The bridge to possible

Cisco Secure Firewall in ACI

L4-L7 Integration

Fabien Gandola , EMEA Security TSA

BRKDCN-3612

cisco Live!

Cisco Webex App

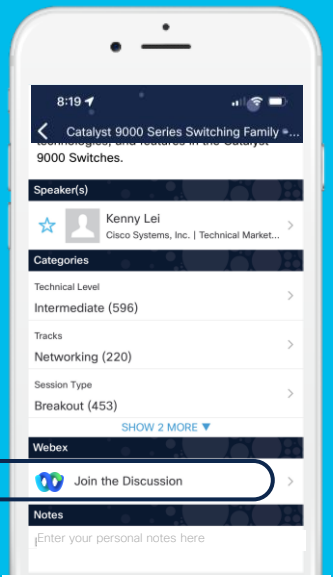
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-3612

Questions?

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

How

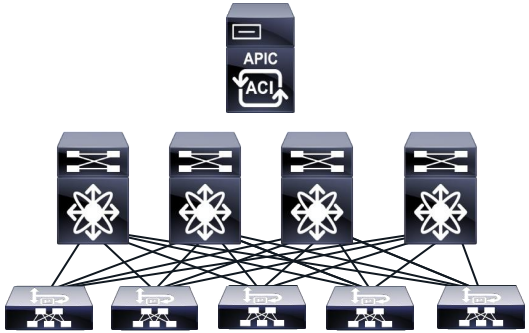
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



Webex spaces will be moderated until February 24, 2023.

Opening Statement

ACI IS NOT A FIREWALL



≠

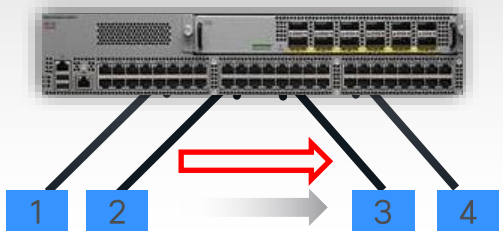
Does ACI help with Security ?

ACI Whitelist Policy supports “Zero Trust” Model

Whitelist policy = Explicitly configured ACI contract between EPG 1 and EPG 2 allowing traffic between their members

TRUST BASED ON LOCATION

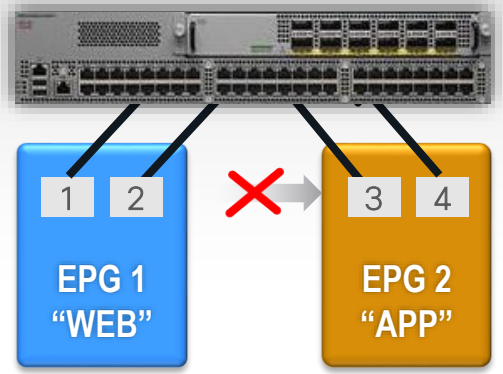
(Traditional DC Switch)



Servers 2 and 3 can communicate unless **blacklisted**

ZERO TRUST ARCHITECTURE

(Nexus 9K with ACI)



No communication allowed between Servers 2 and 3 unless there is a **whitelist policy**

Defining SDN use case for DC security

micro- segmentation

Programmability

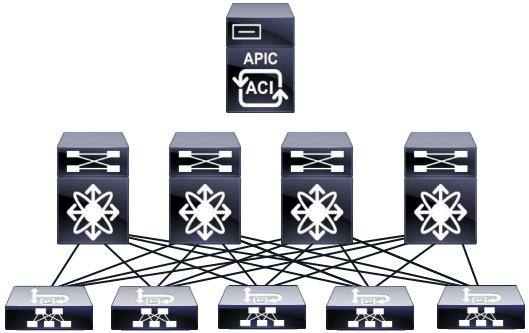
Automatic Remediation

Embedding security policy within Application

Ease of Service Insertion

Repeat after me

ACI IS NOT A FIREWALL



≠

FTD Converged Image

ASA

- L2-L4 Stateful Firewall
- Scalable CGNAT, ACL, routing
- Application inspection

FirePOWER

- Threat-centric NGIPS
- AVC, URL Filtering for NGFW
- Advanced Malware Protection

Firepower Threat Defense (FTD)

- Converged NGFW/NGIPS image on new Firepower and ASA5500-X platforms
- Single point of management with Firepower Management Center (FMC)
- Full FirePOWER functionality for NGFW/NGIPS deployments
- ASA Data Plane with TCP Normalizer, NAT, ACL, dynamic routing, failover, clustering

What should you expect … and not expect

- No Deep dive in ACI

The bridge to possible

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

Minako Higuchi, Technical Marketing Engineer, Cloud Networking Business Group

The bridge to possible

ACI – “not just another network…”

Steve Sharman – Technical Solutions Architect
@sps2101

What should you expect … and not expect

- No Deep dive in ACI
- No Deep dive in FTD
- Troubleshooting guide
- Introduction to FTD insertion in ACI
- Why using FTD in ACI
  - Introduction to “useful” features of FTD relevant to ACI
  - Use cases
  - Config guide overview

Agenda

- ACI Building Blocks *(super quick)*
- FTD Improvements for the DC
- FTD Insertion *(Mostly PBR L3)*
- FTD added value
  - Clustering
  - CSDAC and Dynamic Group
  - FTD + Cisco Secure Workload (Tetration)
  - Remediation module in FMC *(super quick)*

About Me

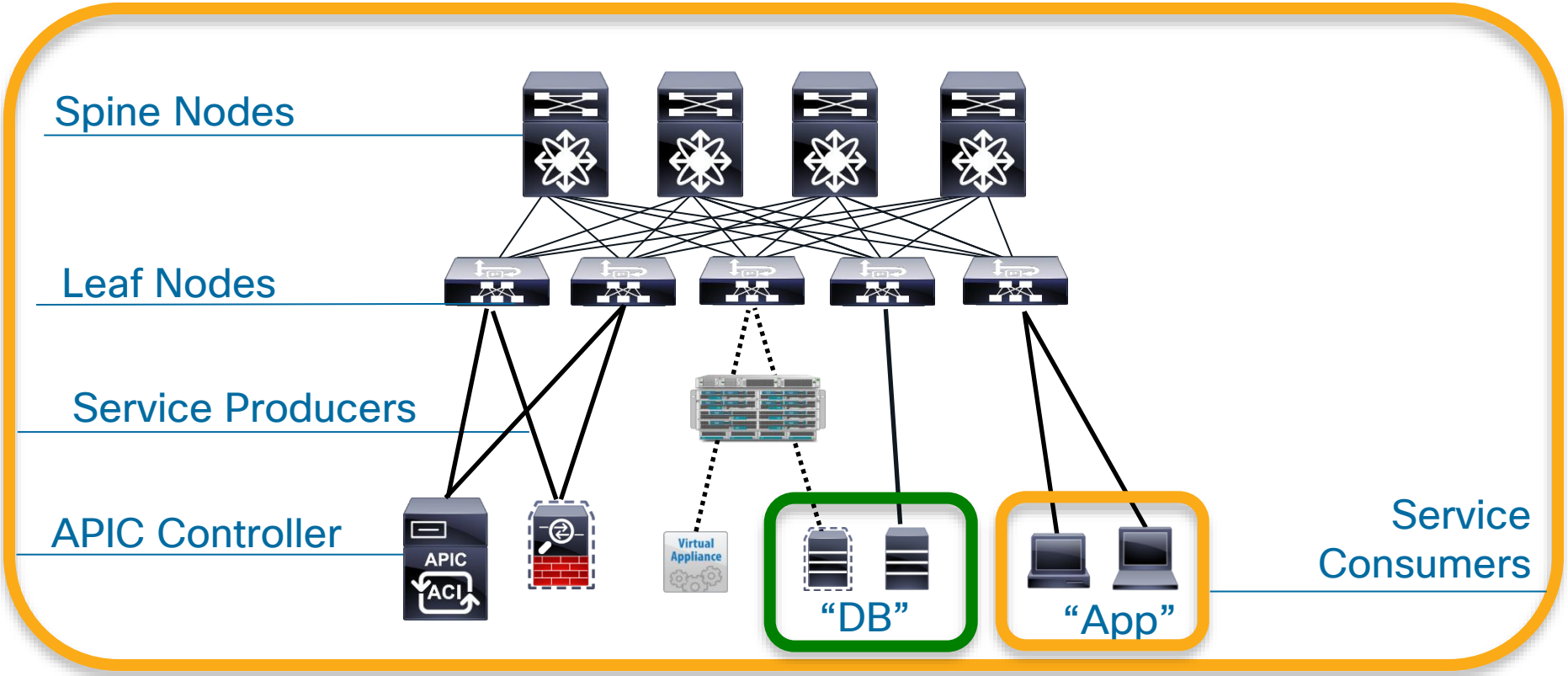
Fabien Gandola
fgandola@cisco.com

TSA Cyber Security EMEA

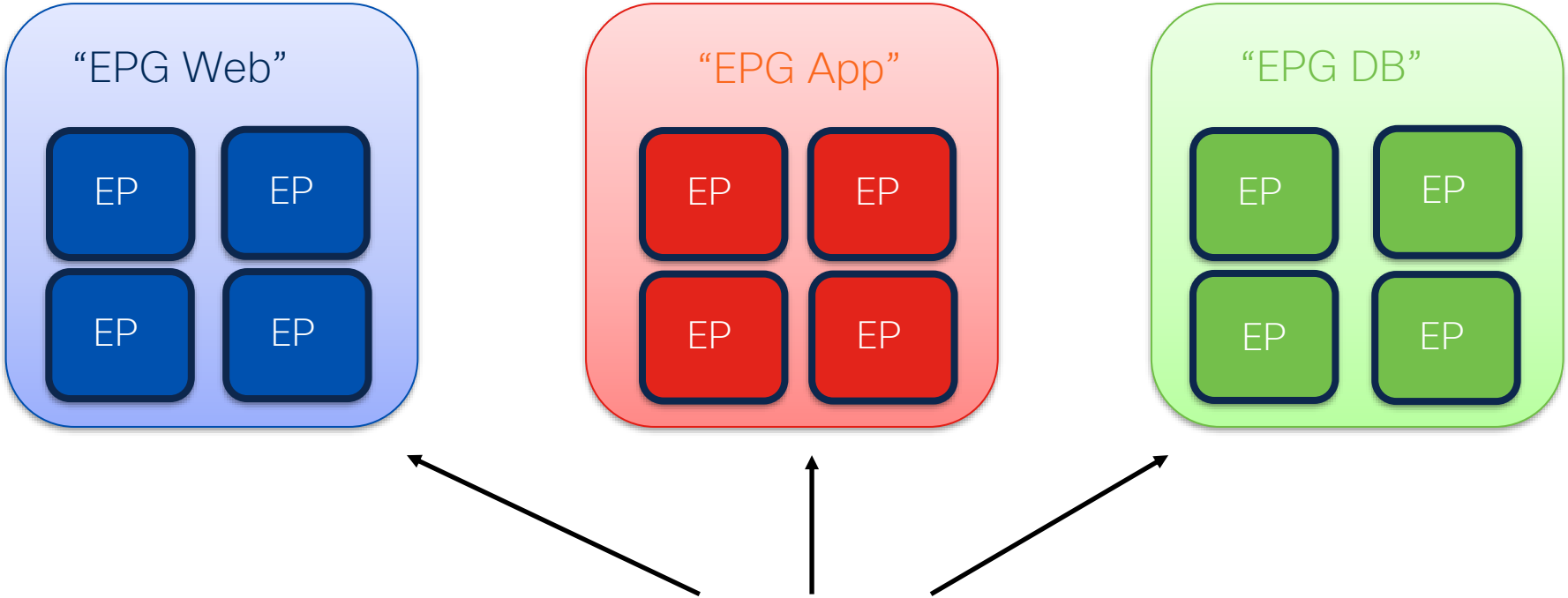
23 years in Cisco

Shortest introduction to ACI ever…

ACI Devices Role

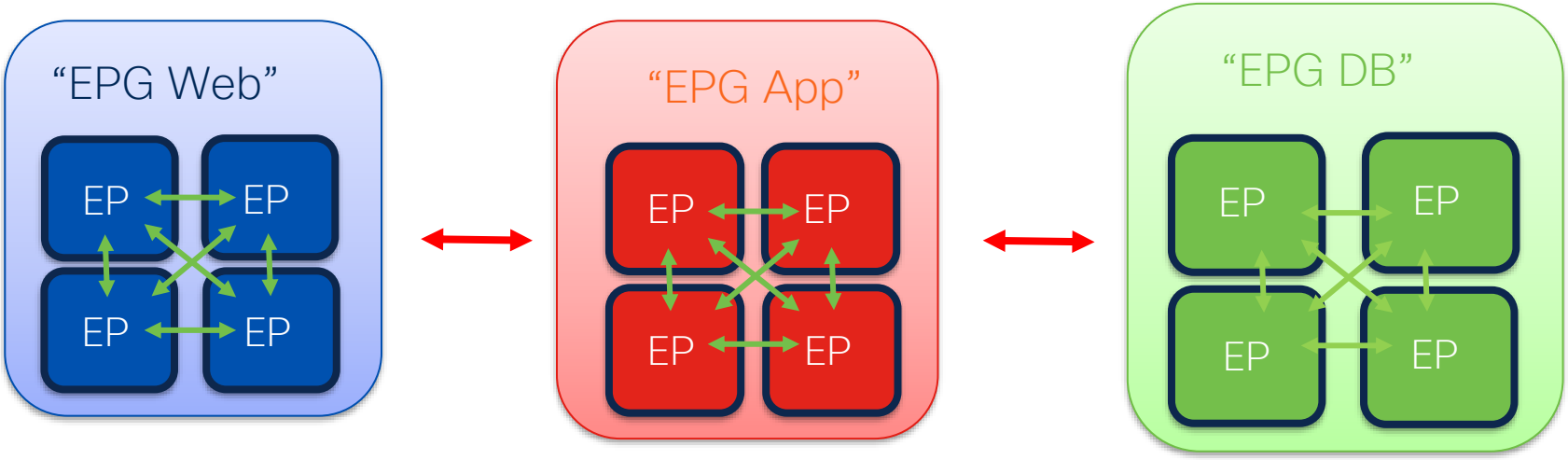


End Point Group



In the ACI model, we do this using the End Point Group (EPG).

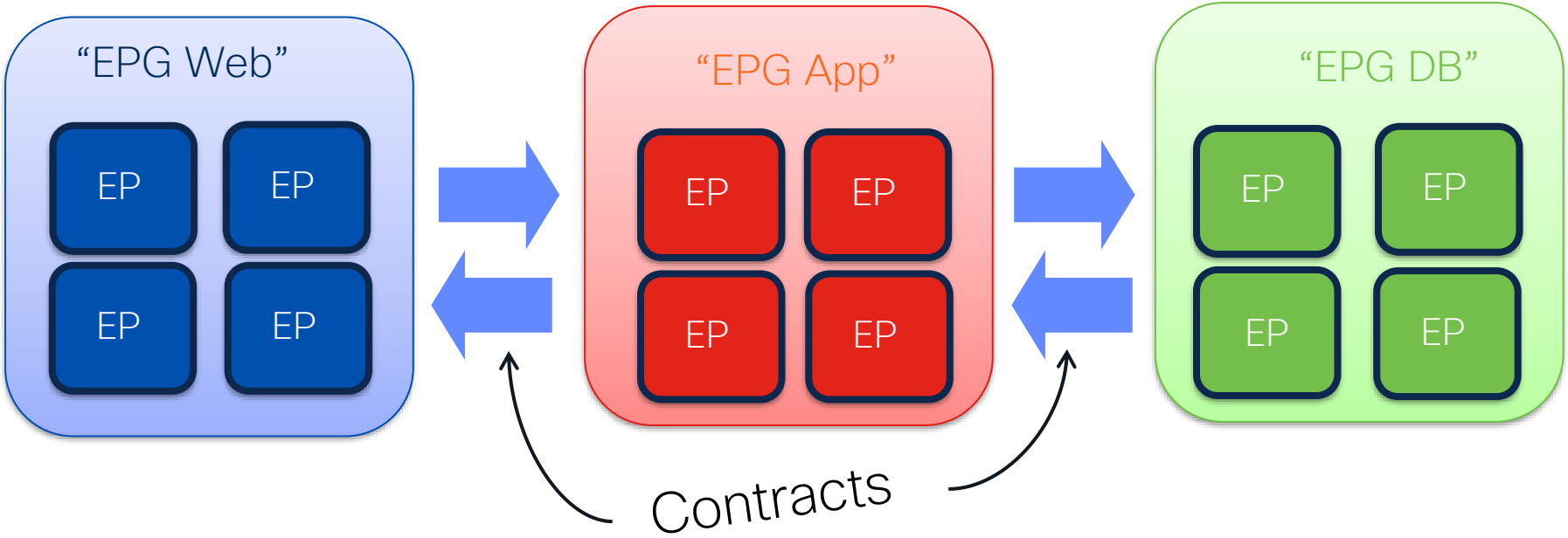
Endpoint Groups Communications



Devices within an Endpoint group can communicate, provided that they have IP reachability (provided by the Bridge Domain/VRF).

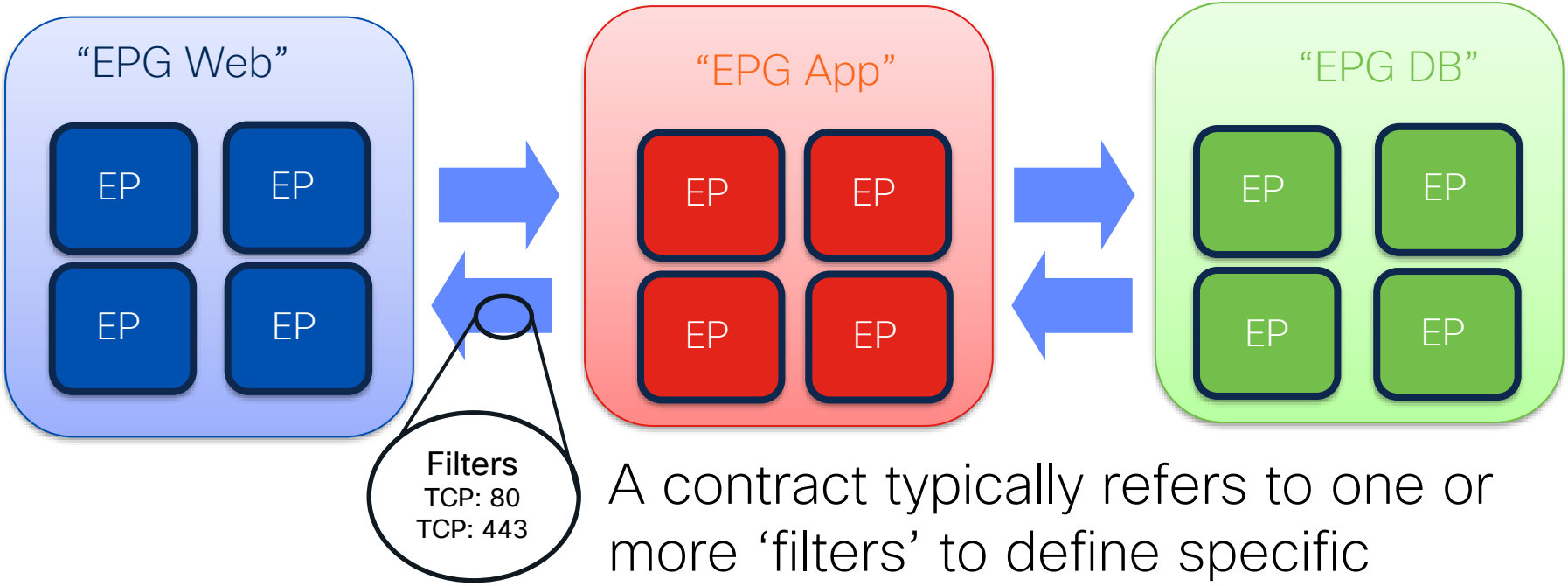
Communication between Endpoint groups is, by default, not permitted.

Contract



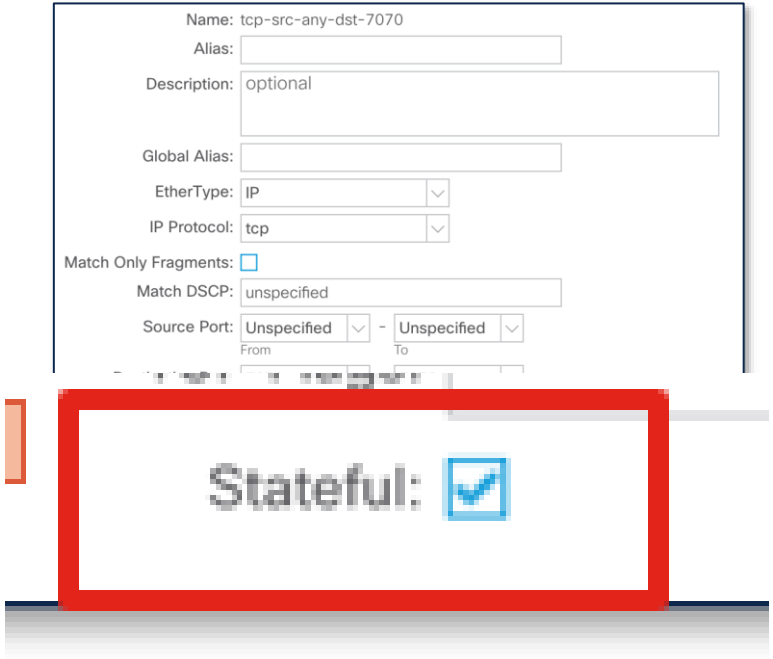
Once we have our EPGs defined, we need to create policies to determine how they communicate with each other.

Contract : Kind of reflexive “Stateless” ACLs



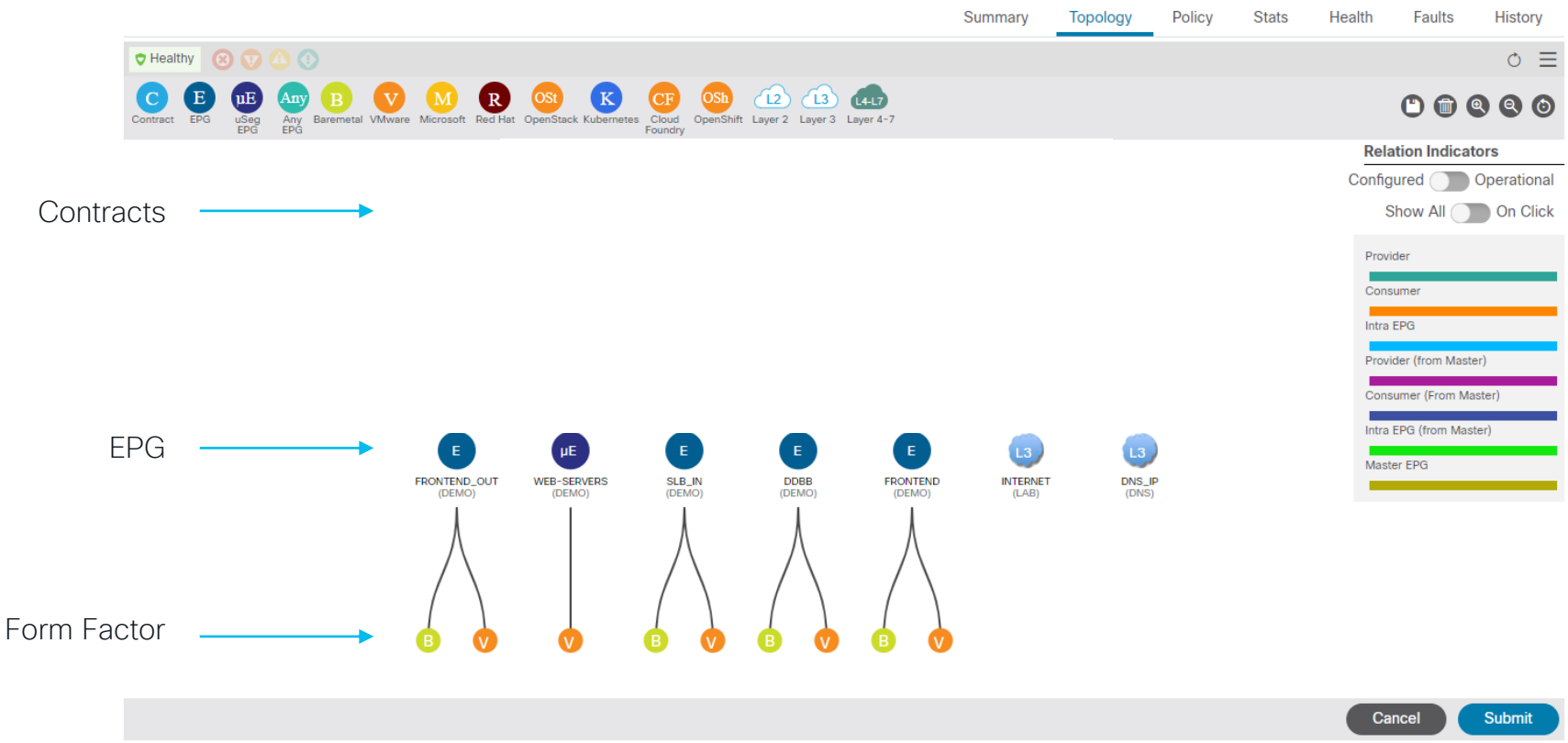
A contract typically refers to one or more ‘filters’ to define specific protocols & ports allowed between EPGs.

Did you say Stateless ?

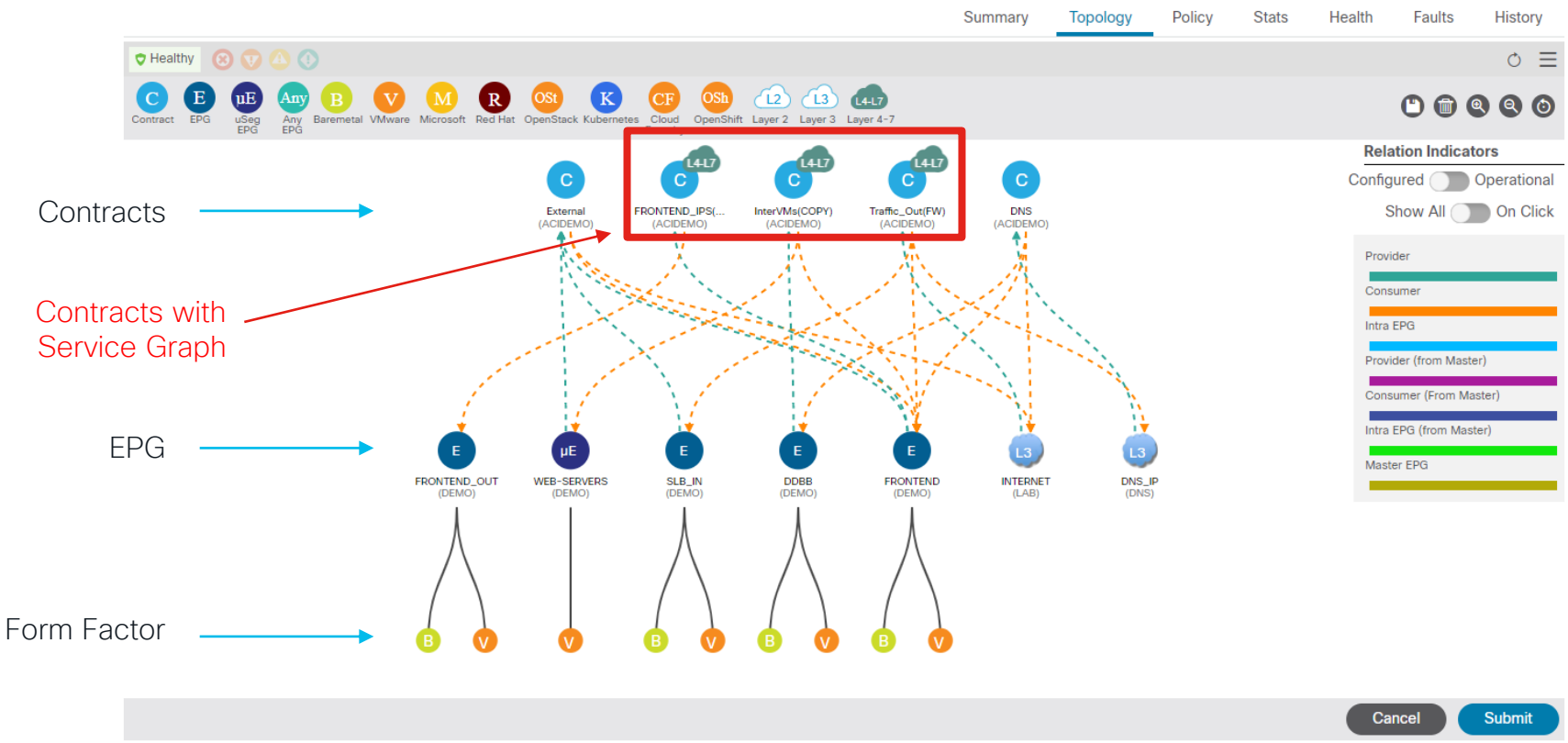


Ensure Ack bit is set so sessions can only be established consumer to provider

Application policy with contract



Application Policy with Contract



EPG and ESG

Create Application EPG

STEP 1 > Identity

Name:
Alias:
Description: optional
Annotations: Click to add a new annotation
Contract Exception Tag:
QoS class: Level3 (Default)
Custom QoS: select a value
Data-Plane Policer: select a value
Intra EPG Isolation: Enforced | Unenforced
Preferred Group Member: Exclude | Include
Flood in Encapsulation: Disabled | Enabled
Bridge Domain: select a value
Monitoring Policy: select a value
FHS Trust Control Policy: select a value
EPG Admin State: Admin Up | Admin Shut
Associate to VM Domain Profiles:
Statically Link with Leaves/Paths:
EPG Contract Master:
Application EPGs

Create Endpoint Security Group

STEP 1 > Identity

1. Identity | 2. Selectors

Name:
Description: optional
VRF: select a value
ESG Admin State: Admin Up | Admin Shut

Create Endpoint Security Group

STEP 2 > Selectors

1. Identity | 2. Selectors | 3. Advanced (Optional)

Tag Selectors:
Tag Key | Value Operator | Tag Value | Description

EPG Selectors:
EPG | Description

IP Subnet Selectors:
IP Subnet | Description

Tag Selector for ESG

Create a Tag Selector

Tag Key: tn-fgandola:applications

In order to match a VM Name, please use key __vmm::vmname

Value Operator: Contains | Equals | Regex

Tag Value: production

Description: optional

APIC

vSphere

- fgandola
  - fab_ubuntu_01
  - fab_ubuntu_02
  - fab_ubuntu_03
  - FMC72.uktme.cisco.com
  - ftdv-03-OLD.uktme.cisco.com
  - ftdv-03.uktme.cisco.com
  - ftdv-04-OLD.uktme.cisco.com

Tags

Assigned Tag	Category
tn-fgandola:applications:production	Function

FTD in 9 slides

Cisco DC Firepower Software to Hardware

Firewall (ASA) App

Modes of Operation:
Transparent &
Routed

Management:
CLI, ASDM,
CDO, & CSM

Multi-Context

FPR9300

FPR4100

FPR3100

NGFW (FTD) App

Modes of Operation:
Transparent, Routed, & IPS

Management:
Firepower Device Mgr / CDO
& FMC

Expansion Modules for
Fail-to-Wire (aka. Bypass)

Multi-Instance, VRF-lite, Multi-
Domain

Firewall Virtual Platforms

Private Cloud

HyperFlex

vmware ESXi

KVM

NUTANIX

openstack.

Public Cloud

Google Cloud Platform

ORACLE CLOUD INFRASTRUCTURE

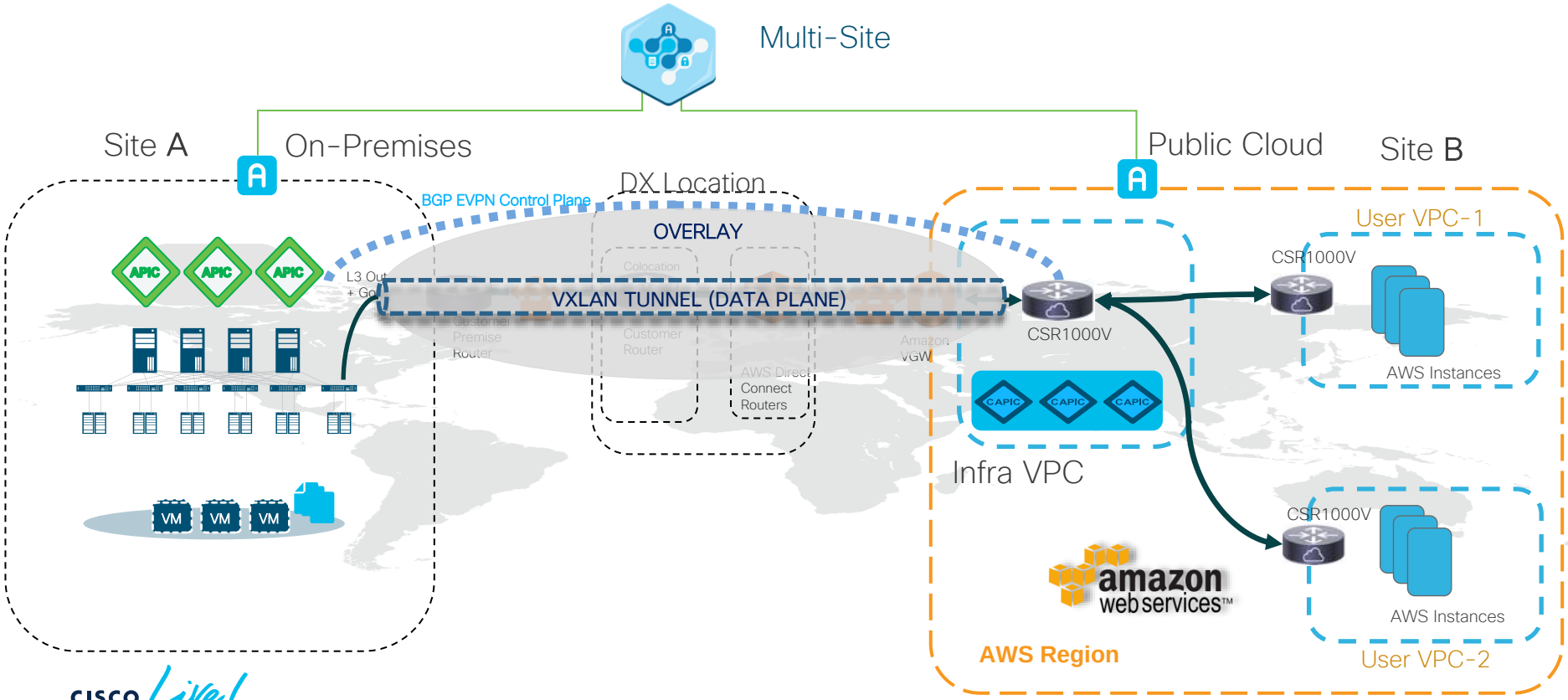
aws

Azure

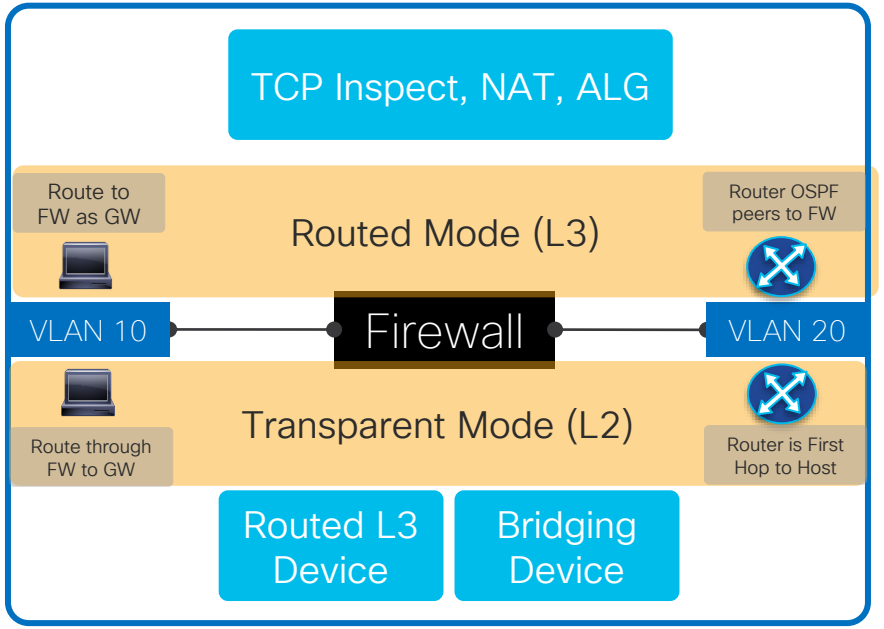
Alibaba Cloud

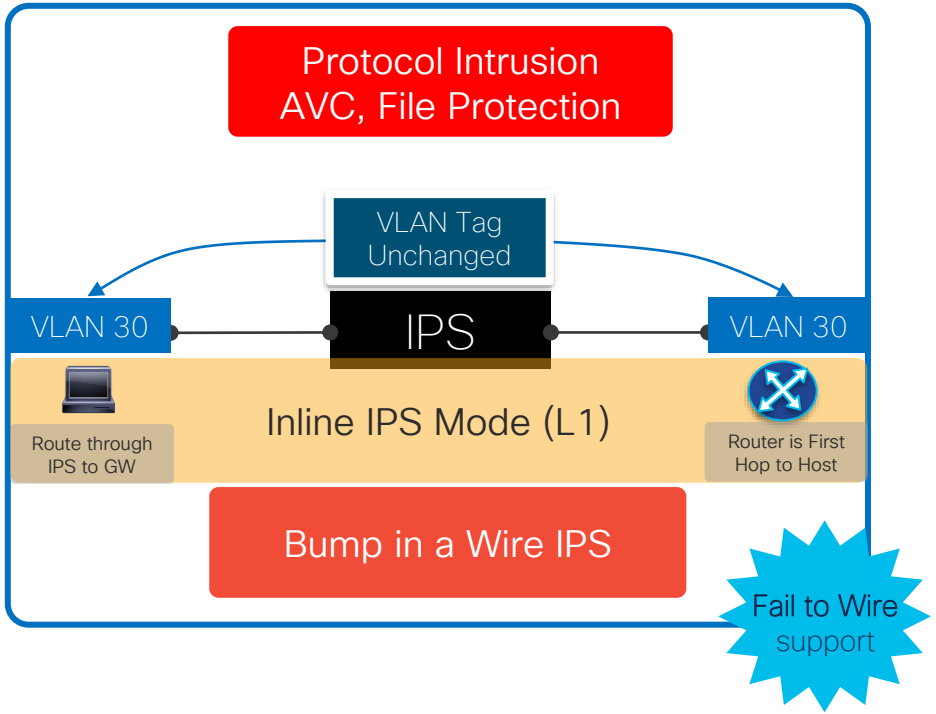
ACI Anywhere: On-Prem Connectivity To AWS

VPC With Direct Connect + VPN



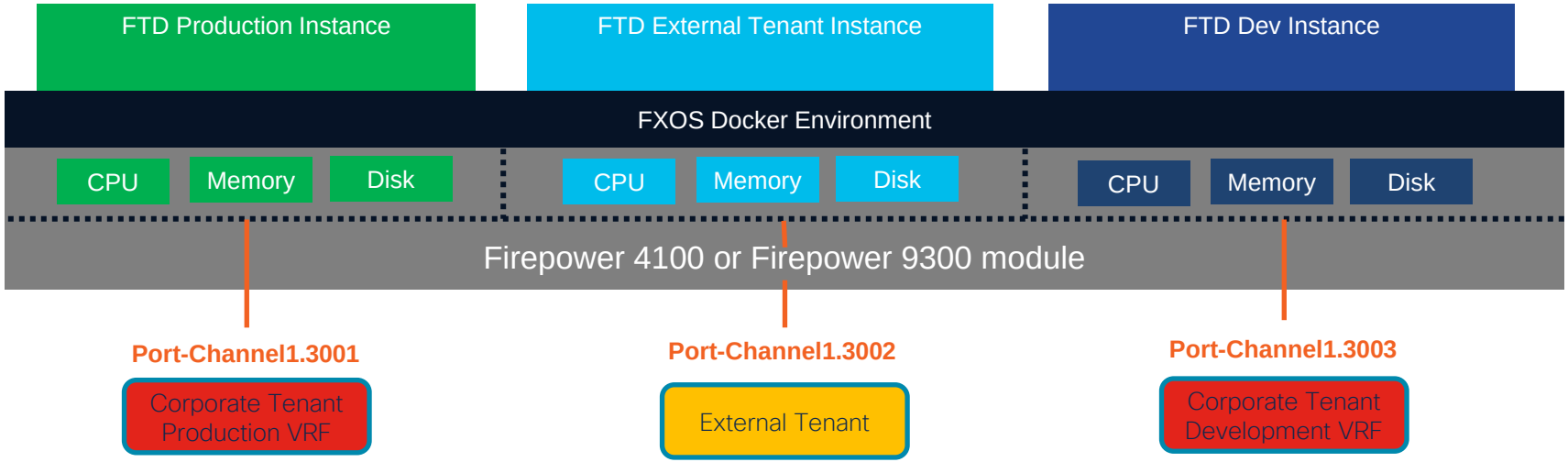
Cisco Secure Firewall Modes of Operation





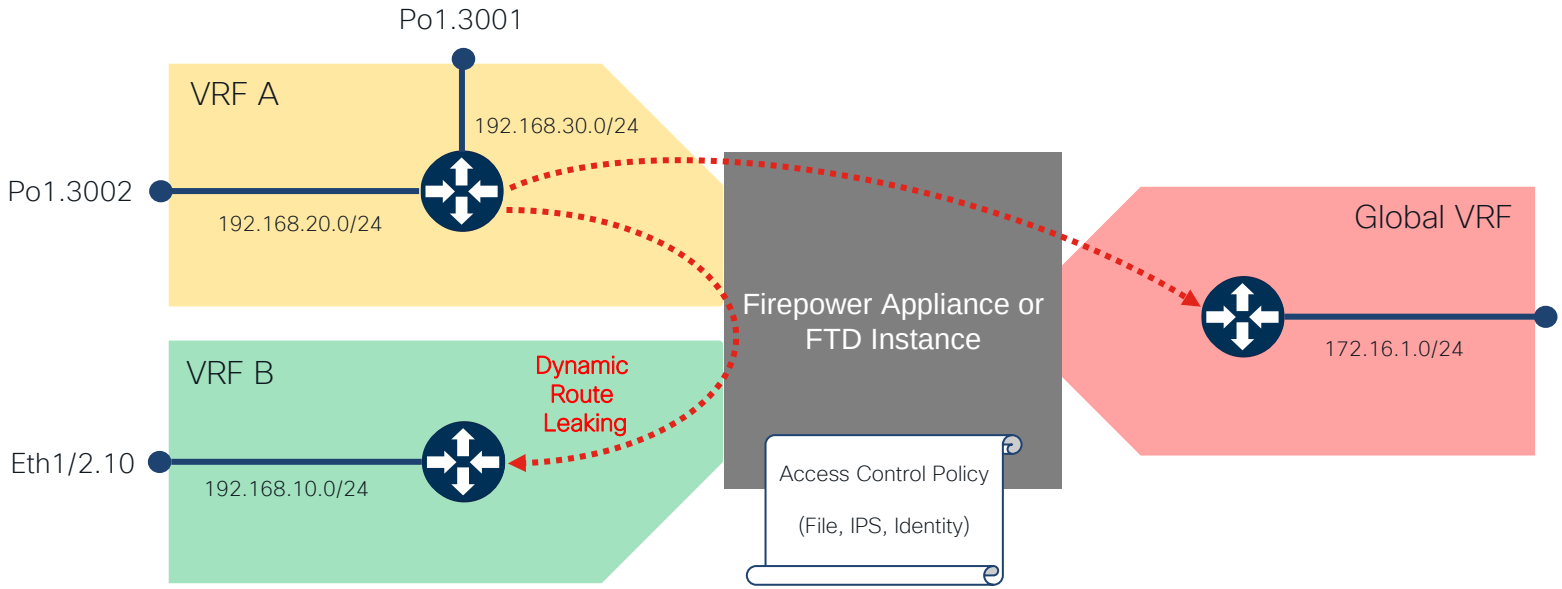
FTD Multi-Instance DC Use Case

- Create multiple logical FTD devices on a single module or appliance, and use as separate devices in the ACI fabric
- Complete traffic processing and management separation while protecting DC apps
- Supported on Firepower 4100 and 9300 only
- Dev firewall can overload/go offline/upgrade with out any effect on Production or External instances

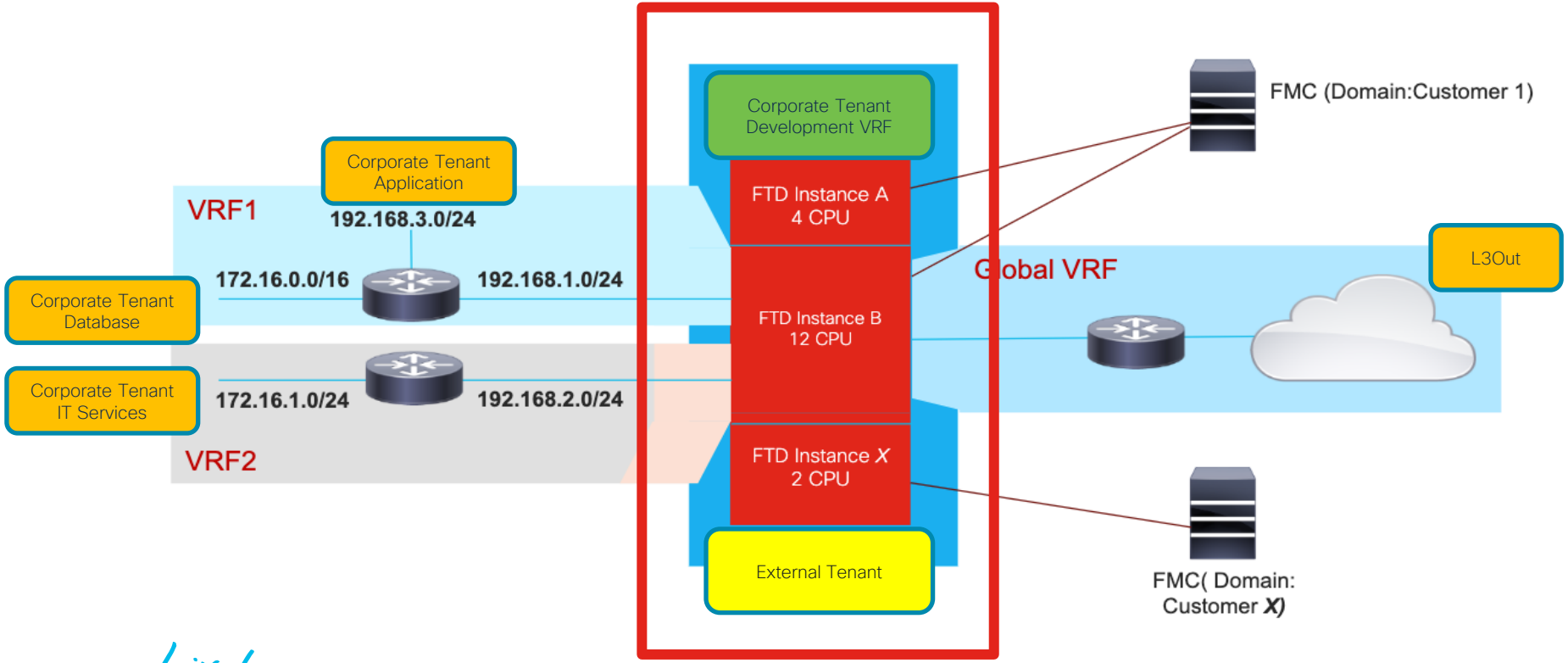


Virtual Routing and Forwarding (VRF) Lite

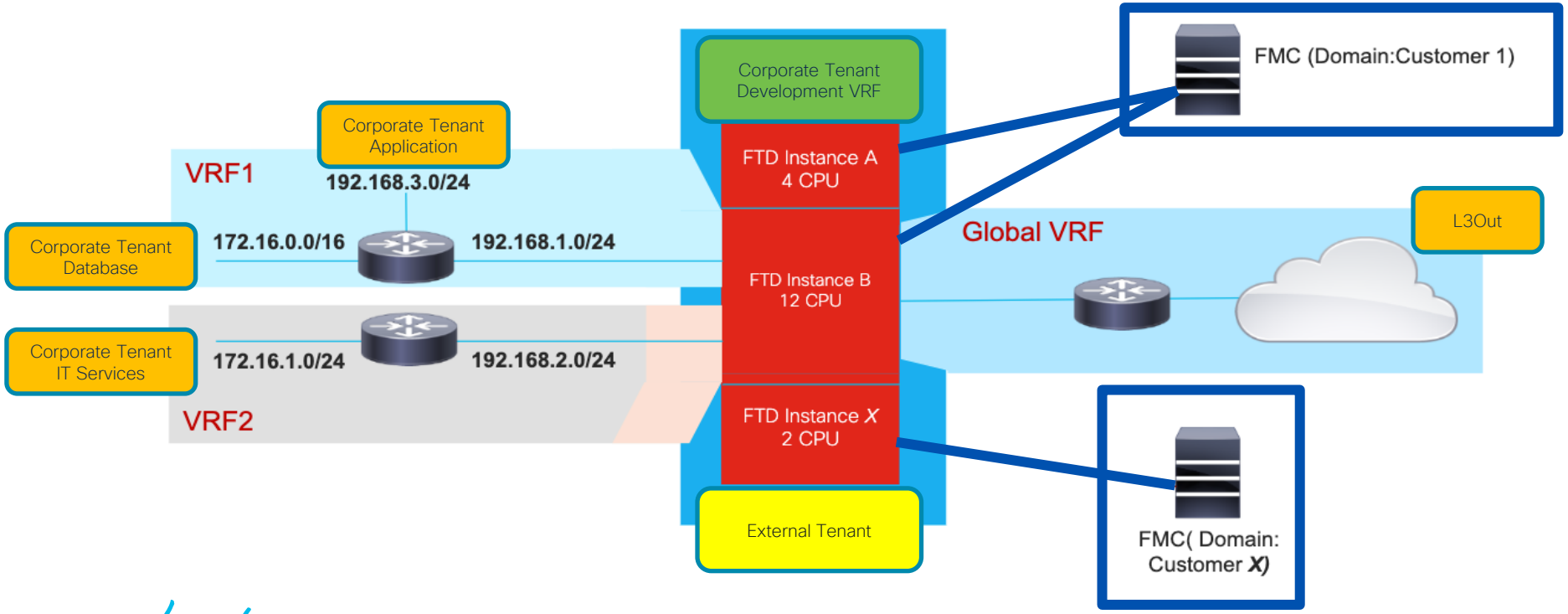
- In FTD 6.6, interfaces can be in different Routing Domains (Overlapping IP address support between User and Global VRF)
- Allows for easy separation of Service Graphs within the same FTD



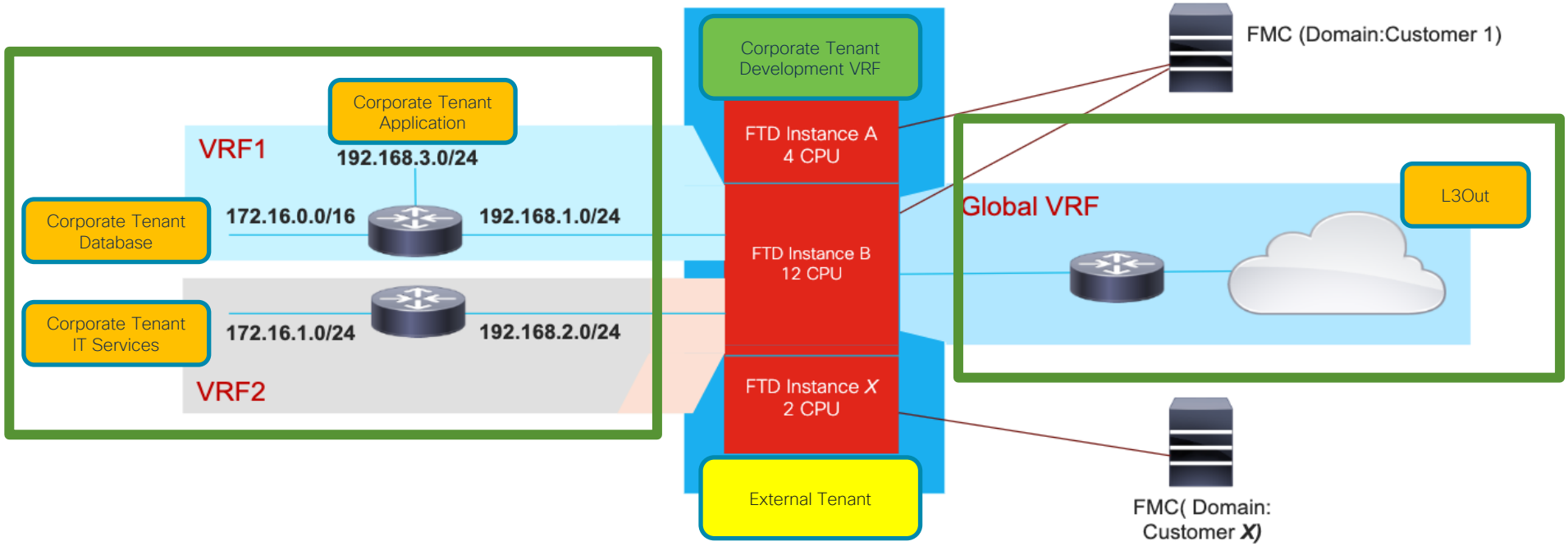
Multi-Instance, VRF and Multi-Domain Combined



Multi-Instance, VRF and Multi-Domain Combined



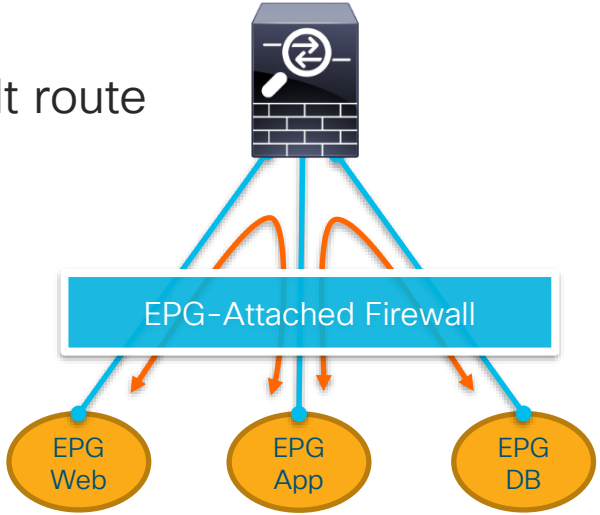
Multi-Instance, VRF and Multi-Domain Combined



Secure Firewall Insertion

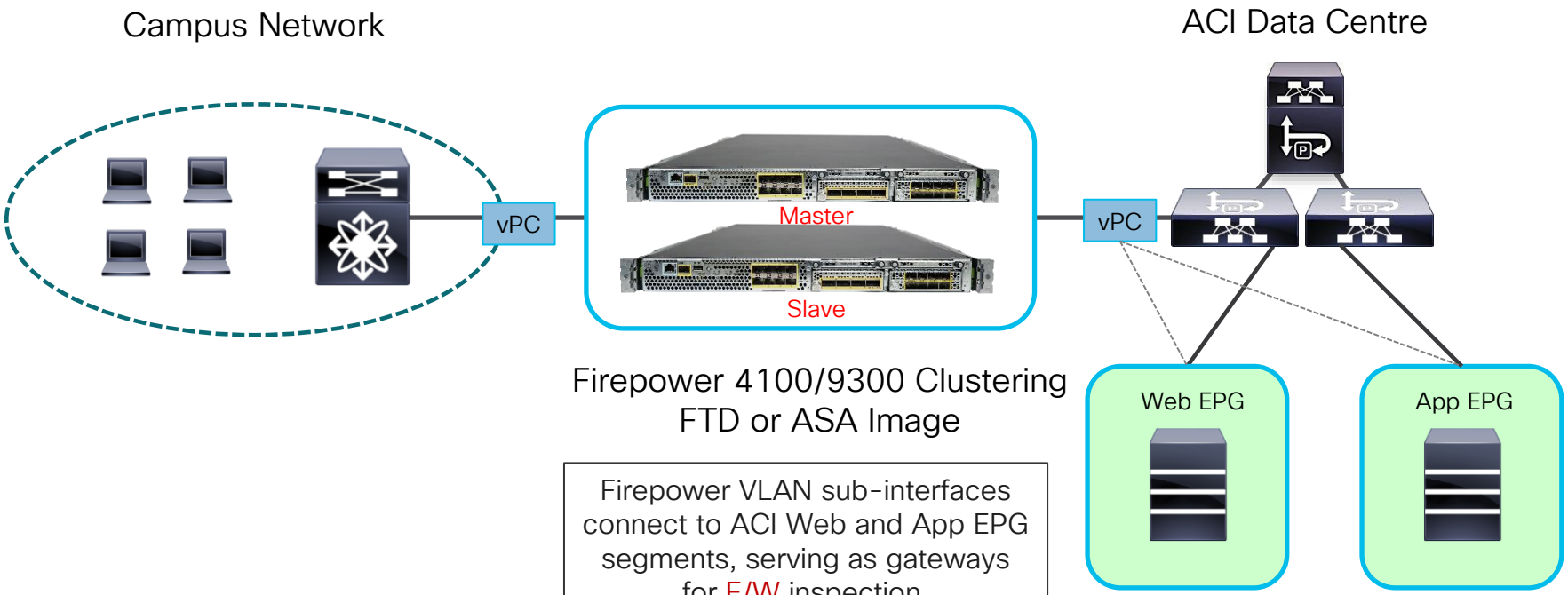
Network-Centric ACI Fabric

- First steps into ACI Fabric
- Simple (familiar) deployment: **EPG = Subnet = VLAN**
- Attach EPGs to firewall
- EPGs point to corresponding FW IP for default route
- Use FW to route and secure between EPGs



Firepower Cluster at Perimeter to ACI Fabric

Classic 'Cut-in' design for N/S and E/W EPG protection – EPG-attached

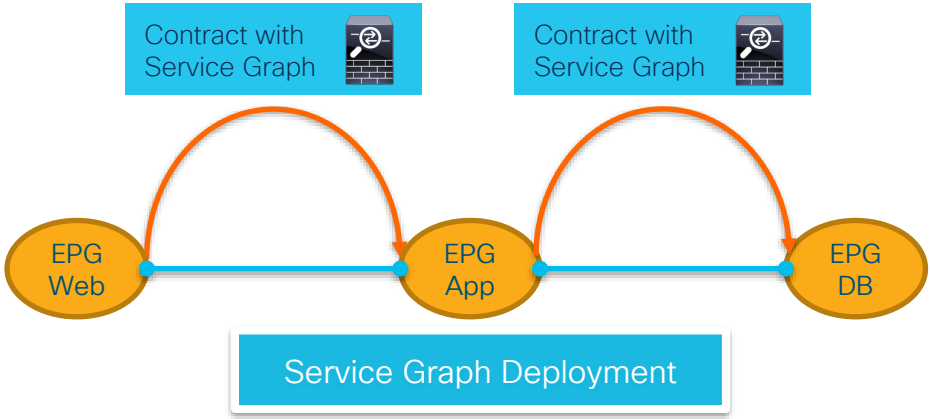


Firepower 4100/9300 Clustering
FTD or ASA Image

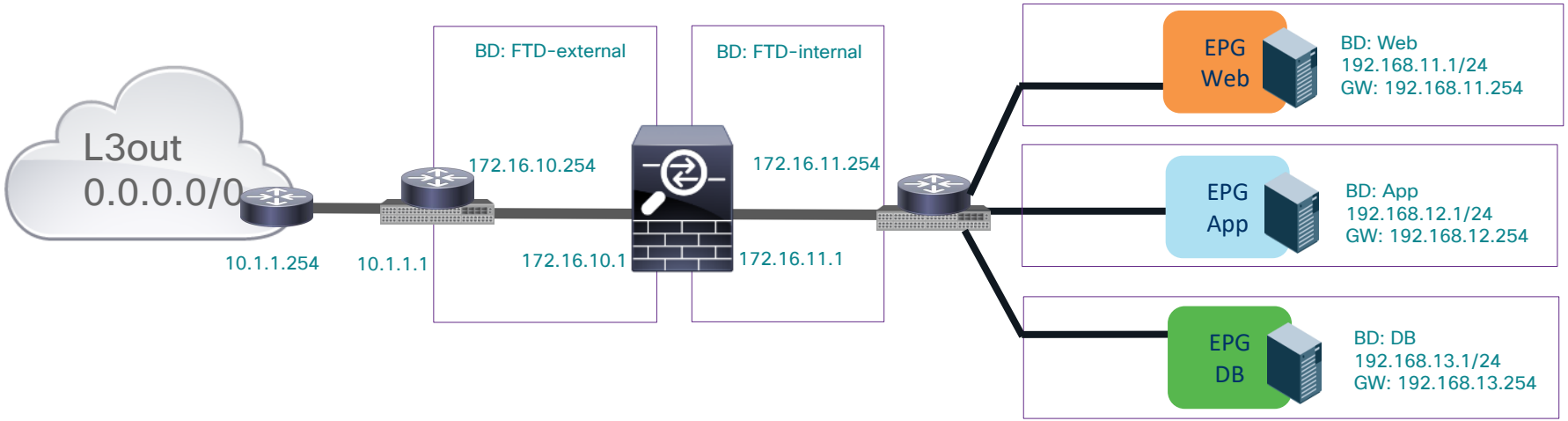
Firepower VLAN sub-interfaces connect to ACI Web and App EPG segments, serving as gateways for E/W inspection.

App-Centric ACI Fabric

- Contracts define communication between EPGs
- Service Graphs specify the services between EPGs and are referred in Contracts
- Configure Firewall in Go-To/Go-Through modes or L1 NGIPS

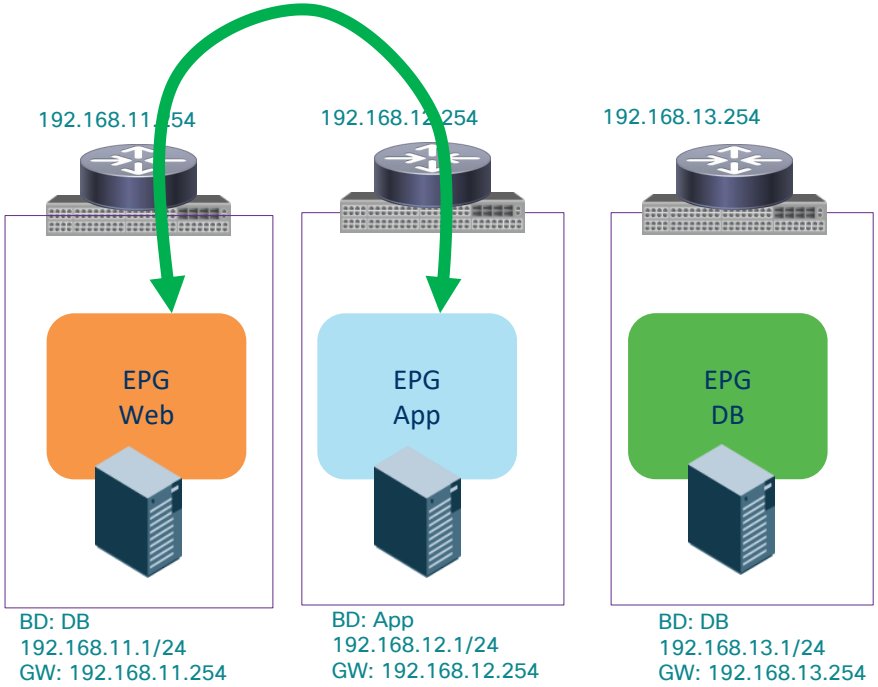


Topology



Policy Based Redirect is your Best Friend

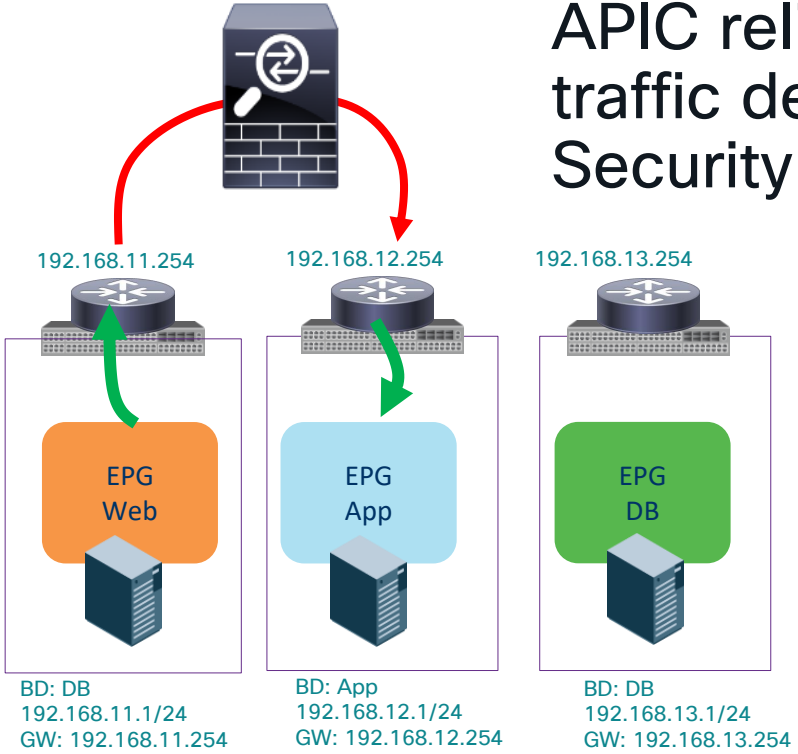
Before Service graph is deployed



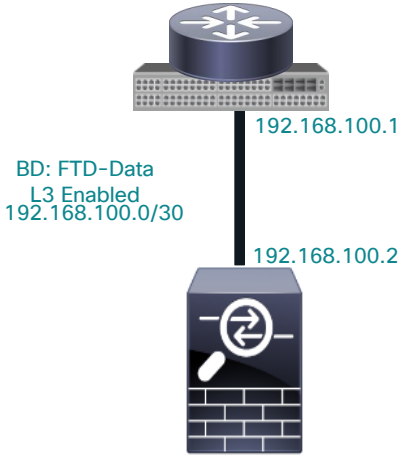
APIC relies on **Routing** to forward traffic from Server in EPG WEB to Server in EPB APP based on contract

Policy Based Redirect is your Best Friend

With PBR Service Graph

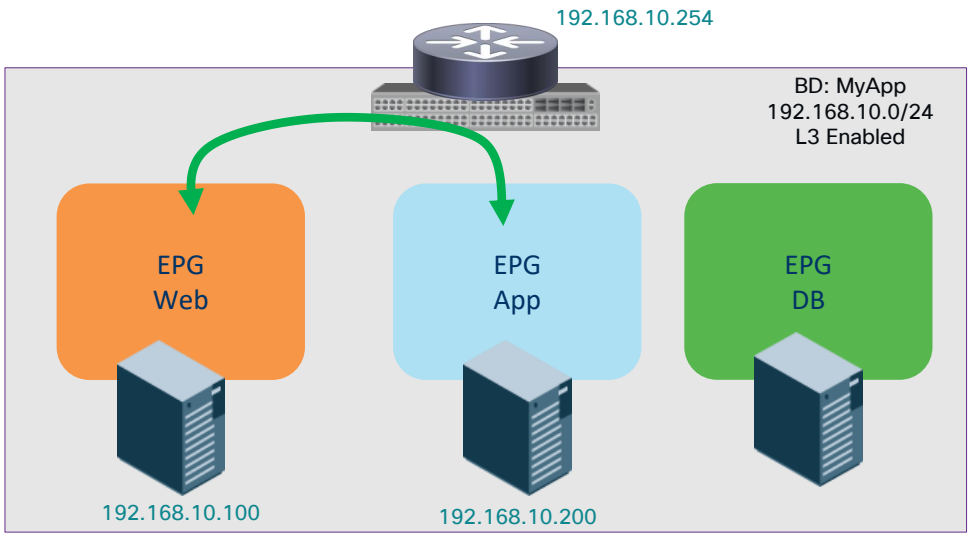


APIC relies on **PBR** to redirect the traffic defined in the contract to the Security Service



PBR for micro-Segmentation

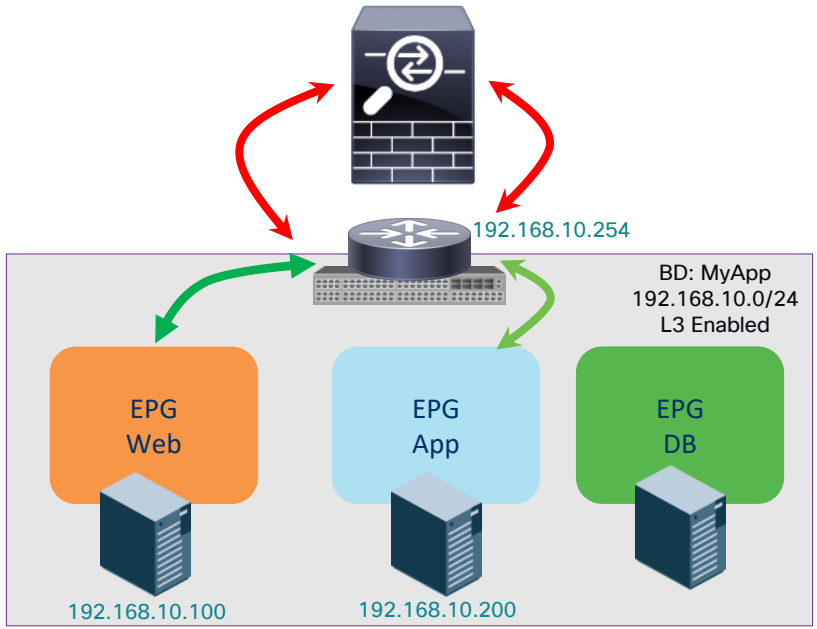
Based only on Contract



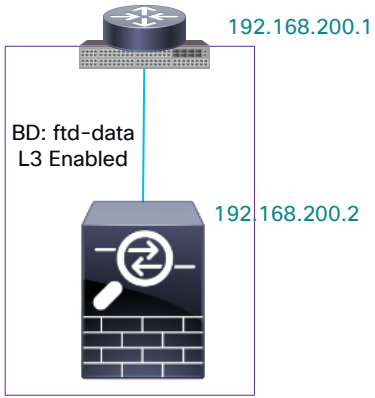
Because this is a communication between two End-points in different EPG, the forwarding decision is made in the leaf switch

PBR for micro-Segmentation

Leveraging PBR



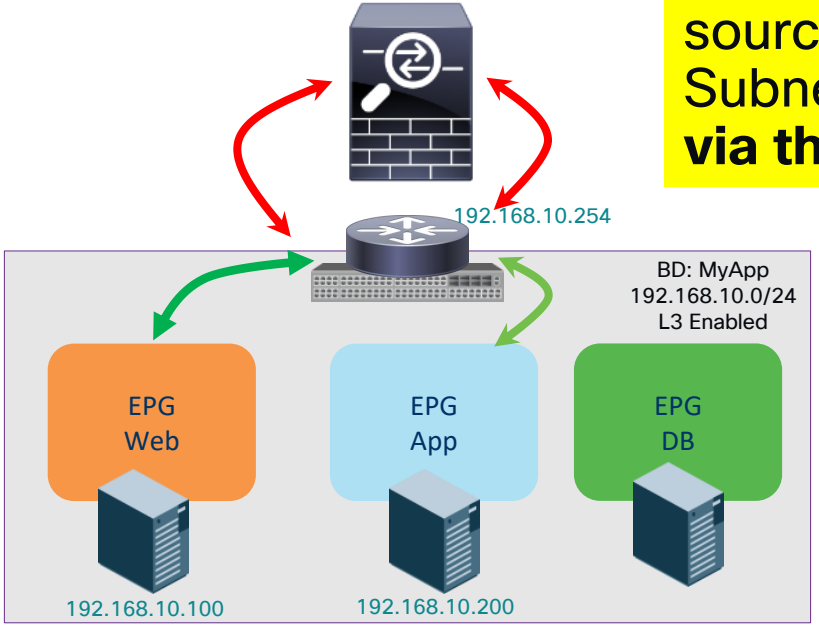
Because the traffic goes to Leaf Switch where PBR rules are enforced, traffic will be sent to the security service defined in the Service Graph.

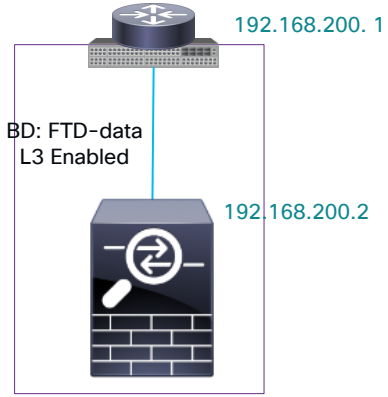


PBR for micro-Segmentation

Leveraging PBR

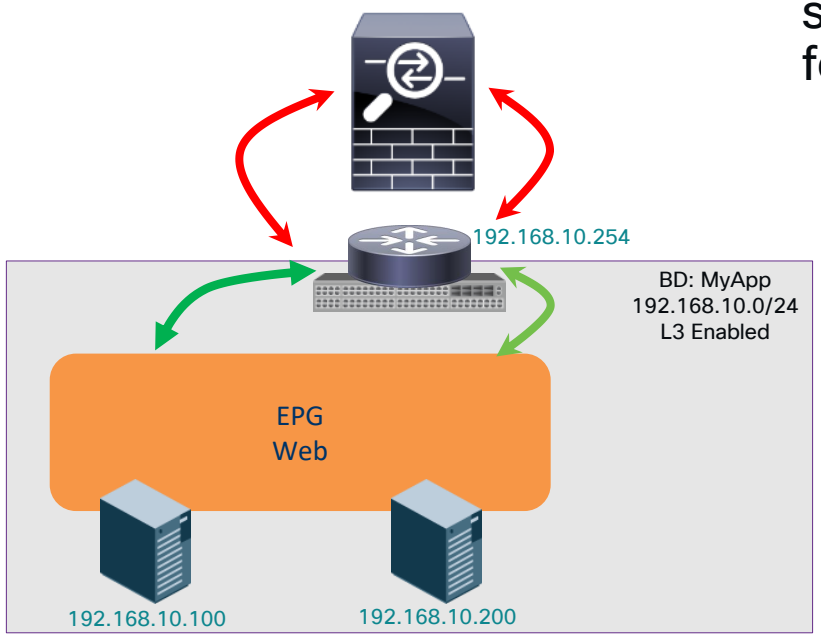
The Firewall must be in **ONE ARM** as source and destination are in the same Subnet. It must **allow traffic in and out via the same interface.**



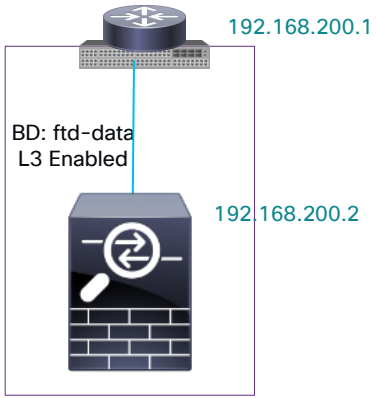


Redirecting traffic within an EPG/ESG

Leveraging PBR

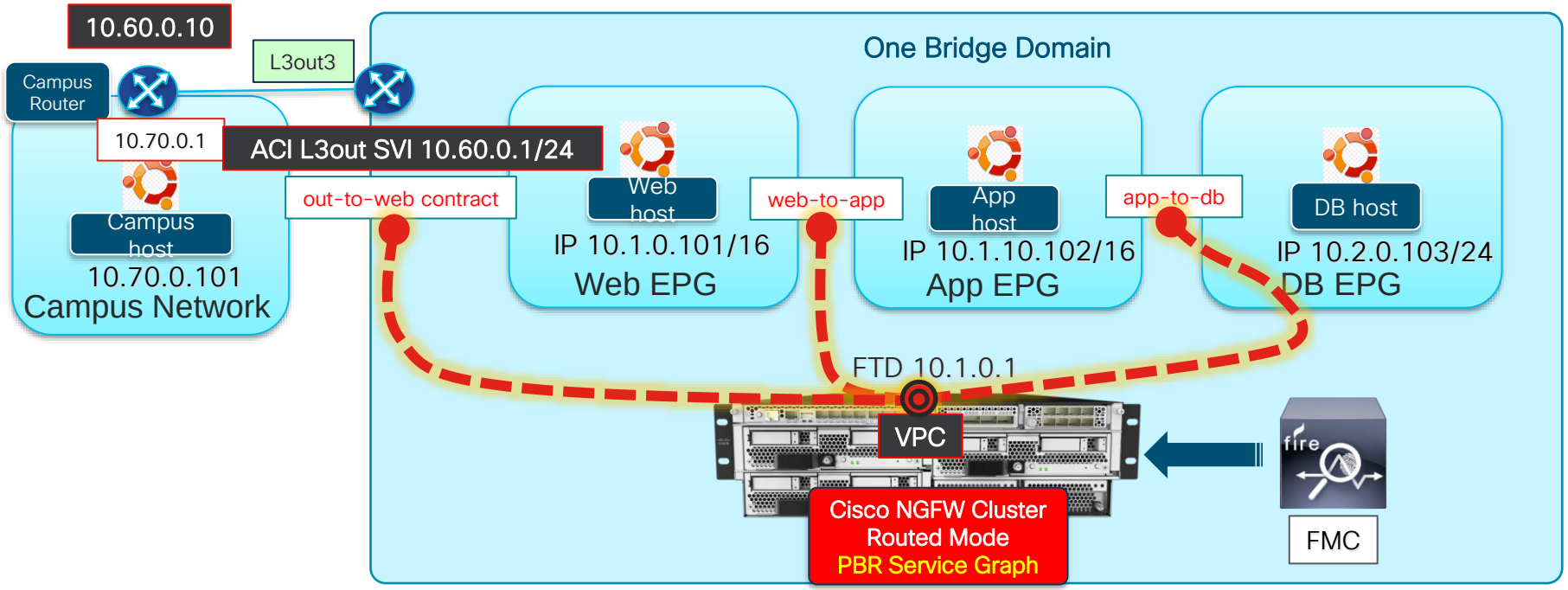


Using PBR, it is possible to attach a service graph to redirect traffic to FTD for traffic inside an EPG



Reuse a PBR Service Graph in Multiple Contracts

Keep the Firewall Network Config Simple



Cisco Secure Firewall and ACI Key Benefits

Multi-Pod Cluster

Single FTD cluster stretched across multiple ACI Pods.

Predictable traffic flow with Firewall localization to a single Pod.

Seamless failover within and between pods with FTD cross-cluster connections state synchronization.

Attribute-Based Policy

Streamline security policy with Dynamic Objects, Security Group Tags and User information.

Keep your policy tight and always up-to-date with dynamic EPG/ESG updates.

Rapid Threat Containment

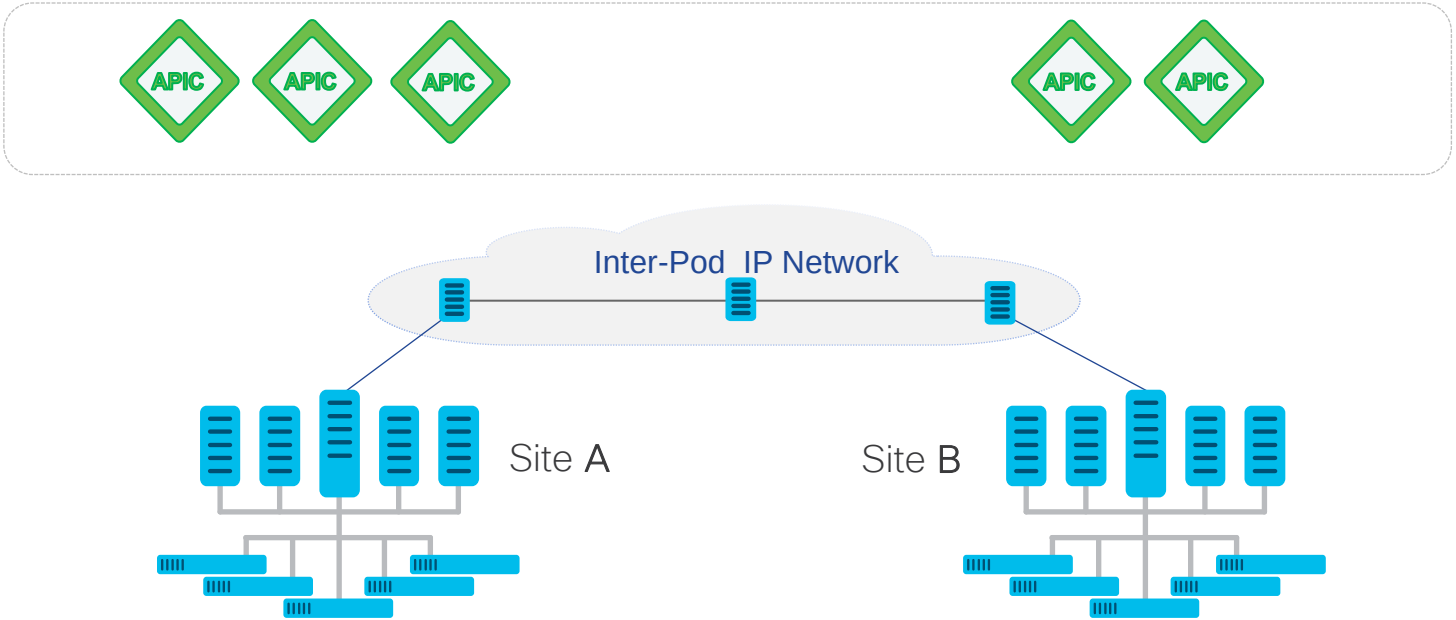
Automatic network threat containment using the network as an enforcer

Threat-centric network access determines network access based on IoCs

Multi-Pod Resilience with FTD Cluster

ACI MultiPod

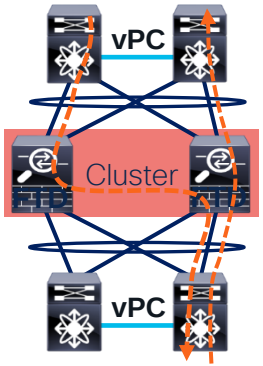
Single APIC Cluster Extends Network Virtualization, Policy, Services to Multiple PODs



Active-Active Datacenters | Virtual Metro Clusters | Stretch VRF, EPG, BD Across PoDs with VXLAN | Up to 50ms Latency

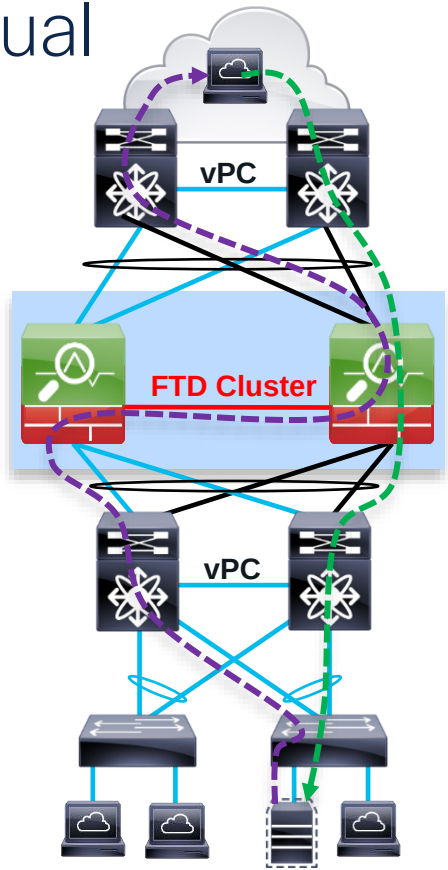
ASA and FTD Clustering

- Up to 16 appliances or modules combine in one traffic processing system
- Preserve the benefits of failover
  - All members are managed as a single entity
  - Virtual IP and MAC addresses for first-hop redundancy
  - Connection states are preserved after a single member failure
- Implement true scalability in addition to high availability
  - Fully distributed data plane for new and existing connections
  - Elastic scaling of throughput and maximum concurrent connections
  - Stateless external load-balancing through standard Etherchannel or routing
  - Out-of-band Cluster Control Link for asymmetry normalization
  - No member-to-member communication on data interfaces

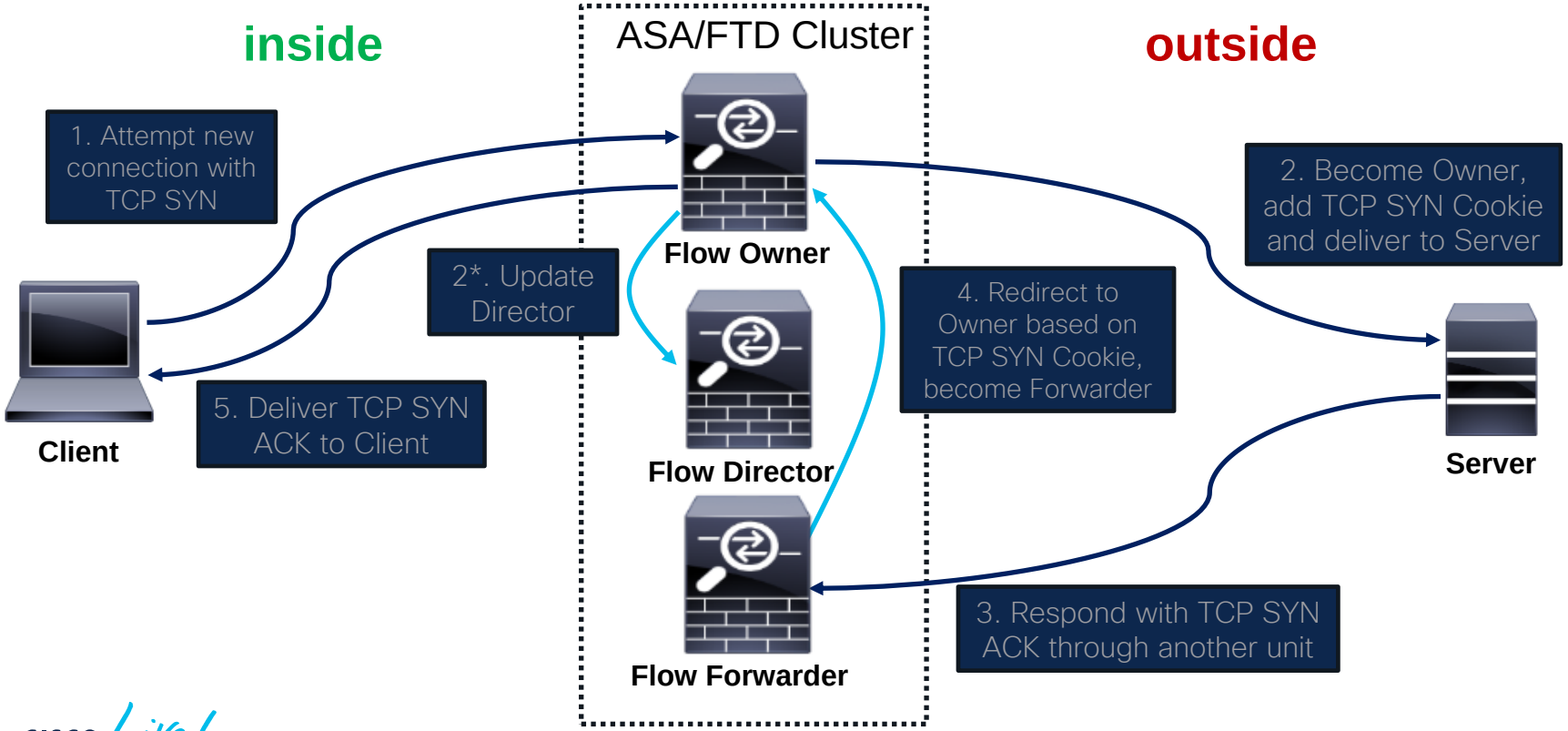


Clustering Concepts – Physical and Virtual

- Cluster roles
  - Control Node – synchronizes cluster configuration
  - Flow Director (deterministic) – keeps track of owner
  - Flow Owner (nondeterministic) – receiver of first packet of flow
- Cluster Control Link (CCL)
  - Internode communication
  - Asymmetric traffic redirection to flow owner
- State sharing
  - Cluster nodes share connection state
    - Each connection state is stored on two nodes
  - Cluster nodes *do not share* IPS state



New TCP Connection



Create an FTD cluster in FMC

Name

Secret Key

First Cluster Node

CCL Information

Add cluster members

Add Cluster Wizard

1 Configuration — 2 Summary

Create a cluster for supported models. Note: For the Firepower 4100/9300/AWS/Azure/GCP, use the Add Device option.

Cluster Name*

Cluster Key

Type an ASCII string between 1 and 63 characters

Confirm Key

Control Node

You can form the cluster with just the control node to reduce formation time.

Node*

Type device name

Cluster Control Link Network*

For Example 10.10.4.0 / 27 (30 addresses)

Cluster Control Link*

EtherChannel or Physical Interface

Cluster Control Link IPv4 Address*

For Example 10.10.4.1

Priority*

1

Site ID

0

Data Nodes (Optional)

Data node hardware needs to match the control node hardware.

Node*

Type device name

Cluster Control Link IPv4 Address*

For Example 10.10.4.1

Priority*

2

Site ID

0

Remove

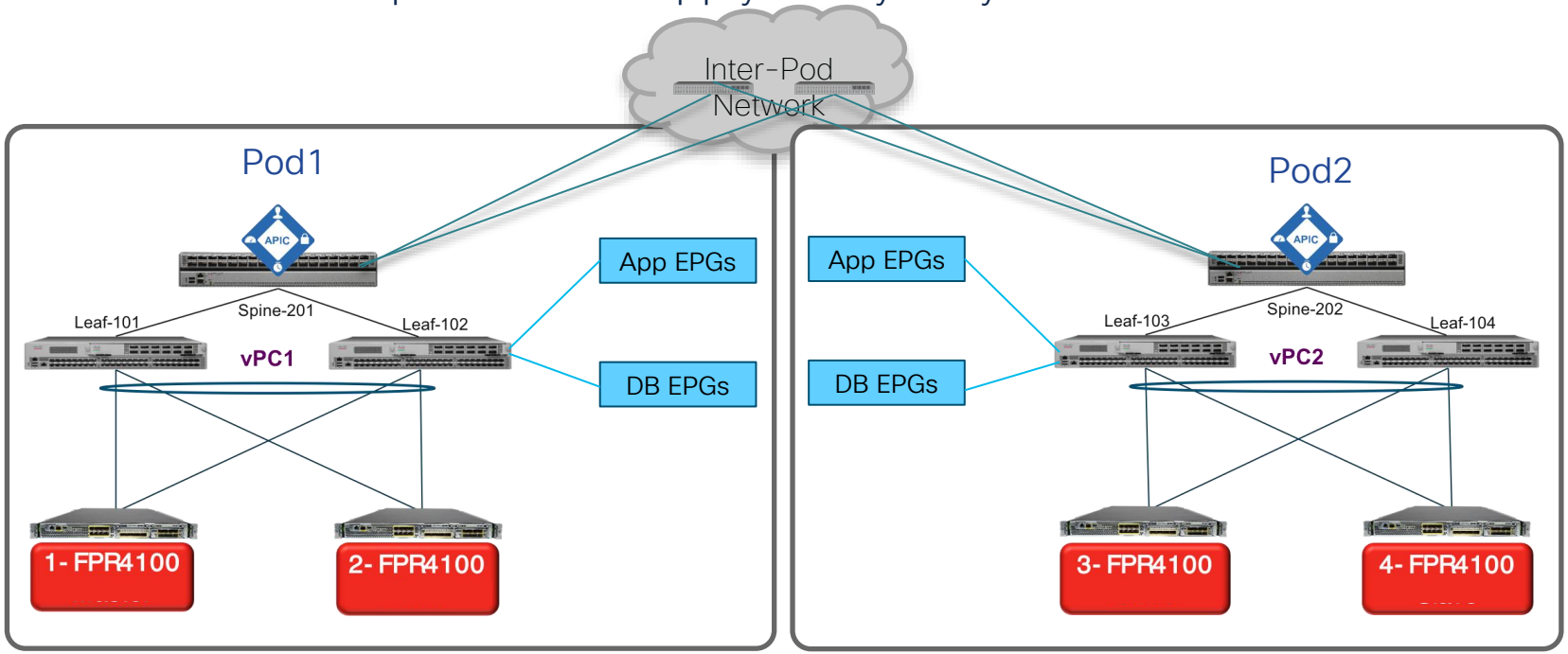
Add a data node

Cancel

Continue

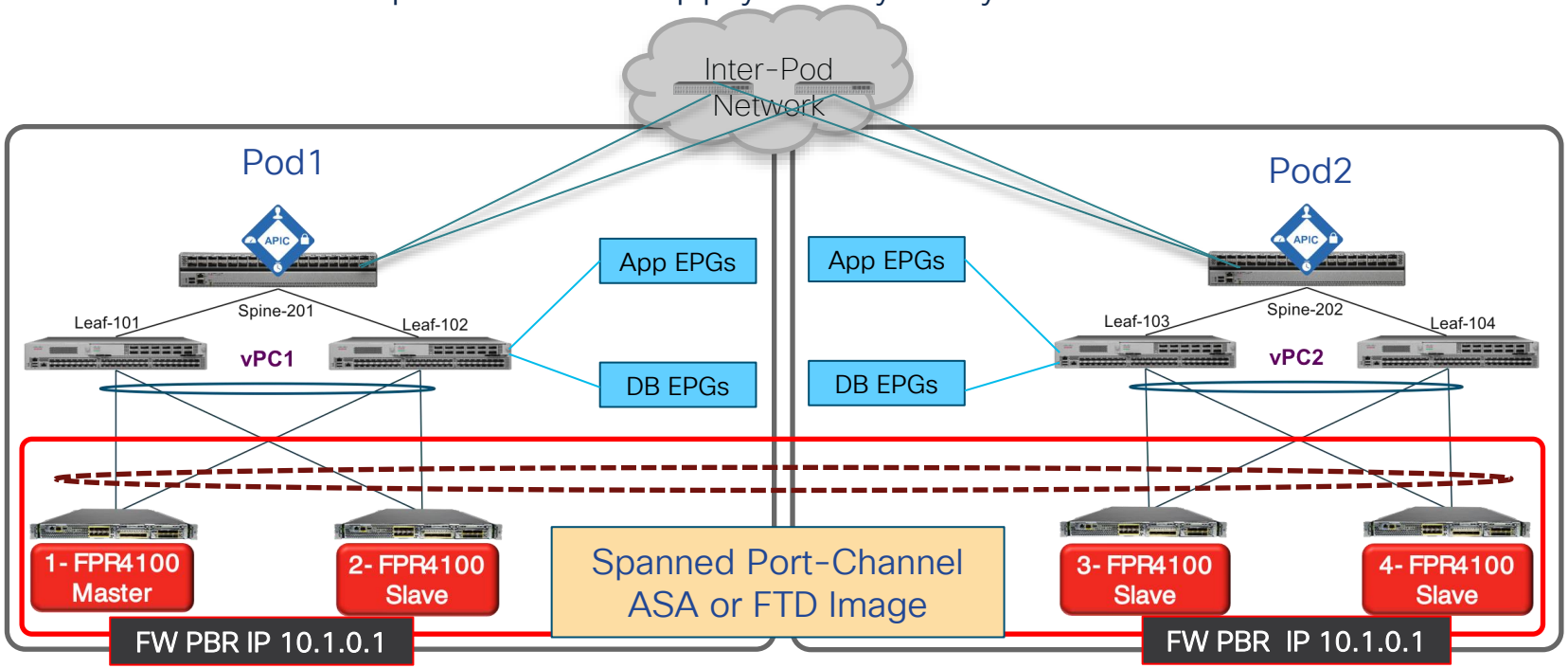
Extend PBR Inter-site Cluster to ACI Multi-Pod

Localize Firewall Inspection and Apply Policy Only to Master



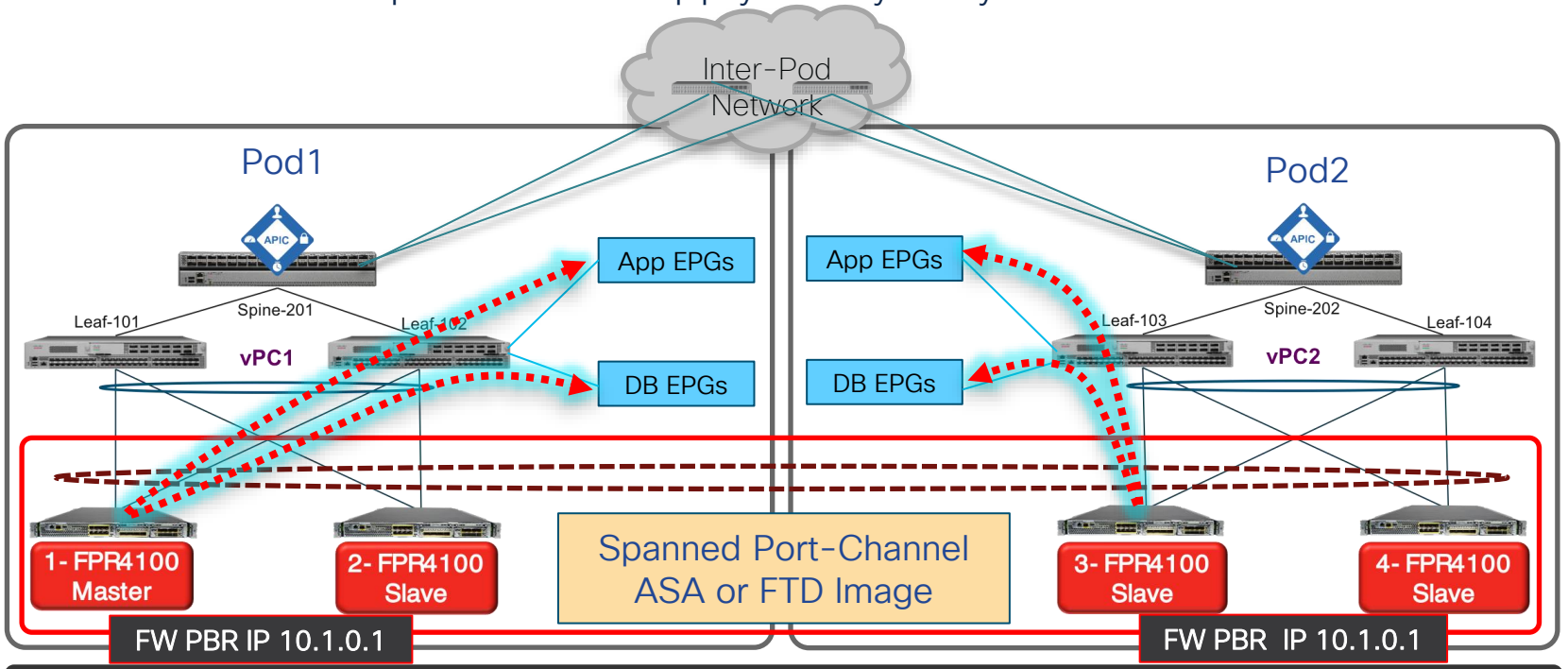
Extend PBR Inter-site Cluster to ACI Multi-Pod

Localize Firewall Inspection and Apply Policy Only to Master



Extend PBR Inter-site Cluster to ACI Multi-Pod

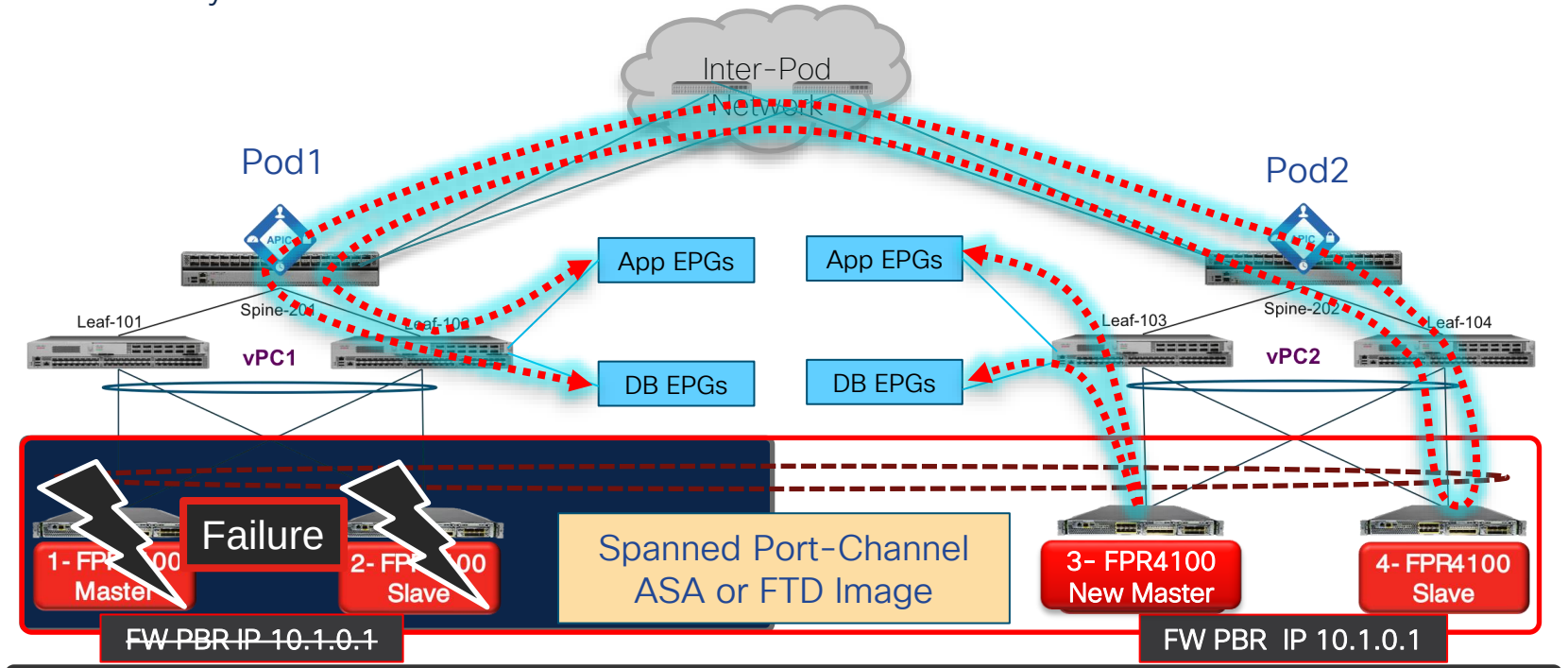
Localize Firewall Inspection and Apply Policy Only to Master



ACI fabric tracks 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.

Firepower Cluster Resiliency

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.

DEMO

Dynamic Attributes

The Problem Statement

- How to build a policy based on intent instead of static IPs ?
- How to reduce changes on enforcement point?
- How to build a policy with cross security Domain ?

FTD and ASA can leverage SGTs

Action

Block

Time Range

None

Zones | Networks | VLAN Tags | Users | Applications | Ports | URLs | Dynamic Attributes | Inspection | Logging | Comments

Available Attributes

Search by name or value

Security Group Tag

- Employees
- Guests
- Network_Services
- PCI_Servers
- Point_of_Sale_Systems
- Production_Servers
- Production_Users
- Quarantined_Systems

Add to Source

Add to Destination

Selected Source Attributes (1)

Security Group Tags

Developers

Selected Destination Attributes (2)

Security Group Tags

PCI_Servers

Point_of_Sale_Systems

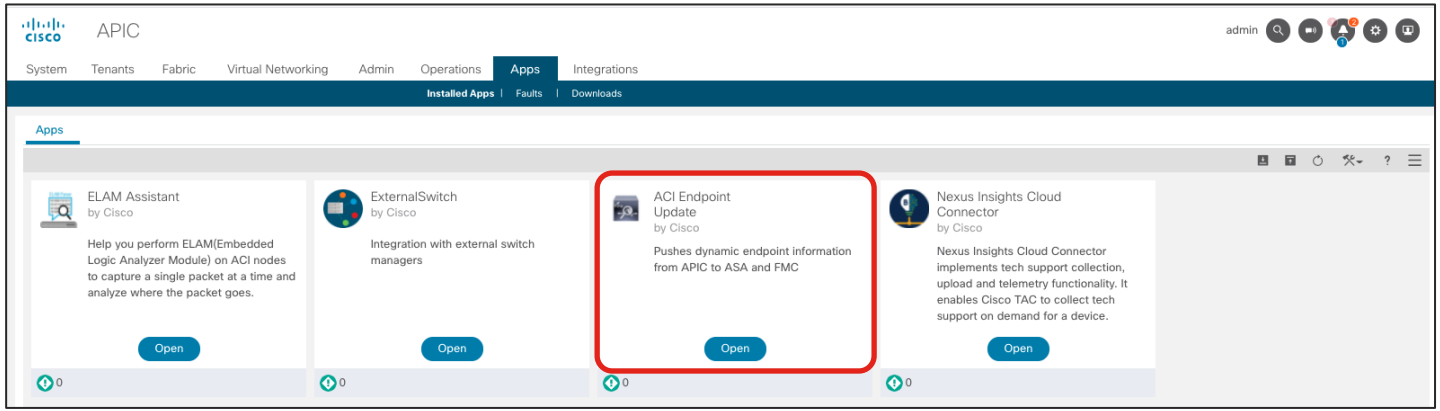
Add a Location IP Address

Add

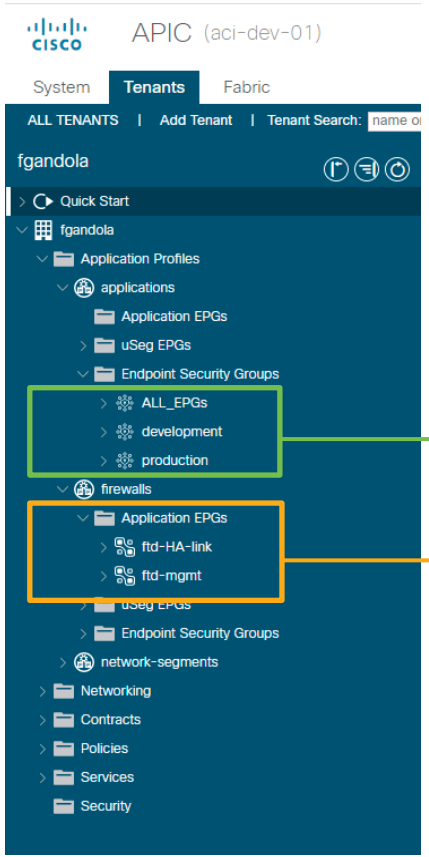
Attributes of the same type (for example, SGT) match the rule if any attribute is matched.
Attributes of different types match the rule only if all attributes are matched. More info

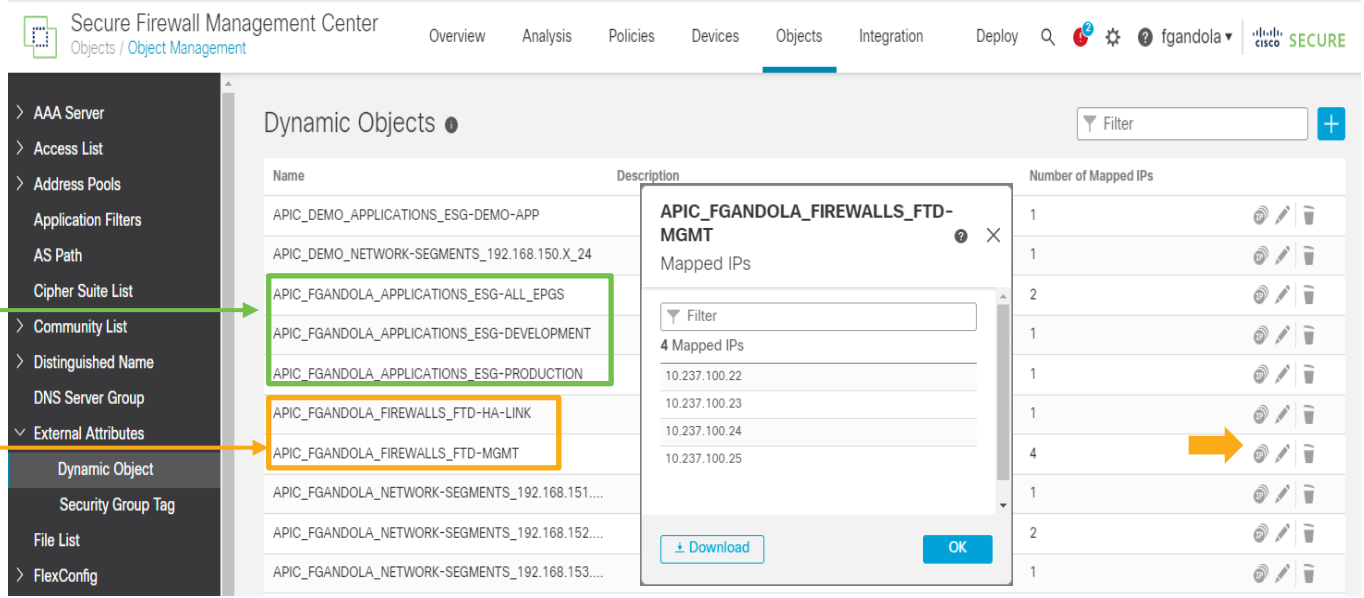
FMC App for APIC – FMC Endpoint Update

- App for APIC enables EPG updates to FMC Network Objects
- FMC is assigned per Tenant or use one FMC for all Tenants
- FTD can learn EPGs/ESGs without using a managed Service Graph
- Update interval, Tenant, Firewall Domains are configurable
- Auto-update/Dynamic Object support for deploying new config

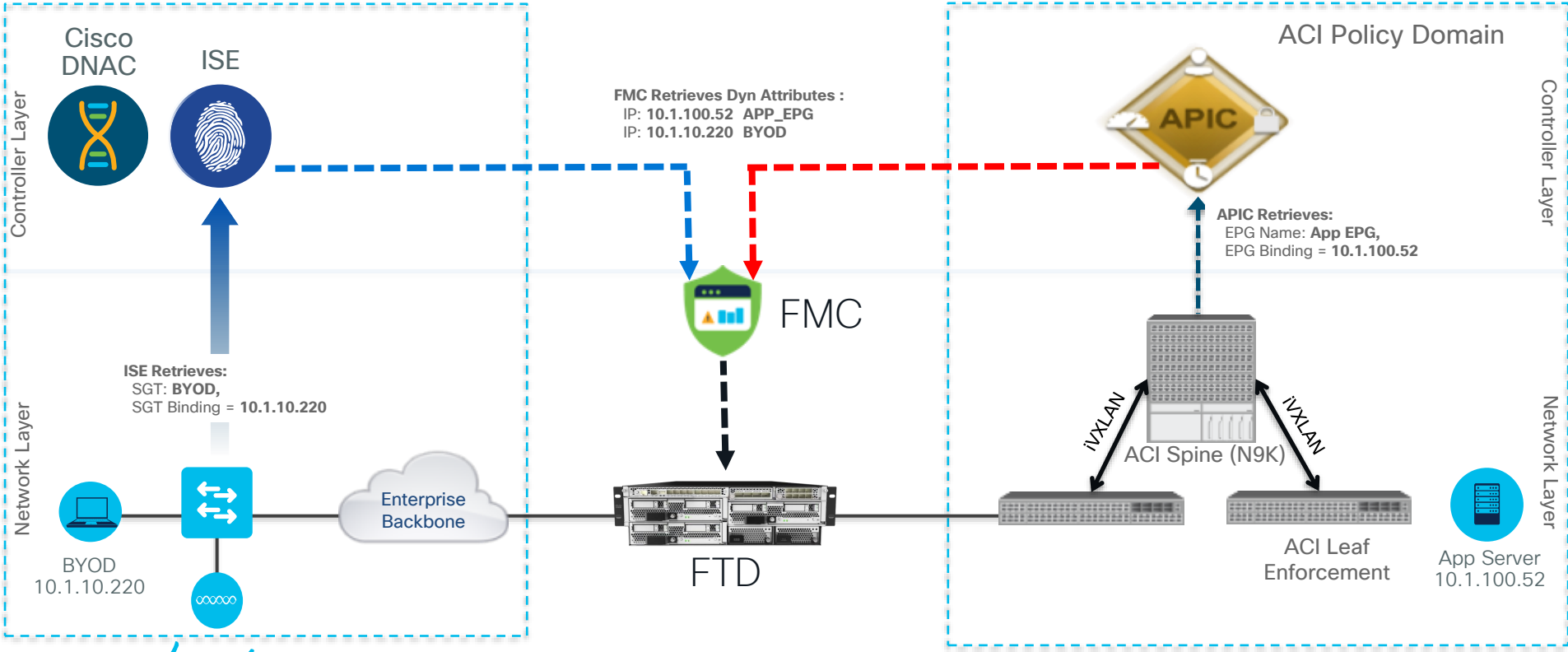


FMC Learns EPGs/ESGs as Dynamic Attributes

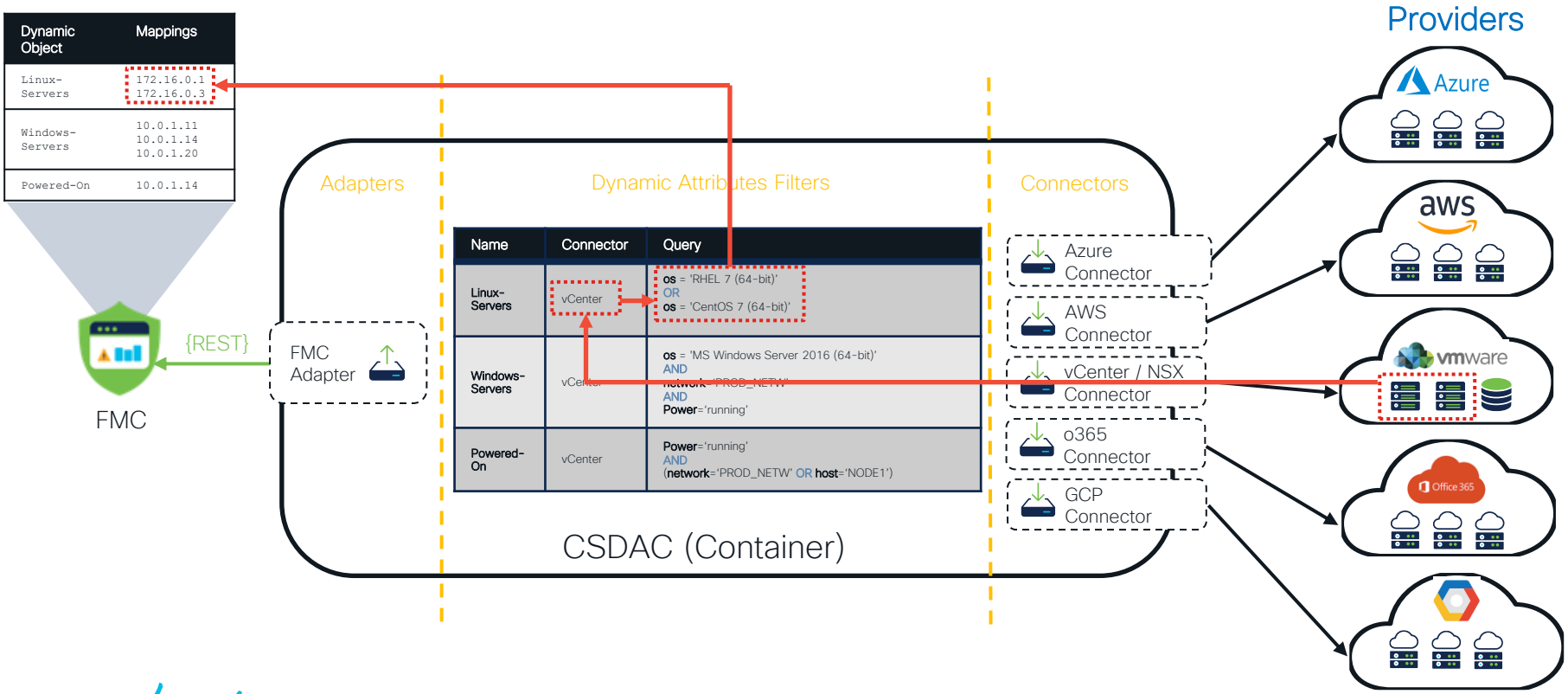




SGT/ACI Firepower Integration



Architecture of the Dynamic Attributes Connector

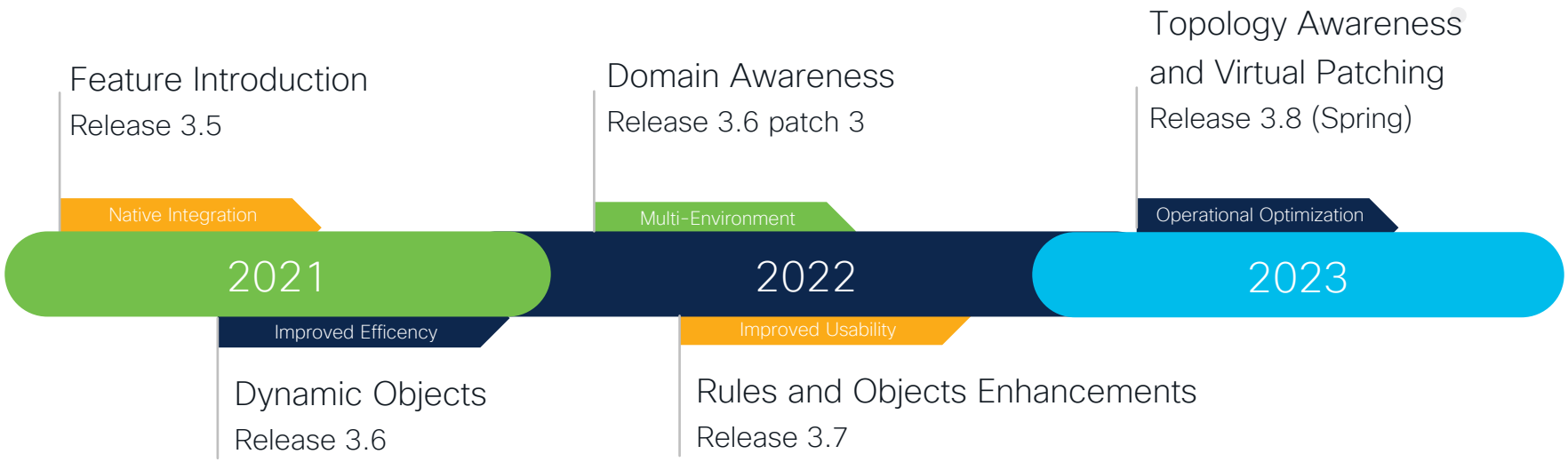


Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
>	Mandatory - Attribute-Based Policy (-)								
v	Default - Attribute-Based Policy (1-9)								
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Pri	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

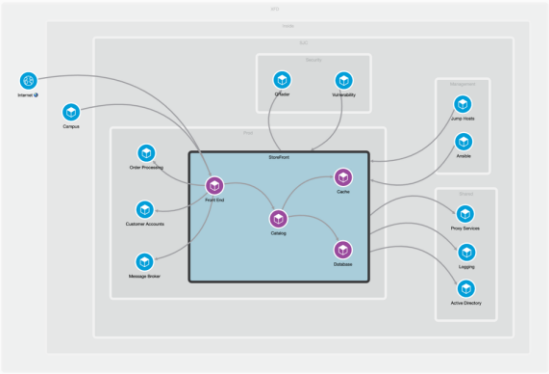
Demo

Secure Firewall integration evolution



Secure Firewall & Secure Workload: better together

Visibility and Enforcement



Cisco Secure Firewall Management Center

- Native Integration
- NSEL Records for ADM Policy
- Access Control Policy (Dynamic Objects)
- FMC Domain Awareness
- Meaningful Dynamic Object names
- Rule Ordering

Use-Cases

VISIBILITY

- Generate policies for agentless workloads across multi-cloud environment
- Workload attribute import with integrations such as IPAM, CMDB, AWS, and more
- User and endpoint context with ISE and AnyConnect integration
- Verify and analyze flows for policy compliance

ENFORCEMENT

- Defense In-Depth
  - Attribute-Based hierarchical policies for agentless workloads
  - Rapid Threat Containment for agent and agentless workloads with FMC Remediation Module
- Policy Lifecycle Automation
- Enforce zero trust microsegmentation policies to applications where agent installation is not feasible

End-to-end protection

North-South

Secure Firewall

Perimeter Protection

- Threat inspection at the data center or cloud edge
- Visibility into Internet, Branch, and Campus

East-West

Secure Firewall
Secure Workload

Zones

- Segment zones within your data center and cloud
- Supplementary coverage for workloads with or without agents

Microsegmentation

Secure Workload

Zero Trust

- Zero trust microsegmentation enforcement at the workload
- Automated policy discovery and compliance

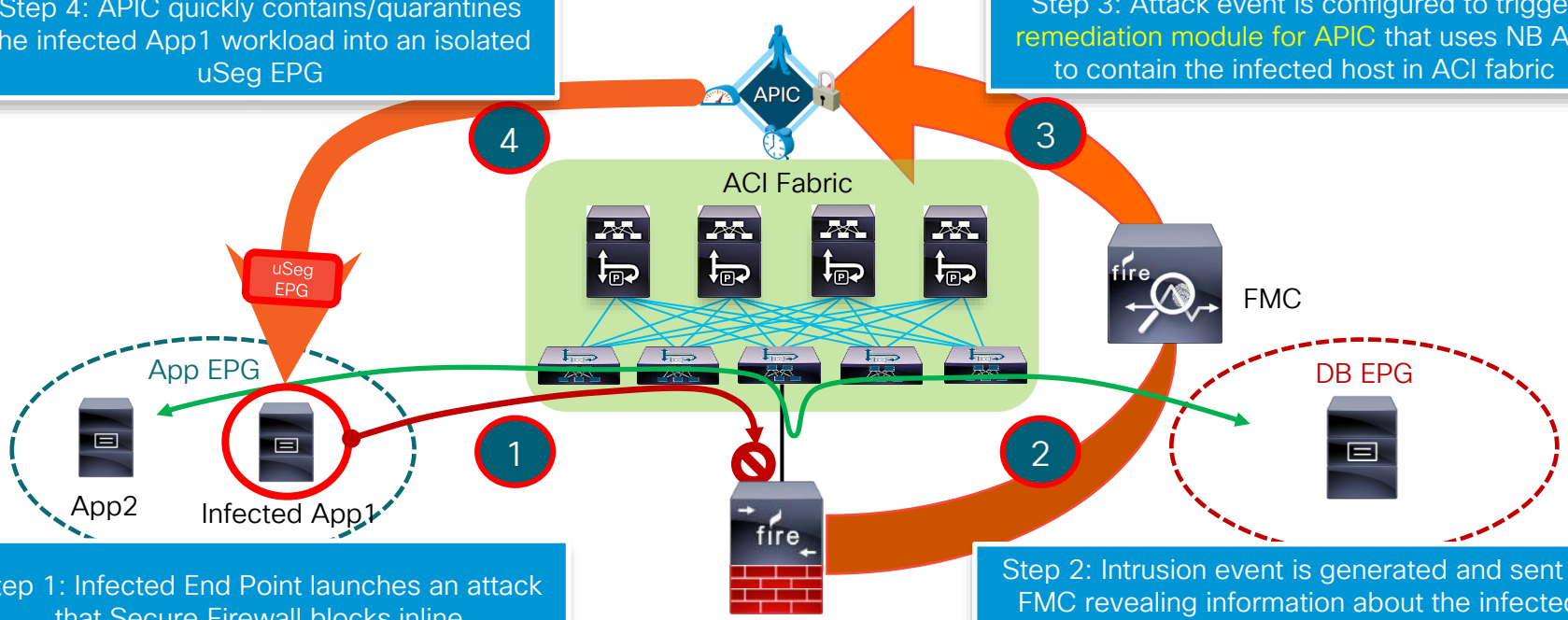
Closer to application

Remediation Module

FMC to APIC Rapid Threat Containment

Step 4: APIC quickly contains/quarantines the infected App1 workload into an isolated uSeg EPG

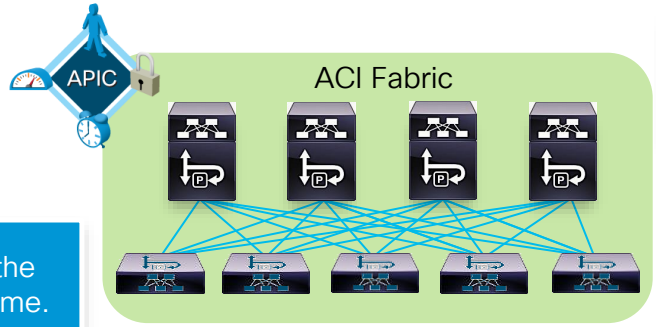
Step 3: Attack event is configured to trigger remediation module for APIC that uses NB API to contain the infected host in ACI fabric



Step 1: Infected End Point launches an attack that Secure Firewall blocks inline

Step 2: Intrusion event is generated and sent to FMC revealing information about the infected host

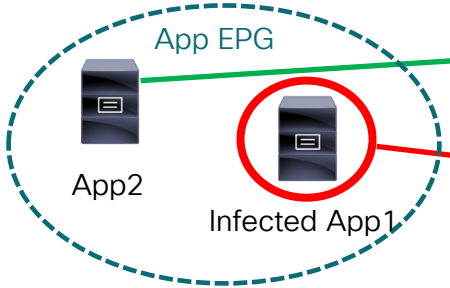
Contract Based Rapid Threat Containment

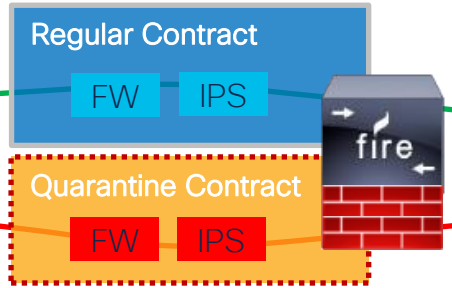


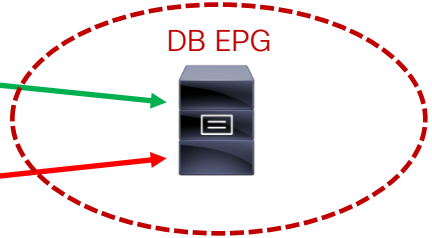
Remediation module for APIC triggers switchover to **quarantine contract**

FMC

APIC attaches **quarantine contract** to the infected End Point. EPG remains the same.







Quarantine contract imposes more thorough FW and IPS policy inspections to closely monitor infected endpoint.

Remediation Module in FMC

Secure Firewall Management Center
Policies / Actions / Modules

Overview | Analysis | Policies | Devices | Objects | Integration

Installed Remediation Modules

Module Name	Version	Description
APIC/Secure Firewall Remediation Module	3.0.1	APIC/Secure Firewall Remediation Module
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Adaptive Network Control (ANC) Policy Assignment	1.0	Apply or clear an ANC policy for the endpoint at the involved IP addresses
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value

Install a new module

Choose File No file chosen

Install

Secure Firewall Management Center

Policies / Actions / Module Detail

Overview | Analysis | Policies | Devices | Objects | Integration

Details for module APIC/Secure Firewall Remediation Module

Name	APIC/Secure Firewall Remediation Module
Version	3.0.1
Description	APIC/Secure Firewall Remediation Module

Configured Instances

Name	Description
Steve_Fabric	APIC owned by Steve

Available Remediation Types forAPIC/Secure Firewall Remediation Module (Select an Instance to Configure a Remediation)

Name
Quarantine the destination End Point on APIC
Quarantine the source End Point on APIC

Configure the APIC details in module

Edit Instance

Instance Name	Steve_Fabric
Module	APIC/Secure Firewall Remediation Module(v3.0.1)
Description	APIC owned by Steve
APIC server username*	fmcuser
APIC server password*	•••••••••
Retype to confirm	•••••••••
APIC cluster instance 1 IP*	10.237.97.182
APIC cluster instance 2 IP	
APIC cluster instance 3 IP	
APIC cluster instance 4 IP	
APIC cluster instance 5 IP	
IP addresses NOT to quarantine (a list of strings)	
Management Contract Name	mgmt_remediation_contract
Management EPG Name	mgmtEPG
L3Out Name	
L3Out EPG Name	
Audit-only	On / Off

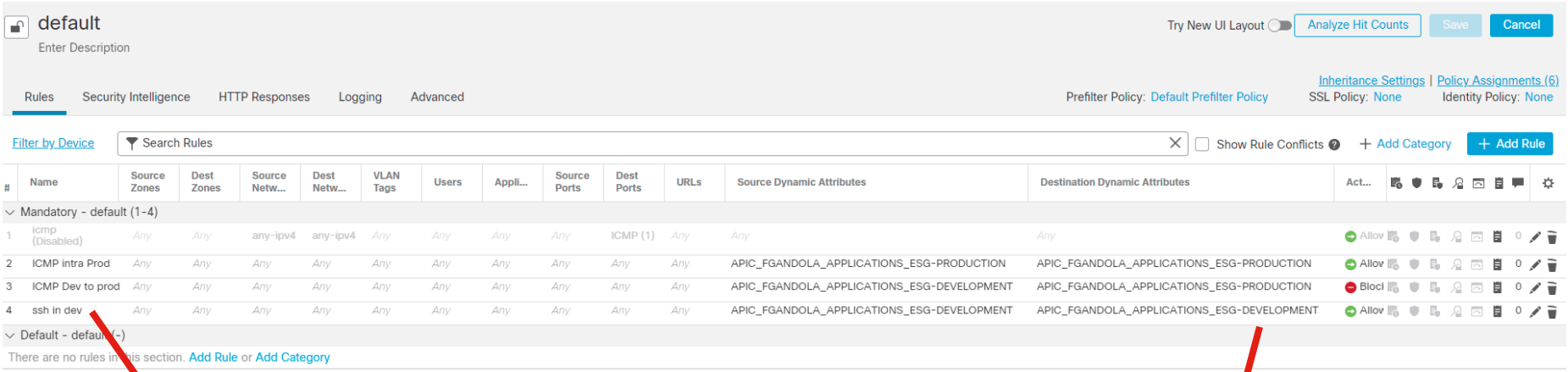
Cancel Save

Configured Remediations

Remediation Name	Remediation Type	Description	
Fab_qurantine_dest	Quarantine the destination End Point on APIC	test for CL22	

Add a new remediation of type Quarantine the destination End F Add

Rule



Correlation Rule

Policy Management | Rule Management | Allow List | Traffic Profiles

Rule Information

Rule Name: test for CL22

Rule Description: trigger in ssh session in dev ESG

Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at any point of the connection and it meets the following conditions:

Add condition | Add complex condition

AND
- Access Control Policy is default
- Access Control Rule Name contains the string ssh

Select the type of event for this rule

If an intrusion event occurs

- a VPN troubleshoot event occurs
- an intrusion event occurs
- a discovery event occurs
- user activity is detected
- a host input event occurs
- a connection event occurs
- a traffic profile changes
- a Malware event occurs

Policy Management | Rule Management | Allow List | Traffic Profiles

Correlation Policy Information

Policy Name: fab-test-remediation

Policy Description: trigger on SSH

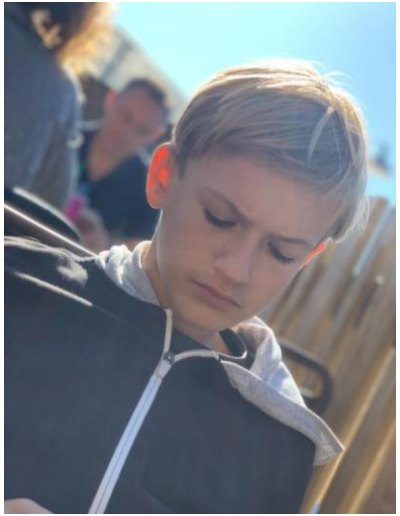
Default Priority: None

Policy Rules

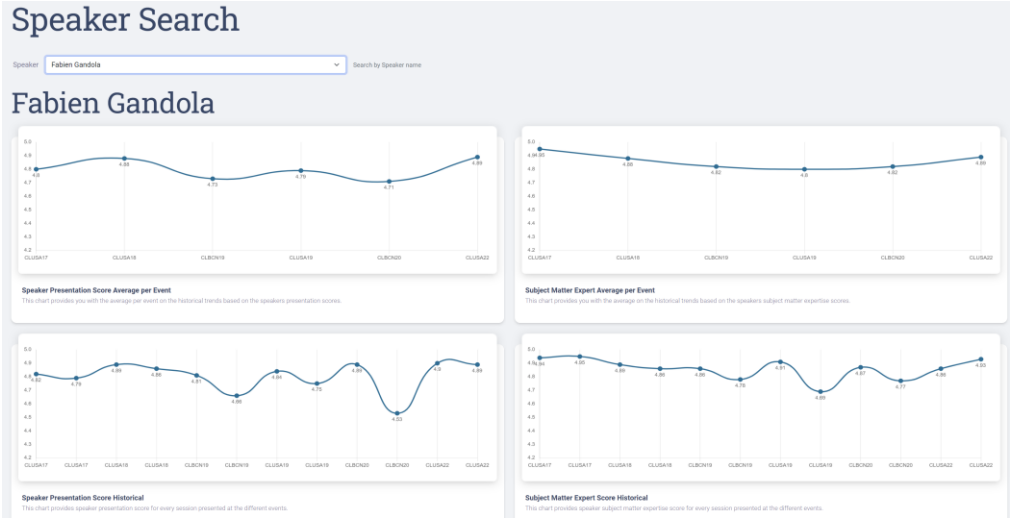
Rule	Responses
test for CL22 trigger in ssh session in dev ESG	Fab_qurantine_dest (Remediation)

Summary

The most boring part of Cisco Live



Is that a 4 or 5 ?



You are accepted – what to do?

- First time Speakers or Speakers below 4.2 score are strongly encouraged to attend the Speaker Training

I DO VALUE YOUR COMMENTS

« The speaker BUTCHERED english ! »

« Could you teach English to my husband speaking with your sexy accent ? »

« Best session of the week but it is only the first day…»

« They should create a 6th star for you »

« The chairs ain't suitable for long session. »

« Room temperature would have been perfect … if i was a PINGUIN !»

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.

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.

The bridge to possible

Thank you

cisco Live!

CISCO Live!

ALL IN