The bridge to possible

ACI L4-L7 Policy-Based Redirect (PBR) Deep Dive and tips

Minako Higuchi, Technical Marketing Engineer, Cloud Networking Business Group

Cisco Webex App

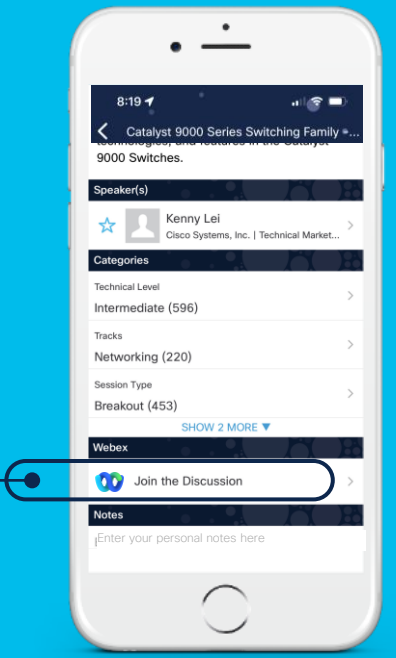
Questions?

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

How

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

Webex spaces will be moderated until February 24, 2023.



Session Objectives

- At the end of the session, the participants should be able to:
  - Understand ACI PBR use cases.
  - Understand how ACI PBR works.
  - Understand design considerations.
- What is not covered in this session.
  - Cloud ACI. We are going to focus on on-prem ACI.
- Initial assumption:
  - The audience already has a good knowledge of ACI main concepts: VRF, BD, EPG, ESG, L3Out, Contract, Multi-Pod, Multi-Site, Remote Leaf etc
- Note: This session uses ESGs mainly, but the PBR features are applicable to EPGs and uSeg EPGs.

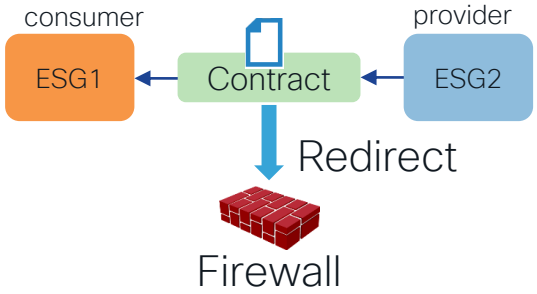
Agenda

- ACI PBR Use cases
- PBR Forwarding and zoning-rules
- FAQs and Advanced use cases
- Multi-location Data Centers

ACI PBR Use Cases

PBR (redirect) is one of the contract actions!

Permit, Deny, Redirect and Copy

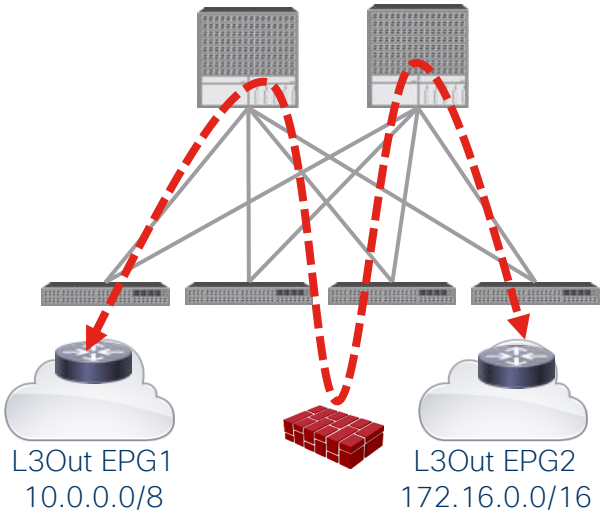


Where can we use PBR?

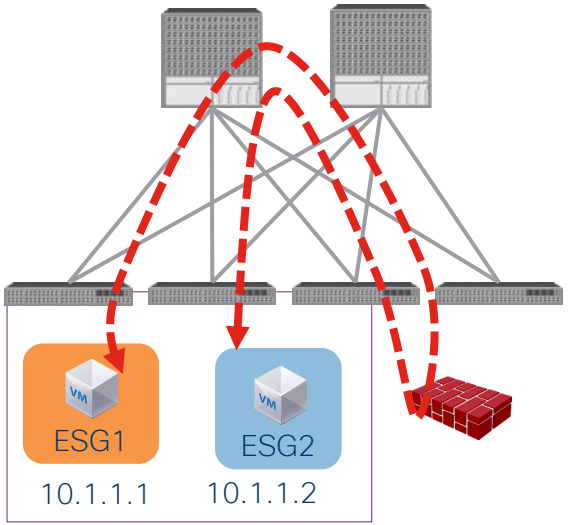
Wherever contracts can be applied!

PBR is a contract action. It's based on source, destination EPG/ESG and filter matching.

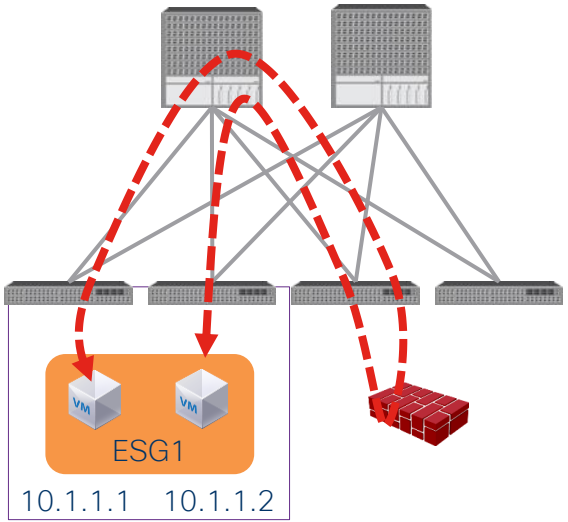
- Between EPGs or ESGs.
- Between L3Out EPGs.



- Between EPGs or ESGs in the same subnet.



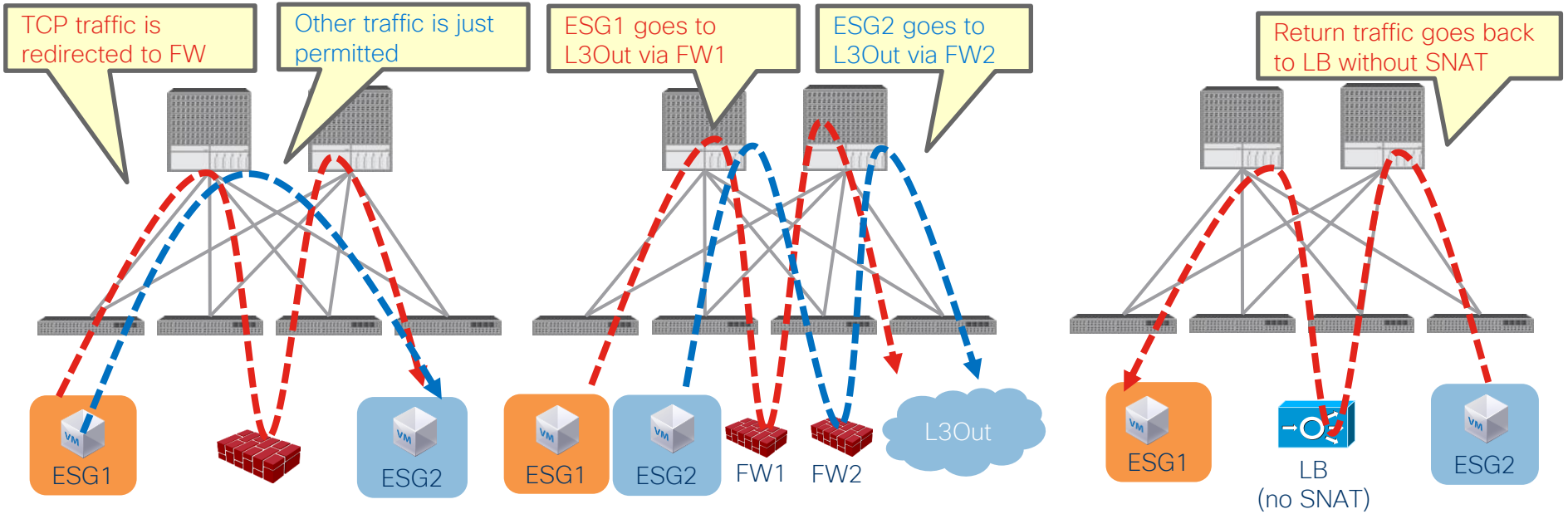
- Between endpoints in the same EPG or ESG.



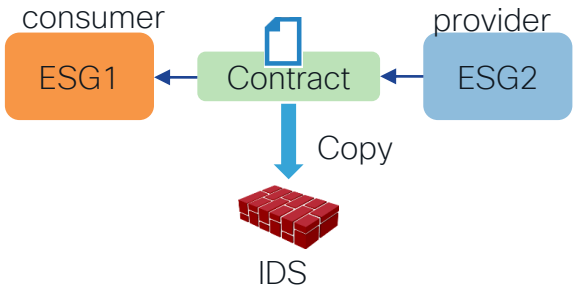
PBR use cases

PBR can be applied to each direction

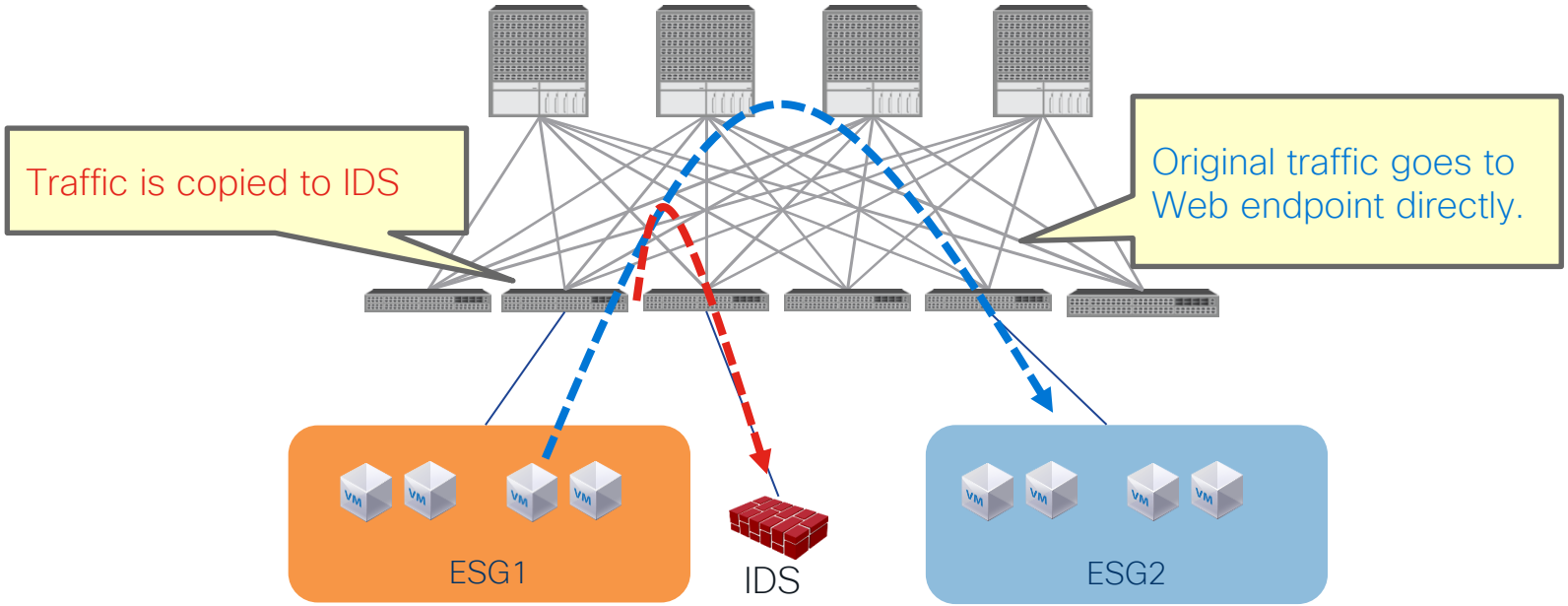
- Inspect specific traffic
- Use different Firewall
- LB without SNAT (uni-directional PBR)



ACI Copy service



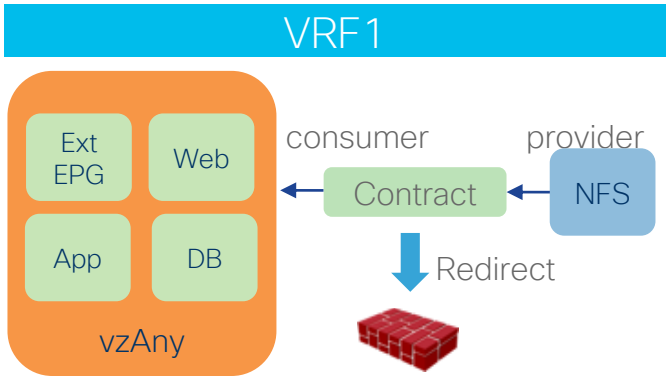
- Copy specific traffic instead of redirect.

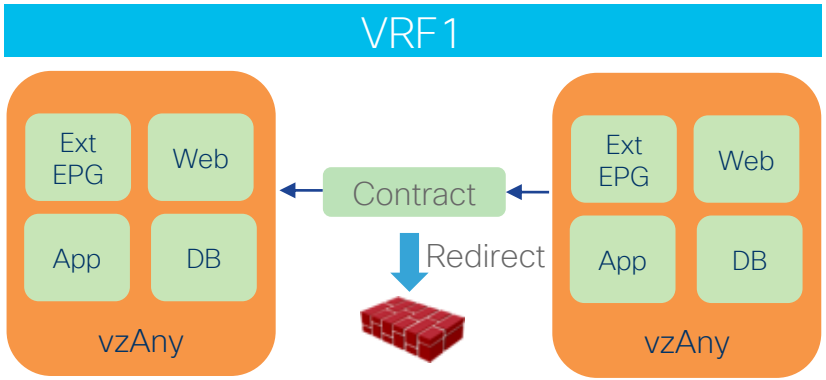


Important note

Please see
ACI Contract guide
for detail

- **ACI must be Layer 3**. (L2Out EPG is not supported)
- **VRF must be in enforced mode.** (PBR cannot be used in a VRF with unenforced mode)
  - If you want common permit or redirect rules in the VRF, you can use vzAny (All EPGs and ESGs in a VRF)
  - If you don't need contract enforcement for specific EPGs/ESGs in the VRF, you can still use Preferred Group.





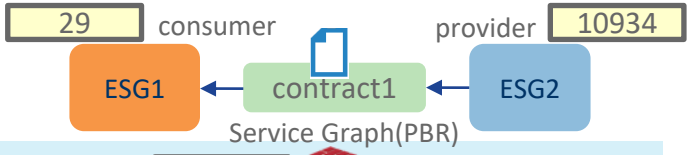
PBR Forwarding and zoning-rules

Zoning-rules (1-node Service Graph)

- Without PBR (permit action)


```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+----------------+---------+---------+------------------+----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |       Name       |  Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------------------+----------+----------------------+
<snip>
|    4157 |     29 |  10934 |       14 |         bi-dir | enabled | 2195459 | tenant1:contract1 |  permit  |    fully_qual(7)     |
|    4144 |  10934 |     29 |       14 | uni-dir-ignore | enabled | 2195459 | tenant1:contract1 |  permit  |    fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------------------+----------+----------------------+
```

- With PBR (Service Graph)

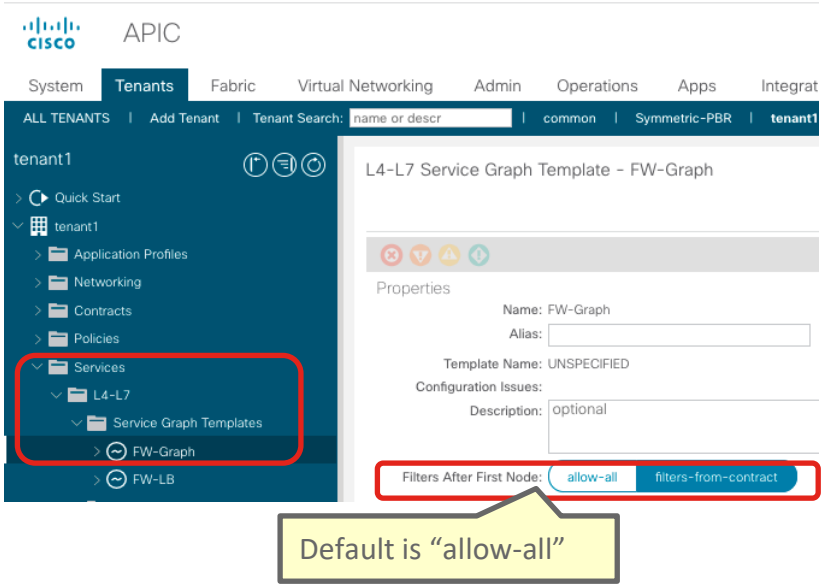


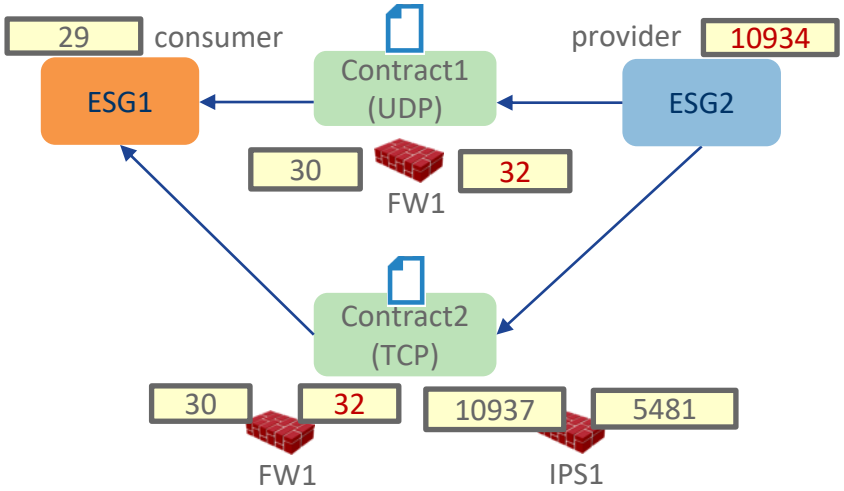

```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
<snip>
|    4144 |     29 |  10934 |       14 |         bi-dir | enabled | 2195459 |      | redir(destgrp-11) |    fully_qual(7)     |
|    4157 |  10934 |     29 |       14 | uni-dir-ignore | enabled | 2195459 |      | redir(destgrp-12) |    fully_qual(7)     |
|    4140 |     32 |  10934 |  default |        uni-dir | enabled | 2195459 |      |       permit      |    src_dst_any(9)    |
|    4136 |     30 |     29 |       14 |        uni-dir | enabled | 2195459 |      |       permit      |    fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
```

By default, unspecified default filter (any) is used for a zoning-rule entry without the consumer EPG.

Filter-from-contract

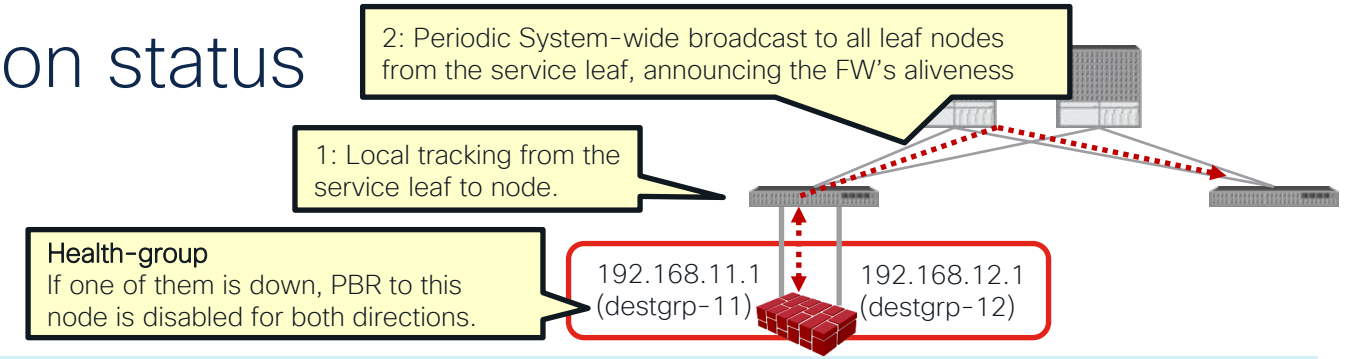
- To use the specific filter in the contract, “filters-from-contract” needs to be checked.
- Use case: use a different forwarding action based on the filter.





By default, forwarding actions are duplicated.
- 32-to-10934: permit (contract1 with UDP)
- 32-to-10934: redirect to IPS1 (contract2 with TCP)

PBR destination status



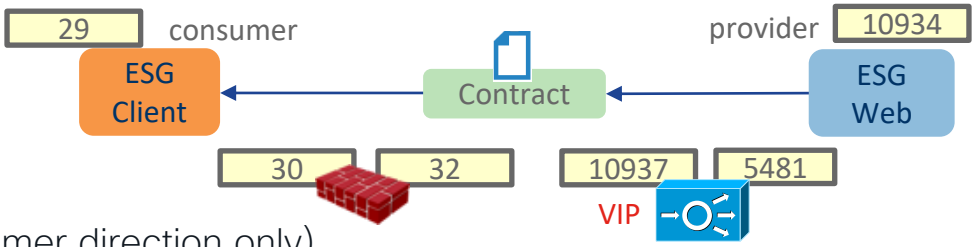

```
Pod1-Leaf1# show service redir info
========================================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  TRA: Tracking  | RES: Resiliency
========================================================================================================================================
List of Dest Groups
GrpID Name            destination                              HG-name           BAC  operSt     operStQual      TL   TH   HP   TRAC RES
===== ====            ===========                              ==============    ===  =======    ============    ===  ===  ===  ===  ===
11    destgrp-11      dest-[192.168.11.1]-[vxlan-2195459]      tenant1::HG1      N    enabled    no-oper-grp     0    0    sym  yes  no
12    destgrp-12      dest-[192.168.12.1]-[vxlan-2195459]      tenant1::HG1      N    enabled    no-oper-grp     0    0    sym  yes  no


List of destinations
Name                                     bdVnid          vMac               vrf             operSt     operStQual      HG-name
====                                     ======          ====               ====            =====      ==========      =======
dest-[192.168.11.1]-[vxlan-2195459]      vxlan-16678782  00:50:56:AF:6C:16  tenant1:VRF1    enabled    no-oper-dest    tenant1::HG1
dest-[192.168.12.1]-[vxlan-2195459]      vxlan-16121790  00:50:56:AF:DF:55  tenant1:VRF1    enabled    no-oper-dest    tenant1::HG1

List of Health Groups
HG-Name                                  HG-OperSt  HG-Dest                                  HG-Dest-OperSt
=======                                  =========  =======                                  ==============
tenant1::HG1                             enabled    dest-[192.168.11.1]-[vxlan-2195459]]     up
                                                    dest-[192.168.12.1]-[vxlan-2195459]]     up
```

Zoning-rules (2-nodes Service Graph)

- With Service Graph (PBR)
  - First node: FW (PBR for both directions)
  - Second node: LB (PBR for provider to consumer direction only)



- Consumer to provider direction
- Provider to consumer direction

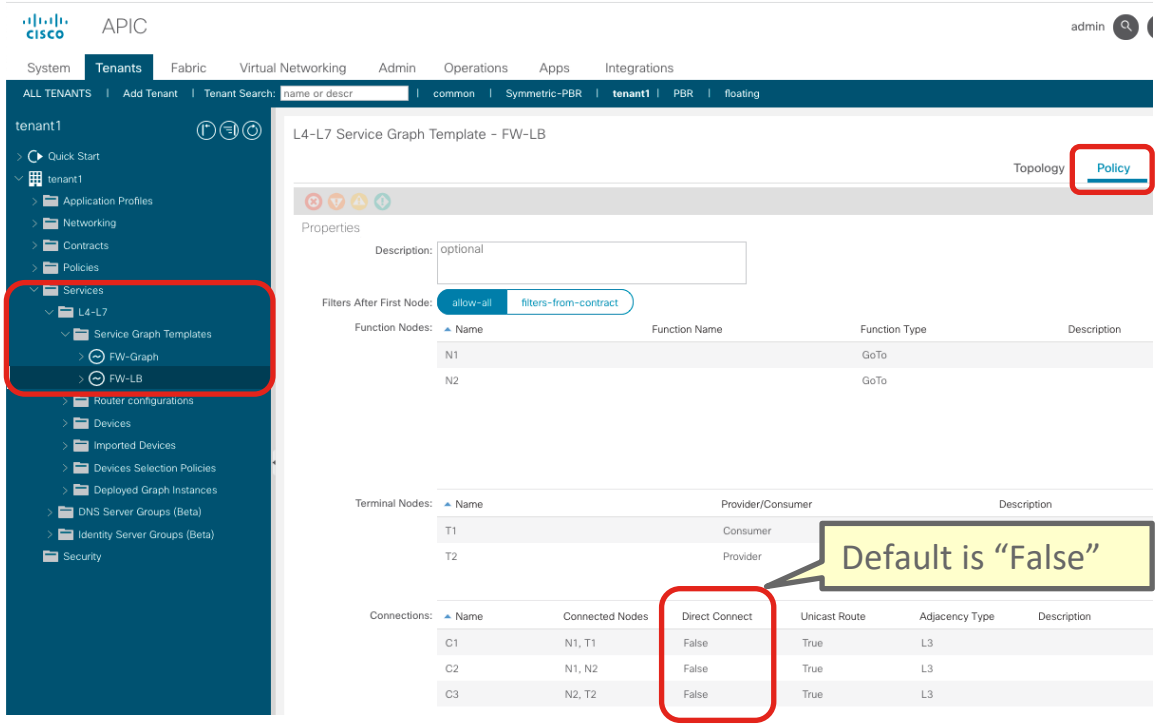
```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+-----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |        Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+-----------------------+
<snip>
|   4195  |   29   | 10937  |    14    |     bi-dir     | enabled | 2195459 |      | redir(destgrp-11) |    fully_qual(7)      |
|   4196  |   32   | 10937  | default  |    uni-dir     | enabled | 2195459 |      |       permit      |    src_dst_any(9)     |
|   4193  |  5481  | 10934  | default  |    uni-dir     | enabled | 2195459 |      |       permit      |    src_dst_any(9)     |
|   4198  | 10934  |   29   |    14    |    uni-dir     | enabled | 2195459 |      | redir(destgrp-17) |    fully_qual(7)      |
|   4181  | 10937  |   29   |    14    | uni-dir-ignore | enabled | 2195459 |      | redir(destgrp-12) |    fully_qual(7)      |
|   4194  |   30   |   29   |    14    |    uni-dir     | enabled | 2195459 |      |       permit      |    fully_qual(7)      |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+-----------------------+
```

To permit traffic from the provider EPG to the LB (10934 to 5481), Direct Connect option must be enabled.

Direct Connect (False by default)

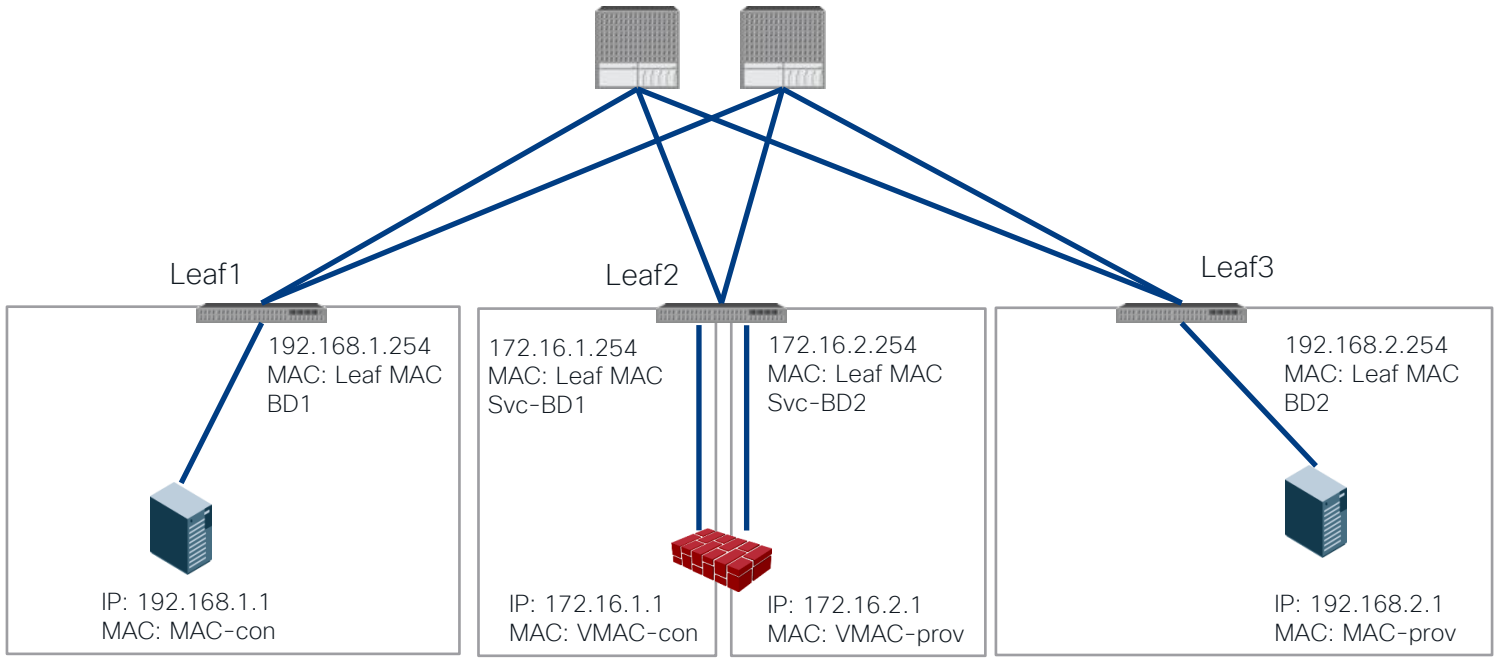
Direct Connect must be “True” for communication between the consumer/provider and the PBR destination.

- Tenant > Services > L4-L7 > Service Graph templates > Service Graph_NAME > Policy



How forwarding works

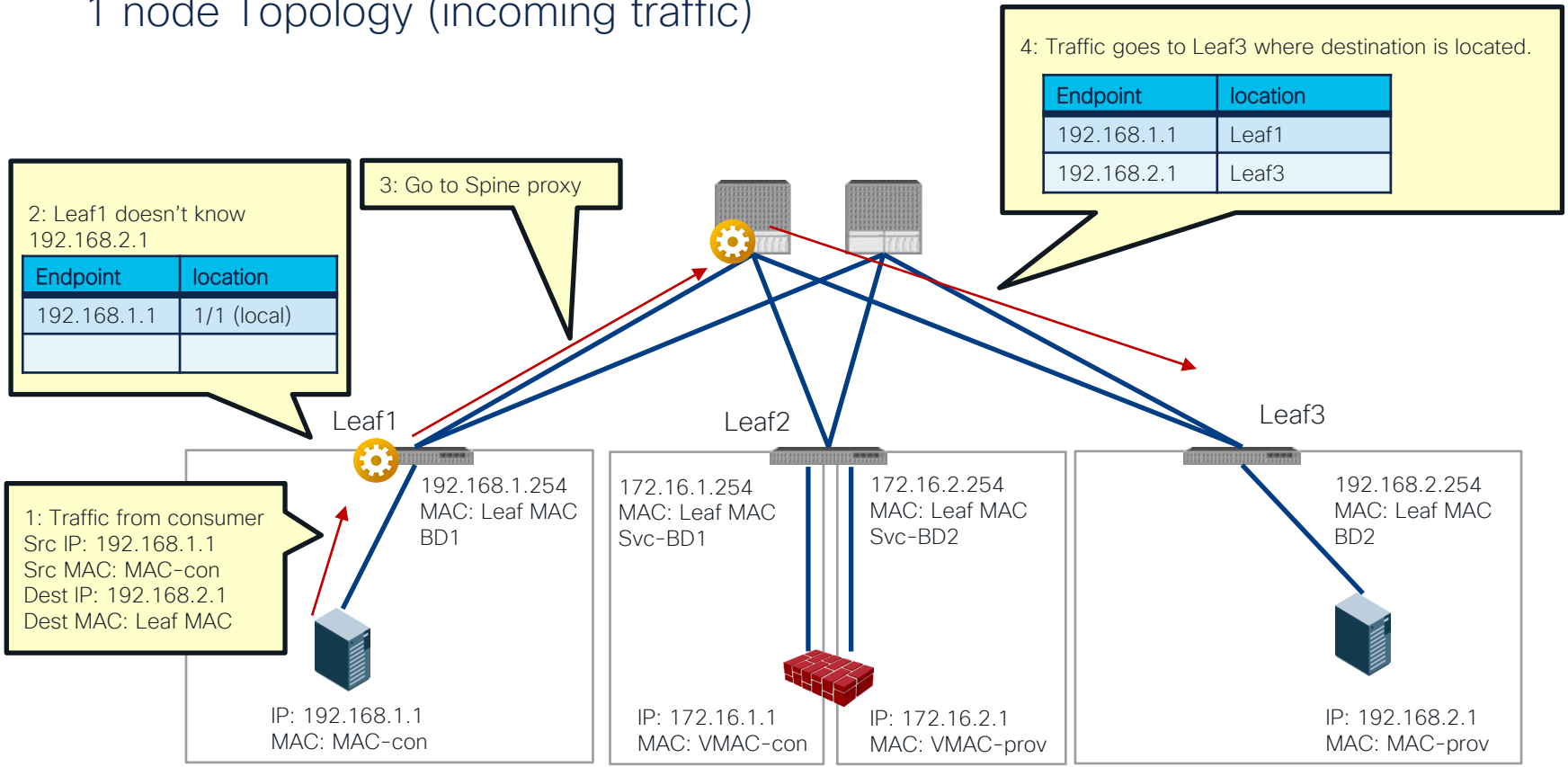
1 node Topology



How forwarding works

1 node Topology (incoming traffic)

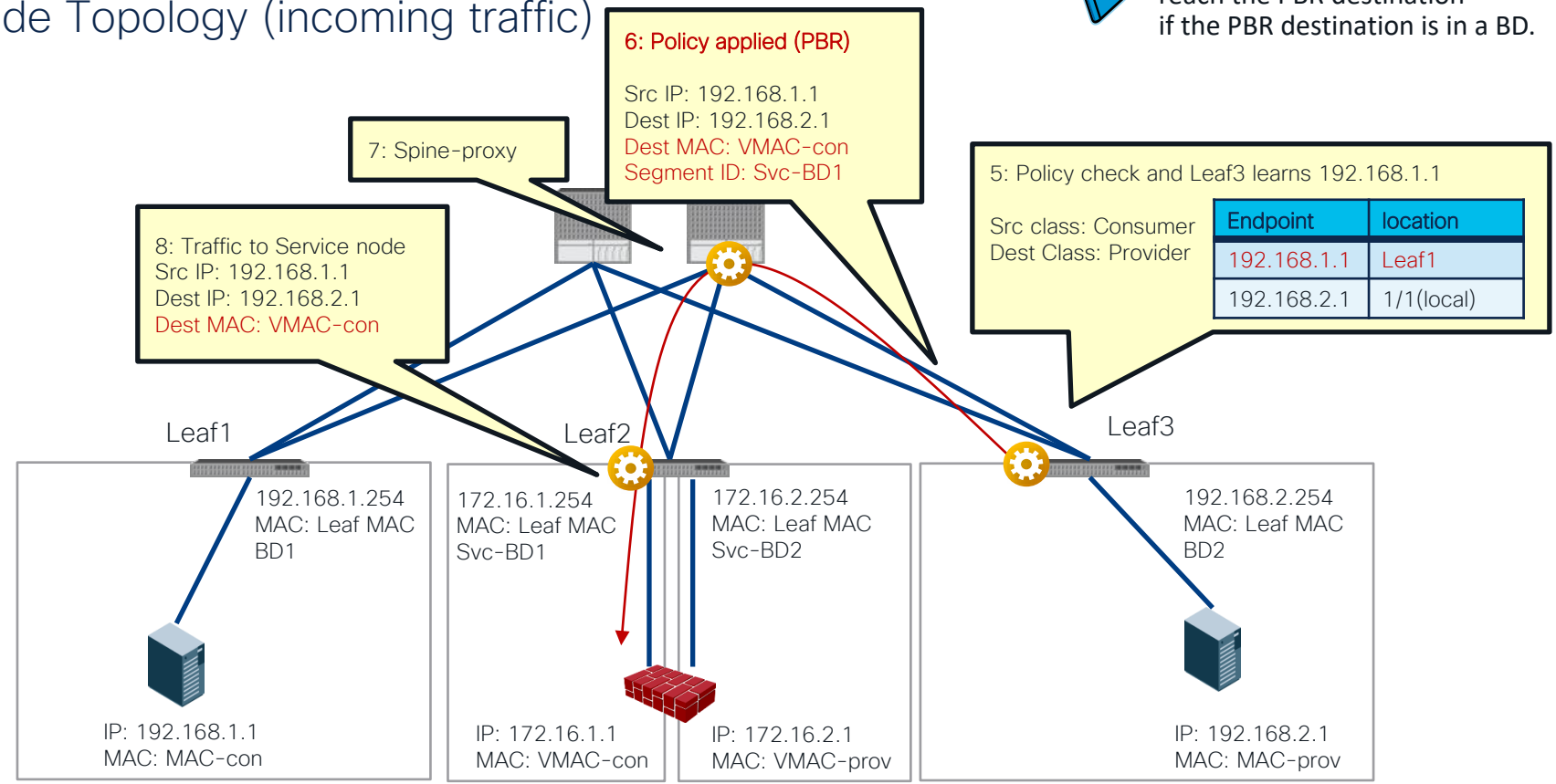
= VXLAN Encap/Decap



How forwarding works

1 node Topology (incoming traffic)

Leaf applies policy.
It's always spine-proxy to reach the PBR destination if the PBR destination is in a BD.

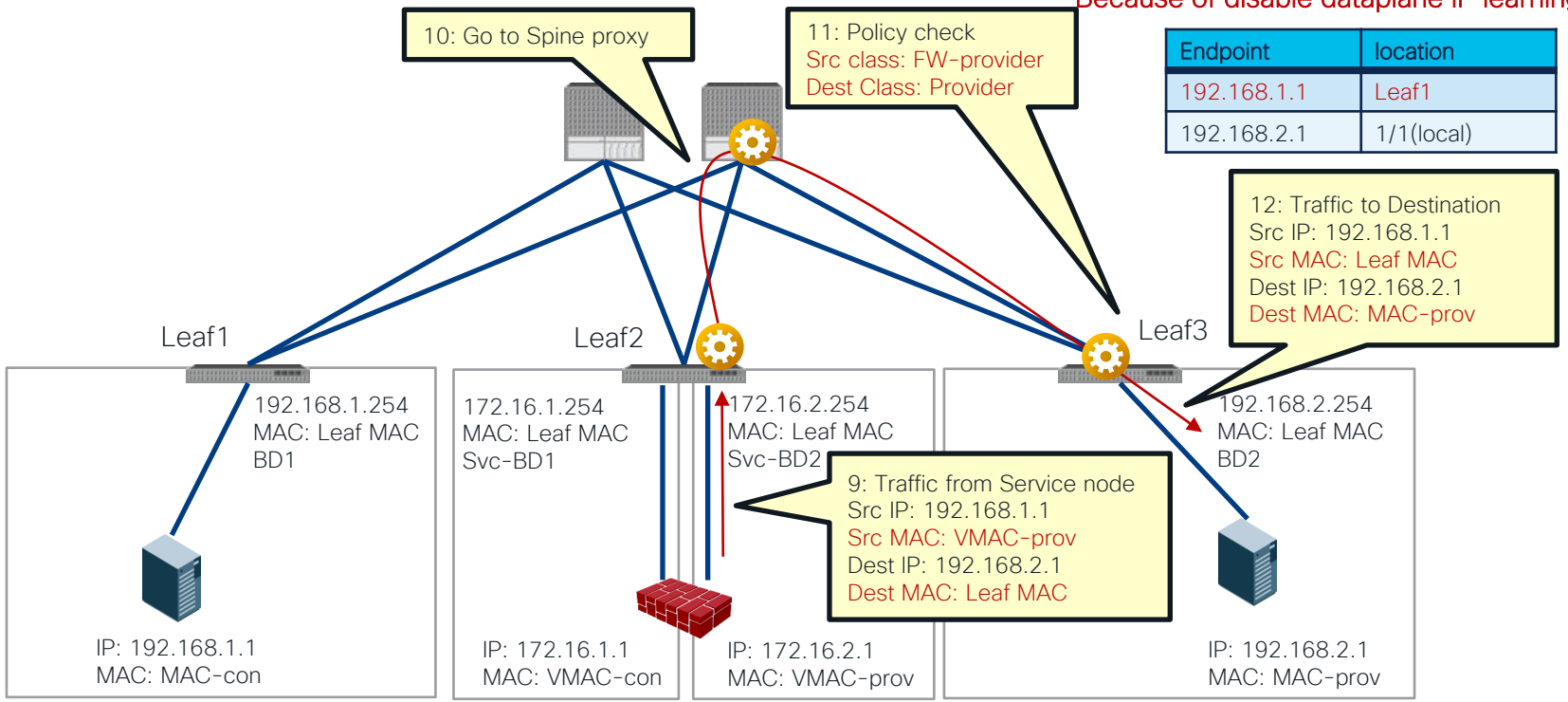


How forwarding works

1 node Topology (incoming traffic)

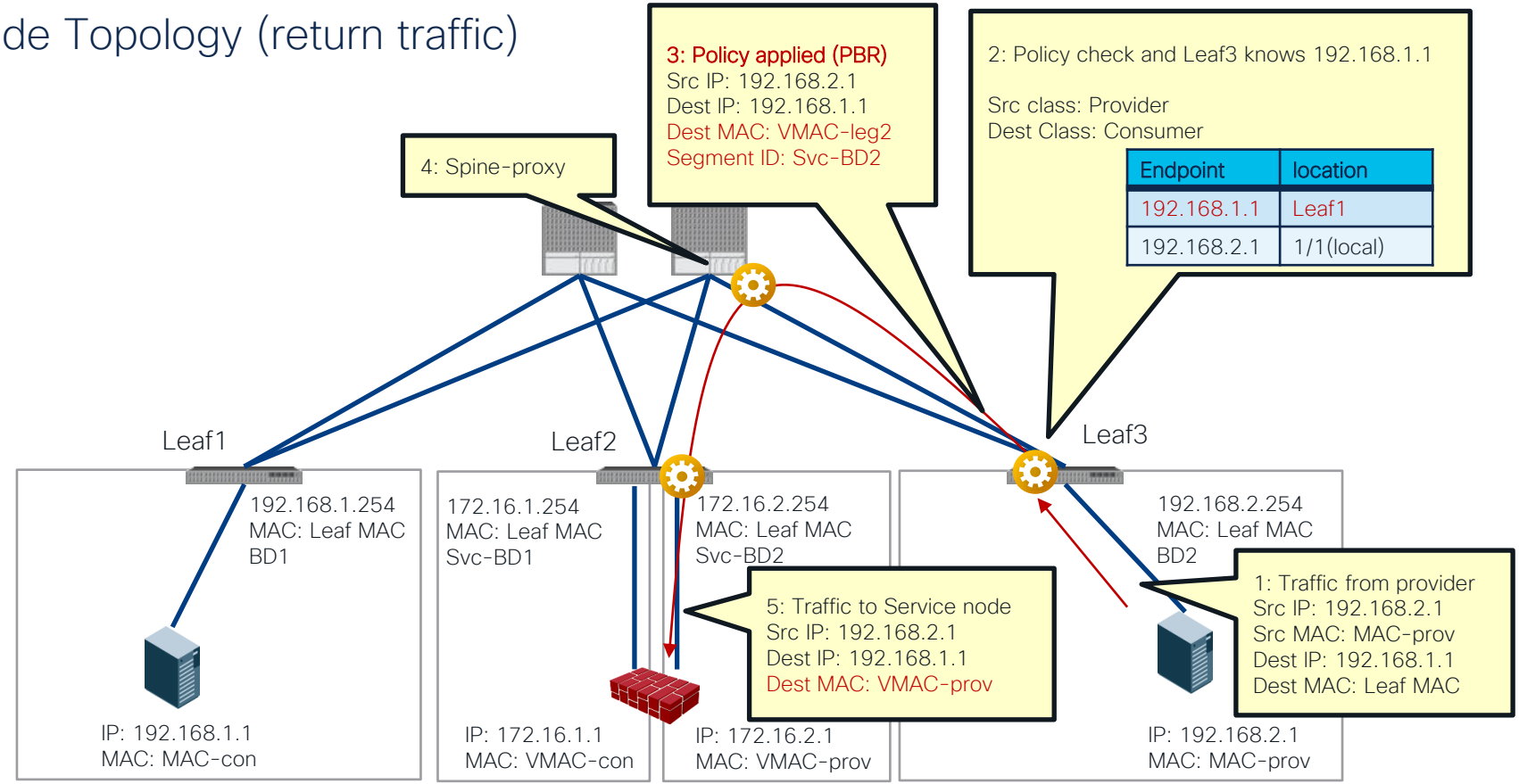
Dataplane IP learning
Is automatically disabled
for the service EPG.
(starting from 3.1)

Leaf3 doesn't re-learn 192.168.1.1 here
Because of disable dataplane IP learning



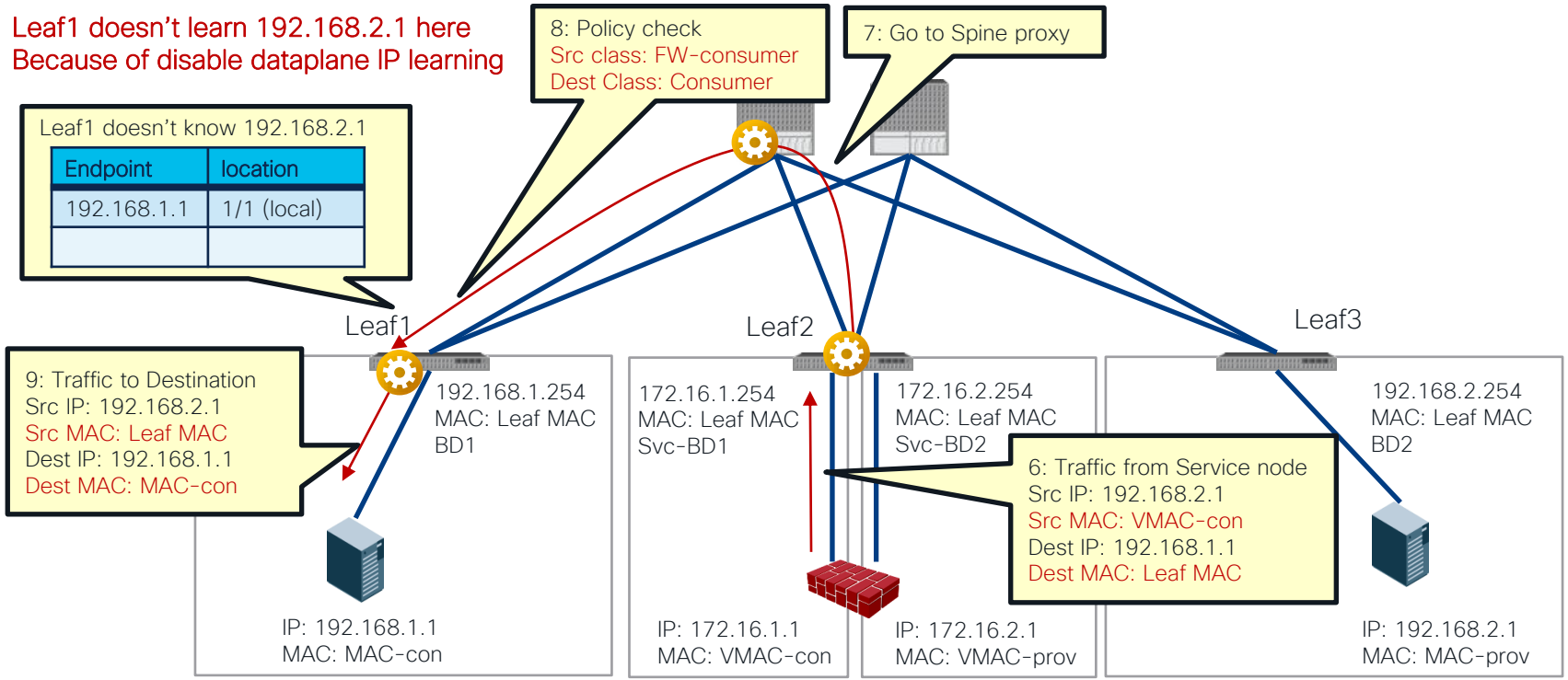
How forwarding works

1 node Topology (return traffic)



How forwarding works

1 node Topology (return traffic)



Where is the policy applied?

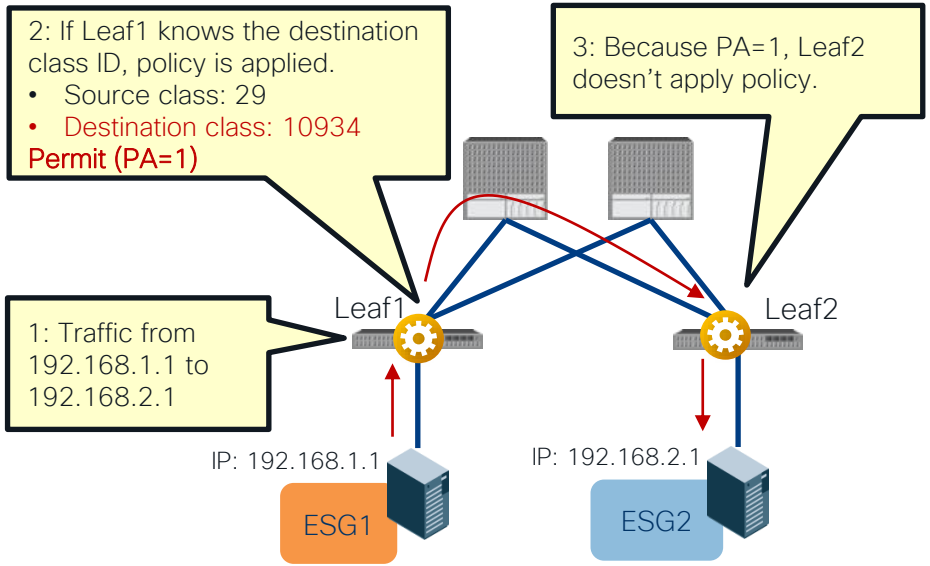
Please see ACI Contract guide for detail

Scenario	VRF enforcement mode	Consumer	Provider	Policy enforced on
Intra-VRF	Ingress/egress	EPG	EPG	• If destination endpoint is learned: ingress leaf • If destination endpoint is not learned: egress leaf
	ingress	EPG	L3Out EPG	Consumer leaf (non-border leaf)
	ingress	L3Out EPG	EPG	Provider leaf (non-border leaf)
	egress	EPG	L3Out EPG	Border leaf -> non-border leaf traffic • If destination endpoint is learned: border leaf • If destination endpoint is not learned: non-border leaf Non-border leaf-> border leaf traffic • Border leaf
	egress	L3Out EPG	EPG	
	Ingress/egress	L3Out EPG	L3Out EPG	Ingress leaf
Inter-VRF	Ingress/egress	EPG	EPG	Consumer leaf
	Ingress/egress	EPG	L3Out EPG	Consumer leaf (non-border leaf)
	Ingress/egress	L3Out EPG	EPG	Ingress leaf
	Ingress/egress	L3Out EPG	L3Out EPG	Ingress leaf

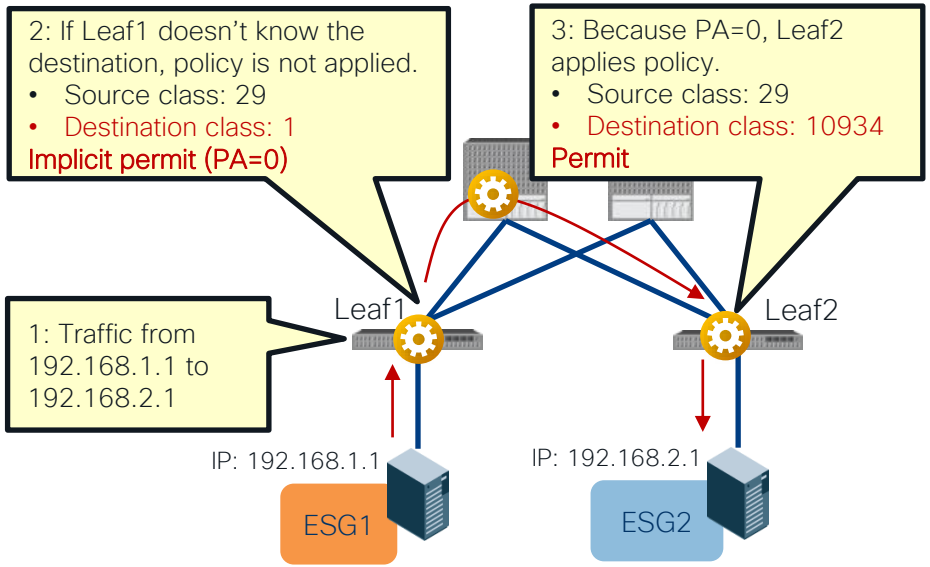
How ingress/egress leaf enforcement works?

Policy Applied (PA) bit

- Intra-VRF ESG-to-ESG ingress leaf enforcement



- Intra-VRF ESG-to-ESG egress leaf enforcement



Please see
ACI Contract guide
for detail

Contract Priority

Look at your zoning-rule priority and then filter priority!

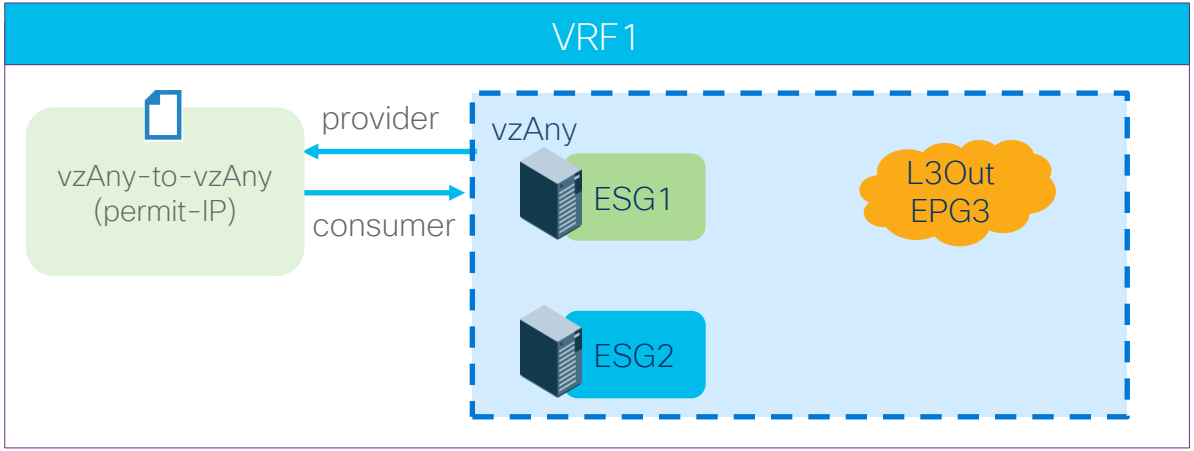
- More specific EPGs win over vzAny and preferred groups.
  - EPG-to-EPG wins over EPG-to-vzAny/vzAny-to-EPG that wins over vzAny-to-vzAny.
  - Specific source wins over specific destination. (EPG-to-vzAny wins over vzAny-to-EPG)

- Deny actions win. Specific protocol wins.
  - If the zoning-rule priority is the same, deny wins over redirect or permit action.
  - Between redirect and permit, a more specific protocol and a specific L4 protocol wins.

- More specific L4 rules win.
  - Specific filter wins over “any” filter.
  - Specific destination wins over specific source (“s-any to d-80” wins over “s-80 to d-any”)

Example 1

What's the forwarding action?

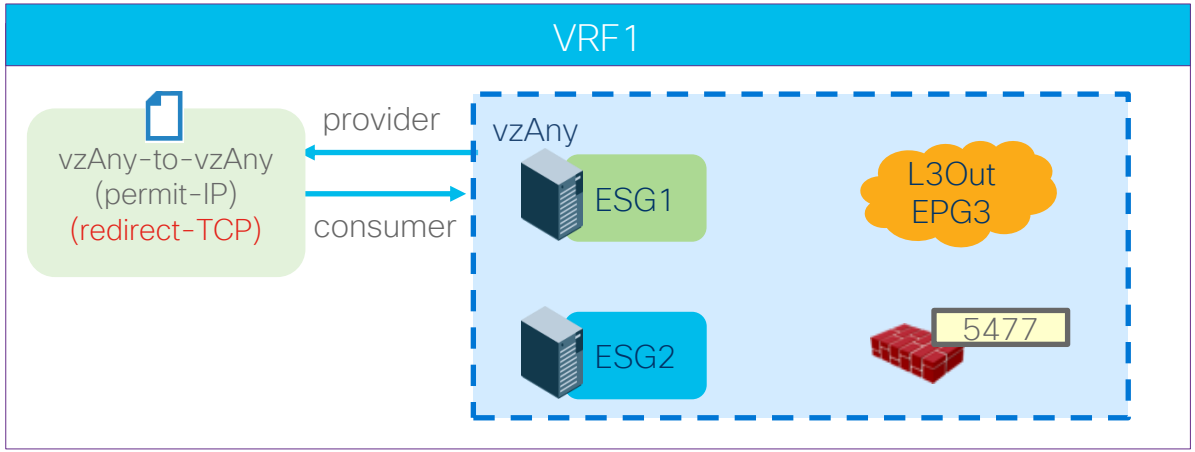


- ESG1-to-ESG2 (IP)
  Permit
- ESG1-to-L3OutEPG3 (IP)
  Permit
- ESG2-to-L3OutEPG3 (IP)
  Permit

```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+---------+---------+---------+------------------------+------------------+--------------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |          Name          |       Action     |         Priority         |
+---------+--------+--------+----------+---------+---------+---------+------------------------+------------------+--------------------------+
<snip>
|   4194  |   0    |   0    |    74    | uni-dir | enabled | 2195459 | tenant1:vzAny-to-vzAny |      permit      |    any_any_filter(17)    |
+---------+--------+--------+----------+---------+---------+---------+------------------------+------------------+--------------------------+
```

Example 2

What's the forwarding action?



- ESG1-to-ESG2 (TCP)
  Redirect
- ESG1-to-ESG2 (UDP)
  Permit

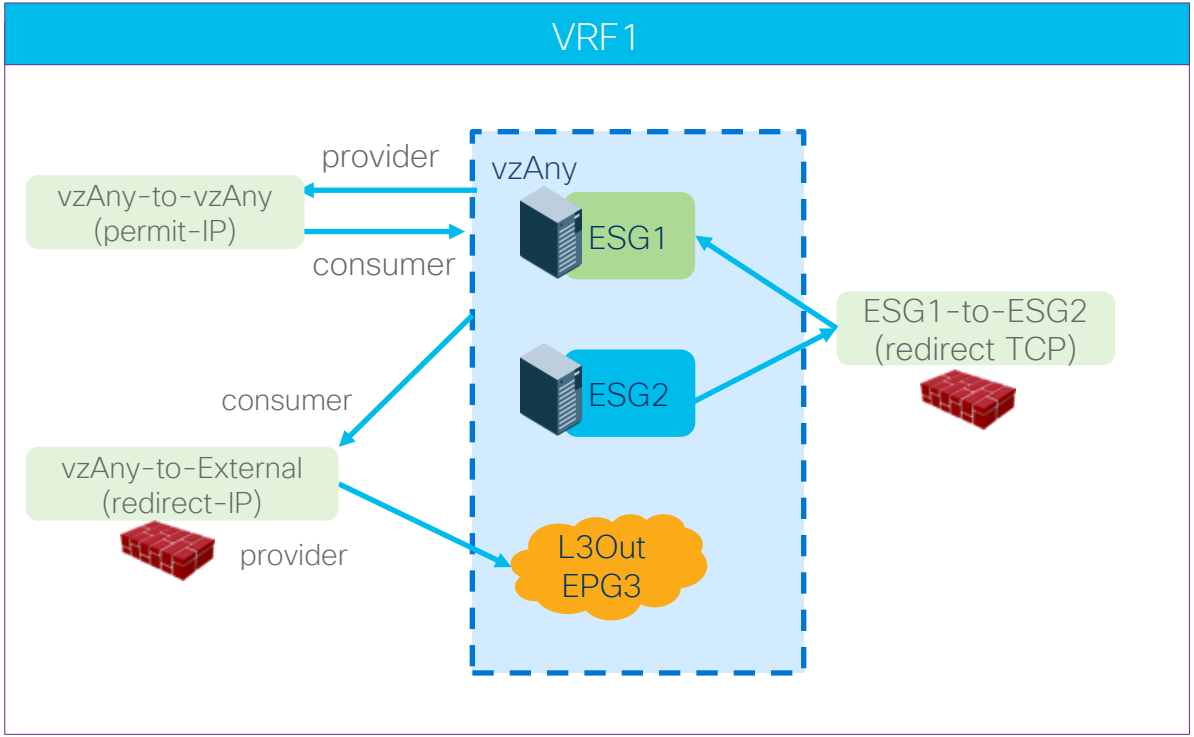
More specific L4 rules win though the zoning-rule priority is the same.

```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+---------+---------+---------+-----------------------+-------------------+-------------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |         Name          |       Action      |         Priority        |
+---------+--------+--------+----------+---------+---------+---------+-----------------------+-------------------+-------------------------+
<snip>
|   4194  |   0    |   0    |    74    | uni-dir | enabled | 2195459 | tenant1:vzAny-to-vzAny |       permit      |    any_any_filter(17)   |
|   4248  |   0    |   0    |    14    | uni-dir | enabled | 2195459 |                       | redir(destgrp-20) |    any_any_filter(17)   |
|   4186  |  5477  |   0    |    14    | uni-dir | enabled | 2195459 |                       |       permit      | shsrc_any_filt_perm(10) |
|   4193  |  5477  |   0    | default  | uni-dir | enabled | 2195459 |                       |       permit      |  shsrc_any_any_perm(11) |
+---------+--------+--------+----------+---------+---------+---------+-----------------------+-------------------+-------------------------+
```

In this example:
- Filter ID 74: Permit-IP all
- Filter ID 14: Permit-TCP all

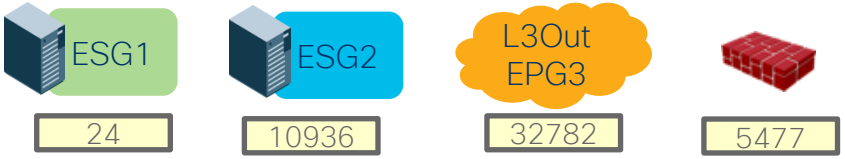
Example 3

What's the forwarding action?



- ESG1-to-ESG2 (TCP)
  Redirect
- ESG1-to-L3OutEPG3 (IP)
  Redirect
- ESG1-to-ESG2 (UDP)
  Permit

Example 3
Why?



- ESG-to-ESG (priority 7) wins over External-to-vzAny/vzAny-to-External (priority 13 or 14) that wins over vzAny-to-vzAny (priority 17) .

```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+----------------+---------+---------+-----------------------+-----------------+-------------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       | operSt  |  Scope  |         Name          |      Action     |         Priority        |
+---------+--------+--------+----------+----------------+---------+---------+-----------------------+-----------------+-------------------------+
<snip>
|   4194  |   0    |   0    |    74    |    uni-dir     | enabled | 2195459 | tenant1:vzAny-to-vzAny |      permit     |    any_any_filter(17)   |

|   4172  |   0    | 32782  |    74    |    uni-dir     | enabled | 2195459 |                       | redir(destgrp-1) |   any_dest_filter(14)   |
|   4196  |  5477  | 32782  | default  |    uni-dir     | enabled | 2195459 |                       |      permit      |      src_dst_any(9)     |
|   4201  | 32782  |   0    |    74    |    uni-dir     | enabled | 2195459 |                       | redir(destgrp-1) |    src_any_filter(13)   |
|   4242  |  5477  |   0    |    74    |    uni-dir     | enabled | 2195459 |                       |      permit      | shsrc_any_filt_perm(10) |

|   4186  |   24   | 10936  |    14    |     bi-dir     | enabled | 2195459 |                       | redir(destgrp-1) |      fully_qual(7)      |
|   4193  |  5477  | 10936  | default  |    uni-dir     | enabled | 2195459 |                       |      permit      |      src_dst_any(9)     |
|   4209  |  5477  |   24   |    14    |    uni-dir     | enabled | 2195459 |                       |      permit      |      fully_qual(7)      |
|   4248  | 10936  |   24   |    14    | uni-dir-ignore | enabled | 2195459 |                       | redir(destgrp-1) |      fully_qual(7)      |

+---------+--------+--------+----------+----------------+---------+---------+-----------------------+-----------------+-------------------------+
```

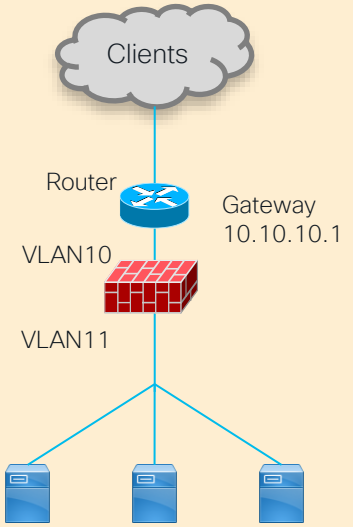
FAQs and advanced use cases

Should we use PBR for FW insertion?

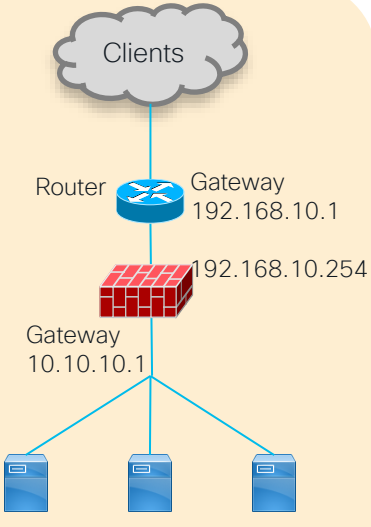
Typical Firewall Design Options

For your reference

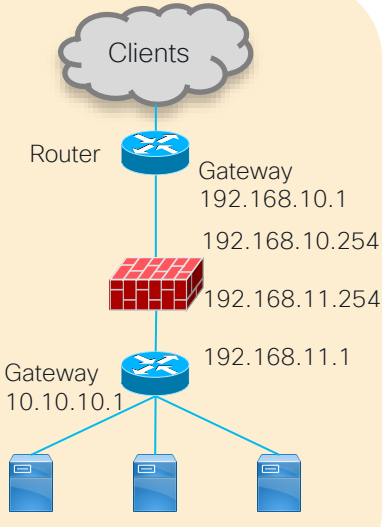
L2 FW
VLAN stitching



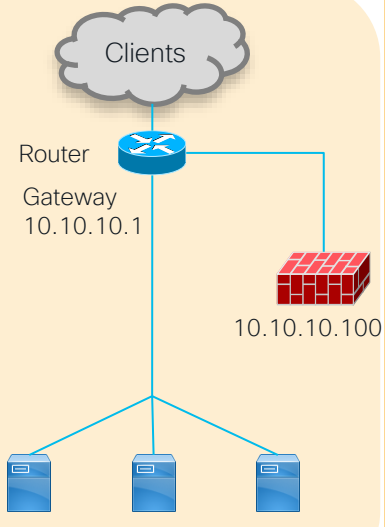
L3 FW
FW as gateway



L3 FW
Fabric as gateway
VRF sandwich



L3 FW
Fabric as gateway
PBR

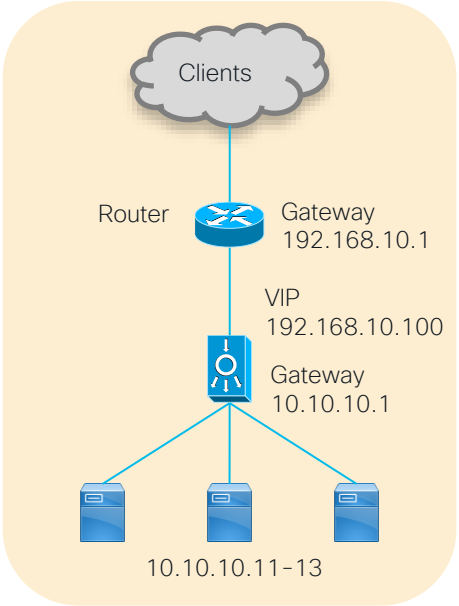


Should we use PBR for LB insertion?

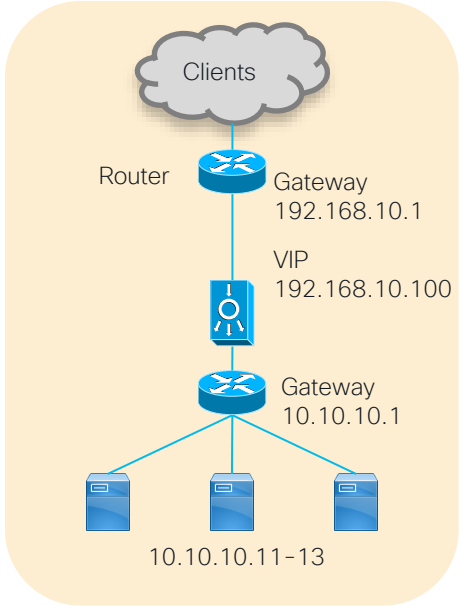
Typical Load Balancer Design Options

For your reference

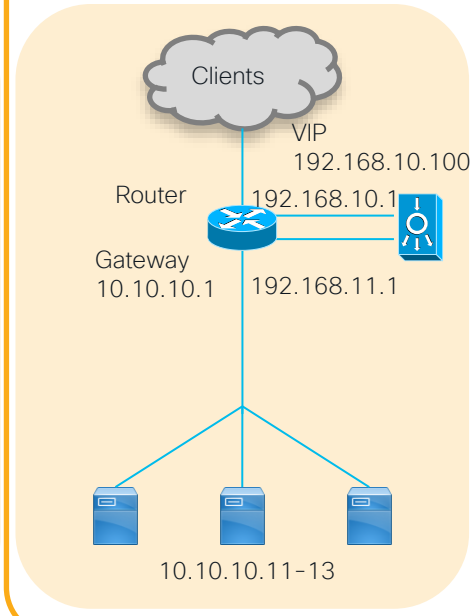
Two-arm (inline) LB as Gateway No SNAT/PBR



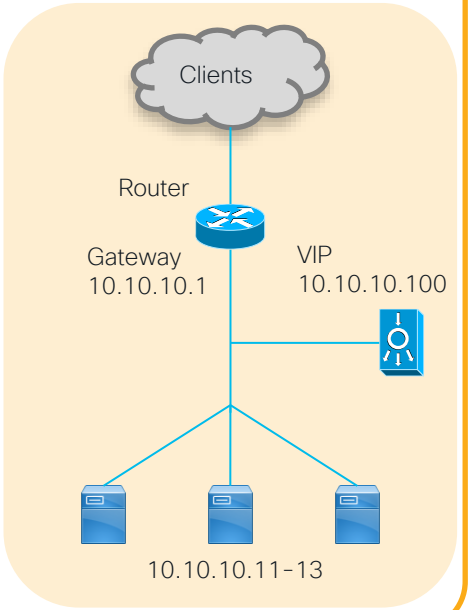
Two-arm (inline) Fabric as Gateway VRF sandwich



Two-arm Fabric as Gateway SNAT/PBR

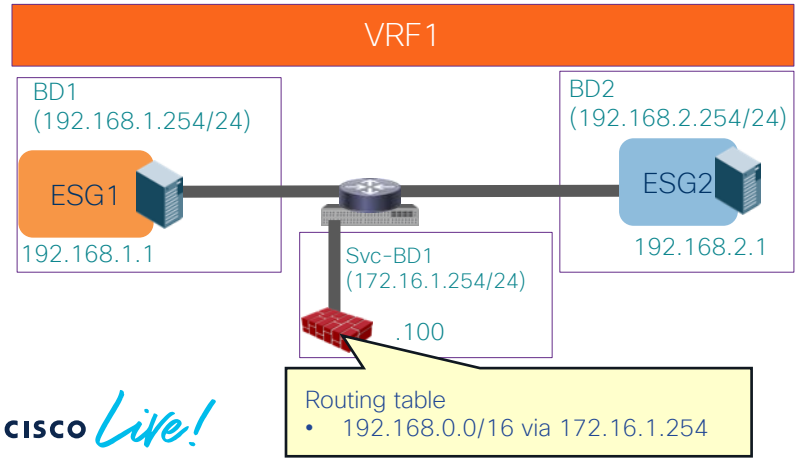


One-arm Fabric as Gateway DSR/SNAT/PBR

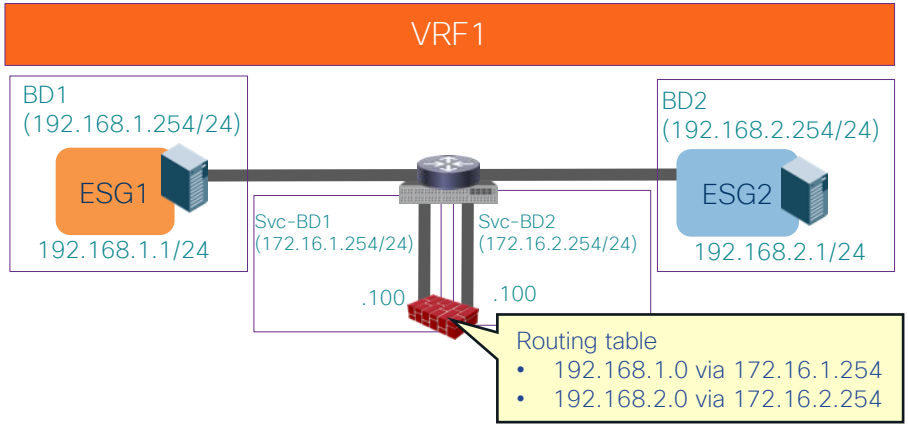


One-arm vs Two-arm?

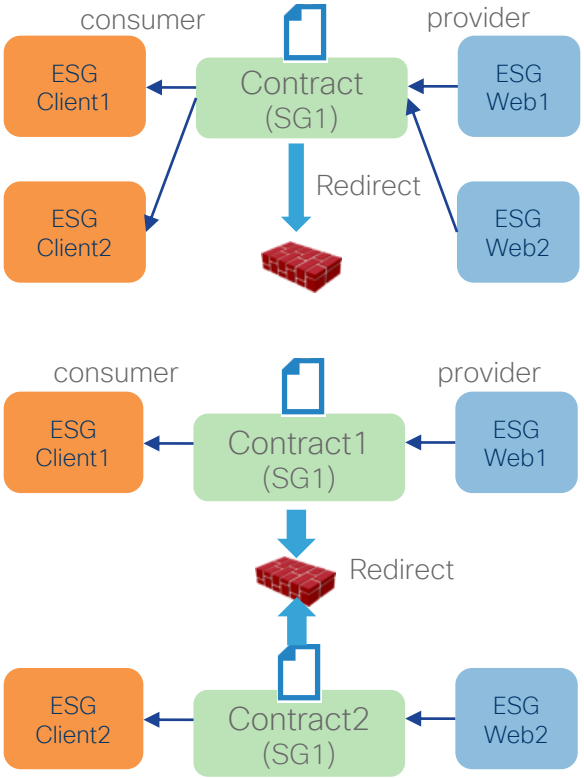
- One-arm
  - Simple routing design on service node.
  - One-arm must be used for intra-subnet or intra-EPG/ESG contract.
  - Some firewall doesn't allow intra-interface traffic by default.



- Two-arm
  - Need to manage routing design on service node.
  - Different security level on each interface.



Can we reuse same PBR destination multiple times?



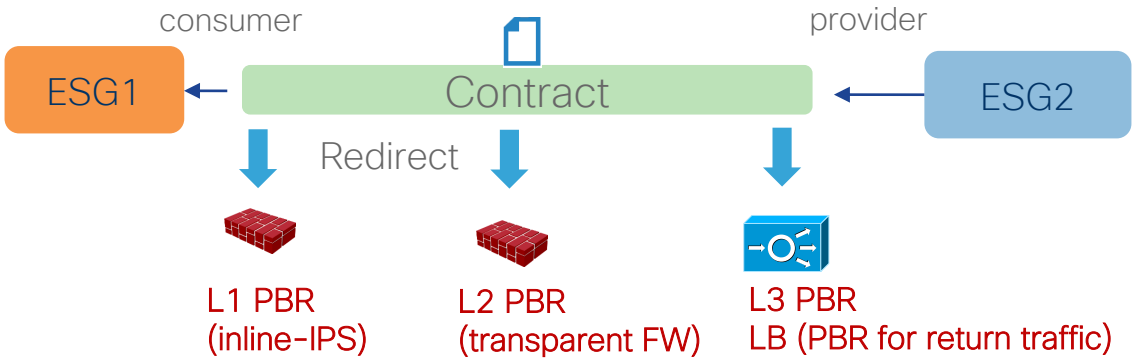
- Multiple consumer/provider ESGs/EPGs
- Multiple contracts can use the same PBR destination and Service Graph.

- Note
  - It could consume more TCAM resources if many EPGs consume and provide the same contract. The use of vzAny might be more efficient.
  - Depending on routing design, one-arm mode deployment may be required.

What types of devices can be PBR destinations?

L1/L2/L3 device

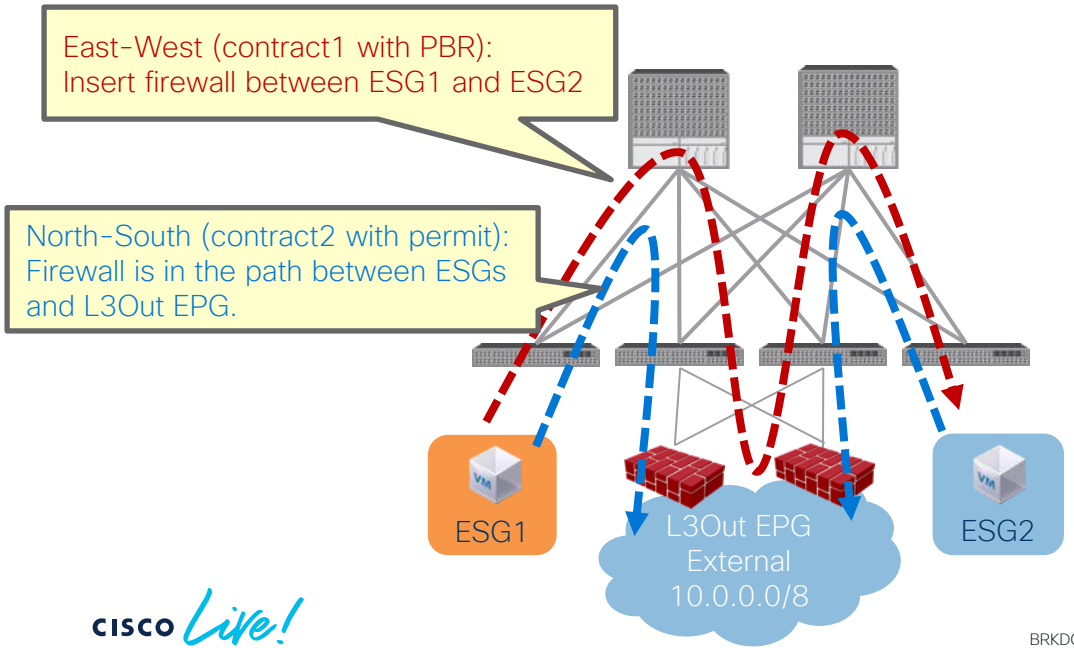
- Prior to ACI Release 5.0, a Symmetric PBR destination must be an L3 routed device (L3 PBR).
- Starting from ACI Release 5.0, L1/L2 Symmetric PBR is supported to insert L1/L2 devices.
  - Insert firewall without relying on BD/VLAN stitching.
  - L1/L2 service device BD must be dedicated BD that cannot be shared with other endpoints.
  - L1/L2/L3 PBR can be mixed in a service graph.

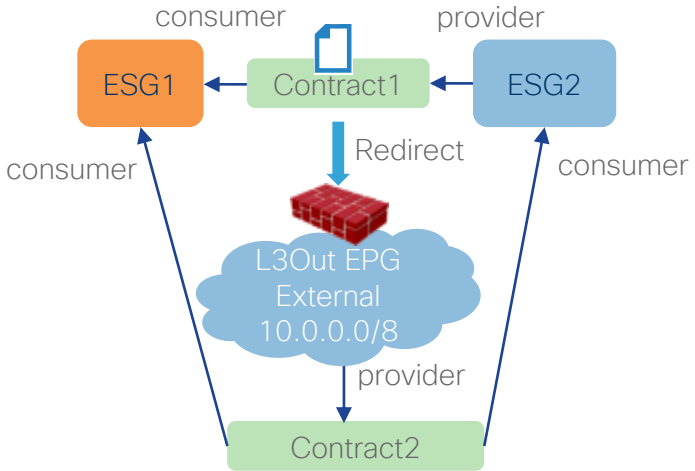


Can we use North-South firewall for East-West inspection?

PBR destination in an L3Out

- Prior to ACI Release 5.2, PBR destination must be in a BD.
- Starting from ACI Release 5.2, PBR destination can be in an L3Out.





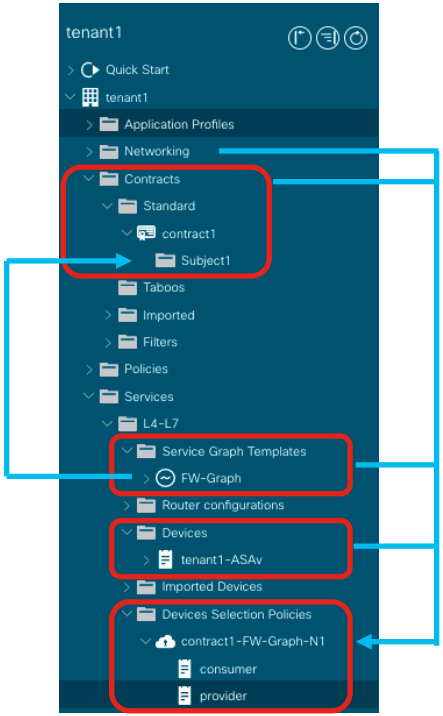
Advanced use cases

- Inter-VRF inter-tenant contract with PBR
  - The provider is in the common tenant. The consumer is in a user tenant.
  - The provider is in a user tenant. The consumer is in the common tenant.
  - The provider is in a user tenant. The consumer is in another user tenant.

- High Availability designs
  - Active/Standby
  - Active/Active
  - Independent Active nodes with Symmetric PBR

Inter-VRF, Inter-tenant contract with PBR

Configuration for PBR



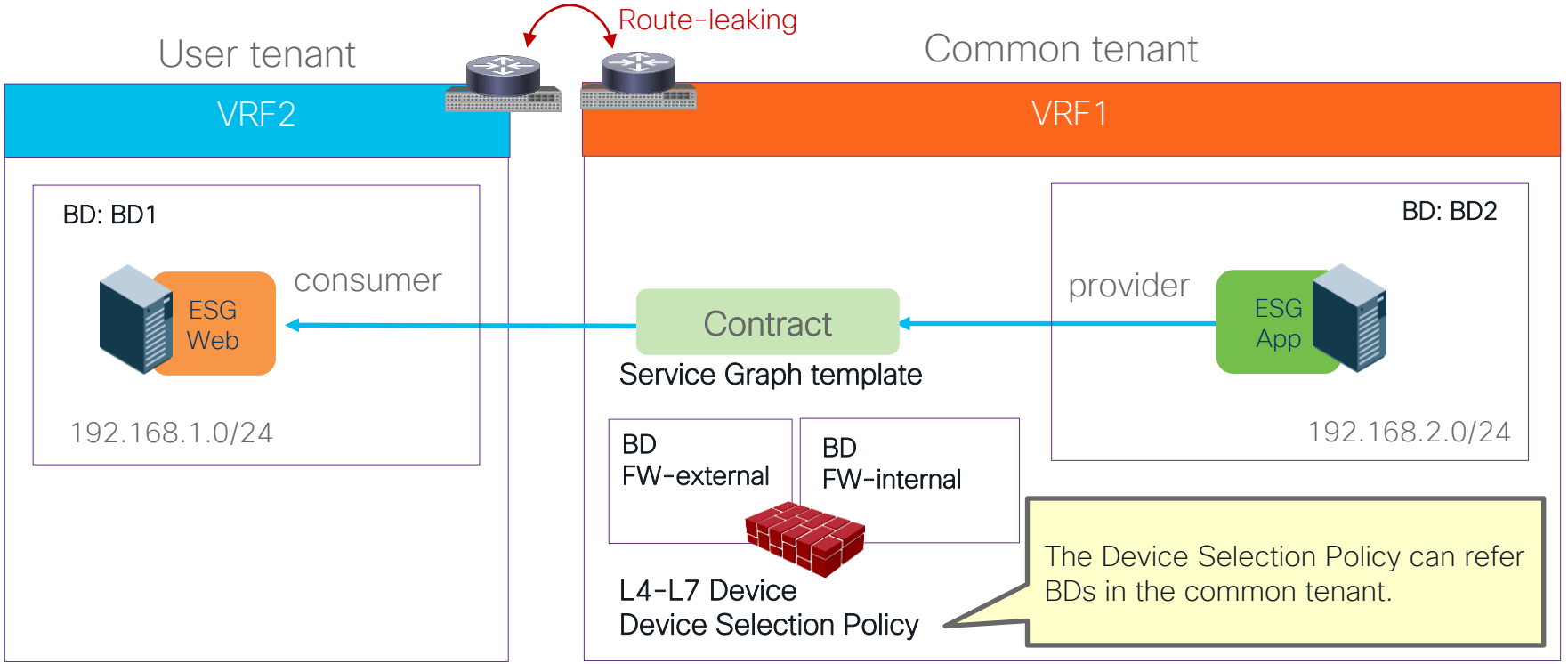
- Contract in the provider or common tenant
- Service Graph template
  - Service Graph template is attached to a contract subject
- L4-L7 Device
- Device Selection Policy
  - It's based on
    - Contract name
    - Service Graph template name
    - Node name in the Service Graph
  - Then, select BD/L3Out etc, for the consumer and provider connector of the service node.

Important consideration
- Device Selection policy must be in the provider tenant.
- Device Selection policy must be able to refer:
  - L4-L7 Device
  - The BD/L3Out for the service device

Note: vzAny cannot be a provider for an inter-VRF contract.

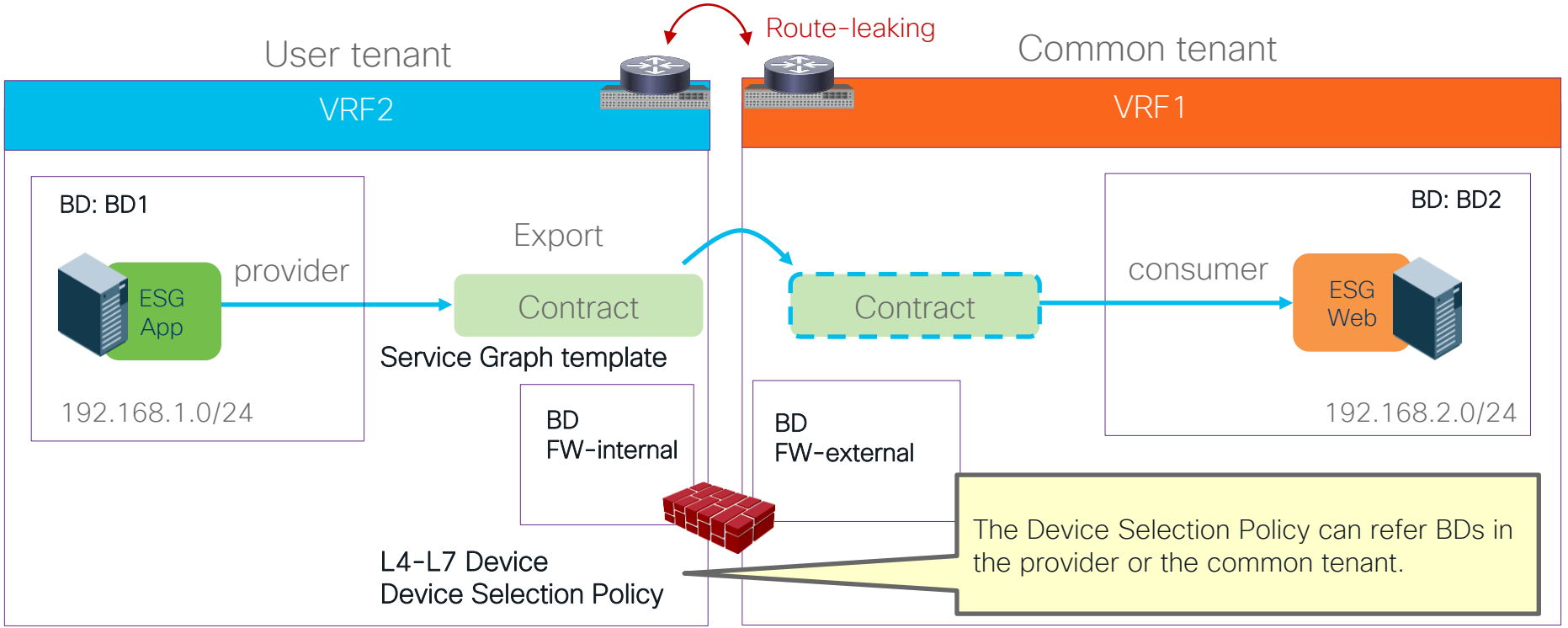
Inter-VRF, Inter-tenant contract with PBR

Example 1: The provider is in the common tenant. (BDs for PBR destinations are in the provider tenant)



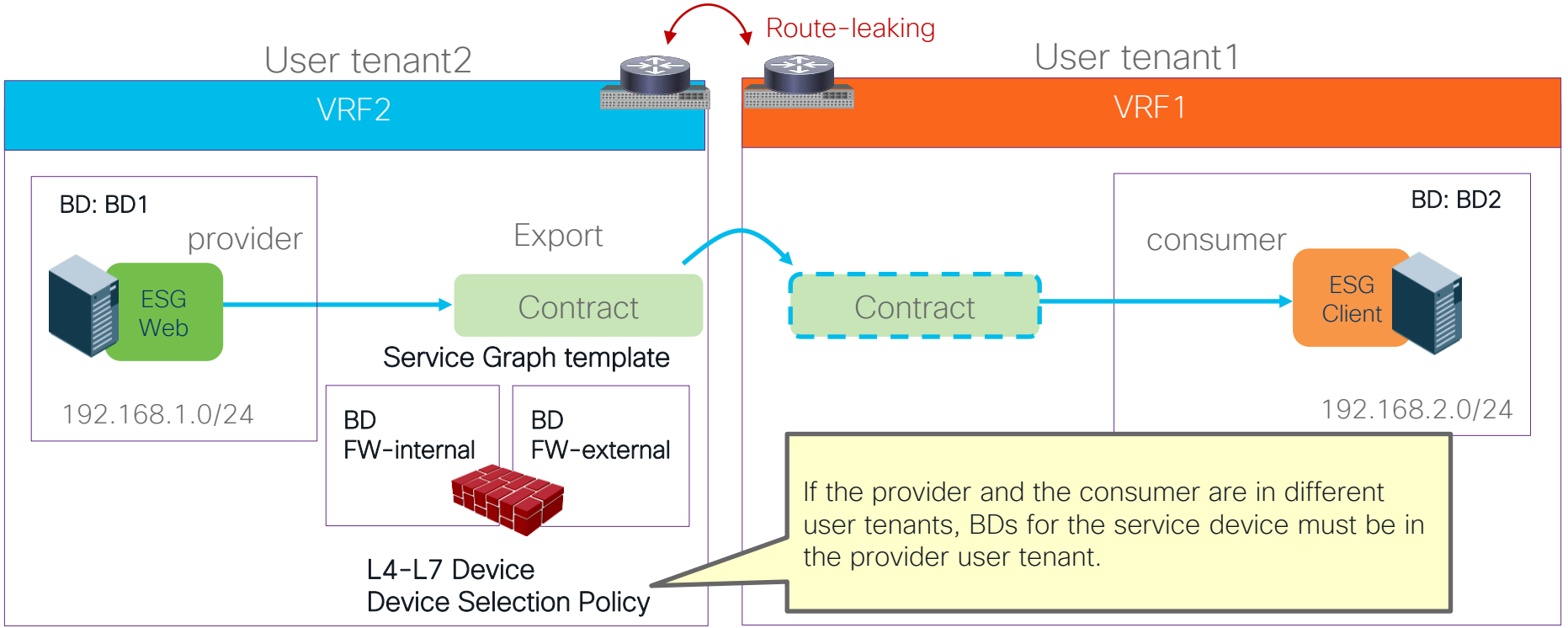
Inter-VRF, Inter-tenant contract with PBR

Example 2: The provider is in a user tenant and the consumer is in the common tenant.



Inter-VRF, Inter-tenant contract with PBR

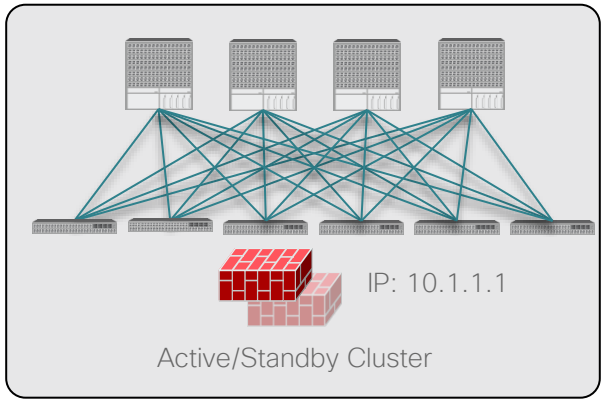
Example 3: The provider is in a user tenant and the consumer is in another user tenant.



HA design options

One PBR destination IP
One Logical device with two concrete devices

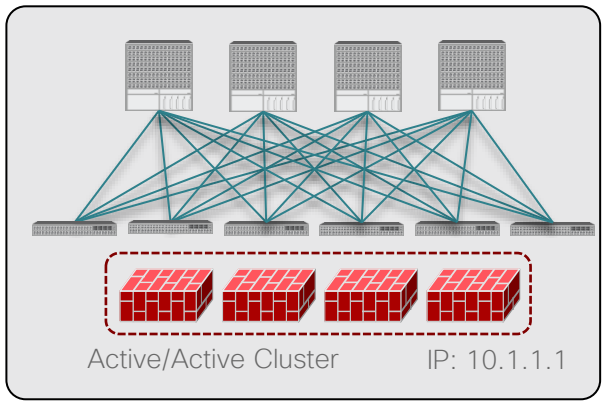
Active/Standby Cluster



- PBR is not mandatory
- The Active/Standby pair represents a single MAC/IP entry.

One PBR destination IP
One Logical device with one concrete device

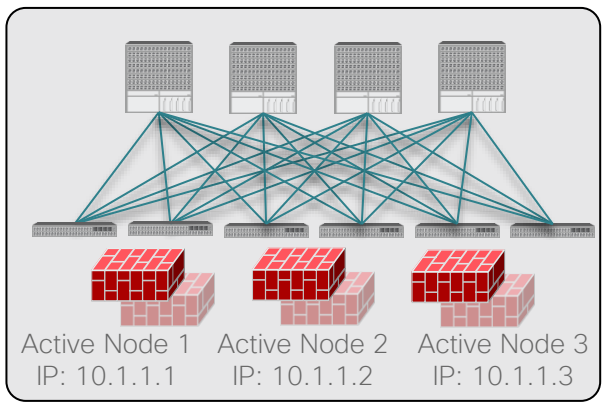
Active/Active Cluster ('Scale-Up' Model)



- PBR is required if the cluster is stretched across pods.
- The Active/Active cluster represents a single MAC/IP entry.
- Spanned Ether-Channel Mode supported with Cisco ASA/FTD platforms

Multiple PBR destination IPs (Symmetric PBR)
One Logical device with multiple concrete devices

Independent Active Nodes ('Scale-Out' Model)

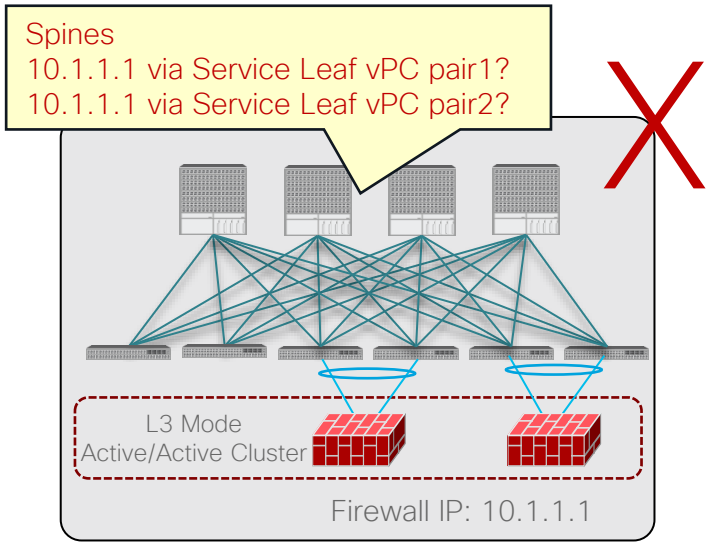


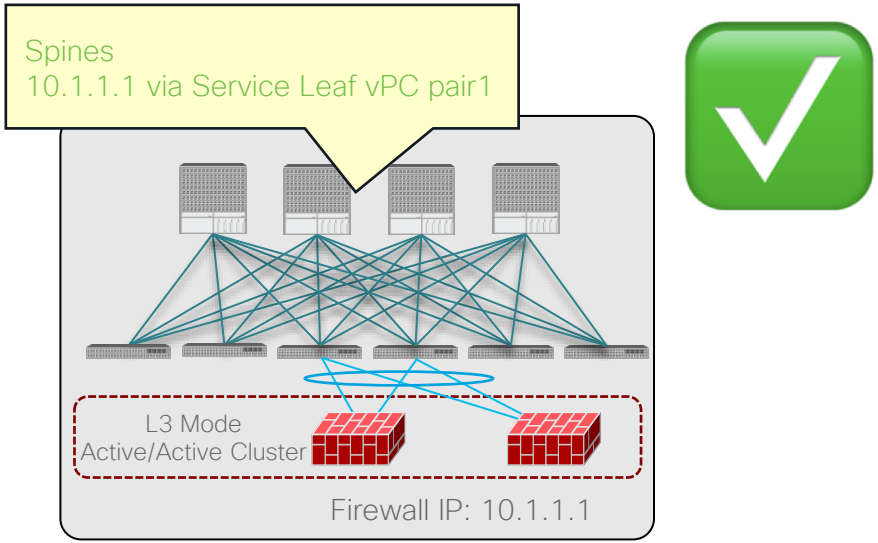
- PBR is required.
- Each Active node represent a unique MAC/IP entry.
- Use of Symmetric PBR to ensure each flow is handled by the same Active node in both directions

Active/Active cluster

One PC/vPC to all devices in the cluster

- Firewalls in the same cluster must be connected via the same PC/vPC in each pod. Otherwise, the same endpoint will be learned via different locations, which results in endpoint flapping.

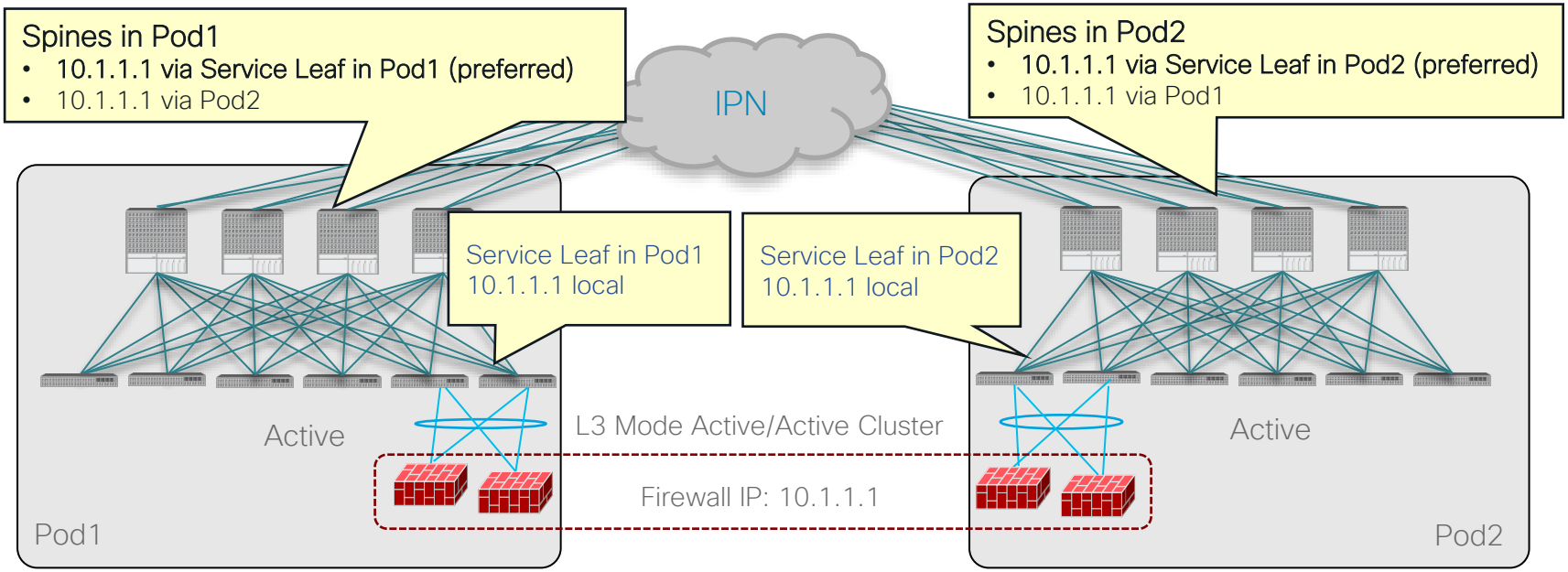




Active/Active cluster across pods

Anycast service

- For Multi-pod, Anycast service feature must be enabled.

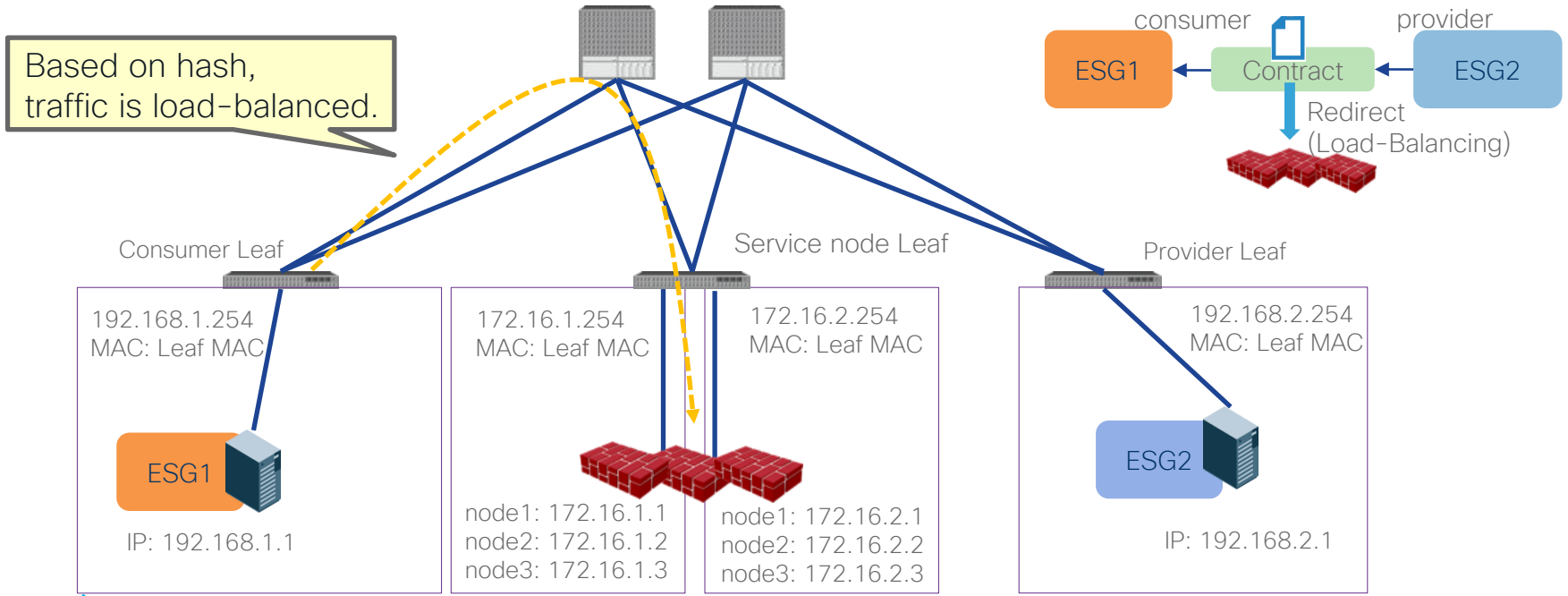


Independent Active Nodes

Symmetric PBR: Scale Firewall Easily

- Ensure incoming and return traffic go to the same firewall

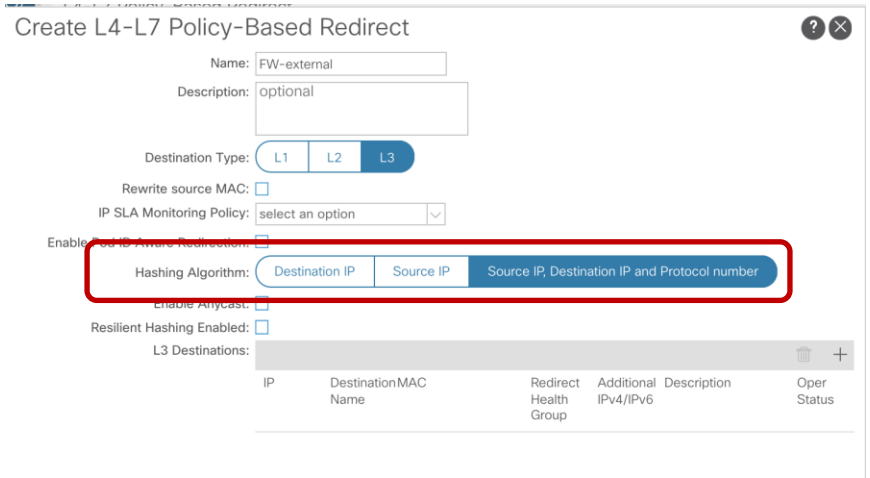
PBR destinations can be distributed across multiple leaf nodes.



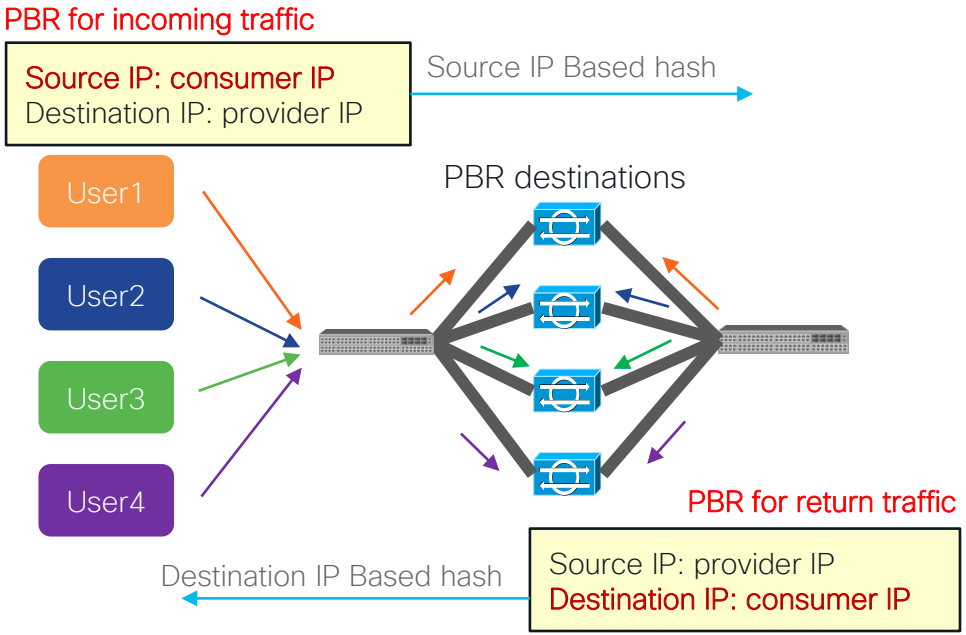
Independent Active Nodes

Symmetric PBR: Hash algorithm option

- Source IP, Destination IP and Protocol number (default)
- Source IP only
- Destination IP only



Example: same user (IP) will go through the same device

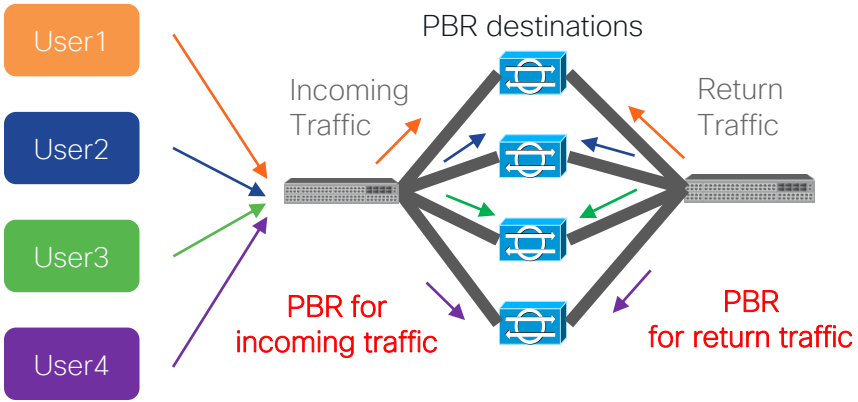


What happens if an L4-L7 device is down?

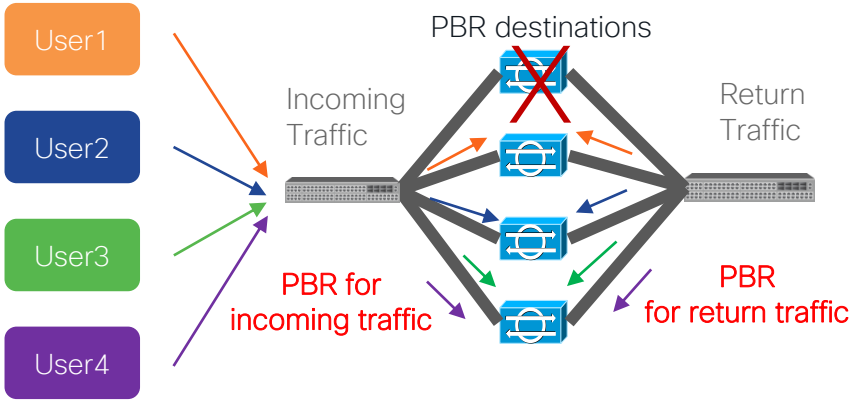
Without Resilient Hash (Default behavior)

- If one of the PBR nodes goes down, existing traffic flows will be rehashed. This could lead to the connection being reset.

Thanks to Symmetric PBR, incoming and return traffic go to same PBR node.



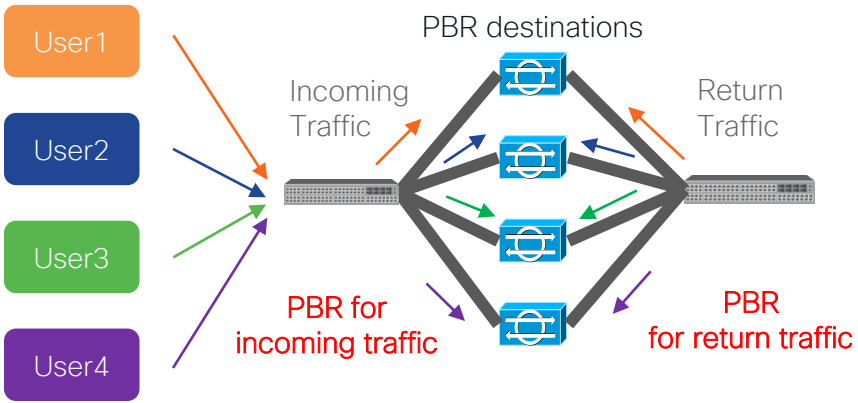
Some traffic could be load-balanced to different PBR nodes that don't have existing connection info.

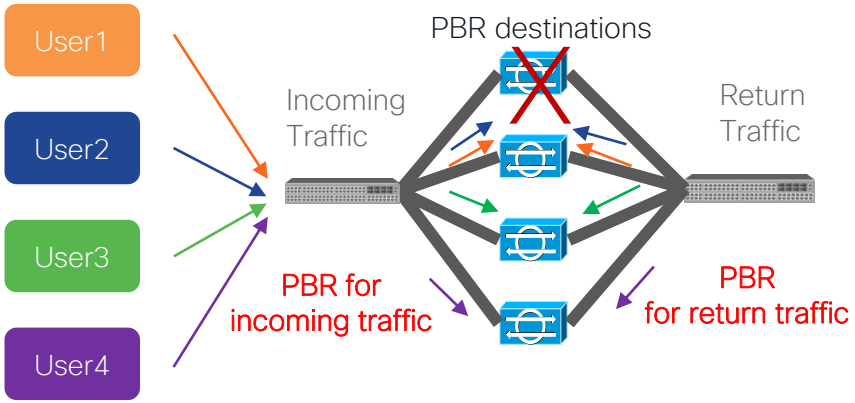


I want to minimize impact on the existing flow!

With Resilient Hash

- With Resilient Hash PBR, only the traffics that went through failed node will be rerouted to one of the available nodes.

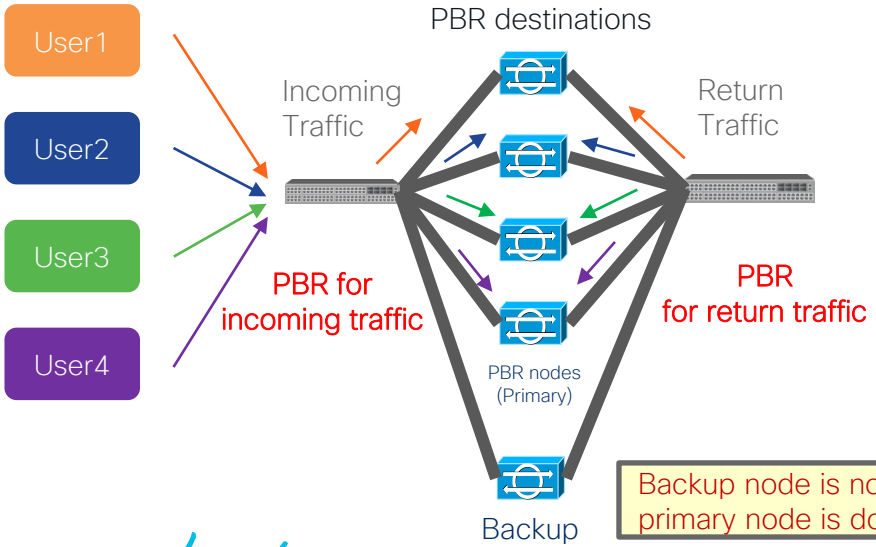


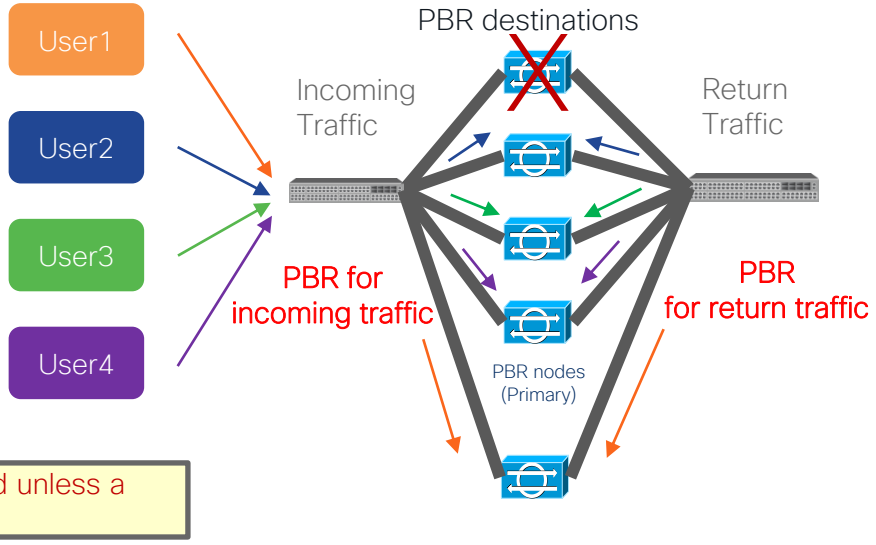


Can we use standby PBR destination?

Resilient Hash PBR with N+M backup

- As all the traffic that went through the failed node will go to one of the available nodes, capacity of the node is a concern. (The node would have doubled amount of traffic compared with usual)
- Instead of using one of the available primary nodes, a backup node in the group will be used. (N+M)





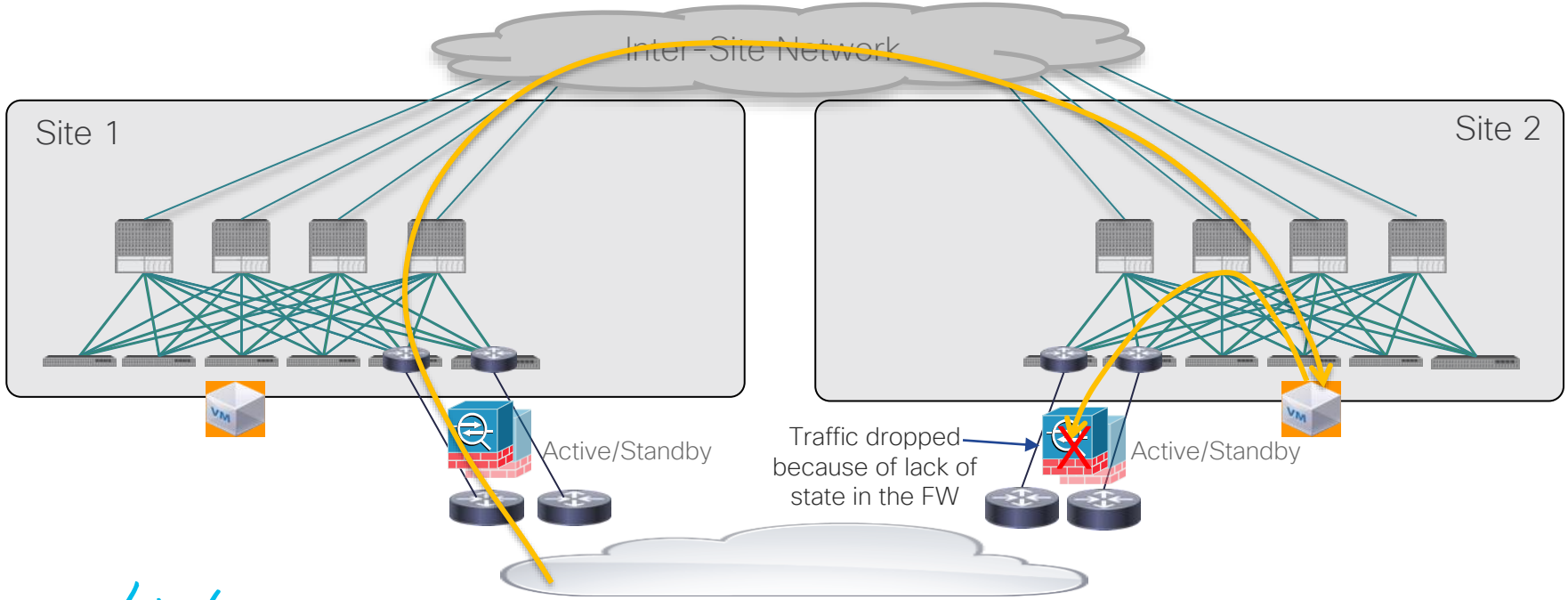
Backup node is not used unless a primary node is down.

Multi-location Data Centers

Service insertion in multiple DC locations

What is the challenge of service insertion in multiple DC locations?

- Traffic Symmetricity is important

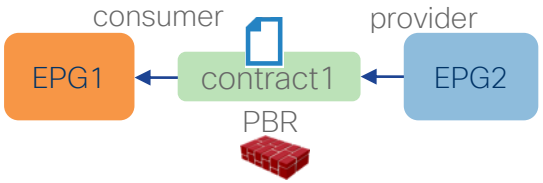


Multi-location Data Centers

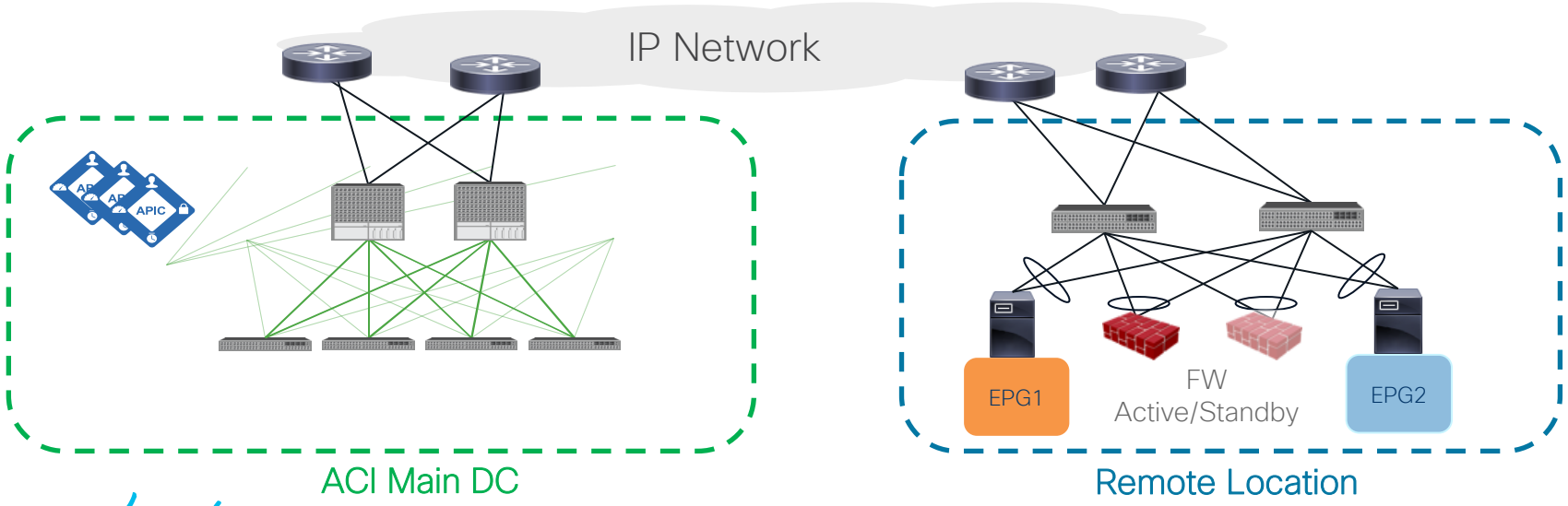
- Remote Leaf
- Multi-Pod
- Multi-Site

ACI Remote Leaf

Design consideration

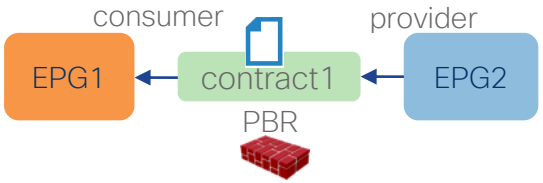


- Service devices in the same service chain shouldn't be distributed across main location and remote location.
- Recommendation: Connect service device, consumer and provider EPs in vPC mode at Remote Location for local forwarding

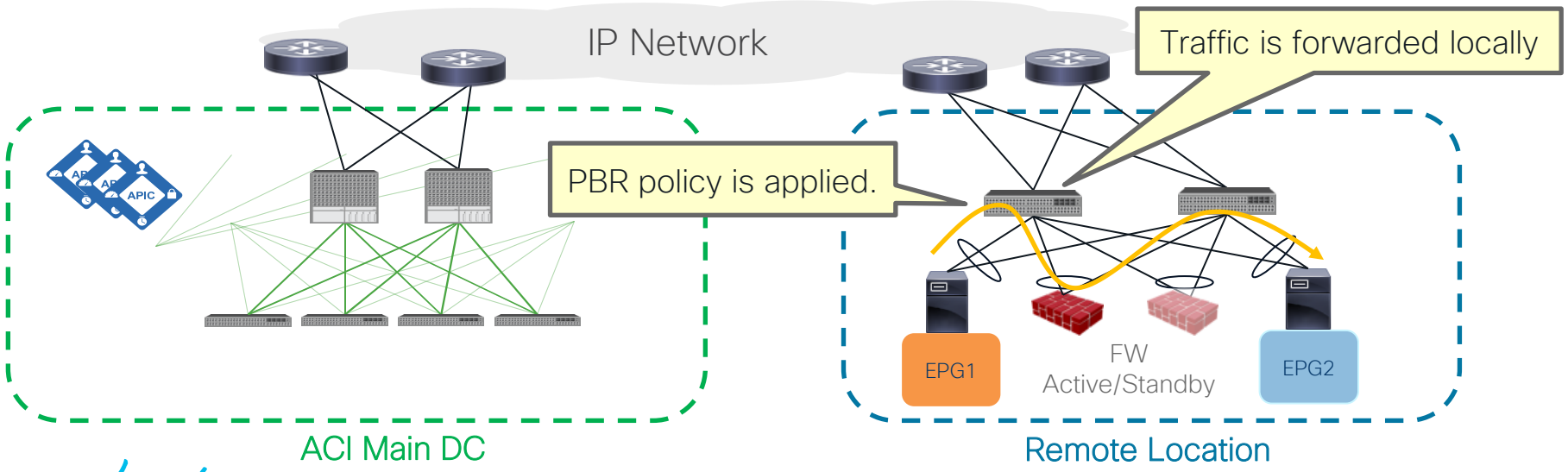


ACI Remote Leaf

PBR traffic forwarding after ACI 4.0



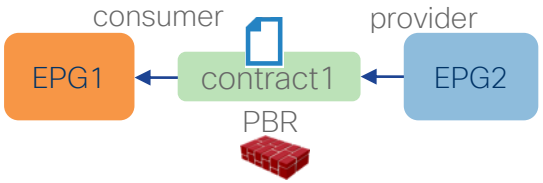
- Prior to ACI 4.0, PBR traffic was always sent to Spine even when the source EP, destination EP and service EP (PBR destination) are under same Remote Leaf pair.
- Starting from ACI 4.0, service EPs (PBR destinations) information are learnt on Remote Leaf. So that traffic is locally forwarded.

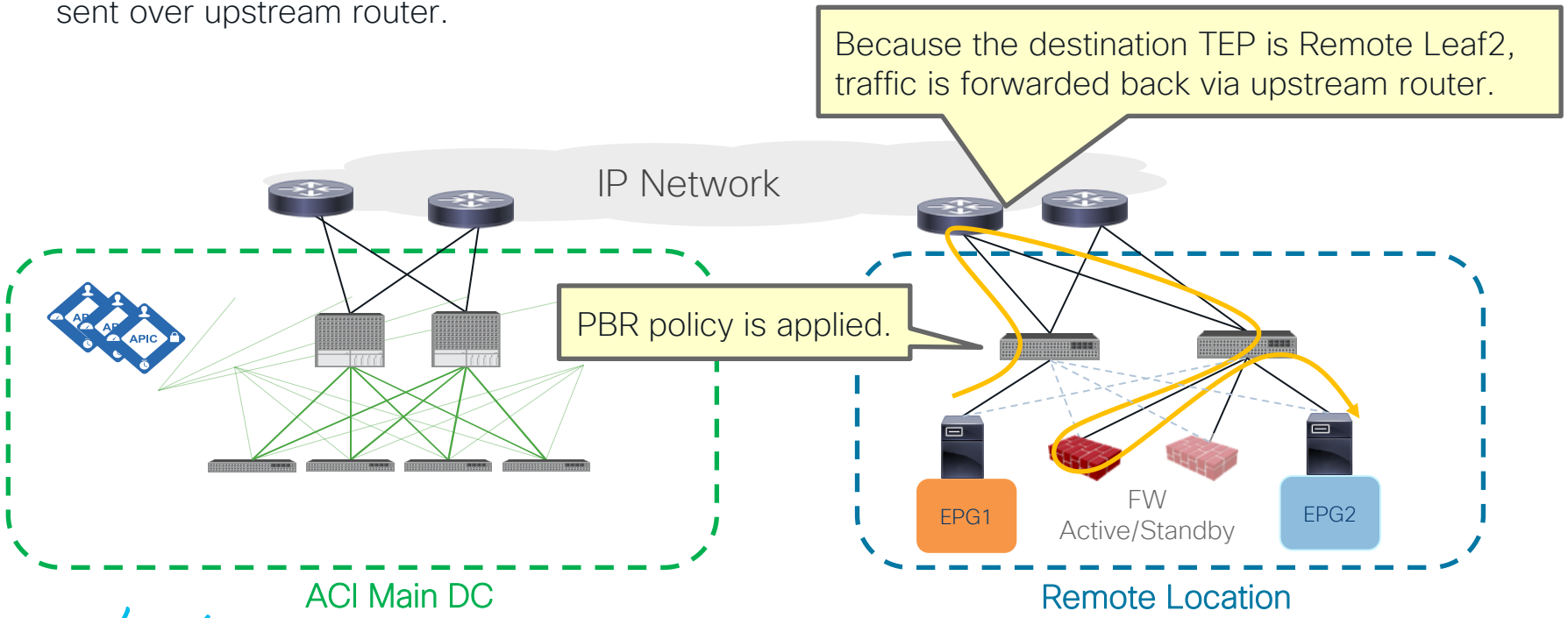


ACI Remote Leaf

If it's not vPC (orphan port)

- If the end points and service node is connected using orphan port, traffic to peer Remote Leaf is sent over upstream router.



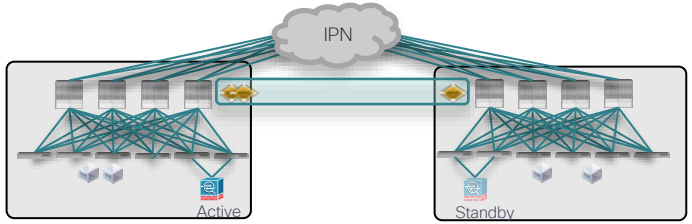


ACI Multi-Pod

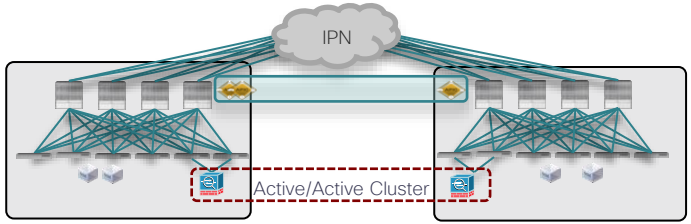
Design options

For your reference

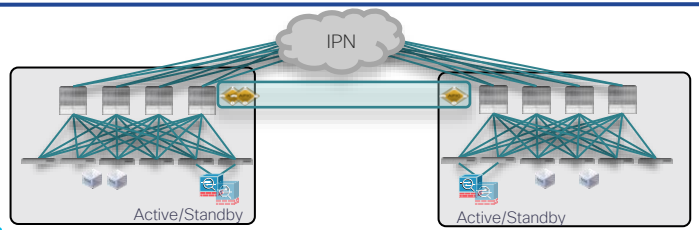
Typical options for an Active/Active DC use case



- Active and Standby pair deployed across Pods
- No issues with asymmetric flows



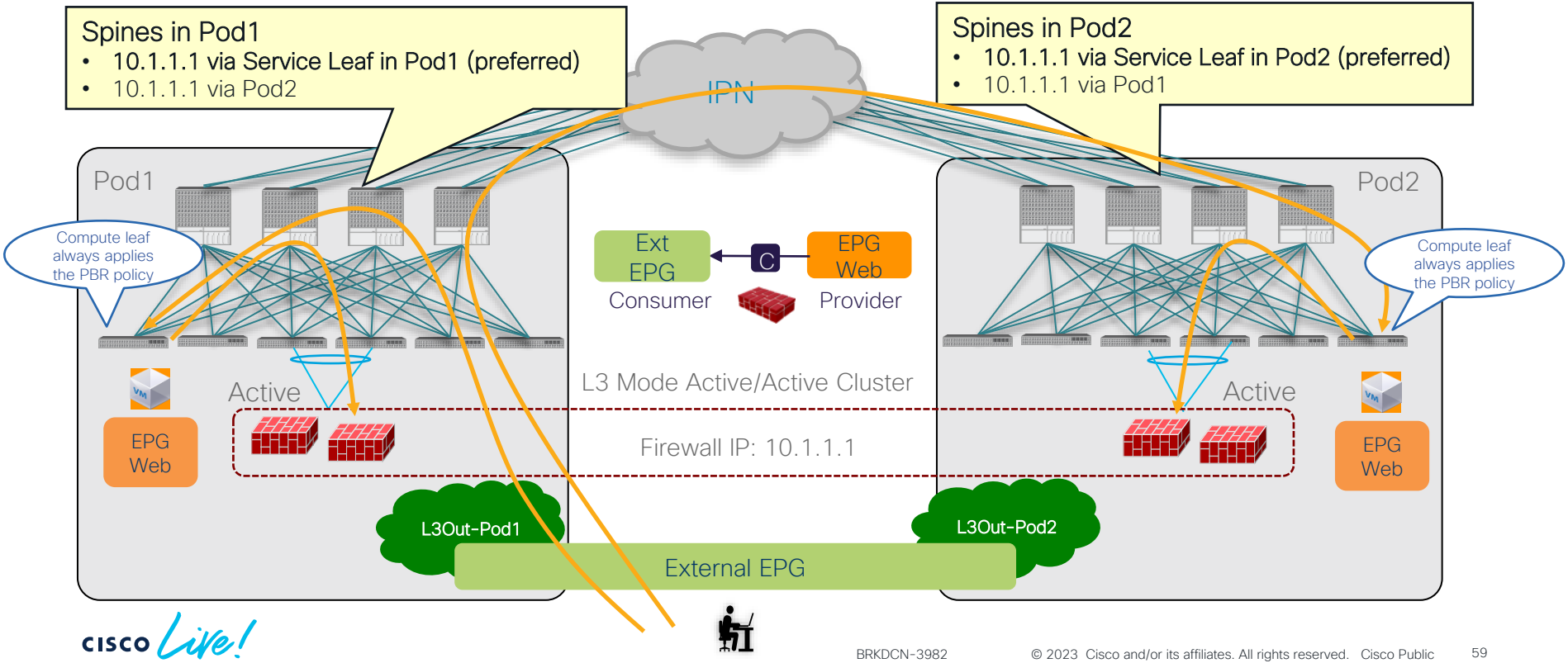
- Active/Active FW cluster nodes stretched across Sites (single logical FW)
- Requires the ability of discovering the same MAC/IP info in separate pods at the same time
- Supported from ACI release 3.2(4d) with the use of Service-Graph with PBR



- Independent Active/Standby pairs deployed in separate Pods
- Use of Symmetric PBR to avoid the creation of asymmetric paths crossing different active FW nodes

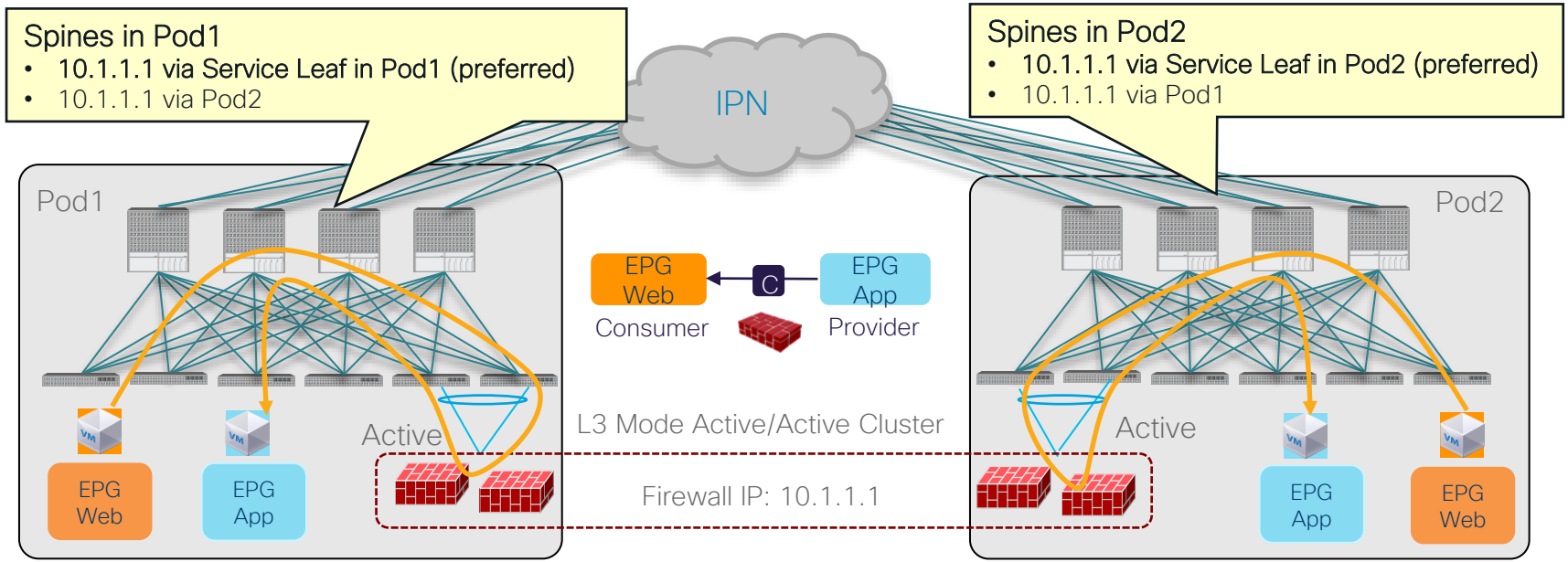
ACI Multi-Pod: Active/Active cluster across pods

North-South Traffic Flow



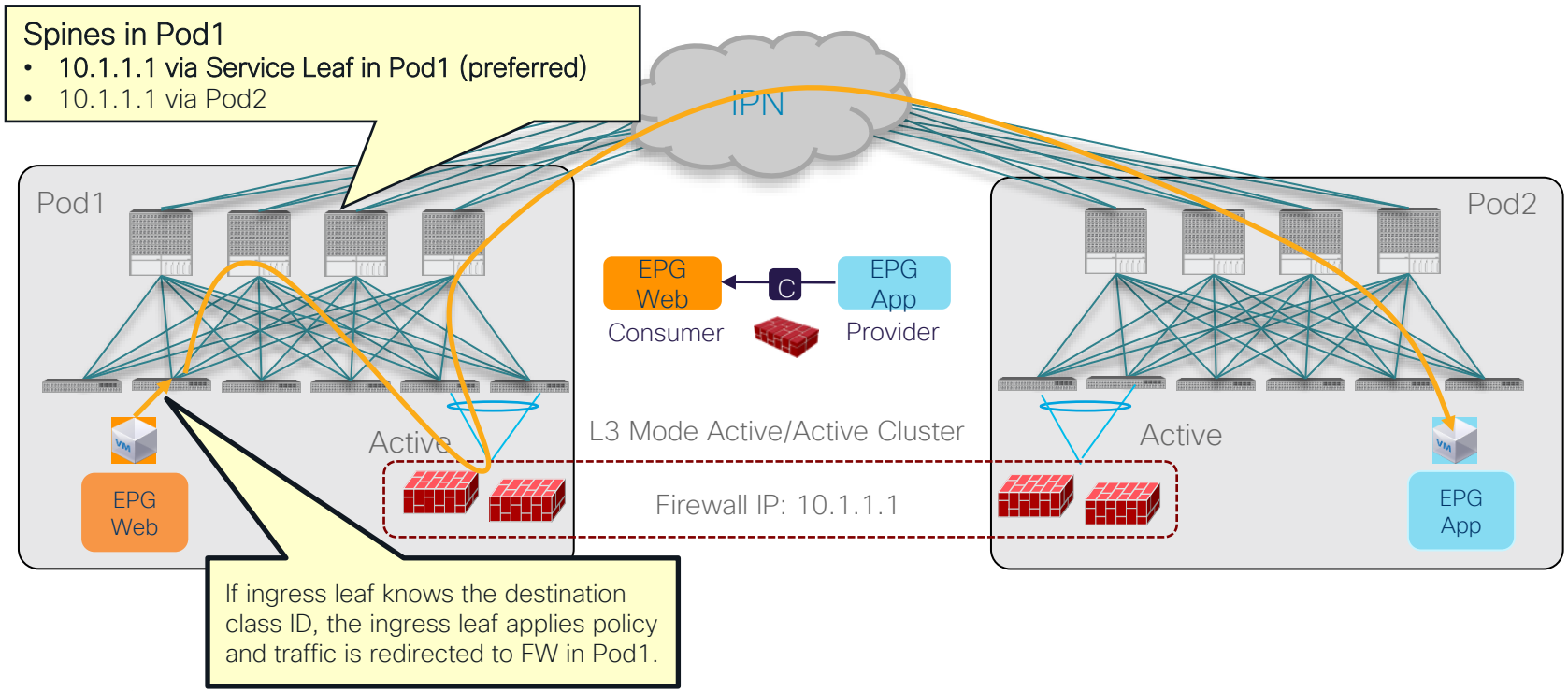
ACI Multi-Pod: Active/Active cluster across pods

East-West Traffic Flow (Intra-Pod)



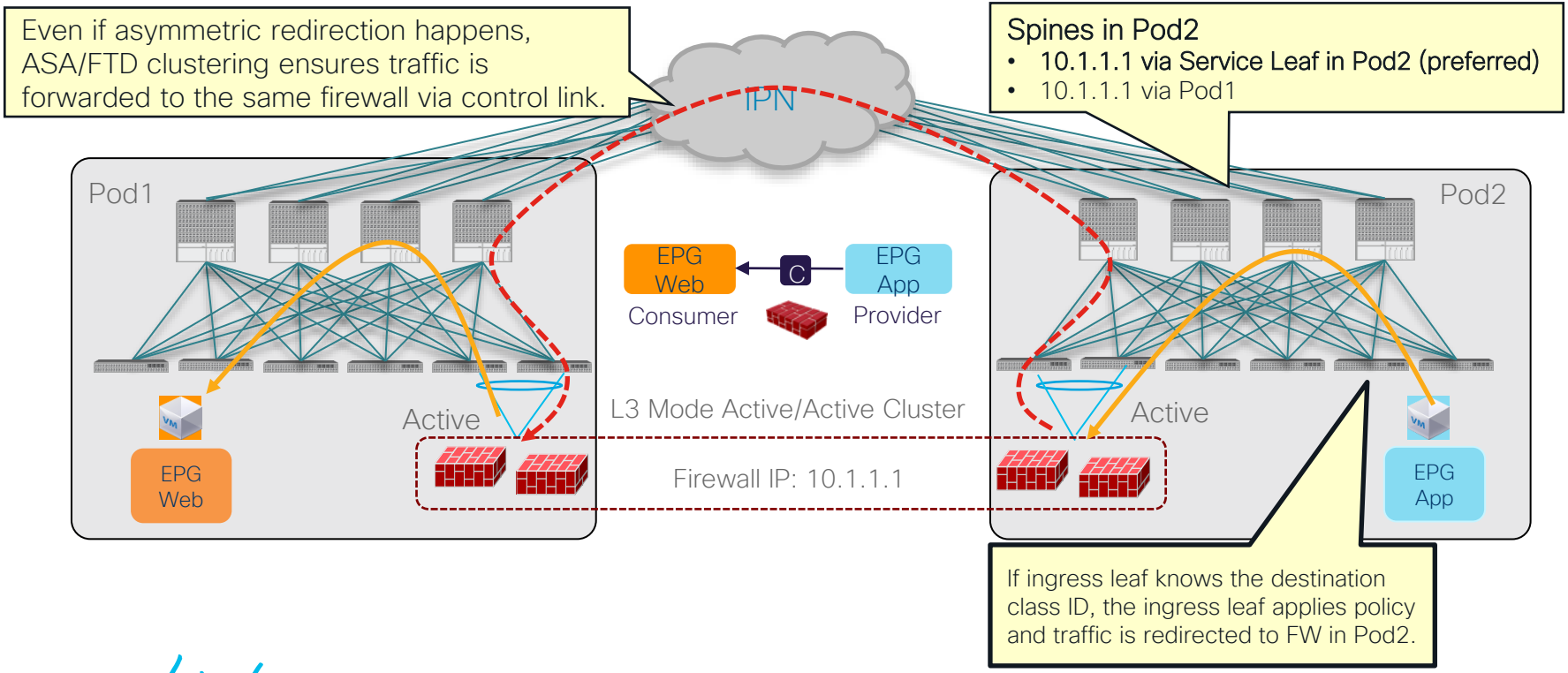
ACI Multi-Pod: Active/Active cluster across pods

East-West Traffic Flow (Inter-Pod) incoming traffic



ACI Multi-Pod: Active/Active cluster across pods

East-West Traffic Flow (Inter-Pod) return traffic



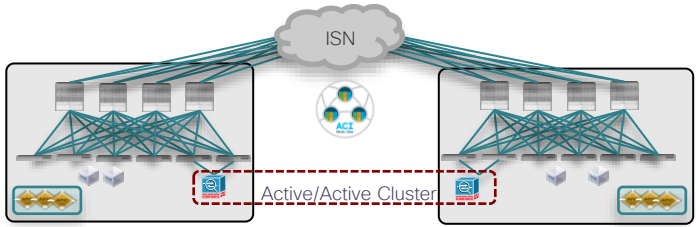
ACI Multi-Site

Design options

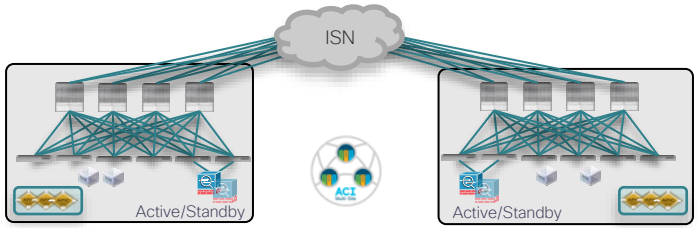
For your reference

Deployment options fully supported with ACI Multi-Pod

- Active and Standby pair deployed across Pods
- Limited supported options



- Active/Active FW cluster nodes stretched across Sites (single logical FW)
- Not supported



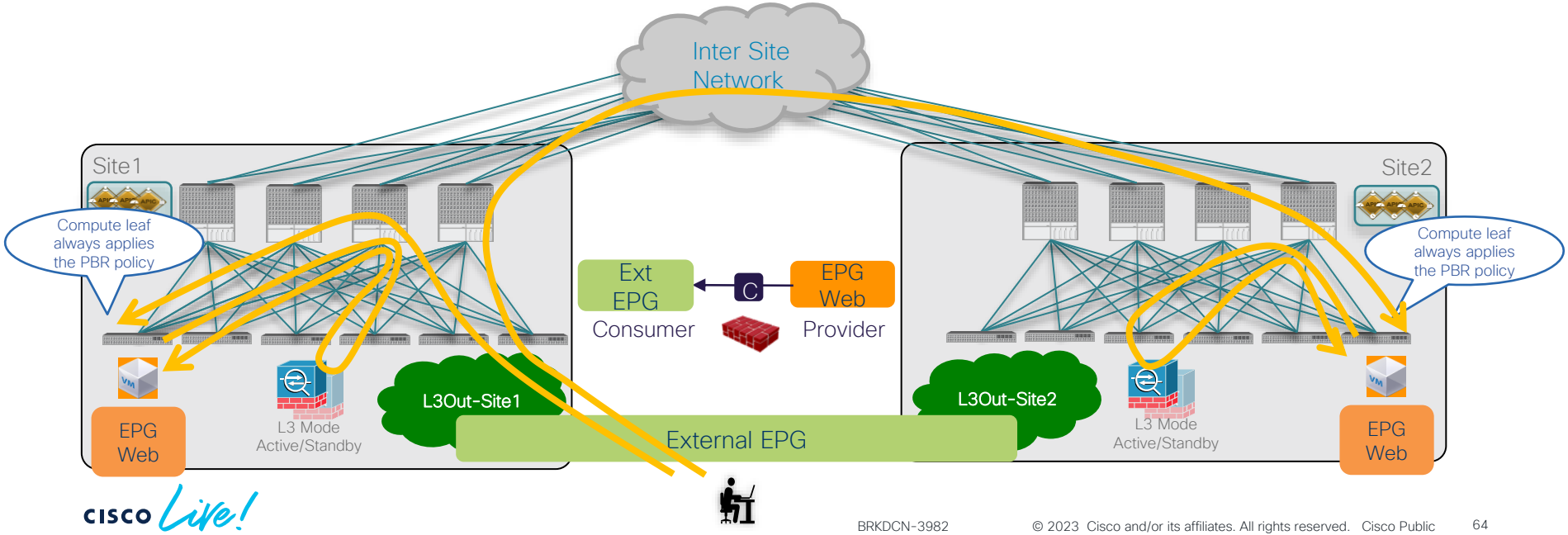
- Recommended deployment model for ACI Multi-Site
- Supported from 3.2 release with the use of Service Graph with Policy Based Redirection (PBR)

ACI Multi-Site: service nodes in each site

North-South Traffic Flow: compute leaf enforcement

Policy is always applied on the compute leaf

- North-South (L3Out-to-EPG) intra-VRF and inter-VRF contract with PBR
  - For inter-VRF contract, L3Out must be the provider.

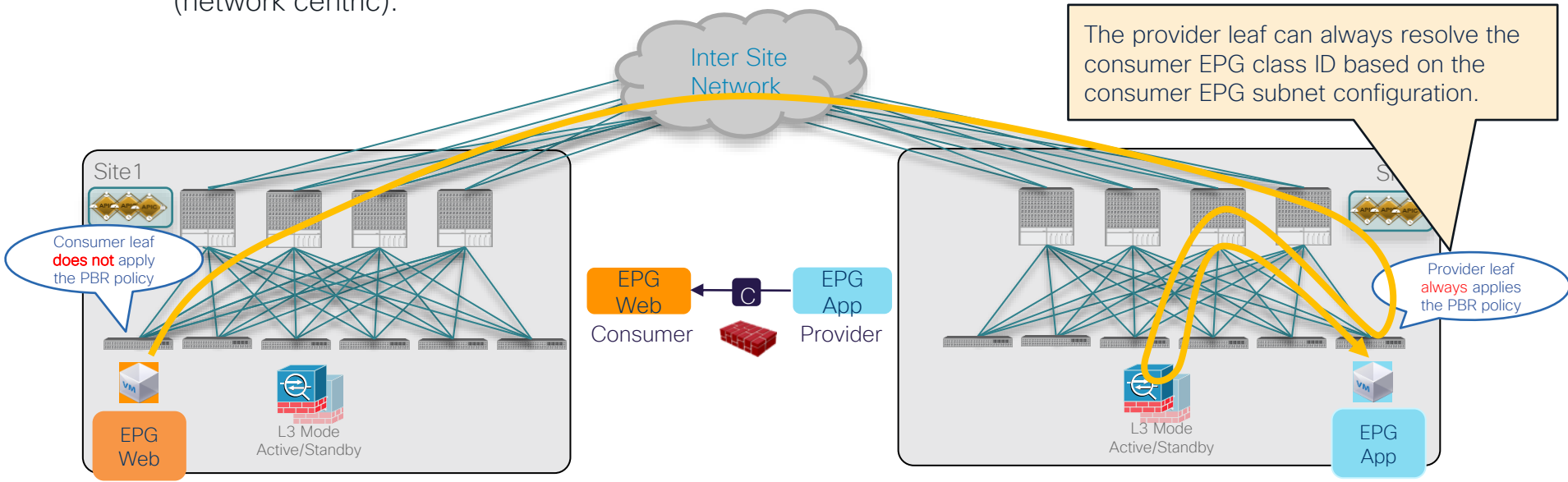


ACI Multi-Site: service nodes in each site

East-West Traffic Flow: provider leaf enforcement

Policy is always applied on the provider leaf

- East-West (EPG-to-EPG) intra-VRF and inter-VRF contract with PBR
  - The consumer EPG subnet must be configured, which means the design must be 1 BD subnet = 1 EPG (network centric).

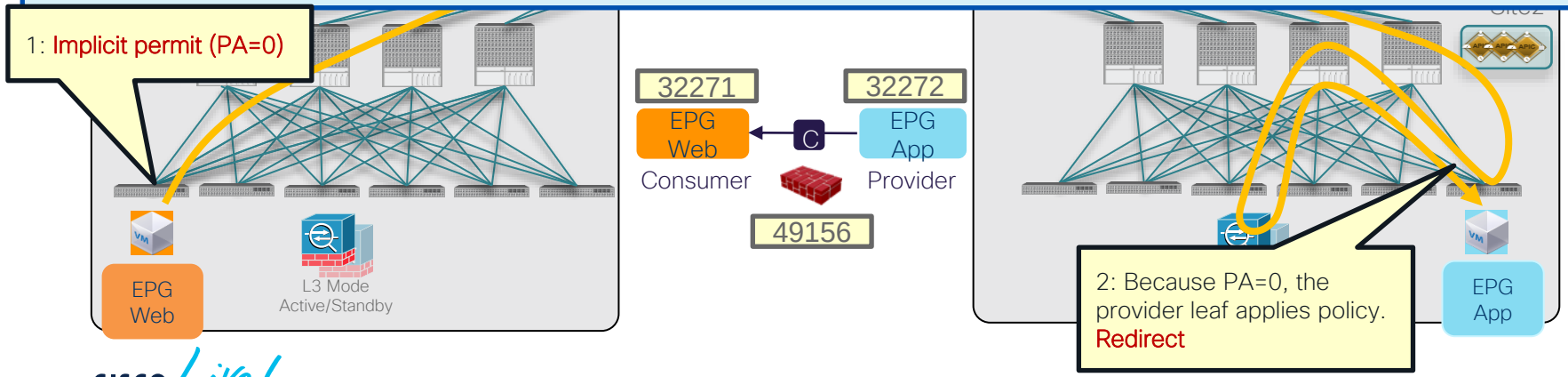


How to ensure the provider leaf enforcement?

Special rule for consumer-to-provider traffic

- redir_override: If the destination is NOT a local endpoint, the leaf doesn't apply policy (PA=0)

```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+----------------+---------+---------+------+-----------------------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action                      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------------------------------+----------------------+
<snip>
|   4144  | 32271  | 32272  |    14    |     bi-dir     | enabled | 2195459 |      | redir(destgrp-1),redir_override   |    fully_qual(7)     |
|   4157  | 32272  | 32271  |    14    | uni-dir-ignore | enabled | 2195459 |      | redir(destgrp-1)                  |    fully_qual(7)     |
|   4140  | 49156  | 32272  | default  |    uni-dir     | enabled | 2195459 |      |       permit                      |    src_dst_any(9)    |
|   4136  | 49156  | 32271  |    14    |    uni-dir     | enabled | 2195459 |      |       permit                      |    fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------------------------------+----------------------+
```

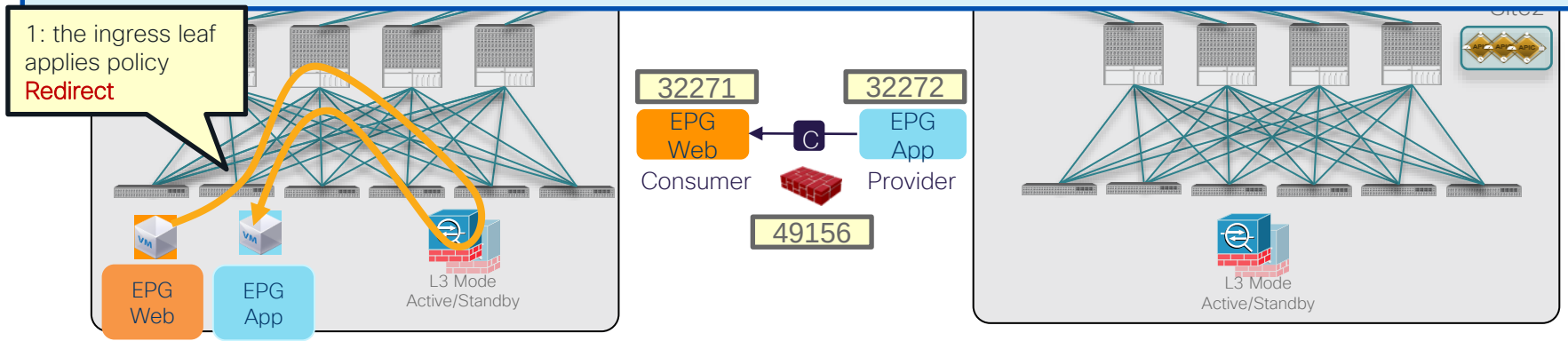


How to ensure the provider leaf enforcement?

Special rule for consumer-to-provider traffic

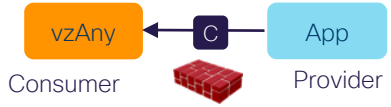
- If the destination is under the same leaf, the leaf applies policy.

```
Pod1-Leaf1# show zoning-rule scope 2195459
+---------+--------+--------+----------+----------------+---------+---------+------+-----------------------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action                      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------------------------------+----------------------+
<snip>
|   4144  | 32271  | 32272  |    14    |     bi-dir     | enabled | 2195459 |      | redir(destgrp-1),redir_override   |    fully_qual(7)     |
|   4157  | 32272  | 32271  |    14    | uni-dir-ignore | enabled | 2195459 |      | redir(destgrp-1)                  |    fully_qual(7)     |
|   4140  | 49156  | 32272  | default  |    uni-dir     | enabled | 2195459 |      |       permit                      |    src_dst_any(9)    |
|   4136  | 49156  | 32271  |    14    |    uni-dir     | enabled | 2195459 |      |       permit                      |    fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------------------------------+----------------------+
```



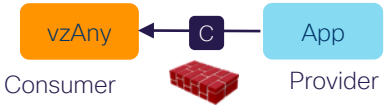
Multi-Site PBR Roadmap

- vzAny-to-EPG
- vzAny-to-vzAny



ACI Multi-Site vzAny-to-EPG PBR

Challenges



- How to keep traffic symmetric
  → Provider leaf enforcement

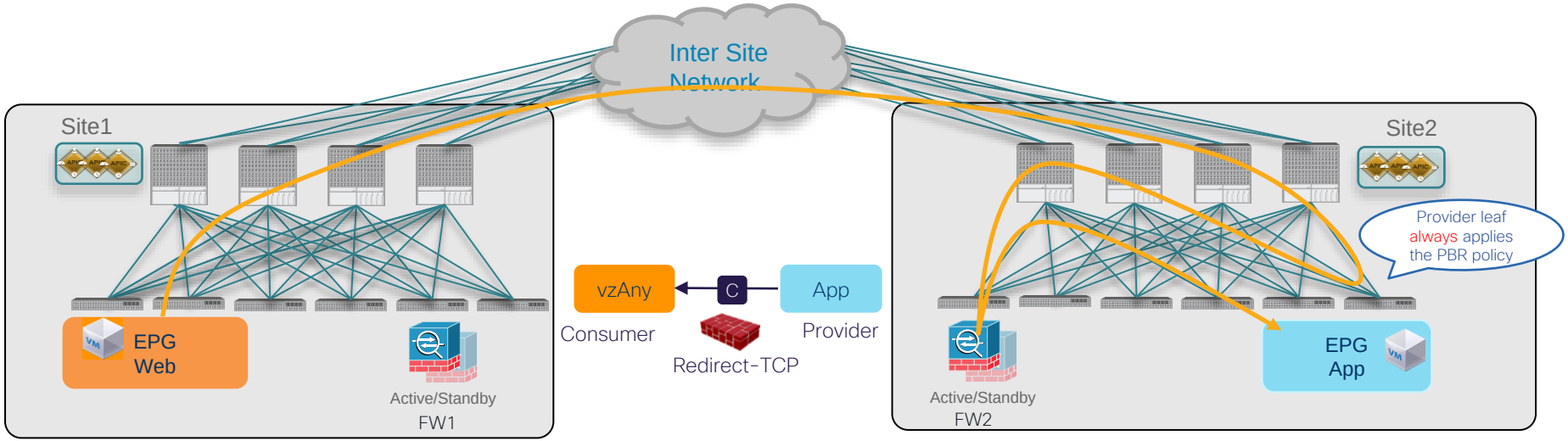
- How to ensure the provider leaf nodes can resolve destination class ID without EPG subnet.
  → Conversational learning

ACI Multi-Site vzAny-EPG PBR

Consumer to provider direction

Roadmap

- Provider leaf enforcement to keep traffic symmetric.

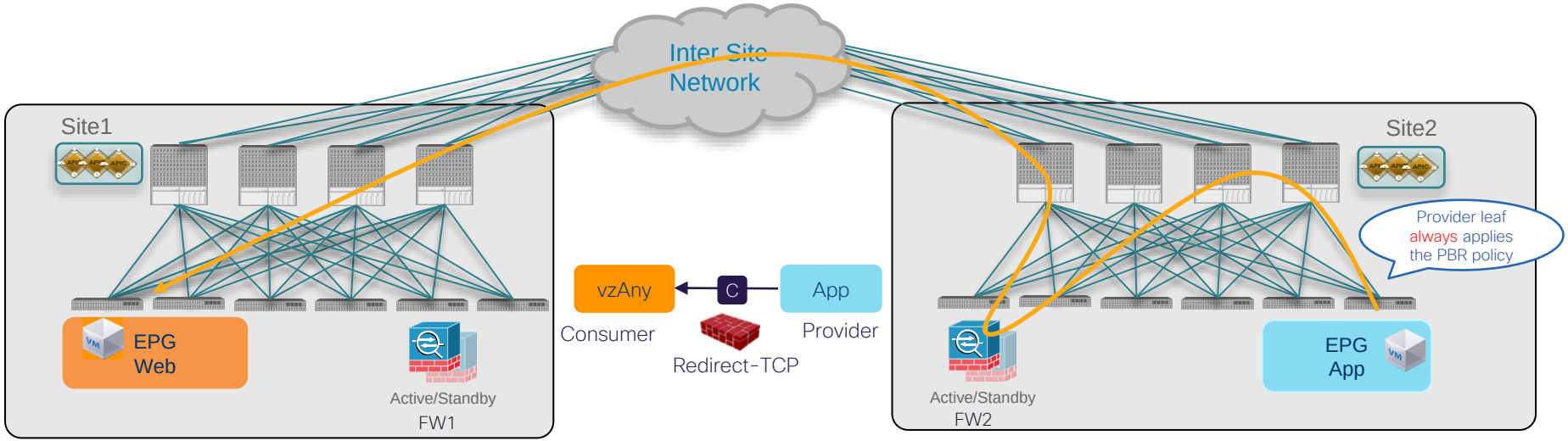


ACI Multi-Site vzAny-EPG PBR

Provider to consumer direction

Roadmap

- Provider leaf enforcement to keep traffic symmetric.

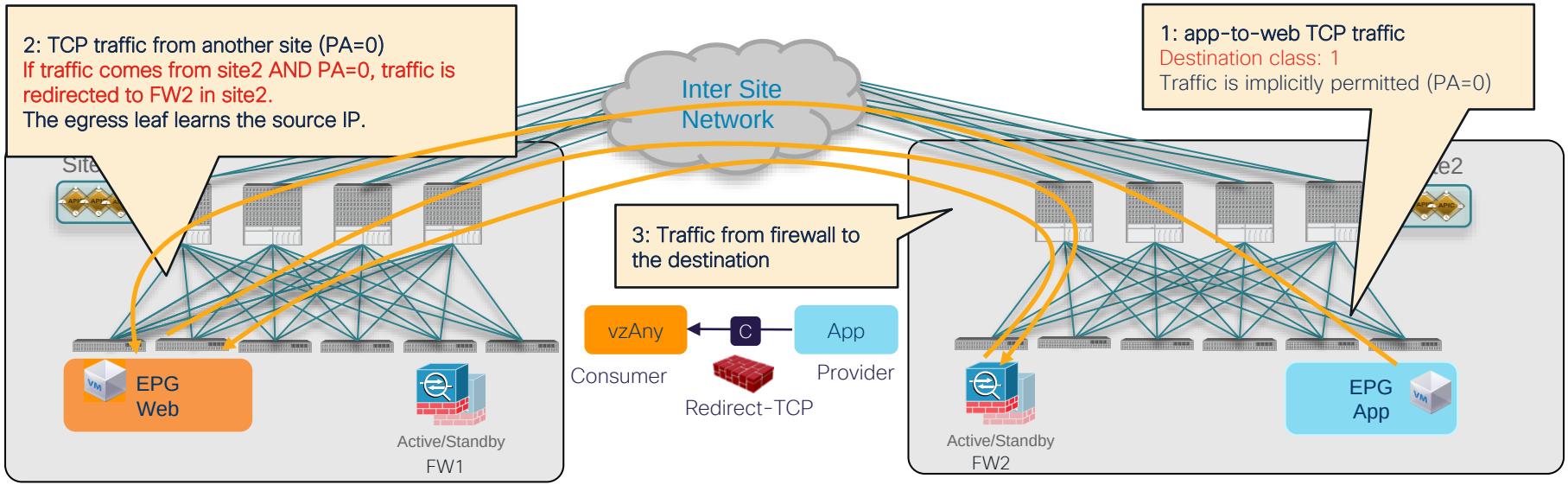


ACI Multi-Site vzAny-EPG PBR

What if the provider leaf doesn't know the consumer endpoint? (1/2)

Roadmap

- Force traffic inspected by the service device in the provider site

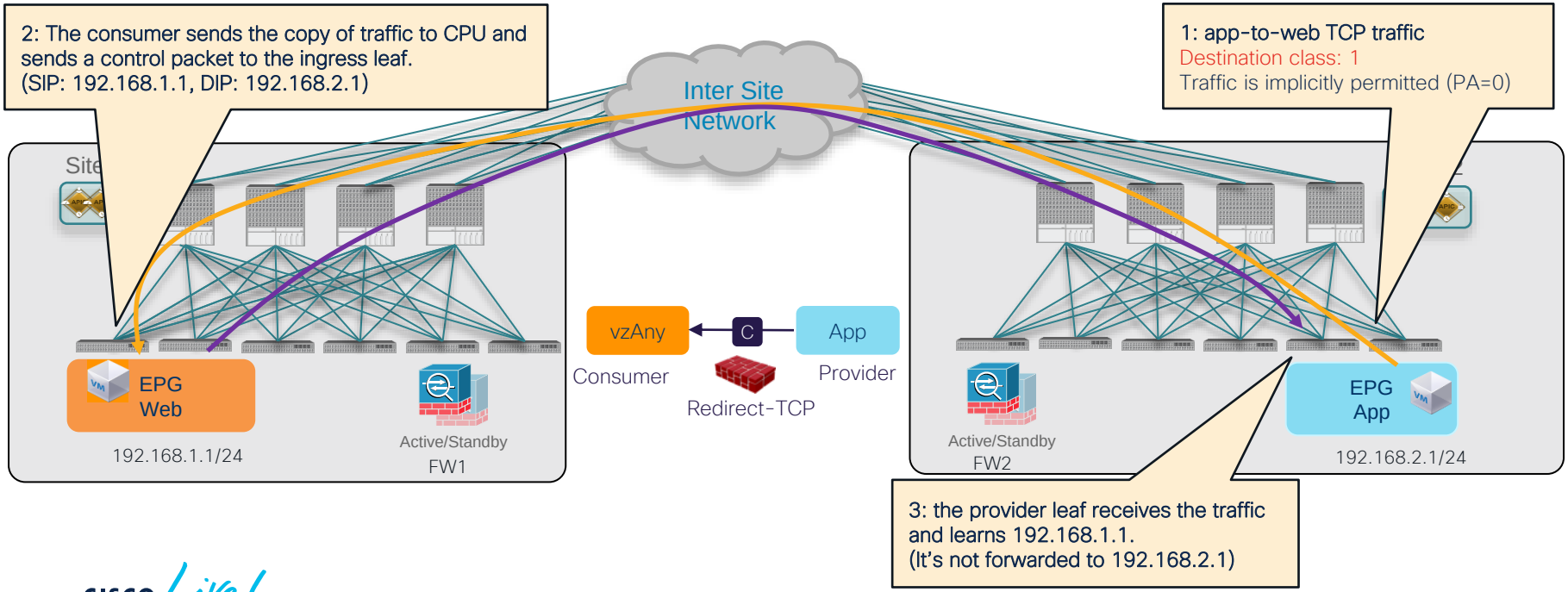


ACI Multi-Site vzAny-EPG PBR

What if the provider leaf doesn't know the consumer endpoint? (2/2)

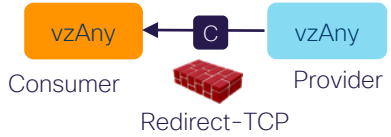
Roadmap

- Conversational Learning to get the ingress leaf learn the destination EP.



Multi-Site PBR Roadmap

- vzAny-to-EPG
- vzAny-to-vzAny



ACI Multi-Site vzAny-to-vzAny PBR

Challenges

- How to keep traffic symmetric

  → redirect “inter-site” traffic in both ingress and egress sites.

  Note: If it’s intra-site traffic, redirect doesn’t happen twice.

- How to ensure the ingress leaf nodes can resolve the destination class ID without the EPG subnet.

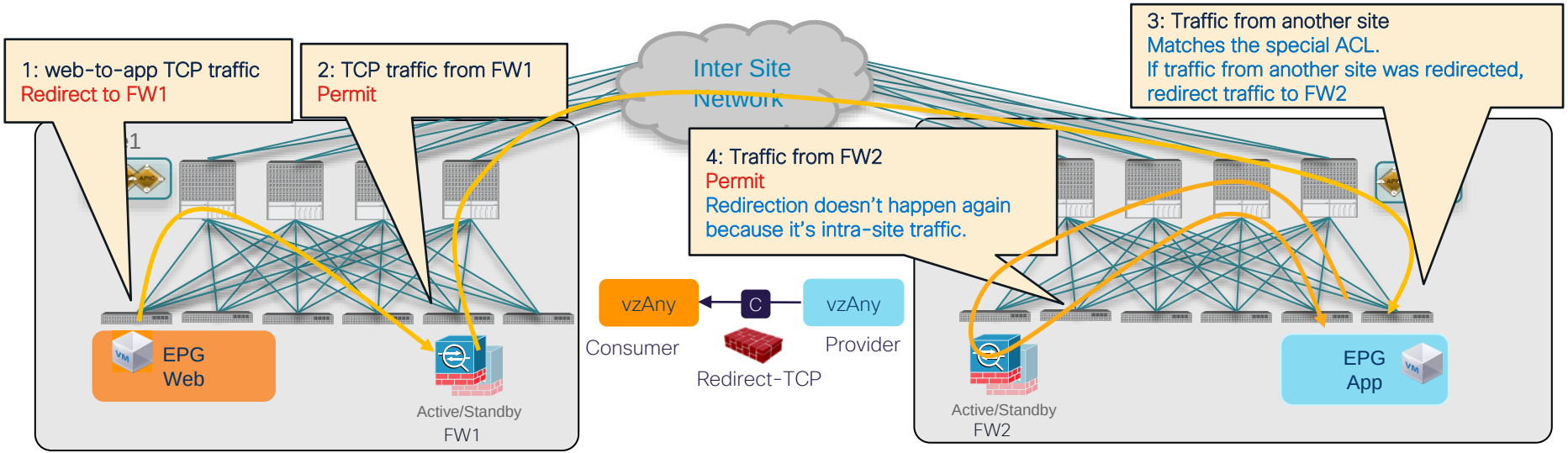
  → Conversational learning

ACI Multi-Site vzAny-to-vzAny PBR

Consumer to provider direction

Roadmap

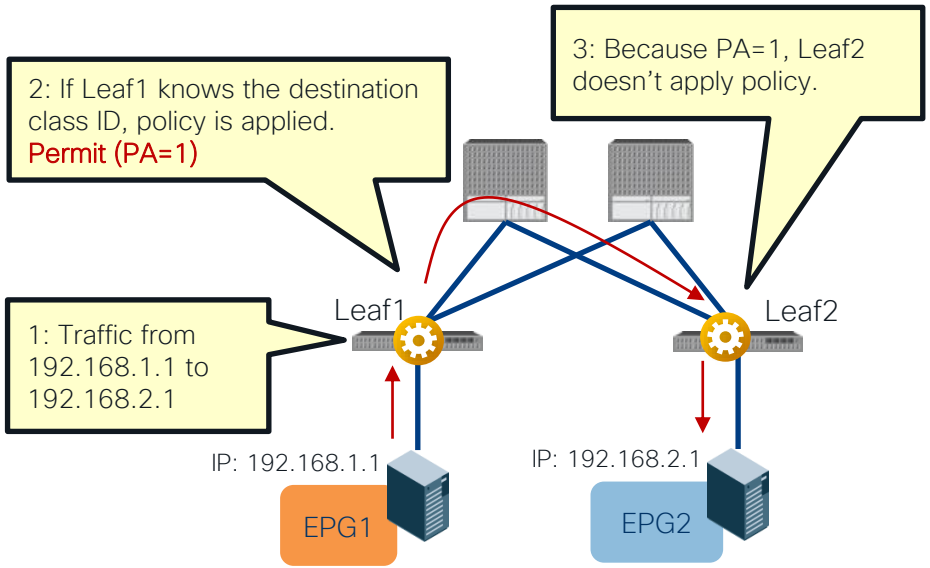
- Redirect “inter-site” traffic in both ingress and egress sites.



How to identify traffic was redirected?

Policy Applied (PA) bit

- PA bit (2 bit): Source Policy (SP) bit and Destination Policy (DP) bit



	SP	DP	Behavior
PA=1	1	1	The egress leaf doesn't apply policy because policy was applied.
PA=0	0	0	The egress leaf should apply policy because policy is not applied yet.

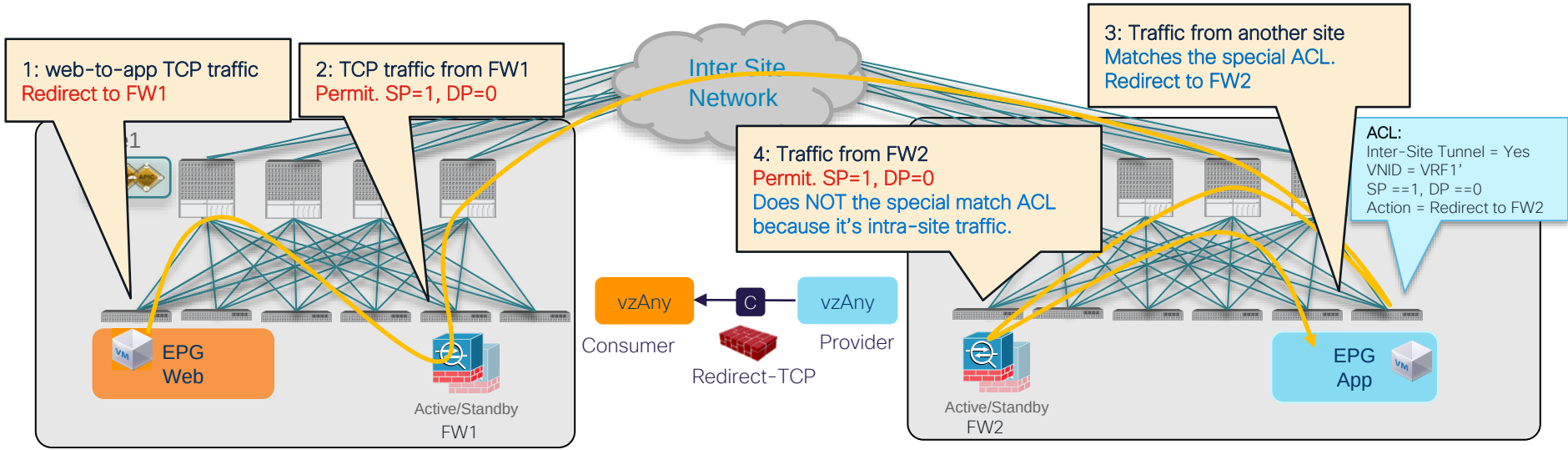
"SP=1, DP=0"
will be used for traffic from service EPG to indicate traffic was redirected

ACI Multi-Site vzAny-to-vzAny PBR

Consumer to provider direction

Roadmap

SP=1, DP=0
for traffic from
the service EPG

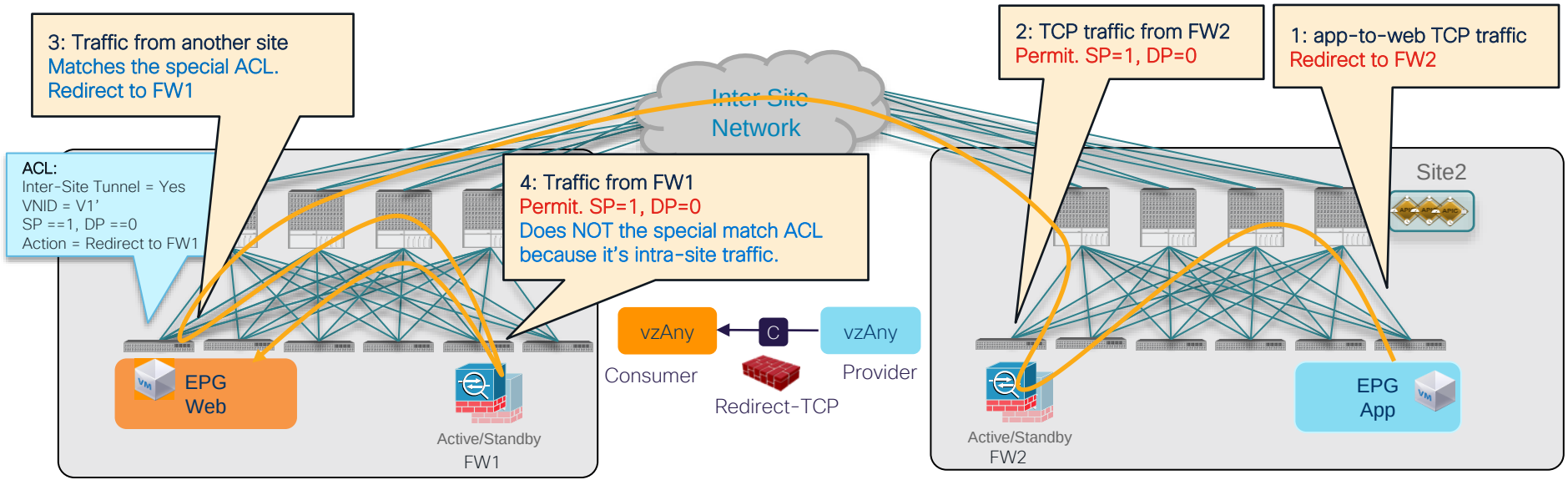


ACI Multi-Site vzAny-to-vzAny PBR

Provider to consumer direction

Roadmap

SP=1, DP=0
for traffic from
the service EPG

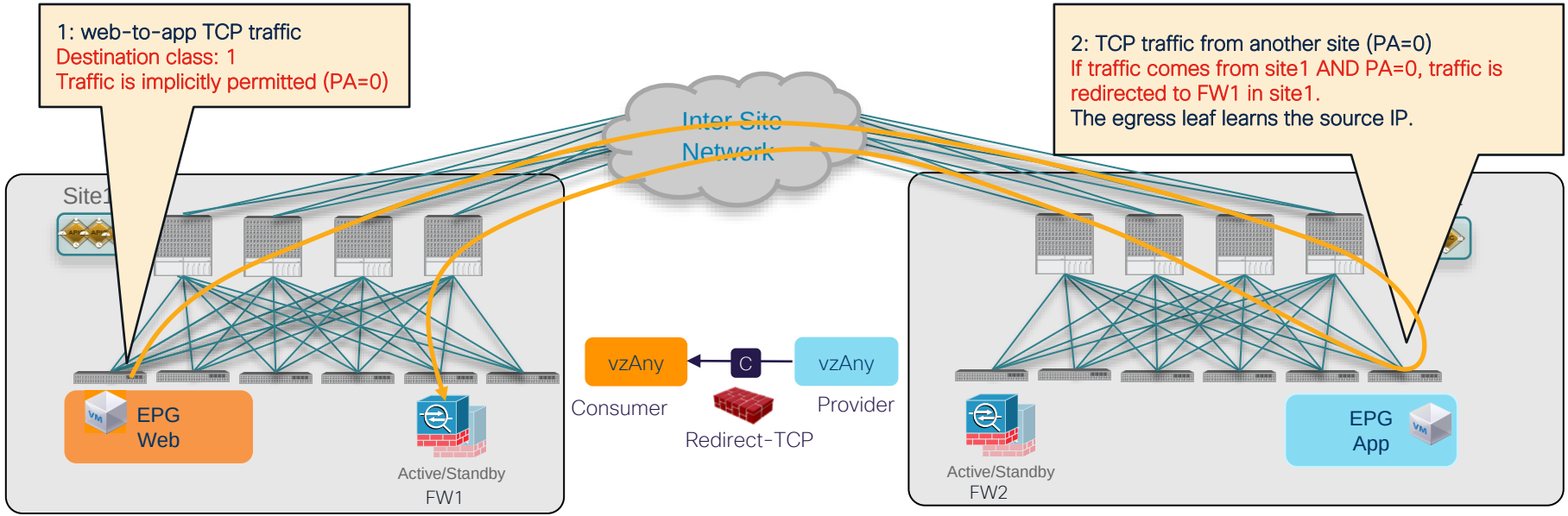


ACI Multi-Site vzAny-to-vzAny PBR

What if the ingress leaf doesn't know the destination class ID (1/3)

Roadmap

- Force traffic inspected by the service device in the source site.

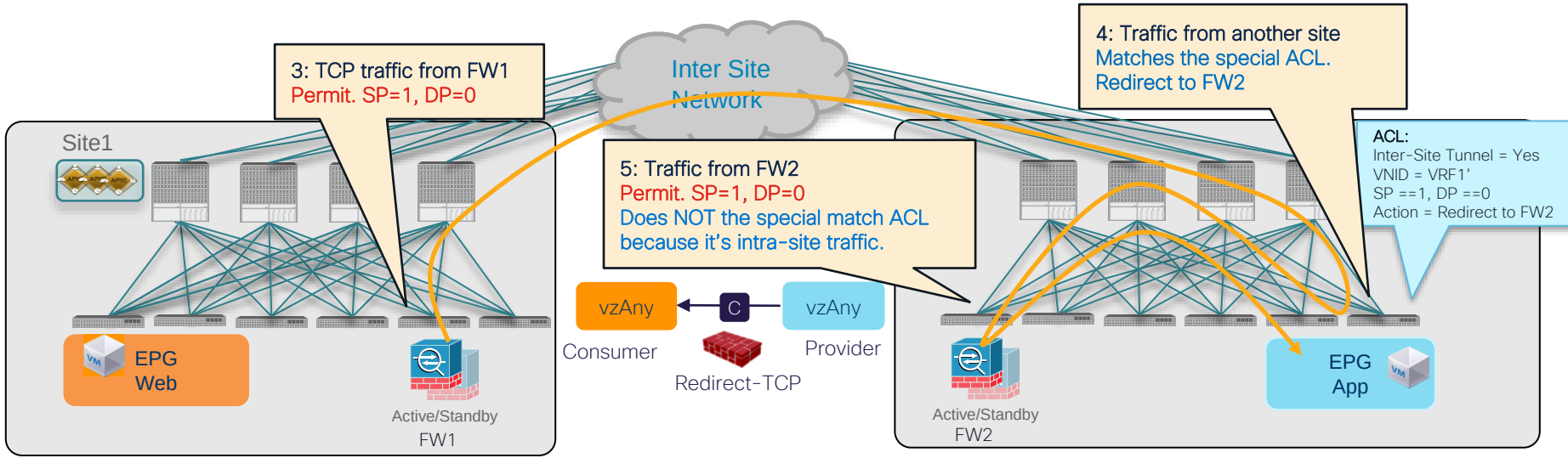


ACI Multi-Site vzAny-to-vzAny PBR

What if the ingress leaf doesn't know the destination class ID (2/3)

Roadmap

- Force traffic inspected by the service device in the destination site

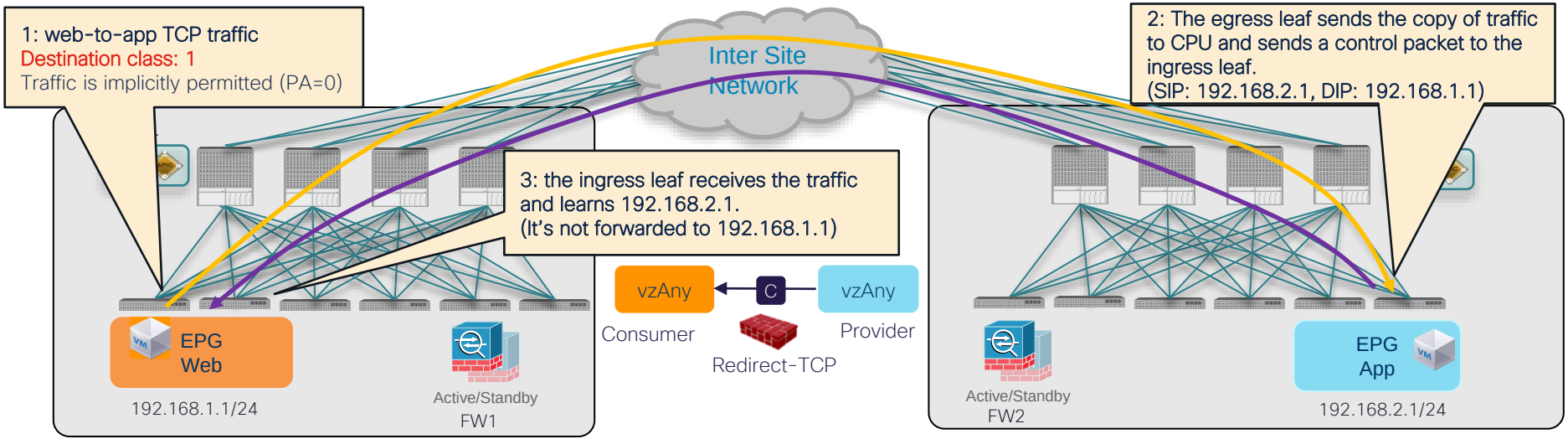


ACI Multi-Site vzAny-to-vzAny PBR

What if the ingress leaf doesn't know the destination class ID (3/3)

Roadmap

- Conversational Learning to get the ingress leaf learn the destination EP.

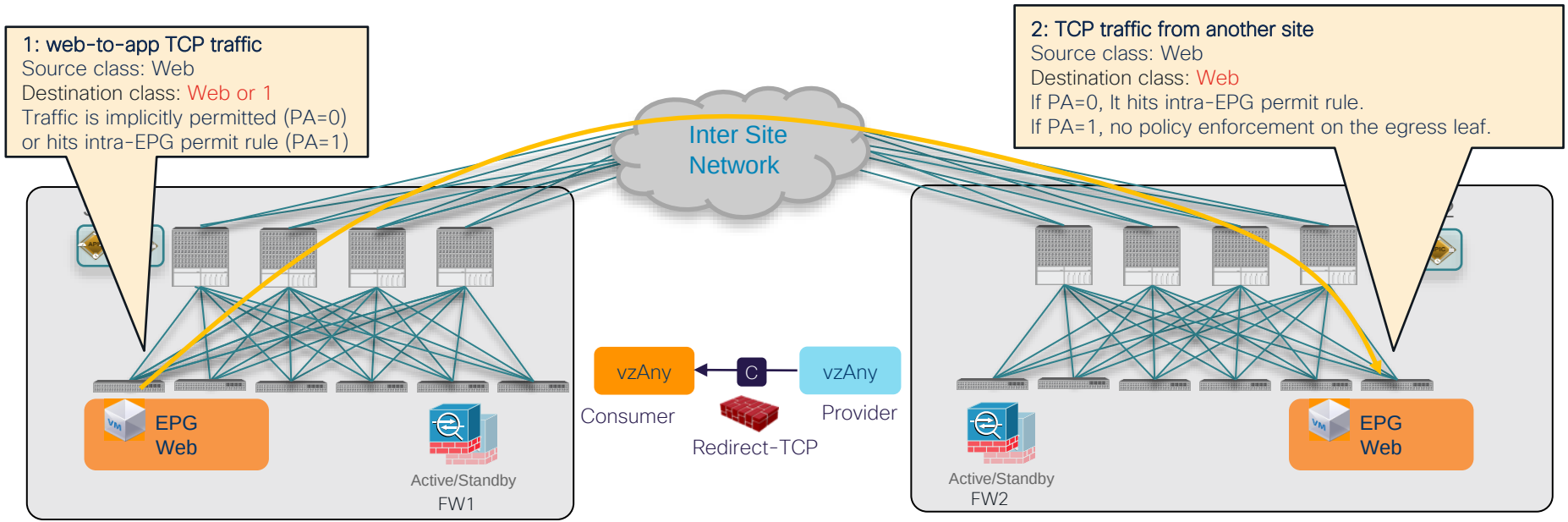


ACI Multi-Site vzAny-to-vzAny PBR

Intra-EPG traffic

Roadmap

- Intra-EPG permit rule (priority 3) wins over vzAny-to-vzAny rule (priority 17).

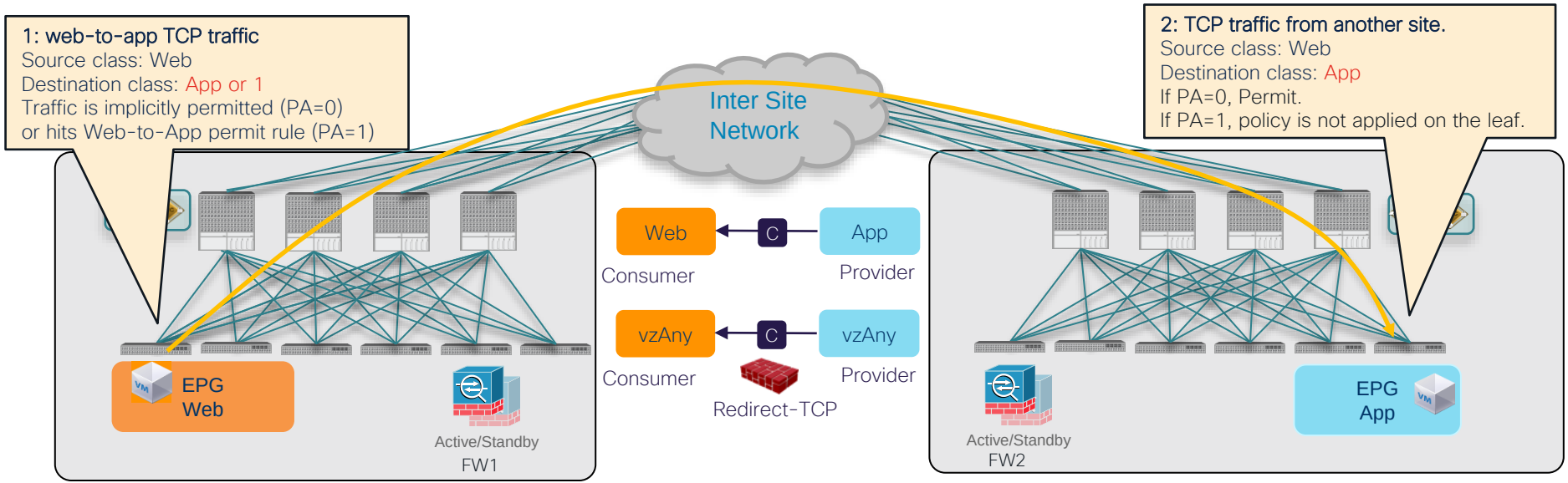


ACI Multi-Site vzAny-to-vzAny PBR

Bypass firewall for specific EPG-to-EPG traffic

Roadmap

- EPG-to-EPG permit rule (priority 7 or 9) wins over vzAny-to-vzAny rule (priority 17).



ACI Multi-Site

Roadmap: vzAny PBR and L3Out-to-L3Out PBR

	vzAny-to-vzAny	vzAny-to-EPG	vzAny-to-L3Out	L3Out-to-L3Out
Redirection	Both sites	Site for the specific EPG	Both sites	Both sites
Service node	One-node One-arm	Single and two-node One-arm and two-arm	One-node One-arm	One-node One-arm
VRF	Intra-VRF	Intra-VRF	Intra-VRF	Intra-VRF and Inter-VRF

- By configuring specific EPG-to-EPG contract, firewall can be bypassed. EPG subnet configuration is not required for the specific EPGs.
- Each site needs to have PBR destination with decent high availability within the site.

Conclusions

Summary

- How ACI PBR works, use cases and design tips
- Flexible traffic redirection.
  - Redirect specific traffic based on contract.
  - Intra-subnet and intra-EPG/ESG redirection.
  - Any-to-Any, Any-to-EPG/ESG redirection.
- Scale easily.
  - Symmetric PBR with tracking and resilient hash
  - PBR destinations can be L1/L2/L3 devices anywhere in the fabric.
- Multi-Location Data Centers
  - Multi-Site vzAny PBR will be coming!
- For configuration steps, please check ACI PBR white paper!

Useful Links

- Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Design White Paper

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739971.html

- Cisco ACI Contract Guide

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html

- Service Graph Design with Cisco ACI (Updated to Cisco APIC Release 5.2) White Paper

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-2491213.html

- ACI Fabric Endpoint Learning White Paper

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739989.html

Useful Links

- Cisco ACI and F5 BIG-IP Design Guide White Paper

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743890.html

- Cisco ACI Multi-Pod and Service Node Integration White Paper

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739571.html

- Cisco ACI Multi-Site and Service Node Integration White Paper

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743107.html

Complete your 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 (open from 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 Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN