Konfiguration und Überprüfung der Layer-2-Servicediagrammkonfiguration mit ASAv

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

- [Anforderungen](#)
- [Verwendete Komponenten](#)

[Topologie](#)

[Warum ist ein L2-Servicediagramm für die ACI erforderlich?](#)

[Konfiguration für L2-Servicediagramm](#)

[Validierung des L2-PBR-Datenverkehrs auf der ASA](#)

[L2-PBR auf Leaf überprüfen](#)

[Fehler in Fall L2Ping fehlgeschlagen](#)

- [Erfassen von L2-Pings](#)

[Datenverkehrsfluss vom SRC zum Ziel-Endpunkt](#)

[ASA-Konfiguration](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Layer-2-Servicediagrammkonfiguration in der Cisco Application Centric Infrastructure (ACI) konfigurieren und überprüfen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Layer-3-Servicediagramm in der ACI
- Konfiguration von Endpunkt-Richtliniengruppen, Bridge-Domänen und Verträgen in der ACI
- Informationen zur Konfiguration von (Adaptive Security Appliance Virtual) ASAv als transparente Firewall

Verwendete Komponenten

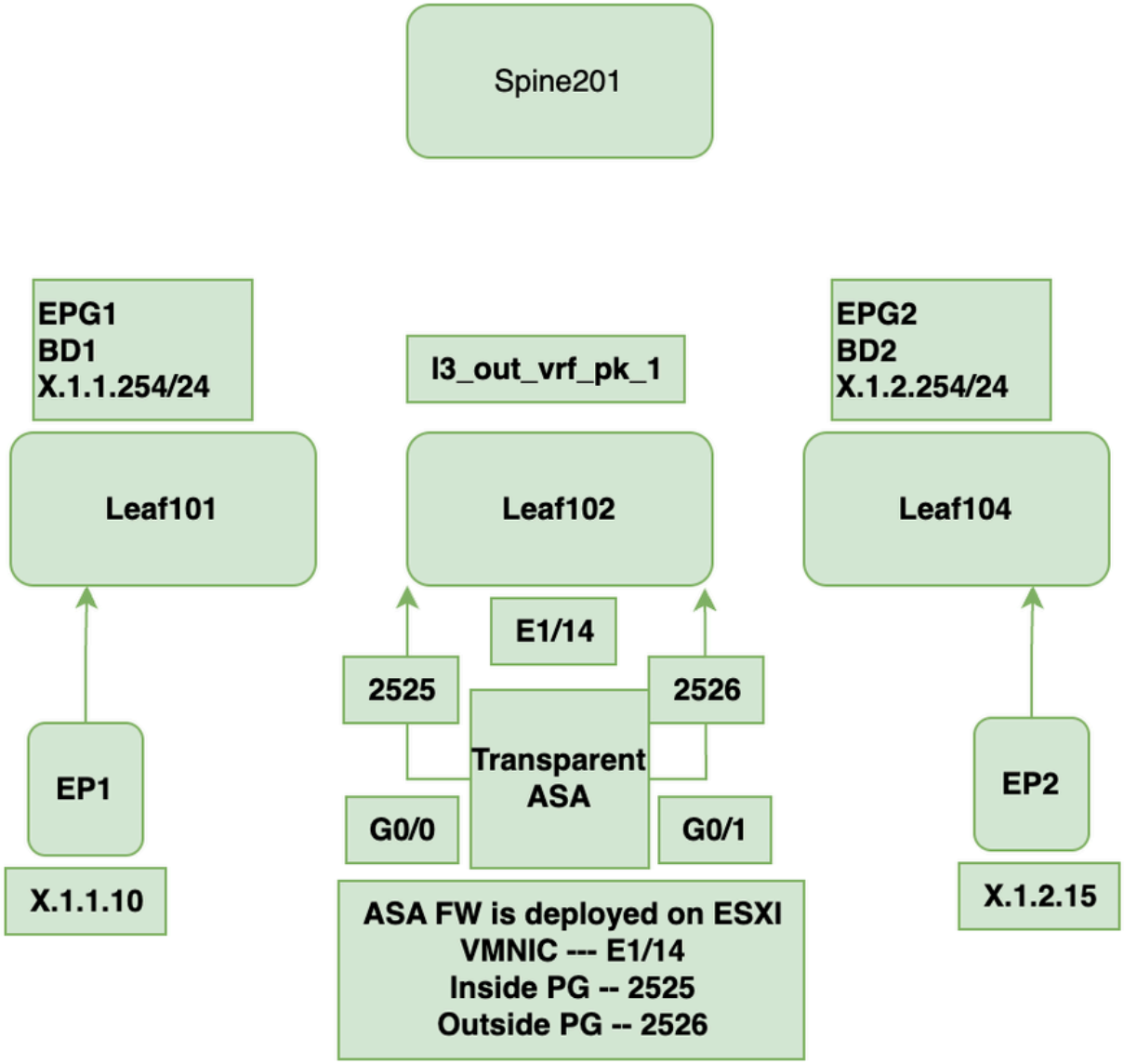
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- APIC-Version: 6.0 (3g)
- Blatt Hardware: N9K-C93180YC-FX

- Blatt S/W: n9000-16,0 (3 g)
- Leaf-Knoten 101, 102, 103
- ASAv bereitgestellt auf ESXi-Server

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

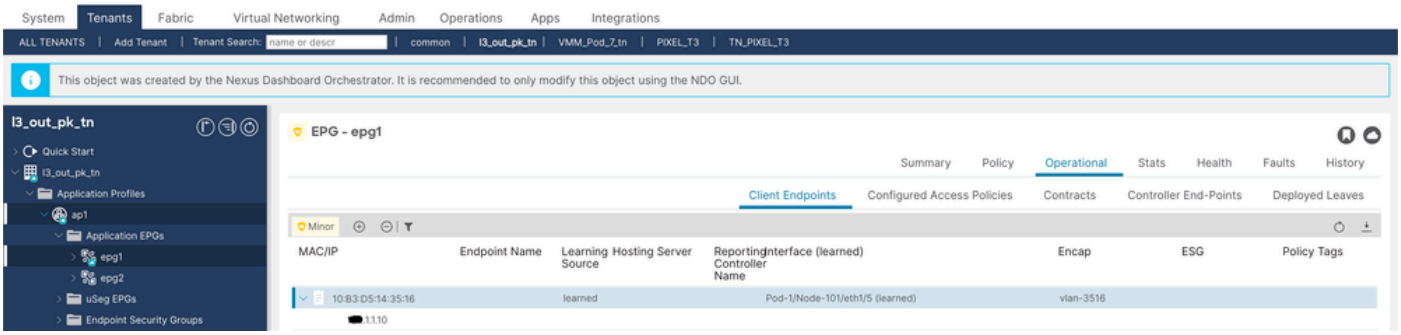
Topologie



Topologie

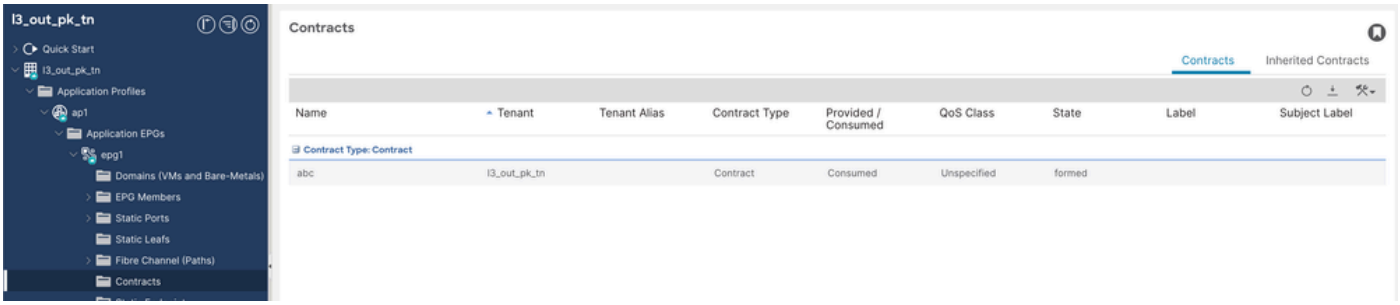
Die EPG1- und EPG2-Konfiguration wird in diesem Dokument nicht angezeigt. Sie muss konfiguriert werden, bevor die Informationen vorliegen, und der Endpunkt muss gelernt werden.

1. Validieren Sie EPG1 haș Endpunkt X.1.1.10 gelernt (Knoten 101).



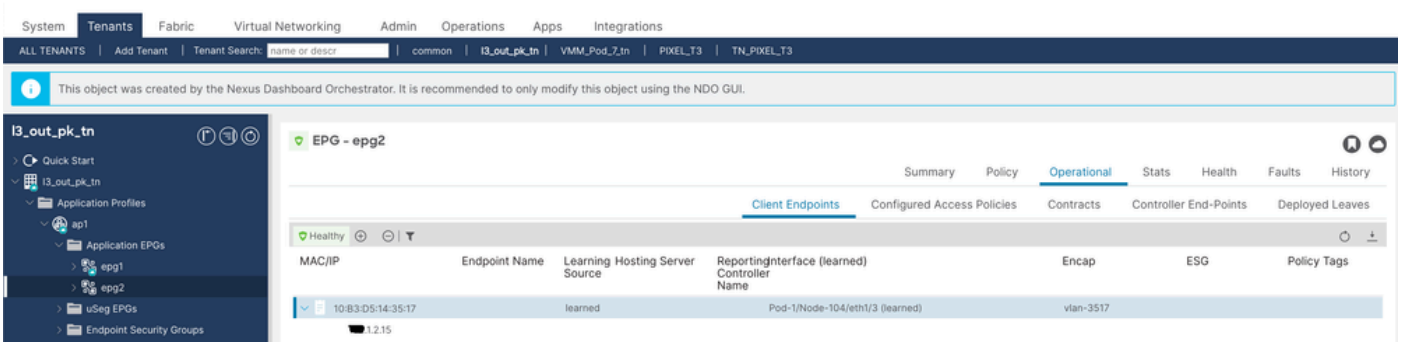
Client-Endgeräte

2. Vertrag abc wird von EPG1 verbraucht.



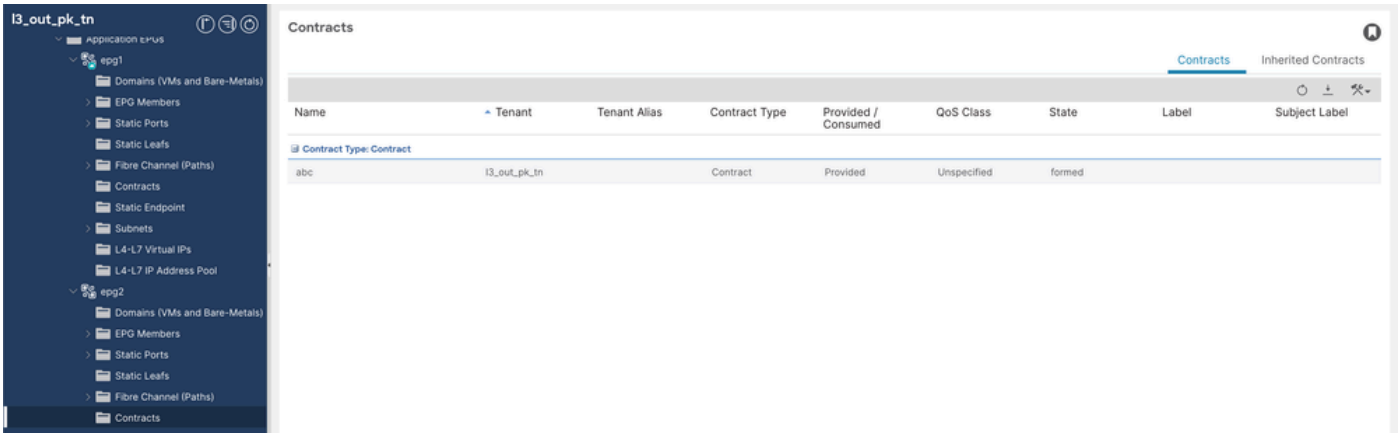
Konsumierter Vertrag

3. Validierung von EPG2 hat Endpunkt X.1.2.15gelernt (Node 104).



Client-Endpunkt

4. Vertrag abc wird von EPG2 zur Verfügung gestellt.



Warum ist ein L2-Servicediagramm für die ACI erforderlich?

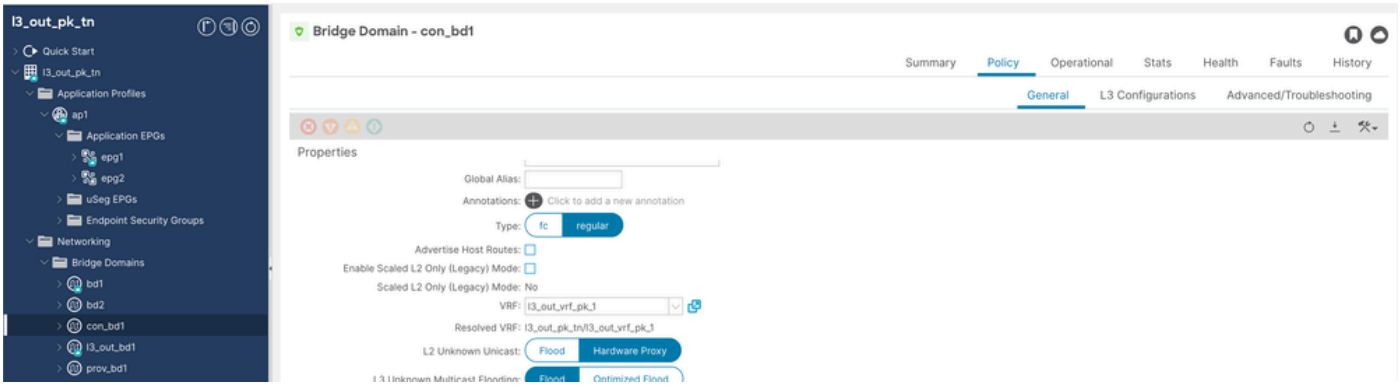
- In der Cisco ACI können L4-L7-Service-Geräte auf Layer 3 (L3), Layer 2 (L2) oder Layer 1 (L1) eingefügt werden.
- Layer-3-Serviceeinfügung: Das externe Gerät (z. B. die Firewall, das Intrusion Prevention System (IPS)) trifft Routing-Entscheidungen und leitet den Datenverkehr basierend auf IP-Adressen weiter.
- Layer-2-Serviceeinfügung: Der Datenverkehr wird basierend auf MAC-Adressen ohne Routing-Beteiligung weitergeleitet. Dies ist für transparente Firewalls oder IPS-Geräte nützlich.
- L2 Policy-Based Routing (PBR) wird beim Einfügen eines L2-Service-Geräts, z. B. eines IPS oder einer transparenten Firewall in der ACI, verwendet.
- Der Weiterleitungsmechanismus für Datenverkehr bleibt für L3- und L2-PBR unverändert.
- Der Hauptunterschied:
    - L3-PBR: Der Datenverkehr wird an eine IP-Adresse umgeleitet (das Gerät ist am Routing beteiligt).
    - L2-PBR: Der Datenverkehr wird an eine MAC-Adresse umgeleitet (Gerät arbeitet auf Layer 2).
- In L2 PBR werden MAC-Adressen statisch an Leaf-Schnittstellen gebunden, um eine ordnungsgemäße Weiterleitung des Datenverkehrs sicherzustellen.

Weitere Informationen zu den Anwendungsfällen für Active/Stanby- oder Active/Active L1/L2-PBR finden Sie im PBR-Whitepaper.

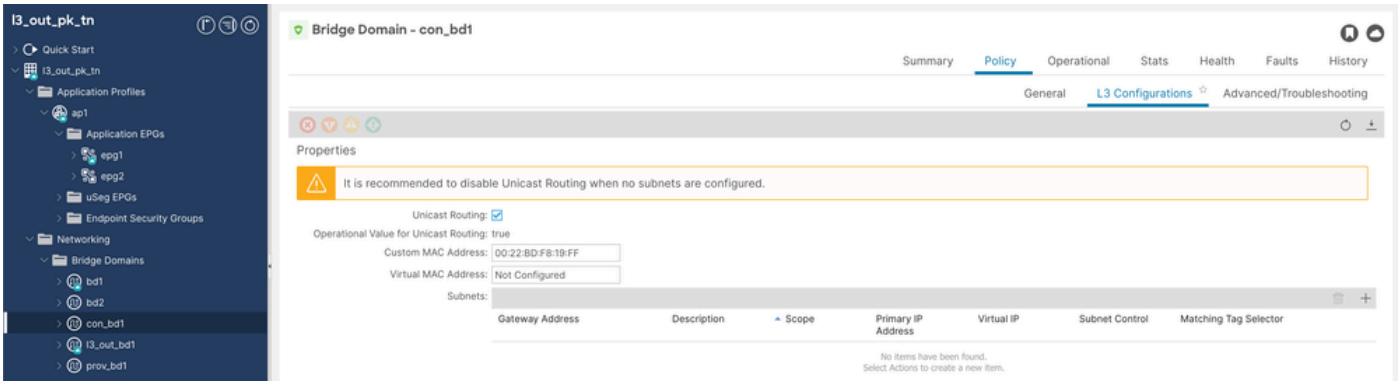
Konfiguration für L2-Servicediagramm

Schritt 1: Konfigurieren Sie das Consumer-BD mit dem Namen con-bd1.

Unicast-Routing muss aktiviert werden, L2 Unicast muss auf Hardware-Proxy festgelegt werden, und für con- und prov-Bridge-Domänen (BDs) ist kein Subnetz erforderlich.

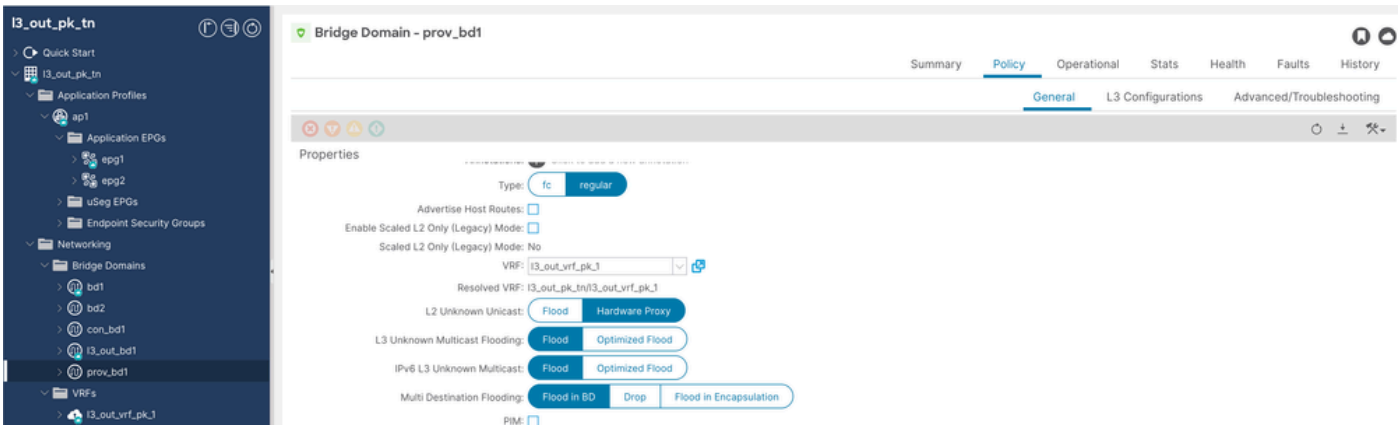


Konfig. BD-Konfiguration

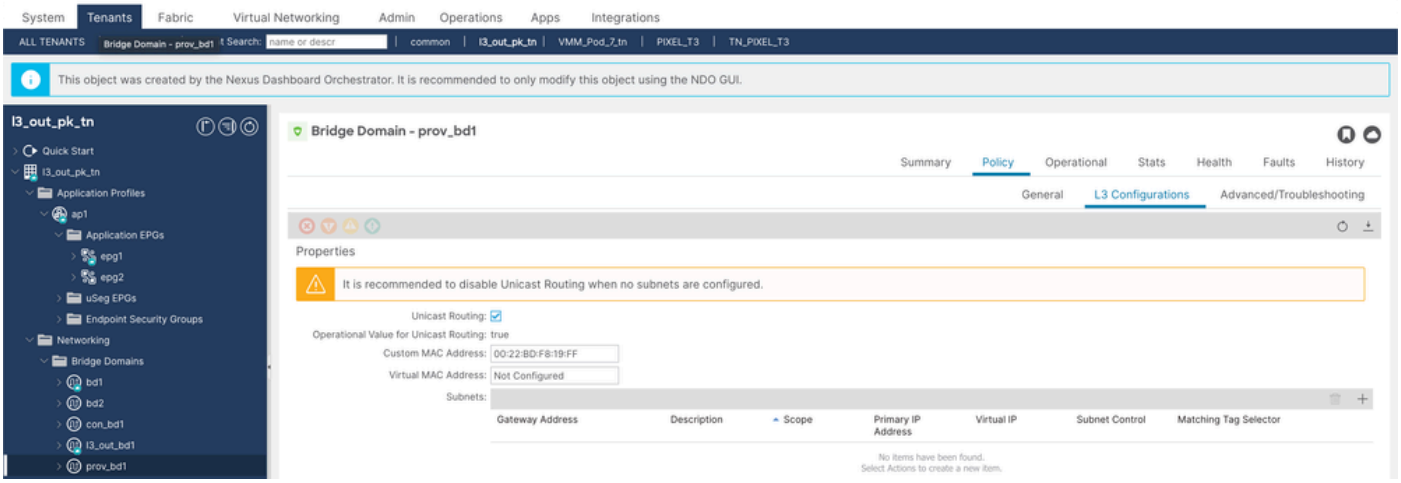


Konfig. BD-Konfig. 2

Schritt 2: Konfigurieren Sie den Anbieter bd mit dem Namen prov-bd1.



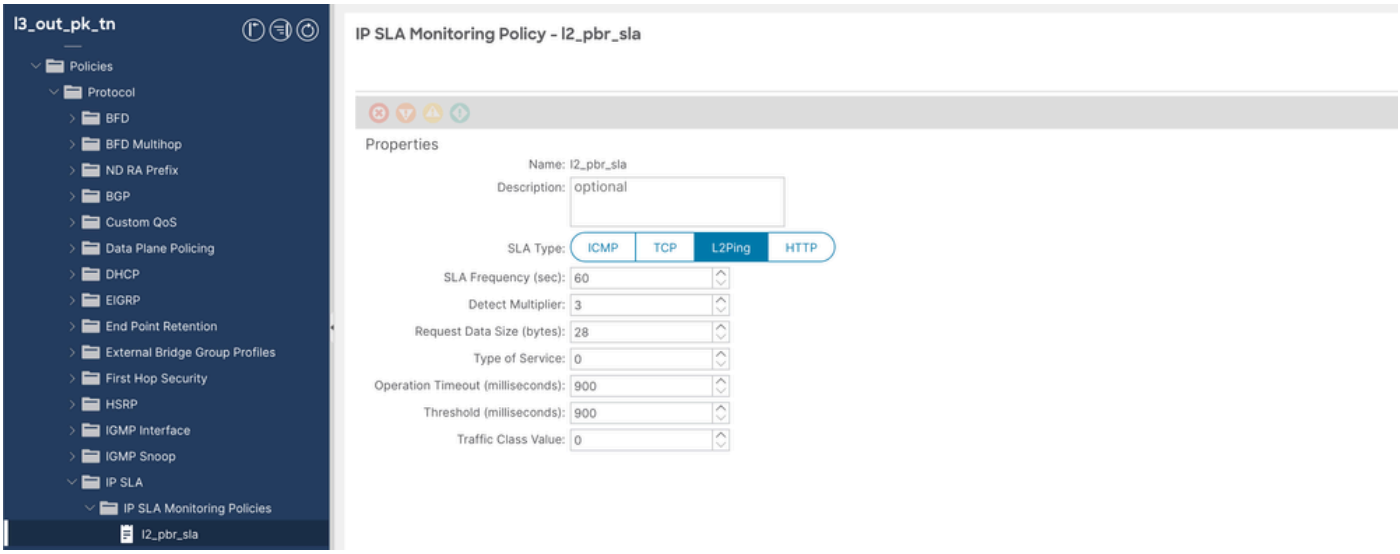
Bewährte BD-Konfiguration



Prov. BD-Konfig. 2

Schritt 3: Konfigurieren der IP Service Level Agreement (SLA)-Richtlinie mit dem SLA-Typ "L2Ping"

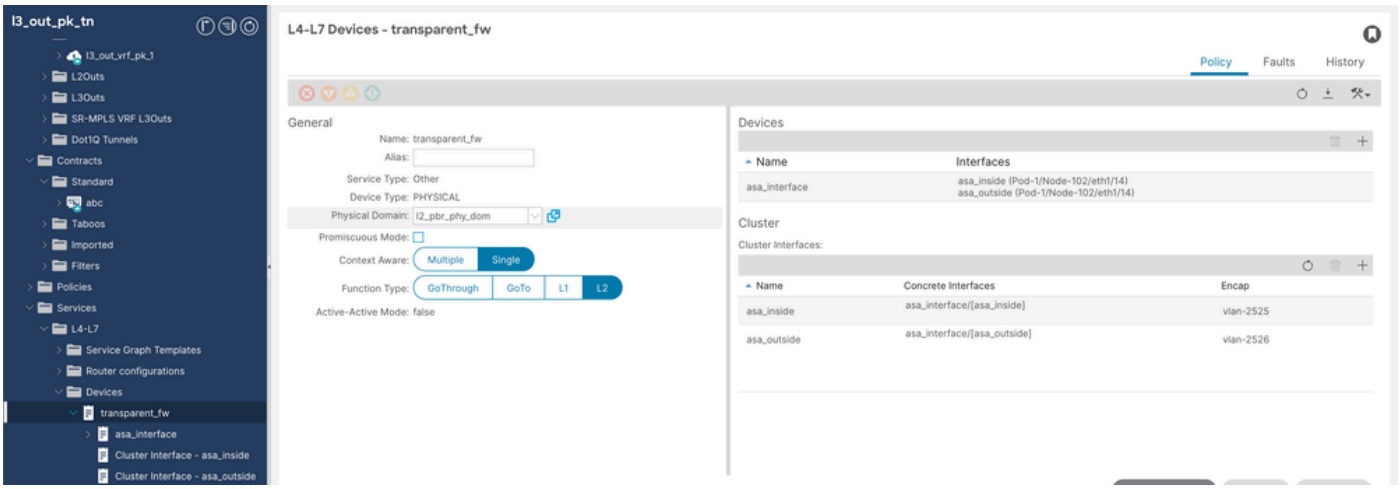
Navigieren Sie zu Tenant > Policies > Protocol > IP SLA > IP SLA Monitoring Policies, und klicken Sie dann mit der rechten Maustaste, und erstellen Sie eine Richtlinie.



IP SLA-Richtlinie

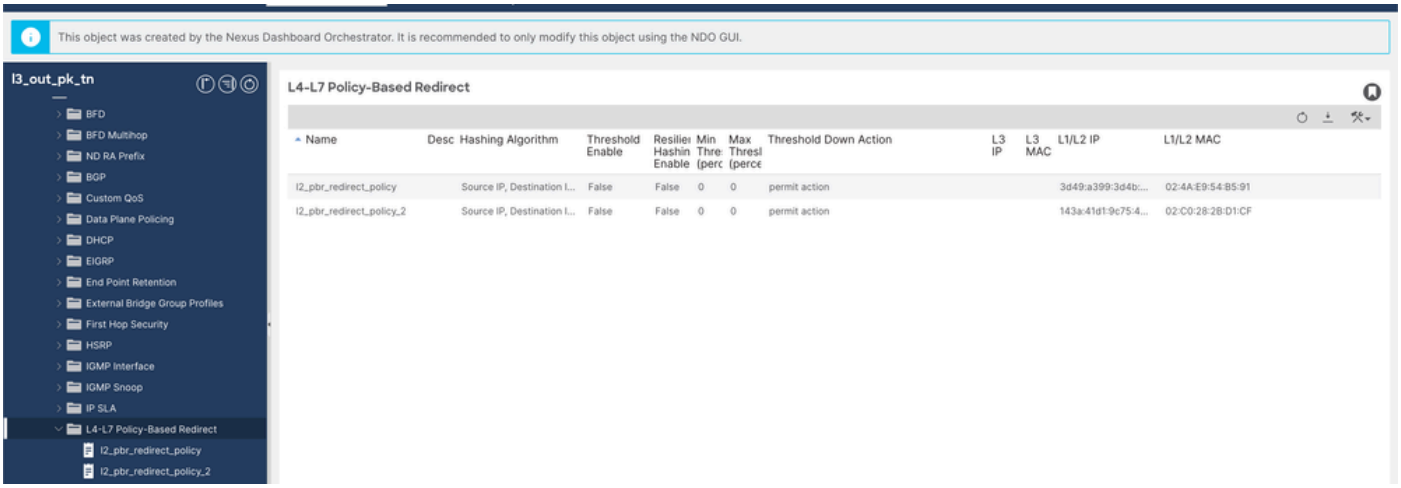
Schritt 4: Konfigurieren des L4-/L7-Geräts

Navigieren Sie zu Tenant > Services > Devices, klicken Sie mit der rechten Maustaste, und erstellen Sie ein L4-L7-Gerät.



L4-L7-Gerät

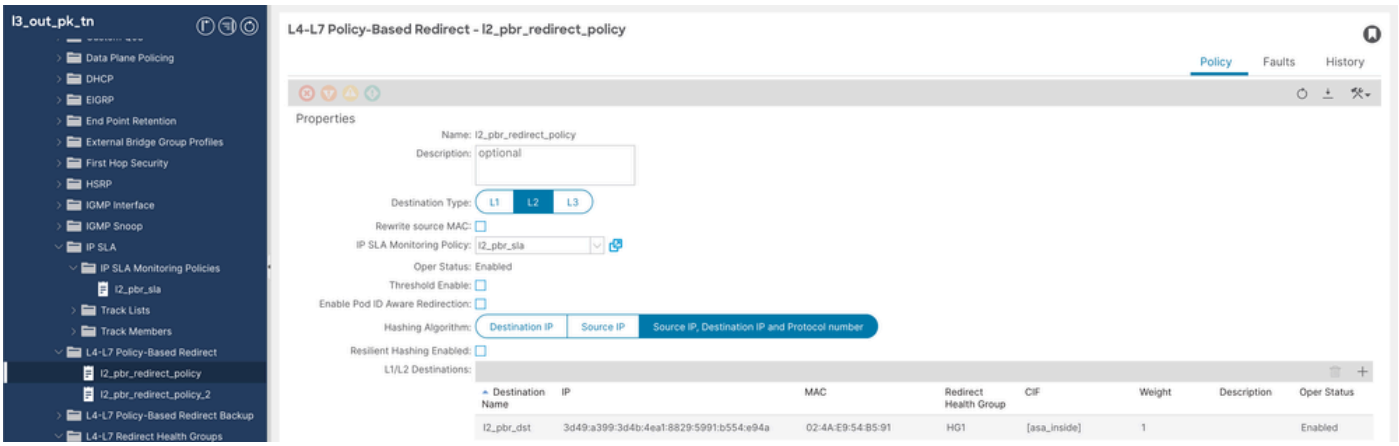
Schritt 5: Validieren der richtlinienbasierten Umleitung (Sie können dies nach der Konfiguration von 5a und 5b überprüfen).



L4-L7-Umleitungsrichtlinie

Schritt 5.1. Konfigurieren Sie eine auf L4-L7-Richtlinien basierende Umleitungsrichtlinie für die ASA (Adaptive Security Appliance) innerhalb der Schnittstelle (keine Angabe von MAC oder IP erforderlich, wird vom APIC selbst übernommen).

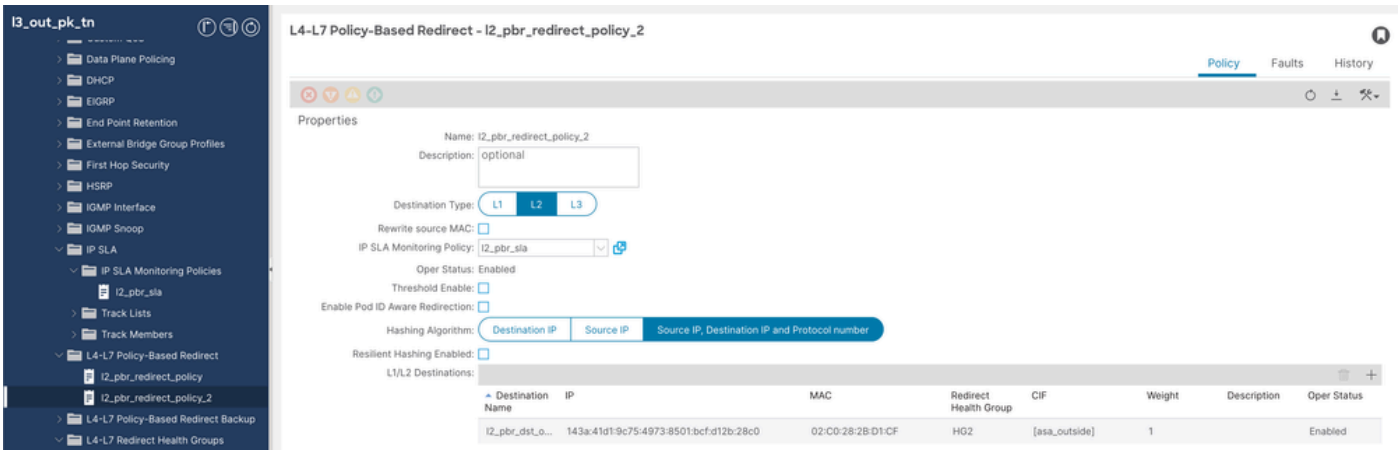
Navigieren Sie zu Tenant > Policies > Protocol > L4-L7 Policy based redirect, klicken Sie dann mit der rechten Maustaste, und erstellen Sie eine Richtlinie.



Richtlinienkonfiguration für L4-L7-Umleitung

Schritt 5.2. Konfigurieren Sie eine auf L4-L7-Richtlinien basierende Umleitungsrichtlinie für eine externe ASA-Schnittstelle (keine Angabe von MAC oder IP erforderlich, da diese vom APIC selbst ausgefüllt wird).

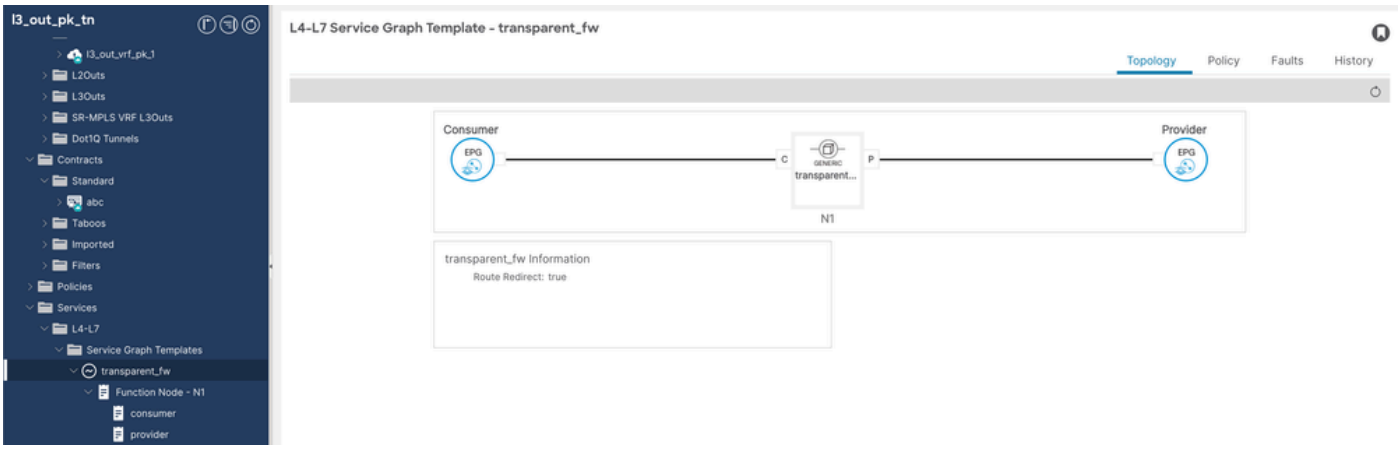
Navigieren Sie zu Tenant > Policies > Protocol > L4-L7 Policy based redirect, klicken Sie dann mit der rechten Maustaste, und erstellen Sie eine Richtlinie.



L4-L7-Umleitungsrichtlinienkonfiguration 2

Schritt 6: Konfigurieren der Servicediagrammvorlage

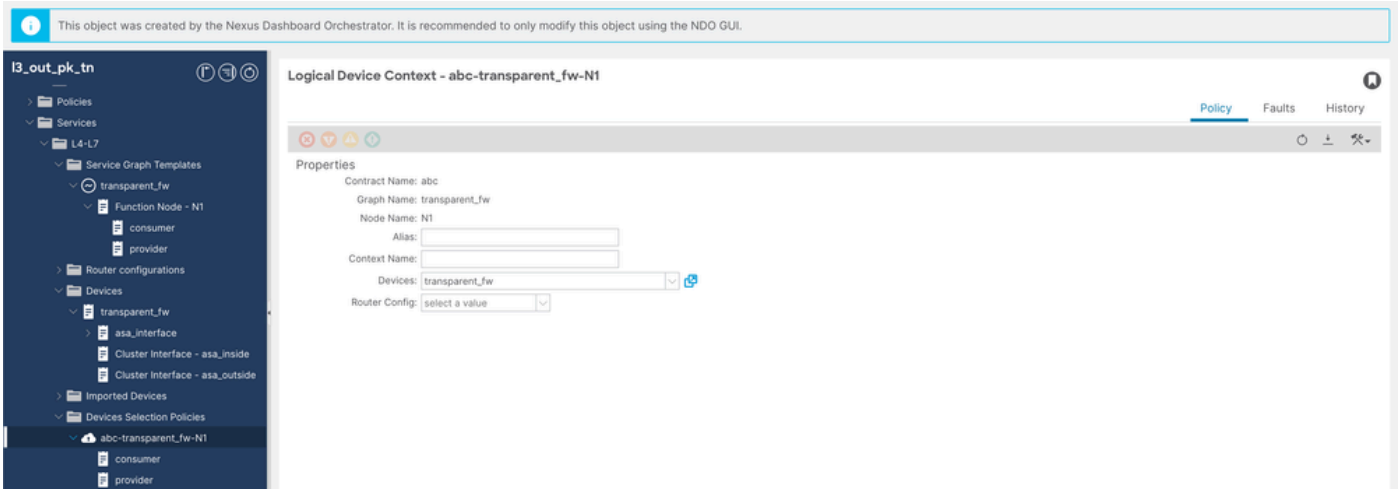
Navigieren Sie zu Tenant > Services > Service Graph Template (Servicediagrammvorlage), klicken Sie mit der rechten Maustaste, und erstellen Sie eine L4-L7-Servicediagrammvorlage.



Konfiguration des Servicediagramms

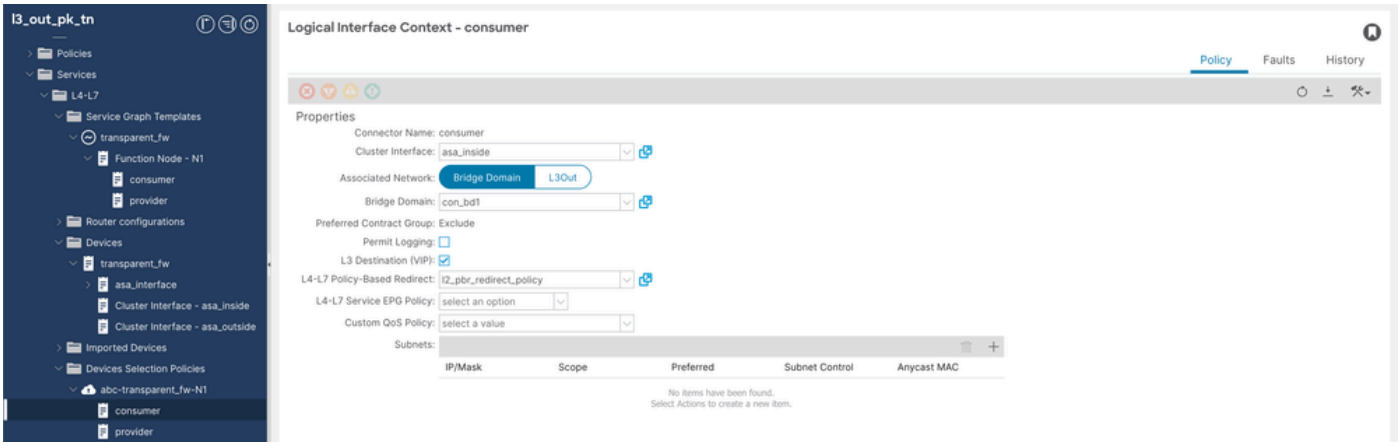
Schritt 7: Konfigurieren Sie die Richtlinie zur Geräteauswahl.

Navigieren Sie zu Tenant > Services > Device Selection Policy, und klicken Sie dann mit der rechten Maustaste, um eine Device Selection Policy zu erstellen.



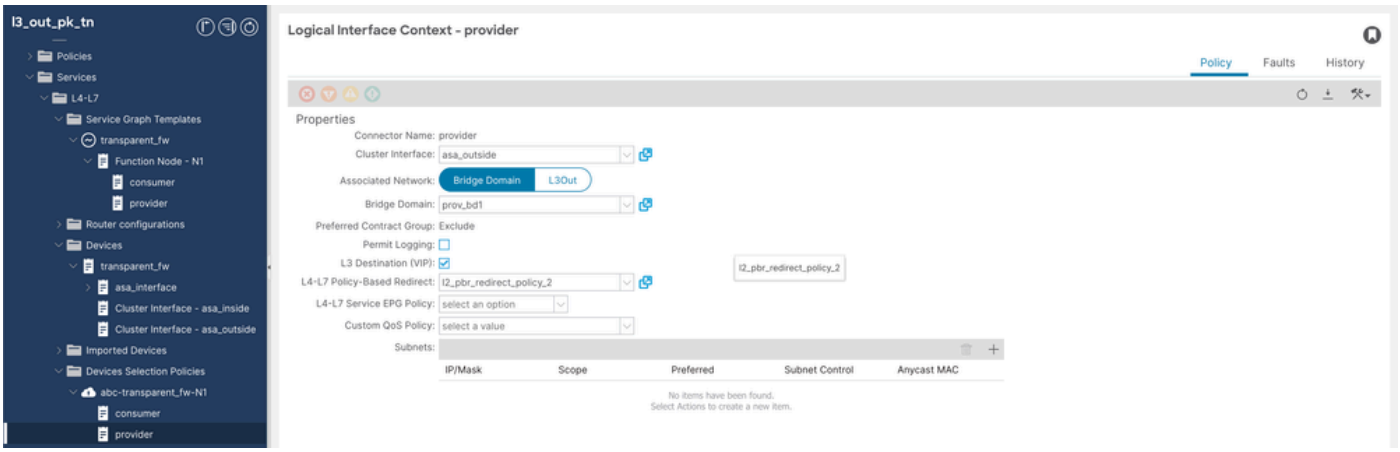
Servicediagramm Konfiguration 2

++ Kontext der logischen Benutzerschnittstelle

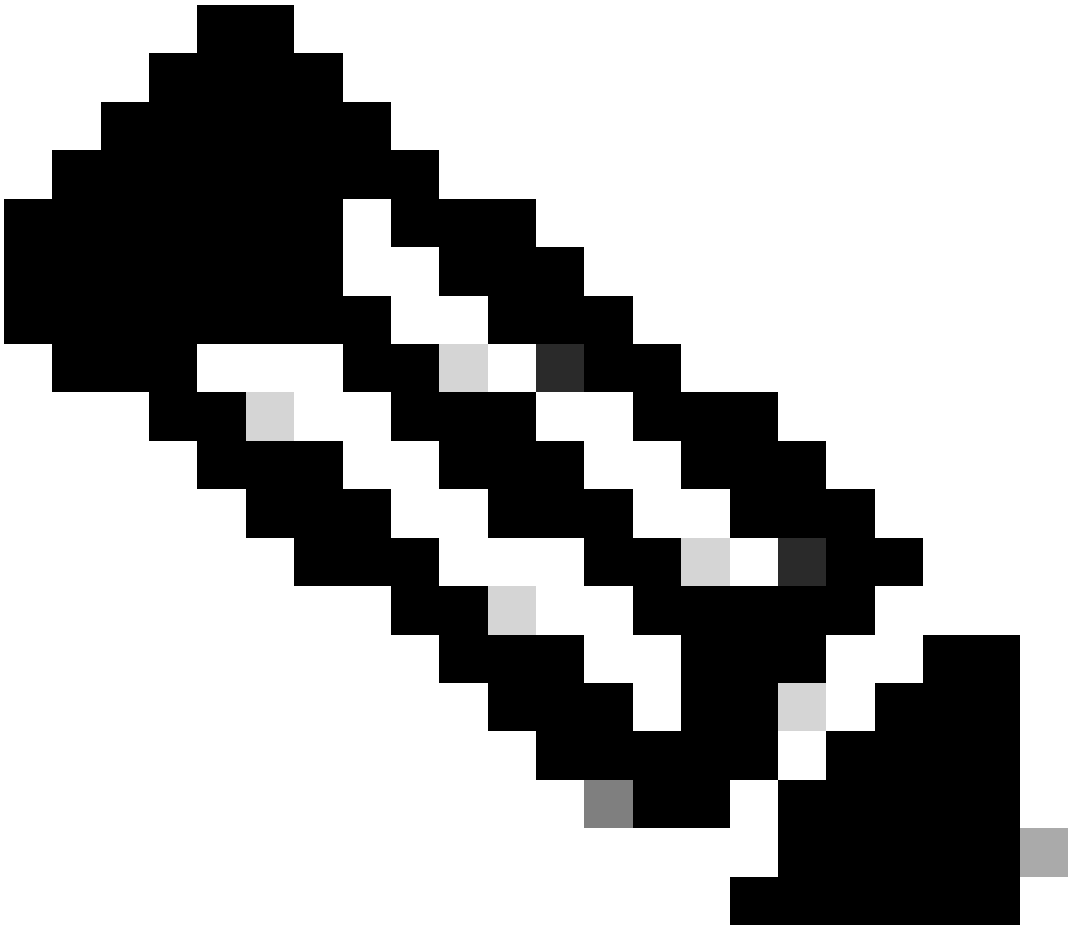


Richtlinie zur Geräteauswahl - Verbraucherkonfiguration

++ Kontext der logischen Anbieterschnittstelle



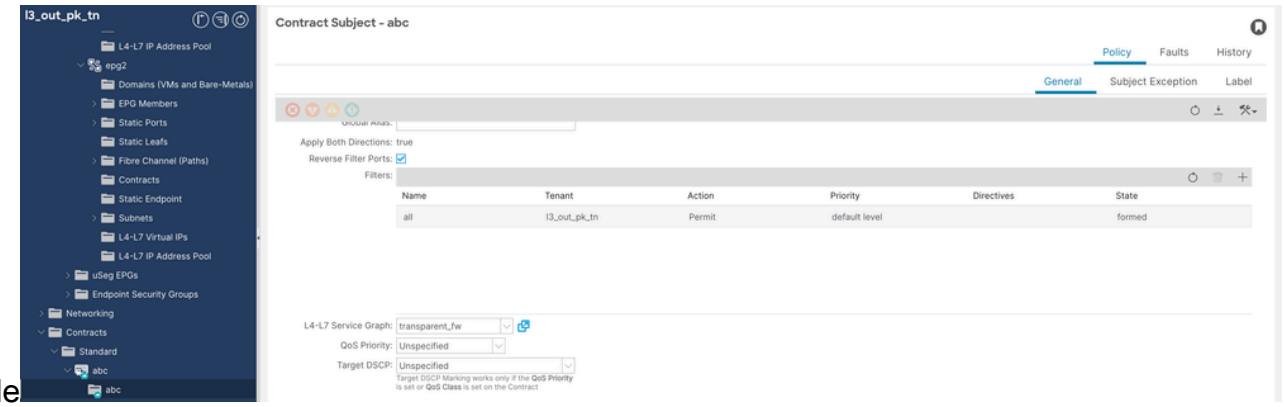
Konfiguration des Geräteauswahl-Richtlinienanbieters



Anmerkung: Richtlinie zur Geräteauswahl, falls automatisch erstellt, falls Sie die Option "Servicediagramm anwenden" verwenden möchten.

Schritt 8. Wenden Sie PBR an, um abc Betreff zu kontrahieren.

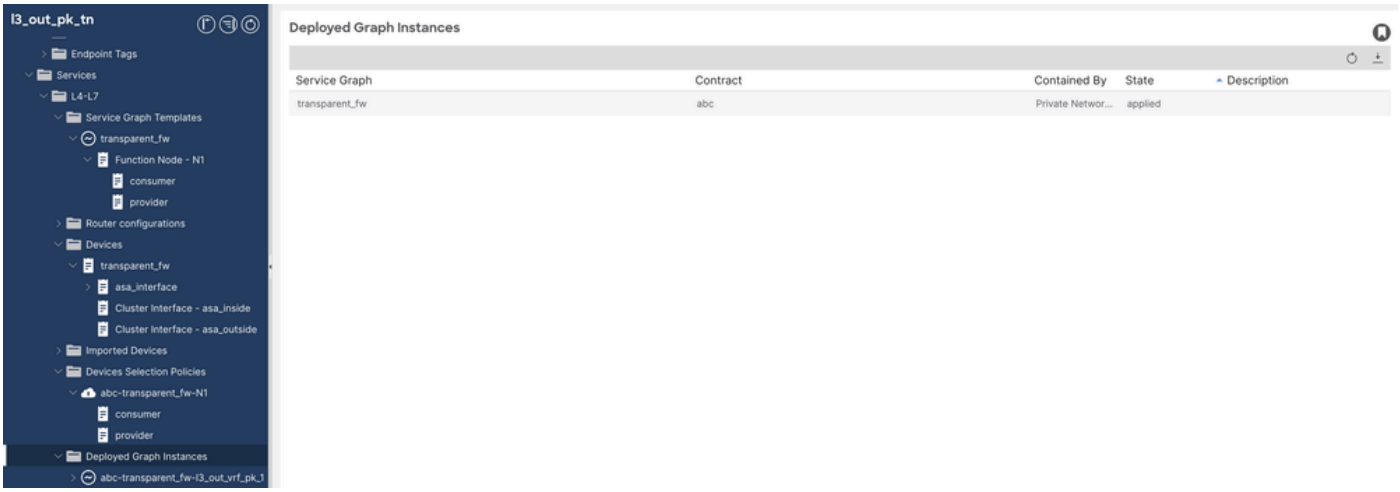
Navigieren Sie zu Tenant > Contract > Contract Subject > L4-L7 Service Graph > transparent_fw.



Nachteile

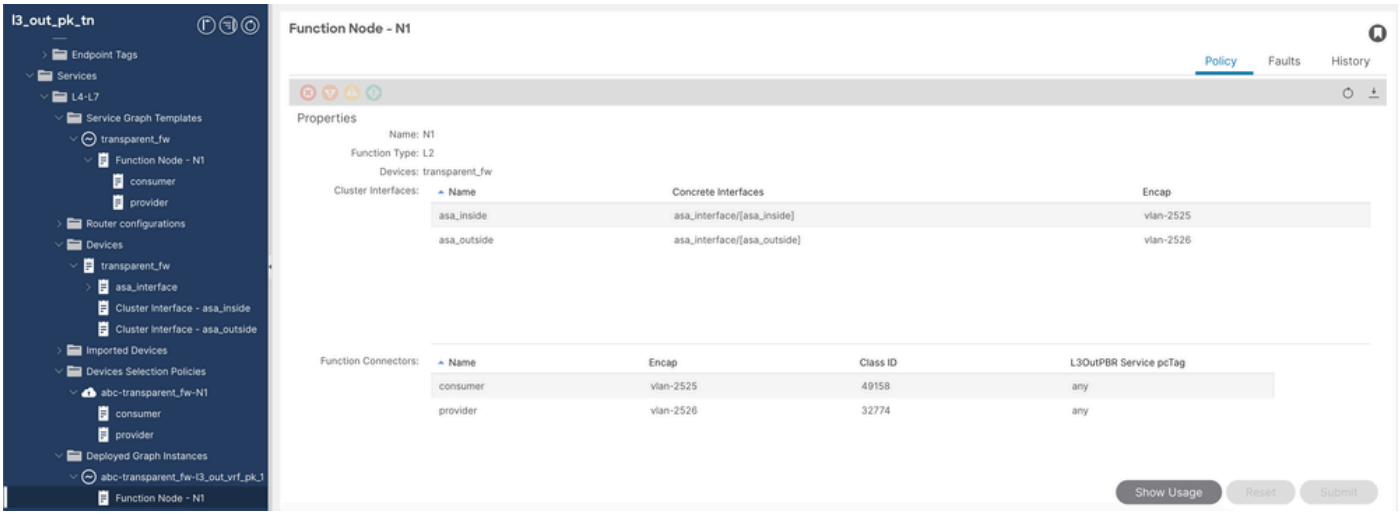
Vertragskonfiguration

Schritt 9: Wenn die Bereitstellung erfolgreich war, überprüfen Sie sie unter dem Diagramm für bereitgestellte Instanzen (nach Status suchen).



Servicediagramm-Validierung

++ Cluster-Schnittstellen, Encap-VLANs und Funktionskonnektor-Klassen-IDs überprüfen.



Servicediagramm-Validierung 2

Validierung des L2-PBR-Datenverkehrs auf der ASA

Secure Shell (SSH) vom SRC-Endpunkt zum DST-Endpunkt wird in der Tabelle "Conn" auf der ASA angezeigt.

ASA-Validierung

L2-PBR auf Leaf überprüfen

1. VLAN-Programmierung auf Leaf Node 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. Richtlinien und Zoning-Regeln auf Consumerknoten (101) und Anbieterknoten (104) umleiten.

<#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-apic1OO#
```

`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-apic1OO#
```

`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  |
```

Fehler in Fall L2Ping fehlgeschlagen

Falls L2pings auf dem PBR-Gerät fehlschlagen, stellen Sie fest, dass sich das PBR noch im Bereitstellungsstatus befindet und die Fehler F4203, F2833 und F2911 mit dem Status "track/health group" ausgefallen sind.

Erfassen von L2-Pings

Sie können L2Pings mit tcpdump auf dieser Schnittstelle erfassen, um zu erfahren, ob sie richtig gesendet und empfangen werden. Wenn Sie sehen, dass nur CPU-Übertragungen gesendet und nicht empfangen wurden, werden die oben genannten Fehler erwartet, und Sie müssen auf ASA weiter beheben, warum sie verworfen wurden (weitere Informationen finden Sie im ASA-Konfigurationsabschnitt).

<#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

Datenverkehrsfluss vom SRC zum Ziel-Endpunkt

<#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 |  T
================================================================================================================
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-Konfiguration

Schritt 1: Schnittstellenkonfiguration.

<#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
!
```

Schritt 2: MAC-Lernen muss deaktiviert werden.

<#root>

```
ASA(config)#
```

show run mac-learn

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

PBR:

Schritt 3: Statische MAC-Adresstabelle für 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
```

Schritt 4: Konfigurieren der Zugriffskontrollliste (ACL) zum Übergeben von L2pings

<#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
```

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.