CISCO

You make **possible**

Troubleshooting ACI

Policy Based Redirect (PBR)

Carlo Schmidt
Technical Solutions Architect

BRKACI-2644

Barcelona | January 27-31, 2020

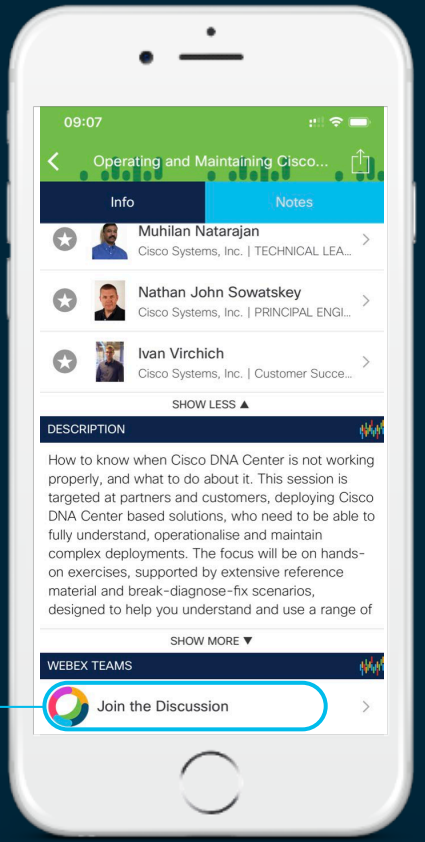
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Agenda

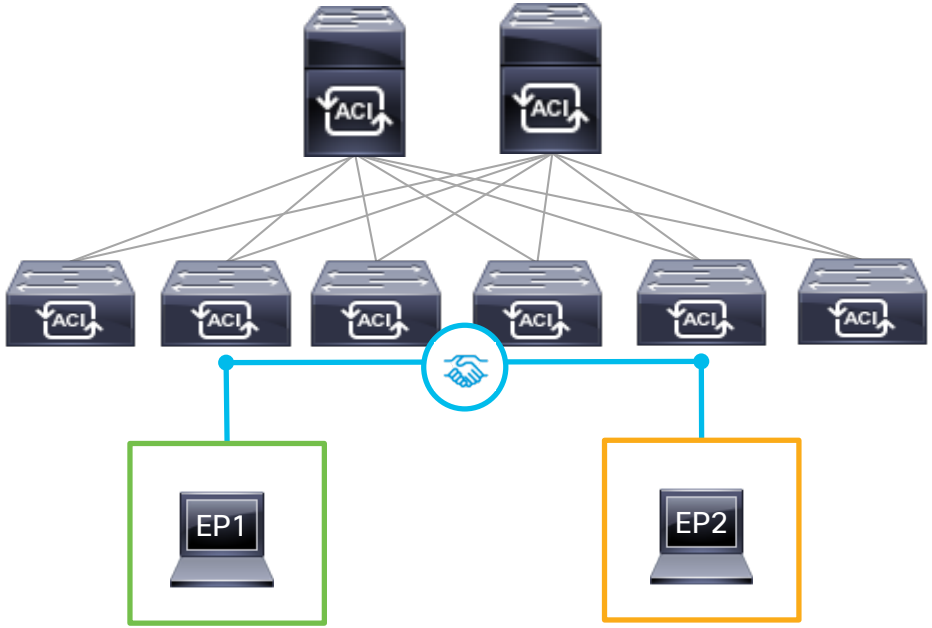
- Overview
- How Service Graphs work
- Shadow EPGs
- Path of a Policy redirected packet
- Additional Features

Service Insertion

Traditional Contract

VRF	Route	pcTag	Flags
V1	S1	1	proxy
V1	EP1	EPG1	Enforce Policy
V1	S2	1	proxy
V1	EP2	EPG2	Enforce Policy

Contract	VRF	Action	Src	Dst	Filter
C1	V1	permit	EPG1	EPG2	HTTP
	V1	permit	EPG2	EPG1	HTTP
implicit	V1	deny	any	any	all



Consumer
BD1, EPG1
Subnet S1

Provider
BD2, EPG2
Subnet S2

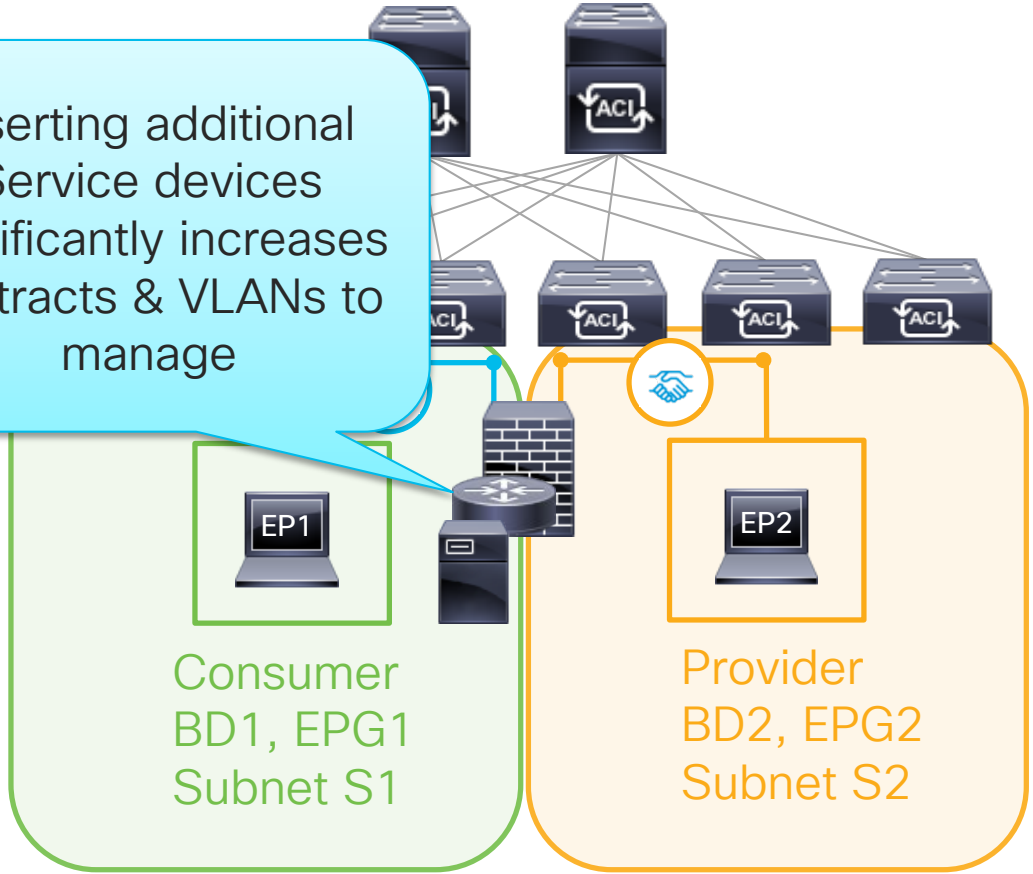
Service Insertion

Traditional Service Insertion

VRF	Route	pcTag	Flags
V1	S1	1	proxy
V1	S2	FW1	Enforce Policy
V2	S1	FW2	Enforce Policy
V2	S2	1	proxy

Contract	VRF	Action	Src	Dst	Filter
C1	V1	permit	EPG1	FW1	HTTP
	V1	permit	FW1	EPG1	HTTP
implicit	V1	deny	any	any	all
C1	V2	permit	EPG2	FW2	HTTP
	V2	permit	FW2	EPG2	HTTP
implicit	V2	deny	any	any	all

Inserting additional Service devices significantly increases contracts & VLANs to manage

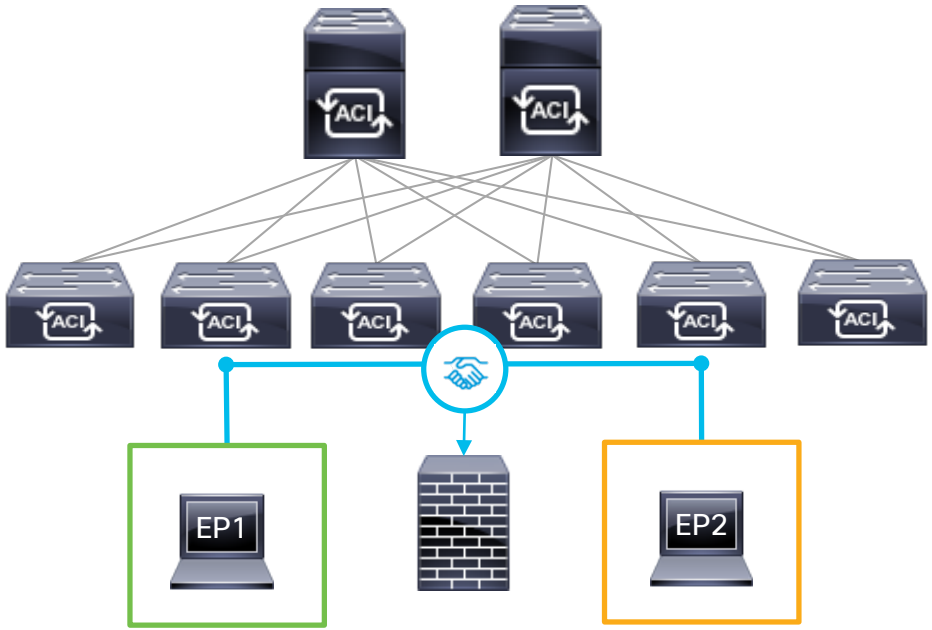


Service Insertion

Policy Based Redirect

VRF	Route	pcTag	Flags
V1	S1	1	proxy
V1	EP1	EPG1	Enforce Policy
V1	S2	1	proxy
V1	EPG2	EPG2	Enforce Policy

Contract	VRF	Action	Src	Dst	Filter
C1	V1	redir	EPG1	EPG2	HTTP
	V1	redir	EPG2	EPG1	HTTP
implicit	V1	deny	any	any	all



Consumer
BD1, EPG1
Subnet S1

Provider
BD2, EPG2
Subnet S2

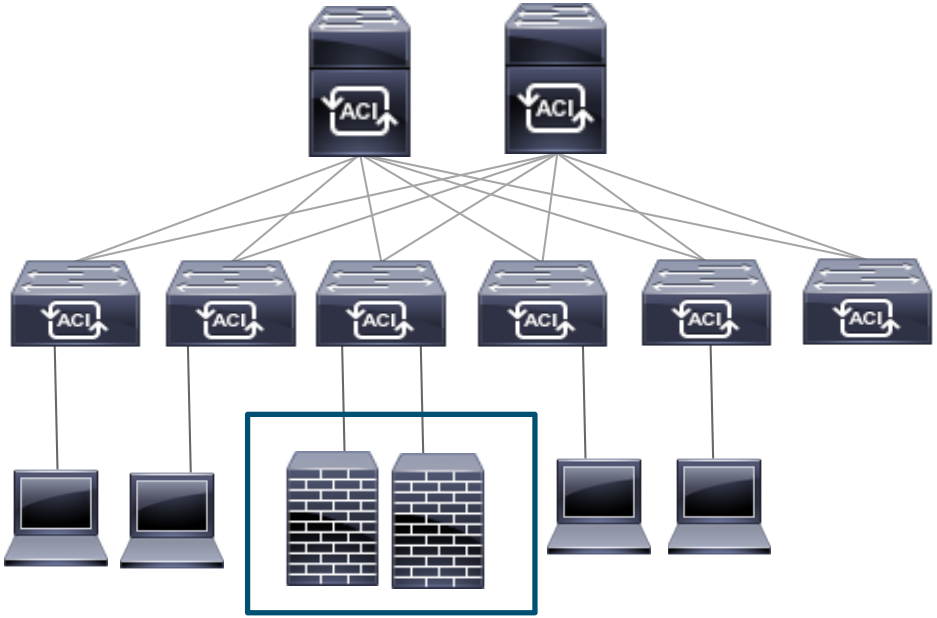
How Service Graphs work

Service Graphs

What is our goal?

Use contracts to determine which traffic should be sent to a firewall cluster called ASA_FW connected to an ACI Leaf

Configure Service Graph in 1 ARM Mode



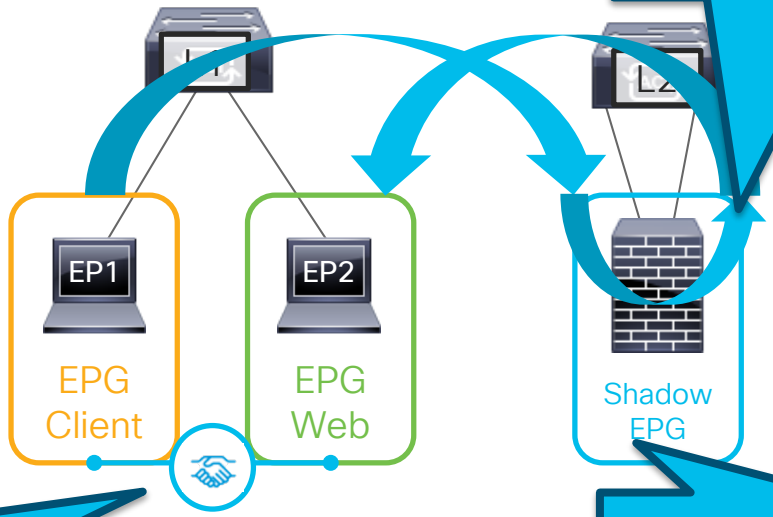
We will have to define two different pieces:

- Contract Policy to allow traffic to flow within an enforced VRF
- Layer 2 and Layer 3 connectivity for the FW

How Service Graphs work

Service Graph Templates defines HOW traffic should flow

The **Device** tells us how many interfaces and logical connectors on the Service Devices



Contract selects traffic to redirect

The **Device Selection Policy** defines how the Device will communicate with the fabric

The

Physical Devices part of device Cluster. Defines how the fabric connects to the interface(s)

Cluster Interface or logical interfaces. Separate the interfaces into two functions – inside/ outside or provider consumer

The Shadow EPG/ VLAN ID that will be used when deploying this device & needs to match device config

ciscoLive
- Quick Start
- ciscoLive
  - Application
  - Networking
  - Contracts
  - Policies
  - Services
    - L4-L7
      - Service Parameters
      - Service Graph Templates
      - Router configurations
      - Function Profiles
      - Devices
        - ASA_FW
          - ASA_1
          - ASA_2
          - Cluster Interface - consumer
          - Cluster Interface - provider
      - Imported Devices
      - Devices Selection Policies
      - Deployed Graph Instances
      - Deployed Devices
      - Device Managers

Name: ASA_FW
Alias:
Service Type: Firewall
Device Type: PHYSICAL
Physical Domain: csStaticPhyDom
Promiscuous Mode:
Context Aware: Multiple | Single
Function Type: GoThrough | GoTo | L1 | L2

Devices

Name
ASA_1
ASA_2

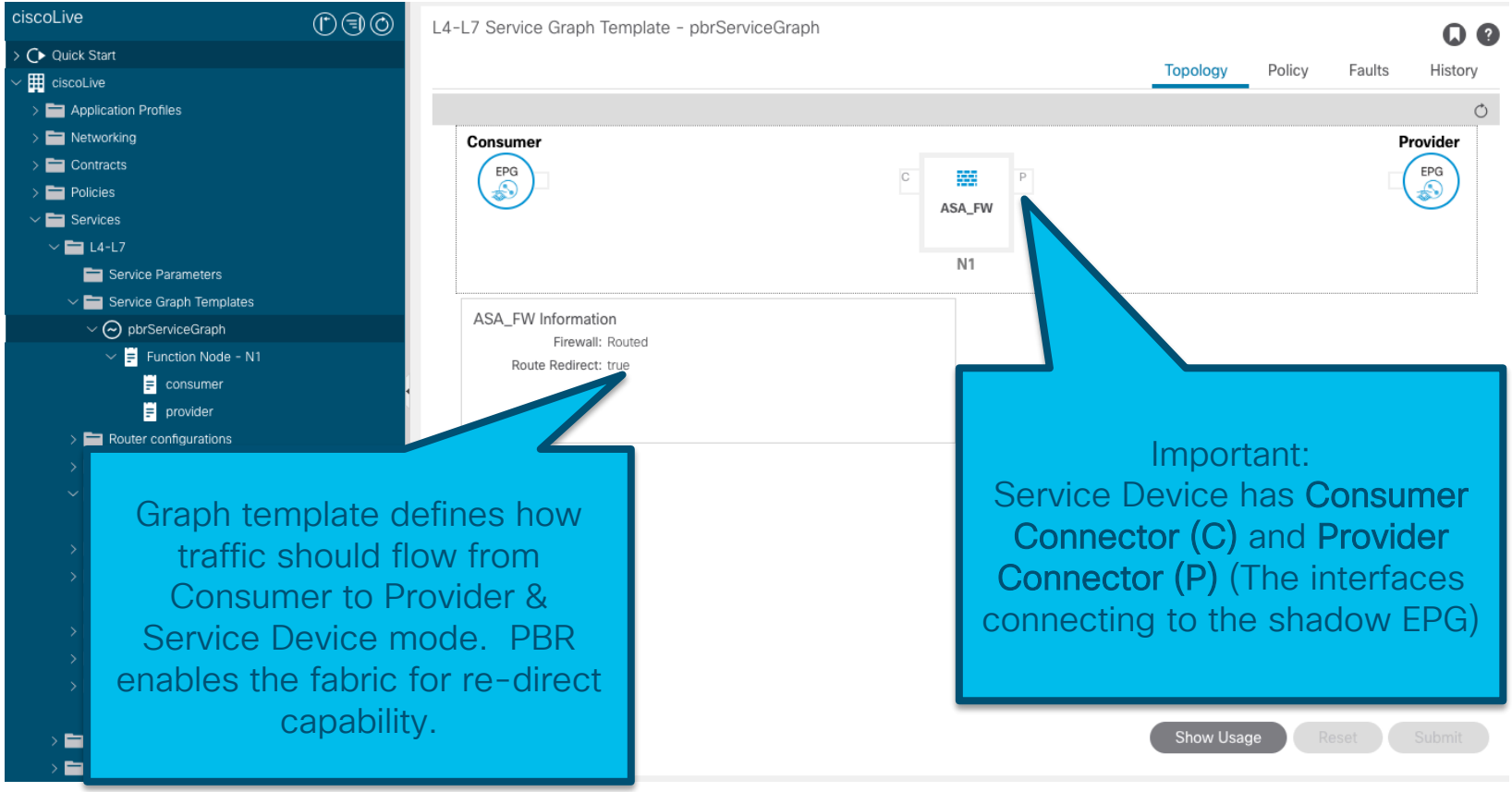
Cluster

Cluster Interfaces:

Name	Concrete Interfaces	Encap
provider	ASA_1/[eth2/5], ASA_2/[eth2/6]	vlan-3100
consumer	ASA_1/[eth2/5], ASA_2/[eth2/6]	vlan-3100

Reset | Submit

The Graph Template



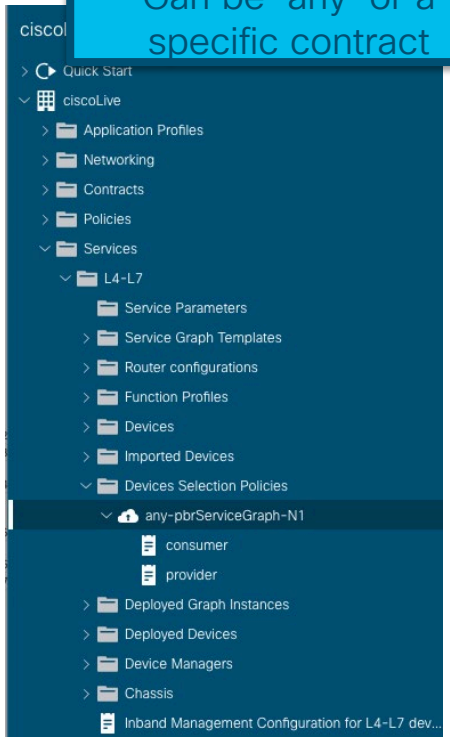
Graph template defines how traffic should flow from Consumer to Provider & Service Device mode. PBR enables the fabric for re-direct capability.

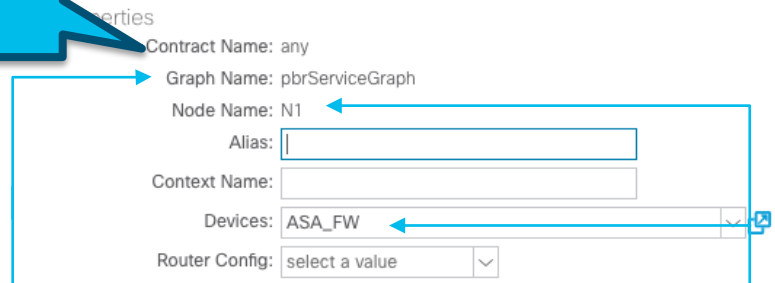
Important:
Service Device has **Consumer Connector (C)** and **Provider Connector (P)** (The interfaces connecting to the shadow EPG)

Device Selection Policy

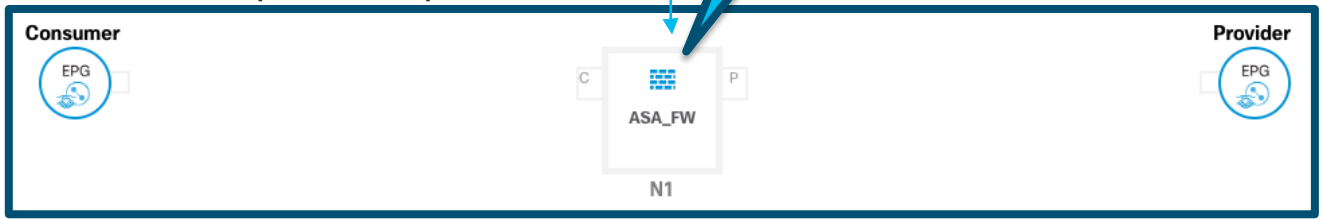
Contract name:
Can be ‘any’ or a specific contract

Service Graph Template is flexible, any ‘Devices’ can be selected as a Node (i.e N1) in a Service Graph

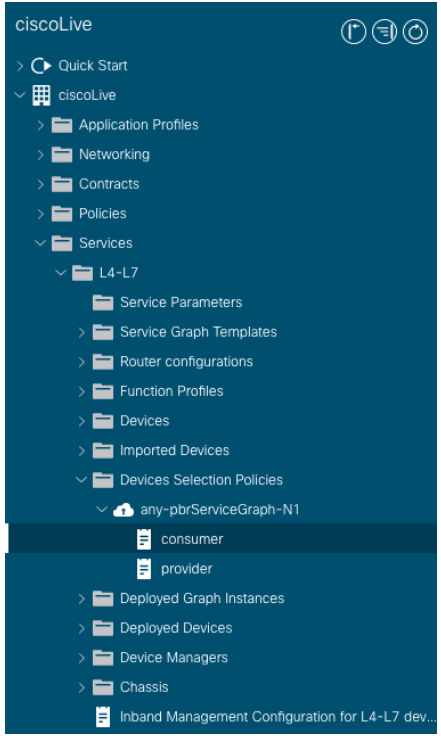




Service Graph Template



Device Selection Policy



Device

Cluster Interfaces:

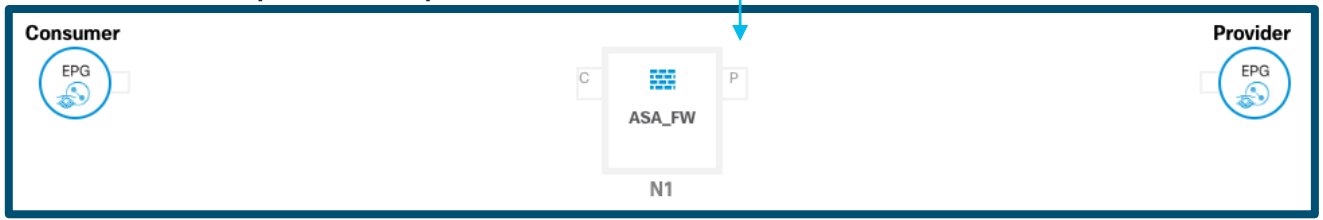
Name	Concrete Interfaces	Encap
provider	ASA_1/[eth2/5], ASA_2/[eth2/6]	vlan-3100
consumer	ASA_1/[eth2/5], ASA_2/[eth2/6]	vlan-3100

Properties

Connector Name: provider
Cluster Interface: provider
Associated Network: Bridge Domain | L3 External Network
Bridge Domain: pbrBD
Preferred Contract Group: Exclude
Permit Logging: ☐
L3 Destination (VIP): ☑
L4-L7 Policy-Based Redirect: ASA_Cluster
L4-L7 Service EPG Policy: select an option
Custom QoS Policy: select a value

PBR Redirect Policy

Service Graph Template



Redirect Policy

Packet rewrite info for compute leaf to know what L2 Dest Mac to send packet to

Properties

Name: ASA_Cluster

Description: optional

Destination Type: L1 L2 L3

IP SLA Monitoring Policy: select an option

Oper Status: Enabled

Enable Pod ID Aware Redirection: ☐

Hashing Algorithm: dip sip sip-dip-prototype

Anycast Endpoint: ☐

Resilient Hashing Enabled: ☐

L3 Destinations:

IP	MAC	Redi Gro	Health	Additional IPv4/IPv6	Description	Oper Status
172.16.1.5	00:00:25:25:25:25			0.0.0.0		Enabled
172.16.1.6	00:00:26:26:26:26			0.0.0.0		Enabled

Contract

Least specific filter used should be ‘IP’ not ‘default’

Adding a Service Graph to a contract. This will tell the fabric when to add contracts between the Consumer/Provider EPG and the shadow EPGs

Contract Subject - webRedirect

Global A

Apply Both Direction

Reverse Filter Ports:

Filters:

Name	Tenant	Action
webRedirect	ciscoLive	Permit

L4-L7 Service Graph: pbrServiceGraph

QoS Priority: Unspecified

Target DSCP: Unspecified

Wan SLA Policy: select an option

How Service Graphs work

A quick review

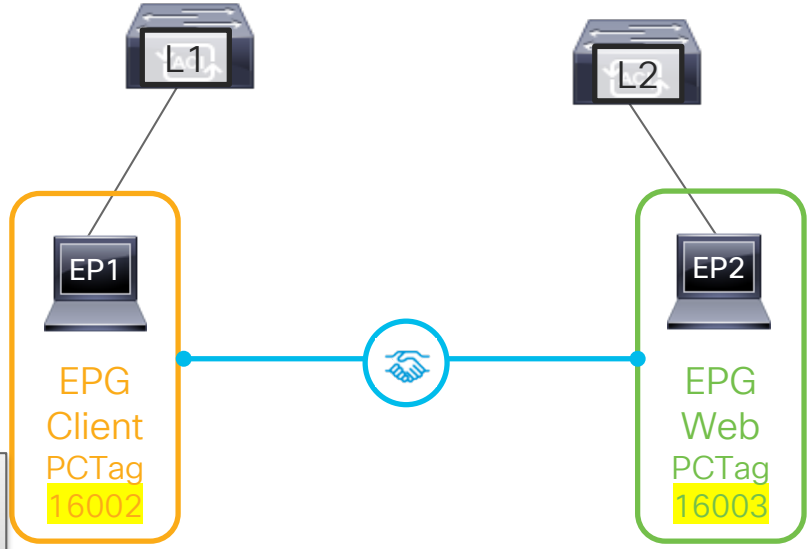
- Service Graph Template
  - Define the flow of traffic
- Devices
  - Physical Device & interfaces it connects to in fabric. Converted to Consumer Connector and Provider Connector
- Device Selection Policy
  - Ties the physical device to a Graph template and contract
- Contract
  - Places Contract between Consumer & Provider and the shadow EPG

Shadow EPGs

Quick Review!

How does policy enforcement work

- Each EPG is represented by a policy tag, or PCTag
- Source Tag (sClass, or source class) is applied on ingress
- Source PCTag is carried in VXLAN header



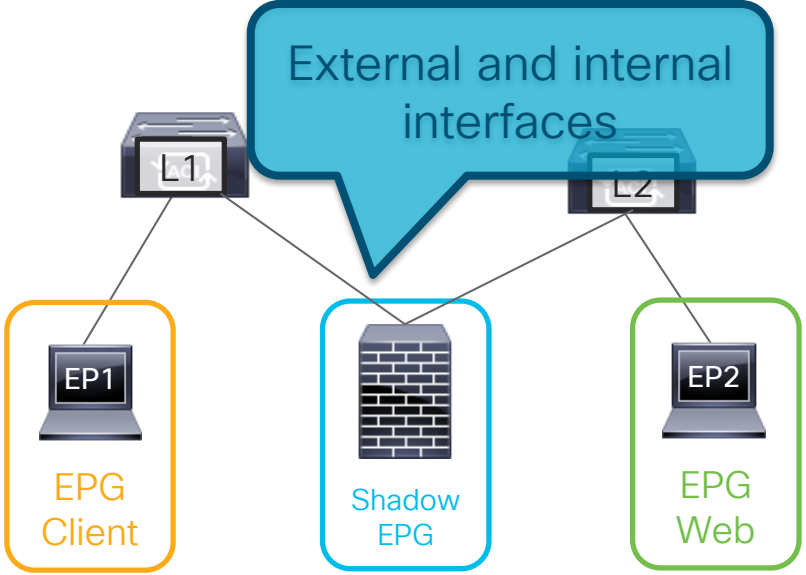

```
leaf1# show vlan id 64 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------
 64   ciscoLive:PBR:Web                vlan-3067        Eth1/1, Eth1/2,

leaf1# vsh_lc -c "show system internal eltmc info vlan 64" | egrep sclass
              sclass:          16002
```

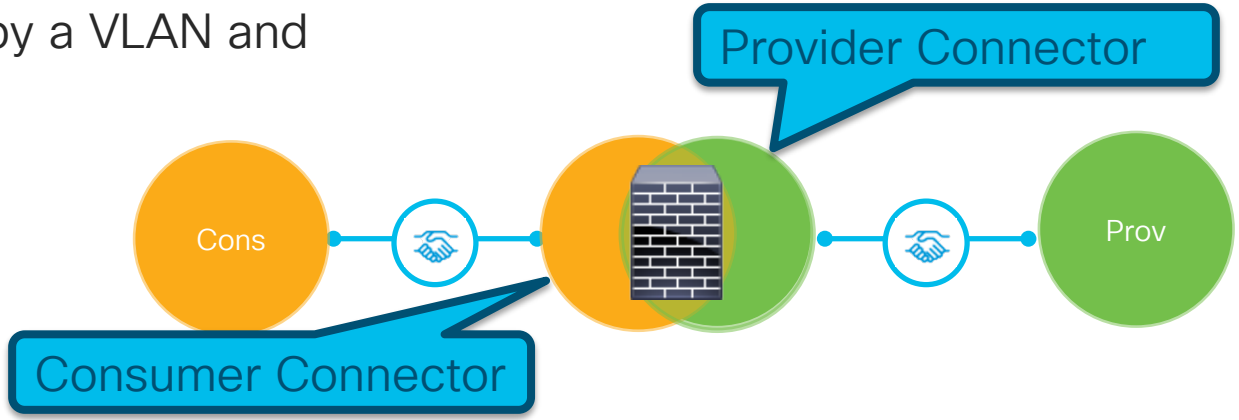
```
Leaf 1# show zoning-rule scope 2490374
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
|   4269  | 16002  | 16003  |    16    |    uni-dir     | enabled | 2490374 |      |      permit       |    fully_qual(7)     |
```

What are shadow EPGs?

A *'two armed'* example

- Shadow EPGs connect to the service Device
- External Interface is called the "Consumer Connector"
- Internal interface is the "Provider Connector"
- Each is represented by a VLAN and has its own PCTag

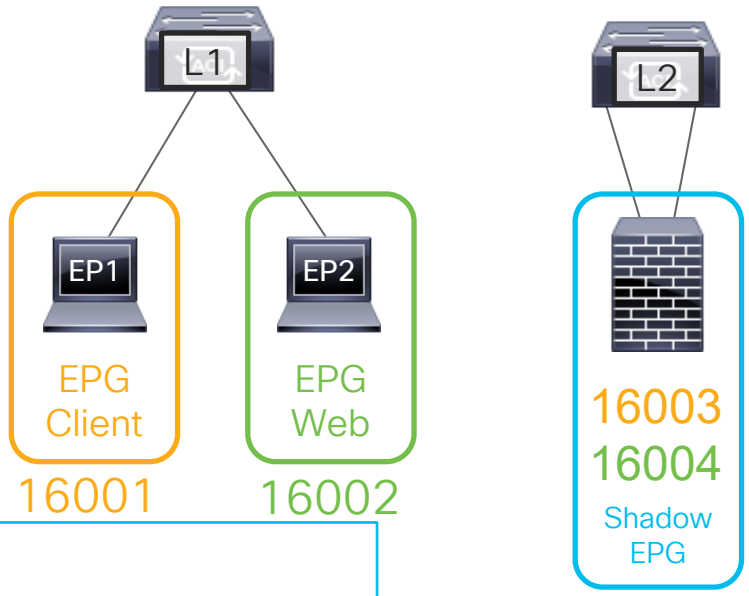




EPGs and PCTags

```
leaf1# show vlan id 64 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------
 64   ciscoLive:PBR:Web            vlan-3067        Eth1/1, Eth1/2,

leaf1# show vlan id 140 extended


 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------
 140  ciscoLive:ASA_FWctxv1:provider:  vlan-3100        Eth1/23, Eth1/24
```

```
leaf1# vsh_lc -c "show system internal eltmc info vlan 64" | egrep sclass
              sclass:          16002

leaf1# vsh_lc -c "show system internal eltmc info vlan 140" | egrep sclass
              sclass:          16004
```

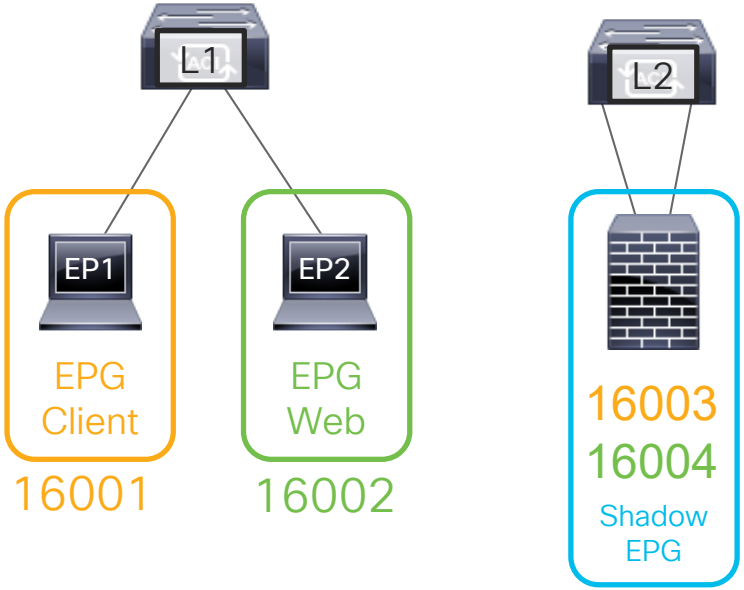


Cluster Interfaces:

Name	Concrete Interfaces	Encap
provider	ASA_1/[eth2/5], ASA_2/[eth2/6]	vlan-3100
consumer	ASA_1/[eth2/5], ASA_2/[eth2/6]	vlan-3100

Shadow EPGs & contracts

- EPG Client to EPG Web (Redirect)
- EPG Web to EPG Client (Redirect)
- Consumer Conn to Client (uni-dir Filter)
- Provider Conn to Web (uni-dir default)



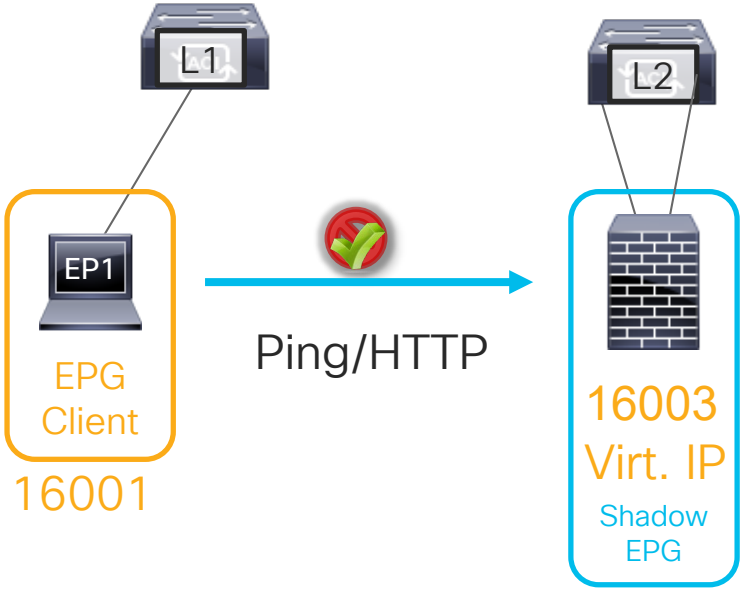

```
Leaf 1# show zoning-rule scope 2490374
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
|   4269  | 16003  | 16001  |    16    |    uni-dir     | enabled | 2490374 |      |       permit      |    fully_qual(7)     |
|   4561  | 16001  | 16002  |    15    |     bi-dir     | enabled | 2490374 |      | redir(destgrp-24) |    fully_qual(7)     |
|   4537  | 16002  | 16001  |    16    | uni-dir-ignore | enabled | 2490374 |      | redir(destgrp-24) |    fully_qual(7)     |
|   4536  | 16004  | 16002  | default  |    uni-dir     | enabled | 2490374 |      |       permit      |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
```

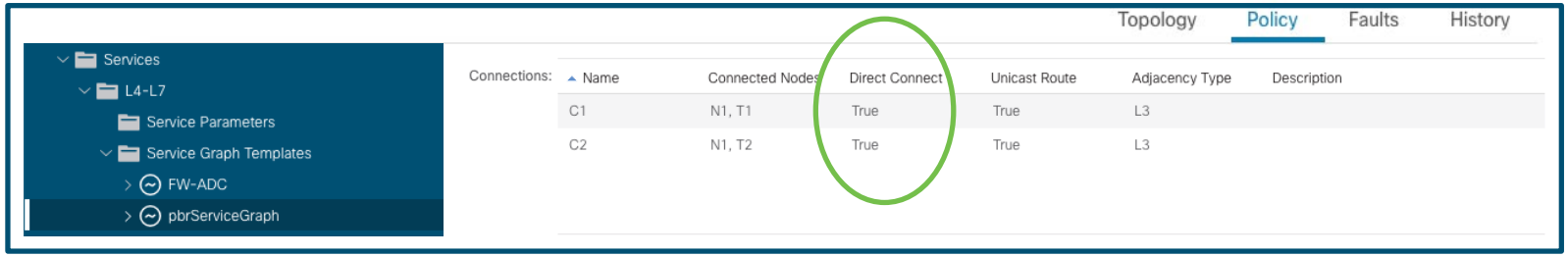
Common issues

1) Unable to ping Consumer connector

The filter between shadow EPG and Consumer or provider is unidirectional by default.

Enable **Direct Connect** on the Graph Template to create EPG to Shadow EPG contracts



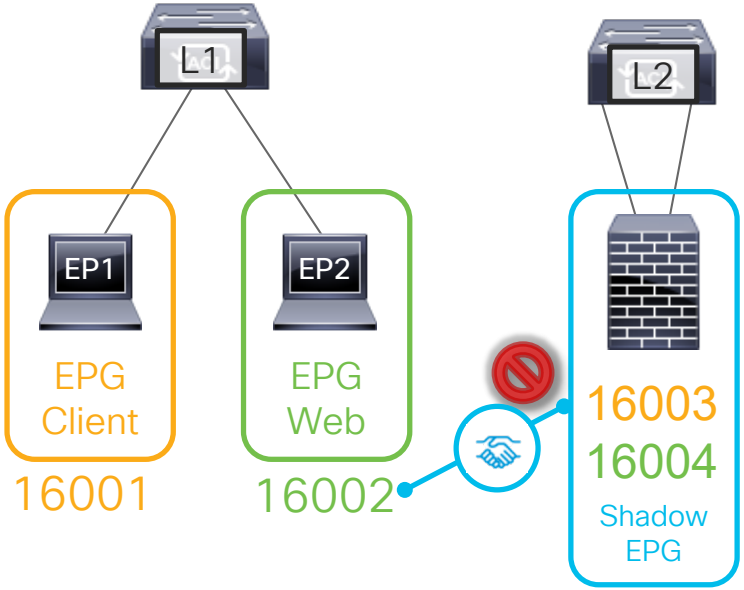


Common Issues

2) Routing on Service Device

Service Device route for Provider subnet points through consumer connector

Consumer connector does not have a contract and direct connect does not fix this



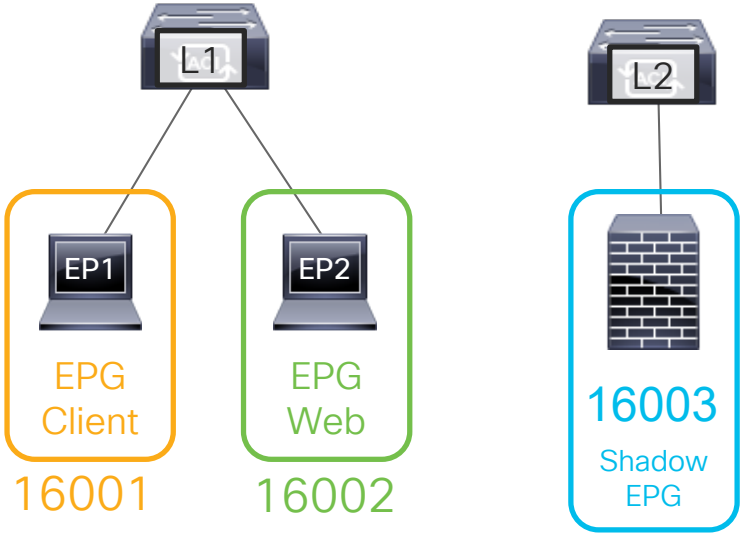

```
ciscoasa# show route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 172.16.2.2, inside
S        192.168.1.0 255.255.255.0 [1/0] via 172.16.1.2, outside
S        192.168.2.0 255.255.255.0 [1/0] via 172.16.1.2, outside
```

Common Issues

2) Routing on Service Device

Use a 1 arm service graph for PBR!

Service device (FW etc) should know if traffic should be allowed or not!



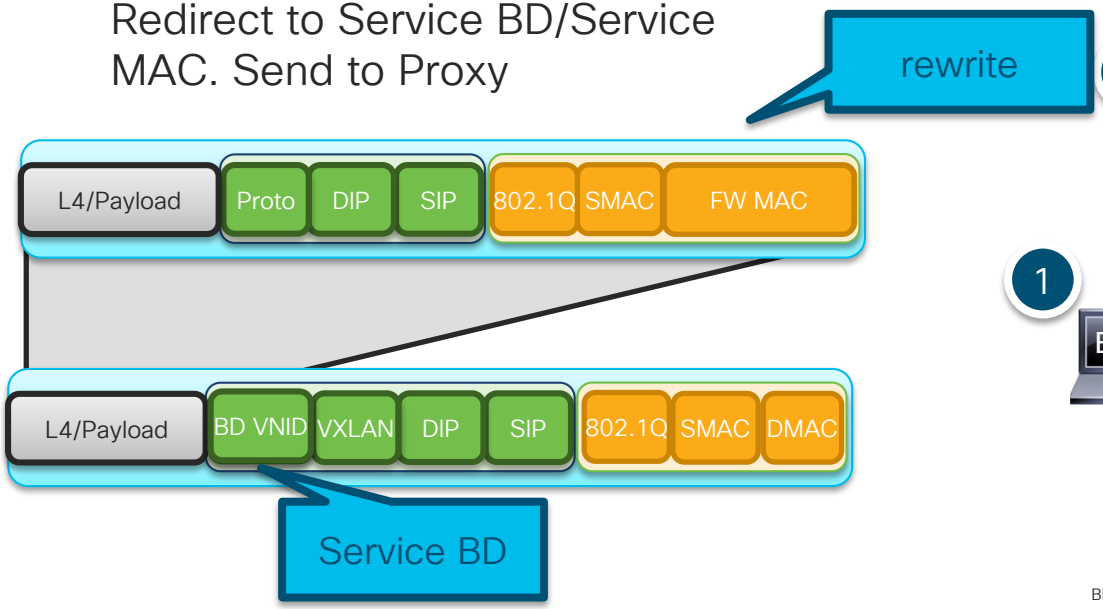

```
ciscoasa# show route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 172.16.2.2, inside
```

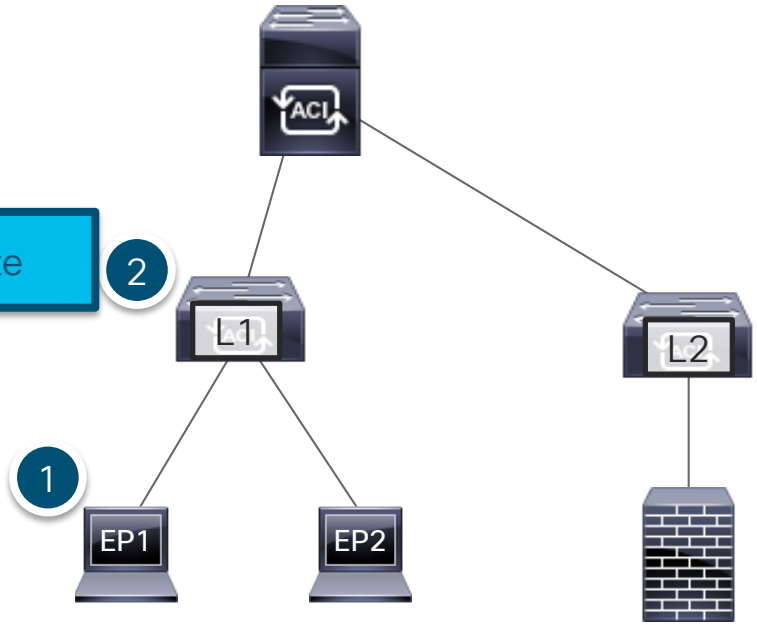
```
Leaf 1# show zoning-rule scope 2490374
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
|   4269  | 16003  | 16001  |    16    |    uni-dir     | enabled | 2490374 |      |       permit      |    fully_qual(7)     |
|   4561  | 16001  | 16002  |    15    |     bi-dir     | enabled | 2490374 |      | redir(destgrp-24) |    fully_qual(7)     |
|   4537  | 16002  | 16001  |    16    | uni-dir-ignore | enabled | 2490374 |      | redir(destgrp-24) |    fully_qual(7)     |
|   4536  | 16003  | 16002  | default  |    uni-dir     | enabled | 2490374 |      |       permit      |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
```

Path of a policy redirected packet

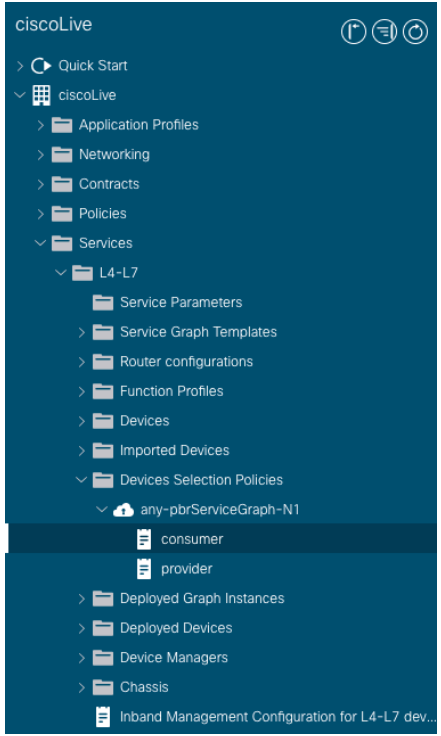
Path of Packet

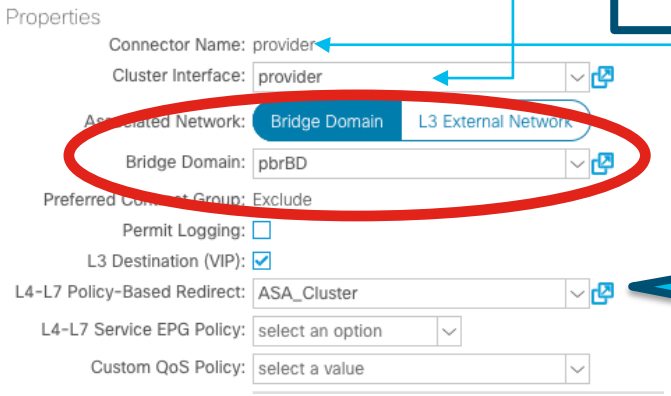
1. EP1 sends packet to EP2 via Leaf 1 (L1)
2. L1 does route & policy lookup – Redirect to Service BD/Service MAC. Send to Proxy

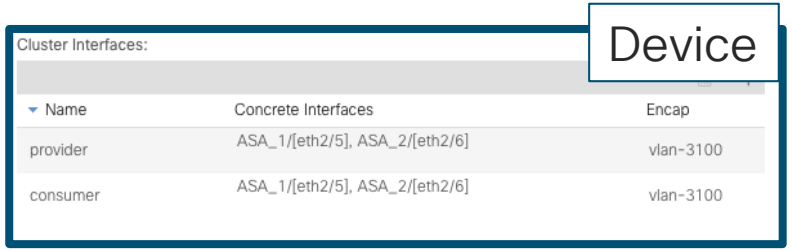




Device Selection Policy

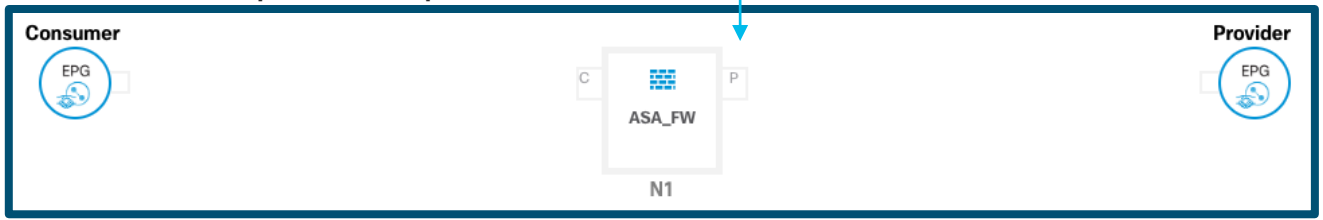






PBR Redirect Policy

Service Graph Template



Redirect Policy

Packet rewrite info for compute leaf to know what L2 Dest Mac to send packet to

Properties

Name: ASA_Cluster

Description: optional

Destination Type: L1 L2 L3

IP SLA Monitoring Policy: select an option

Oper Status: Enabled

Enable Pod ID Aware Redirection:

Hashing Algorithm: dip sip sip-dip-prototype

Anycast Endpoint:

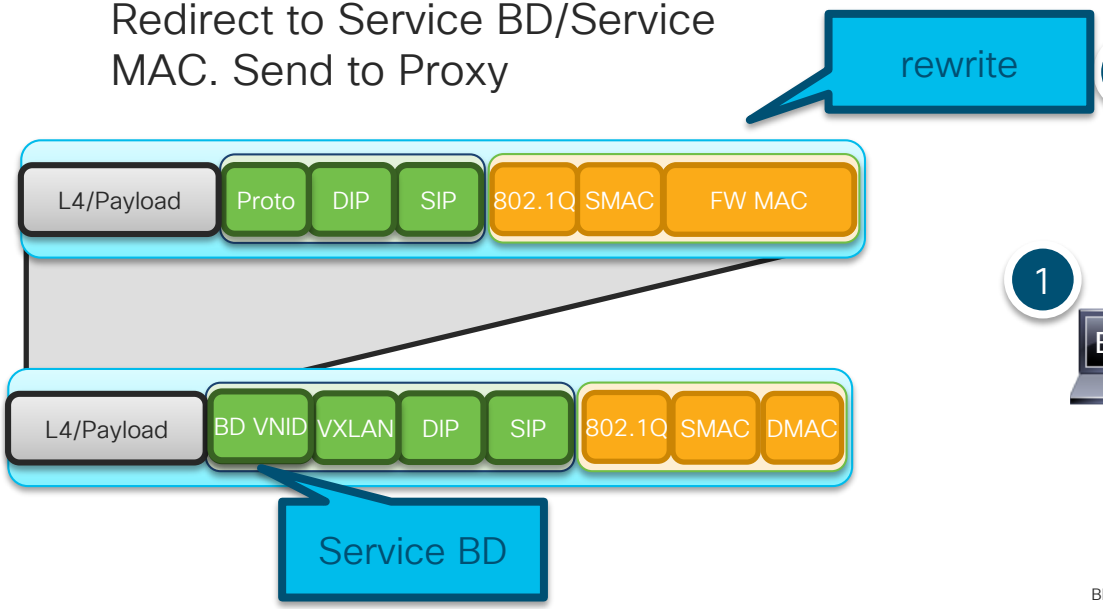
Resilient Hashing Enabled:

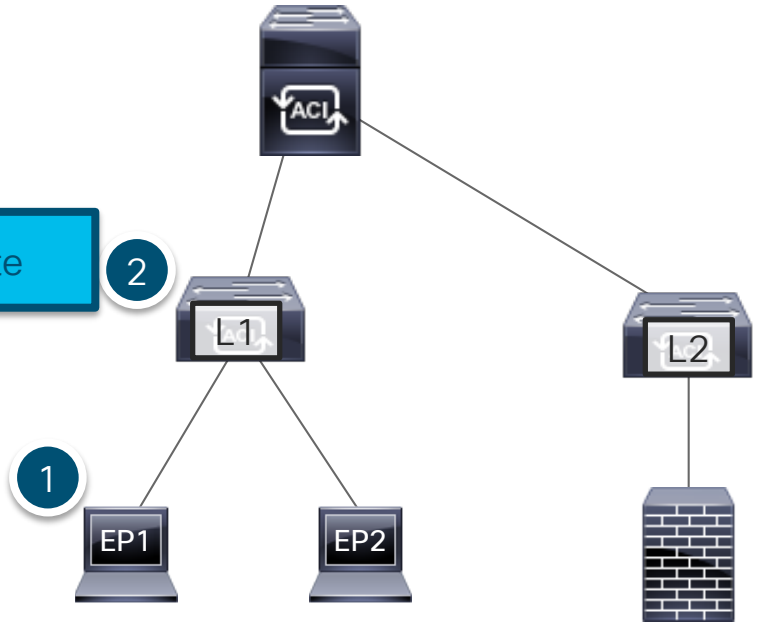
L3 Destinations:

IP	MAC	Redi	Health	Additional IPv4/IPv6	Description	Oper Status
172.16.1.5	00:00:25:25:25:25			0.0.0.0		Enabled
172.16.1.6	00:00:26:26:26:26			0.0.0.0		Enabled

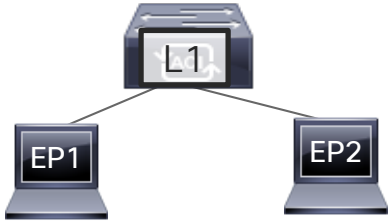
Path of Packet

1. EP1 sends packet to EP2 via Leaf 1 (L1)
2. L1 does route & policy lookup – Redirect to Service BD/Service MAC. Send to Proxy





Command Line verification



A Confirm sclass & dclass of traffic flow

```
leaf1# show system internal epm endpoint ip 192.168.1.10 |
egrep  "VRF vnid|sclass "
BD vnid : 16285645 ::: VRF vnid : 2490374
Flags : 0x80005c04 ::: sclass : 49154 ::: Ref count : 5
```

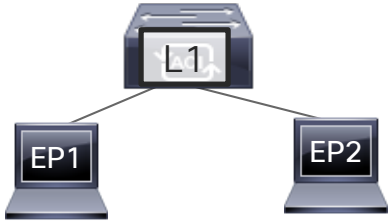
```
leaf1# show system internal epm endpoint ip 192.168.2.20 |
egrep "VRF vnid|sclass "
BD vnid : 16678793 ::: VRF vnid : 2490374
Flags : 0x80005c04 ::: sclass : 49155 ::: Ref count : 5
```

B Verify zoning rule is configured with ‘redir’ action and matches desired traffic

```
leaf1# show zoning-rule scope 2490374 src-epg 49154 dst-epg 49155
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+---------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |    Priority   |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+---------------+
|   4236  | 49154  | 49155  |   15     | uni-dir-ignore | enabled | 2490374 |      | redir(destgrp-17) | fully_qual(7) |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+---------------+
```

```
leaf1# show zoning-filter filter 15
+----------+------+--------+-------------+------+-------------+----------+-------------+-------------+-------------+-------------+
| FilterId | Name | EtherT |    ArpOpc   | Prot | ApplyToFrag | Stateful |  SFromPort  |   SToPort   |  DFromPort  |   DToPort   |
+----------+------+--------+-------------+------+-------------+----------+-------------+-------------+-------------+-------------+
|   15     | 15_0 |   ip   | unspecified | tcp  |      no     |    no    | unspecified | unspecified | http        | http        |
+----------+------+--------+-------------+------+-------------+----------+-------------+-------------+-------------+-------------+
```


Command Line verification



C

Verify zoning rule is configured with ‘redir’ action and matches desired traffic

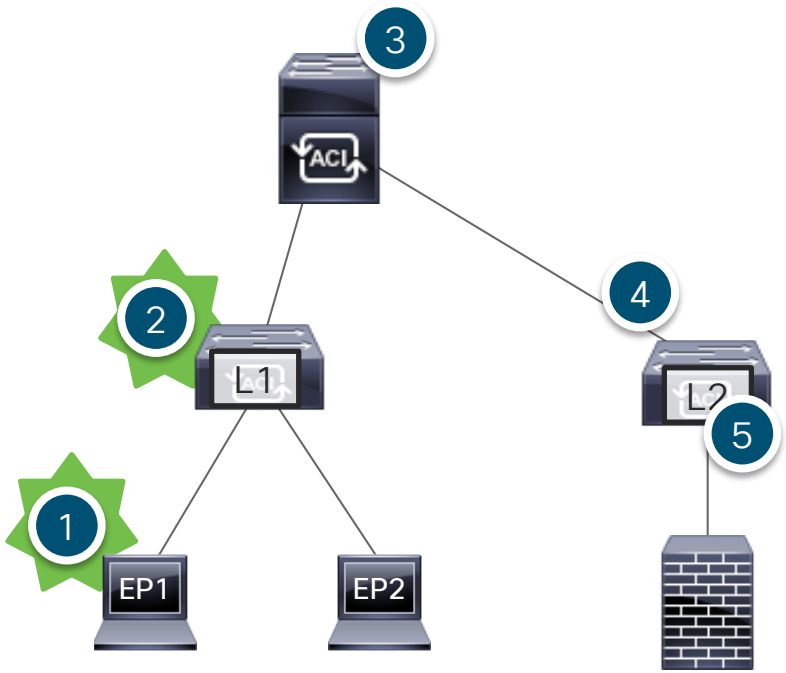
```
Leaf1# show service redir info group 17
==========================================================================================
LEGEND
TL: Threshold(Low)   |     TH: Threshold(High)   |   HP: HashProfile     |     HG: HealthGrp
==========================================================================================
GrpID Name            destination                              HG-name         operSt     operStQual      TL   TH    HP         Tracking
===== ====            ===========                              ==============  =======    ============    ===  ====  ========   ========
17    destgrp-17      dest-[172.16.1.5]-[vxlan-2490374]        Not attached    enabled    no-oper-grp     0    0     symmetric  no
                      dest-[172.16.1.6]-[vxlan-2490374]        Not attached
```

```
Leaf1# show service redir info destination ip 172.16.1.5 vnid 2490374
==========================================================================================
LEGEND
TL: Threshold(Low)   |     TH: Threshold(High)   |   HP: HashProfile     |     HG: HealthGrp
==========================================================================================
Name                                  bdVnid          vMac                vrf             operSt     operStQual      HG-name
====                                  ======          ====                ====            =====      =========       =======
dest-[172.16.1.5]-[vxlan-2490374]     vxlan-16482210  00:00:25:25:25:25   ciscoLive:v1    enabled    no-oper-dest    Not attached
```

Spine Lookup using following key
vxlan-16482210 **00:00:25:25:25:25**

Path of Packet

1. EP1 sends packet to EP2 via Leaf 1 (L1)
2. L1 does policy lookup – Redirect to Service BD/Service MAC. Send to Proxy
3. MAC Proxy does MAC lookup in hardware COOP DB
4. Traffic is sent to Service Leaf (L2) & L2 sends traffic to Service Device
5. Service Device sends traffic back to router MAC. Dest IP is EP2 Policy lookup is made



Command Line verification

A Verify Spine has learned MAC EP

```
Spine# show coop internal info repo ep key 16482210 00:00:25:25:25:25 | egrep "Tunnel|EP" | head -n 3
EP bd vnid : 16482210
EP mac :  00:00:25:25:25:25
Tunnel nh : 10.0.200.67
```

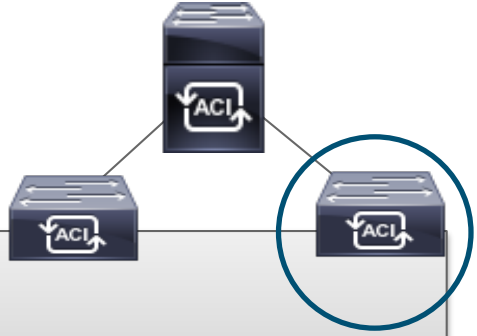
B Map tunnel destination address to leaf

```
Spine# vsh -c "show isis database detail vrf overlay-1" | egrep 10.0.200.67
    TEP Address    :  IPv4         DomainWide AppId 1 [10.0.200.67, 0.0.0.0, 0.0.0.0]
```

If Destination address is a vPC IP, 2 TEP addresses will show. PTep and VTep

```
Spine# acidiag fnvread | egrep 10.0.200.67
     102        2            Leaf2       FDO21050JDE     10.0.200.67/32    leaf         active   0
```

Command Line verification



C

Verify Service Device/ FW programming on Leaf 102

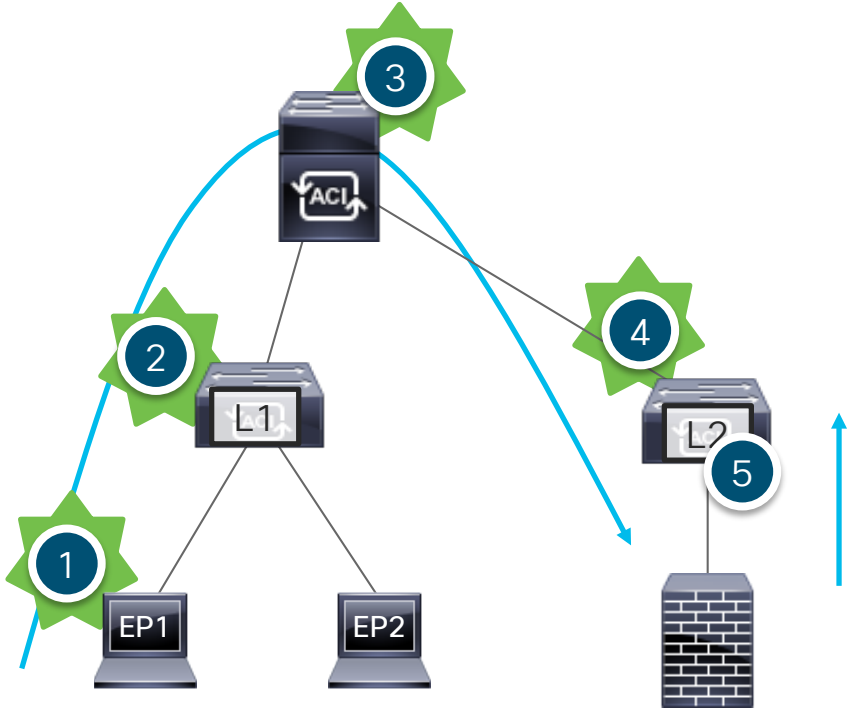
```
leaf2# show endpoint mac 00:00:25:25:25:25
+-----------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+-----------------------------------+---------------+-----------------+--------------+-------------+
52                                        vlan-3100    0000.2525.2525 L                    eth1/23
ciscoLive:v1                              vlan-3100        172.16.1.5 L                    eth1/23
```

We can confirm VLAN 52 is mapped to the Service Graph and BD

```
leaf2# show vlan id 52 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------------
 52   ciscoLive:ASA_FWctxv1:provider: vlan-3100        Eth1/23, Eth1/24

leaf2# show system internal epm vlan 52
+----------+---------+-----------------+----------+------+----------+-----------
   VLAN ID     Type      Access Encap     Fabric    H/W id  BD VLAN    Endpoint
                         (Type Value)     Encap                          Count
+----------+---------+-----------------+----------+------+----------+-----------
 52           FD vlan 802.1Q       3100 20392      61     51         2

leaf2# show vlan id 51 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------------
 51   ciscoLive:pbrBD                  vxlan-16482210   Eth1/23, Eth1/24
```

Path of Packet

1. EP1 sends packet to EP2 via Leaf 1 (L1)
2. L1 does policy lookup – Redirect to Service BD/Service MAC. Send to Proxy
3. MAC Proxy does MAC lookup in hardware COOP DB
4. Traffic is sent to Service Leaf (L2) & L2 sends traffic to Service Device
5. Service Device sends traffic back to router MAC. Dest IP is EP2 Policy lookup is made



Command Line verification

D

Traffic is sent to 1 arm service device. After inspection, traffic will come back to Leaf via Service Device VLAN

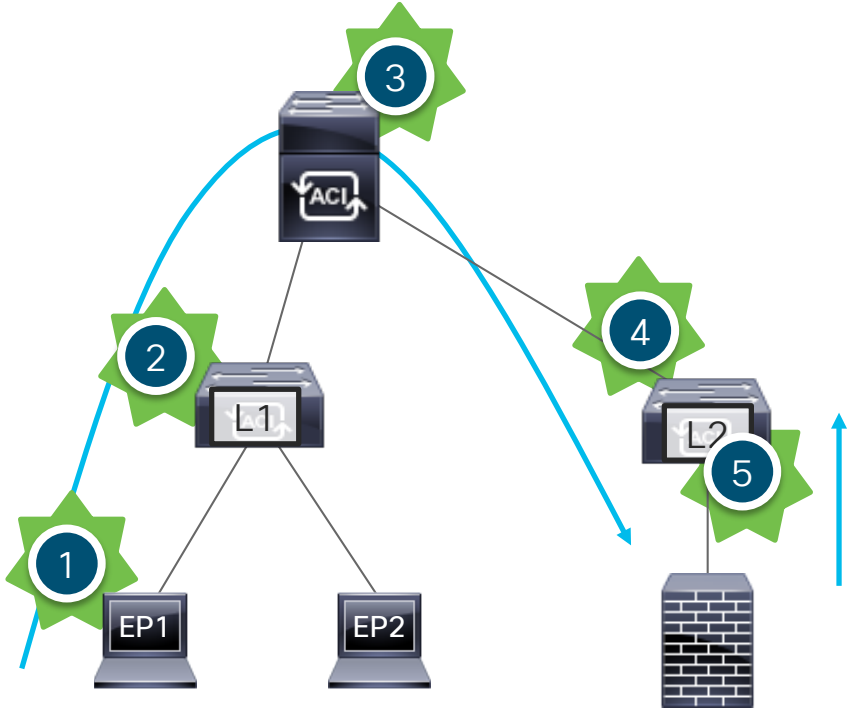
```
leaf2# show system internal epm endpoint mac 0000.2525.2525 |
egrep "VRF vnid|sclass "
BD vnid : 16482210 ::: VRF vnid : 2490374
Flags : 0x80004c04 ::: sclass : 49157 ::: Ref count : 5
```

```
leaf2# show system internal epm endpoint ip 192.168.2.20 |
egrep "VRF vnid|sclass "
BD vnid : 16678793 ::: VRF vnid : 2490374
Flags : 0x80005c04 ::: sclass : 49155 ::: Ref count : 5
```

```
leaf2# show zoning-rule scope 2490374 src-epg 49157 dst-epg 49155
+---------+--------+--------+----------+---------+---------+---------+------+--------+---------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name | Action |    Priority   |
+---------+--------+--------+----------+---------+---------+---------+------+--------+---------------+
|   4196  | 49157  | 49155  |   16     | uni-dir | enabled | 2490374 |      | permit | fully_qual(7) |
+---------+--------+--------+----------+---------+---------+---------+------+--------+---------------+
leaf2# show zoning-filter filter 16
+----------+------+--------+-------------+------+-------------+----------+-------------+-------------+
| FilterId | Name | EtherT |    ArpOpc   | Prot | ApplyToFrag | Stateful |  SFromPort  |   SToPort   |
+----------+------+--------+-------------+------+-------------+----------+-------------+-------------+
|   16     | 16_0 |   ip   | unspecified | tcp  |      no     |    no    | unspecified | unspecified |
+----------+------+--------+-------------+------+-------------+----------+-------------+-------------+
```

Path of Packet

1. EP1 sends packet to EP2 via Leaf 1 (L1)
2. L1 does policy lookup – Redirect to Service BD/Service MAC. Send to Proxy
3. MAC Proxy does MAC lookup in hardware COOP DB
4. Traffic is sent to Service Leaf (L2) & L2 sends traffic to Service Device
5. Service Device sends traffic back to router MAC. Dest IP is EP2 Policy lookup is made



Common Issues

1) Encap is already configured for a different EPG

```
a-leaf205# show vlan id 52 extended
VLAN Name                                Encap            Ports
---- -------------------------------- ---------------- -------------------------
52   ciscoLive:ASA_FWctxv1:provider: vlan-3100        Eth1/23, Eth1/24
```

L4-L7 Devices - N77-PBR

General

Managed: ☐

Name: N77-PBR

Alias:

Service Type: Firewall

Device Type: PHYSICAL

Physical Domain: csStaticPhyDom

Promiscuous Mode: ☐

Context Aware: Multiple | Single

Function Type: GoThrough | GoTo

Devices

Name	Interfaces
N77-e2-5	Eternet2/5 (Pod-2/Node-205/eth1/23)
n77-e2-6	Ethernet2/6 (Pod-2/Node-205/eth1/24)

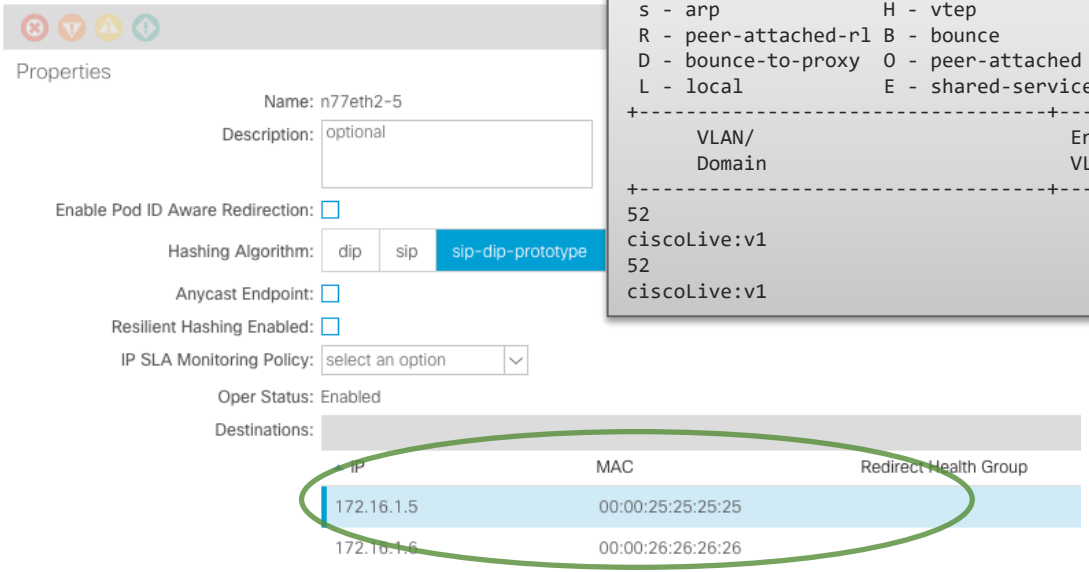
Cluster

Cluster Interfaces:

Name	Concrete Interfaces	Encap
consumer	N77-e2-5/[Eternet2/5], n77-e2-6/[Ether...	vlan-3100
provider	N77-e2-5/[Eternet2/5], n77-e2-6/[Ether...	vlan-3100

Common Issues

2) Next hop IP is not defined




```
Leaf2# show endpoint vlan 52
Legend:
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
 L - local            E - shared-service
+-----------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+-----------------------------------+---------------+-----------------+--------------+-------------+
52                                        vlan-3100    0000.2626.2626 L                    eth1/24
ciscoLive:v1                              vlan-3100        172.16.1.6 L                    eth1/24
52                                        vlan-3100    0000.2525.2525 L                    eth1/23
ciscoLive:v1                              vlan-3100        172.16.1.5 L                    eth1/23
```

Common issues

3) Think about routing and PCTags

```
Leaf1# show ip route vrf ciscoLive:v1
IP Route Table for VRF "ciscoLive:v1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.0.0.0/8, ubest/mbest: 1/0
    *via 10.0.72.64%overlay-1, [200/0], 3d19h, bgp-65000, internal, tag 65000
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.120.34%overlay-1, [1/0], 00:00:08, static, tag 4294967294
192.168.2.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.120.34%overlay-1, [1/0], 5d02h, static, tag 4294967294
```

```
leaf1 # vsh -c “show system internal policy-mgr prefix” | egrep ciscoLive
2490374 32     0x20          Up     ciscoLive:v1                                    10.0.0.0/8    32777    True    True    False
2490374 32     0x20          Up     ciscoLive:v1                                     0.0.0.0/0    15       True    True    False
```

Additional Features

Managed Service Graph Tip

L4-L7 Devices - ASAv-2

Policy | Parameters | Faults | History

General

Managed: ☑

Name: ASAv-2

Alias:

Device Package: CISCO-ASA-1.2

Service Type: Firewall

Device Type: VIRTUAL

Trunking Port: ☐

VMM Domain: VMware/shared-DVS

Promiscuous Mode: ☑

Context Aware: Multiple | Single

Function Type: GoThrough | GoTo | L1 | L2

Credentials

Username: admin

Password: ••••••••

Confirm Password: ••••••••

Configuration State

Configuration Issues:

Devices State: init

Fault Code: F0324

Severity: major

Last Transition: 2019-06-07T20:02:59.061-04:00

Lifecycle: Soaking

Affected Object: **uni/ten-[uni/tn-cs]-scriptHandlerState/cDevState-[uni/tn-cs/lDevVip-ASAv-2/cDev-ASAv-2]/devHealth-[uni/tn-cs/lDevVip-ASAv-2/cDev-ASAv-2]**

Description: Fault delegate: Device configuration resulted in *Major script error : Connection error : 401 Client Error: Unauthorized* for ASAv-2 on device ASAv-2 in cluster ASAv-2 in tenant cs

Type: Config

Cause: configuration-failed

Change Set: faultCode:20, faultMessage:Major script error : Connection error : 401 Client Error: Unauthorized, faultSeverity:major, name:ASAv-2

Created: 2019-06-07T20:02:59.061-04:00

Code: F0324

Number of Occurrences: 1

Original Severity: major

Previous Severity: major

Highest Severity: major

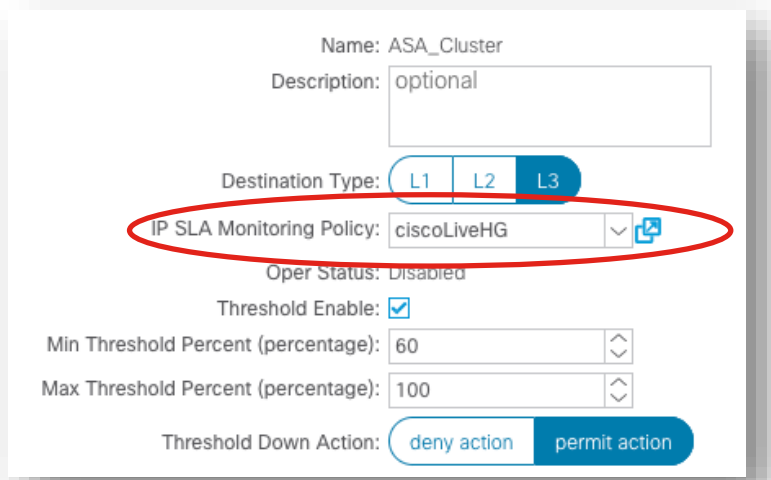
Managed Service Graph Tip

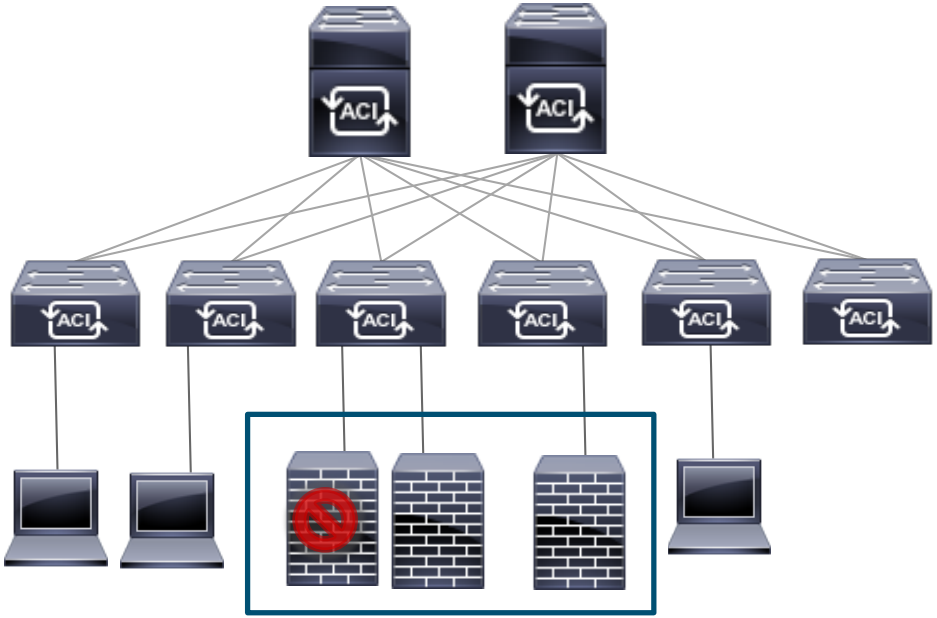
```
a-apic1# less /data/devicescript/CISCO.ASA.1.2/log/apic.log

2019-04-11 14:24:48.162132 DEBUG Thread-10 89536 [14.2.104.107, 5105] request: clusterAudit pformat={'device': {'dn': u'uni/tn-cs/lDevVip-ASAv-
2', 'name': 'ASAv-2', 'virtual': True, 'vdevs': [], 'devs': {'ASAv-2': {'dn': u'uni/tn-cs/lDevVip-ASAv-2/cDev-ASAv-2', 'host': '14.2.104.107',
'virtual': True, 'state': 0, 'version': '9.7(1)4', 'contextaware': False, 'port': 443, 'creds': {'username': 'apic', 'password': '<hidden>'}}},
'host': '14.2.104.107', 'contextaware': False, 'funcmode': 2, 'port': 443, 'creds': {'username': 'apic', 'password': '<hidden>'}}, 'args':
({(12, '', 'inside'): {'state': 0, 'cifs': {'ASAv-2': 'GigabitEthernet0/1'}, 'label': 'int'}, (12, '', 'outside'): {'state': 0, 'cifs': {'ASAv-
2': 'GigabitEthernet0/0'}, 'label': 'ext'}}, {})}
2019-04-11 14:24:52.171643 DEBUG Thread-10 89539 [14.2.104.107, 5105] result: clusterAudit pformat={'stats': {'max': 4.012045860290527, 'num':
2, 'last': 4.009513854980469, 'avg': 4.010779857635498, 'min': 4.009513854980469}, 'result': {'faults': [([], 20,
"HTTPSConnectionPool(host='14.2.104.107', port=443): Max retries exceeded with url: /admin/exec/show%20mode (Caused by
ConnectTimeoutError(<requests.packages.urllib3.connection.VerifiedHTTPSConnection object at 0x7f29c8085350>, 'Connection to 14.2.104.107 timed
out. (connect timeout=4.0)'))")], 'state': 3}}
2019-04-11 14:24:52.173349 DEBUG Thread-10 89544 [None, None] Waiting for task
2019-04-11 14:24:52.177372 DEBUG MainThread 89545 [None, None] Recv num: 5106, type: 30, len: 359
2019-04-11 14:24:52.177670 DEBUG MainThread 89546 [None, None] Received: 359
2019-04-11 14:24:52.178360 DEBUG MainThread 89547 [None, None] Adding Task to queue: 0
2019-04-11 14:24:52.178480 DEBUG MainThread 89548 [None, None] Waiting for data


a-apic1# pwd
/data/devicescript/CISCO.ASA.1.2/
```

Folder per Device Package

Node Tracking

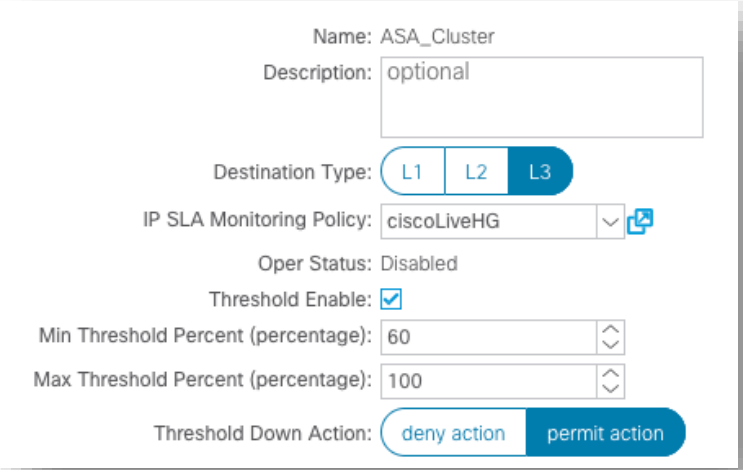
Leaf tracks state of service node using IP SLA policy. A fabric wide heartbeat informs other switches if a node fails

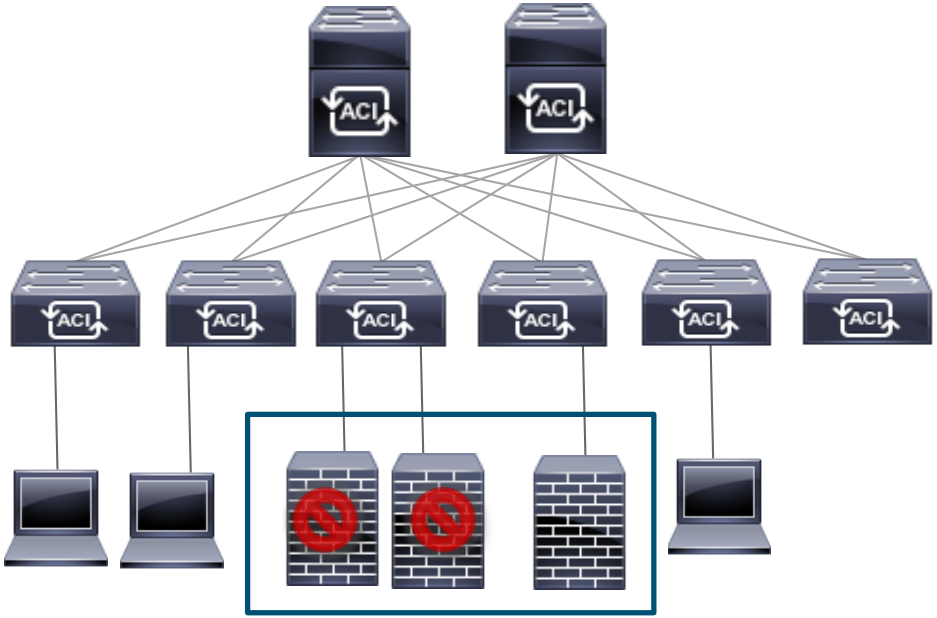




Node *Threshold Enable*

If a X number of nodes become unavailable, redirect can be disabled and traffic is either allowed or dropped



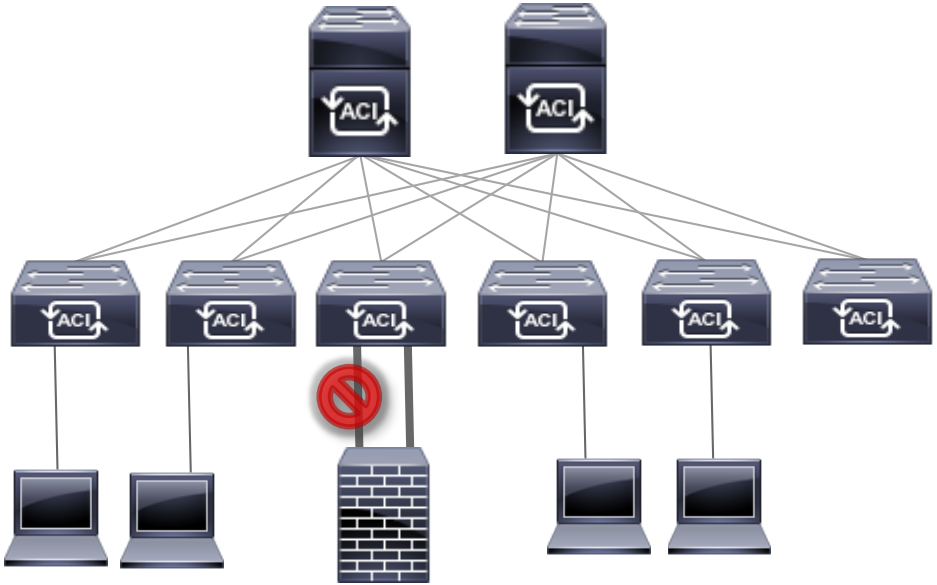


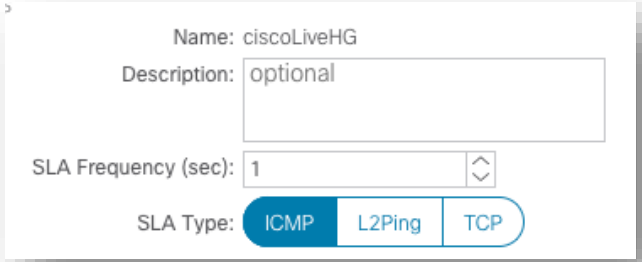
Health Groups

If a single interface on a two arm node fails, this node should no longer be used.

Inside and outside interface should be in same Health Group to disable the remaining interface if single interface fails

Support ICMP, TCP & L2Ping





IP	MAC	Health Group	Status
172.16.1.5	0000.2525.2525	GroupA	Enabled
172.16.1.6	0000.2626.2626	GroupA	Enabled

Agenda

- Overview
- How Service Graphs work
- Shadow EPGs
- Path of a Policy redirected packet
- Additional Features

Troubleshooting Cisco Application Centric Infrastructure

Troubleshooting Cisco Application Centric Infrastructure
Second Edition

Domenico Dastoli, Roland Ducomble, Minako Higuchi, Takuya Kishida, Jessica Kurtz, Joe LeBlanc, Gabriel Monroy, Austin Peacock, Pieter Schoenmaekers, Yuji Shimazaki, Ramses Smeyers, Joseph Young

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**