cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Cisco Secure Firewall in ACI

L4-L7 Integration

Goran Saradzic, CX Solutions Architect

BRKDCN-3712

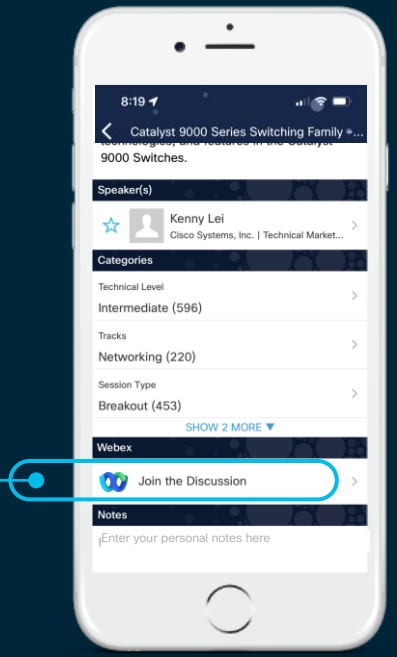
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-3712

Webex spaces will be moderated by the speaker until June 17, 2022.

Let Me Introduce Myself

'84

Then…

- From the Balkans – Sarajevo
- High School exchange in U.S.
- Enjoy skiing, so studied and settled in Colorado

- Two years in IT Services – IBM
- A decade in Cisco Engineering
- 7 years in Technical Marketing
- 3 years a Manager of TME

…and Now

- CXPM Solutions Architect

Netview	AIX	PIX	ASA	ACI	Hypervisor	Cloud	FTD
Perl	Bash	Expect	Tcl	Python	PowerCLI	APIs	

Agenda

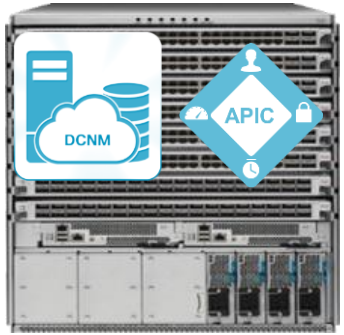
- Introduction
  - Quick Prep and Review before our Topics
  - L3 PBR with Firewall Clustering in ACI Multi-pod
  - L2 PBR with Secure Firewall – All Options
  - L1 PBR with Stand-alone and Clustered Firewall
  - ACI Endpoint Update app
  - Rapid Threat Containment for APIC
- Conclusion

Brief Review

Cisco Data Center Security Portfolio Brief

Fabric

ACI Fabric Spine/Leaf



Nexus Switching

Firewall/IPS/AMP

Cisco Secure Firewalls – ASA and FTD

VM Options Available

Endpoint Group (EPG):
A collection of virtual or physical endpoints in a base or micro-segmented grouping

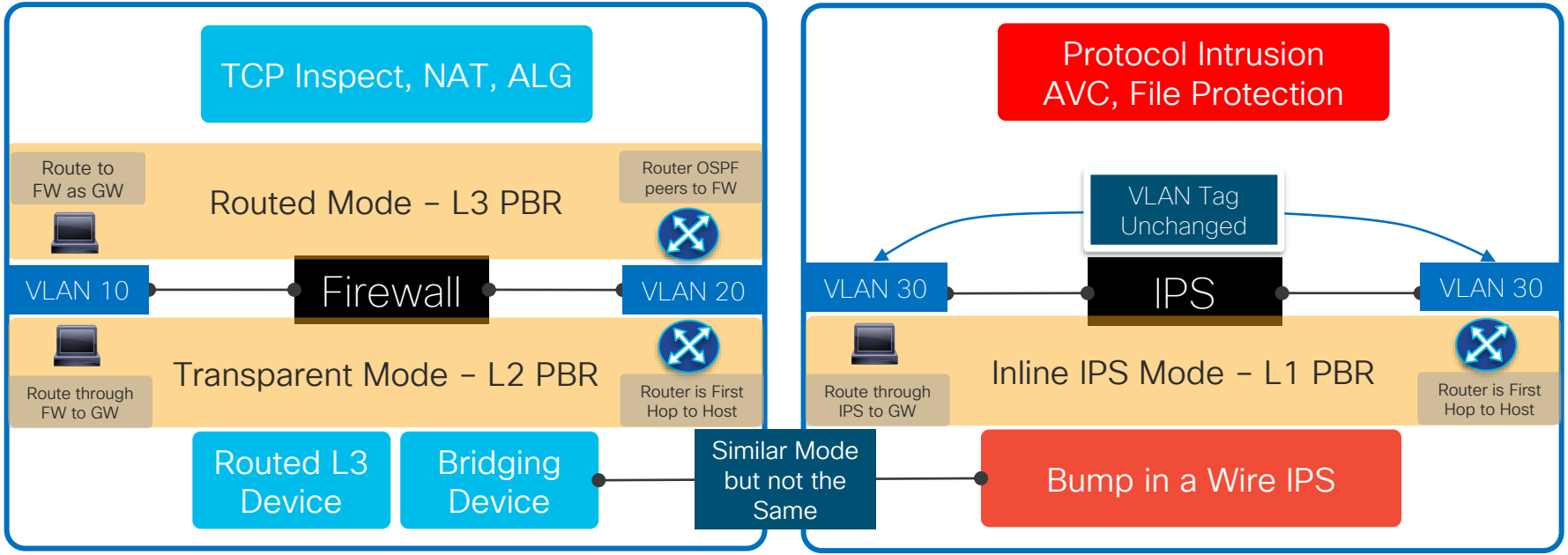
Endpoint Security Group (ESG)

Contract:
A set of rules governing communication between endpoint groups

Service Graph (Chain):
A chain of L4-L7 services inspecting traffic between endpoint groups.

Core Security Functions and L3 / L2 / L1 PBR

Firewall vs. Inline IPS Network Integration



NGFW combines Traditional FW and NGIPS Functions

NGIPS Deployment Options for Port-Channels

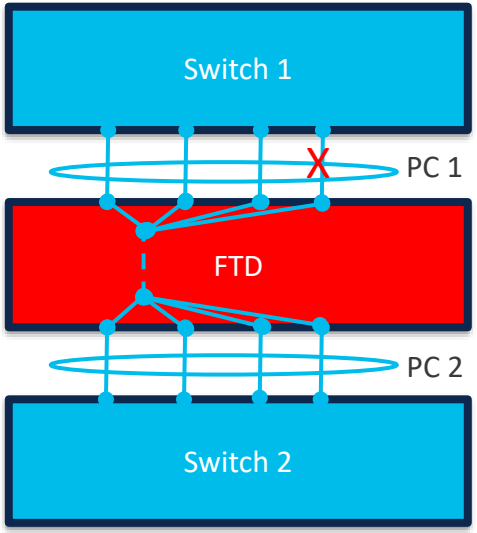
Port-Channel Termination on the NGIPS

Port-channel terminates on the IPS device and an inline pair is formed between two port channels

Asymmetric Traffic flows are not a problem

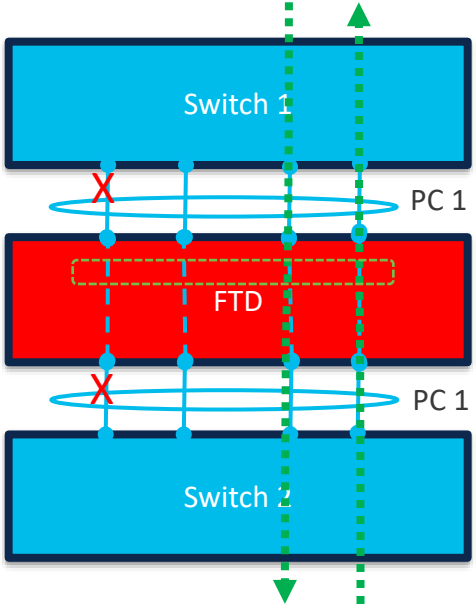
Traffic is resilient to individual link failures in the port-channels

Can enable HA or cluster for box-to-box resiliency



Network and Security continuity in case of device failure

LACP Pass-Through on the NGIPS



Port-channel passes through the IPS device and inline pairs are formed between individual port member interfaces.

Inline Set of multiple inline pairs is created to handle asymmetric traffic flows

Must enable link state propagation to avoid traffic black-holing in case of link failures

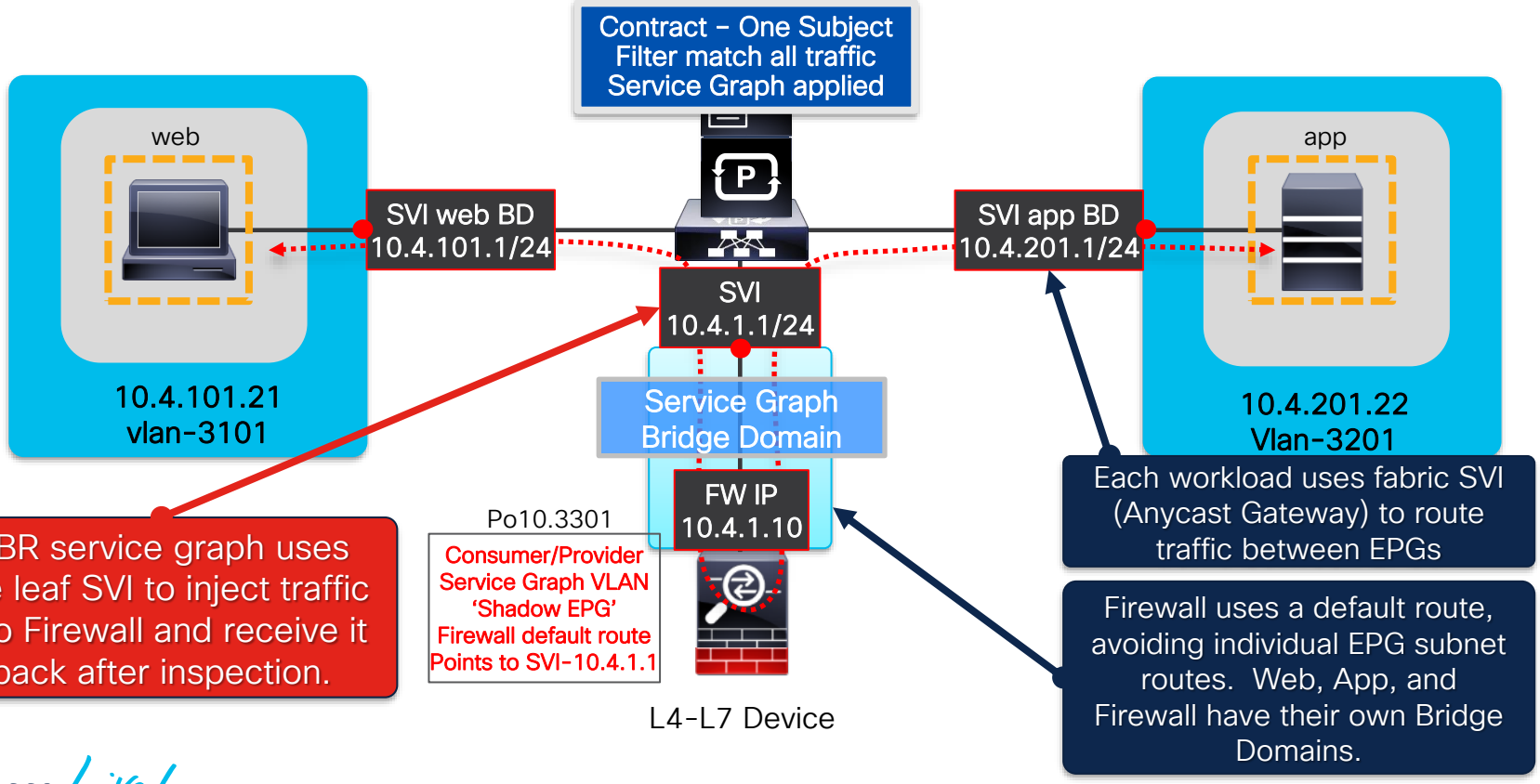
FTW or HA can provide resiliency

Only Network continuity in case of device failure with FTW

L3 PBR with Firewall Clustering in ACI Multi-pod

Service Graph Routing Separation from Workload

Benefits of One-Arm Policy Based Redirect Graph Injects Traffic into Firewall

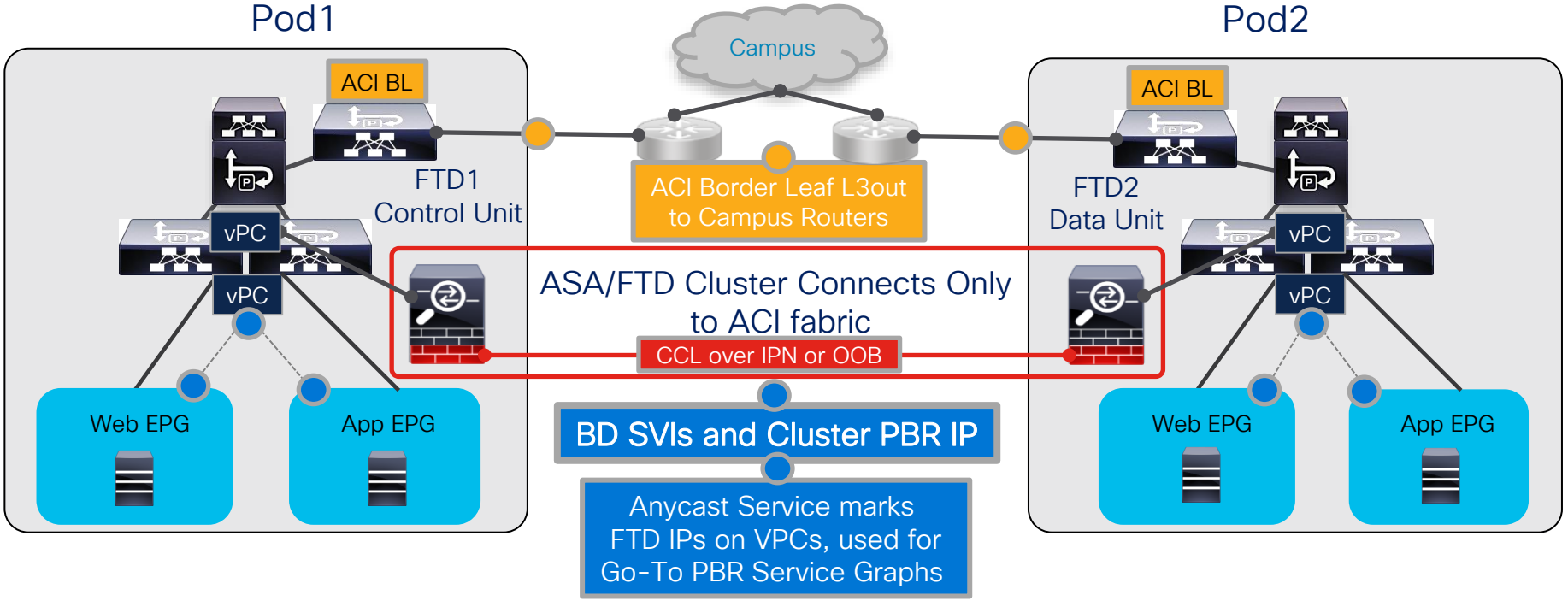


PBR service graph uses the leaf SVI to inject traffic into Firewall and receive it back after inspection.

Each workload uses fabric SVI (Anycast Gateway) to route traffic between EPGs

Firewall uses a default route, avoiding individual EPG subnet routes. Web, App, and Firewall have their own Bridge Domains.

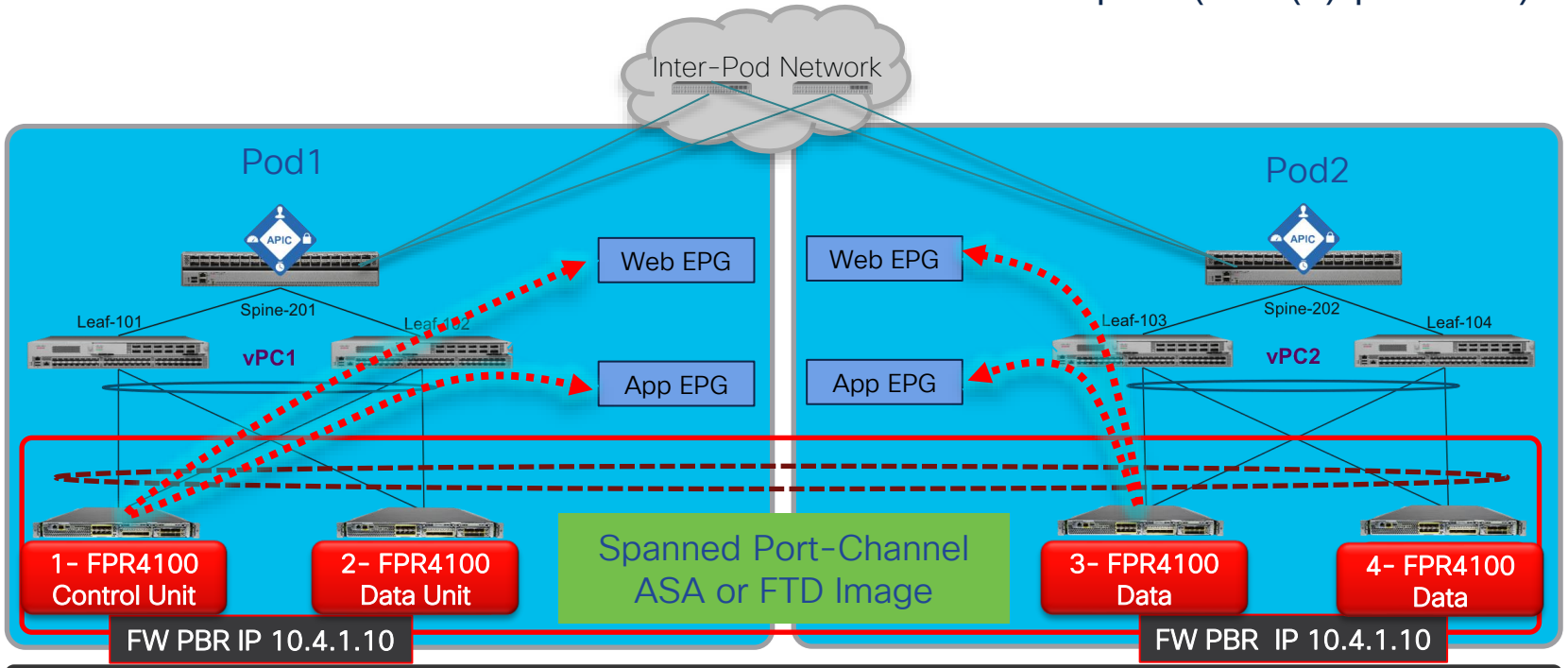
Secure Firewall Inter-site Cluster in ACI Multi-Pod



Apply security policy once on master, localize inspection within a Pod, and track remote FTD cluster IPs.

Localize PBR Inspection and Push Policy Only to Master

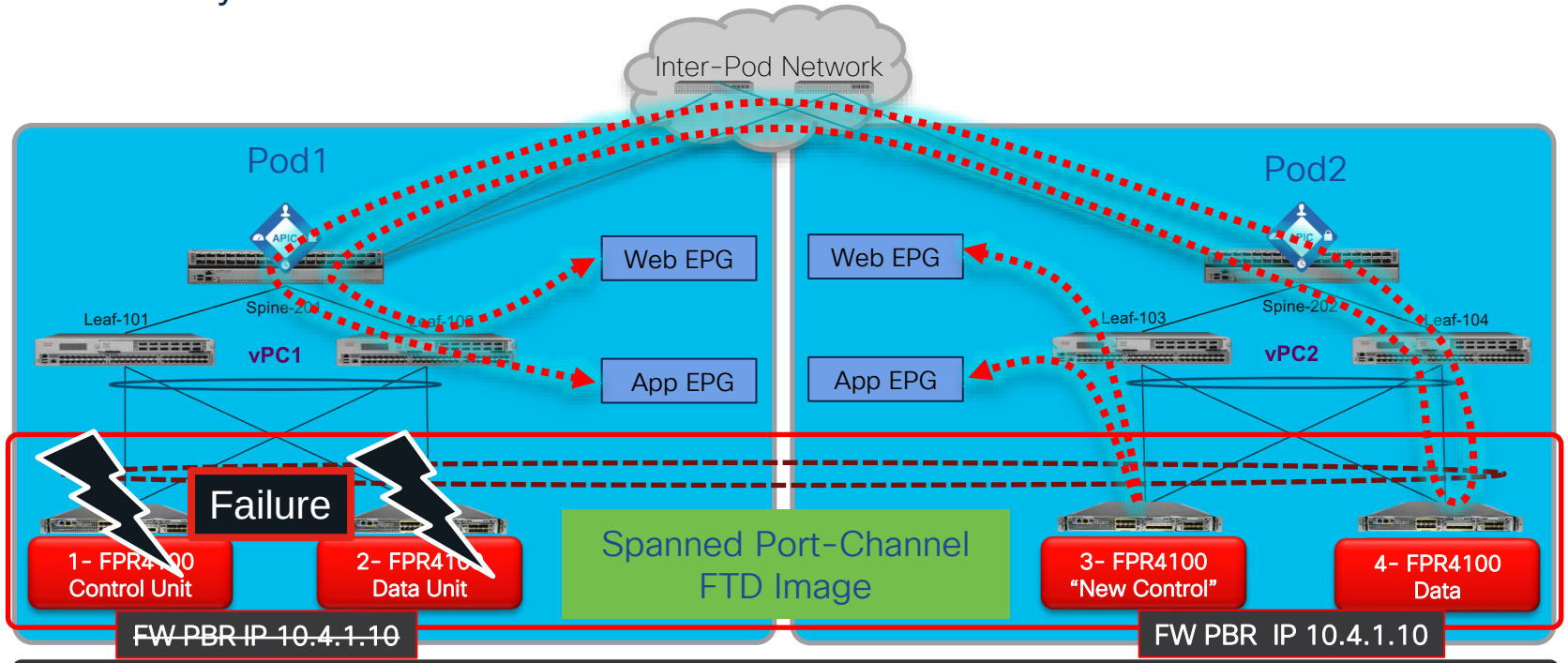
Extend PBR Inter-site Cluster to all ACI Pods in Multi-pod (Unit(s) per Pod)



ACI fabric learns local and remote Anycast Service IPs of the firewall cluster units. Fabric always prefers a local firewall IP. If local Anycast Service IP fails, fabric will send to the remote firewall IP.

Resiliency of the Secure Firewall Threat Defence Cluster

Firewalls Sync the State of Workload Connections



In case of failure of both firewalls in Pod1, fabric forwards traffic for PBR service graph inspection to Pod2 firewalls. Pod1 App to DB connections continue because Firepower cluster syncs connection state.

ACI Anycast Service on ASA or FTD Active/Active Cluster

Cisco Firewall Only Feature Matches Spanned Ether-Channel Clustering

L4-L7 Policy-Based Redirect - ftd-cluster-pbr

Properties

Name: ftd-cluster-pbr

Description: optional

Enable Pod ID Aware Redirection: ☐

Hashing Algorithm: dip | sip | sip-dip-prototype

Anycast Endpoint: ☑

Resilient Hashing Enabled: ☐

IP SLA Monitoring Policy: select an option

Oper Status: Enabled

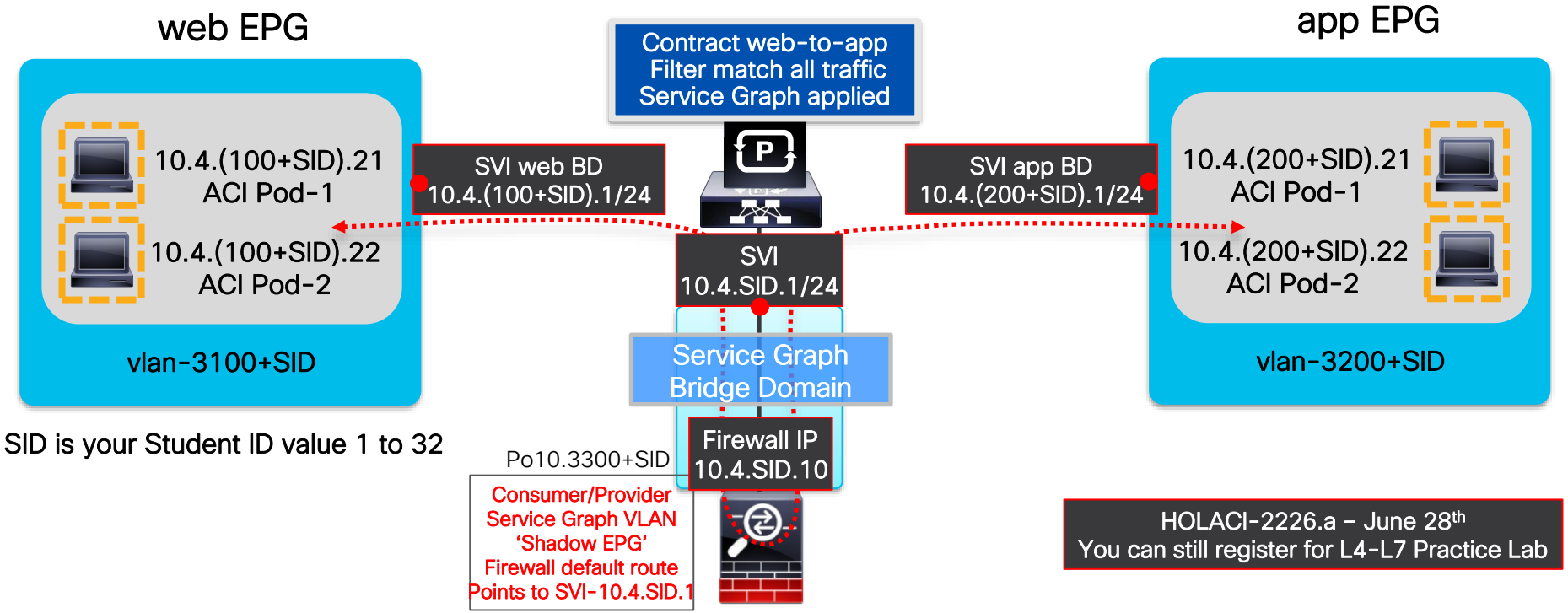
Destinations:

IP	MAC
10.1.0.2	00:00:01:02:01:02

Simple Config
Replaces OTV MAC filters and automation to take them out.

PBR target, being ASA or FTD IP / MAC on units in one cluster distributed across ACI Pods.

Demo 1 Diagram – ACI Multi-pod Anycast Service



SID is your Student ID value 1 to 32

HOLACI-2226.a – June 28th
You can still register for L4-L7 Practice Lab

Demo 1 – L3 PBR

Connections Sync within a Pod and Across Pods

Backup Unit Different Pod

Backup Unit Same Pod

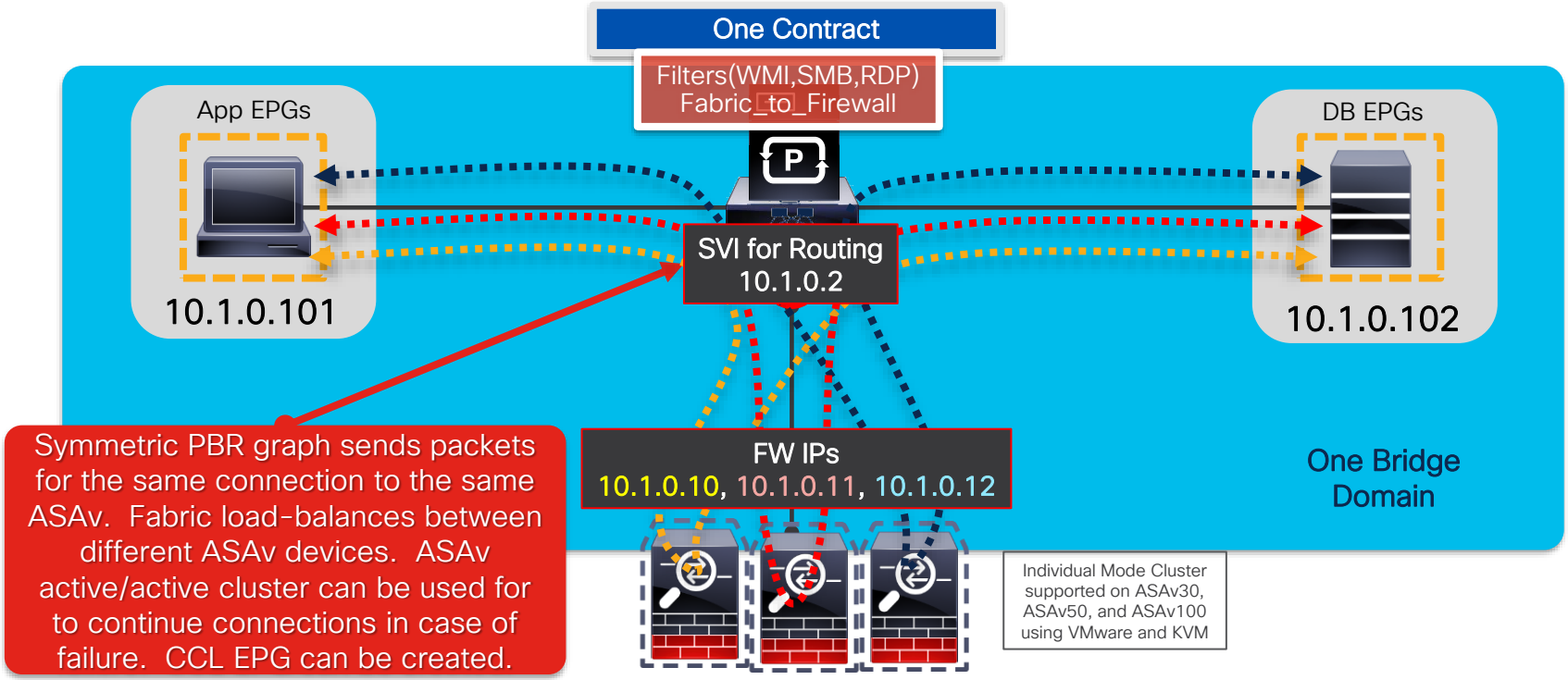
Owner Unit

Firepower 9300

```
firepower# cluster exec show conn | i \*\*|pbr
unit-1-1(LOCAL):**************************************************
TCP pbr-graph  10.1.0.102:41088 pbr-graph  10.70.0.104:22, idle 0:00:15, bytes 0, flags  Y

unit-1-3:**************************************************

unit-2-2:**************************************************
TCP pbr-graph  10.1.0.102:41088 pbr-graph  10.70.0.104:22, idle 0:00:00, bytes 0, flags  Yl

unit-2-1:**************************************************

unit-2-3:**************************************************
TCP pbr-graph  10.70.0.104:22 pbr-graph  10.1.0.102:41088, idle 0:00:00, bytes 218166, flags UIO N
1

unit-1-2:**************************************************
firepower#
```

ASAv ECMP Cluster – Symmetric PBR Scale Out

Use up to 16 clustered of ASAv devices with connection state sync

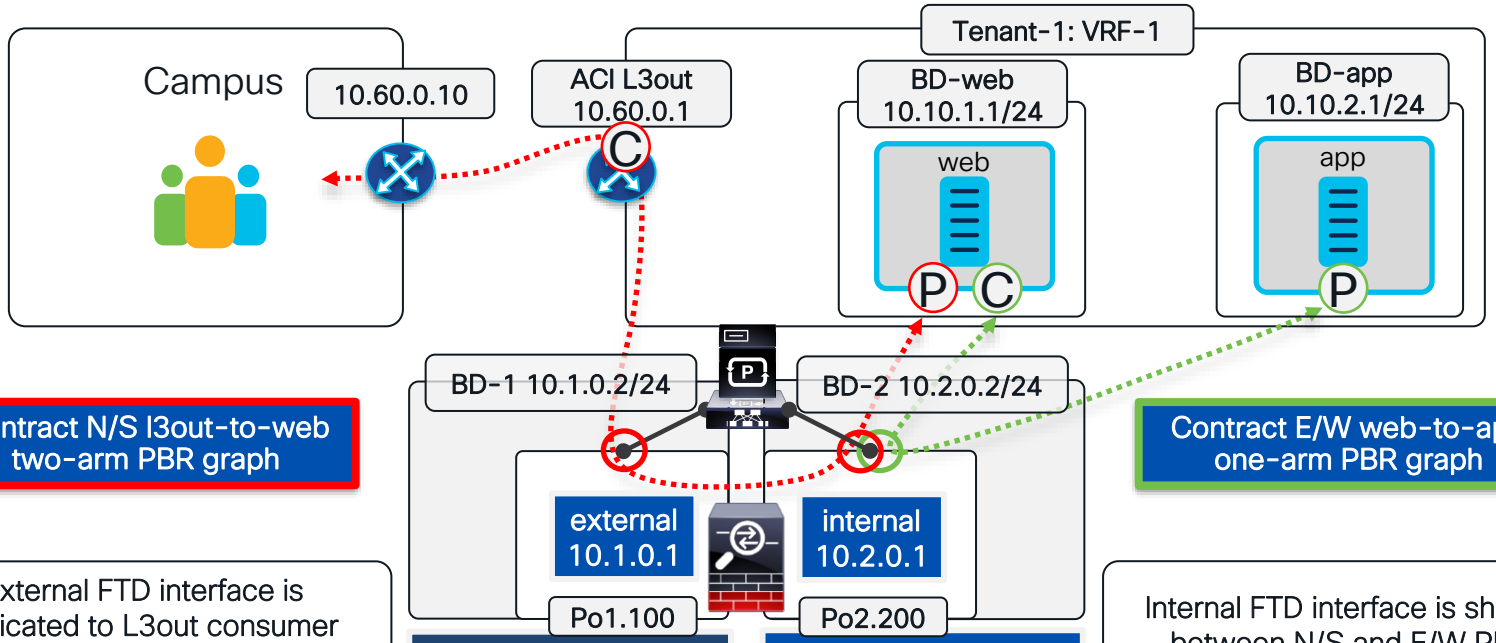


Symmetric PBR graph sends packets for the same connection to the same ASAv. Fabric load-balances between different ASAv devices. ASAv active/active cluster can be used for to continue connections in case of failure. CCL EPG can be created.

Pool of Clustered ASAv Devices

PBR Real Use Case: N/S Two-Arm and E/W One-Arm

Sharing Firewall Interface between Service Graphs



Contract N/S l3out-to-web two-arm PBR graph

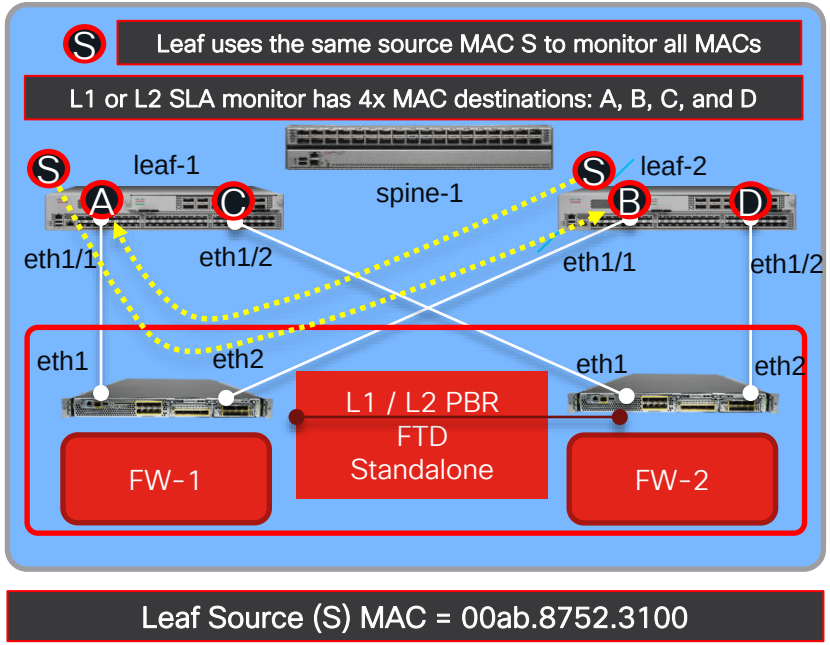
Contract E/W web-to-app one-arm PBR graph

External FTD interface is dedicated to L3out consumer terminal, allowing stricter controls on the untrusted security zone. Both graphs reside in the same VRF on an FTD device.

Internal FTD interface is shared between N/S and E/W PBR service graphs. One-arm firewall for E/W enables use of one-to-many contracts (vzAny) with PBR.

L2 PBR with Standalone, HA, or Clustered Firewall

L2Ping – How It Works and Relates to MAC Learning



Leaf Source (S) MAC = 00ab.8752.3100

- Leaf-1 and Leaf-2 use A, B, C, and D destination MACs to monitor firewall/L2 and IPS/L1 interfaces
- I.e., FW-1 eth1 and eth2 ports are monitored in both directions
- leaf-1 eth1/1 sends a packet with source S to destination B.
- leaf-2 eth1/1 sends source S to A
- MAC learning sees MAC S move between eth1 and eth2, causing blocking of traffic (must disable it)

L2 PBR Transparent Firewall and ACI Configurations

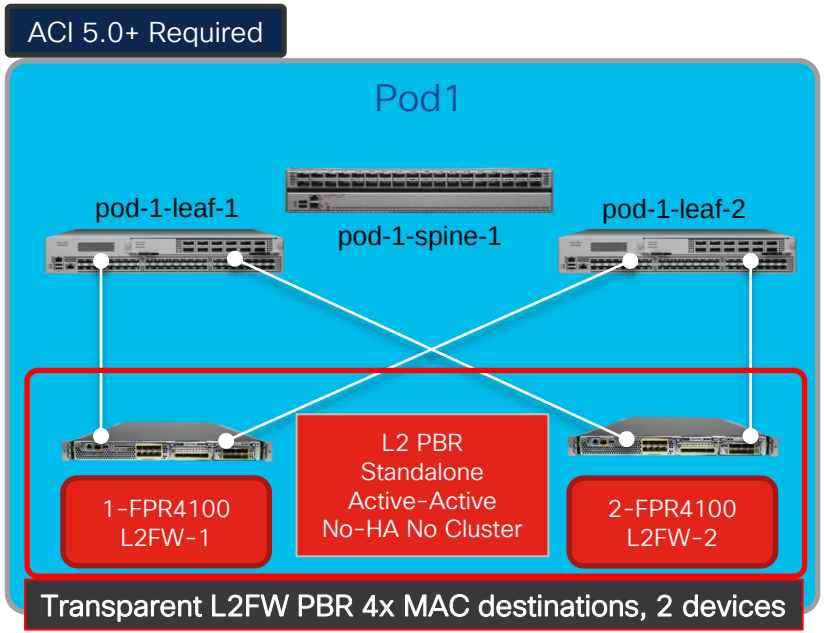
Firewall

- Access-list must permit ethertype 0x0721 for L2Ping
- MAC learning must be disabled
- Static MACs need to be defined for leaf PBR destinations
- Two-arm interfaces need to be placed in the same bridge-group

ACI

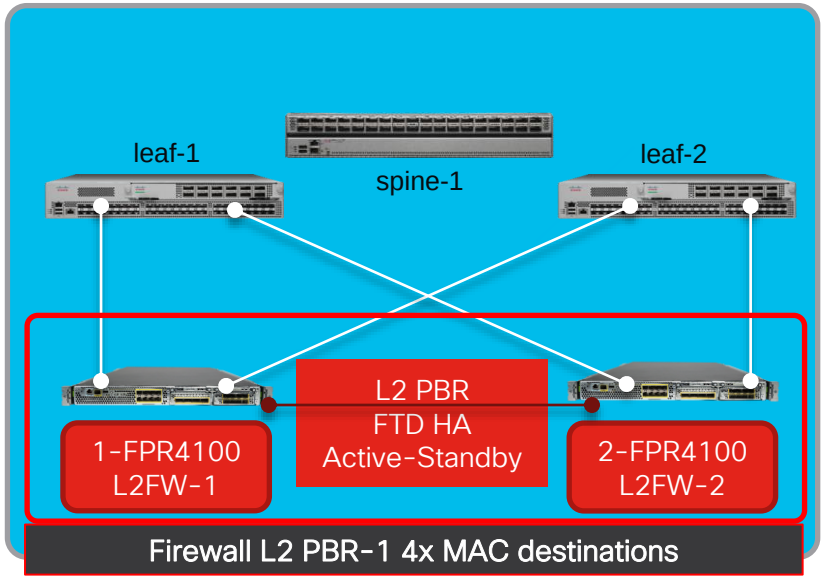
- Define a Health Group for each device
- IP SLA Monitoring Policy is required
- SLA frequency is defined in seconds with Detect multiplier
- Define PBR MAC destinations for L2Ping monitoring

L2 PBRs - Stand-alone FTD L2FW Units per Pod



- Two or more independent L2 PBR are used as Active-Active devices
- ACI load-balances traffic to two active L2 PBR destinations
- Each PBR device interface is monitored from leaf side using L2ping from the same source MAC
- L2FW must disable MAC learning to avoid problems

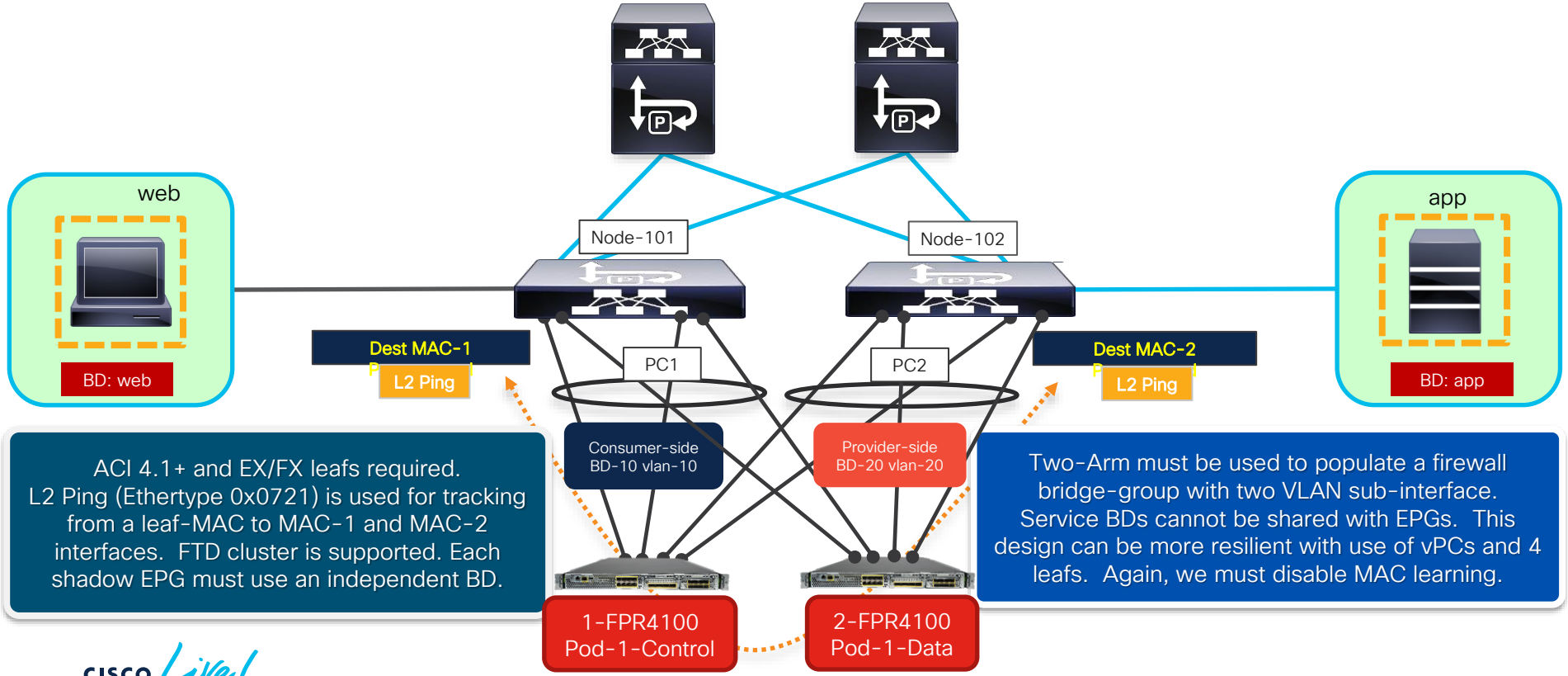
L2 PBR on FTD L2FW HA Pair – Transparent Firewall



- L2FW HA must have ability to disable MAC learning
- Standby L2FW always blocks traffic
- Switchover still dictated by ACI (multiple seconds), even though firewall HA supports a sub-second switchover
- ACI SLA frequency and detect multiplier govern switchover time

L2 PBR: FTD Cluster L2FW with Port-Channel Pair

ACI has L2 PBR with an FTD cluster device (2x PCs in a BVI to 2x leafs)



ACI 4.1+ and EX/FX leafs required.
L2 Ping (Ethertype 0x0721) is used for tracking from a leaf-MAC to MAC-1 and MAC-2 interfaces. FTD cluster is supported. Each shadow EPG must use an independent BD.

Two-Arm must be used to populate a firewall bridge-group with two VLAN sub-interface. Service BDs cannot be shared with EPGs. This design can be more resilient with use of vPCs and 4 leafs. Again, we must disable MAC learning.

L1 PBR with Standalone or Clustered Firewall

Leaf Interface Policy Group for L1 PBR – Must Have

Leaf Access Port Policy Group - fw-1120-pg

Policy | Faults

Properties

Alias:	
Attached Entity Profile:	fw-aep
CDP Policy:	CDP_Disabled
Link Level Policy:	select a value
LLDP Policy:	lldp_disabled

Advanced Settings

802.1x Port Authentication:	select a value
CoPP Policy:	select a value
DWDM:	select a value
Egress Data Plane Policing:	select a value
Fibre Channel Interface:	select a value
Ingress Data Plane Policing:	select a value
L2 Interface:	ips-local-scope
MCP:	MCP-disable
Monitoring Policy:	select a value
PoE Interface:	select a value
Port Security:	select a value
Priority Flow Control:	select a value
Slow Drain:	select a value
Storm Control Interface:	select a value

L4-L7 Device for L1 PBR – Active-Active

General

Name: ips-active-active

Service Type: Other

Device Type: PHYSICAL | VIRTUAL

Promiscuous Mode: ☐

Context Aware: Multiple | Single

Function Type: GoThrough | GoTo | L1 | L2

Active-Active Mode: ☑

Enable Active-Active mode then update physical domains

Devices

The configuration can comprise a single device, two devices (su
or two or more standalone devices in a scale-out pool.

Name	Interfaces	Encap
ips-4	Eth1/1 (Pod-2/Node-401/eth1/3) Eth1/2 (Pod-2/Node-402/eth1/3)	vlan-3030 vlan-3030
ips-3	Eth1/1 (Pod-2/Node-401/eth1/2) Eth1/2 (Pod-2/Node-402/eth1/2)	vlan-3030 vlan-3030

Separate physical domains for consumer and provider

Cluster Interfaces:

Name	Concrete Interfaces	Physical Domain
consumer	ips-3/Eth1/1,ips-4/Eth1/1	ips-phys-dom-consumer
provider	ips-3/Eth1/2,ips-4/Eth1/2	ips-phys-dom-provider

Policies > Protocol > L4-L7 Policy Based Redire

Name: ips-3-pbr-outside

Description: optional

Destination Type: L1 | L2 | L3

Rewrite source MAC: ☐

IP SLA Monitoring Policy: ips-monitor

Oper Status: Enabled

Threshold Enable: ☐

Enable Pod ID Aware Redirection: ☐

Hashing Algorithm: Destination IP | Source IP | Source IP, Destination IP and Protocol number

Resilient Hashing Enabled: ☑

Backup Policy: select an option

L1/L2 Destinations:

Destination Name	IP	Redirect Health Group	MAC	CIF	Description	Oper Status
outside-3	34cf:1b25:7012:...	ips-health-group-3	00:03:03:03:03:02	[Eth1/2]		Enabled
outside-4	d2d9:a85a:1046:...	ips-health-group-4	00:04:04:04:04:02	[Eth1/2]		Enabled

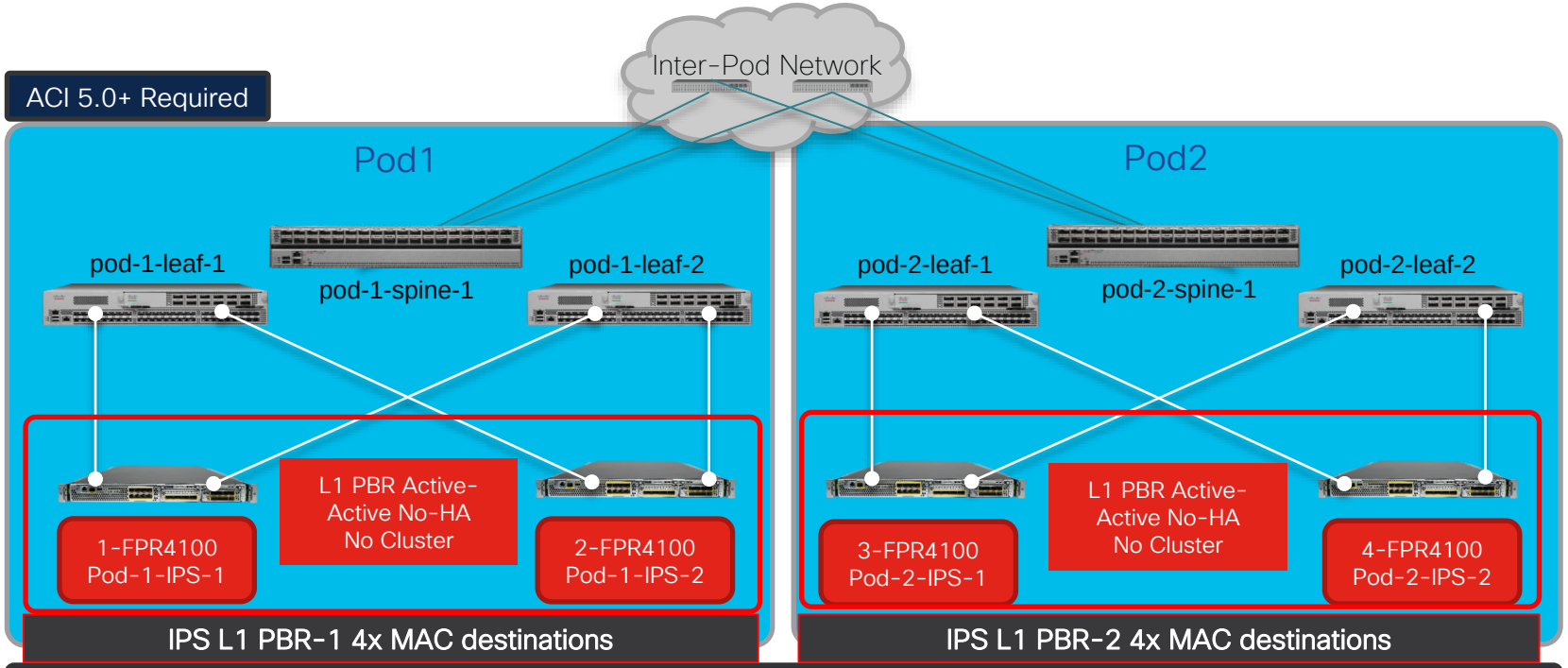
Must define interfaces under L4-L7 device, then come back to L1/L2 destinations to select interfaces

L1/L2 Destinations: L4-L7 Policy-Based Redirect - ips-3-pbr-inside

Destination Name	IP	Redirect Health Group	MAC	CIF	Description	Oper Status
inside-3	9c39:7791:741f:...	ips-health-group-3	00:03:03:03:03:01	[Eth1/1]		Enabled
inside-4	cc6:4bff:8ec1:44...	ips-health-group-4	00:04:04:04:04:01	[Eth1/1]		Enabled

L1 PBRs - Stand-alone FTD IPS Units per Pod

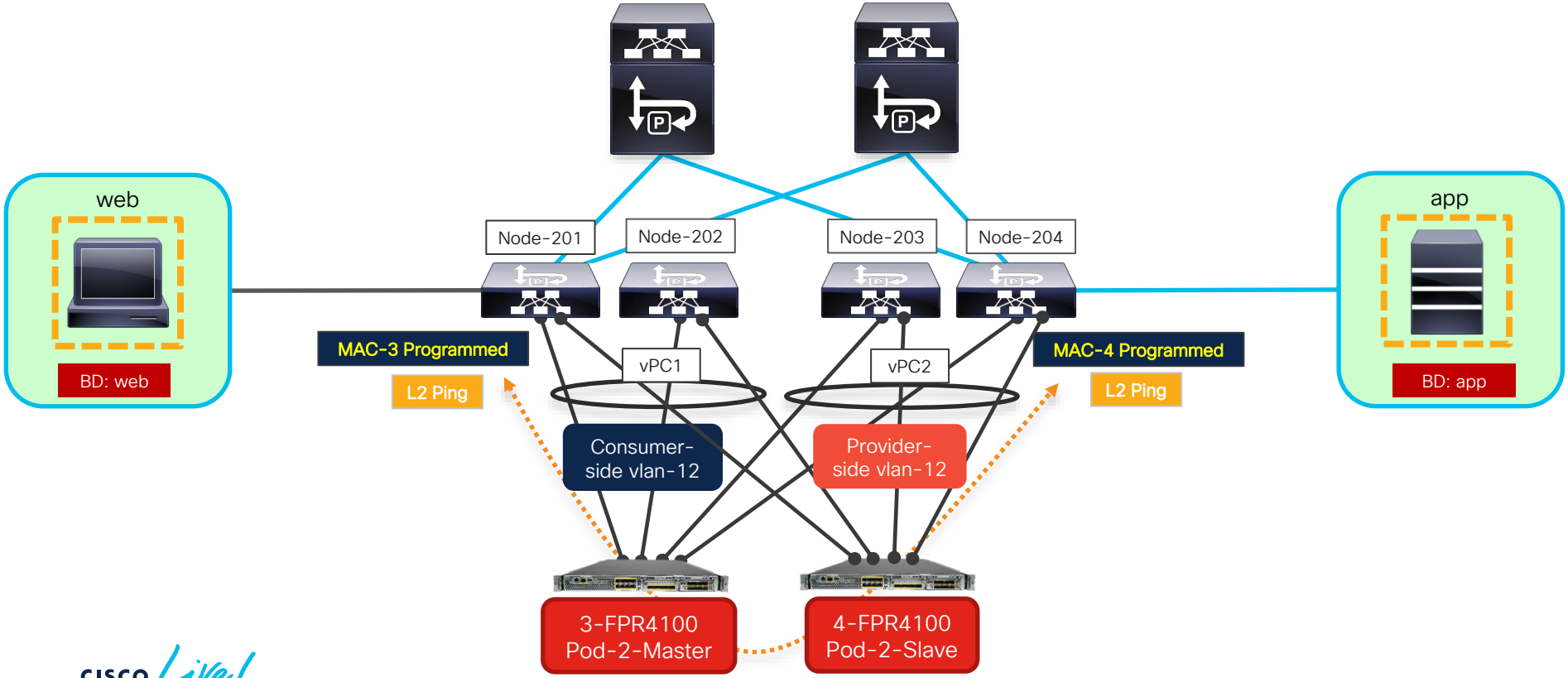
Two L1 PBR Active-Active – ACI load-balances traffic to two active L1 PBR devices



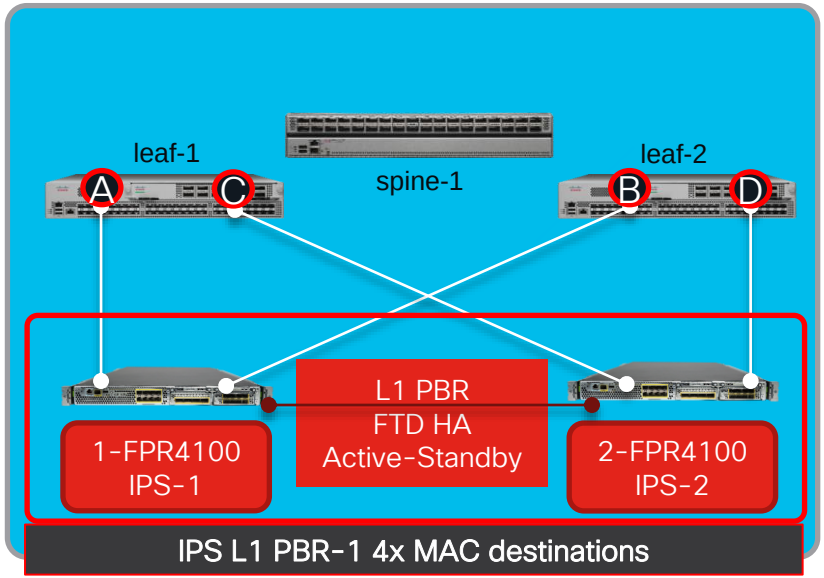
ACI fabric has a stand-alone IPS devices per Pod using a dedicated L1 PBR. Each PBR device has MAC destinations monitored by L2 ping from ACI leafs. Two IPS devices are used as active-active per each L1 PBR. Any contract trombones traffic to assigned L1-PBR, where EPGs are stretched across Pods and EPs can reside in each Pod.

L1 PBR with FTD Cluster and IPS of a vPC Pair

ACI has L1 PBR with one FTD cluster device (2x VPCs and 4x leaves required)



Problem Design - L1 PBR on FTD IPS HA Pair



- Does not work currently!!!
- FTD IPS nodes in HA need ability to disable MAC learning (enhancement filed)
- L2ping source MAC is always the same when fabric SLA monitors A, B, C, or D destination MACs
- The same Source MAC on both sides of FTD causes a MAC move blocking condition on FTD and SLA outage

Demo 2 – L1 PBR

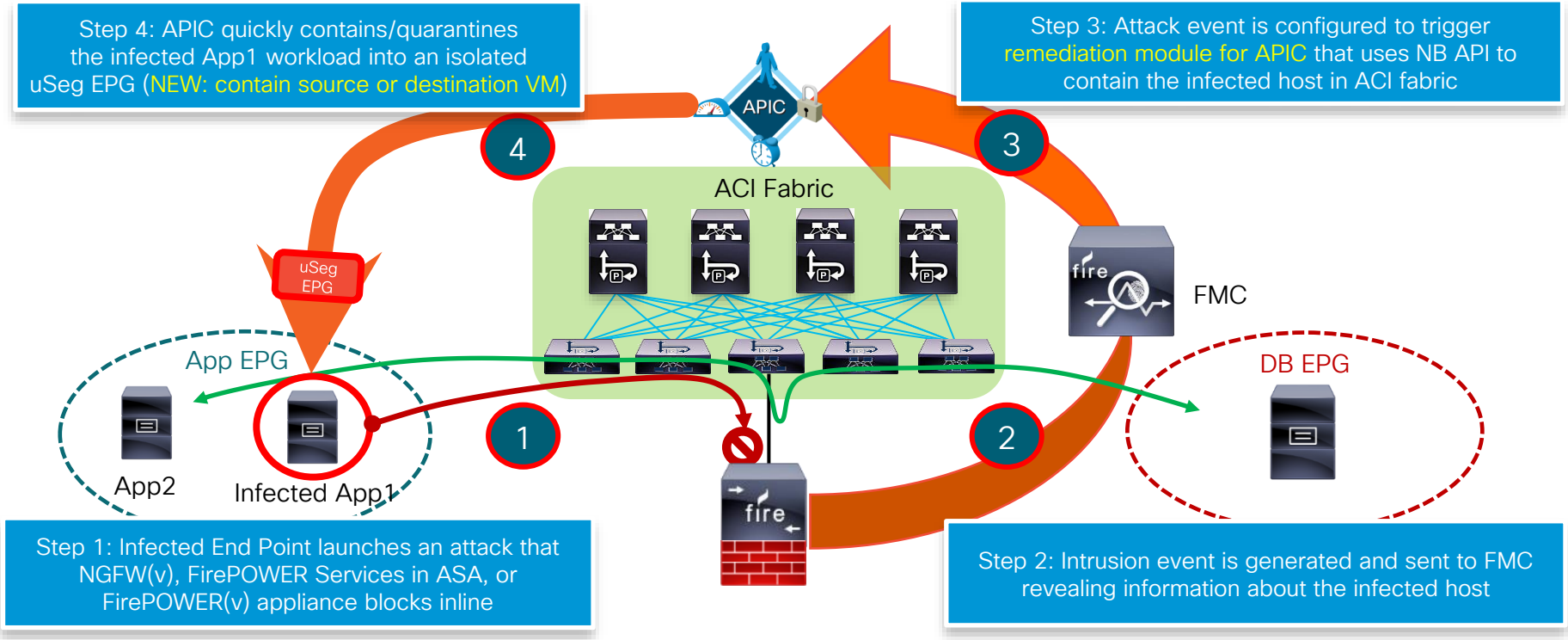
Enrich Firewall Policy from ACI

ACI Endpoint Update 2.1

- Endpoint and EPG updates to FMC and ASA
- Support for updates of FMC dynamic objects – no policy deploy required
- New GUI allowing cleaner updates to group of devices
- Per-device connectivity test
- Review an article on unofficialaciguide.com https://unofficialaciguide.com/2022/03/01/aci-endpoint-update-app-2-1-enhancing-ftd-and-asa-policies/

Rapid Threat Containment

FMC to APIC Rapid Threat Containment



Summary

PBR Deployment Options Summary

- L3 PBR is recommended – most used, enhanced with anycast service in Multi-pod, and supported with NDO in Multi-site deployments

- L2 PBR has a nice set of deployment options and ability to disable MAC learning for all cases. Must define static MAC addresses for PBRs.

- L1 PBR requires more careful configuration due to unchanged VLAN tag. It cannot support an HA option due to MAC learning. Tread carefully.

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

cisco Live!

ALL IN

#CiscoLive