Configuratie van Layer 2-servicegrafiek met ASAv configureren en verifiëren

Inhoud

Inleiding

Dit document beschrijft hoe u Layer 2-servicegrafconfiguratie in Cisco Application Centric Infrastructure (ACI) kunt configureren en verifiëren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Begrijpen hoe Layer 3 Service Graph werkt in ACI
- Inzicht in hoe u de Endpoint-beleidsgroep, brugdomeinen en contract in ACI kunt configureren
- Inzicht in hoe u (adaptieve security applicatie virtueel) ASAv als transparante firewall kunt configureren

Gebruikte componenten

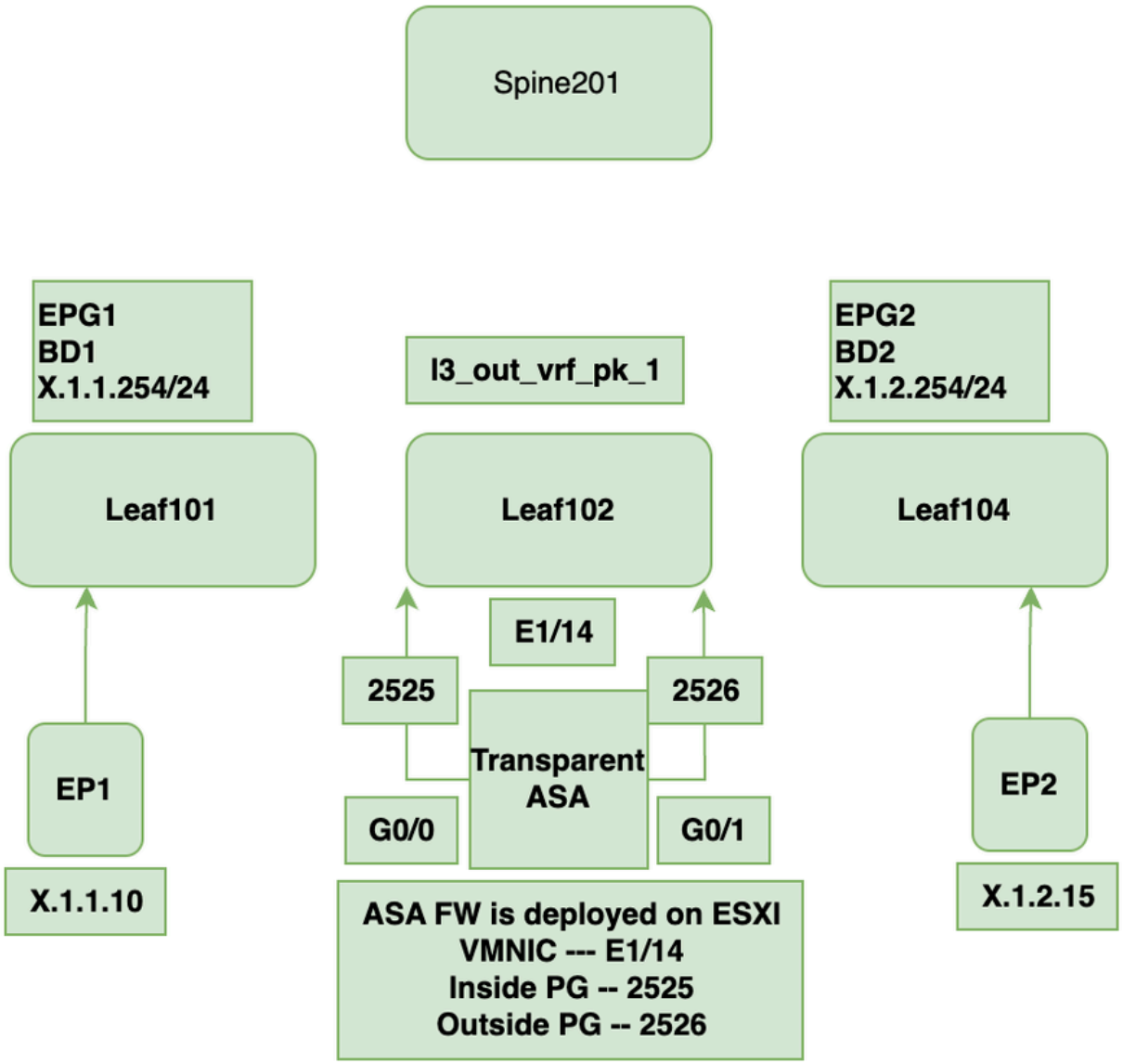
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- APIC versie: 6.0 (3g)
- Blad H/W: N9K-C93180YC-FX

- Blad S/W: n9000-16,0 (3g)
- Bladknooppunt 101, 102, 103
- ASAv geïmplementeerd op ESXi-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

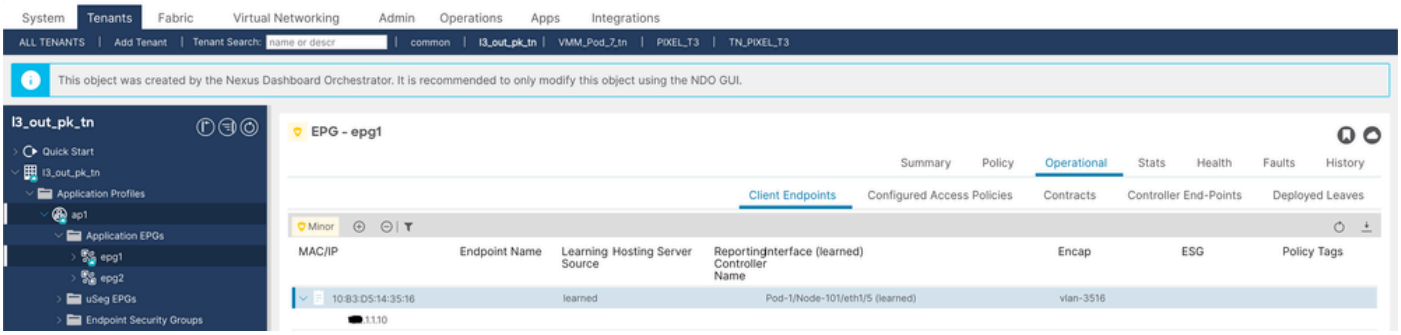
Topologie



Topologie

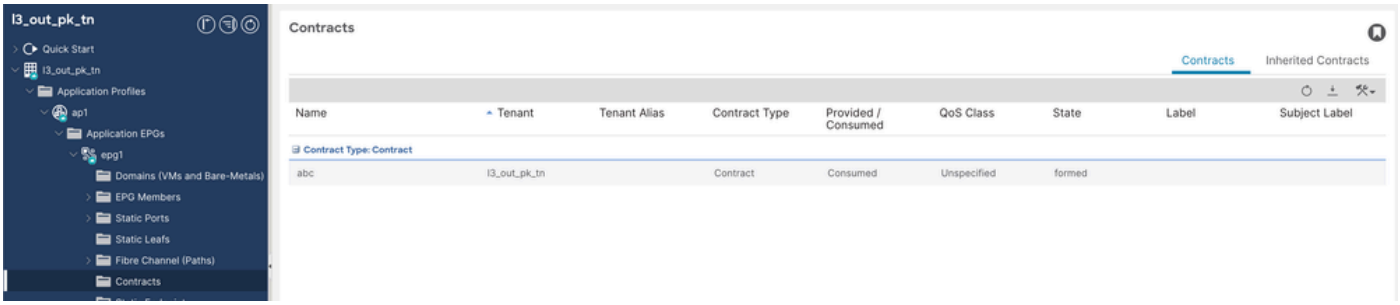
De EPG1- en EPG2-configuratie worden niet in dit document weergegeven. Deze moeten voor de hand worden geconfigureerd en er moet een eindpunt worden geleerd.

1. Valideren van EPG1-eindpunt X.1.1.10 (knooppunt 101).



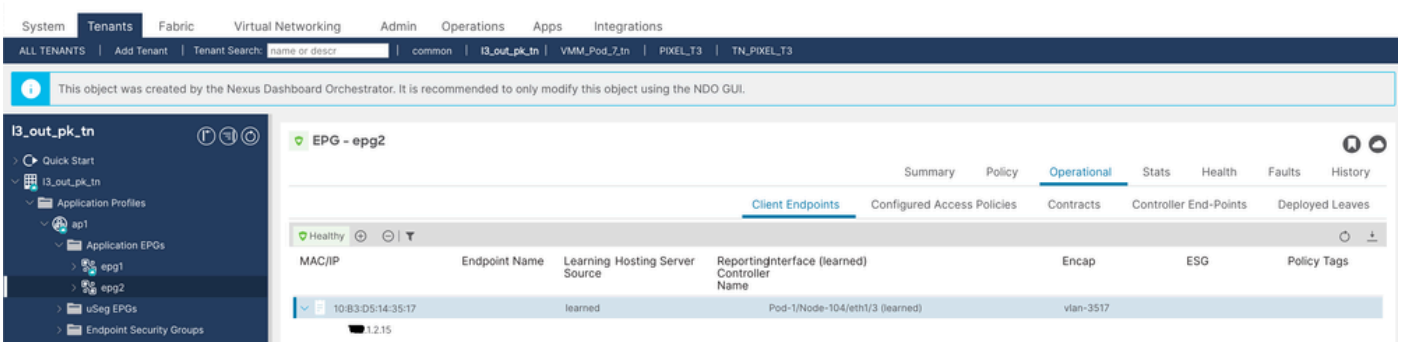
Clientendpoints

2. Abc van het contract wordt door EPG1 verbruikt.



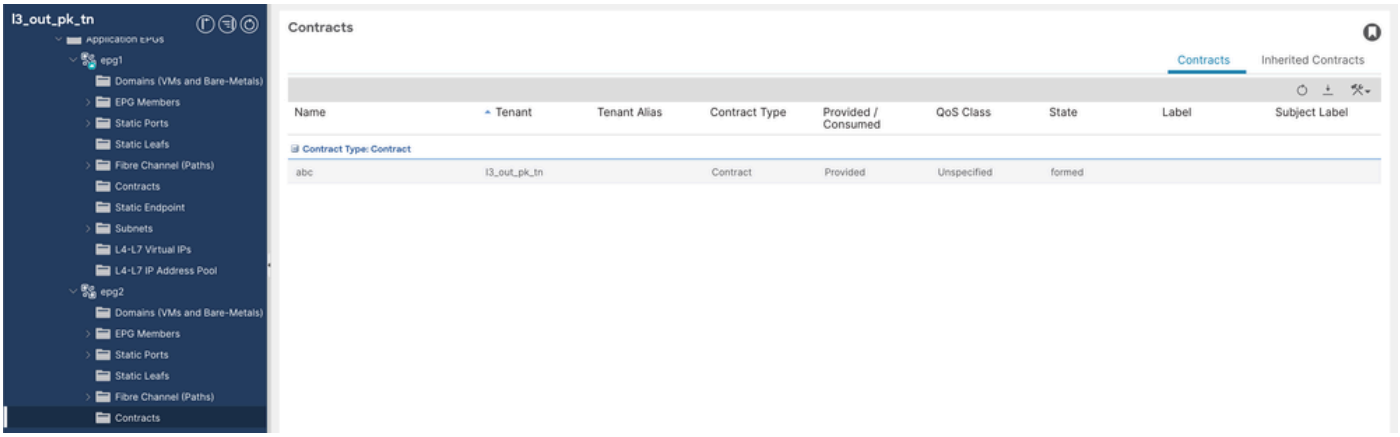
Verbruikt contract

3. Validate EPG2 heeft eindpunt X.1.2.15aangeleerd (knooppunt 104).



Clientendpoint

4. Het contract abc wordt door EPG2 verstrekt.



Waarom L2-servicegrafiek nodig is in ACI?

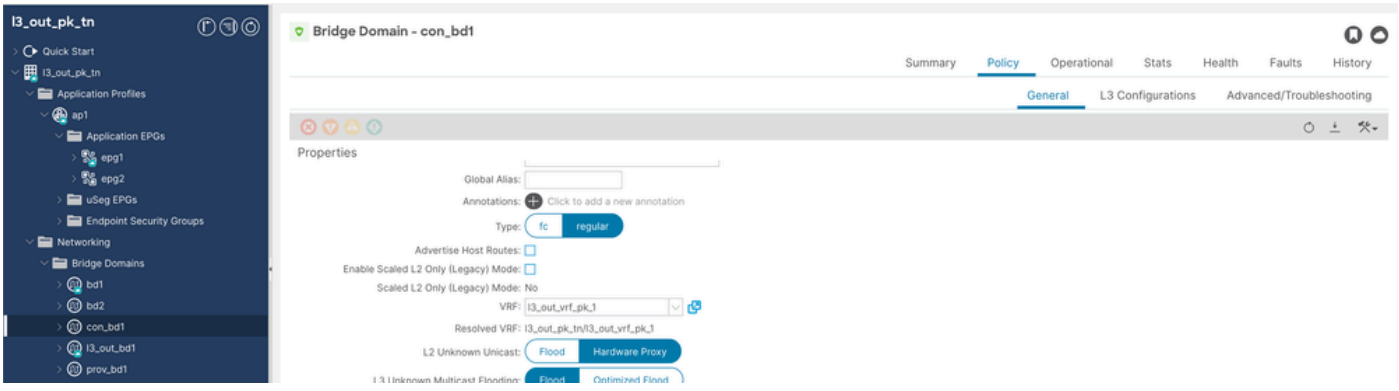
- In Cisco ACI kunnen L4-L7-serviceapparaten worden ingevoegd bij Layer 3 (L3), Layer 2 (L2) of Layer 1 (L1).
- Layer 3-service-invoeging: Het externe apparaat (bijvoorbeeld firewall, Inbraakpreventiesysteem (IPS)) neemt routeringsbeslissingen en doorsturen van verkeer op basis van IP-adressen.
- Layer 2 Service-invoeging: Verkeer wordt doorgestuurd op basis van MAC-adressen zonder routing betrokkenheid. Dit is handig voor transparante firewalls en IPS-apparaten.
- L2 Policy-Based Routing (PBR) wordt gebruikt bij het invoegen van een L2-serviceapparaat, zoals een IPS of transparante firewall in ACI.
- Het verkeersdoorsturen mechanisme blijft hetzelfde voor zowel L3 als L2 PBR.
- Het belangrijkste verschil:
  - L3 PBR: Het verkeer wordt omgeleid naar een IP-adres (apparaat neemt deel aan de routing).
  - L2 PBR: Verkeer wordt omgeleid naar een MAC-adres (apparaat werkt op Layer 2).
- In L2 PBR, zijn de adressen van MAC statisch gebonden aan bladinterfaces om juist verkeer het door:sturen te verzekeren.

Zie PBR-witboek voor meer informatie over actieve/Stanby- of Active/Active L1/L2 PBR-gebruikscases.

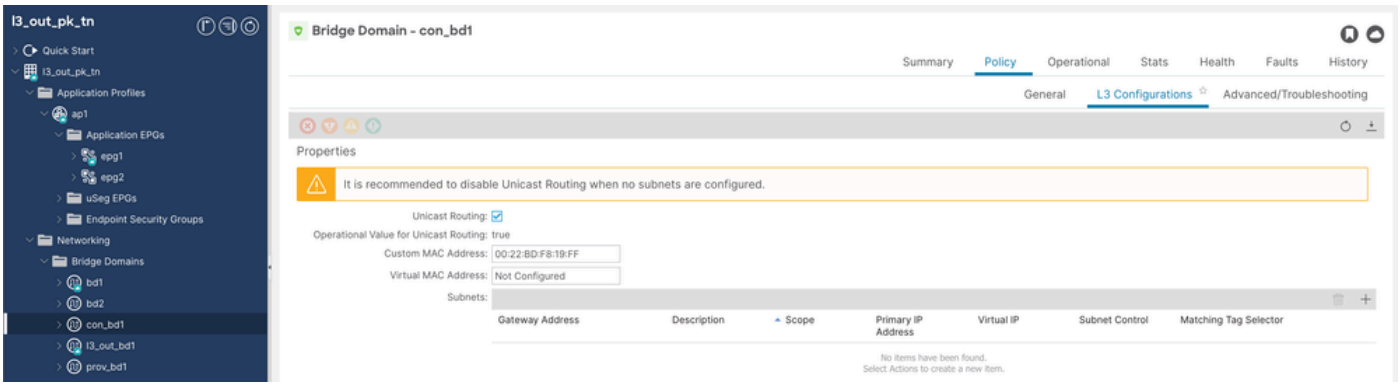
Configuratie voor L2-servicekaart

Stap 1. Configureer consumentenbestand met de naam con-bd1.

Unicast-routing moet worden ingeschakeld, L2 onbekende unicast moet worden ingesteld op Hardware-proxy en er is geen subnetverbinding vereist voor con- en prov-bridgedomeinen (BD's).

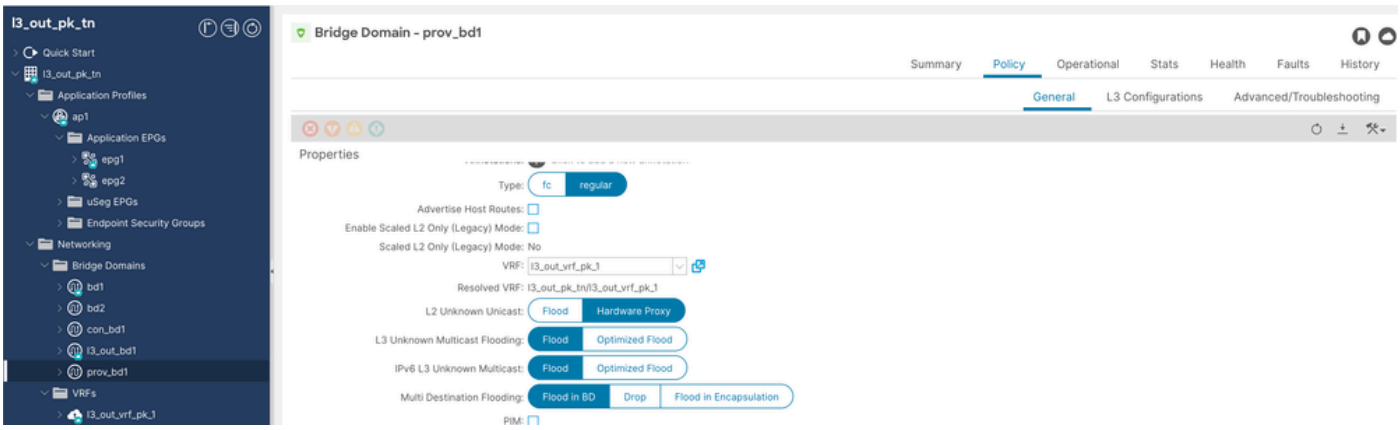


Nadelen BD-configuratie

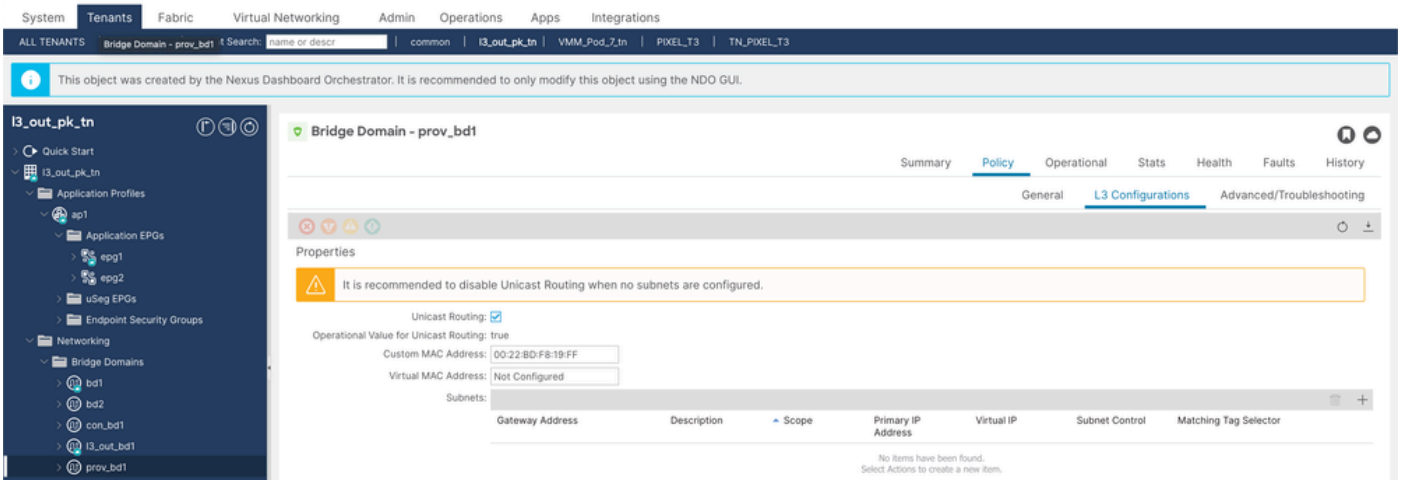


BD-configuratie 2

Stap 2. Configureer provider bd met de naam prov-bd1.



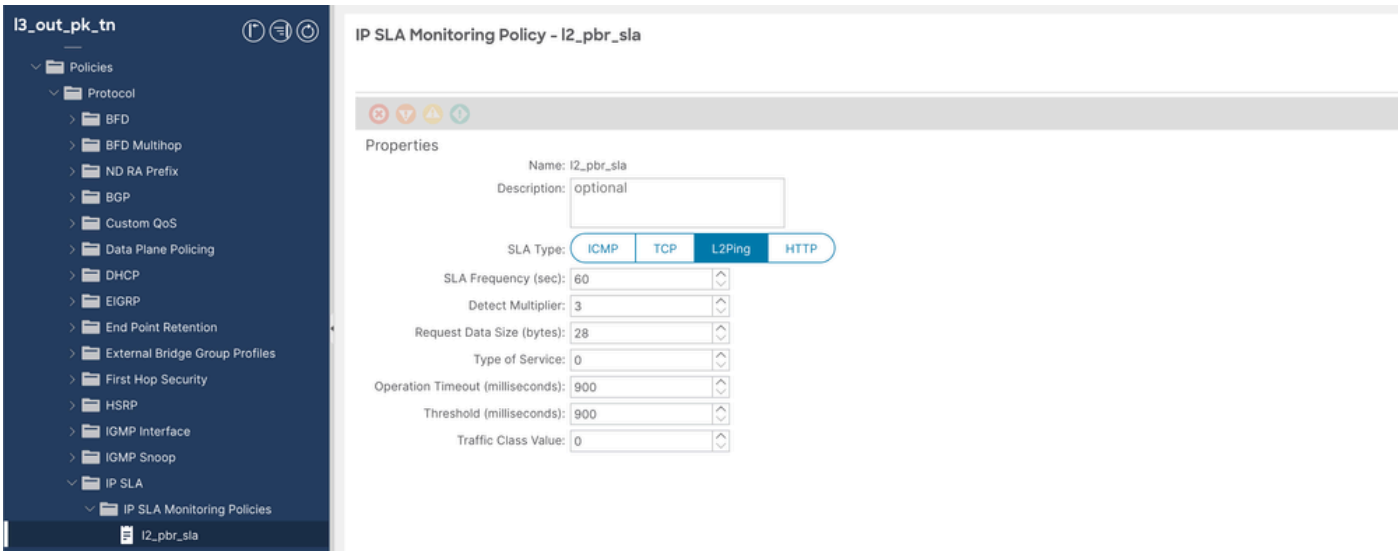
Prov BD-configuratie



Prov BD-configuratie 2

Stap 3. Configureer het beleid voor IP-serviceovereenkomst (SLA) met SLA-type L2Ping.

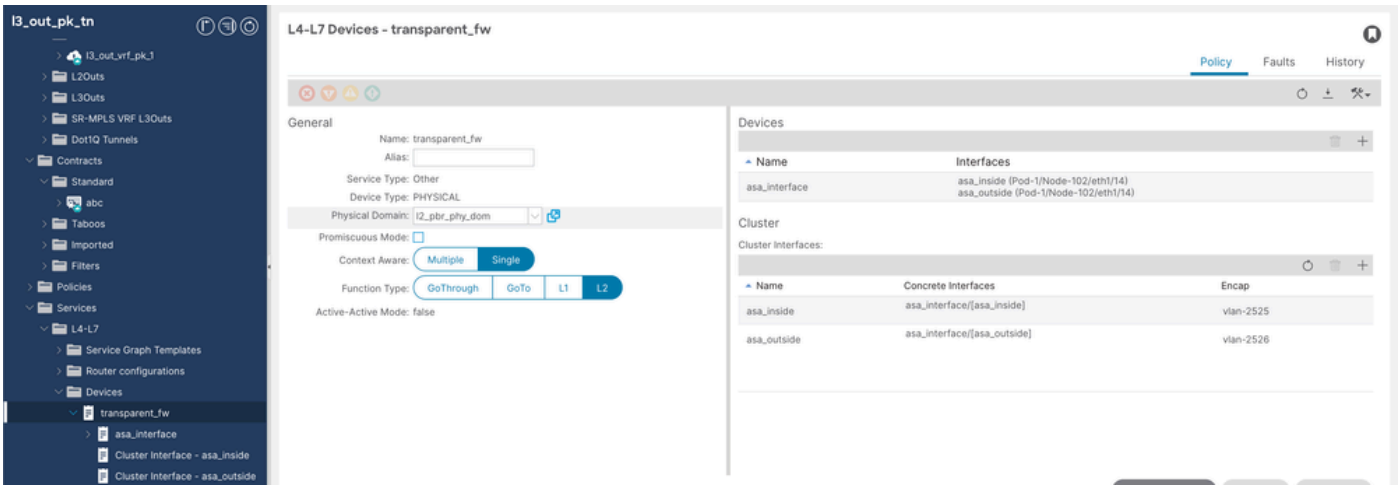
Navigeer naar huurder > Beleid > Protocol > IP SLA > IP SLA Monitoring Policies, klik met de rechtermuisknop en maak beleid.



IP SLA-beleid

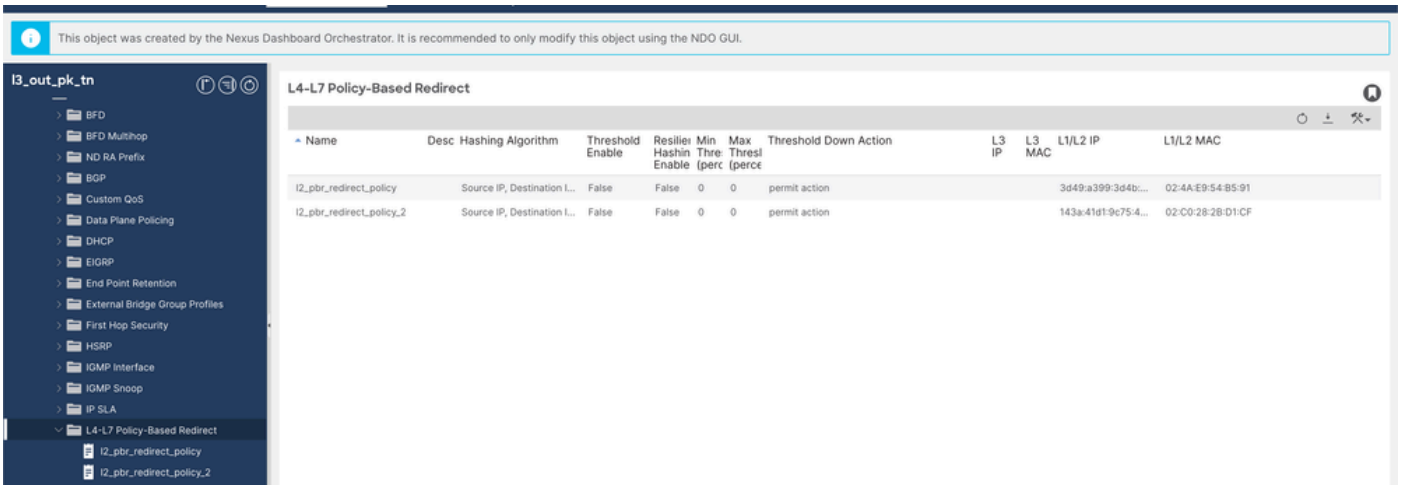
Stap 4. Configureer het L4/L7-apparaat.

Navigeer naar Huurder > Diensten > Apparaten, klik met de rechtermuisknop en maak L4-L7 apparaat.



L4-L7-apparaat

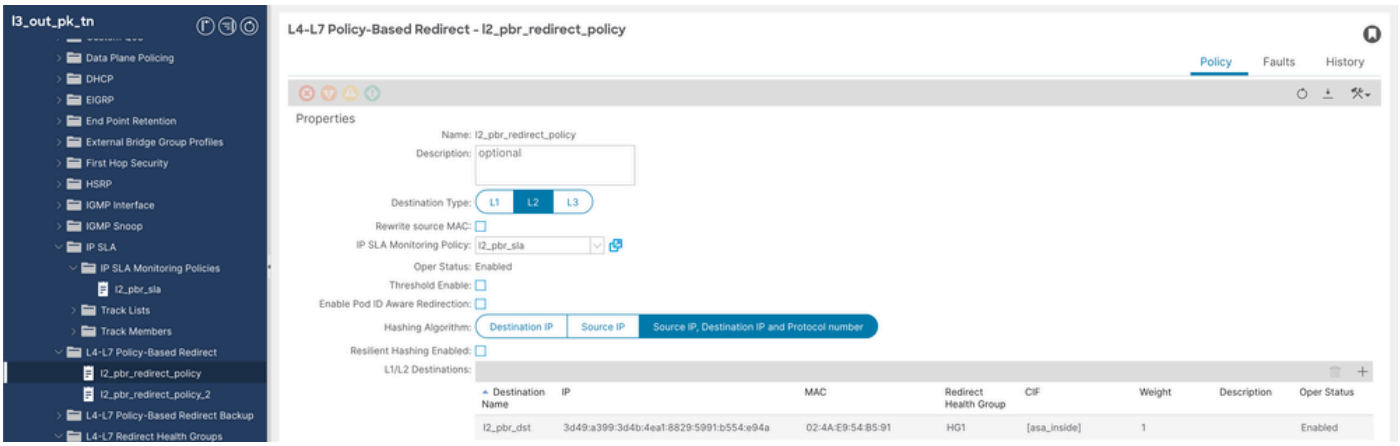
Stap 5. Valideren op beleid gebaseerd redirect overzicht (u kunt dit controleren na het configureren van 5a en 5b).



L4-L7 omleidingsbeleid

Stap 5.1. Configureer op L4-L7-beleid gebaseerd omleidingsbeleid voor adaptieve security applicatie (ASA) binnen interface (u hoeft MAC of IP niet te specificeren, het wordt ingevuld door APIC zelf).

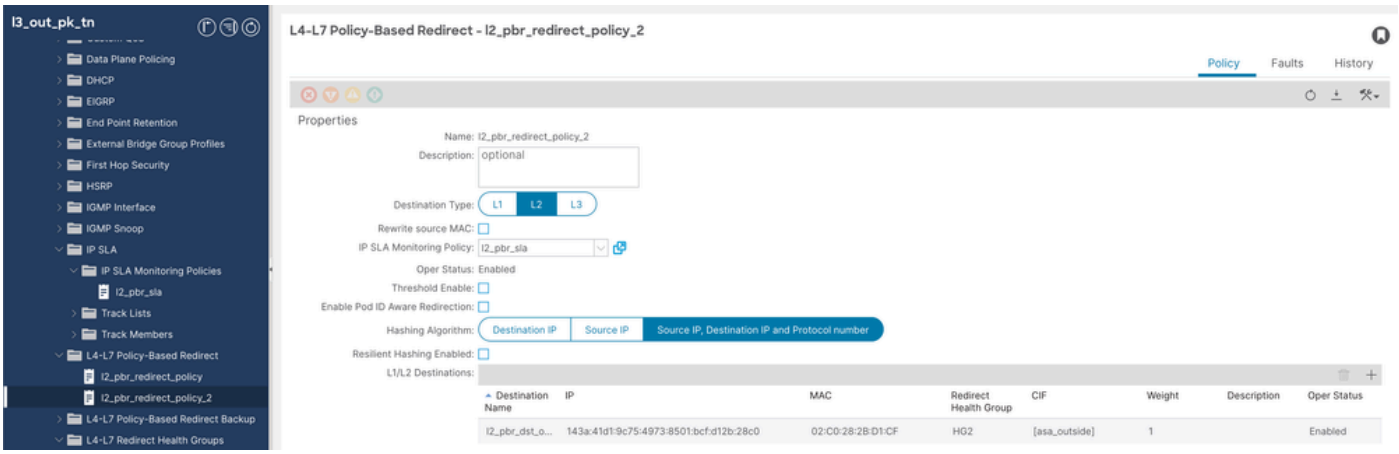
Navigeer naar Huurder > Beleid > Protocol > L4-L7 Beleid gebaseerd omleiden, dan rechtsklik en maak beleid.



L4-L7 omleiden beleidsconfiguratie

Stap 5.2. Configureer op L4-L7-beleid gebaseerd omleidingsbeleid voor ASA buiteninterface (u hoeft geen MAC of IP te specificeren, het wordt door APIC zelf ingevuld).

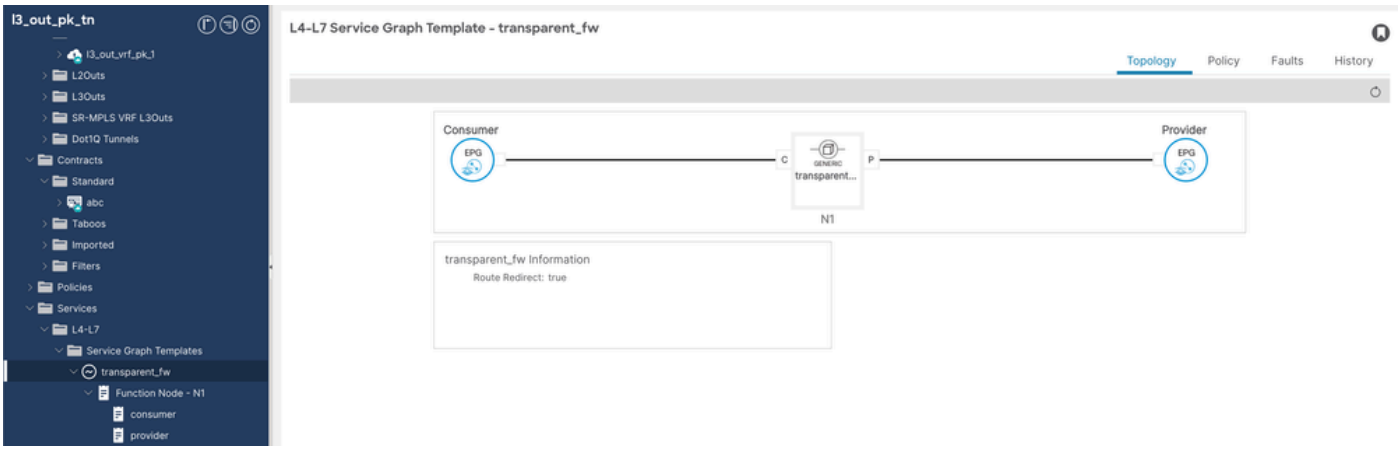
Navigeer naar Huurder > Beleid > Protocol > L4-L7 Beleid gebaseerd omleiden, dan rechtsklik en maak beleid.



L4-L7 omleiden beleid configuratie 2

Stap 6. Configureer de sjabloon voor de servicegrafiek.

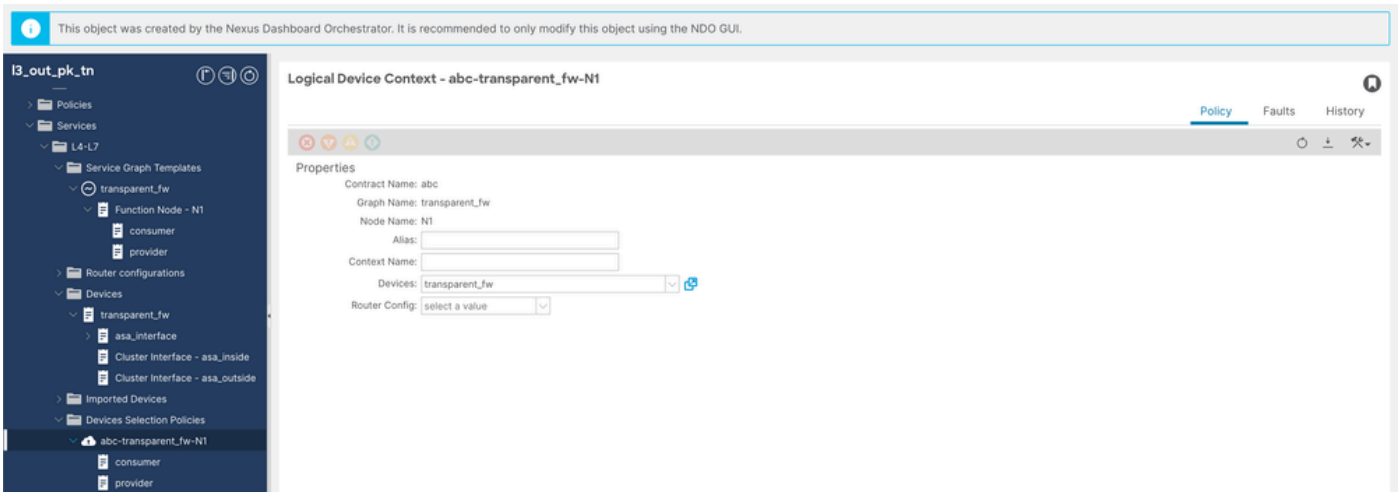
Navigeer naar huurder > Services > Servicegrafsjabloon, klik met de rechtermuisknop en maak L4-L7-servicegrafsjabloon.



Servicegrafische configuratie

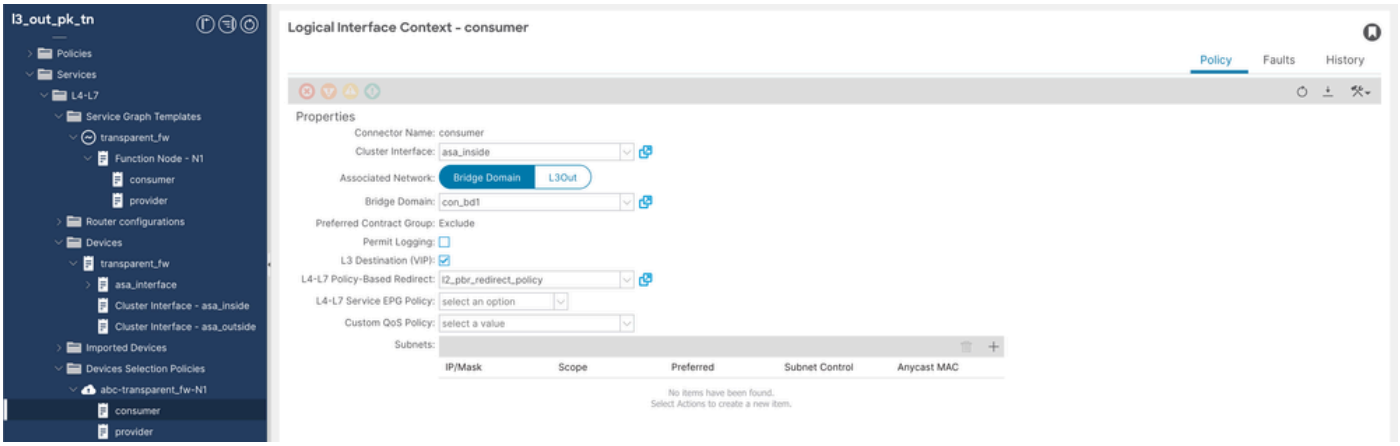
Stap 7. Configureer het beleid voor apparaatselectie.

Navigeer naar Huurder > Services > Apparaatselectiebeleid, klik met de rechtermuisknop en maak Apparaatselectiebeleid.



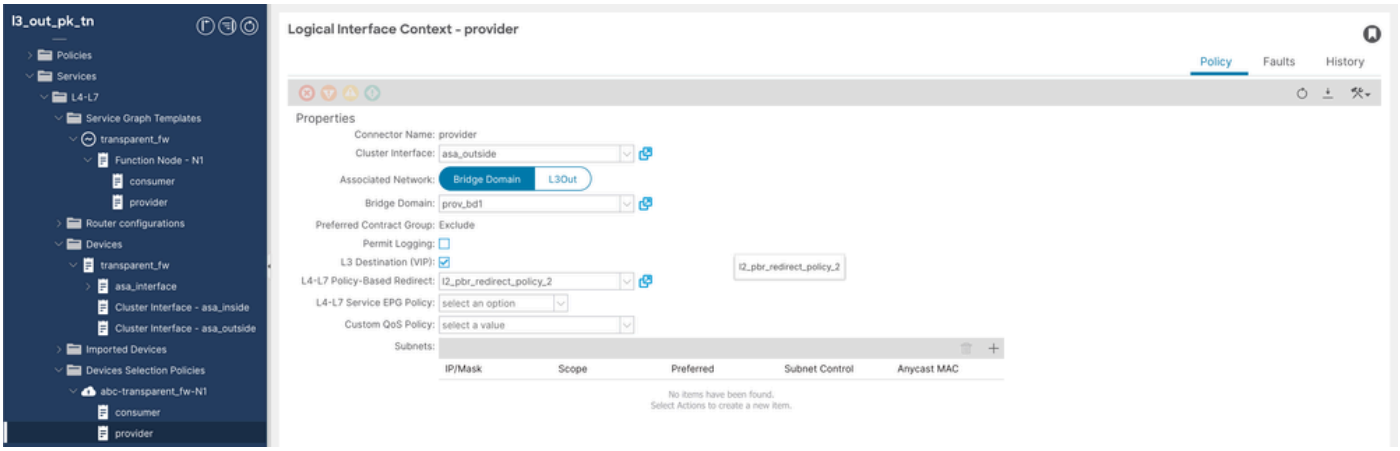
Servicegrafiek, configuratie 2

++ logische interfacecontext voor consumenten

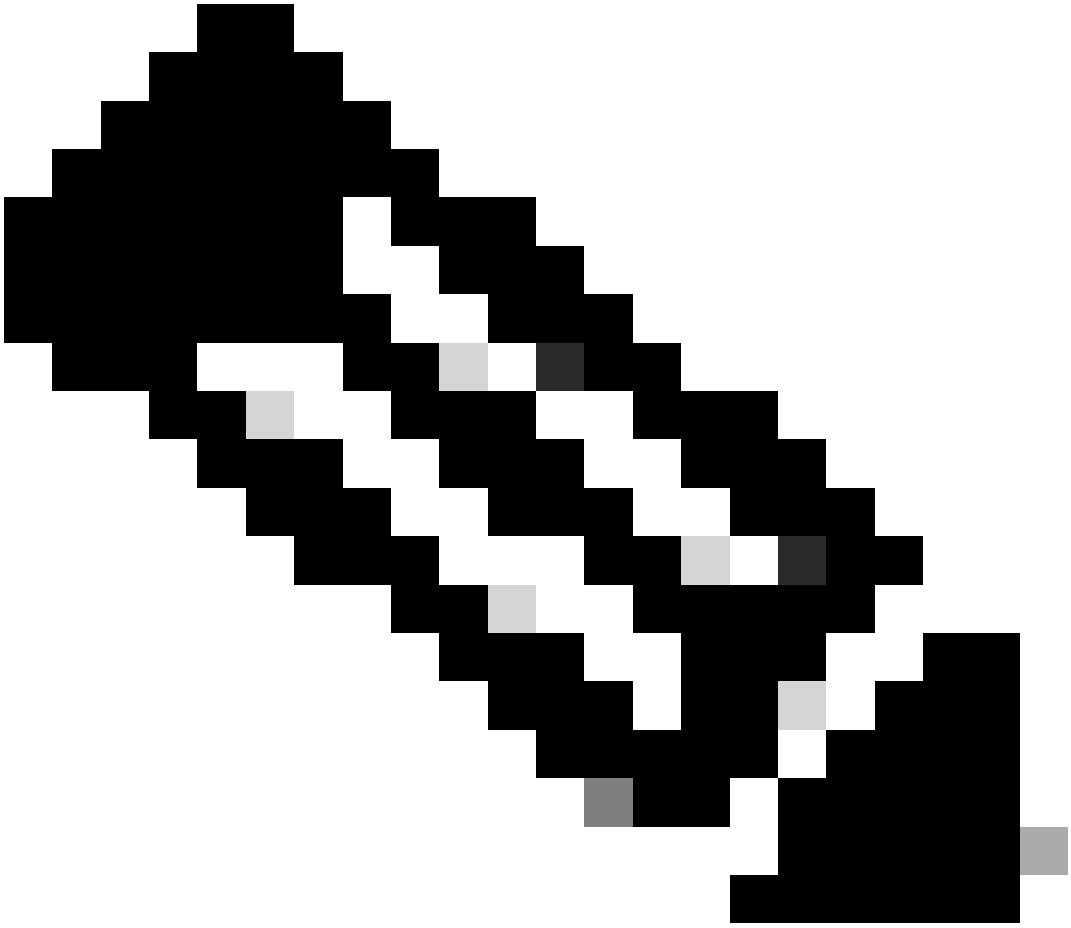


Beleid voor apparaatselectie Consumentenconfiguratie

Logische interfacecontext van ++-providers



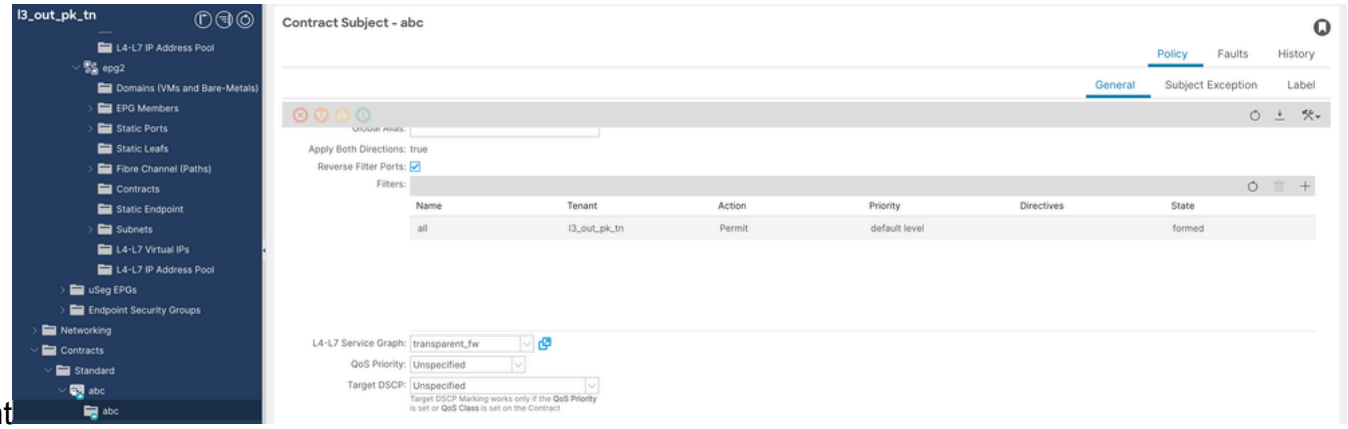
Provider van beleid voor apparaatselectie



Opmerking: Selectiebeleid voor apparaten als deze automatisch worden gemaakt, want u gaat de optie Servicegrafiek toepassen gebruiken.

Stap 8. Pas PBR toe om het onderwerp ABC aan te gaan.

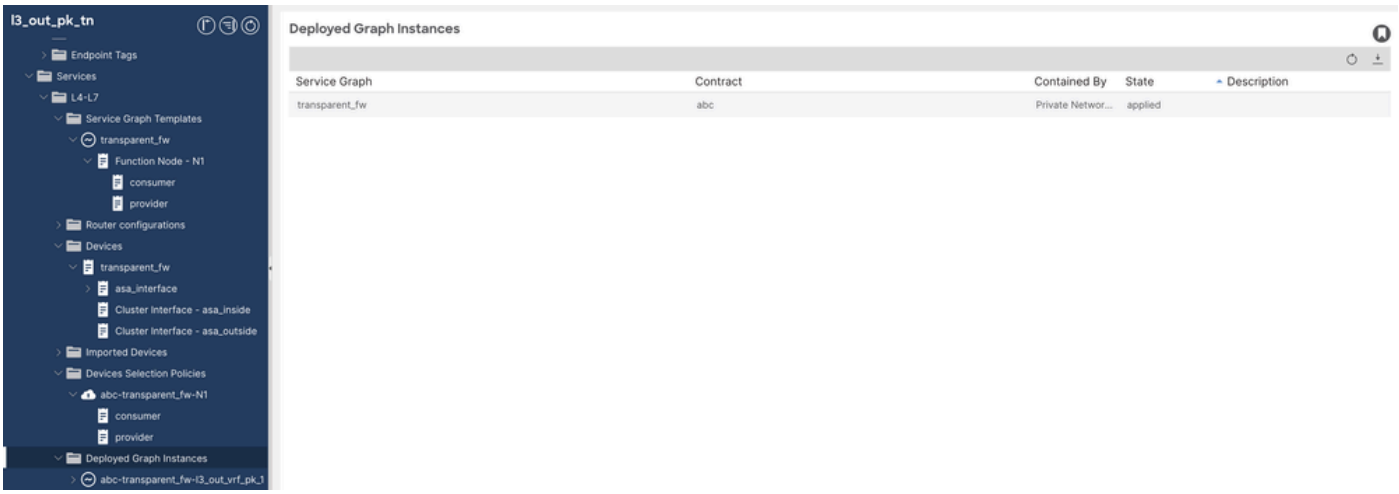
Ga naar huurder > Contract > Onderwerp contract > L4-L7 servicegrafiek > transparency_fw.



kont

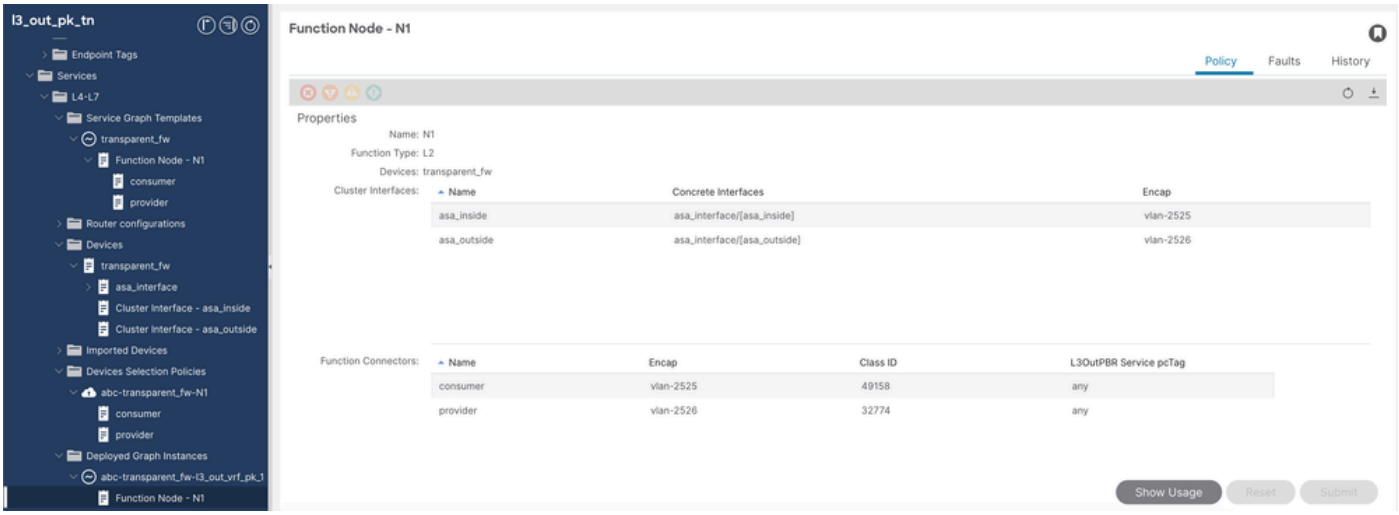
Contractconfiguratie

Stap 9. Indien met succes geïmplementeerd, valideren onder geïmplementeerde instantiegrafiek (naar status zoeken).



Validatie van servicegrafiek

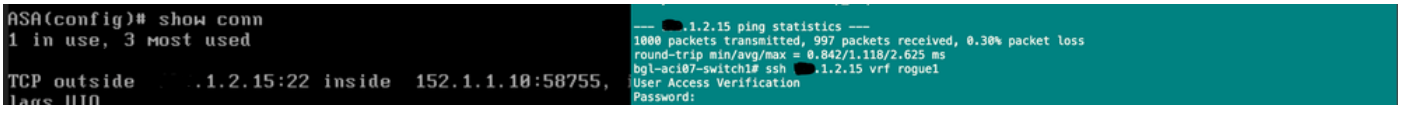
++ Bevestig clusterinterfaces, encap VLAN's en klasse-ID's van functieconnector.



Validatie van servicegrafiek 2

L2 PBR-verkeer valideren op ASA

Secure Shell (SSH) van Src-eindpunt naar dst-eindpunt dat u in een tabel met conn op ASA kunt zien.



ASA-validatie

Controleer L2 PBR op blad

1. VLAN-programmering op bladknooppunt 102.

<#root>

```
PBR vlan 2525 and 2526 will get programmed on leaf node 102 and mac addresses will be statically tied t

bgl-aci07-apic100#

fabric 102 show endpoint


----------------------------------------------------------------
Node 102 (bgl-aci07-leaf2)
----------------------------------------------------------------
Legend:
S - static           s - arp              L - local            O - peer-attached
V - vpc-attached     a - local-aged       p - peer-aged        M - span
B - bounce           H - vtep             R - peer-attached-rl D - bounce-to-proxy
E - shared-service   m - svc-mgr
+-----------------------------------+---------------+-----------------+--------------+--------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+-----------------------------------+---------------+-----------------+--------------+--------------+
28/l3_out_pk_tn:l3_out_vrf_pk_1           vlan-2525    024a.e954.b591 LS                    eth1/14
1/l3_out_pk_tn:l3_out_vrf_pk_1            vlan-2526    02c0.282b.d1cf LS                    eth1/14
```

2. Redirect beleid en zoning-regel op consument (101) en leverancier (104) knooppunt.

<#root>

```
++ Redirect policy on consumer node

bgl-aci07-apic100#

fabric 101 show service redir info


----------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
----------------------------------------------------------------
================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |
================================================================================================================
List of Dest Groups
GrpID Name            destination                                                 HG-name
===== ====            ===========                                                 ==============
7     destgrp-7       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
8     destgrp-8       dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  l3_out_pk_tn::HG2

List of destinations
Name                                                        bdVnid          vMac                vrf
====                                                        ======          ====                ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328  02:4A:E9:54:B5:91    l3_
dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  vxlan-16056296  02:C0:28:2B:D1:CF    l3_

List of Health Groups
```

```
HG-Name                                    HG-OperSt  HG-Dest
=======                                    =========  =======
l3_out_pk_tn::HG1                          enabled    dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
l3_out_pk_tn::HG2                          enabled    dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx

List of Backup Destinations
Name                                                          primaryDestName
====                                                          ==============
List of AclRules
AclRuleVnid     DestGroup       OperSt   OperStQual
===========     =========       ======   ==========

++ Zoning rule on consumer Node

bgl-aci07-apic100#
```

fabric 101 show zoning-rule | grep redir

```
|   4228  | 32771  | 49157  | default  |     bi-dir     | enabled | 2228224  |
|   4231  | 49157  | 32771  | default  | uni-dir-ignore | enabled | 2228224  |
|   4230  | 32771  |   15   | default  |    uni-dir     | enabled | 2228224  |
|   4229  | 16386  | 32771  | default  |    uni-dir     | enabled | 2228224  |
```

<#root>

```
++ Redirect Policy on Provider Node
bgl-aci07-apic100#
```

fabric 104 show service redir info

```
------------------------------------------------------------------
Node 104 (bgl-aci07-leaf4)
------------------------------------------------------------------
================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |
================================================================================================================
List of Dest Groups
GrpID Name            destination                                                    HG-name
===== ====            ===========                                                    ==============
3     destgrp-3       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
4     destgrp-4       dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  l3_out_pk_tn::HG2

List of destinations
Name                                                          bdVnid          vMac                vrf
====                                                          ======          ====                ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328  02:4A:E9:54:B5:91    l3_
dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  vxlan-16056296  02:C0:28:2B:D1:CF    l3_

List of Health Groups
HG-Name                                    HG-OperSt  HG-Dest
=======                                    =========  =======
l3_out_pk_tn::HG1                          enabled    dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
l3_out_pk_tn::HG2                          enabled    dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx
List of Backup Destinations
Name                                                          primaryDestName
====                                                          ==============
```

```
++ Zoning rule on provider node
bgl-aci07-apic100#
```

fabric 104 show zoning-rule | grep redir

```
|   4220  | 32771  | 49157  | default  |     bi-dir     | enabled | 2228224  |
|   4221  | 49157  | 32771  | default  | uni-dir-ignore | enabled | 2228224  |
```

Fouten gezien in geval L2Ping mislukt

In het geval L2pings faalt over PBR apparaat, zult u zien PBR is nog in uitgerold staat en de fouten F4203, F2833, en F2911 omhoog het beginnen van spoor/gezondheidsgroep zijn neer.

L2-pings opnemen

U kunt L2Pings vangen met behulp van tcpdump op tahoe interface om te weten of ze correct verzonden en ontvangen worden. Als u alleen CPU-verzending ziet die verzonden en niet ontvangen is, worden de eerder genoemde fouten verwacht en moet u verder problemen oplossen bij ASA waarom deze worden verwijderd (zie ASA-configuratiesectie).

<#root>

```
Capturing L2Pings using tcpdump on PBR Node 102

bgl-aci07-leaf2#
```

tcpdump -i tahoe0 -w /data/techsupport/l2_pbr1.pcap

```
tcpdump: listening on tahoe0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4858 packets captured
4875 packets received by filter
0 packets dropped by kernel
```

In order to deocde the tcpdump

cat /data/techsupport/l2_pbr1.pcap | knet_parser.py --decode tahoe --pcap | less

```
** Search for mac 00ab.8752.3100

++ CPU transmit packets
Frame 505
Time: 2024-10-29T05:55:28.707136+00:00
Header: ieth
```

CPU Transmit

```
sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x207, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
```

Len: 72
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/

ethertype:0x721

Frame 506
Time: 2024-10-29T05:55:28.707297+00:00
Header: ieth CPU Transmit
sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x208, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
Len: 72
Eth:

00ab.8752.3100 > 02c0.282b.d1cf

, len/

ethertype:0x721

++CPU recived packets

Frame 509
Time: 2024-10-10T20:16:37.580855+00:00
Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH

(0x4d)
Header: ieth
sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x209, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0
src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0
dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0
Len: 76
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/ethertype:0x8100(802.1q)
802.1q:

vlan:2526

, cos:0, len/

ethertype:0x721

Frame 510
Time: 2024-10-10T20:16:37.580891+00:00
Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH(0x4d)

```
Header: ieth
sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x20a, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0
src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0
dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0
Len: 76
Eth:
```

00ab.8752.3100 > 02c0.282b.d1cf

```
, len/ethertype:0x8100(802.1q)
802.1q:
```

vlan:2525

```
, cos:0, len/
```

ethertype:0x721

Traffic Flow van SRC naar DST-endpoint

<#root>

```
++ Endpoint X.1.1.10 want to send traffic to X.1.2.15
++ If destination is not learned on consumer/source leaf, PBR will be performed on destination leaf
++ For this case we are assuming endpoint X.1.2.15 is learned on Leaf 101 so PBR/Redirection will be pe

bgl-aci07-apic100#
```

fabric 101 show endpoint

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
Legend:
S - static           s - arp              L - local            O - peer-attached
V - vpc-attached     a - local-aged       p - peer-aged        M - span
B - bounce           H - vtep             R - peer-attached-rl D - bounce-to-proxy
E - shared-service   m - svc-mgr
+----------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+----------------------------------+---------------+-----------------+--------------+-------------+
l3_out_pk_tn:l3_out_vrf_pk_1                              X.1.2.15                      tunnel6 ===>
17                                    vlan-3516    10b3.d514.3516 L                     eth1/5 ===
l3_out_pk_tn:l3_out_vrf_pk_1          vlan-3516        X.1.1.10 L                       eth1/5
```

```
++ EPM entry to get the PC TAG
bgl-aci07-apic100#
```

fabric 101 show system internal epm endpoint ip X.1.1.10

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
MAC : 10b3.d514.3516 ::: Num IPs : 1
```

```
IP# 0 : X.1.1.10 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 17 ::: Vlan vnid : 11792 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 16744307 ::: VRF vnid : 2228224
Phy If : 0x1a004000 ::: Tunnel If : 0
Interface : Ethernet1/5
Flags : 0x80005c04 ::: sclass :
```

32771

```
 ::: Ref count : 5 ==> sclass
EP Create Timestamp : 10/11/2024 09:15:44.430334
EP Update Timestamp : 10/29/2024 10:45:35.458416
EP Flags : local|IP|MAC|host-tracked|sclass|timer|

bgl-aci07-apic100#
```

fabric 101 show system internal epm endpoint ip X.1.2.15

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
MAC : 0000.0000.0000 ::: Num IPs : 1
IP# 0 : X.1.2.15 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 0 ::: Vlan vnid : 0 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 0 ::: VRF vnid : 2228224
Phy If : 0 ::: Tunnel If : 0x18010006
Interface : Tunnel6
Flags : 0x80004400 ::: sclass :
```

49157

```
 ::: Ref count : 3 ==> sclass
EP Create Timestamp : 10/29/2024 10:38:34.949150
EP Update Timestamp : 10/29/2024 10:45:55.571786
EP Flags : IP|sclass|timer|

++ Traffic will be redirected based on redir(destgrp-7)
bgl-aci07-apic100#
```

fabric 101 show zoning-rule src-epg 32771 dst-epg 49157

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------
| Rule ID | SrcEPG | DstEPG | FilterID |  Dir   |  operSt |  Scope  | Name |      Action      |    Prio
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------
|   4228  | 32771  | 49157  | default  | bi-dir | enabled | 2228224 |      | redir(destgrp-7) | src_dst_
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------

++ Based on redirect policy traffic will be redirected to mac
```

02:4A:E9:54:B5:91

```
bgl-aci07-apic100#
```

fabric 101 show service redir info

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
```

```
================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |
================================================================================================================
List of Dest Groups
GrpID Name            destination                                                    HG-name
===== ====            ===========                                                    ==============
7     destgrp-7       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
List of destinations
Name                                                          bdVnid          vMac                 vrf
====                                                          ======          ====                 ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328
```

02:4A:E9:54:B5:91

```
    l3_out_pk_tn:l3_out_vrf_pk_1 enabled    no-oper-dest    l3_out_pk_tn::HG
1

++ PBR mac addresses are never learnt remotely as IP/MAC learning is disabled for PBR BD
++ PBR mac addresses are statically binded to interfaces where L4/L7 device is connected and reported t
++ Traffic will be forwarded to SPINE PROXY
++ Spine has an COOP entry for 02:4A:E9:54:B5:91

bgl-aci07-apic100#
```

fabric 201 show coop internal info repo ep key 16744328 02:4A:E9:54:B5:91

```
------------------------------------------------------------------
Node 201 (bgl-aci07-spine1)
------------------------------------------------------------------
Repo Hdr Checksum : 49503
Repo Hdr record timestamp : 10 29 2024 10:15:07 658496921
Repo Hdr last pub timestamp : 10 29 2024 10:15:07 661679296
Repo Hdr last dampen timestamp : 01 01 1970 00:00:00 0
Repo Hdr dampen penalty : 0
Repo Hdr flags : IN_OBJ ACTIVE
EP bd vnid : 16744328
EP mac :
```

02:4A:E9:54:B5:91

```
 <<<<========== ASA MAC
flags : 0x480
repo flags : 0x102
Vrf vnid : 2228224
PcTag : 0x100c006
EVPN Seq no : 0
Remote publish timestamp: 01 01 1970 00:00:00 0
Snapshot timestamp: 10 29 2024 10:15:07 658496921
Tunnel nh : 10.0.144.66
MAC Tunnel  : 10.0.144.66
IPv4 Tunnel : 10.0.144.66
IPv6 Tunnel : 10.0.144.66
ETEP Tunnel : 0.0.0.0
num of active ipv4 addresses : 0
num of anycast ipv4 addresses : 0
num of ipv4 addresses : 0
num of active ipv6 addresses : 0
num of anycast ipv6 addresses : 0
num of ipv6 addresses : 0
Primary Path:
Current published TEP :
```

10.0.144.66

```
Backup Path:
BackupTunnel nh : 0.0.0.0
Current Backup (publisher_id): 0.0.0.0
Anycast_flags : 0
Current citizen (publisher_id): 10.0.144.66
Previous citizen : 10.0.144.66
Prev to Previous citizen : 10.0.144.66
Synthetic Flags : 0x5
Synthetic Vrf : 411
Synthetic IP : X.X.83.223
Tunnel EP entry: 0x7f20900167a8
Backup Tunnel EP entry: (nil)
TX Status: COOP_TX_DONE\
Damp penalty: 0
Damp status: NORMAL
Exp status: 0
Exp timestamp: 01 01 1970 00:00:00 0
Hash: 3209430840 owner: 10.0.144.65

++ Spine will forward this to PBR Leaf Node 102 based on COOP entry
++ PBR Leaf Node will forward this to ASA FW on interface E1/14
++ ASA FW will forward the traffic based on mac address table and send it back to PBR Leaf Node 102
++ PBR Leaf Node will look for Dst IP in the traffic and route it to Leaf 104 if remote endpoint entry
++ Leaf 104 will get this traffic forwarded to actual EP X.1.2.15 (Leaf4 does not learn the client IP a
```

ASA-configuratie

Stap 1. Interfaceconfiguratie.

<#root>

ASA(config)#

show running-config interface

```
!
interface GigabitEthernet0/0
 bridge-group 1
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 bridge-group 1
 nameif outside
 security-level 0
!
interface BVI1
ip address 192.168.100.1 255.255.255.0 ==> In case BVI IP is not defined ASA will not switch the packet
!
```

Stap 2. MAC-leren moet worden uitgeschakeld.

<#root>

```
ASA(config)#
```

show run mac-learn

```
mac-learn inside disable
mac-learn outside disable
```

PBR:

Stap 3. Statische MAC-adrestabel voor PBR Mac.

<#root>

```
The mac statically binded to inside interface is the PBR mac generated by provider and vice versa
ASA(config)#
```

show run mac-address-table

```
mac-address-table static outside 024a.e954.b591
mac-address-table static inside 02c0.282b.d1cf
```

Stap 4. Configuratie van toegangscontrolelijst (ACL) om L2pings over te gaan.

<#root>

```
ASA(config)#
```

show access-list

```
access-list L2_PBR ethertype permit 721

ASA(config)# show run access-group
access-group L2_PBR in interface inside
access-group L2_PBR in interface outside
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.