You make **possible**

Let's Get Started with ACI Service Insertion

Minako Higuchi, Technical Marketing Engineer @DCBG

BRKACI-2486

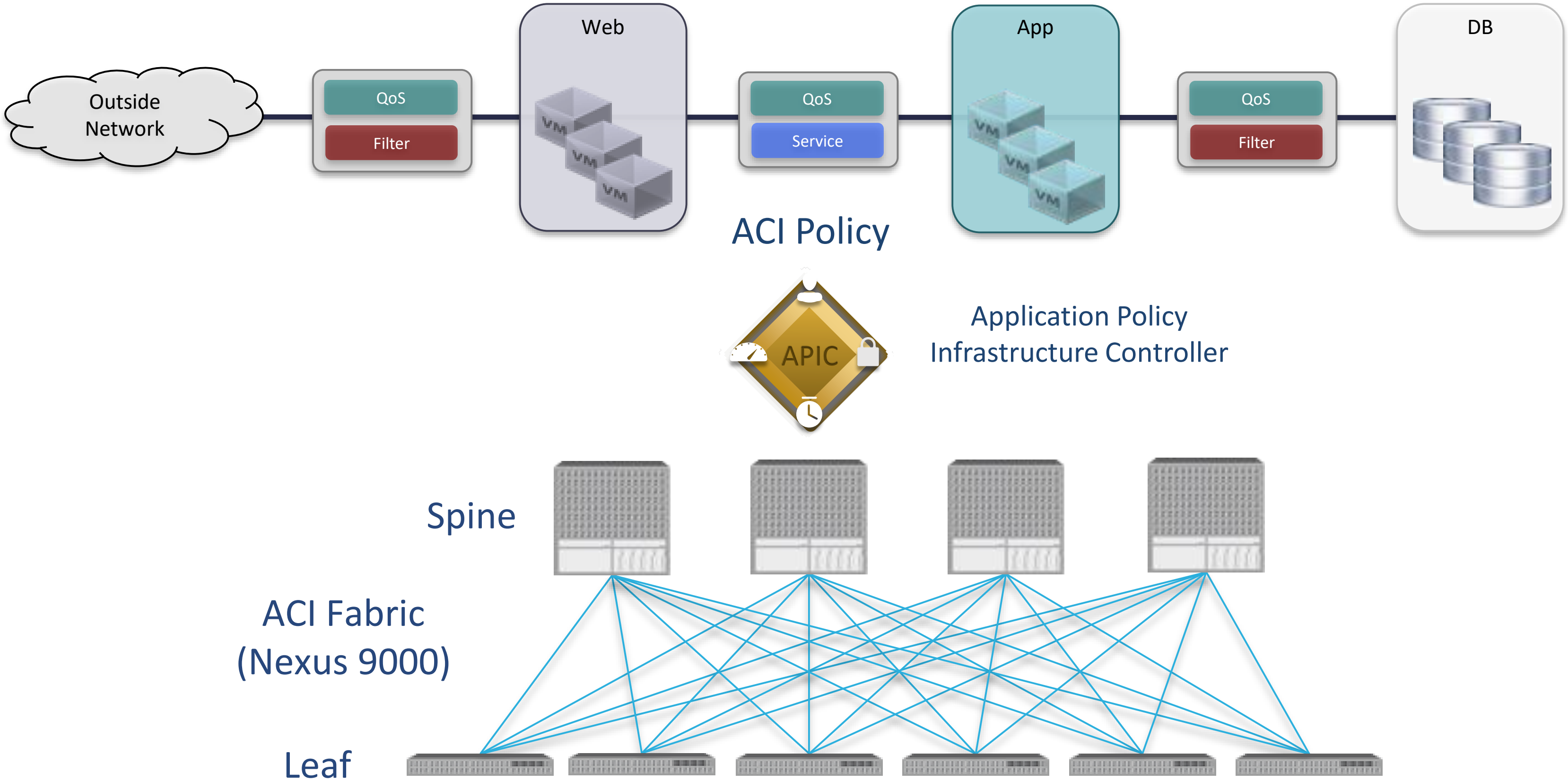
Agenda

- ACI Contract security
- ACI L4-L7 service integration
  - Firewall Design Options
  - Load Balancer Design Options
  - Multi-Pod/Multi-Site Design Options
- Q&A

ACI Contract security

You make networking **possible**

Cisco ACI - Logical Network Provisioning



Outside Network

QoS

Filter

Web

QoS

Service

App

QoS

Filter

DB

ACI Policy

APIC

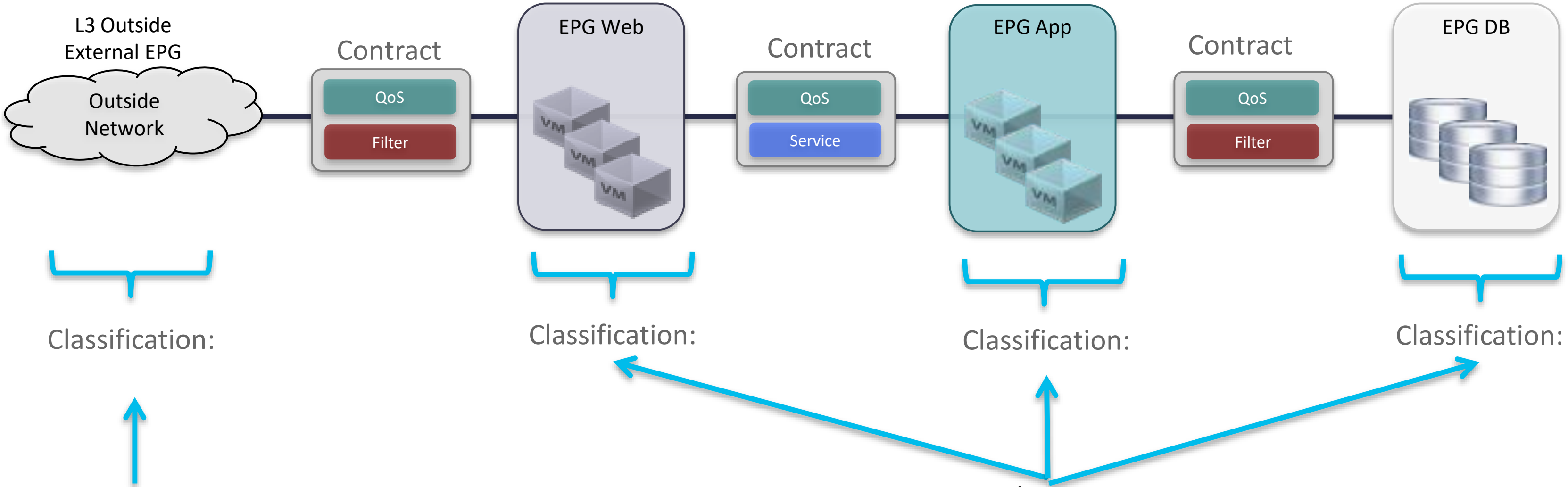
Application Policy Infrastructure Controller

Spine

ACI Fabric (Nexus 9000)

Leaf

Cisco ACI Policy Constructs
EPG (End Point Group) and Contract



EPG Classification on L3 Outside is based on IP address Network/Mask

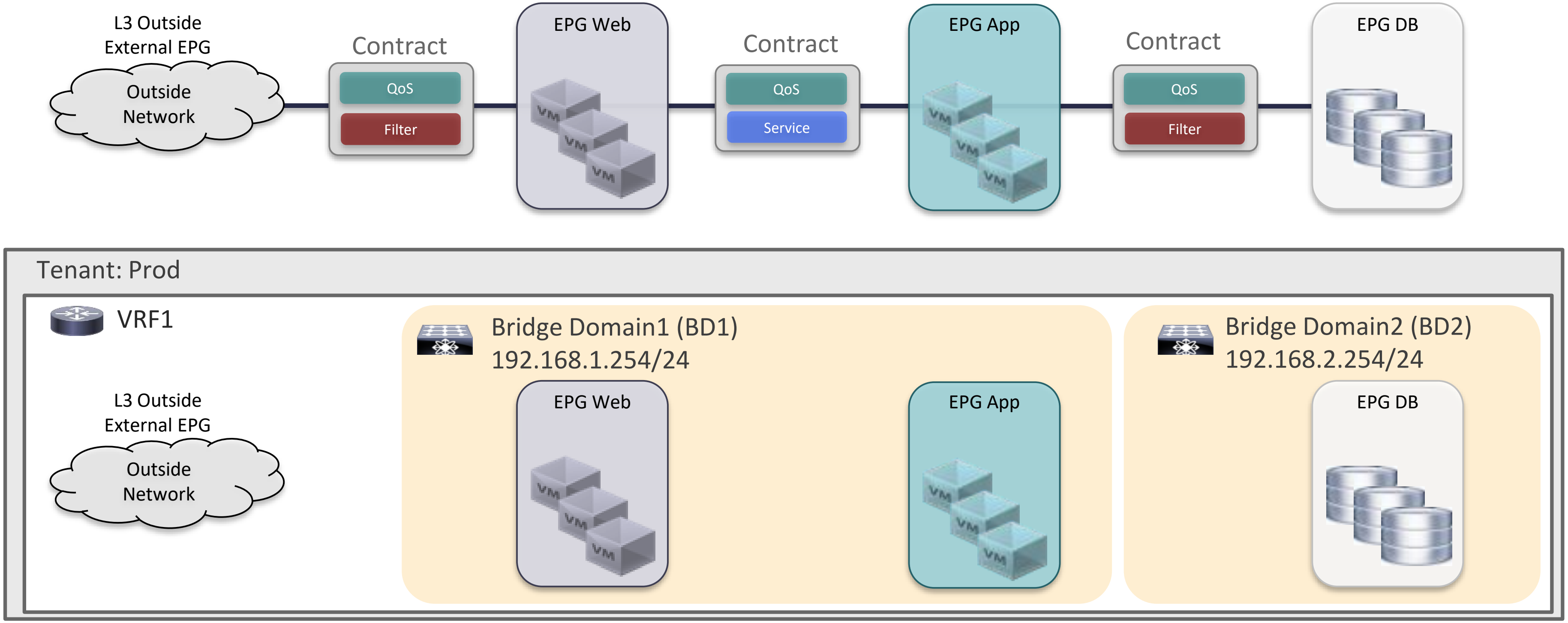
EPG Classification on an access/server port is based on different attributes

- Port + VLAN, Port + VXLAN, Network/Mask
- IP, MAC Address
- IP, MAC, VM Attributes for VM’s

Physical, Virtual, container endpoints can co-exist in same EPG

Cisco ACI Policy Constructs

Tenants, Application Profiles, Bridge Domains, VRFs



Micro-Segmentation with ACI

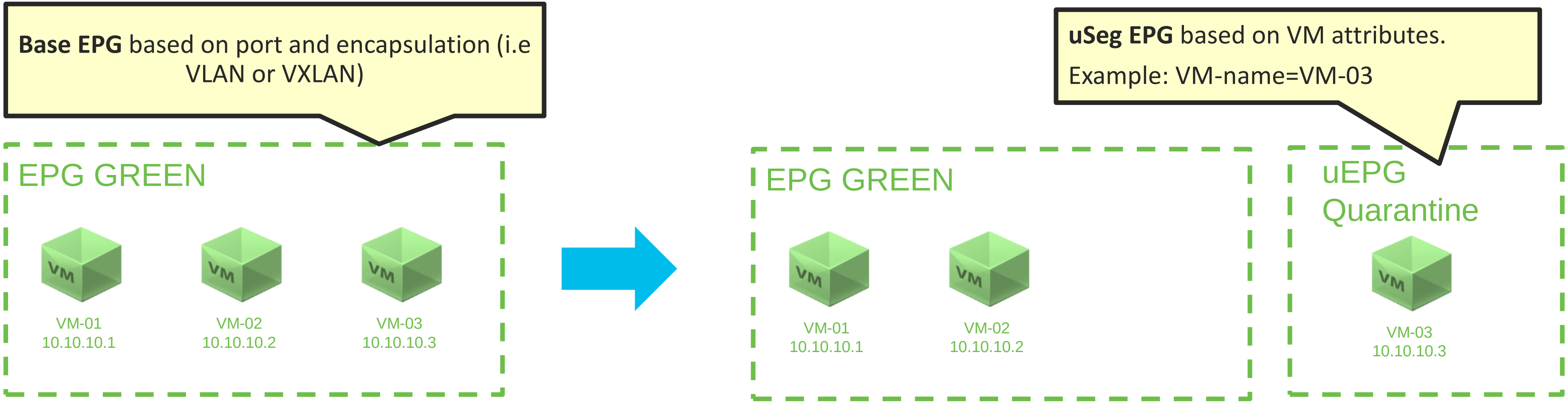
- Micro EPG (uSeg EPG)
  - EPG classification based on IP, MAC, VM attributes

- Intra-EPG isolation
  - Deny traffic between endpoints in same EPG

- Intra-EPG contract
  - Contract enforcement on traffic between endpoints in same EPG

Micro EPG (uSeg EPG)

- EPG classification based on IP, MAC, VM attributes
- Endpoints assigned to the uEPG regardless of the encapsulation/port



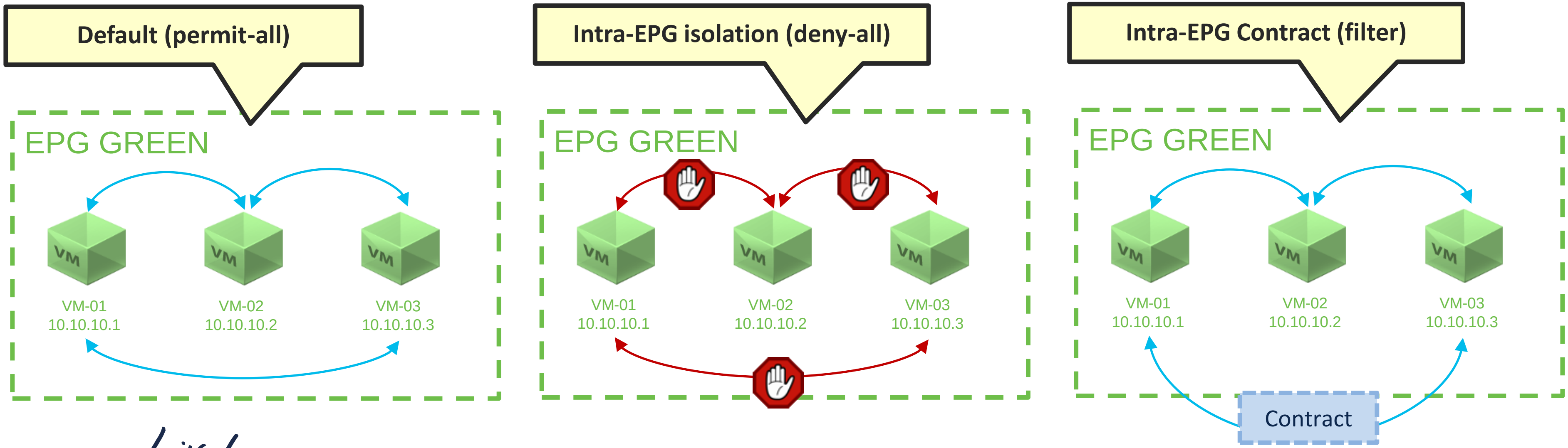
Base EPG based on port and encapsulation (i.e VLAN or VXLAN)

uSeg EPG based on VM attributes.

Example: VM-name=VM-03

Intra-EPG Isolation and Intra-EPG Contract

- By default, endpoints in same EPG can talk without contract (permit-all)
- Intra EPG isolation is an option to deny traffic within an EPG (deny-all)
- Intra EPG contract is an option to filter traffic within an EPG (filter)



ACI L4-L7 Service integration

You make networking **possible**

L4-L7 Design Tips

- Understand desired traffic flow
  - North-South FW?
  - East-West FW?
  - Service Chain order?
  - Is there IP and/or port translation?

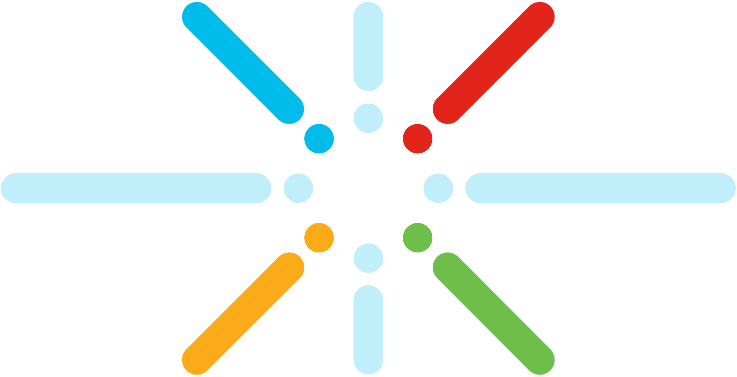
- Are there devices located in multiple DCs?

L4-L7 Design Options

Understand Requirements

- Firewall/IPS
  - Firewall: Layer 1(inline), Layer 2(Transparent) or Layer 3(Routed)?
  - Gateway: ACI or Firewall?
  - Insertion: VLAN/VRF stitching or PBR?
  - HA option: Active/Standby, Active/Active Cluster or Independent Active nodes
- Load Balancer
  - Load Balancer: Layer 3
  - How to handle return traffic: LB as Gateway, SNAT, PBR or DSR?
  - HA option: Active/Standby
  - VIP: Is VIP in self IP subnet range?

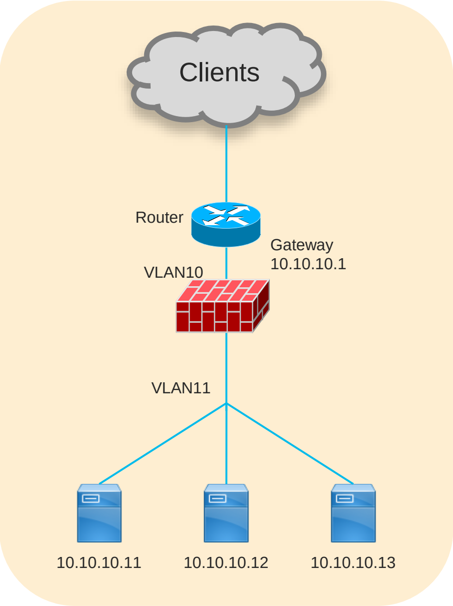
Firewall Design Options



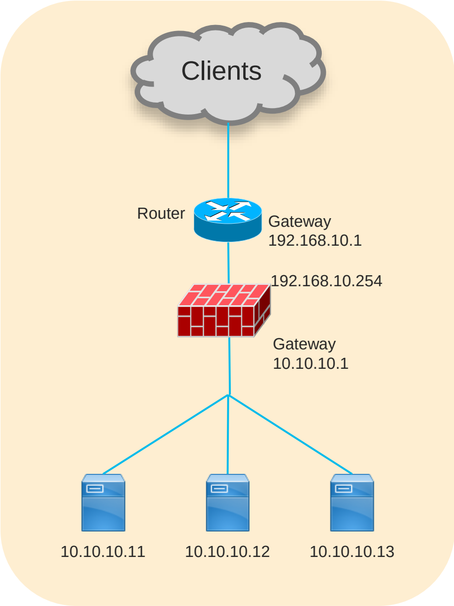
You make networking **possible**

Firewall Design Options

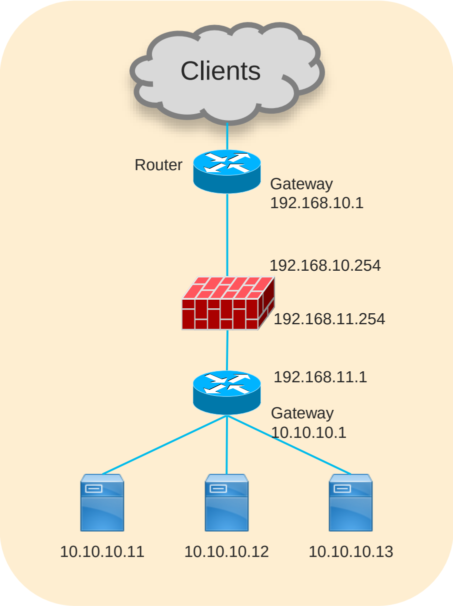
L2 FW
VLAN stitching



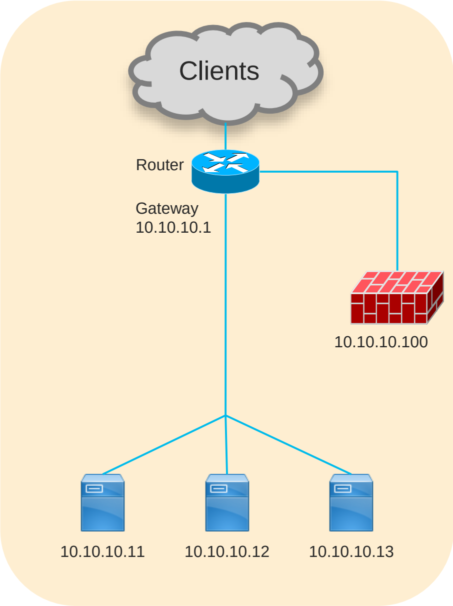
L3 FW
FW as gateway



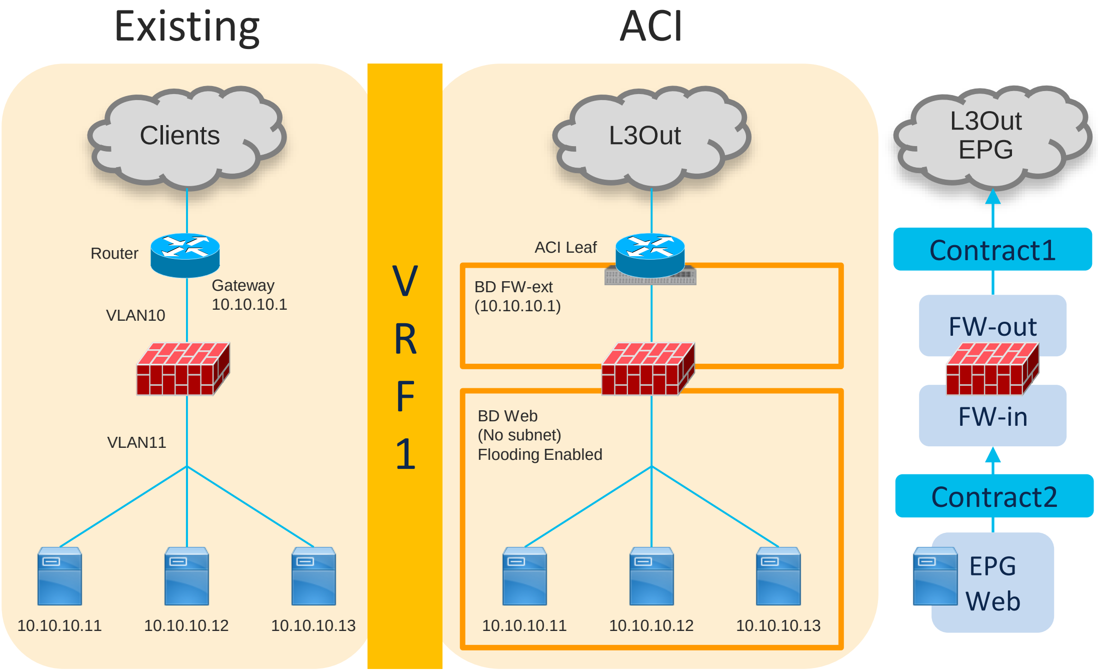
L3 FW
Fabric as gateway
VRF sandwich



L3 FW
Fabric as gateway
PBR



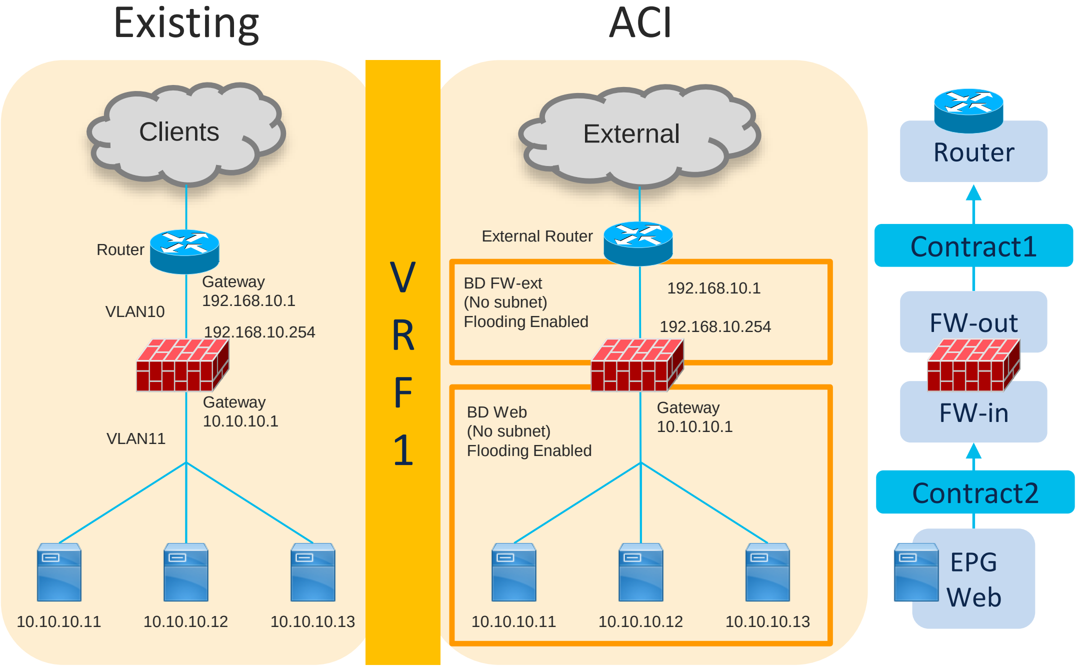
Option 1: L2 Firewall with VLAN Stitching



- Traditional VLAN stitching
- FW and EPG are in same BD
- ACI as L3
- All inter-BD traffic goes through FW
- Simple
- Service Graph is not mandatory

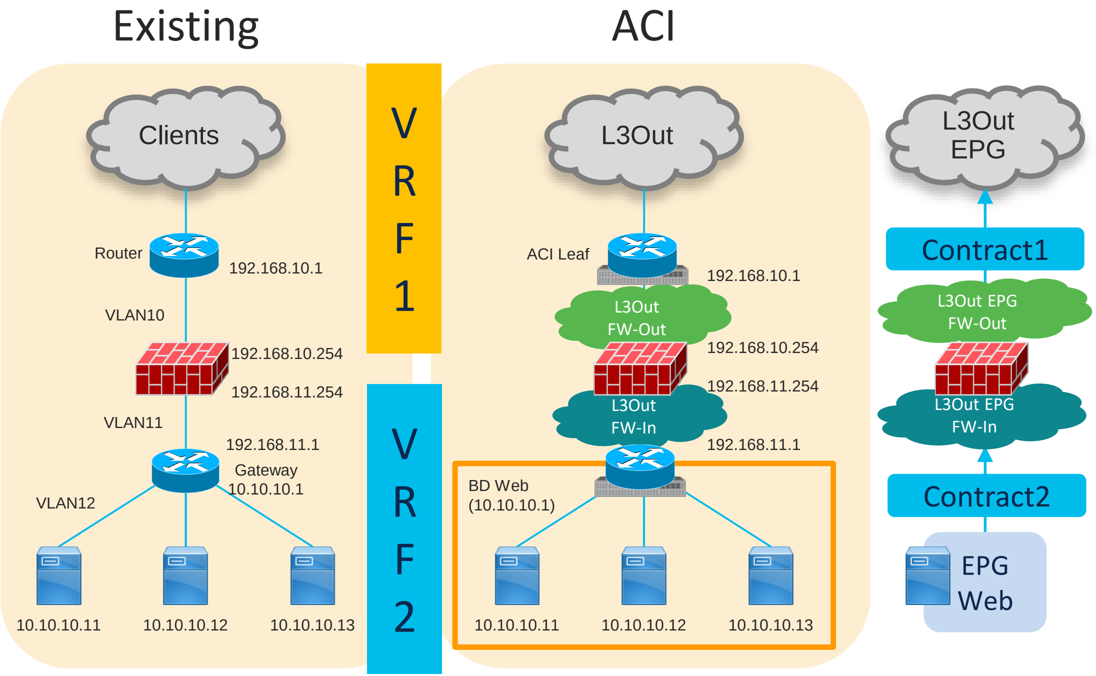
- L1/L2 PBR available in 4.0 that requires ACI as gateway and dedicated service BDs.

Option 2: L3 Firewall with the Firewall as the Default Gateway



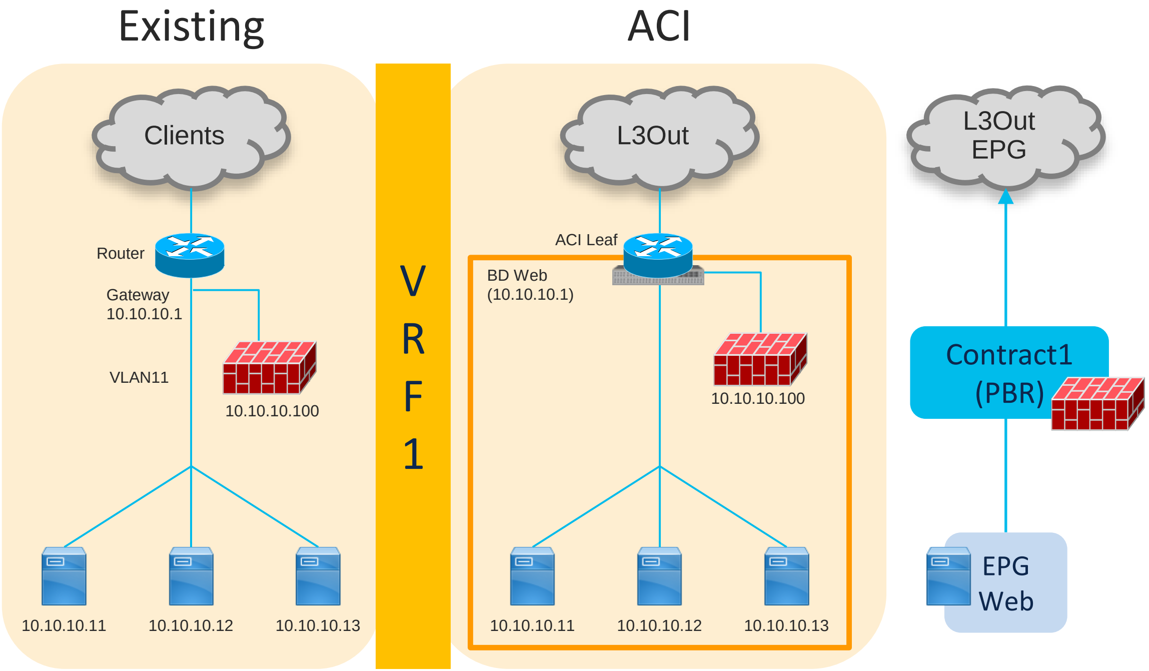
- FW as gateway
- FW and EPG are in same BD
- ACI as L2
- All inter-subnet traffic goes through FW
- Simple
- Service Graph is not mandatory

Option 3: L3 Firewall with the Fabric as the Default Gateway – "VRF sandwich"



- Traditional VRF sandwich.
- FW is in L3out
- ACI as L3
- All inter-VRF traffic goes through FW
- Require multiple VRFs and L3outs
- Service Graph is not mandatory
- Good for North-South FW

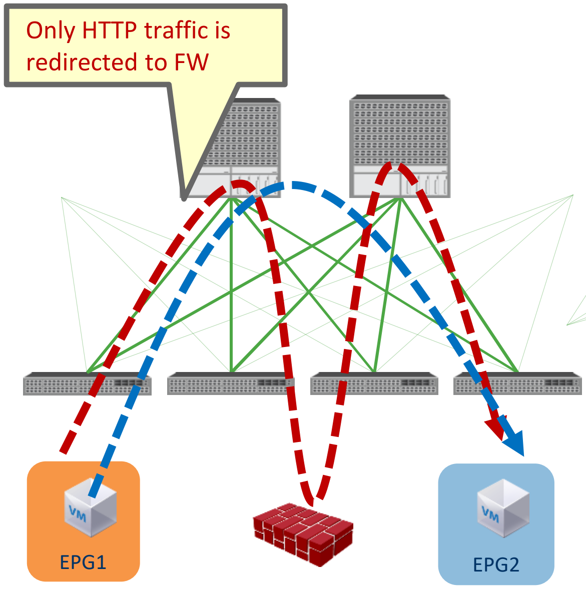
Option 4: L3 Firewall with the Fabric as the Default Gateway, Redirect with PBR



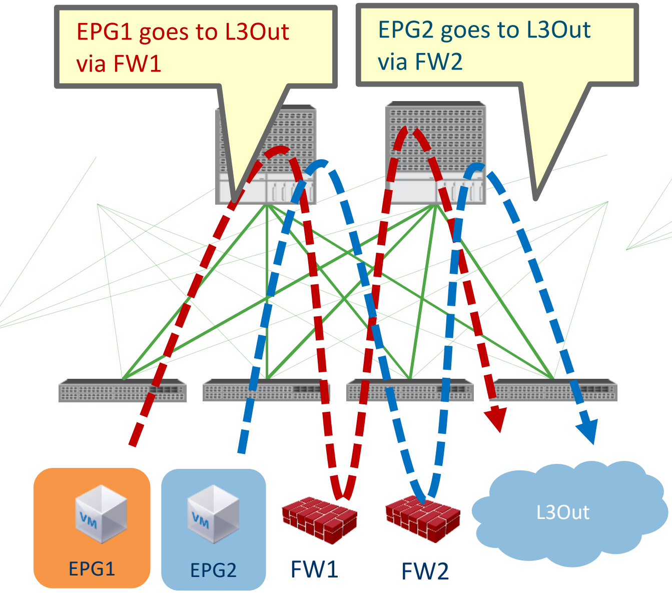
- PBR (Policy Based Redirect).
- ACI as L3
- FW is in BD
- Specific traffic goes through FW
- FW can be two or one arm mode
- Good for East-West
- Requires the use of Service-Graph
- Service device can be in same or different BD with servers

ACI PBR Use Cases

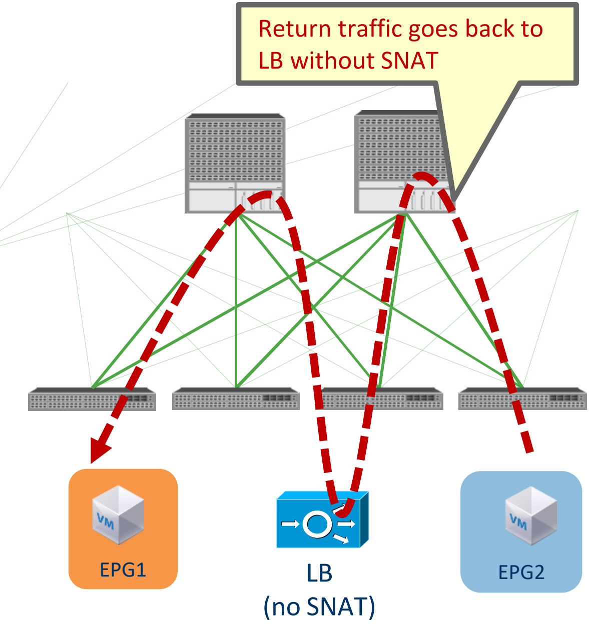
- Inspect specific traffic



- Use different Firewall



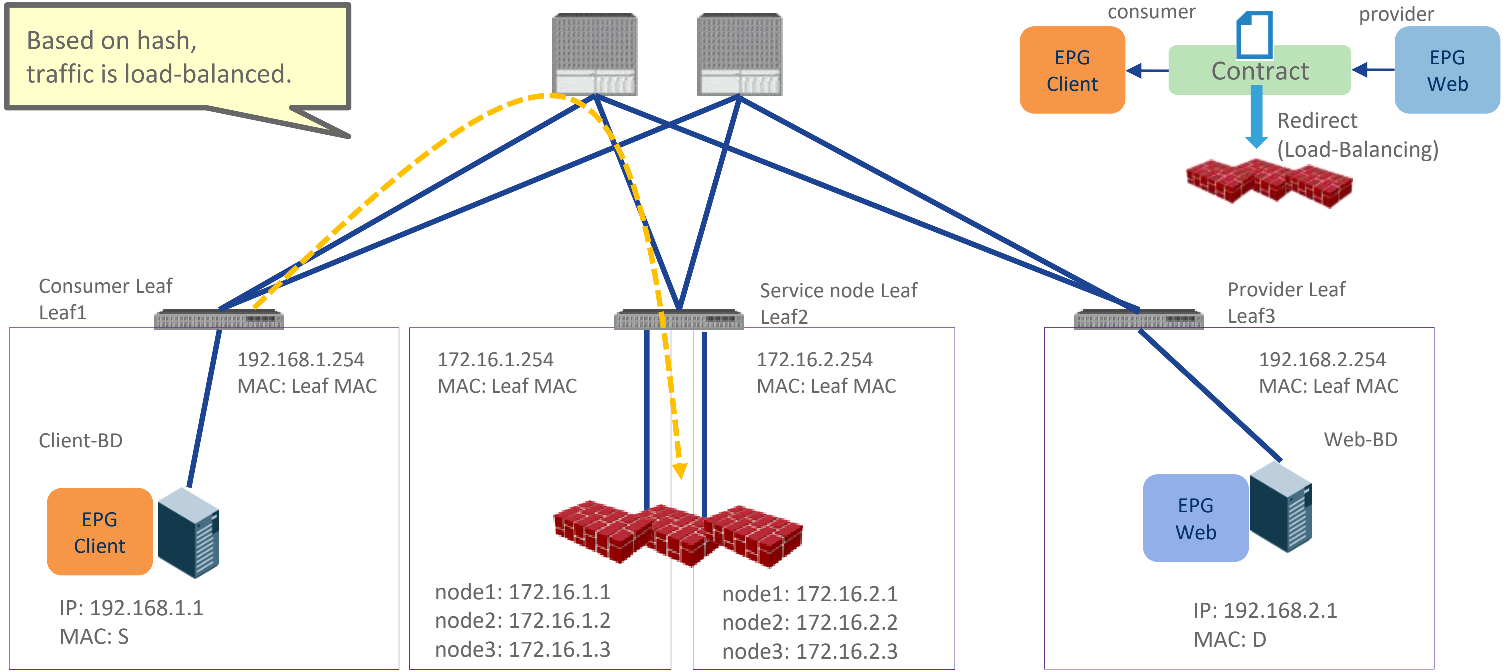
- LB without SNAT



Symmetric PBR: Scale Firewall Easily

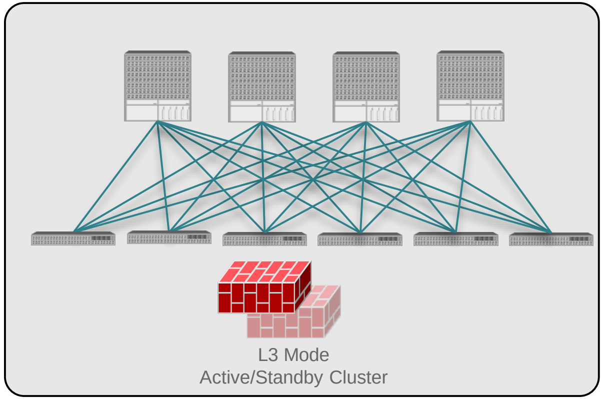
- Ensure incoming and return traffic goes to same firewall

Based on hash,
traffic is load-balanced.



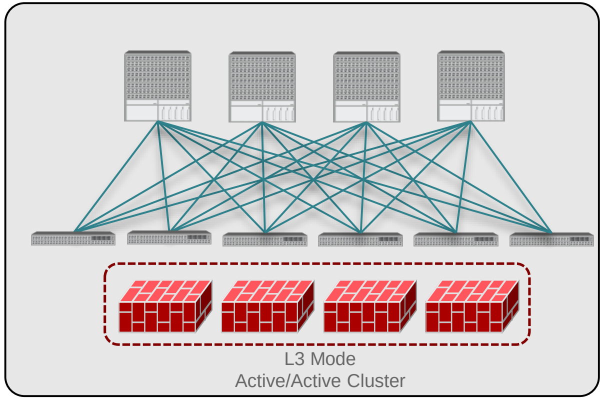
HA Options

Active/Standby Cluster



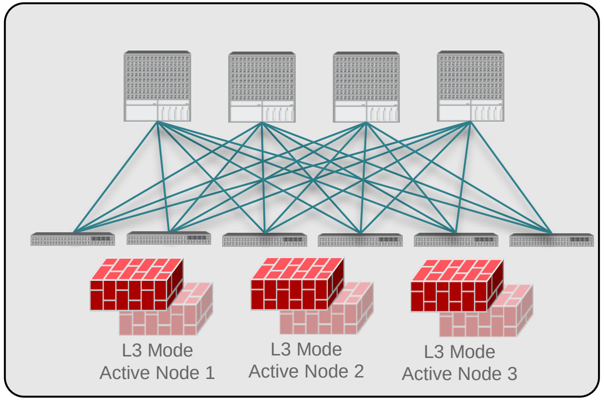
- PBR is not mandatory
- The Active/Standby pair represents a single MAC/IP entry.

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



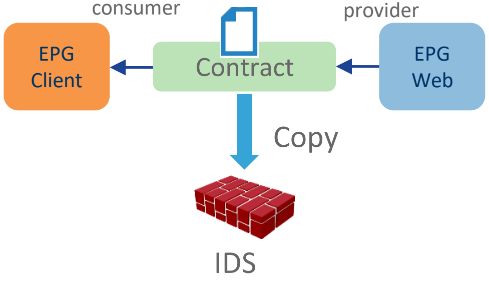
- PBR is required if the cluster is stretched across pods.
- The Active/Active cluster represents a single MAC/IP entry.
- Spanned Ether-Channel Mode supported with Cisco ASA/FTD platforms

Independent Active Nodes ('Scale-Out' Model)

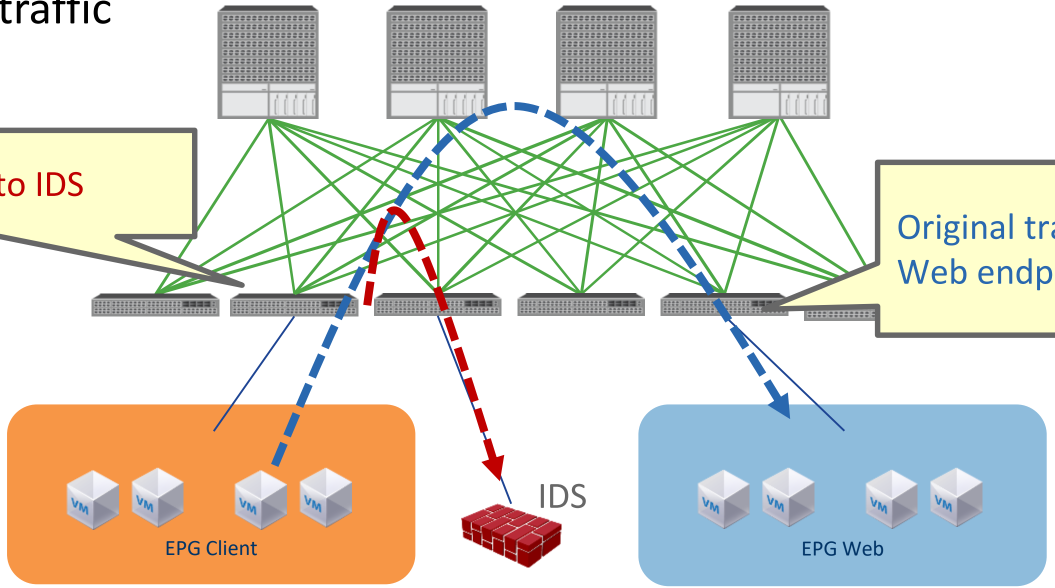


- PBR is required.
- Each Active node represent a unique MAC/IP entry.
- Use of Symmetric PBR to ensure each flow is handled by the same Active node in both directions

Copy Service



- APIC 2.0
- Service Graph is mandatory and EX/FX hardware is required
- Copy specific traffic



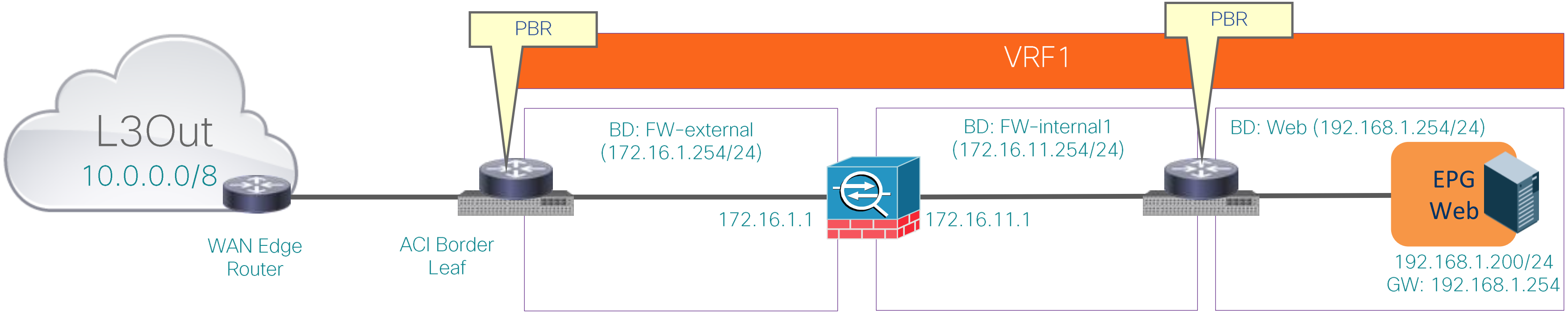
Traffic is copied to IDS

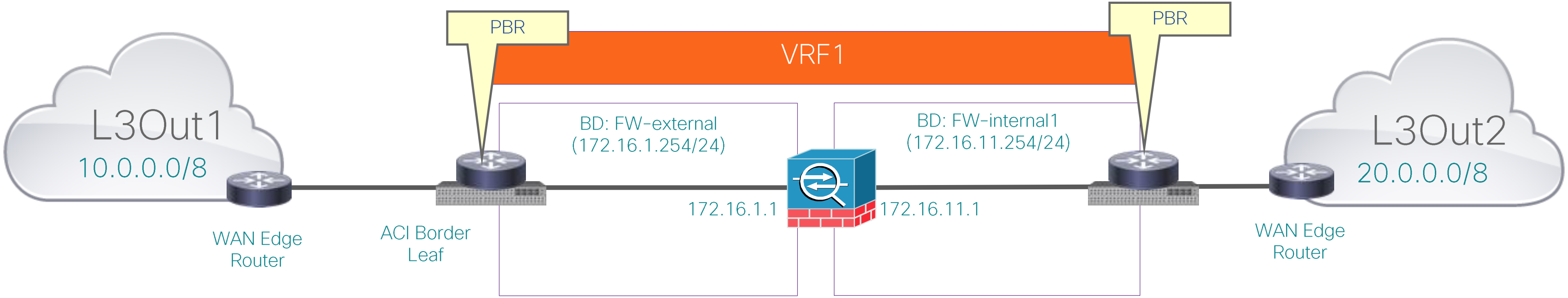
Original traffic goes to Web endpoint directly.

PBR Design FAQ

You make networking **possible**

Can We Use PBR for L3out EPG?

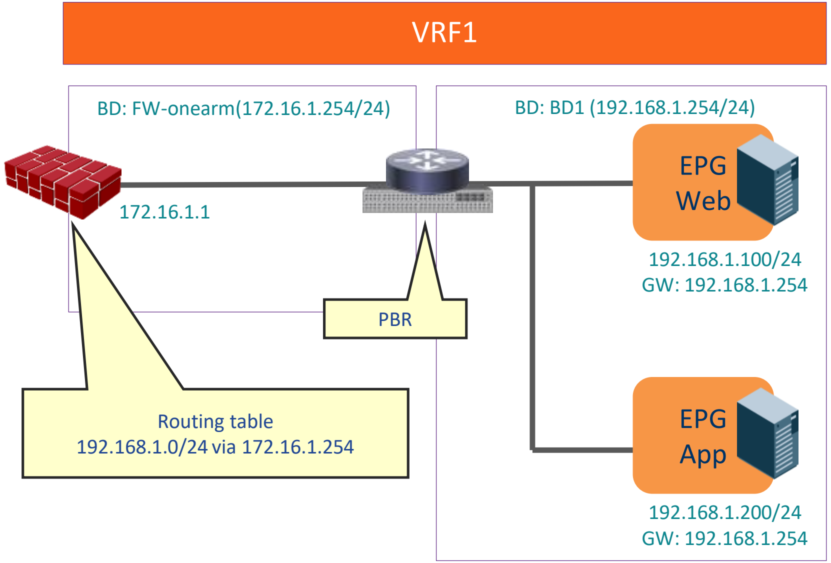


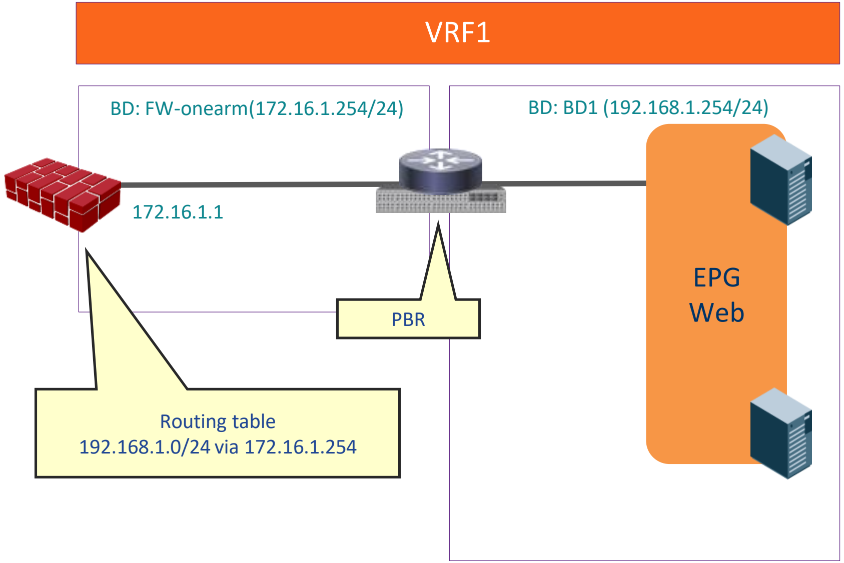


Can We Use PBR for EPGs in Same Subnet?

- Inspection between endpoints in same subnet

- Inspection between endpoints even in same EPG



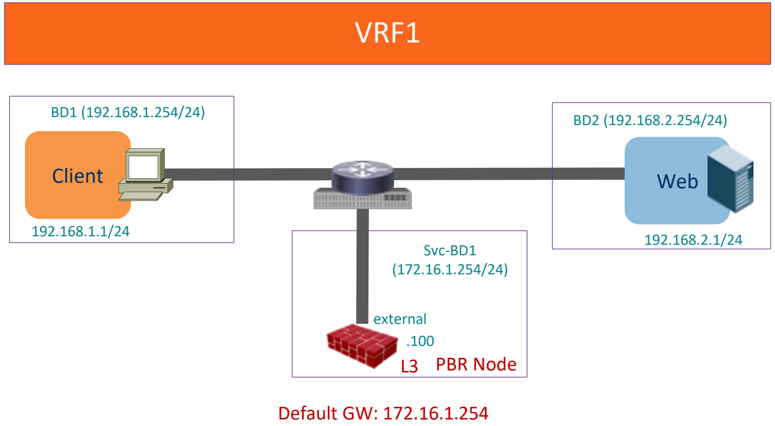


VRF1
BD: FW-onearm(172.16.1.254/24)
BD: BD1 (192.168.1.254/24)
172.16.1.1
PBR
EPG Web
Routing table
192.168.1.0/24 via 172.16.1.254

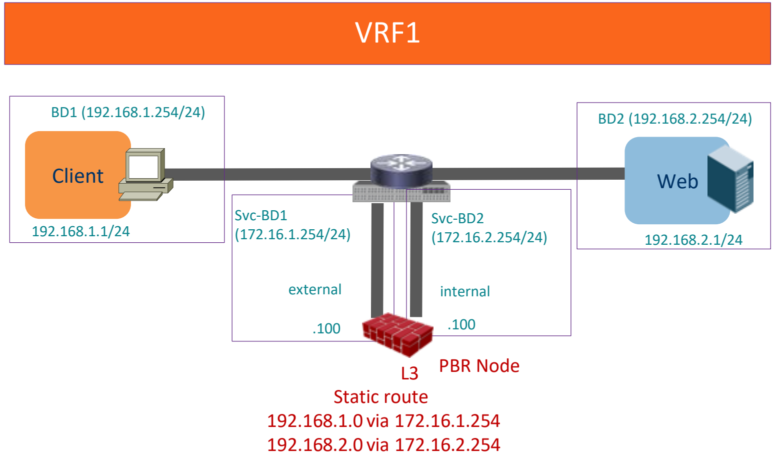
One-Arm vs Two-Arm?

- One-Arm
  - Simple routing design on service node
  - 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

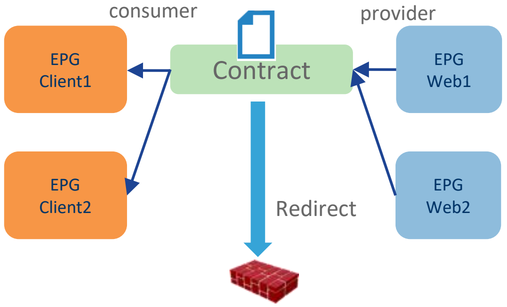


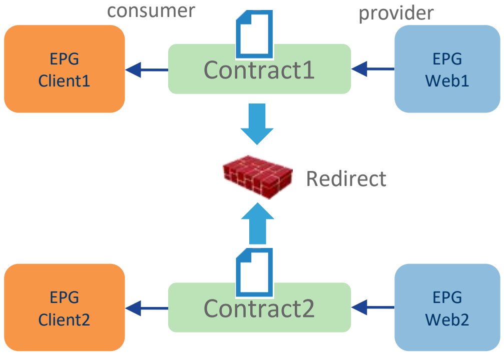
Default GW: 172.16.1.254



Static route
192.168.1.0 via 172.16.1.254
192.168.2.0 via 172.16.2.254

Can We Reuse Same PBR Node Multiple Times?





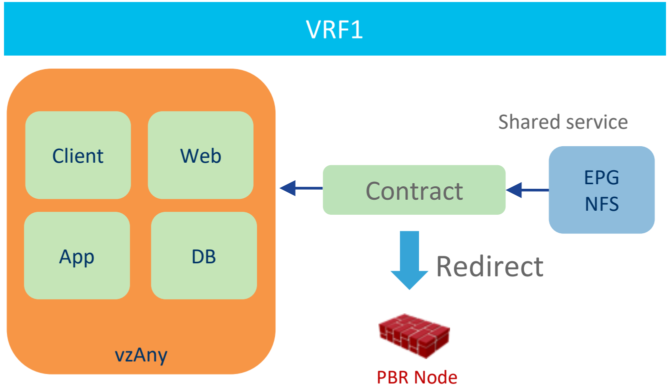
- Multiple consumer/provider EPGs
- Multiple contracts using same PBR destination and Service Graph.

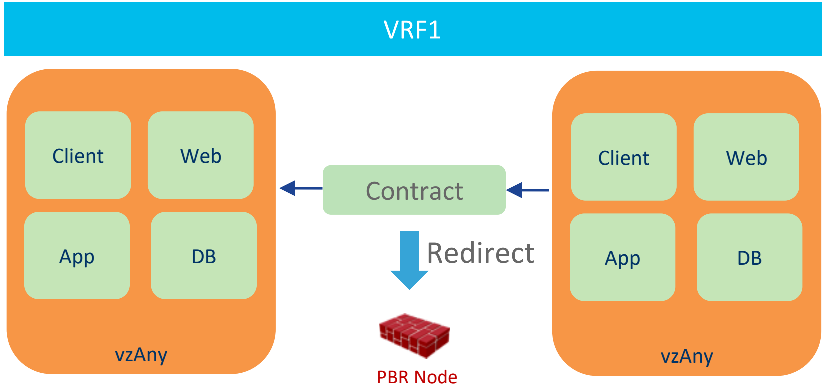
- Note
  - Depending on routing design, one-arm mode deployment may be required.

ACI 3.2

Can We Insert Firewall to Any-To-Shared-Service?

- vzAny is useful if we have a security requirement that is applied to all EPGs in same VRF and also it helps to reduce policy TCAM consumption.
- Prior to 3.2, PBR with vzAny (consumer) is supported.
- In ACI 3.2, PBR with vzAny (provider) is also supported.
- Use case: Insert Firewall everywhere.

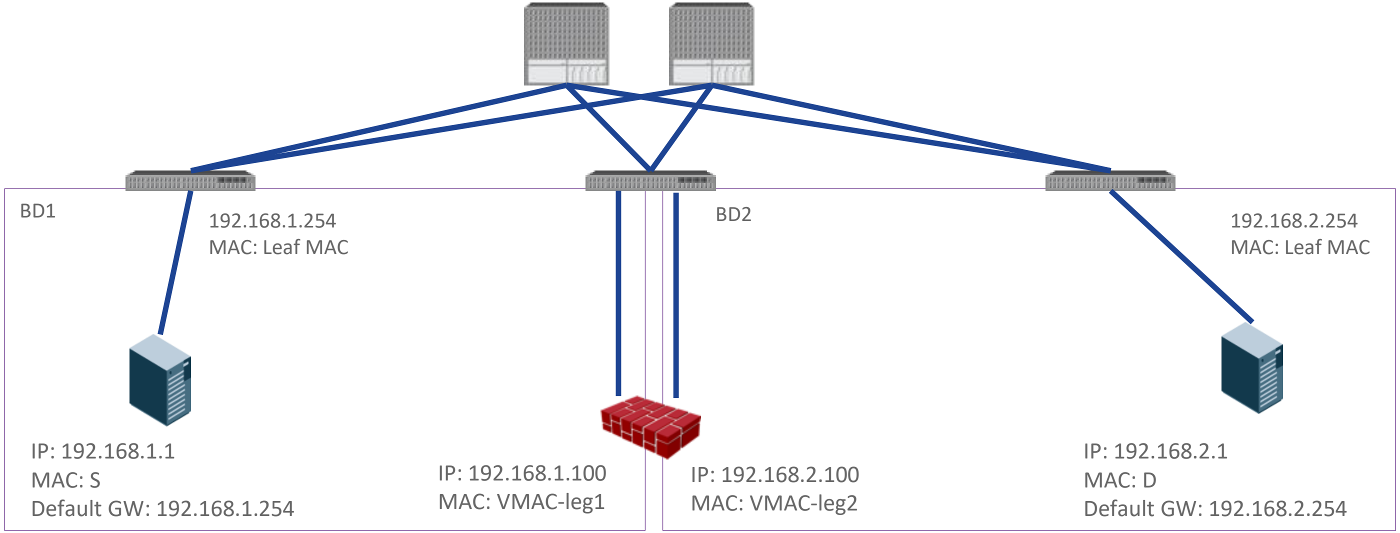




ACI 3.1

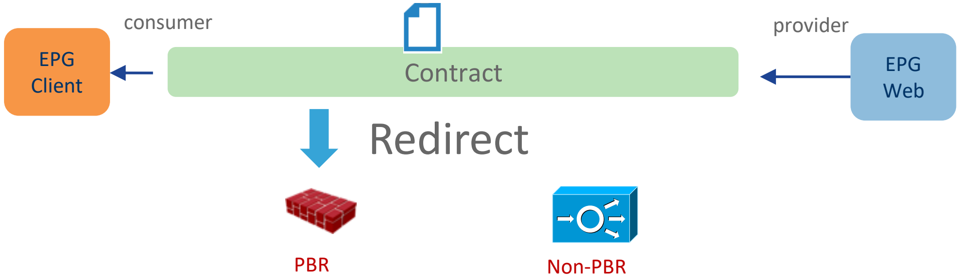
Can PBR Node be in Consumer/Provider Subnet?

- Prior to APIC version 3.1, PBR node must be different than the consumer/provider BDs.
- Starting from APIC version 3.1, this requirement no longer mandatory. (Need EX/FX Leaf)

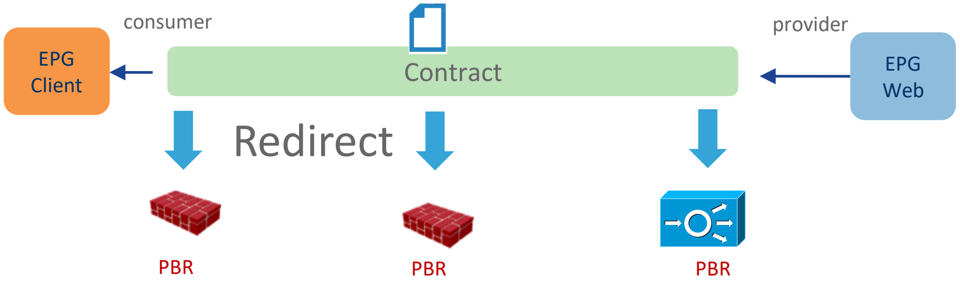


Can We Concatenate Services? Multi-Node PBR

- Prior to ACI 3.2: Concatenating PBR nodes is not supported.
    - For example, both 1st and 2nd node can't be PBR nodes. Either one of them can be.



- ACI 3.2: Support more than 1 node PBR in a Service Graph.

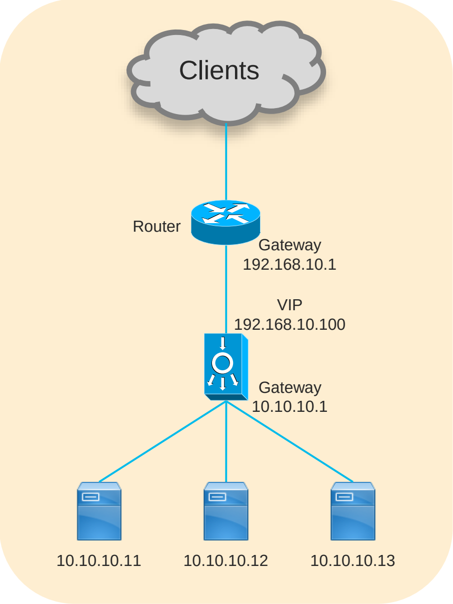


Load Balancer Design Options

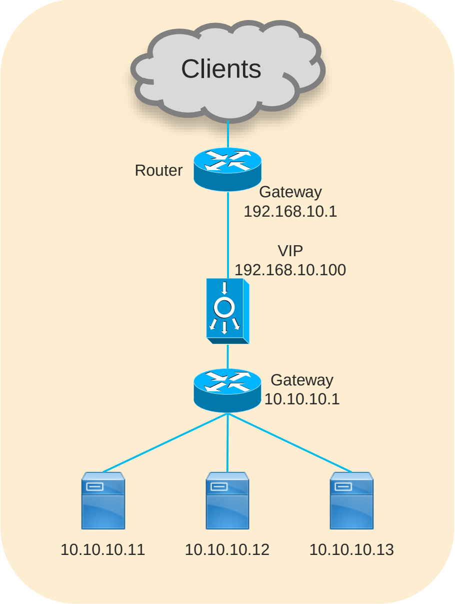
You make networking **possible**

Load Balancer Design Options

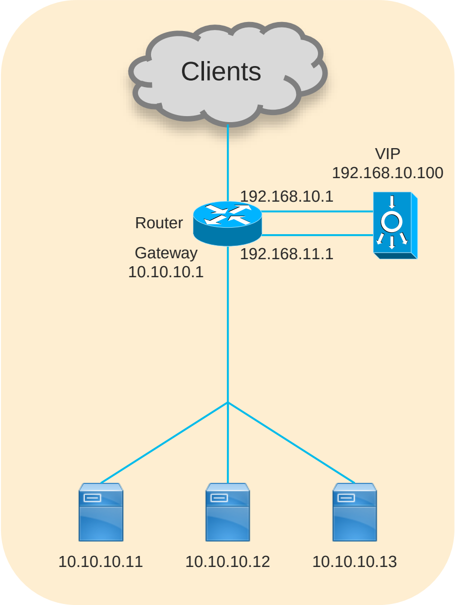
Two-arm (inline)
LB as Gateway
No SNAT/PBR



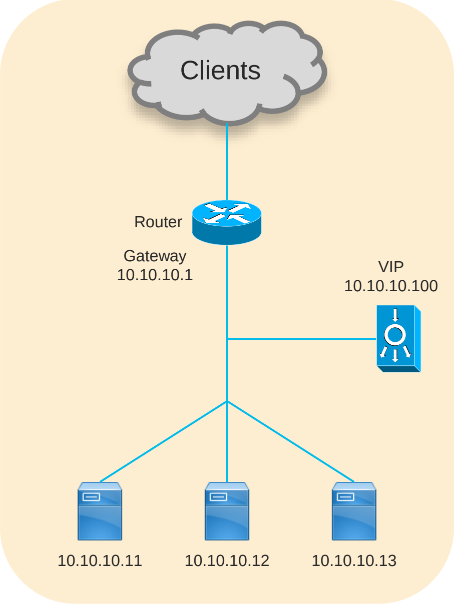
Two-arm (inline)
Fabric as Gateway
VRF sandwich



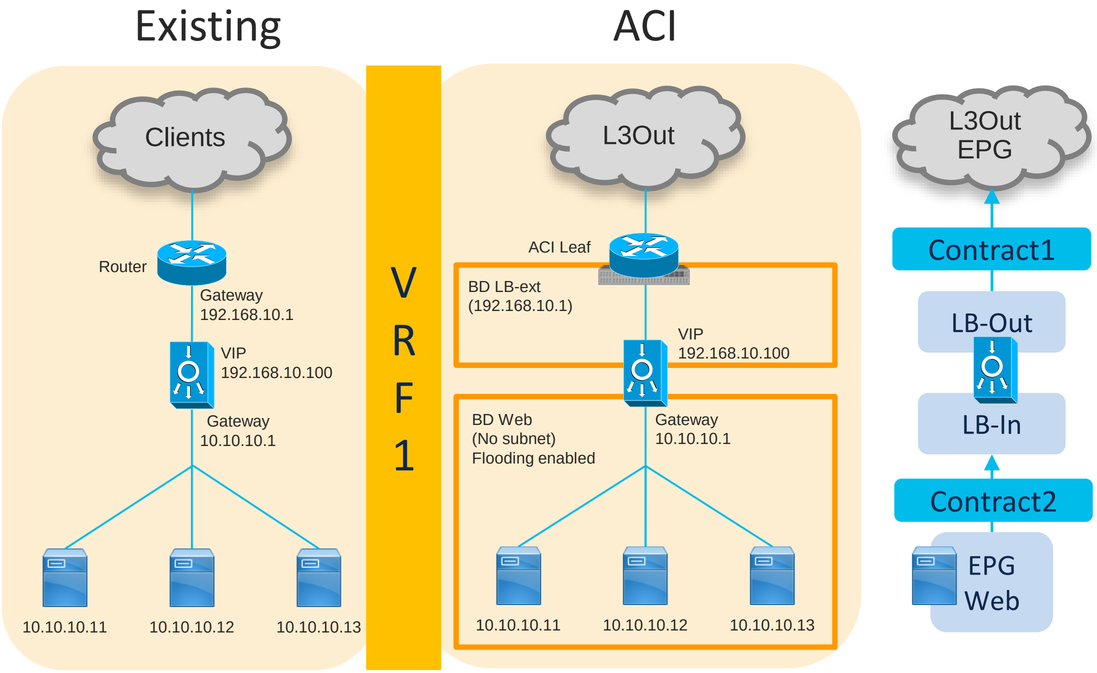
Two-arm
Fabric as Gateway
SNAT/PBR



One-arm
Fabric as Gateway
DSR/SNAT/PBR

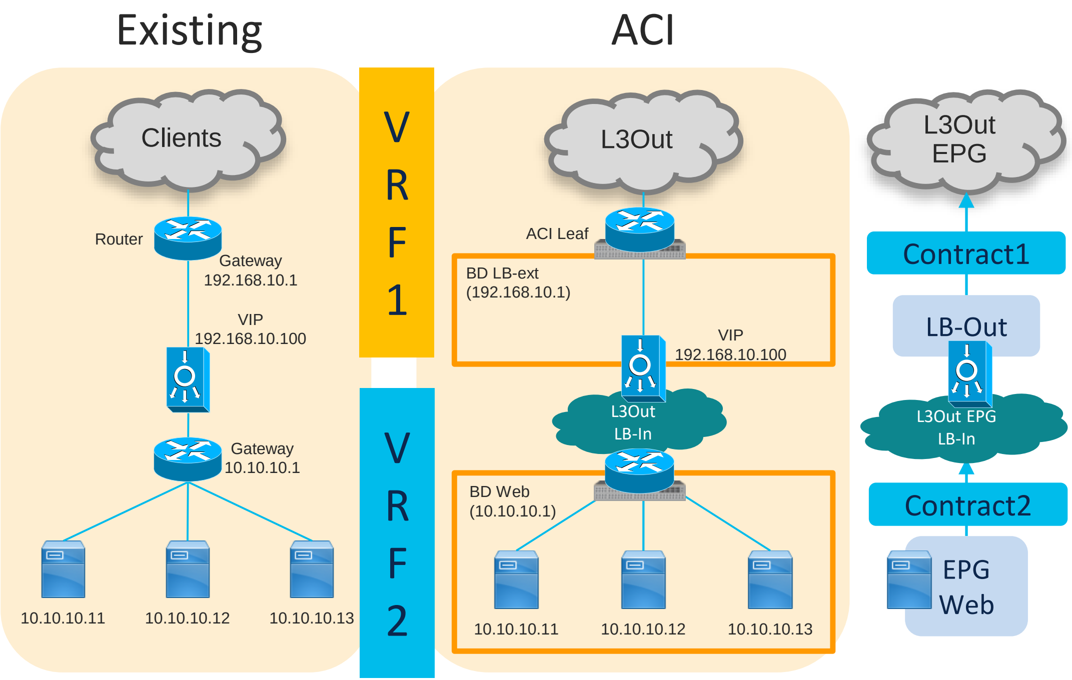


Option 1: Two-Arm (Inline) with the SLB as the Default Gateway



- LB and EPG are in same BD
- ACI as L2
- All inter-BD traffic goes through LB
- Simple
- ACI can be L3 for external side of LB
- Service Graph is not mandatory
- SNAT/PBR is not required

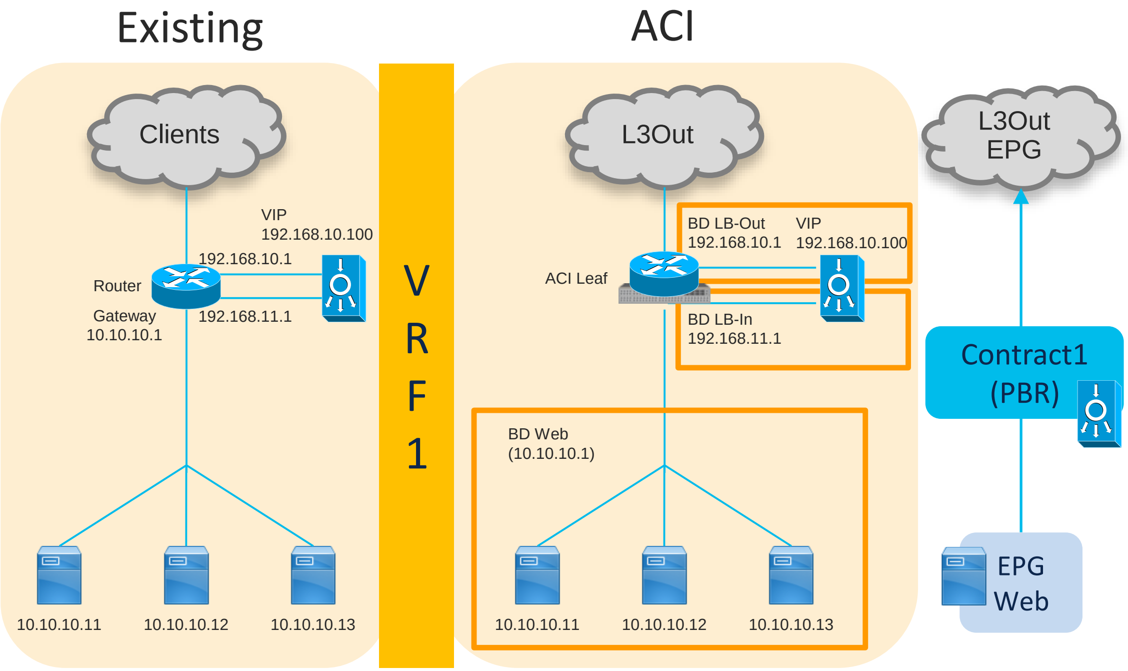
Option 2: Two-Arm (inline) with the Fabric as the Default Gateway



- Traditional VRF sandwich
- ACI as L3
- All inter-VRF traffic goes through LB
- Service Graph is not mandatory
- SNAT/PBR is not required

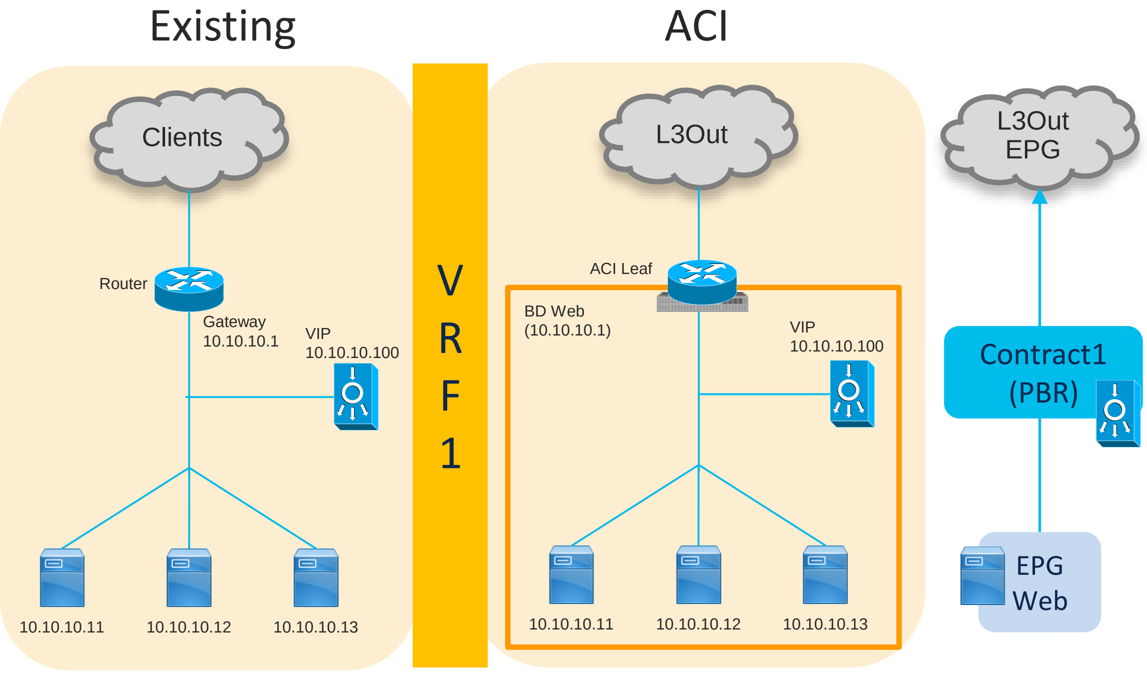
- If SNAT is enabled on LB using LB internal interface as NAT IP, LB-in can be in a BD. VRF2 and L3Out LB-in are not required.

Option 3: Two-Arm with the Fabric as the Default Gateway – SNAT/PBR



- PBR or SNAT is required
- ACI as L3
- Service device can be in same or different BD with servers
- If it's PBR:
  - Service Graph is required
  - Specific traffic goes through LB

Option 4: One-Arm with the Fabric as the Default Gateway - L2DSR/SNAT/PBR



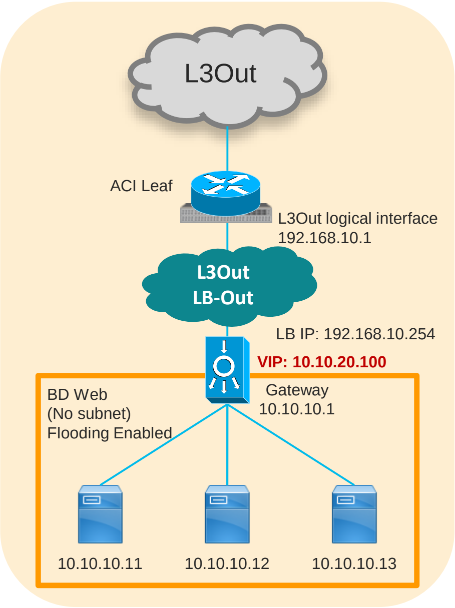
- L2DSR, PBR or SNAT is required
- ACI as L3
- Service device can be in same or different BD with servers

- If it’s PBR:
  - Service Graph is required
  - Specific traffic goes through LB

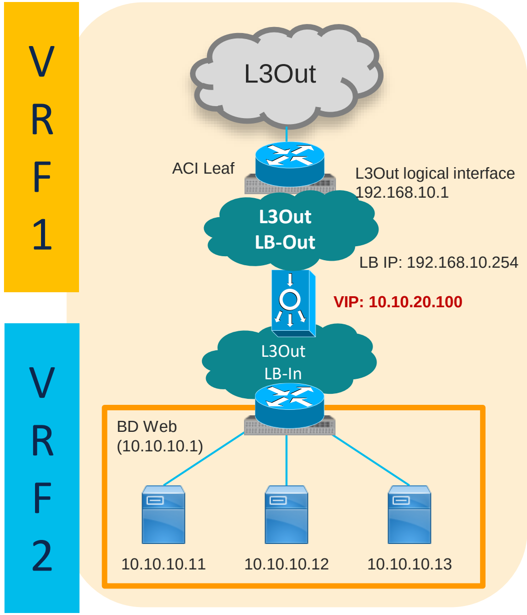
What if the VIP is not in LB Interface IP Subnet Range?

Use L3Out (or /32 static route on BD)

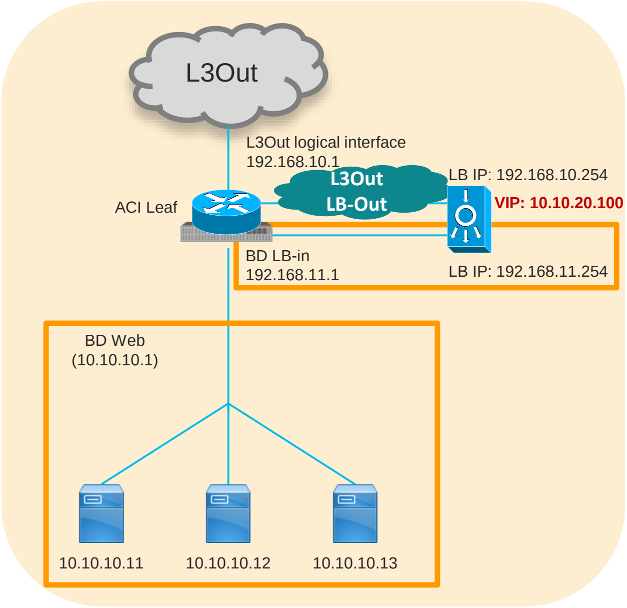
Two-arm (inline)
LB as Gateway
No SNAT/PBR



Two-arm (inline)
Fabric as Gateway
VRF sandwich



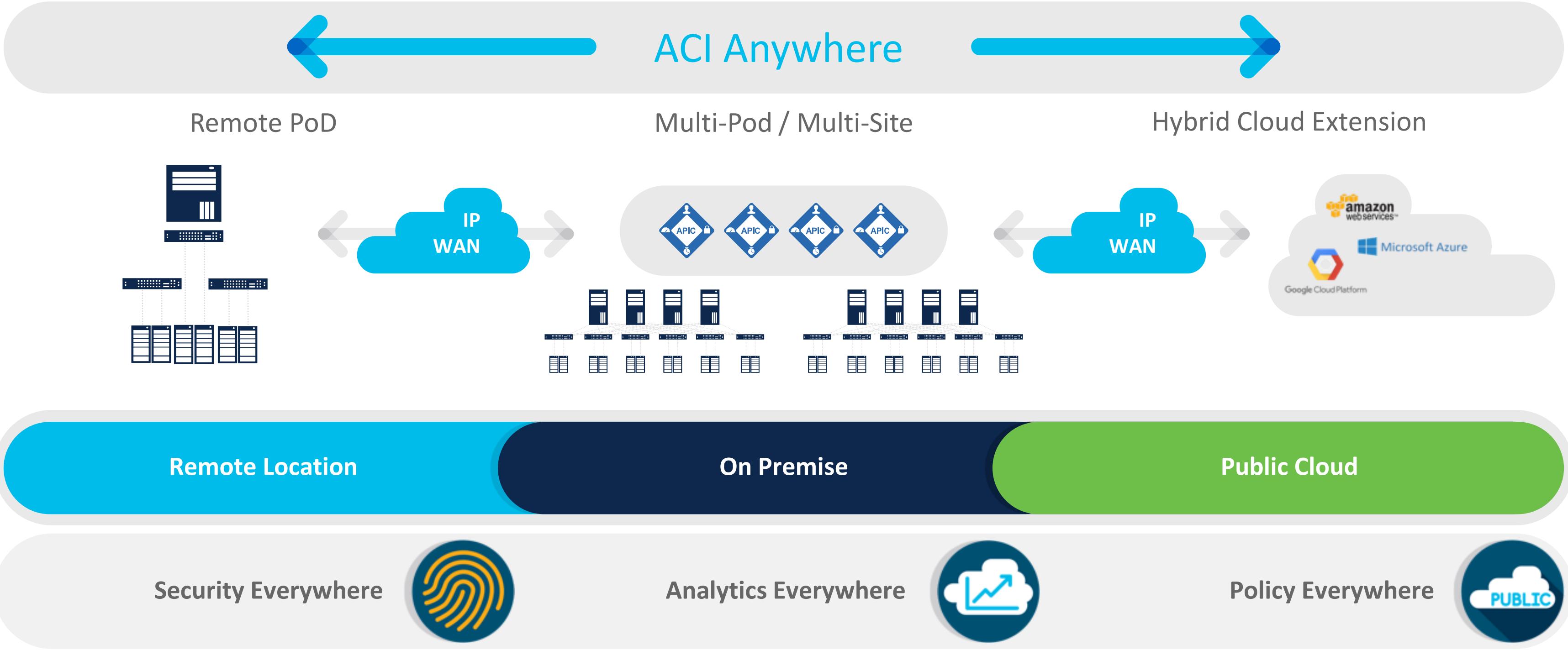
Two-arm
Fabric as Gateway
SNAT or PBR(After 5.0)



Multi-location Data Centres

You make the power of data **possible**

ACI Anywhere



ACI Anywhere

Remote PoD

Multi-Pod / Multi-Site

Hybrid Cloud Extension

Remote Location

On Premise

Public Cloud

Security Everywhere

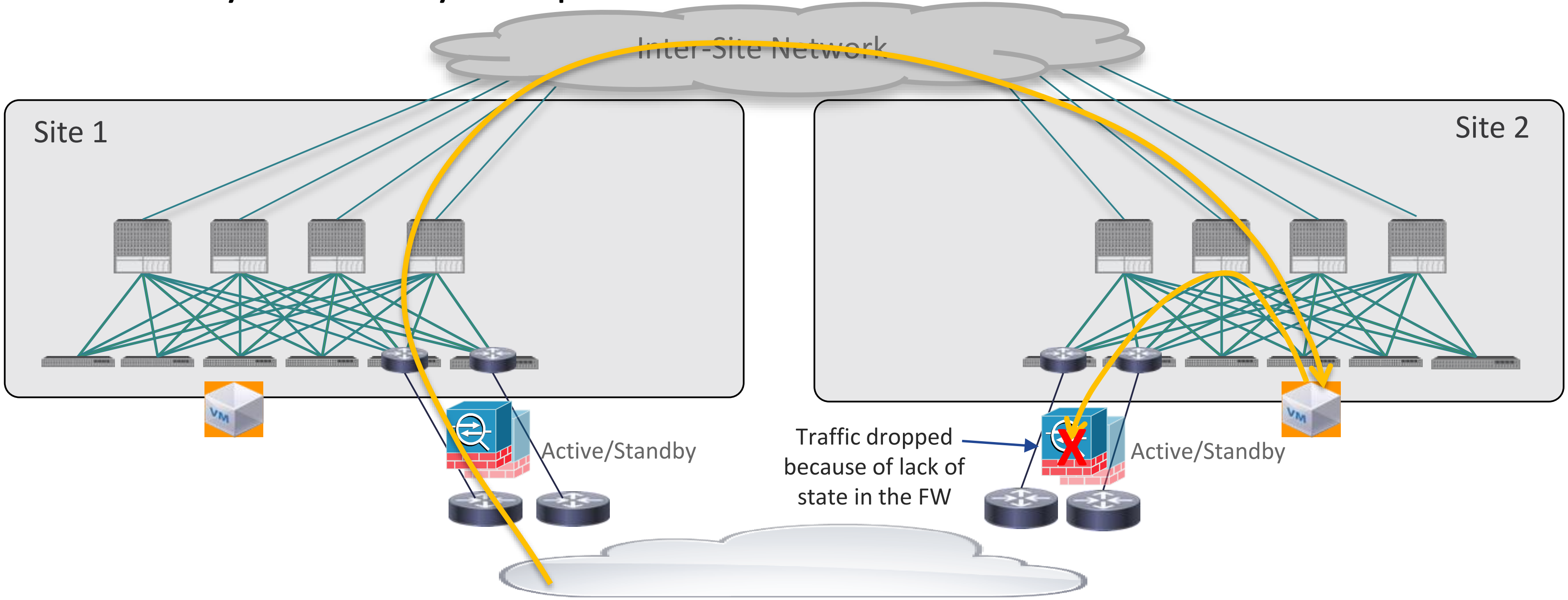
Analytics Everywhere

Policy Everywhere

Service Insertion in Multiple DC Locations

What is the Challenge of Service Insertion in Multiple DC Locations?

- Traffic Symmetricity is important



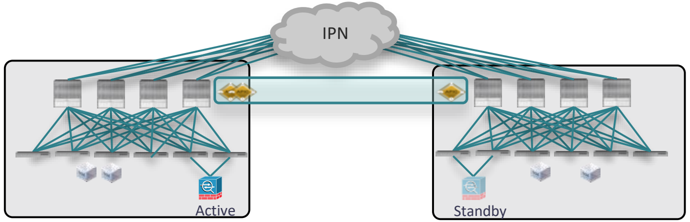
Traffic dropped because of lack of state in the FW

For Your Reference

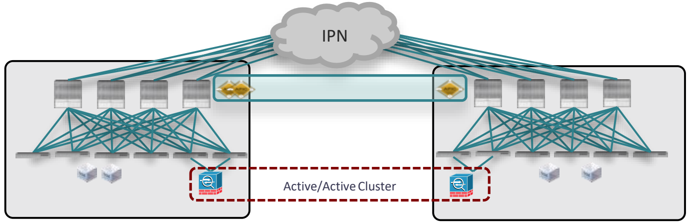
Multi-Pod and Network Services

Integration Models

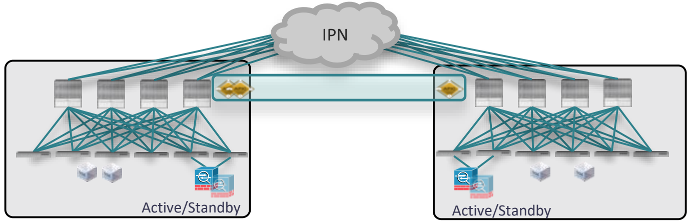
Typical options for an Active/Active DC use case



- 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 sites 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

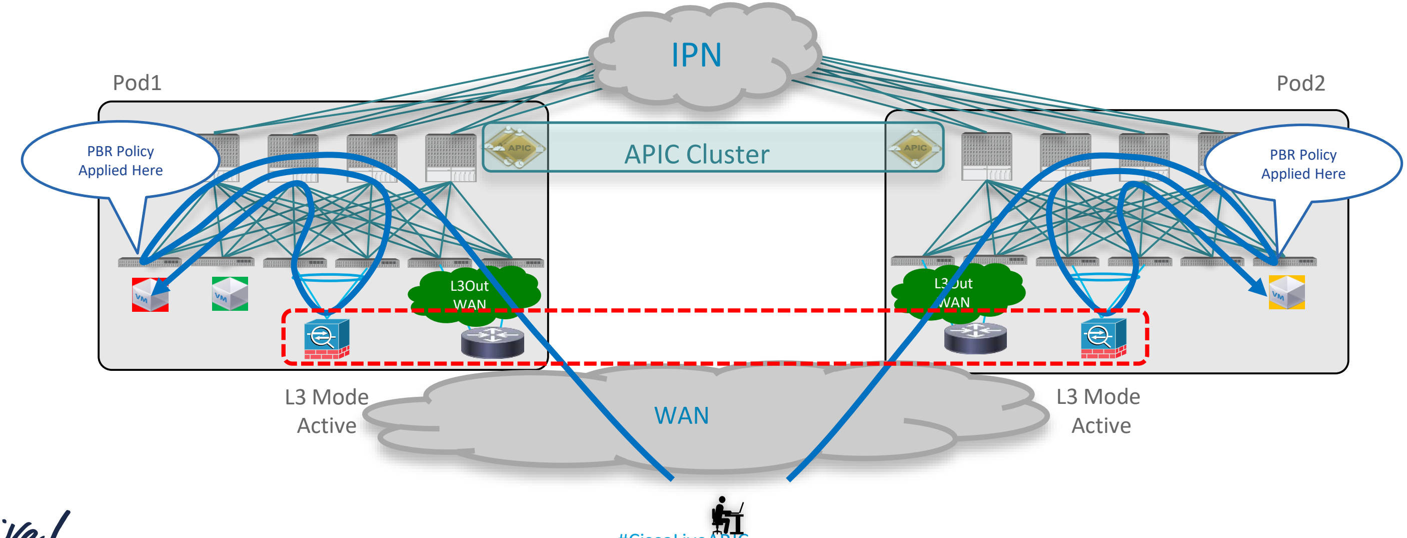
ACI 3.2

Active/Active Cluster Across Pods

Anycast IP/MAC with PBR

- All the active FW nodes have the same IP/MAC identity, so one of them will be picked

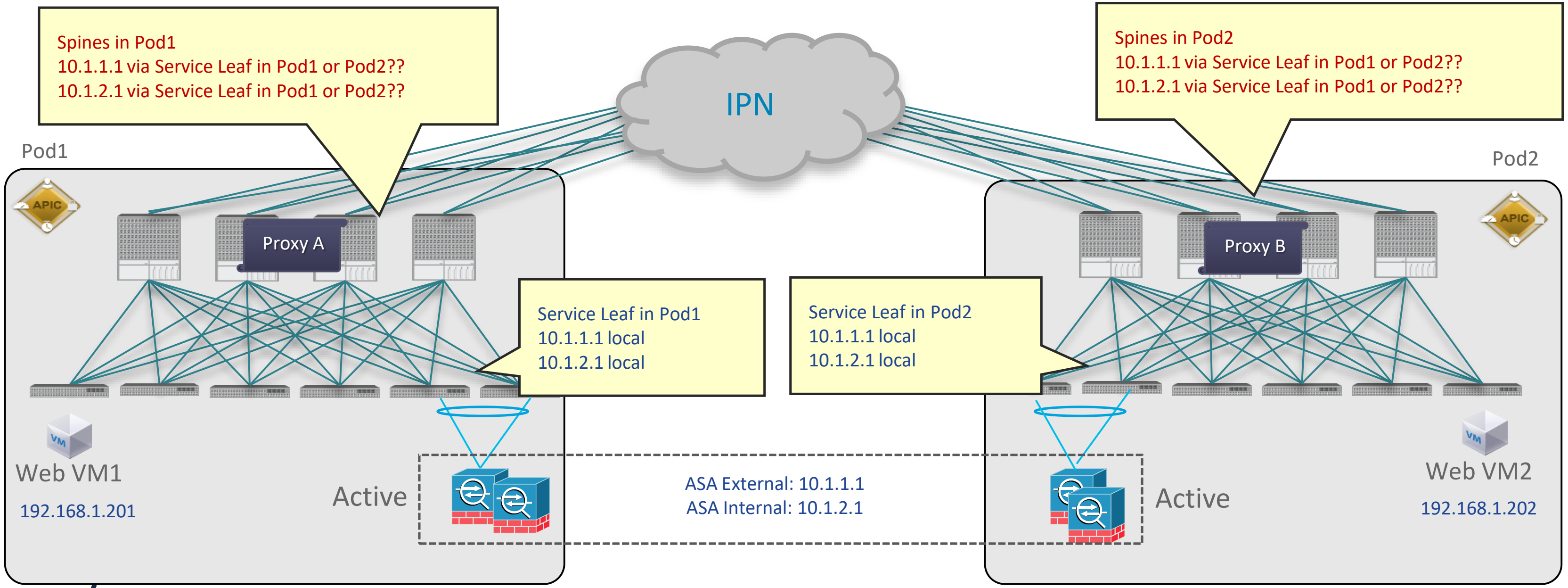
  By default one of the nodes local to a Pod is selected (based on IS-IS metric toward the IP address)



Without Anycast IP/MAC Feature

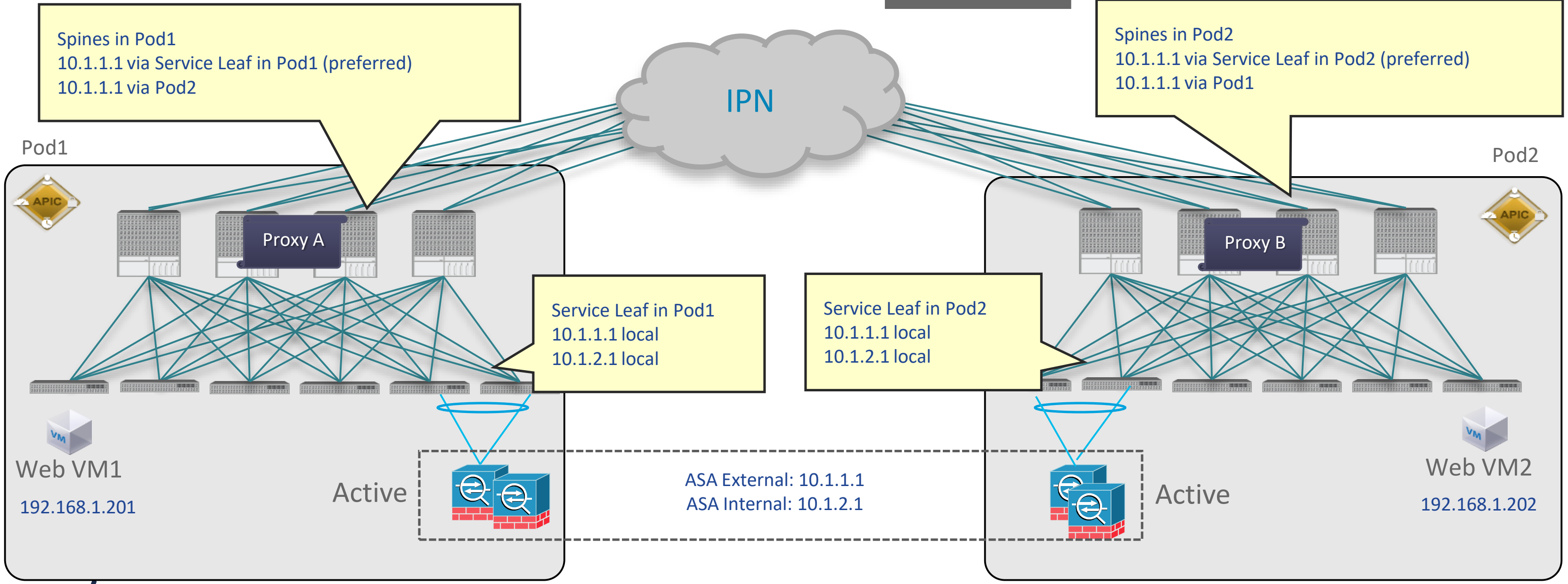
X

THIS IS NOT WORKING WITHOUT ANYCAST SERVICE



With Anycast IP/MAC Feature

✓ Works with
Any Cast Service starting 3.2



Spines in Pod1
10.1.1.1 via Service Leaf in Pod1 (preferred)
10.1.1.1 via Pod2

Spines in Pod2
10.1.1.1 via Service Leaf in Pod2 (preferred)
10.1.1.1 via Pod1

Service Leaf in Pod1
10.1.1.1 local
10.1.2.1 local

Service Leaf in Pod2
10.1.1.1 local
10.1.2.1 local

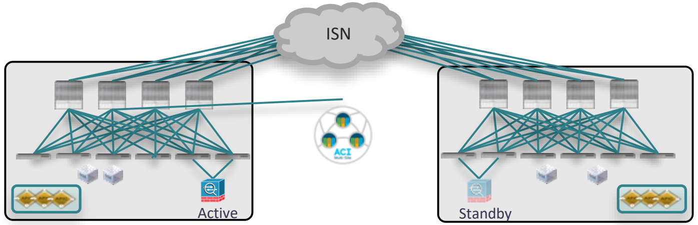
ASA External: 10.1.1.1
ASA Internal: 10.1.2.1

ACI Multi-Site and Network Services

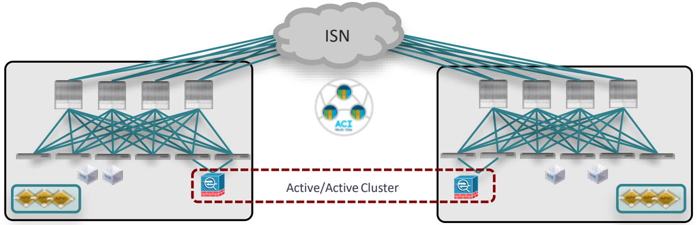
Integration Models

For Your Reference

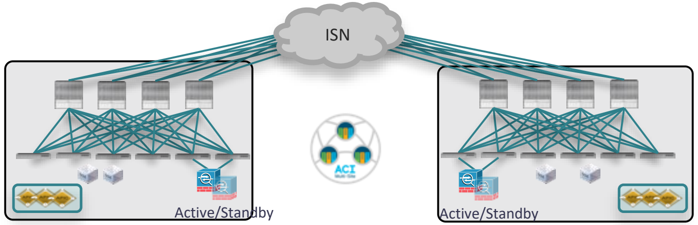
Deployment options fully supported with ACI Multi-Pod



- Active and Standby pair deployed across Pods
- **Currently supported only if the FW is in L2 mode or in L3 mode but acting as default gateway for the endpoints**



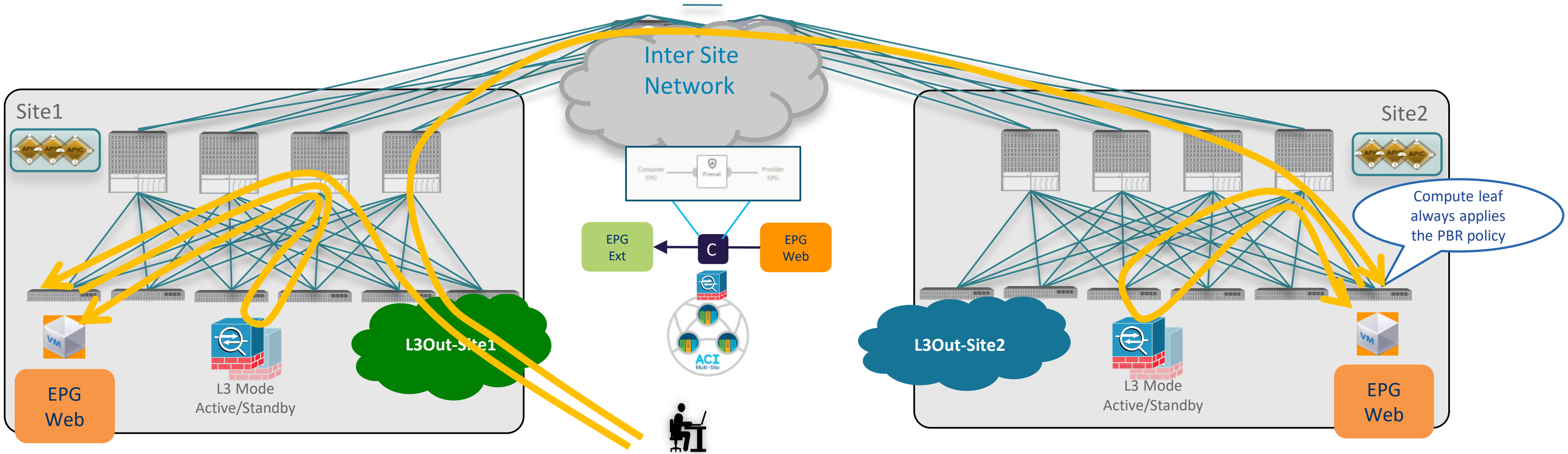
- Active/Active FW cluster nodes stretched across Sites (single logical FW)
- Requires the ability of discovering the same MAC/IP info in separate sites at the same time
- **Not supported**



- **Recommended deployment model for ACI Multi-Site**
- Option 1: supported from 3.0 for N-S if the FW is connected in L3 mode to the fabric → mandates the deployment of traffic ingress optimization
- Option 2: supported from 3.2 release with the use of Service Graph with Policy Based Redirection (PBR)

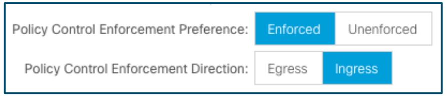
Use of Service Graph and Policy Based Redirection

North-South Communication – Inbound Traffic



Compute leaf always applies the PBR policy

- Inbound traffic can enter any site when destined to a stretched subnet (if ingress optimization is not deployed or possible)
- PBR policy is **always applied on the compute leaf node** where the destination endpoint is connected
  - Requires the VRF to have the Ingress policy enforcement preference and direction
  - Supported only **intra-VRF** in ACI release 4.0.
  - Ext-EPG and Web EPG can indifferently be provider or consumer of the contract

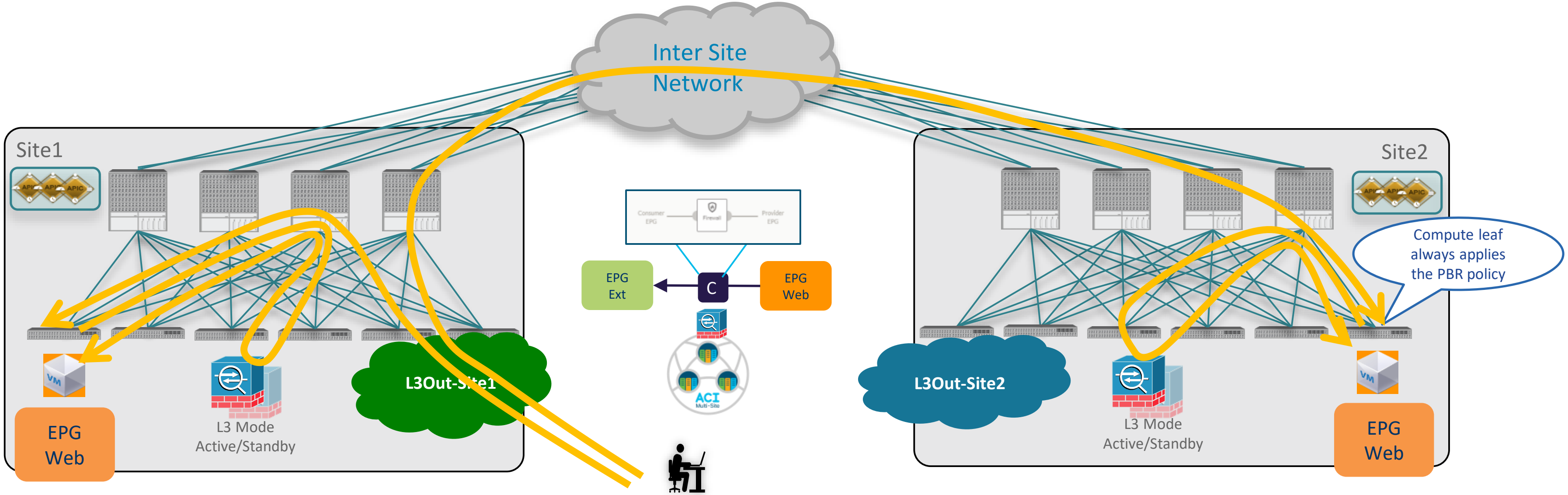


Policy Control Enforcement Preference: Enforced Unenforced

Policy Control Enforcement Direction: Egress Ingress

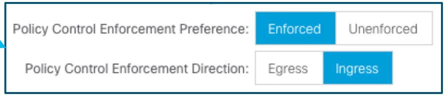
Use of Service Graph and Policy Based Redirection

North-South Communication – Inbound Traffic



Compute leaf always applies the PBR policy

- Inbound traffic can enter any site when destined to a stretched subnet (if ingress optimization is not deployed or possible)
- PBR policy is **always applied on the compute leaf node** where the destination endpoint is connected
  - Requires the VRF to have the Ingress policy enforcement preference and direction
  - Supported only **intra-VRF** in ACI release 4.0.
  - Ext-EPG and Web EPG can indifferently be provider or consumer of the contract

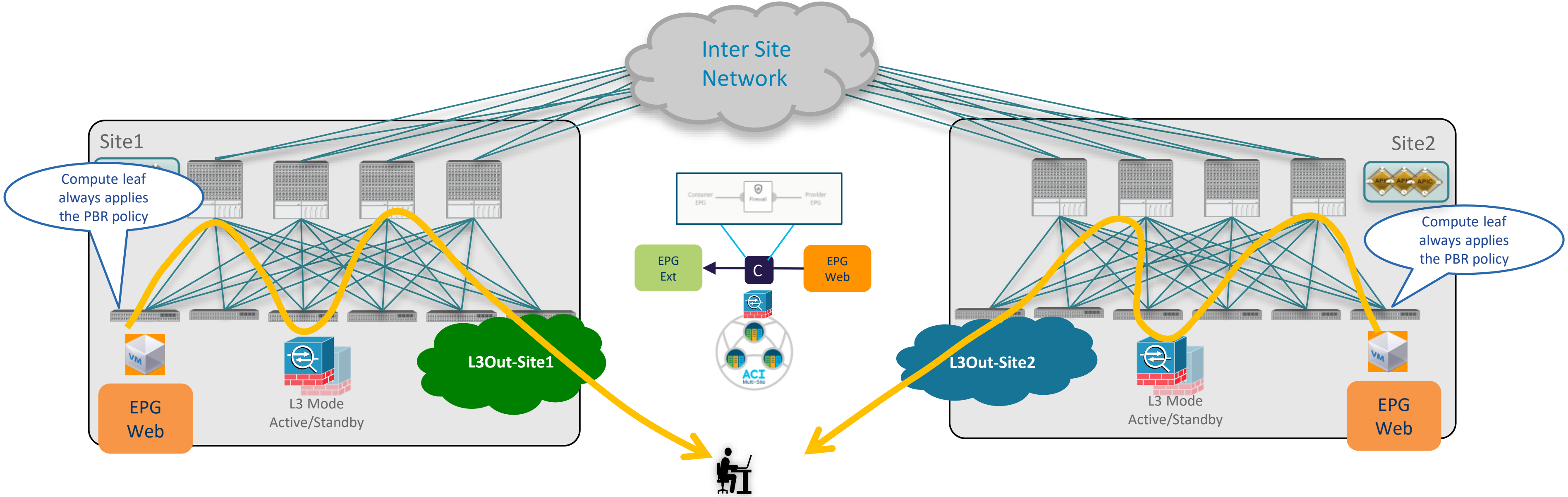


Policy Control Enforcement Preference: [✓ Enforced] Unenforced

Policy Control Enforcement Direction: Egress [✓ Ingress]

Use of Service Graph and Policy Based Redirection

North-South Communication – Outbound Traffic



- PBR policy is **always applied on the same leaf** where it was applied for inbound traffic
- Ensures the same service node is selected for both legs of the flow
- Different L3Outs can be used for inbound and outbound directions of the same flow

Summary

- ACI Contract security
- ACI L4-L7 service integration
  - Firewall Design Options
    - Inline FW, FW as gateway, VRF sandwich or PBR
  - Load Balancer Design Options
    - LB as gateway, SNAT or PBR for return traffic
  - Multi-Pod/Multi-Site Design Options

Useful Links

- Service Graph Design with Cisco Application Centric Infrastructure White Paper

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-734298.html

- 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

- 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

- 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

- 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

Thank you

You make **possible**