ASAv로 레이어 2 서비스 그래프 컨피그레이션 구성 및 확인

목차

소개

이 문서에서는 Cisco ACI(Application Centric Infrastructure)에서 레이어 2 서비스 그래프 컨피그레이션을 구성하고 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ACI에서 레이어 3 서비스 그래프가 작동하는 방식 이해
- ACI에서 엔드포인트 정책 그룹, 브리지 도메인 및 계약을 구성하는 방법에 대한 이해
- (Adaptive Security Applicance Virtual) ASAv를 투명 방화벽으로 구성하는 방법 이해

사용되는 구성 요소

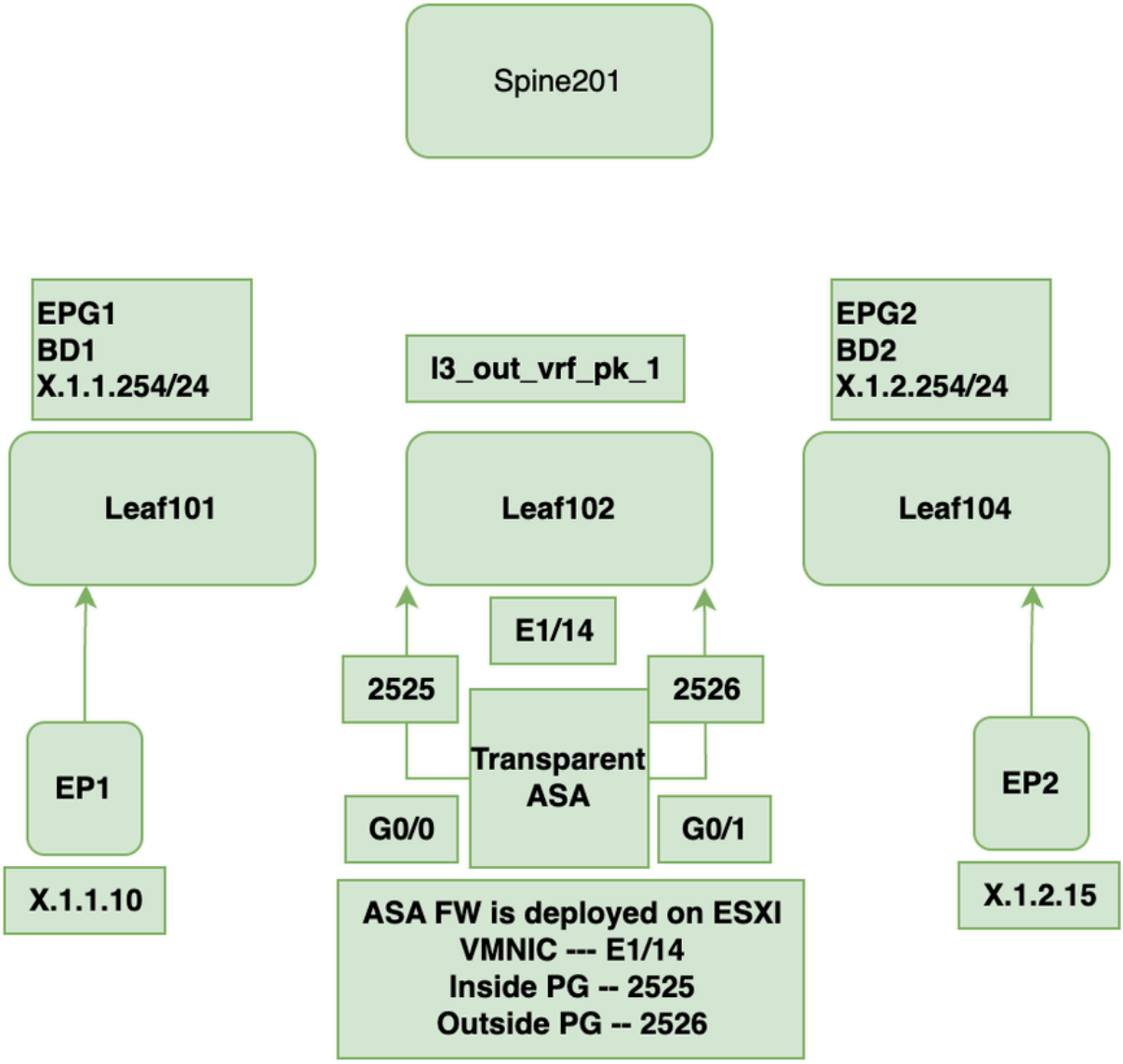
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- APIC 버전: 6.0(3g)
- 리프 하드웨어: N9K-C93180YC-FX
- 리프 소프트웨어: n9000-16.0(3g)
- 리프 노드 101, 102, 103

- ESXi 서버에 ASAv 구축

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

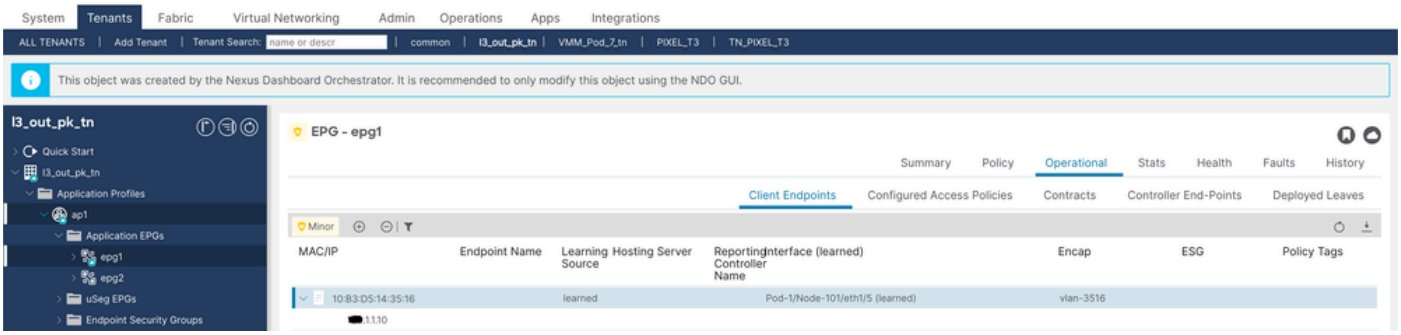
토폴로지



토폴로지

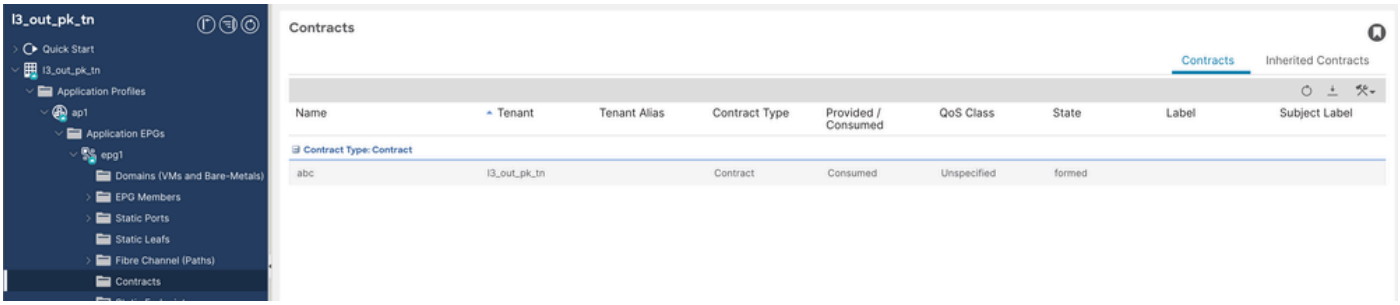
EPG1 및 EPG2 컨피그레이션은 이 문서에 나와 있지 않으며, 핸드와 엔드포인트를 학습하기 전에 구성해야 합니다.

1. 엔드포인트 X.1.1.10$을 학습한 EPG1을 확인합니다(노드 101).



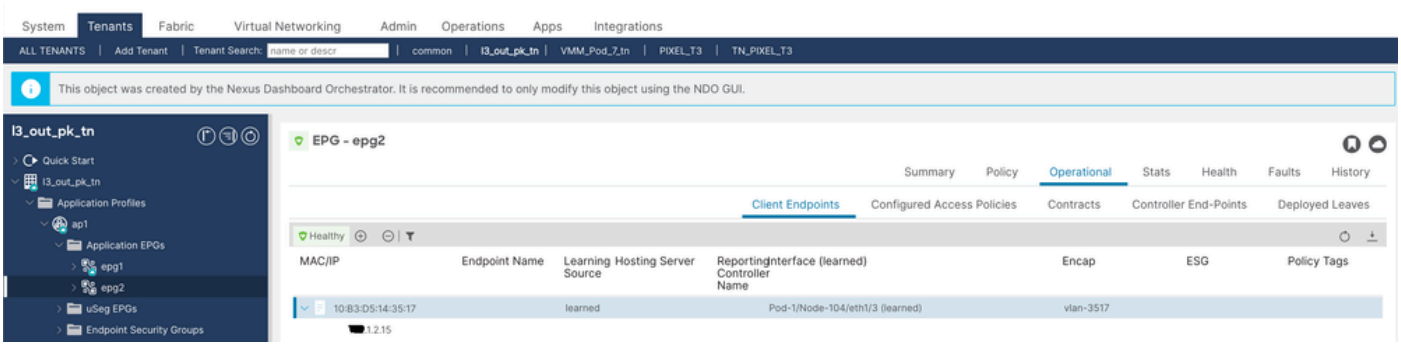
클라이언트 엔드포인트

2. 계약 abc는 EPG1에서 소비됩니다.



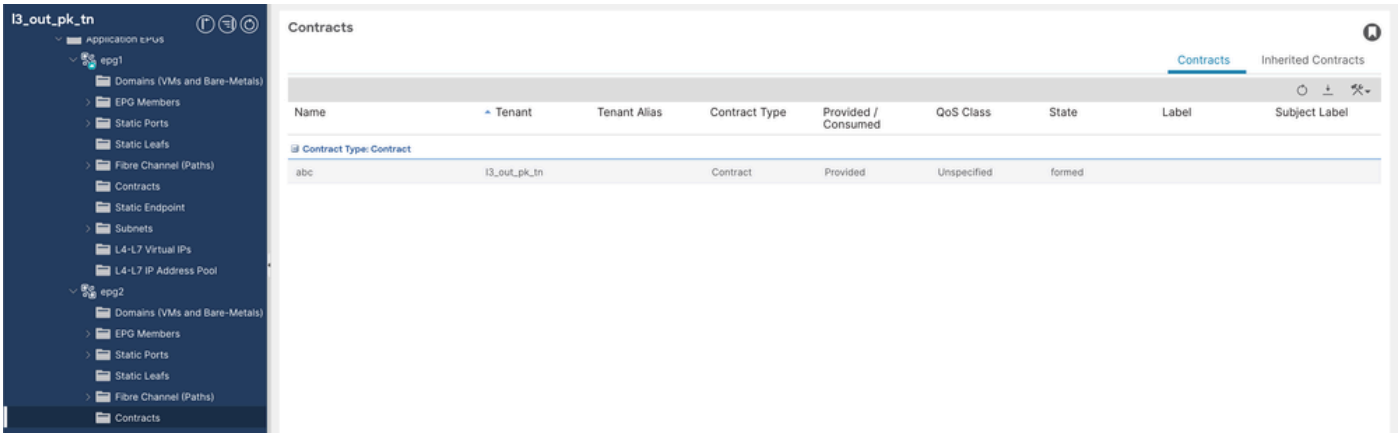
사용된 계약

3. EPG2에 엔드포인트 X.1.2.15가 있는지 확인합니다.학습되었습니다(노드 104).



클라이언트 엔드포인트

4. 계약 abc는 EPG2에서 제공됩니다.



ACI에서 L2 서비스 그래프가 필요한 이유

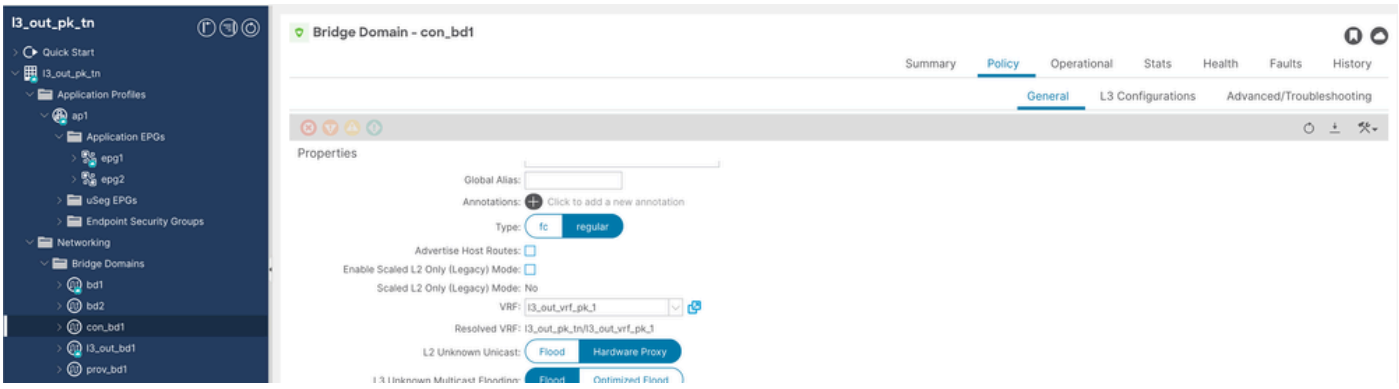
- Cisco ACI에서는 L4-L7 서비스 장치를 L3(Layer 3), L2(Layer 2) 또는 L1(Layer 1)에 삽입할 수 있습니다.
- 레이어 3 서비스 삽입: 외부 디바이스(예: 방화벽, IPS(Intrusion Prevention System))는 라우팅 결정을 내리고 IP 주소를 기반으로 트래픽을 전달합니다.
- 레이어 2 서비스 삽입: 트래픽은 라우팅 개입 없이 MAC 주소를 기반으로 전달됩니다. 이는 투명한 방화벽 또는 IPS 디바이스에 유용합니다.
- L2 PBR(Policy-Based Routing)은 ACI에서 IPS 또는 투명 방화벽과 같은 L2 서비스 디바이스를 삽입할 때 사용됩니다.
- 트래픽 포워딩 메커니즘은 L3 및 L2 PBR 모두에 대해 동일하게 유지됩니다.
- 주요 차이점은 다음과 같습니다.
  - L3 PBR: 트래픽이 IP 주소로 리디렉션됩니다(디바이스가 라우팅에 참여함).
  - L2 PBR: 트래픽이 MAC 주소로 리디렉션됩니다(디바이스는 레이어 2에서 작동).
- L2 PBR에서 MAC 주소는 적절한 트래픽 포워딩을 보장하기 위해 리프 인터페이스에 정적으로 바인딩됩니다.

액티브/스탠바이 또는 액티브/액티브 L1/L2 PBR 활용 사례에 대한 자세한 내용은 PBR 백서를 참조하십시오.

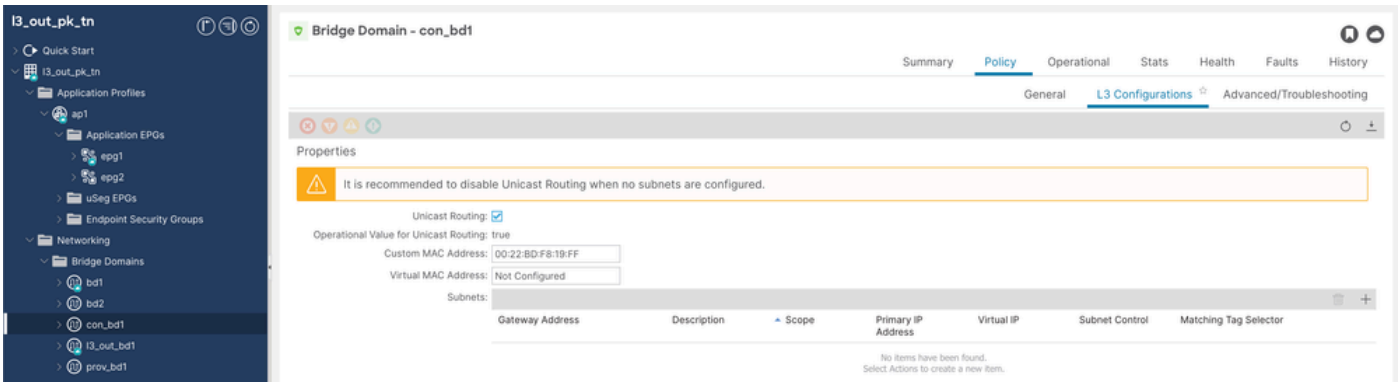
L2 서비스 그래프 컨피그레이션

1단계. consumer bd를 con-bd1로 구성합니다.

유니캐스트 라우팅을 활성화해야 하며, L2 알 수 없는 유니캐스트는 하드웨어 프록시로 설정되어야 하며, con 및 prov BD(Bridge Domain)에는 서브넷이 필요하지 않습니다.

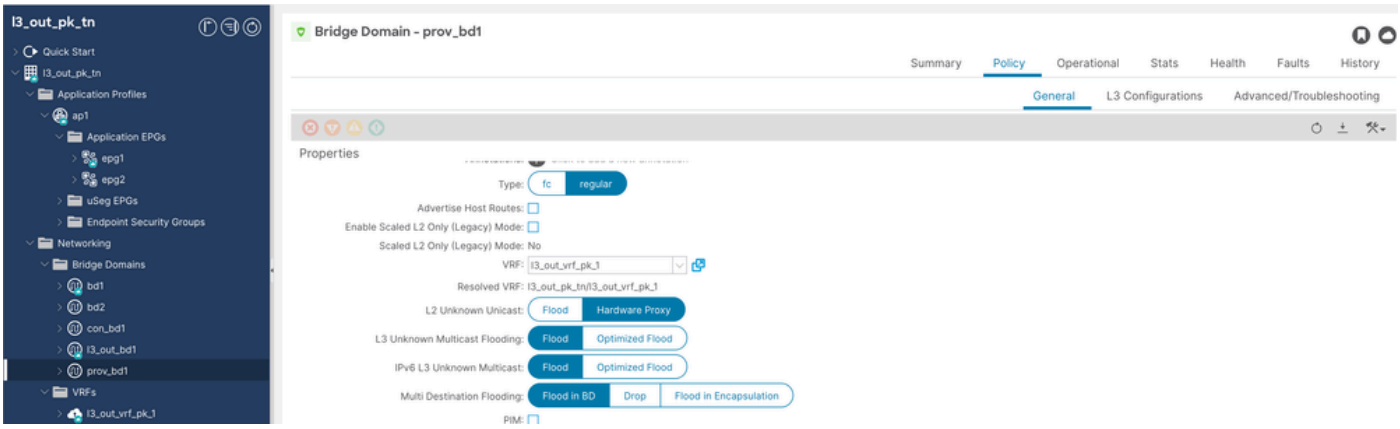


반대 BD 컨피그레이션

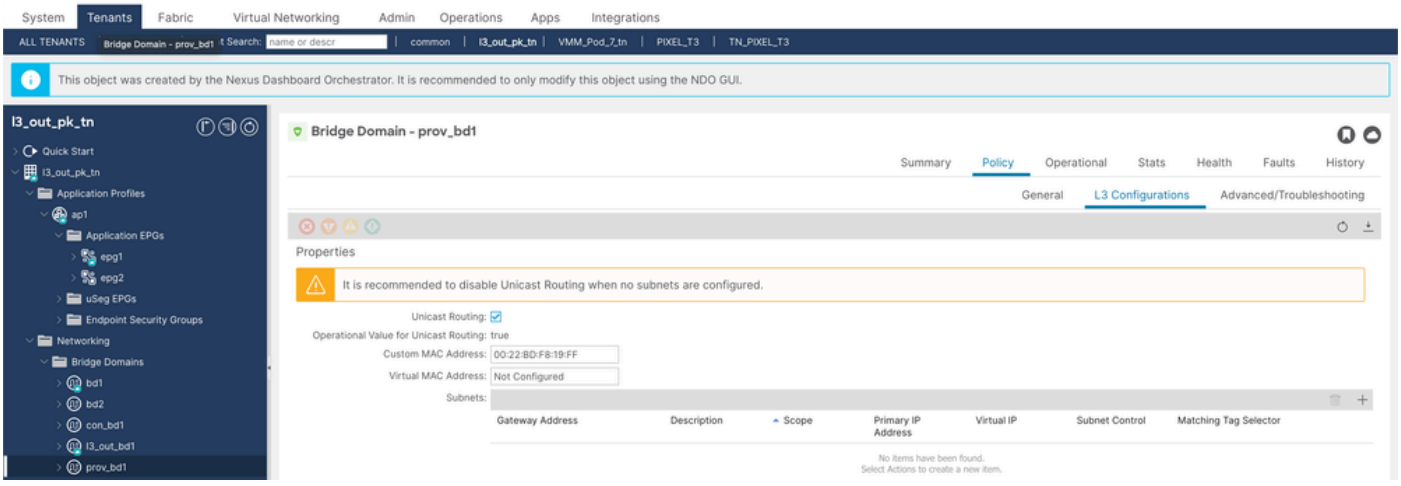


반대 BD 컨피그레이션 2

2단계. prov-bd1이라는 공급자 bd를 구성합니다.



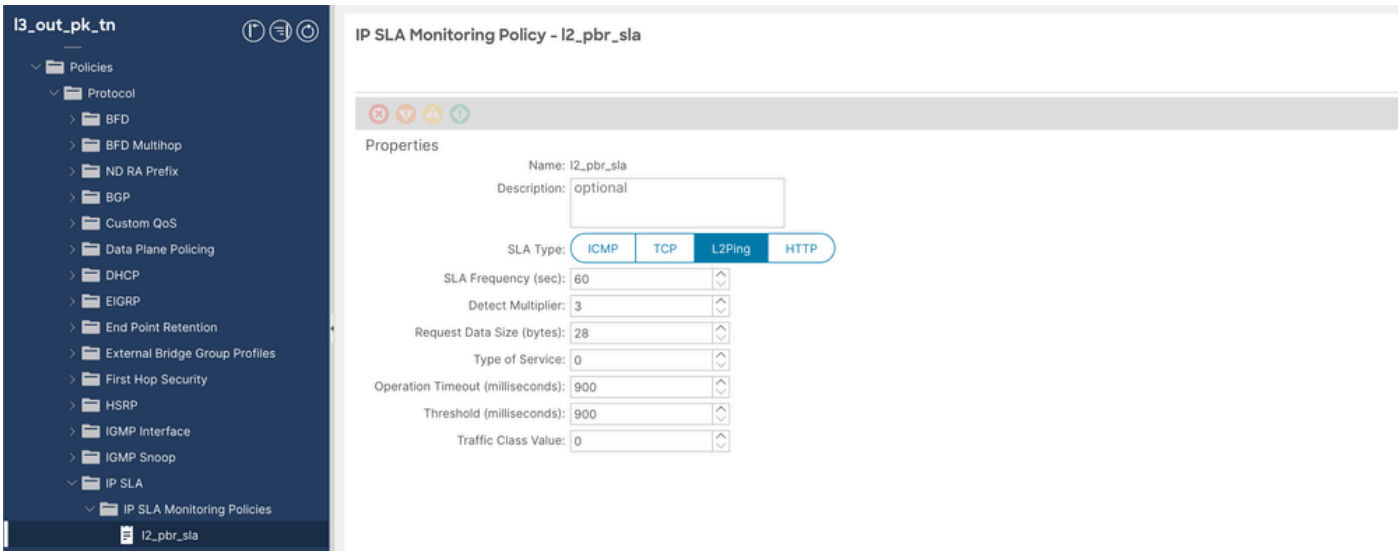
Prov BD 컨피그레이션



Prov BD 컨피그레이션 2

3단계. SLA 유형 L2Ping을 사용하여 IP SLA(서비스 수준 계약) 정책을 구성합니다.

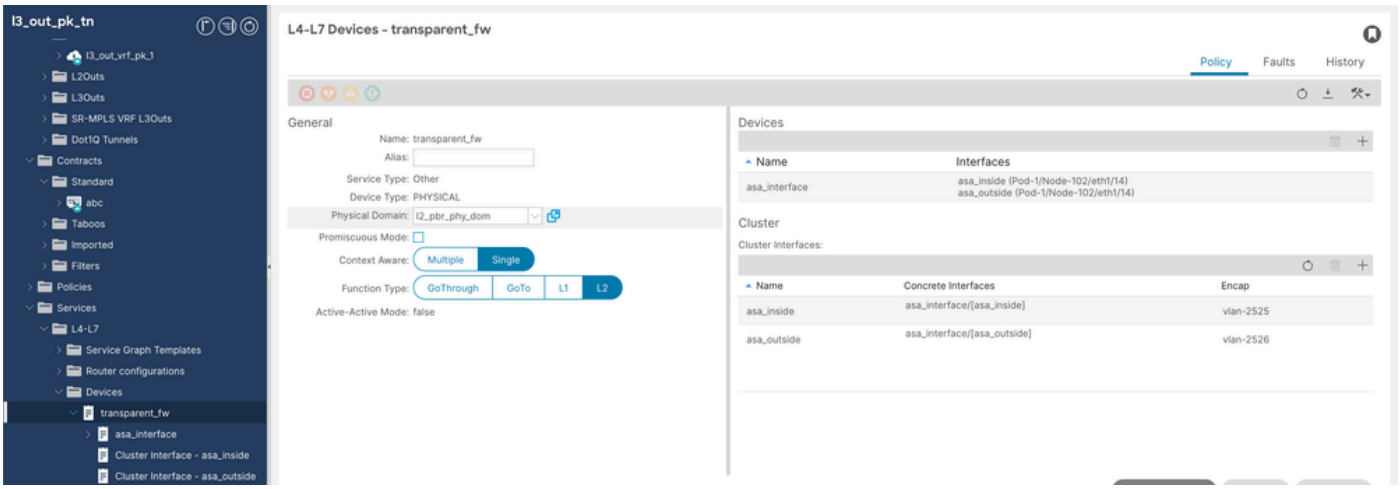
Tenant(테넌트) > Policies(정책) > Protocol(프로토콜) > IP SLA > IP SLA Monitoring Policies(IP SLA 모니터링 정책)로 이동한 다음 마우스 오른쪽 버튼을 클릭하고 policy를 생성합니다.



IP SLA 정책

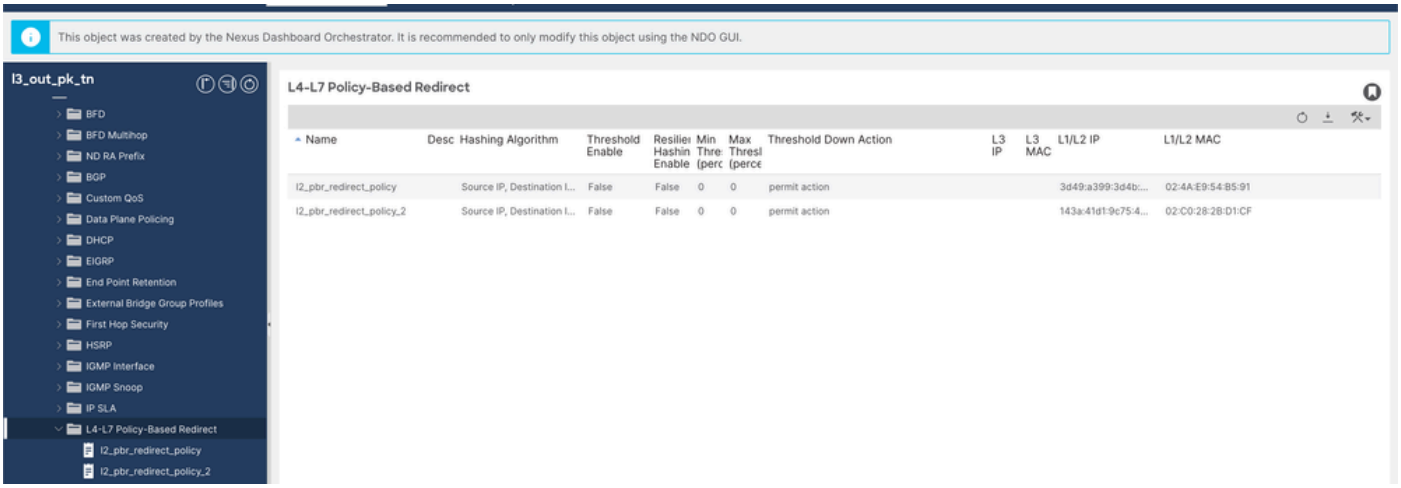
4단계. L4/L7 디바이스를 구성합니다.

Tenant(테넌트) > Services(서비스) > Devices(디바이스)로 이동한 다음 마우스 오른쪽 버튼을 클릭하고 L4-L7 디바이스를 생성합니다.



L4-L7 디바이스

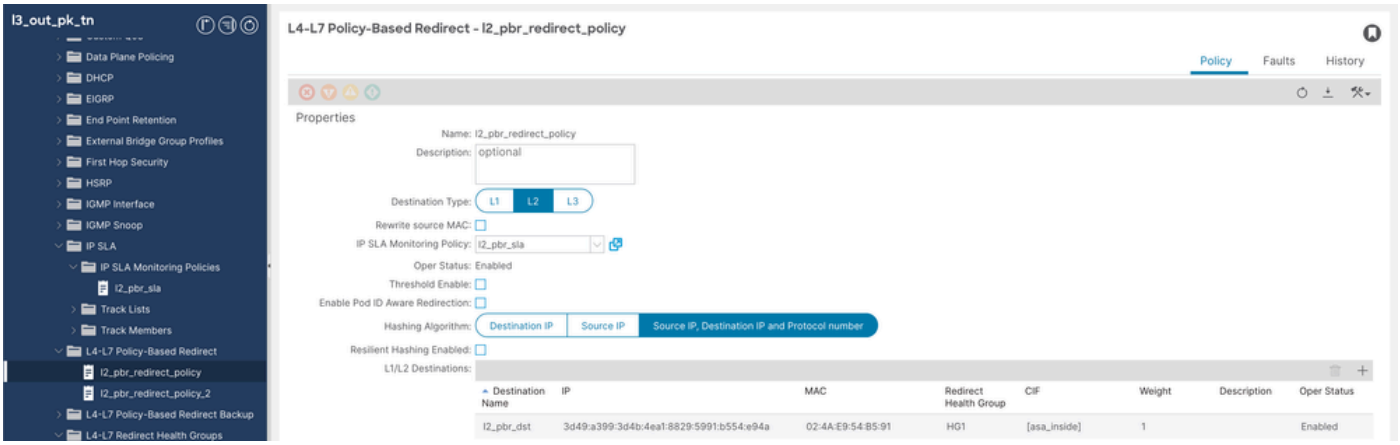
5단계. 정책 기반 리디렉션 개요 확인(5a 및 5b 구성 후 확인 가능)



L4-L7 리디렉션 정책

5.1단계. ASA(Adaptive Security Appliance) 내부 인터페이스에 대한 L4-L7 정책 기반 리디렉션 정책을 구성합니다(MAC 또는 IP를 지정할 필요가 없으며 APIC 자체로 채워짐).

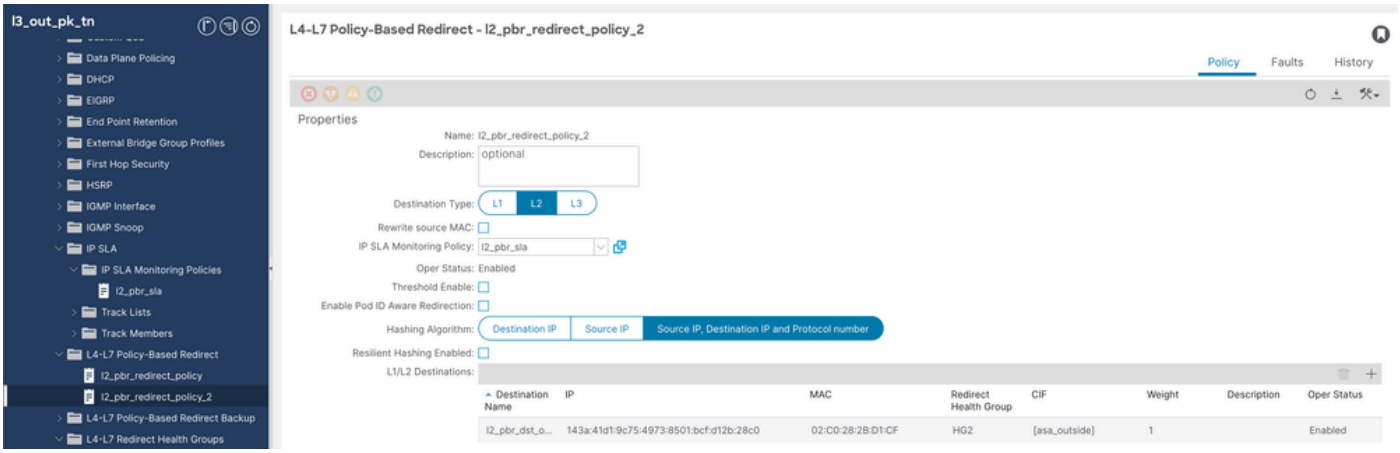
Tenant(테넌트) > Policies(정책) > Protocol(프로토콜) > L4-L7 Policy based redirect(L4-L7 정책 기반 리디렉션)로 이동한 다음 마우스 오른쪽 버튼을 클릭하고 policy를 생성합니다.



L4-L7 리디렉션 정책 구성

5.2단계. ASA 외부 인터페이스에 대한 L4-L7 정책 기반 리디렉션 정책을 구성합니다(MAC 또는 IP를 지정할 필요 없음, APIC 자체로 채워짐).

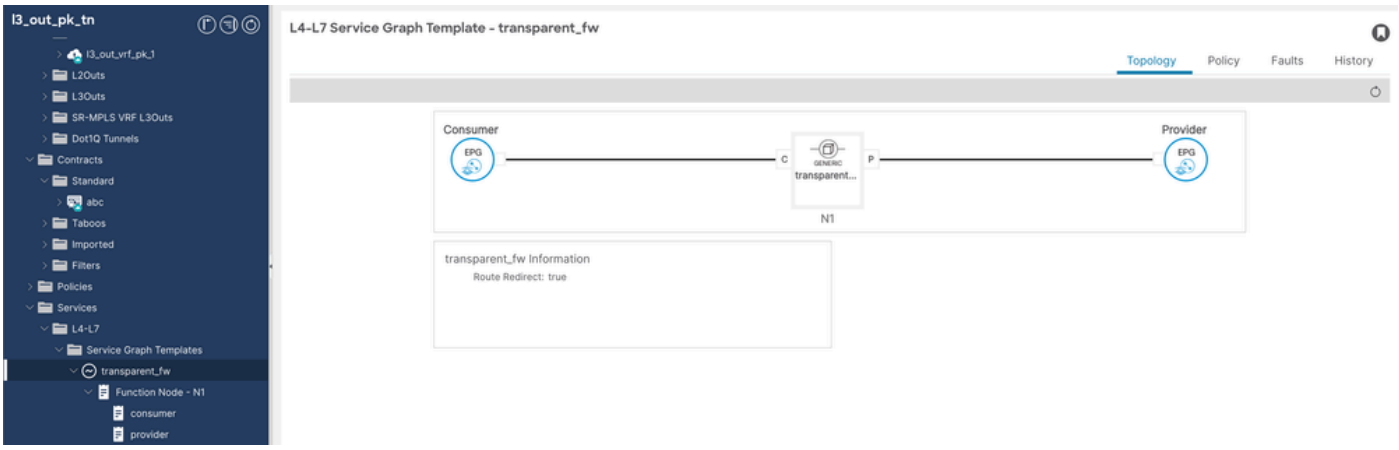
Tenant(테넌트) > Policies(정책) > Protocol(프로토콜) > L4-L7 Policy based redirect(L4-L7 정책 기반 리디렉션)로 이동한 다음 마우스 오른쪽 버튼을 클릭하고 policy를 생성합니다.



L4-L7 리디렉션 정책 컨피그레이션 2

6단계. 서비스 그래프 템플릿을 구성합니다.

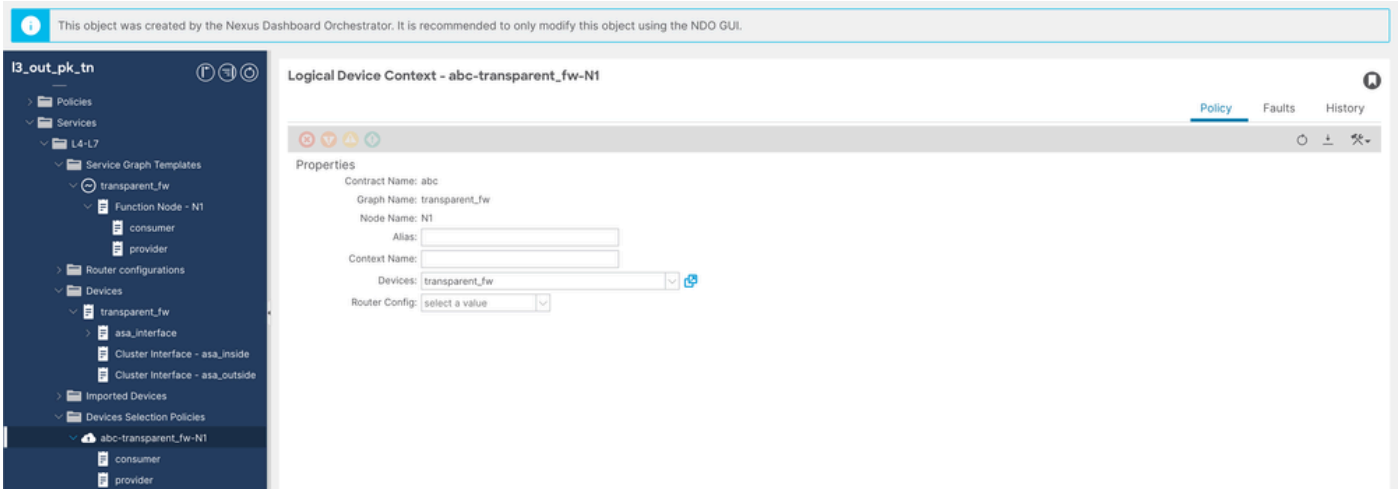
Tenant(테넌트) > Services(서비스) > Service Graph Template(서비스 그래프 템플릿)으로 이동한 다음 마우스 오른쪽 버튼을 클릭하여 L4-L7 서비스 그래프 템플릿을 생성합니다.



서비스 그래프 컨피그레이션

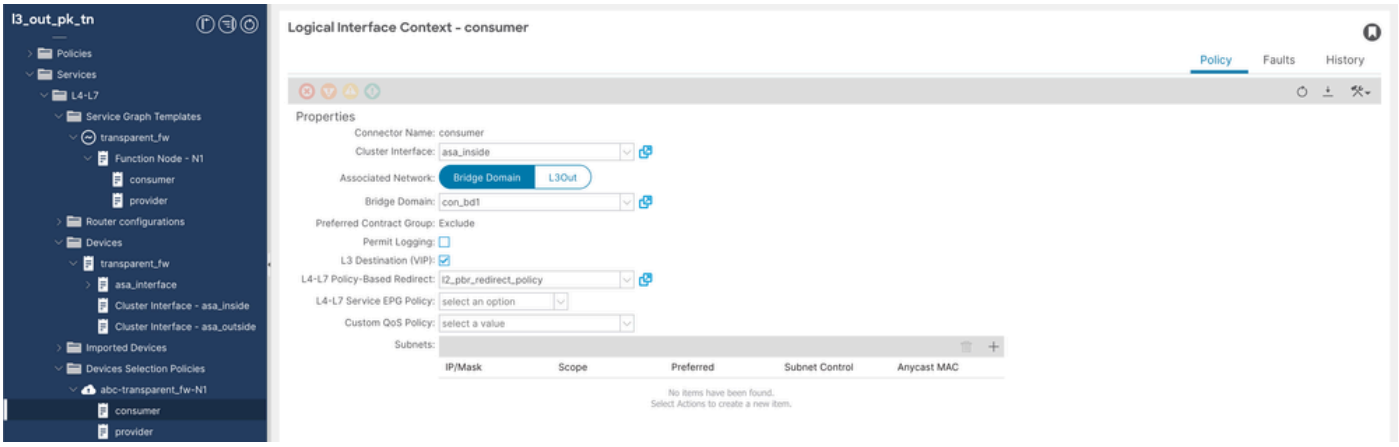
7단계. 디바이스 선택 정책을 구성합니다.

Tenant(테넌트) > Services(서비스) > Device Selection Policy(디바이스 선택 정책)로 이동한 다음 마우스 오른쪽 버튼을 클릭하고 Device Selection Policy(디바이스 선택 정책)를 생성합니다.



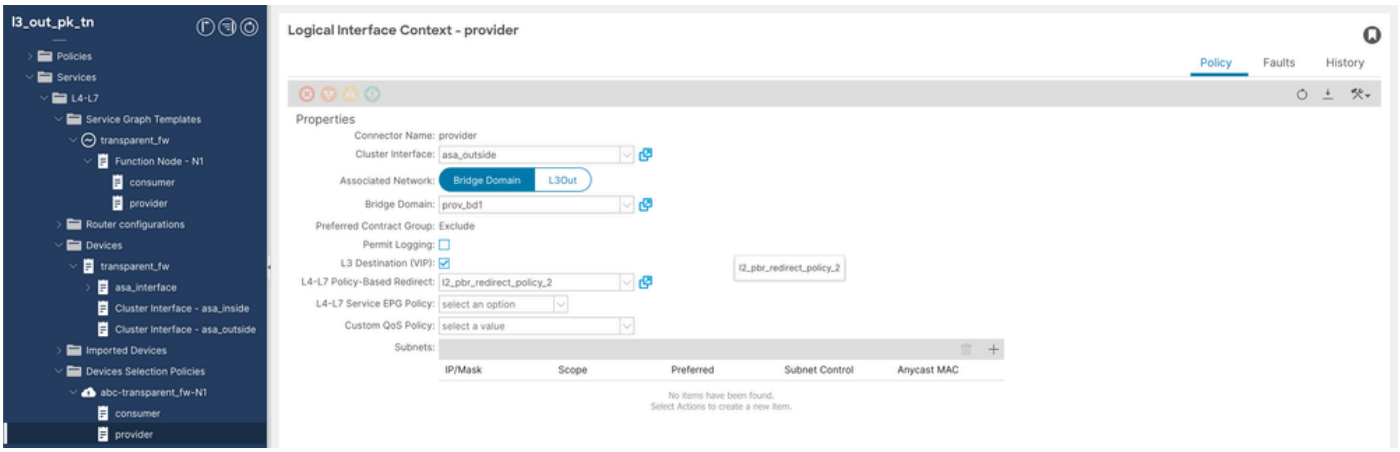
서비스 그래프 컨피그레이션 2

++ 소비자 논리적 인터페이스 컨텍스트

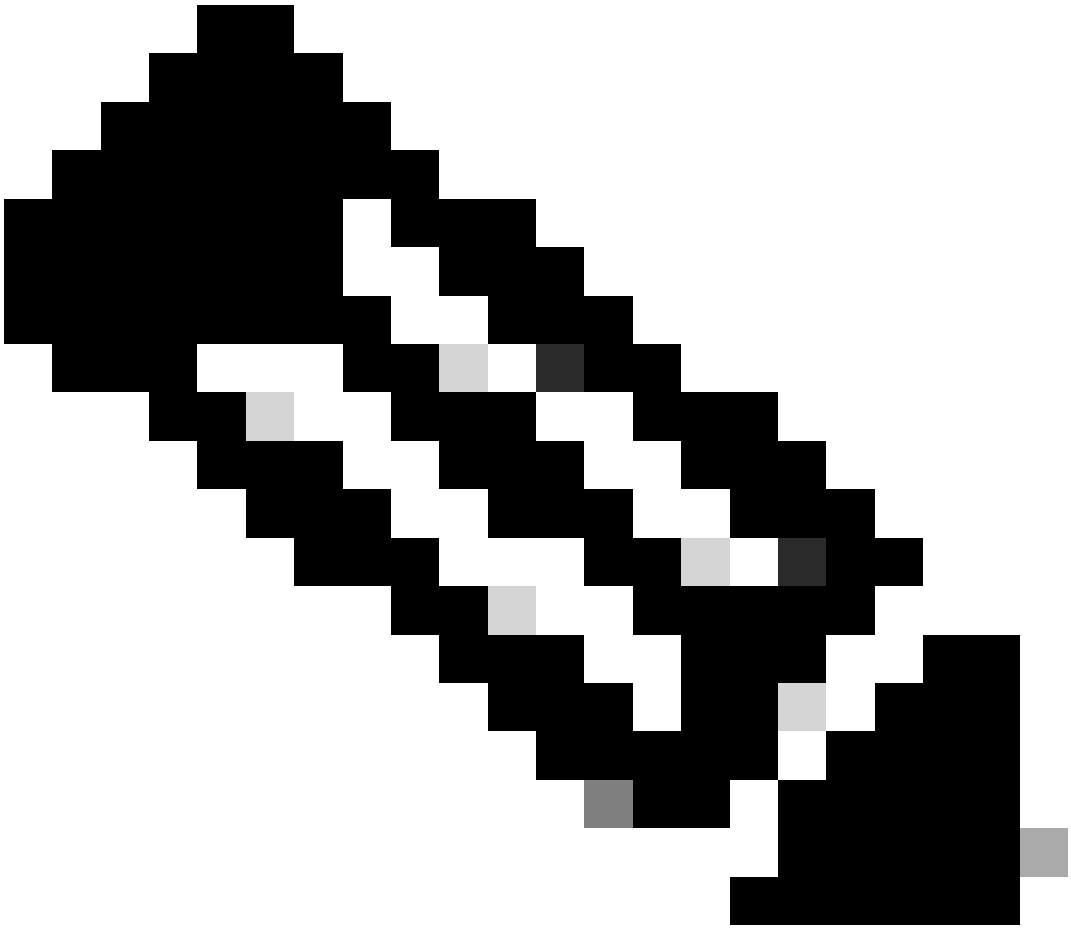


디바이스 선택 정책 소비자 컨피그레이션

++ 공급자 논리적 인터페이스 컨텍스트



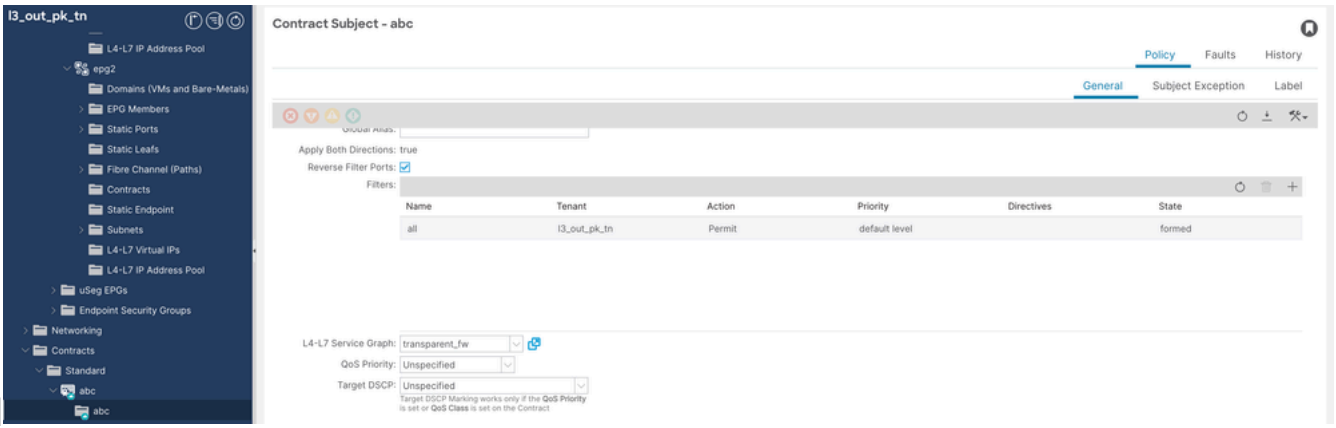
장치 선택 정책 공급자 구성



참고: Apply Service Graph Option(서비스 그래프 옵션 적용)을 사용할 경우 디바이스 선택 정책이 자동으로 생성됩니다.

8단계. abc 주체를 계약하려면 PBR을 적용합니다.

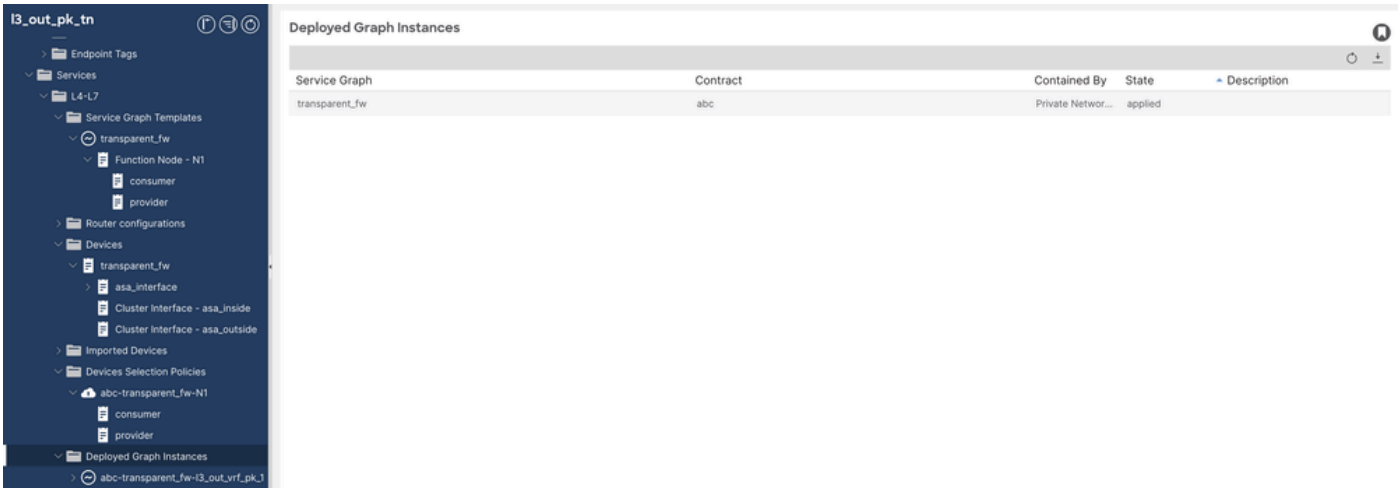
Tenant(테넌트) > Contract(계약) > Contract Subject(계약 제목) > L4-L7 Service Graph(L4-L7 서비스 그래프) > transparent_fw로 이동합니다.



사기

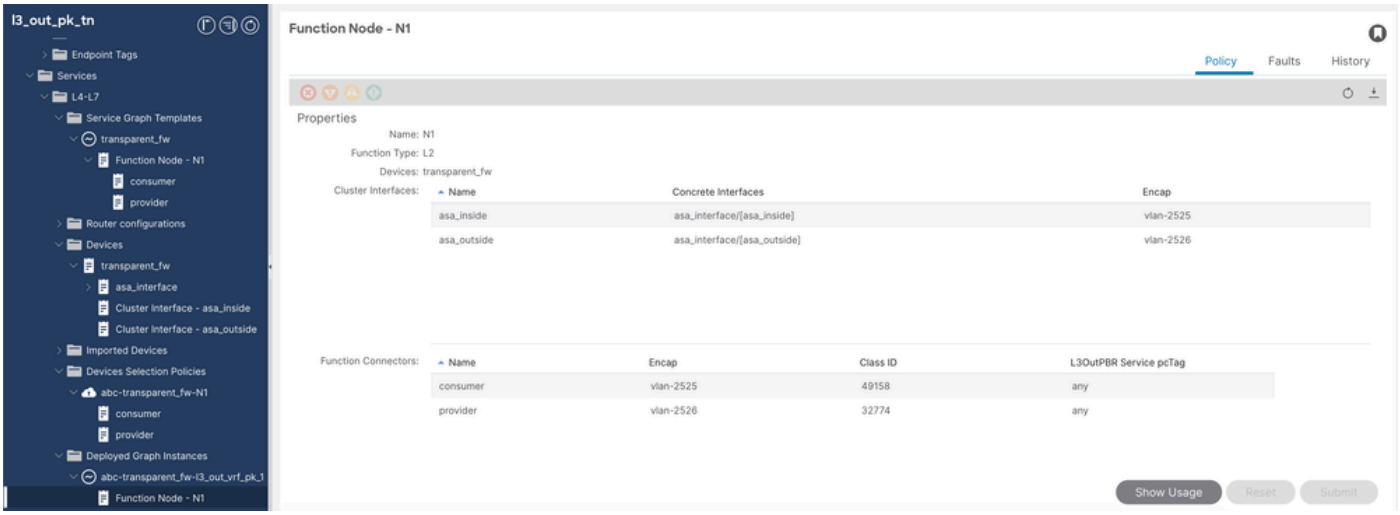
계약 구성

9단계. 성공적으로 구축된 경우 Deployed instance graph(구축된 인스턴스 그래프)에서 검증합니다(state(상태) 검색).



서비스 그래프 검증

++ 클러스터 인터페이스, 캡슐화 VLAN 및 기능 커넥터 클래스 ID를 확인합니다.



서비스 그래프 검증 2

ASA에서 L2 PBR 트래픽 검증

ASA의 연결 테이블 항목에서 볼 수 있는 소스 엔드포인트에서 대상 엔드포인트로의 SSH(Secure Shell)

ASA 검증

Leaf에서 L2 PBR 확인

1. 리프 노드 102의 VLAN 프로그래밍

<#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. 소비자(101) 및 공급자(104) 노드에서 정책 및 영역 지정 규칙을 리디렉션합니다.

<#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  |
```

L2Ping 실패 시 표시되는 결함

PBR 디바이스 전체에서 L2ping이 실패하는 경우 PBR이 여전히 구축됨 상태이며 F4203, F2833 및 F2911 오류가 발생했으며 트랙/상태 그룹이 다운되었음을 나타냅니다.

L2 Ping 캡처

Tahoe 인터페이스의 tcpdump를 사용하여 L2Ping을 캡처하여 올바르게 전송 및 수신되는지 확인할 수 있습니다. CPU 전송이 전송되었지만 수신되지 않은 상태만 보이면 앞서 언급한 장애가 예상되므로 ASA에서 이러한 장애가 삭제된 이유를 추가로 트러블슈팅해야 합니다(ASA 컨피그레이션 섹션 참조).

<#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

Src에서 Dst 엔드포인트로의 트래픽 흐름

<#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 컨피그레이션

1단계. 인터페이스 컨피그레이션

<#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
!
```

2단계. MAC 학습을 비활성화해야 합니다.

<#root>

```
ASA(config)#
```

show run mac-learn

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

PBR:

3단계. PBR Mac용 고정 mac-address-table

<#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
```

4단계. L2ping을 전달하도록 ACL(Access Control List)을 구성합니다.

<#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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.