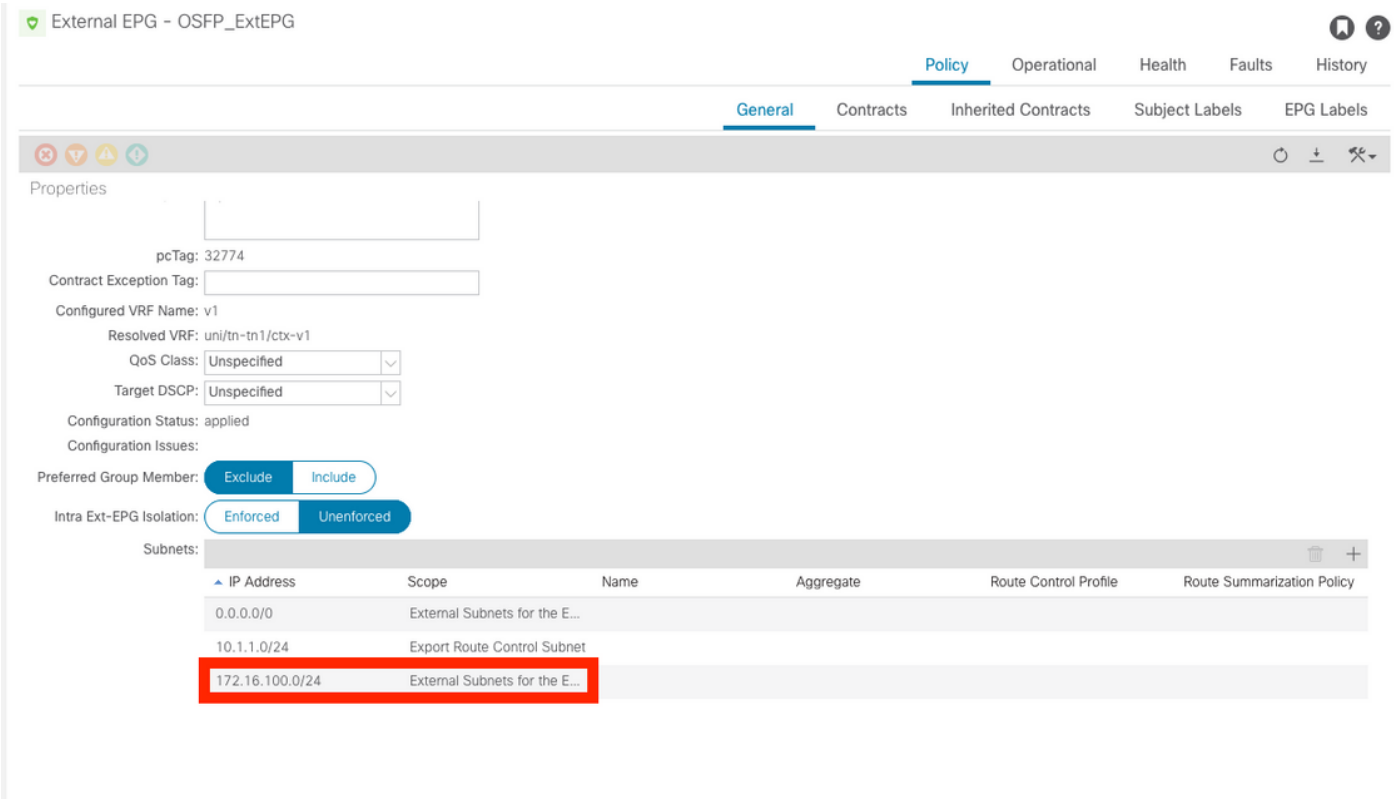
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+--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

Es besteht ein Vertrag für die Kommunikation von EPG_10 (16388) mit Netzwerken hinter dem OSPF L3Out (0.0.0.0/0 = 15). Der Datenverkehr von 172.16.100.2 wird jedoch unter dem pcTag (16386) des VRF v1 getaggt.

Lösung

Fügen Sie das direkt verbundene Subnetz des L3Out unter OSPF Ext_EPG hinzu.



Dieser Zusatz hat 2 Wirkungen:

1. Datenverkehr aus dem direkt verbundenen Subnetz wird mit dem OSPF_ExtEPG pcTag (32774) gekennzeichnet.
2. Es werden Regeln hinzugefügt, um den Datenfluss zu und von EPG_10 und OSPF_ExtEPG zu ermöglichen.

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

Erklärung

Dies funktioniert, wenn FW und Host mit demselben Leaf verbunden sind (ohne L3Out-Subnetz-Hinzufügung), weil direkt verbundene Subnetze ein spezielles pcTag von 1 verwenden, das alle Verträge umgeht. Damit wird implizit eine Routing-Protokoll-Kommunikation in einem Eck-Case-Szenario zugelassen.

Mit diesen Triggern können wir einen Datenverkehrsfluss von 172.16.100.2 bis 10.1.1.1 erfassen, während wir uns auf Leaf102 befinden:

```
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
```

Dieser Bericht zeigt die Suchergebnisse an:

```
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
```

So validieren Sie den Rücklauf:

```
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
```

Die Suchergebnisse des Rückflusses:

```
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
```

Diese Tabelle fasst das erwartete Verhalten bei Switches der 2. Generation zusammen:

Szenario	Richtwirkung	Vertragsverlust	Kein Vertragsverlu
Auf demselben Blatt VRF-Richtliniendurchsetzung: Beide	X bis L3Aus		X
	L3Aus zu X		X
Über 2 Leaf-Knoten VRF-Richtliniendurchsetzung: Eingang	X bis L3Aus	X	
	L3Aus zu X		X
Über 2 Leaf-Knoten VRF-Richtliniendurchsetzung: Ausgehend	X bis L3Aus		X
	L3Aus zu X		X

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.