cisco Live!

Let's go

The bridge to possible

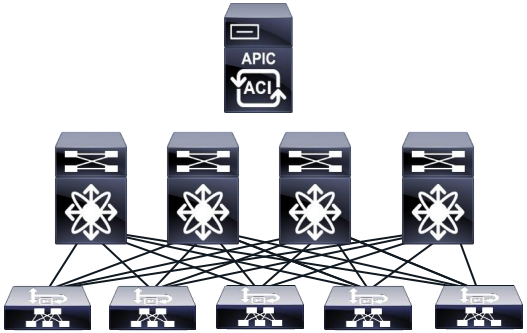
Cisco Secure Firewall in ACI

L4-L7 Integration

Fabien Gandola, EMEA Security TSA

Opening Statement

ACI IS NOT A FIREWALL



≠

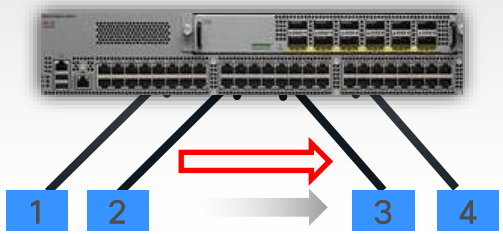
Does ACI help with Security ?

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

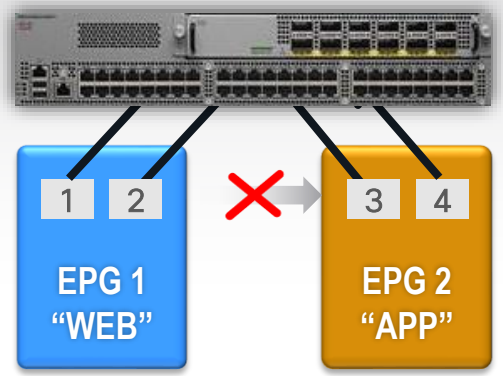
(Traditional DC Switch)



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

What should you expect … and not expect

- No Deep dive in ACI

The bridge to possible

At 3PM today in room A10

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

Minako Higuchi, Technical Marketing Engineer, Cloud Networking Business Group

The bridge to possible

At 9 AM tomorrow in room A5

Cisco ACI: the Foundation of an Internal Private Cloud

BRKDCN-2984

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

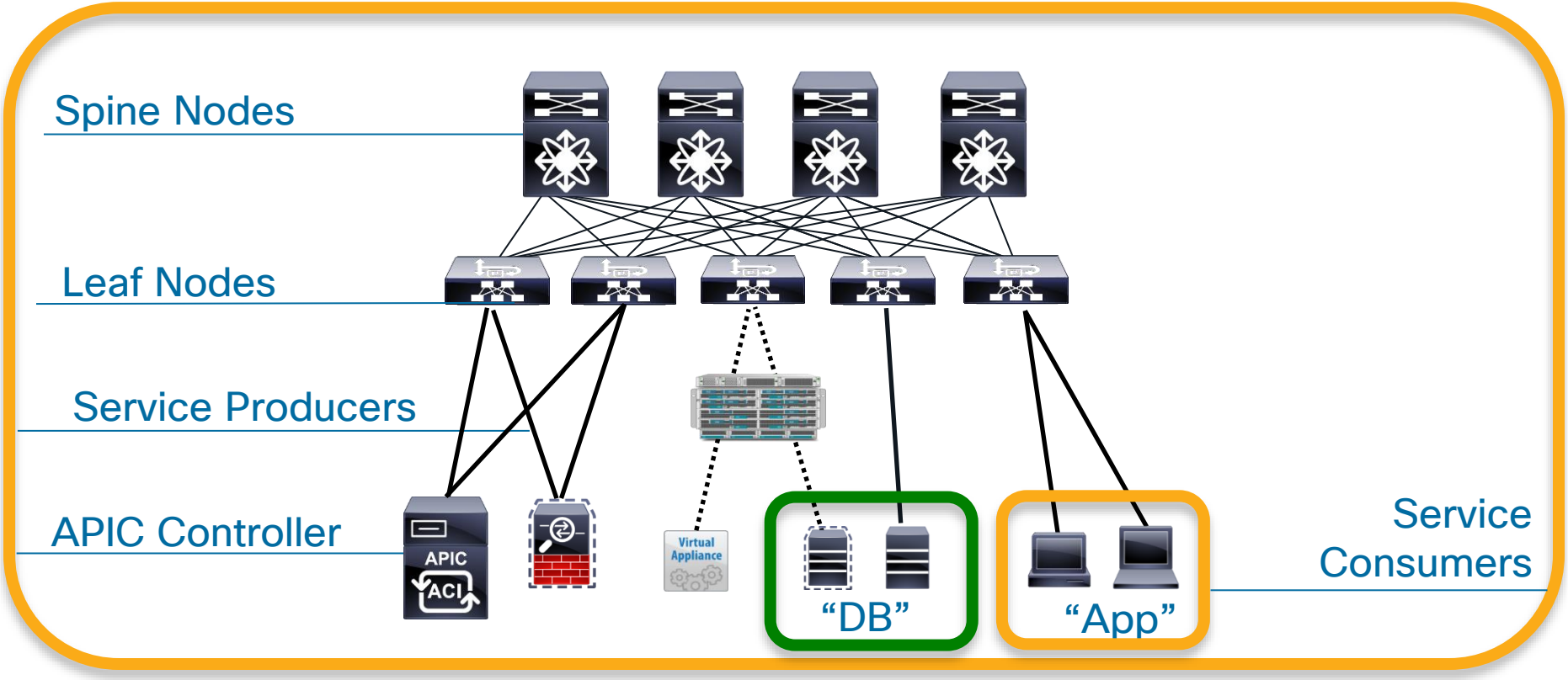
- ACI Building Blocks *(super quick)*
- FTD Improvements for the DC
- FTD Insertion *(Mostly PBR L3)*
- FTD added value
  - Clustering
  - CSDAC and Dynamic Group
  - FTD + Cisco Secure Workload (Tetration)
  - Remediation module in FMC *(super quick)*

About Me

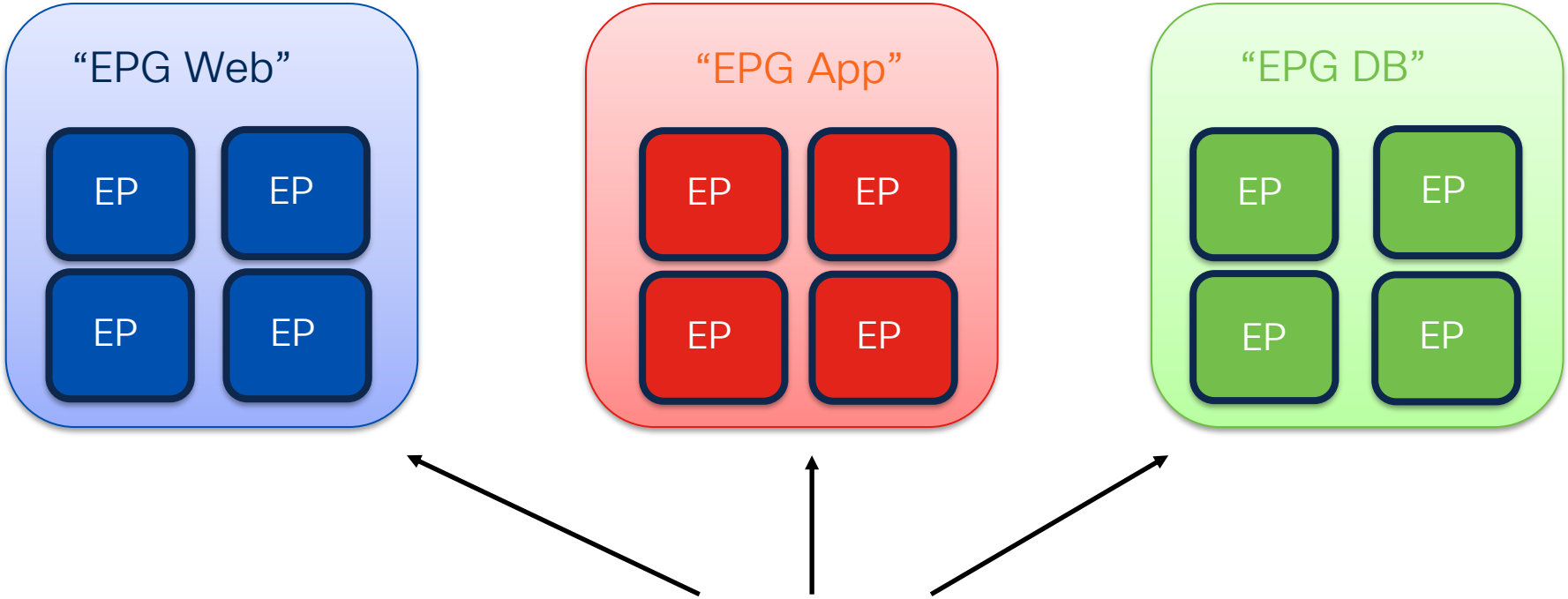
Fabien Gandola
fgandola@cisco.com
TSA Cyber Security EMEA
23 years in Cisco

Shortest introduction to ACI ever...

ACI Devices Role

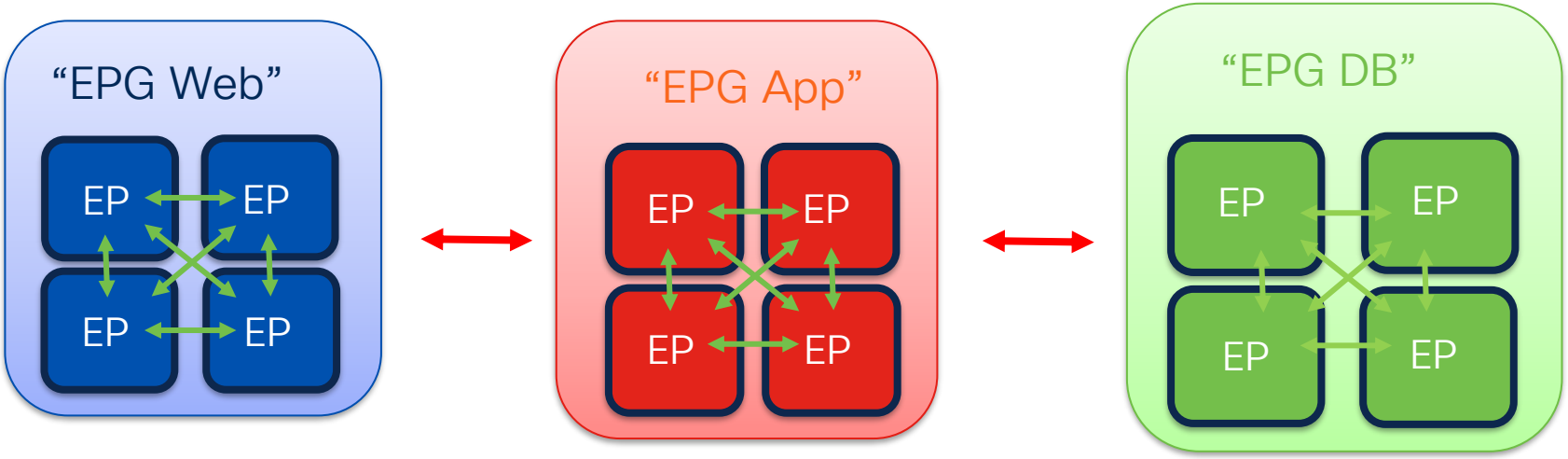


End Point Group



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

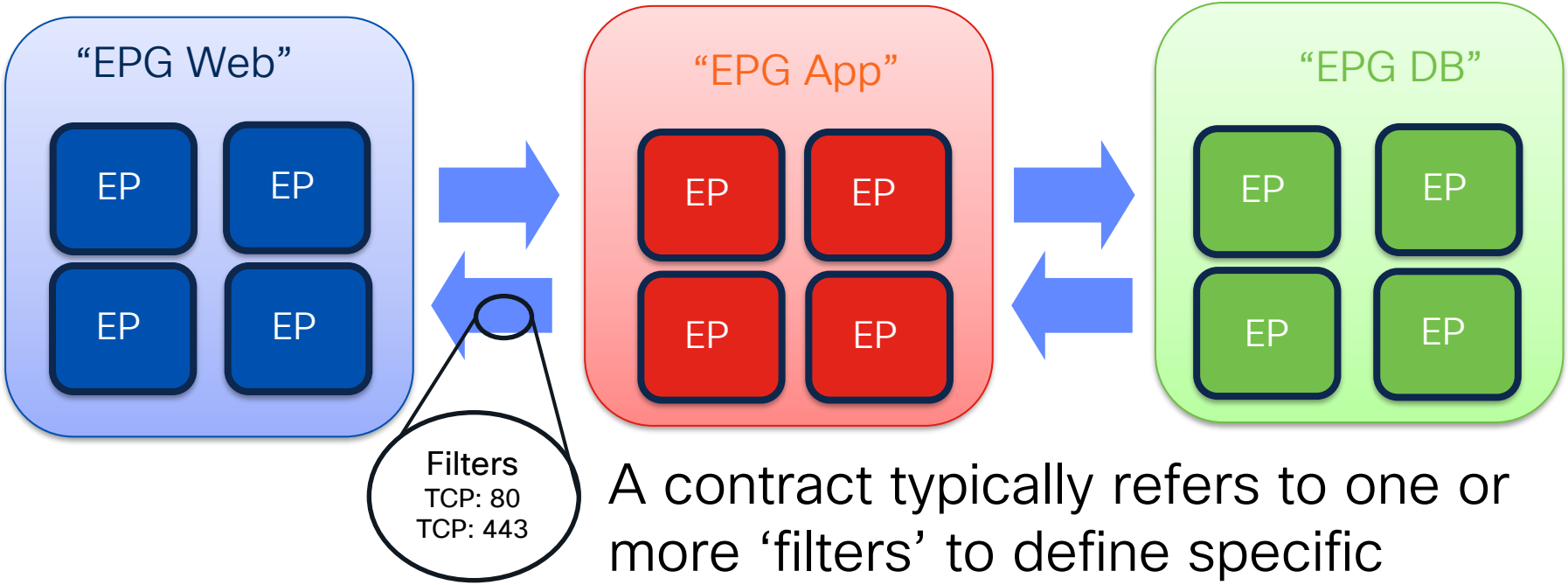
Endpoint Groups Communications



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

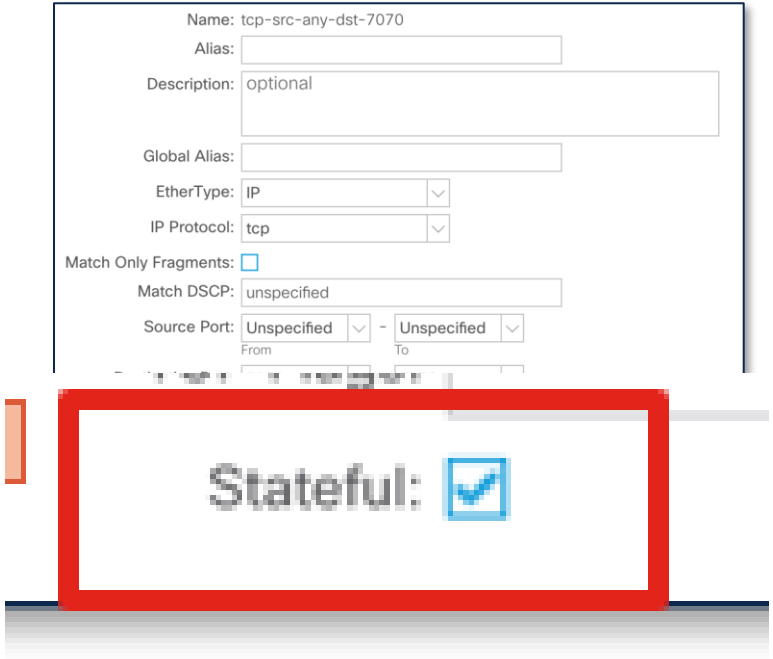
Communication between Endpoint groups is, by default, not permitted.

Contract : Kind of reflexive “Stateless” ACLs



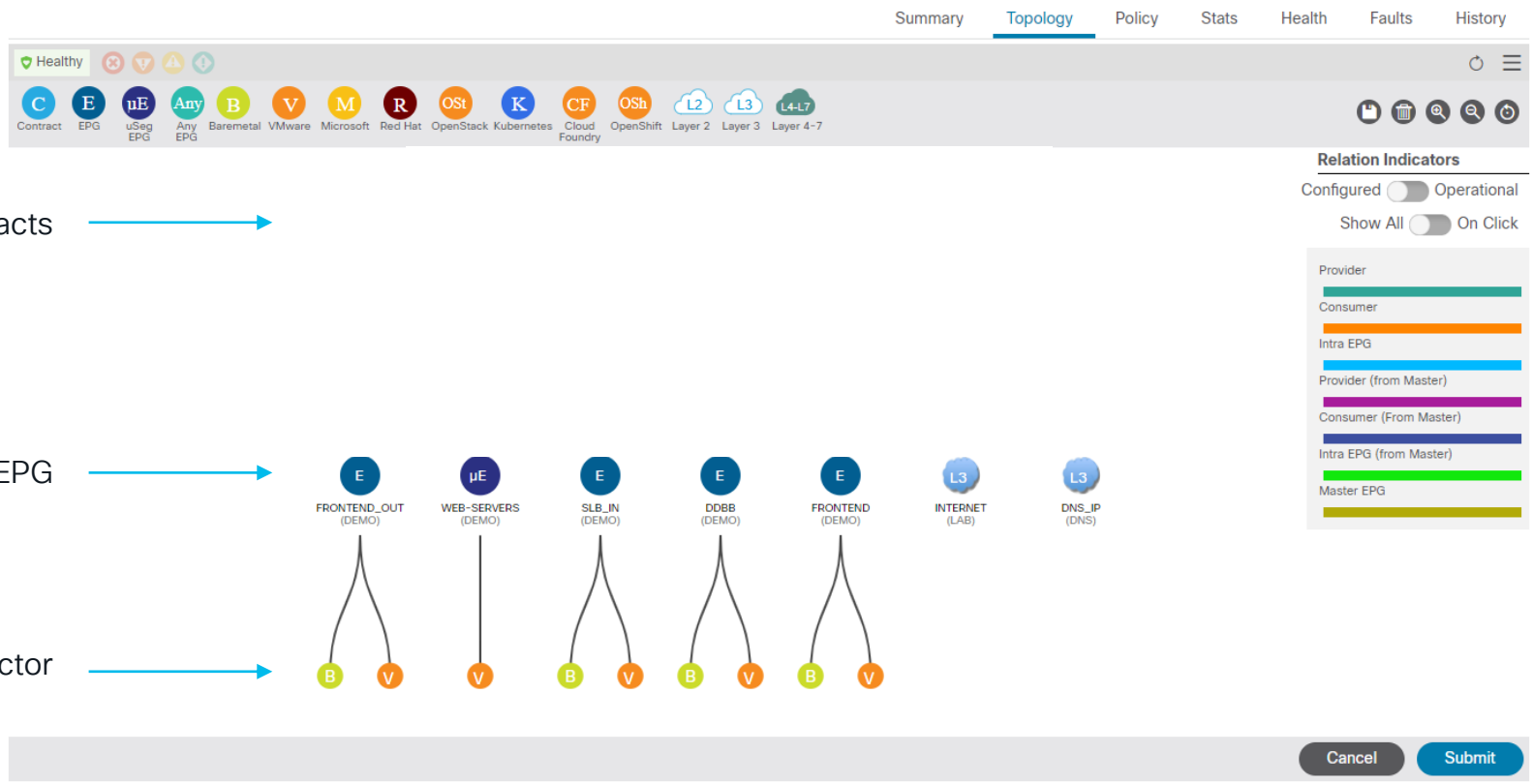
A contract typically refers to one or more ‘filters’ to define specific protocols & ports allowed between EPGs.

Did you say Stateless ?



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

Application policy with contract



Contracts

EPG

Form Factor

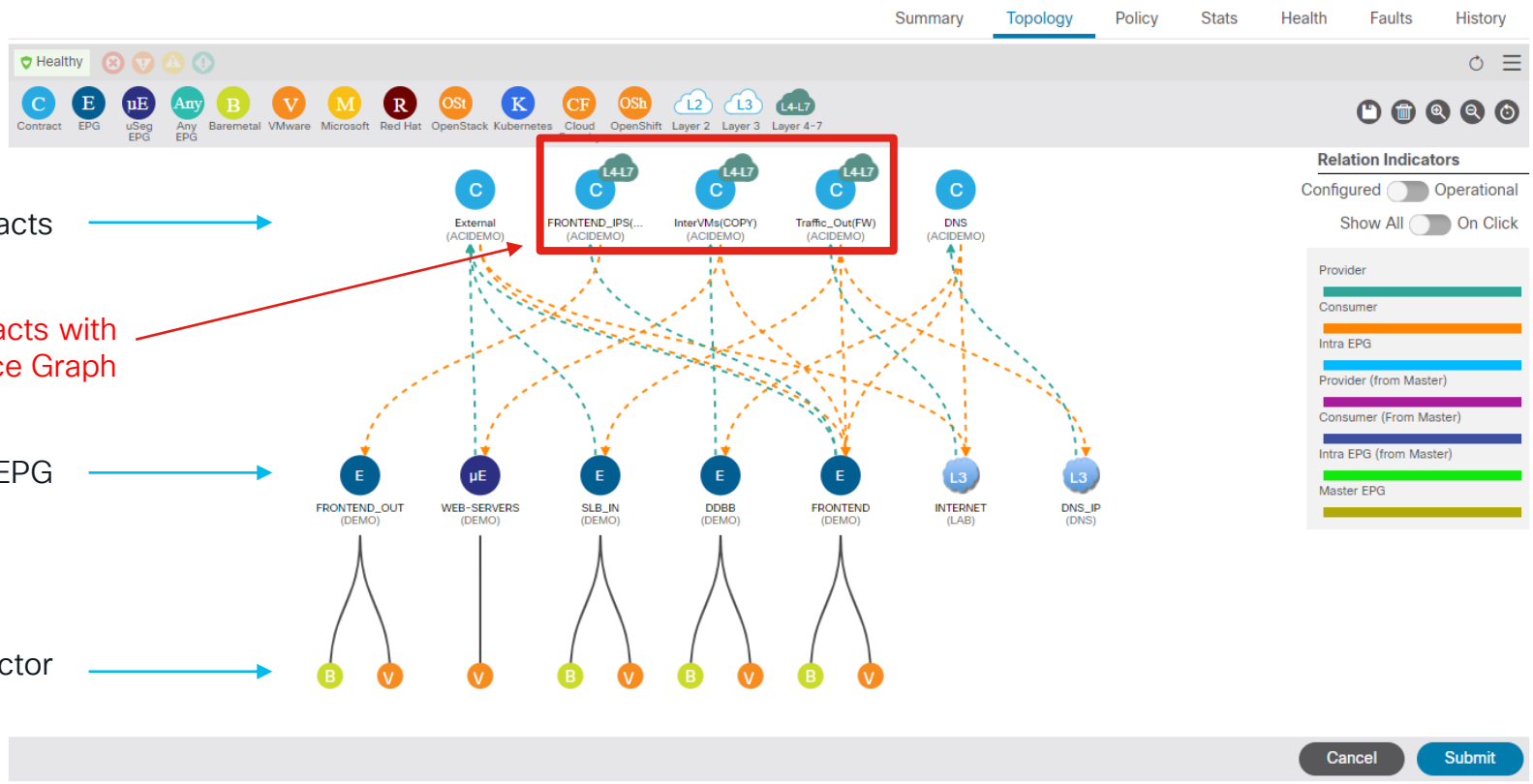
Application Policy with Contract

Contracts

Contracts with Service Graph

EPG

Form Factor



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

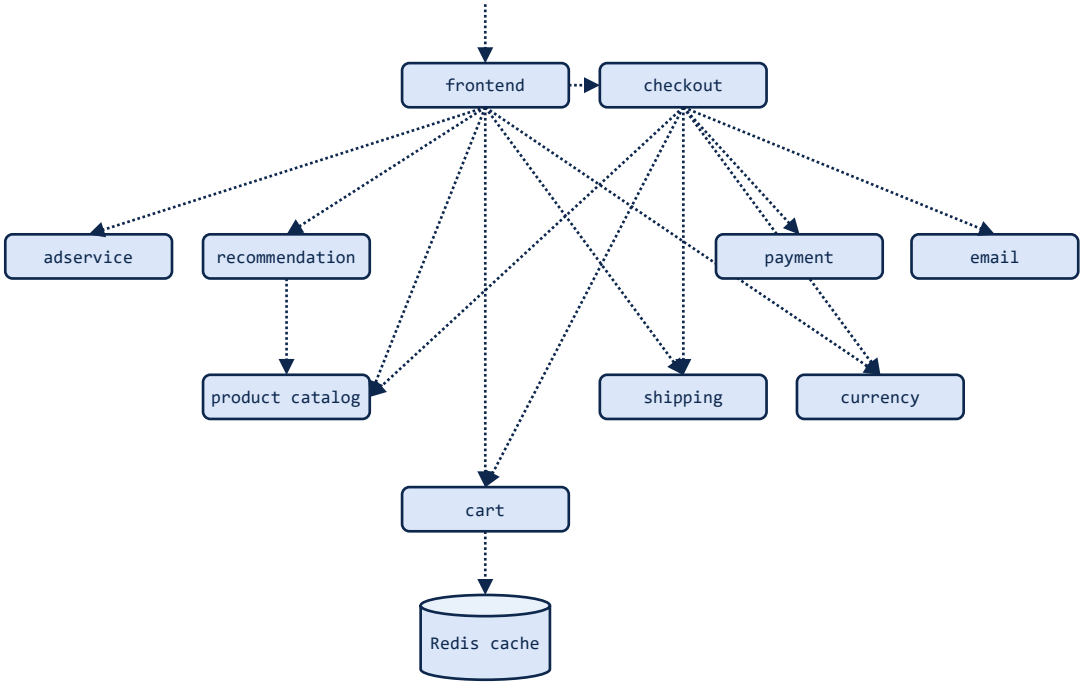
- fgandola
  - fab_ubuntu_01
  - fab_ubuntu_02
  - fab_ubuntu_03
  - FMC72.uktme.cisco.com
  - ftdv-03-OLD.uktme.cisco.com
  - ftdv-03.uktme.cisco.com
  - ftdv-04-OLD.uktme.cisco.com

Tags

Assigned Tag	Category
tn-fgandola:applications:production	Function

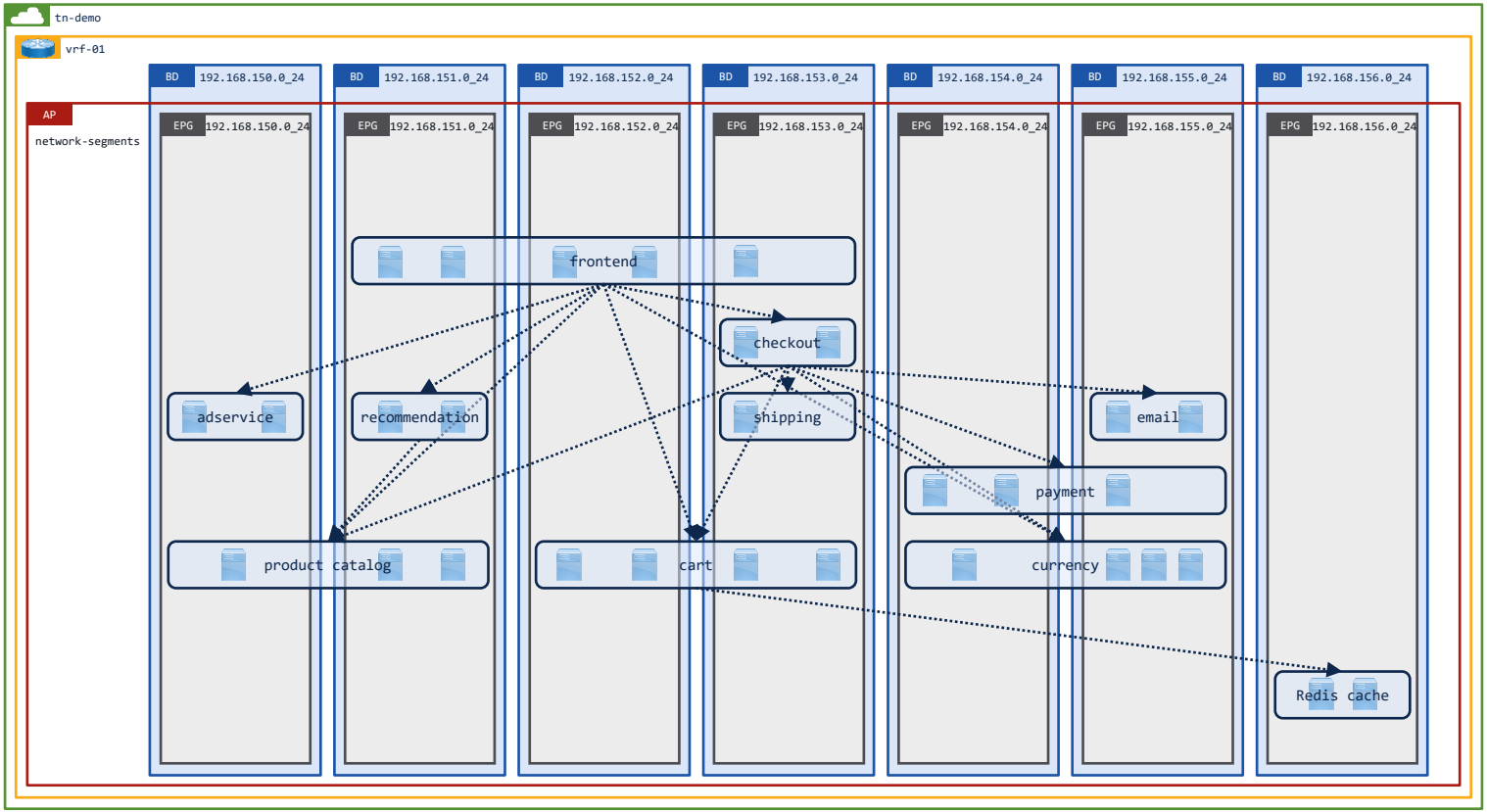
Online Boutique

https://github.com/GoogleCloudPlatform/microservices-demo

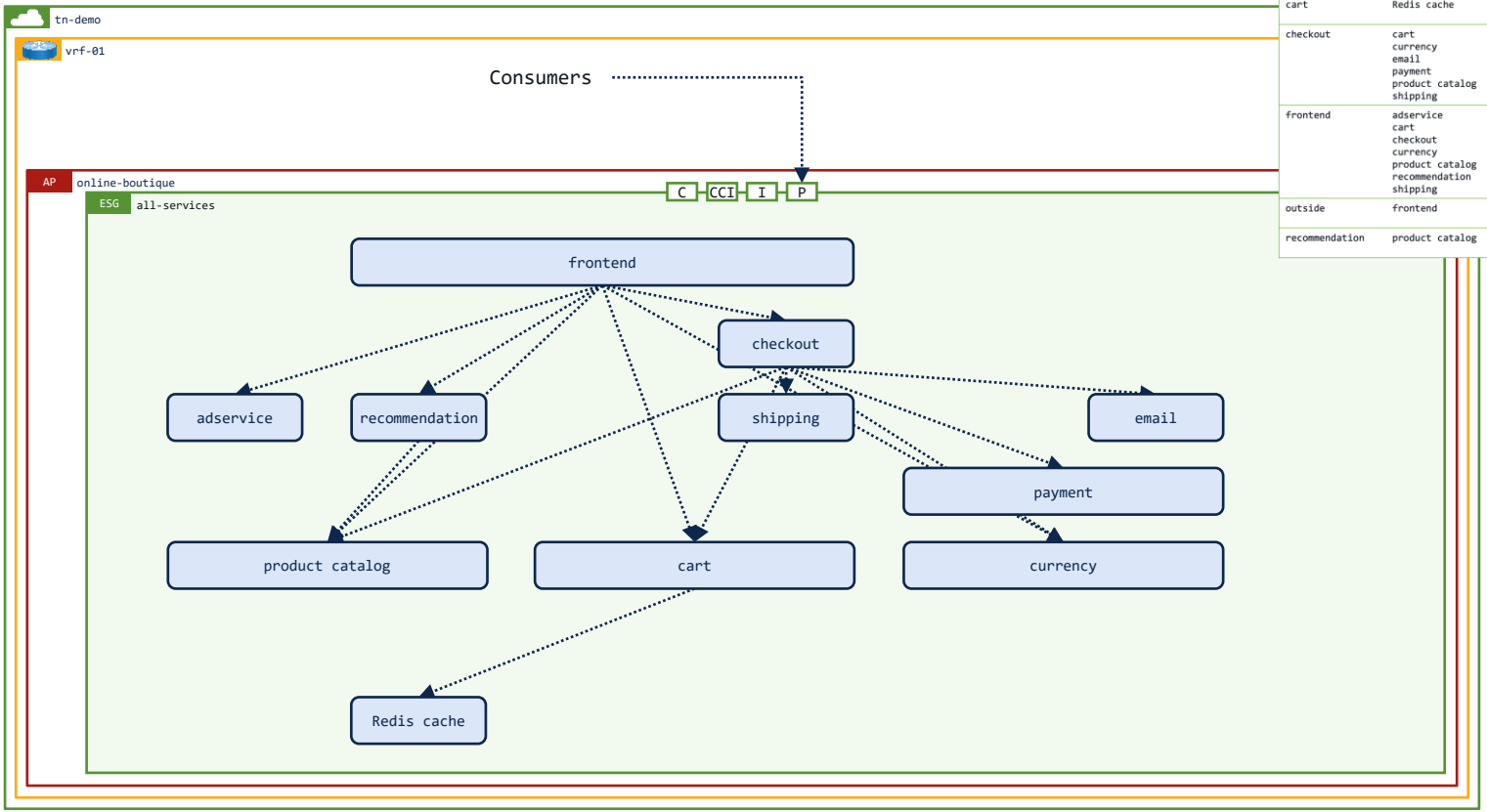


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP 5050 TCP 7000 TCP 3550 TCP 8080 TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Where is our application running...?



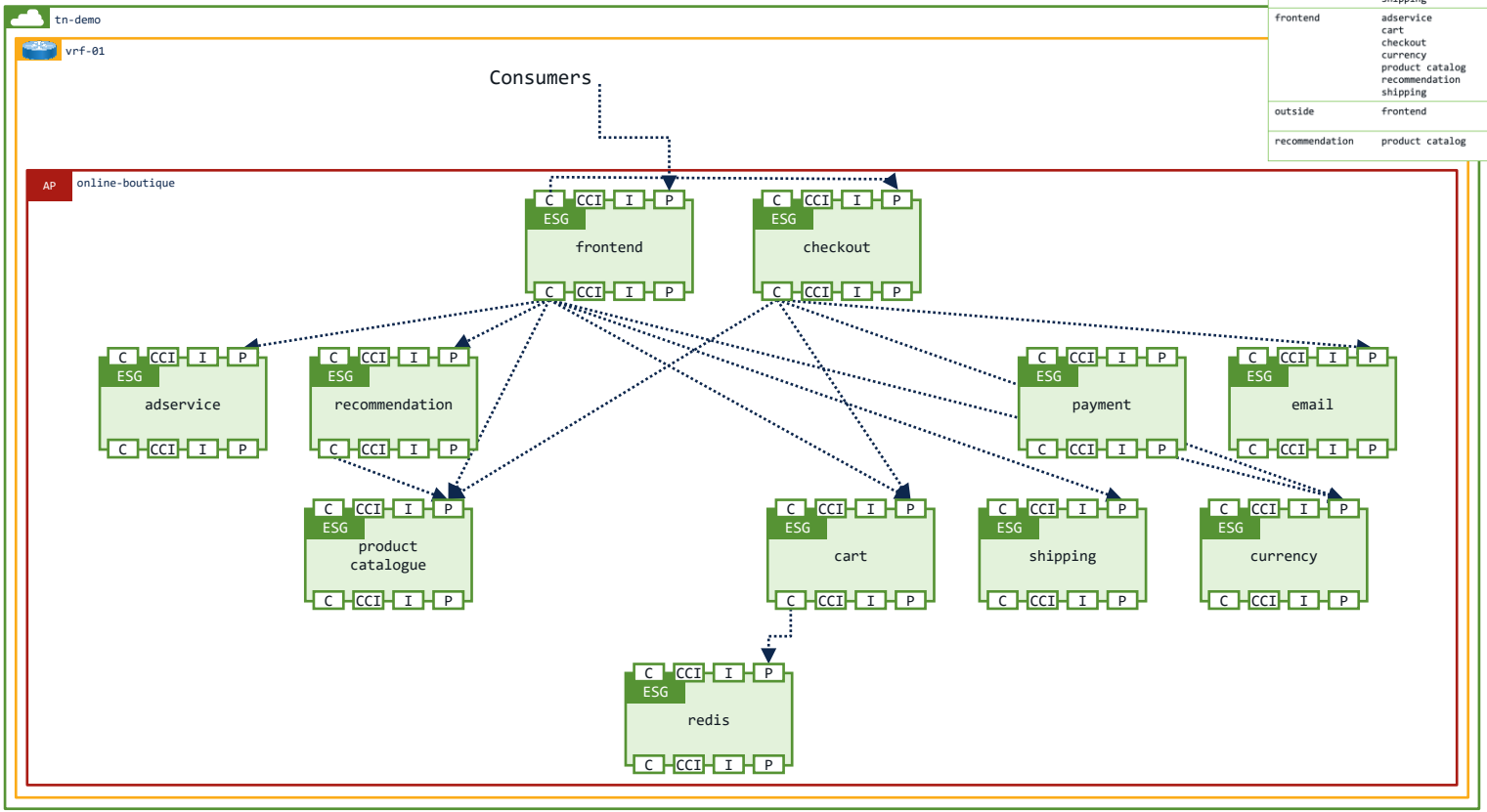
Application tiers across subnets



Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Application tiers across subnets

Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 5000 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP 5050 TCP 7000 TCP 3550 TCP 8080 TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550



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

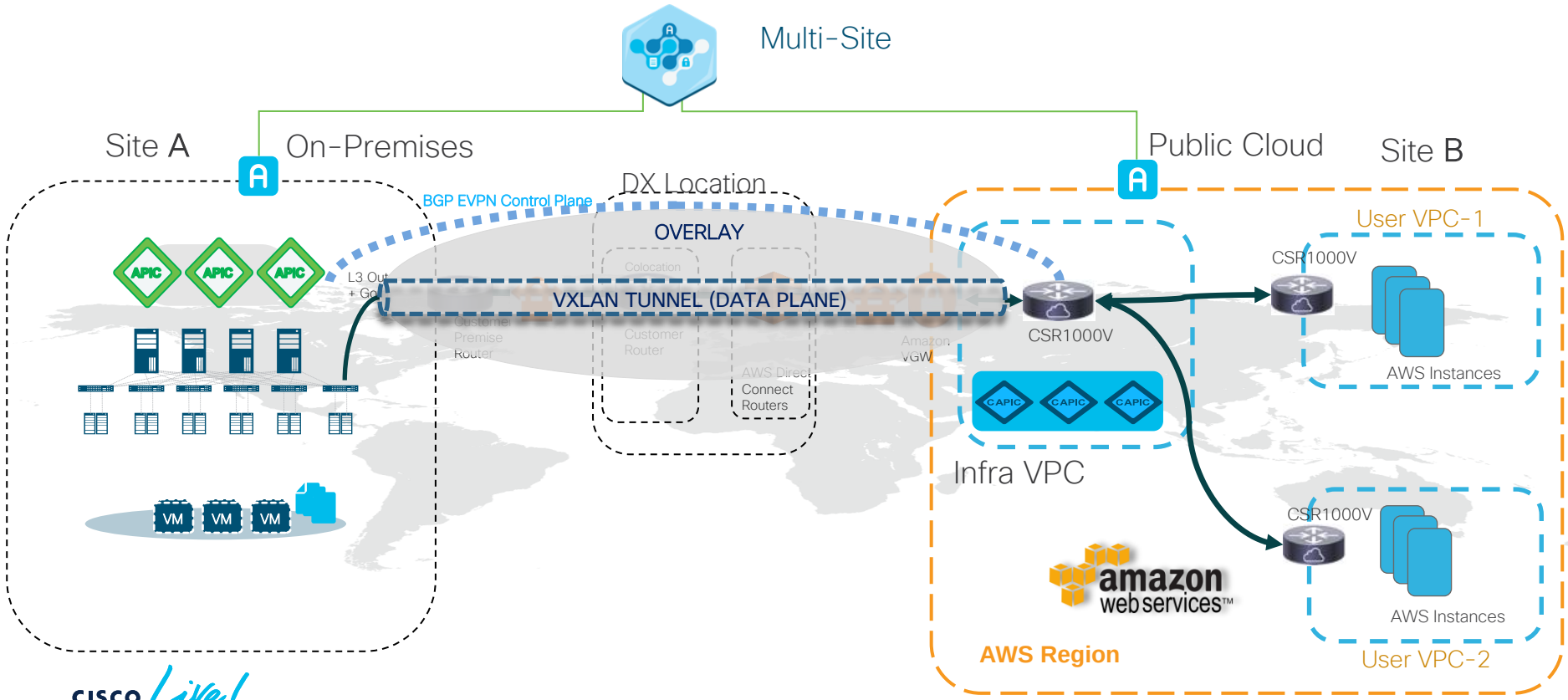
aws

Azure

Alibaba Cloud

ACI Anywhere: On-Prem Connectivity To AWS

VPC With Direct Connect + VPN



FTD Converged Image

ASA

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

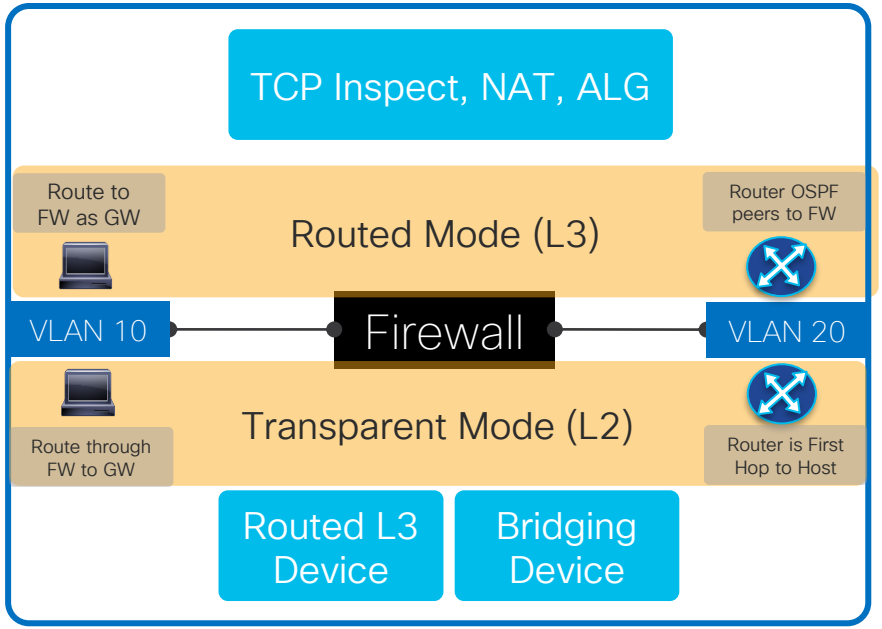
FirePOWER

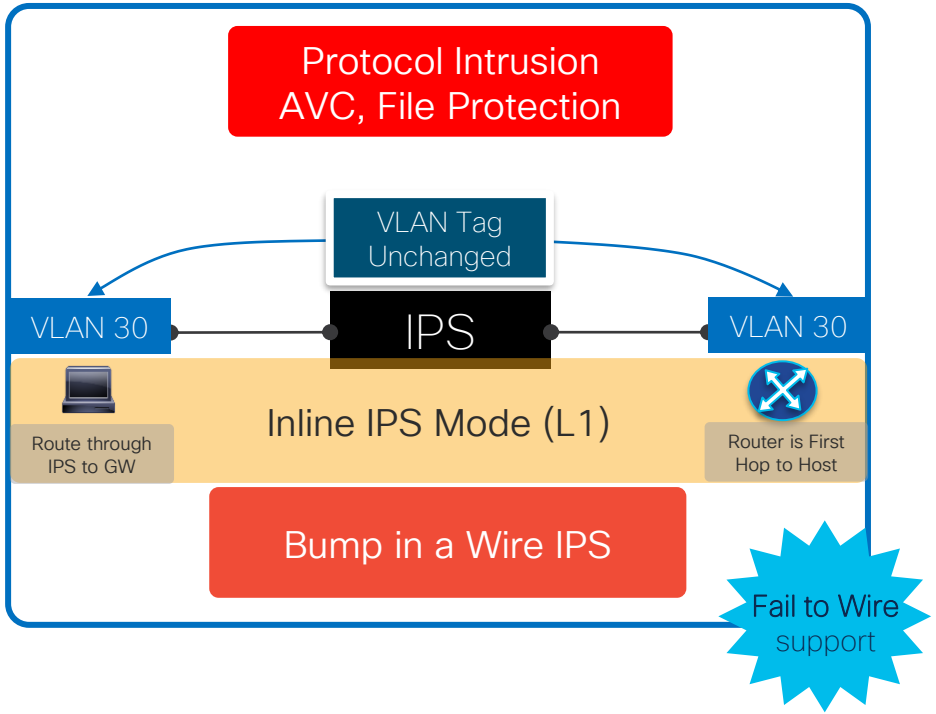
- Threat-centric NGIPS
- AVC, URL Filtering for NGFW
- Advanced Malware Protection

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

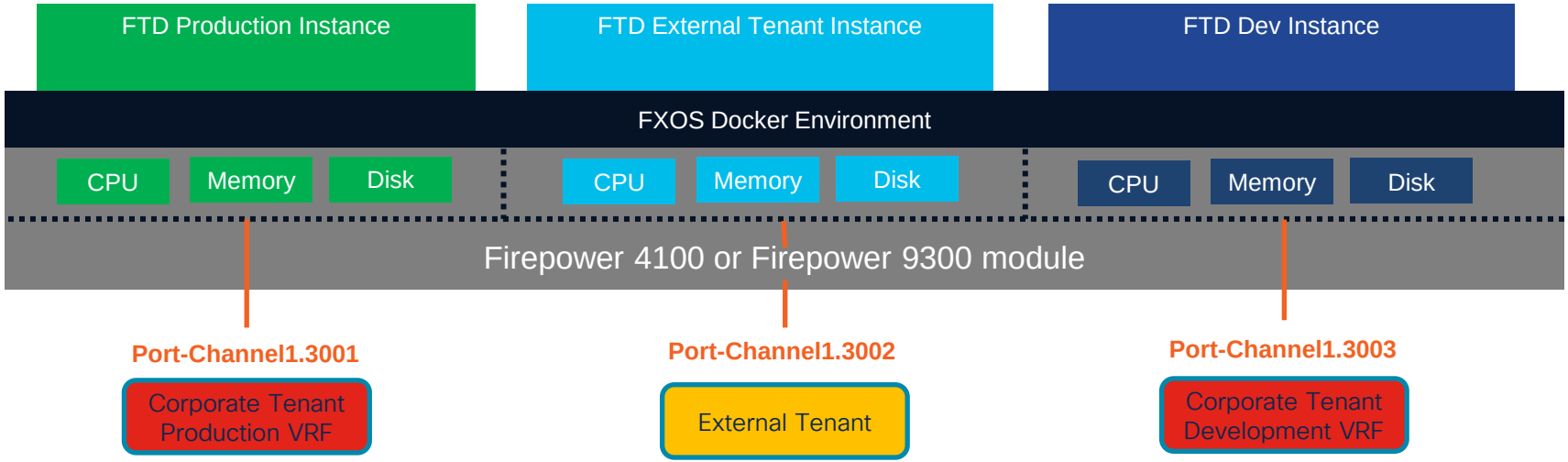
Cisco Secure Firewall Modes of Operation





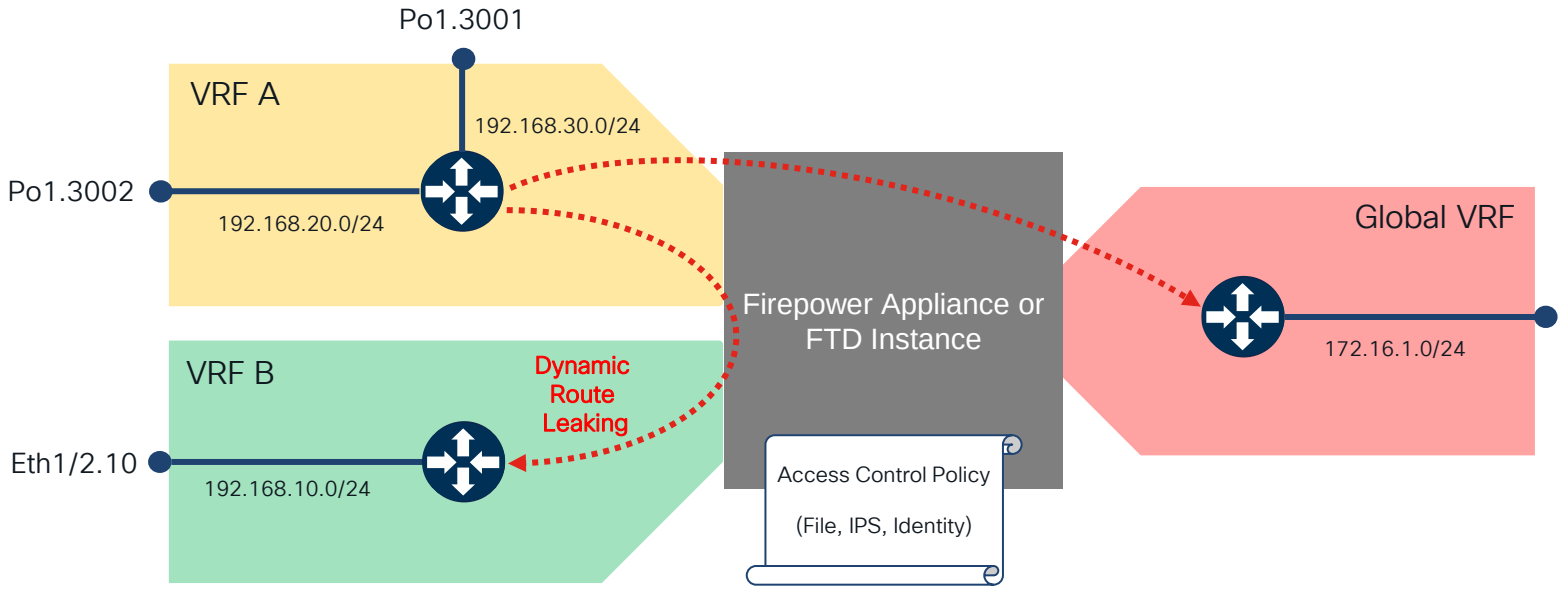
FTD Multi-Instance DC Use Case

- 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

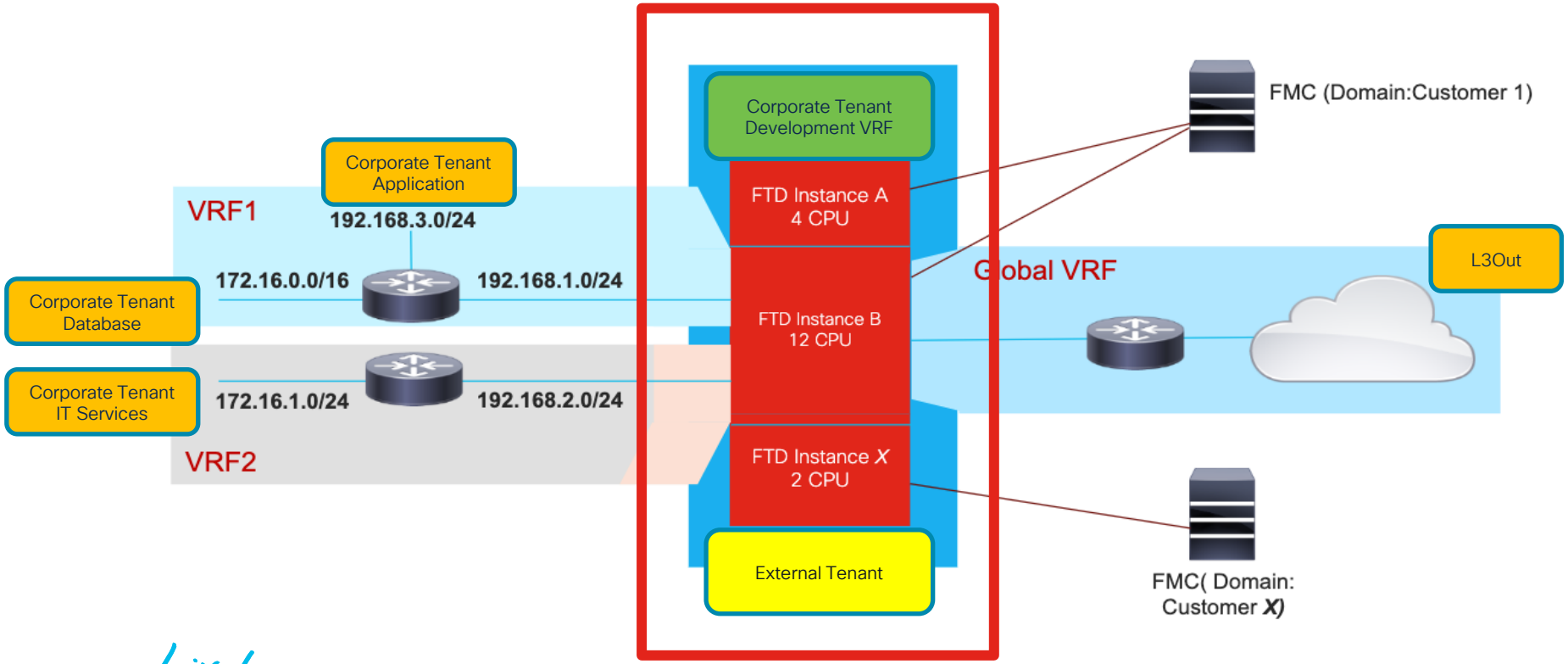


Virtual Routing and Forwarding (VRF) Lite

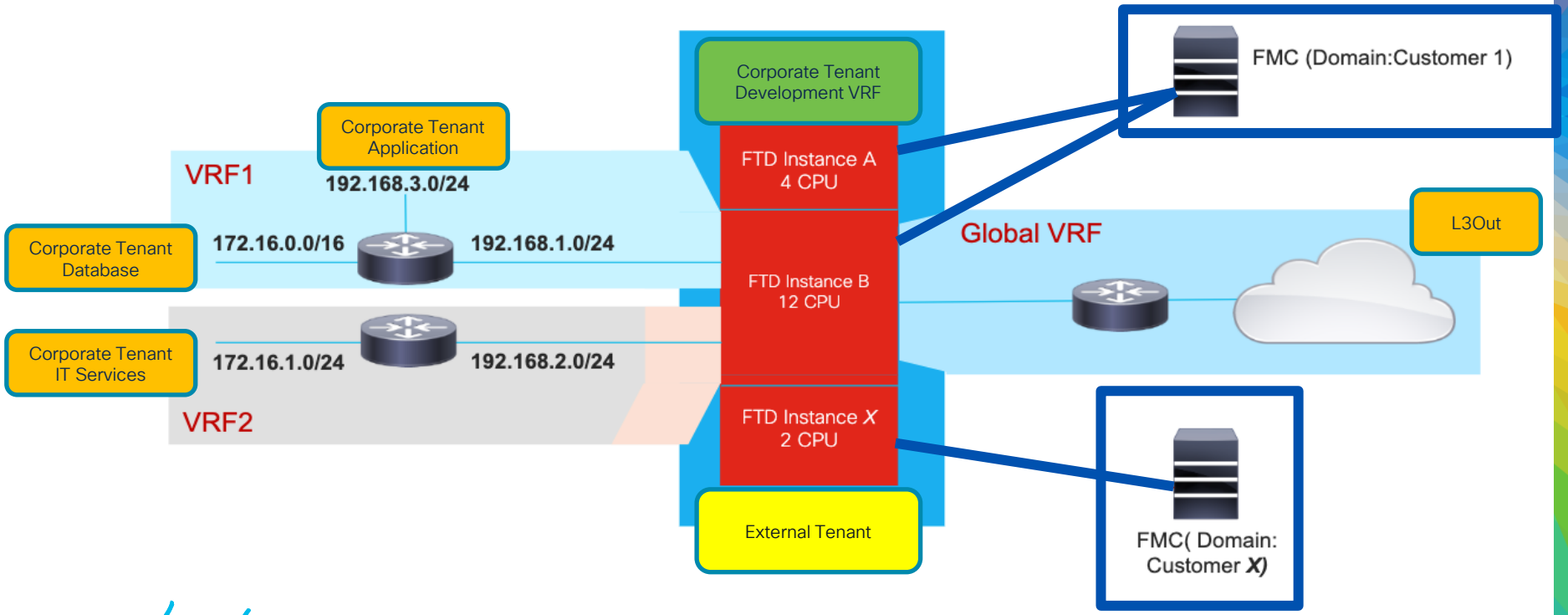
- In FTD 6.6, interfaces can be in different Routing Domains (Overlapping IP address support between User and Global VRF)
- Allows for easy separation of Service Graphs within the same FTD



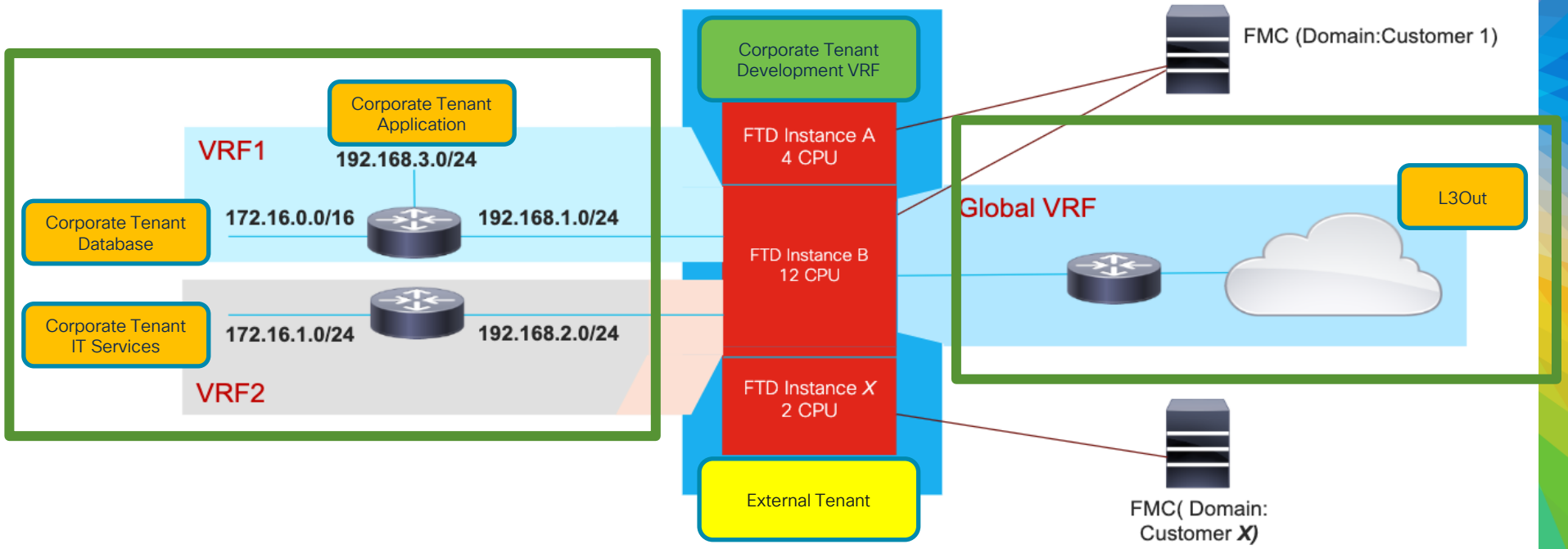
Multi-Instance, VRF and Multi-Domain Combined



Multi-Instance, VRF and Multi-Domain Combined



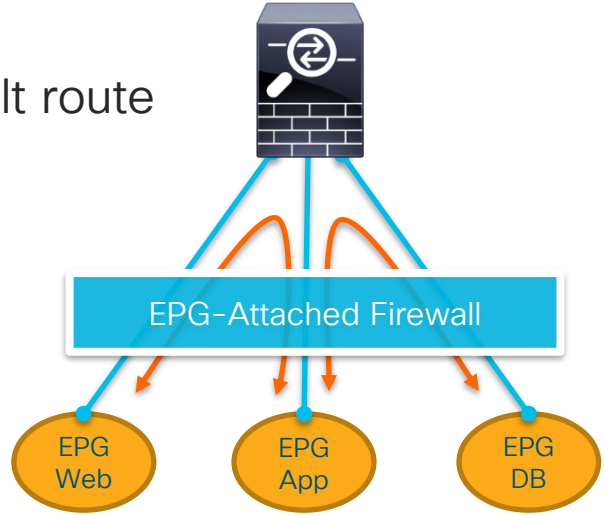
Multi-Instance, VRF and Multi-Domain Combined



Secure Firewall Insertion

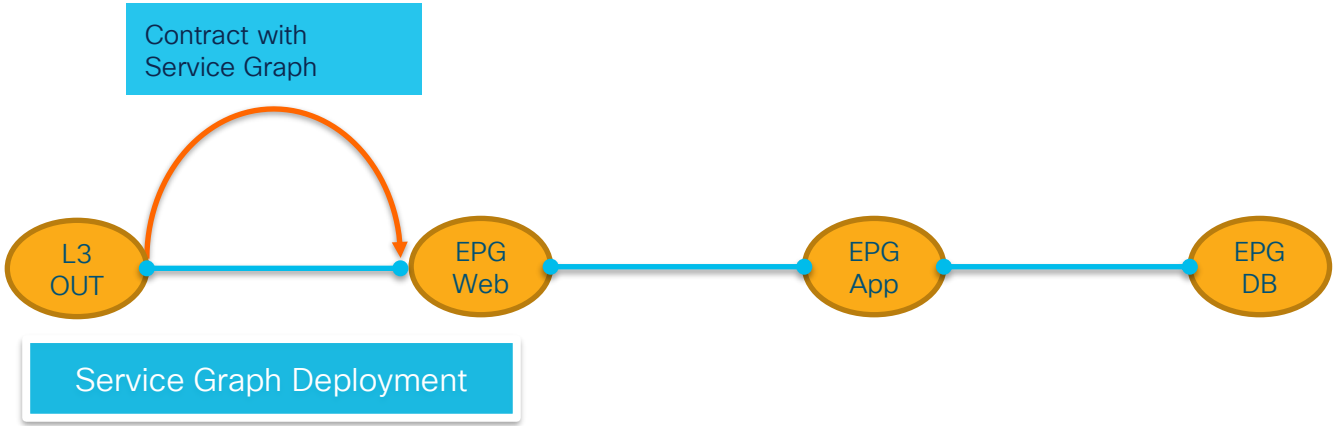
“Network Stitching” Firewall Insertion

- 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

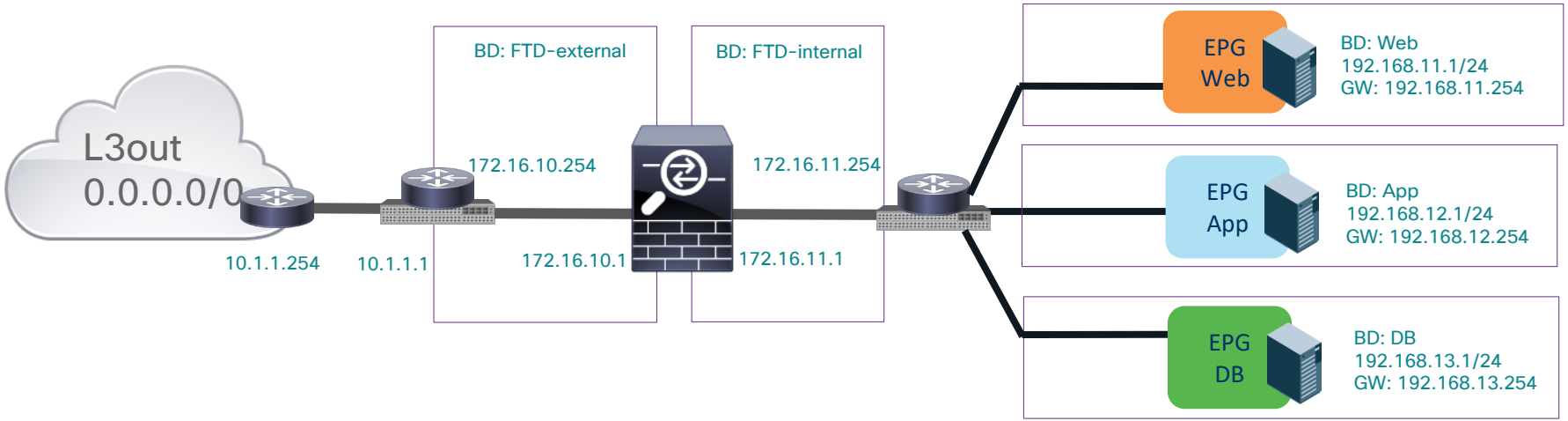


Traditional Service Graph

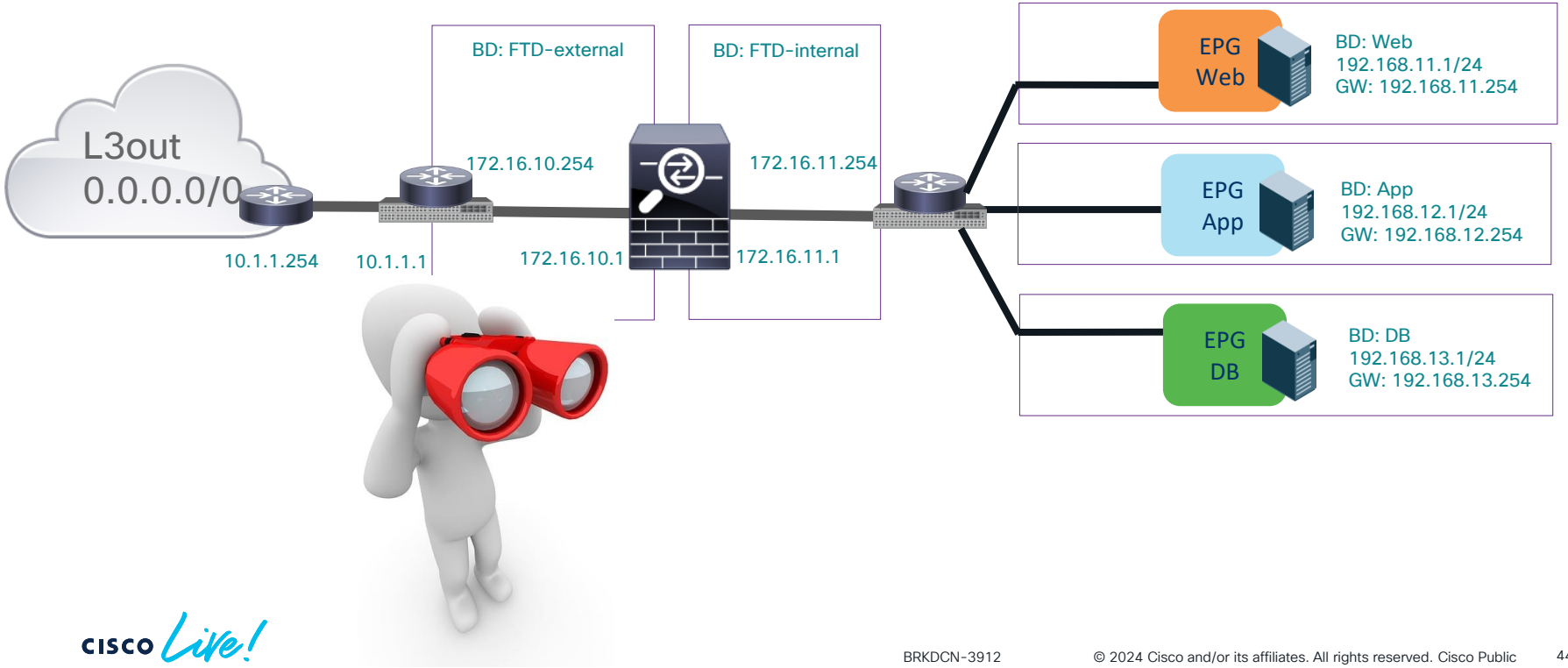
- **Contracts** define communication between EPGs
- **Service Graphs** specify the services between EPGs and are referred in Contracts
- Configure Firewall in **Go-To/Go-Through modes** or L1 NGIPS



Traditional Service GraphTopology

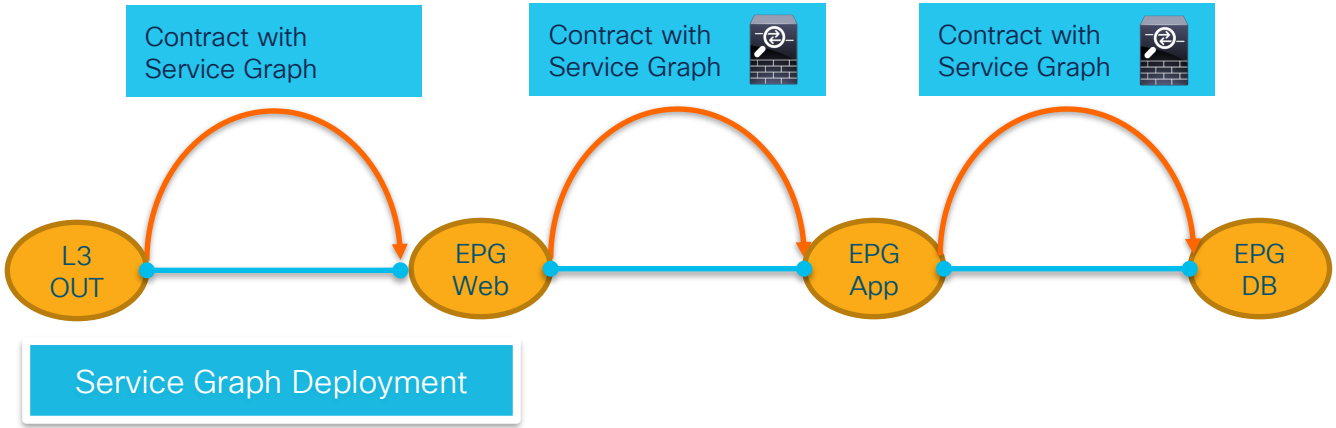


FW is part of the IP connectivity

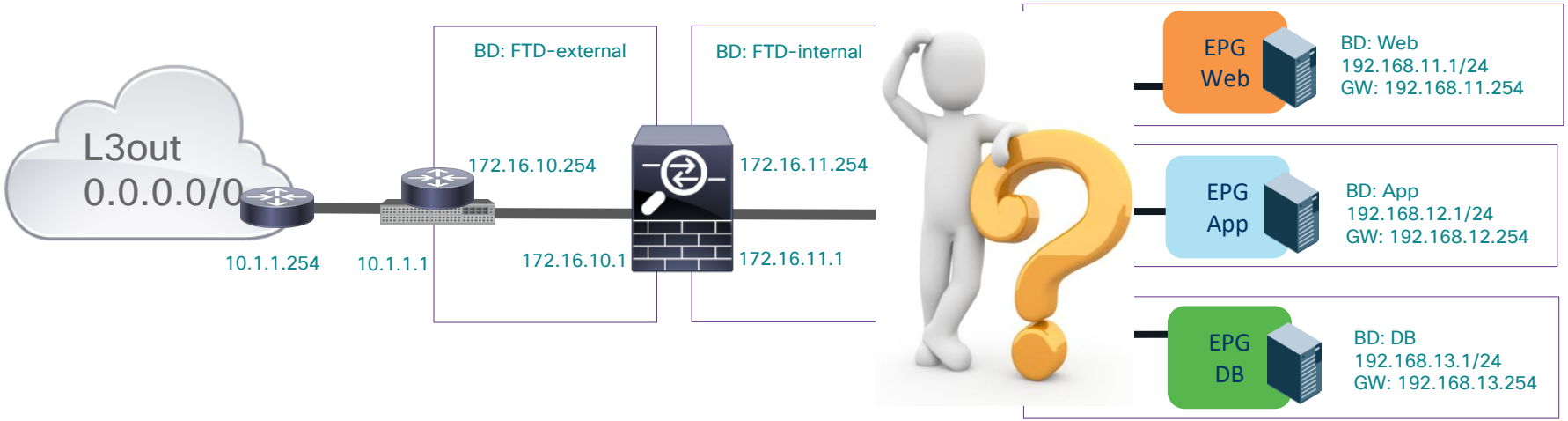


Traditional Service Graph (Episode 2)

- 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

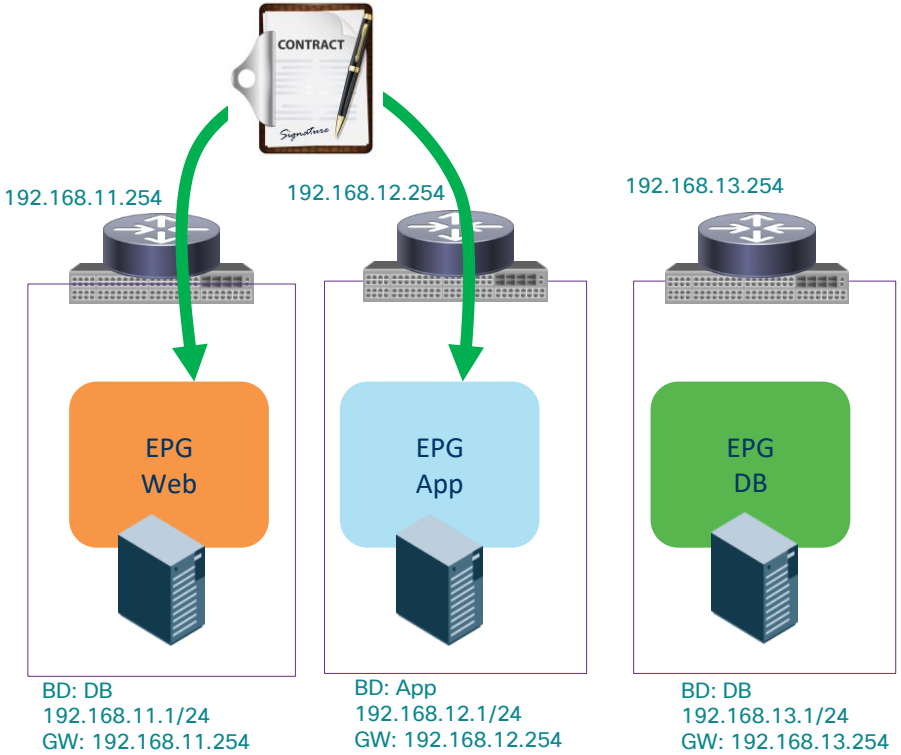


How do i extend my segmentation ?



2 conditions for traffic reaching destination

Before Service graph is deployed

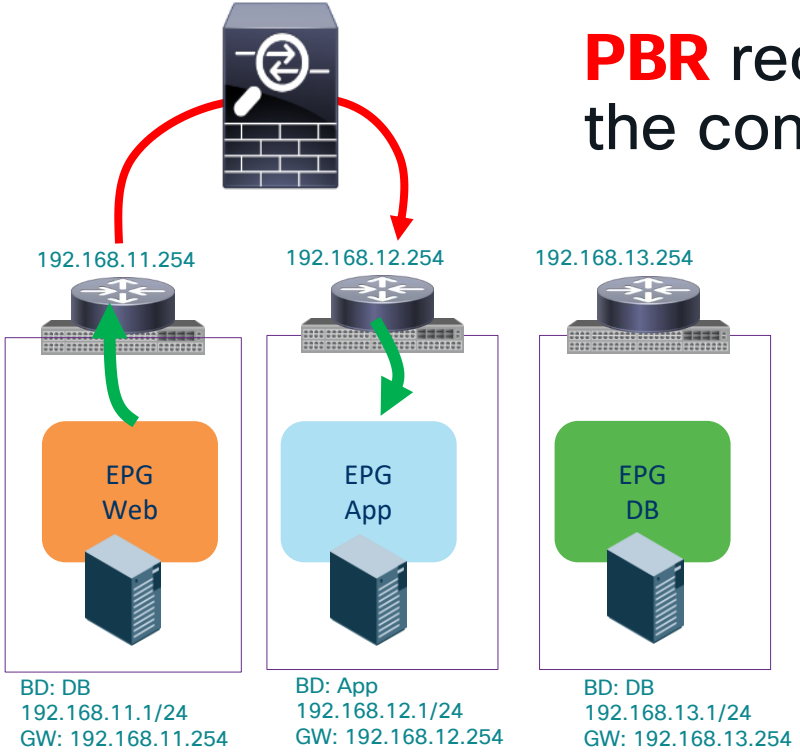


APIC relies on :

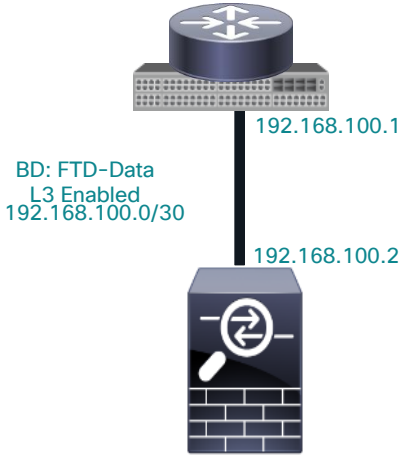
- ✓ **Routing** to forward traffic
- ✓ **Contract** to allow traffic

Policy Based Redirect is your Best Friend

With PBR Service Graph

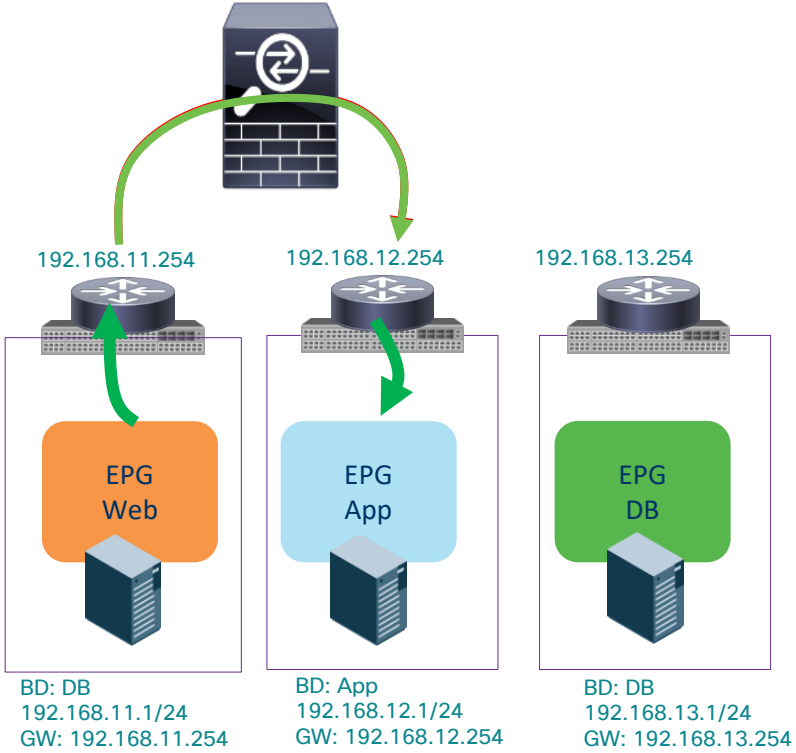


PBR redirects the traffic matching the contract to the Security Service

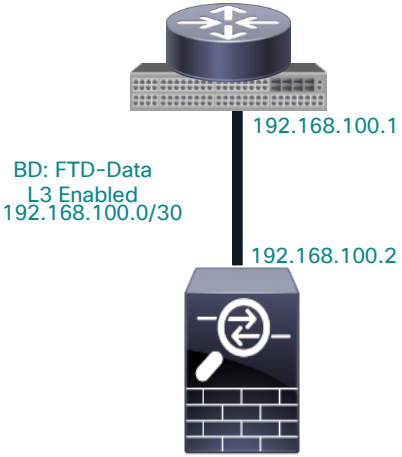


Policy Based Redirect is your Best Friend

With PBR Service Graph

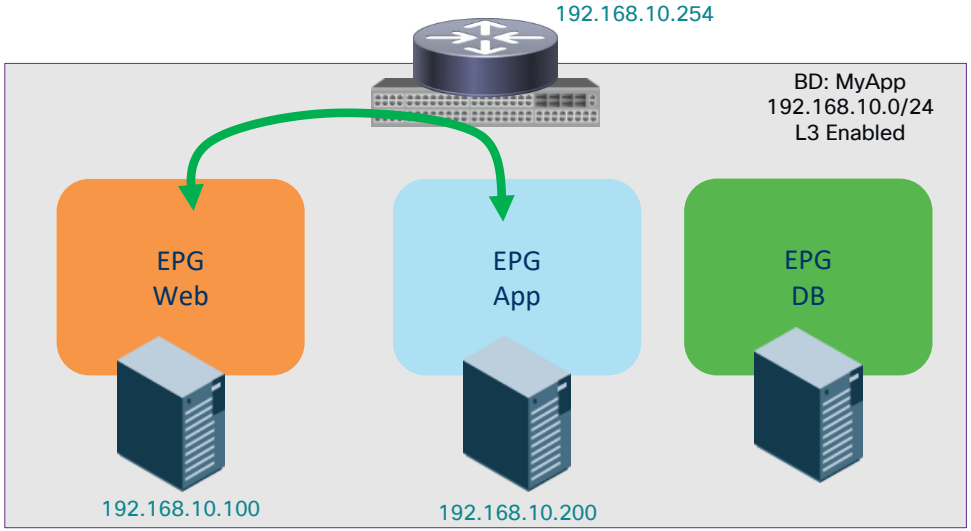


PBR redirects the traffic matching the contract to the **Security Service**



PBR for micro-Segmentation

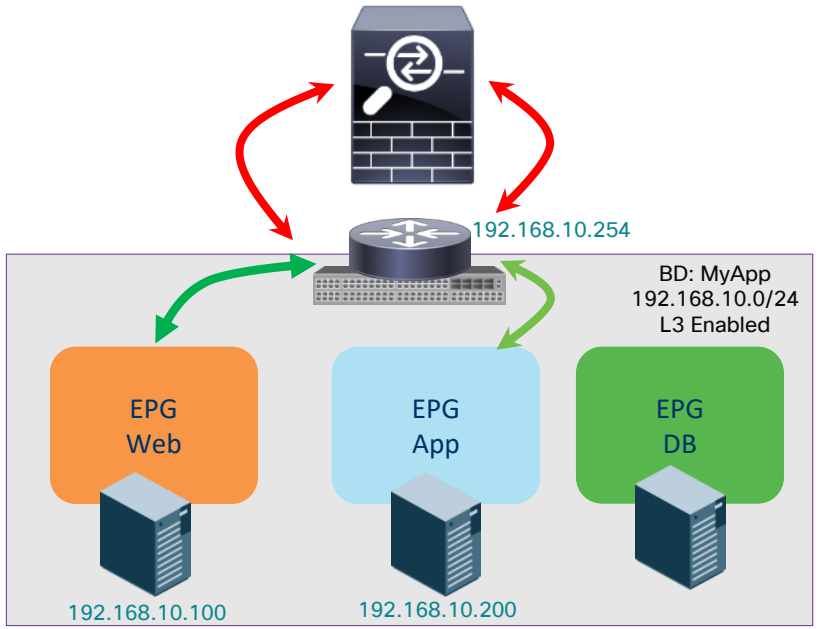
Based only on Contract



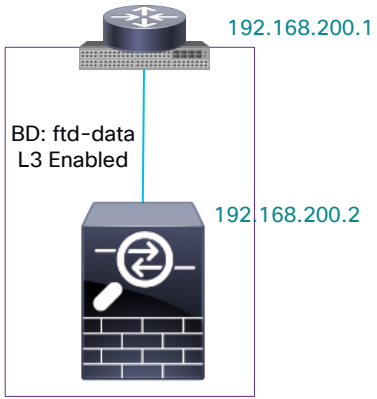
- Workloads in same Subnet
- Workloads in different EPG/ESG
- Leaf switch enforce micro-segmentation with contract

PBR for micro-Segmentation

Leveraging PBR



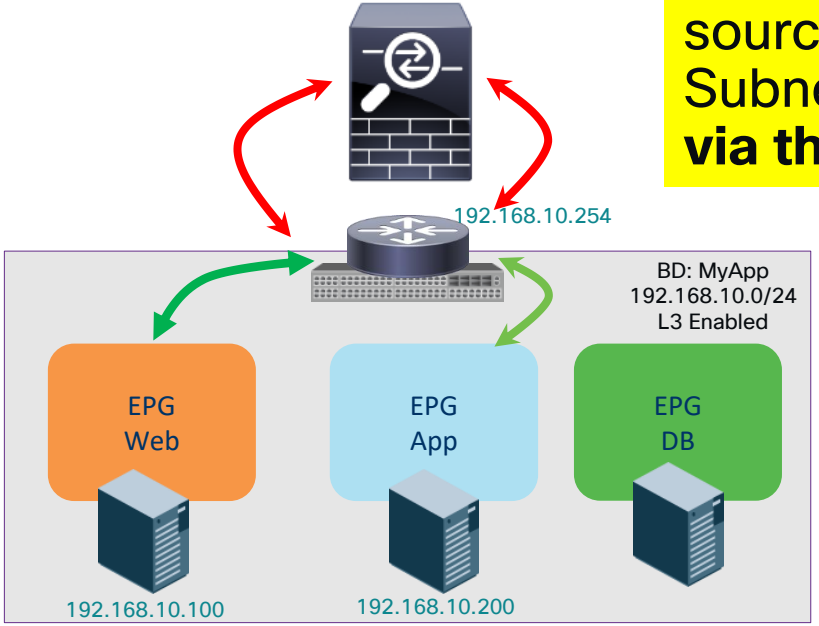
- PBR Service Graph preempts the forwarding decision
- Traffic is sent to the FW

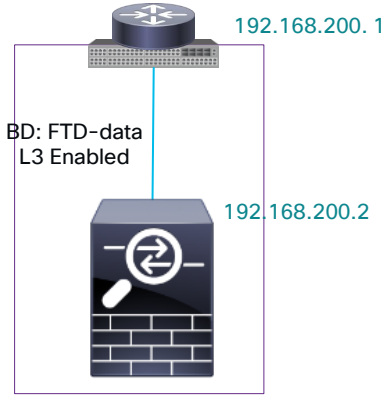


PBR for micro-Segmentation

Leveraging PBR

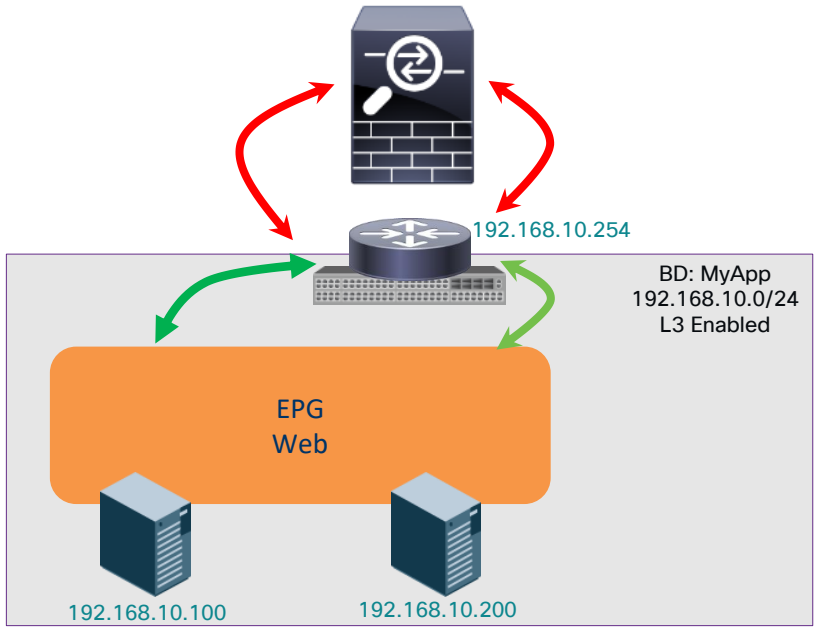
The Firewall must be in **ONE ARM** as source and destination are in the same Subnet. It must **allow traffic in and out via the same interface.**

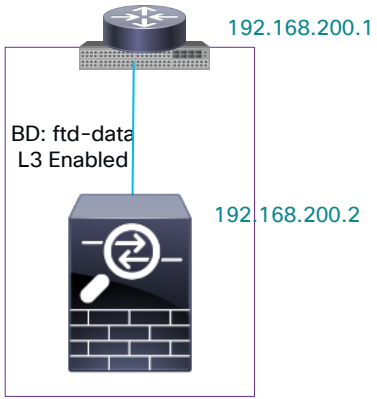




Redirecting traffic within an EPG/ESG

Leveraging PBR

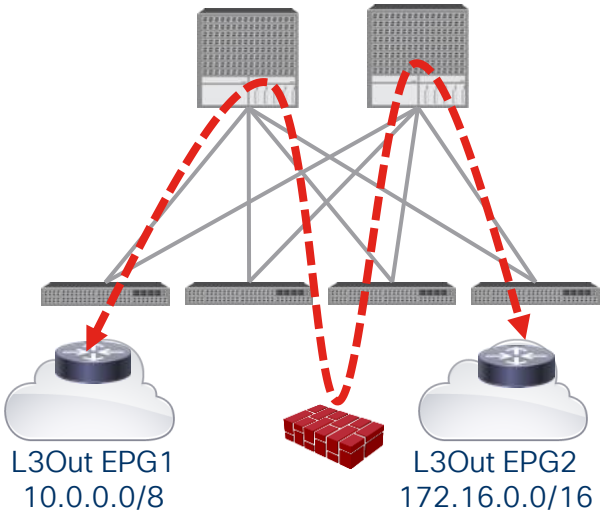




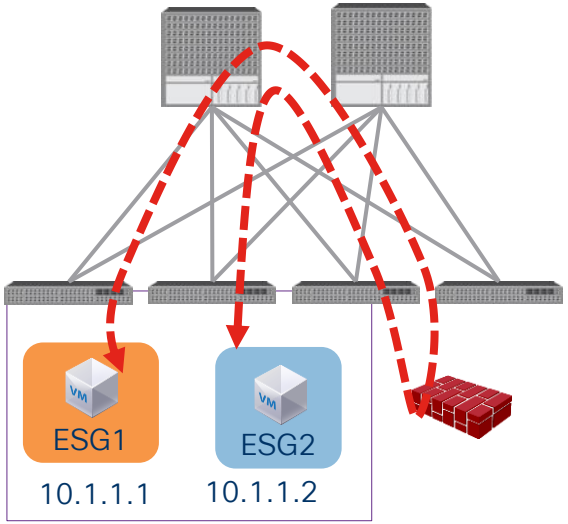
Where can we use PBR?

Wherever contracts can be applied!

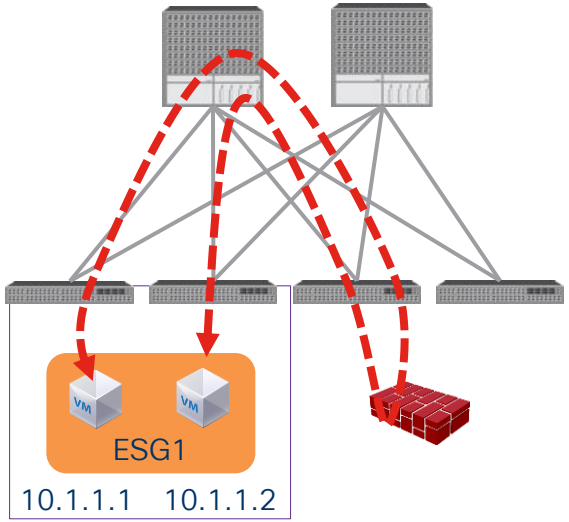
- Between EPGs or ESGs.
- Between L3Out EPGs.



- Between EPGs or ESGs in the same subnet.



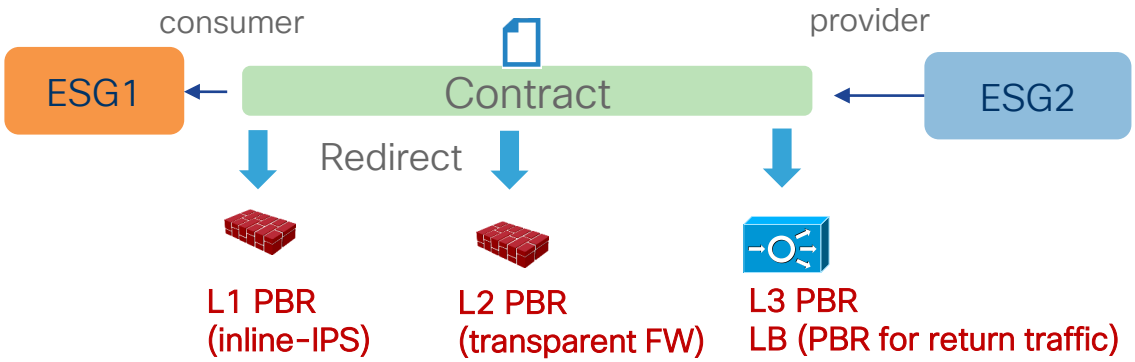
- Between endpoints in the same EPG or ESG.



What types of devices can be PBR destinations?

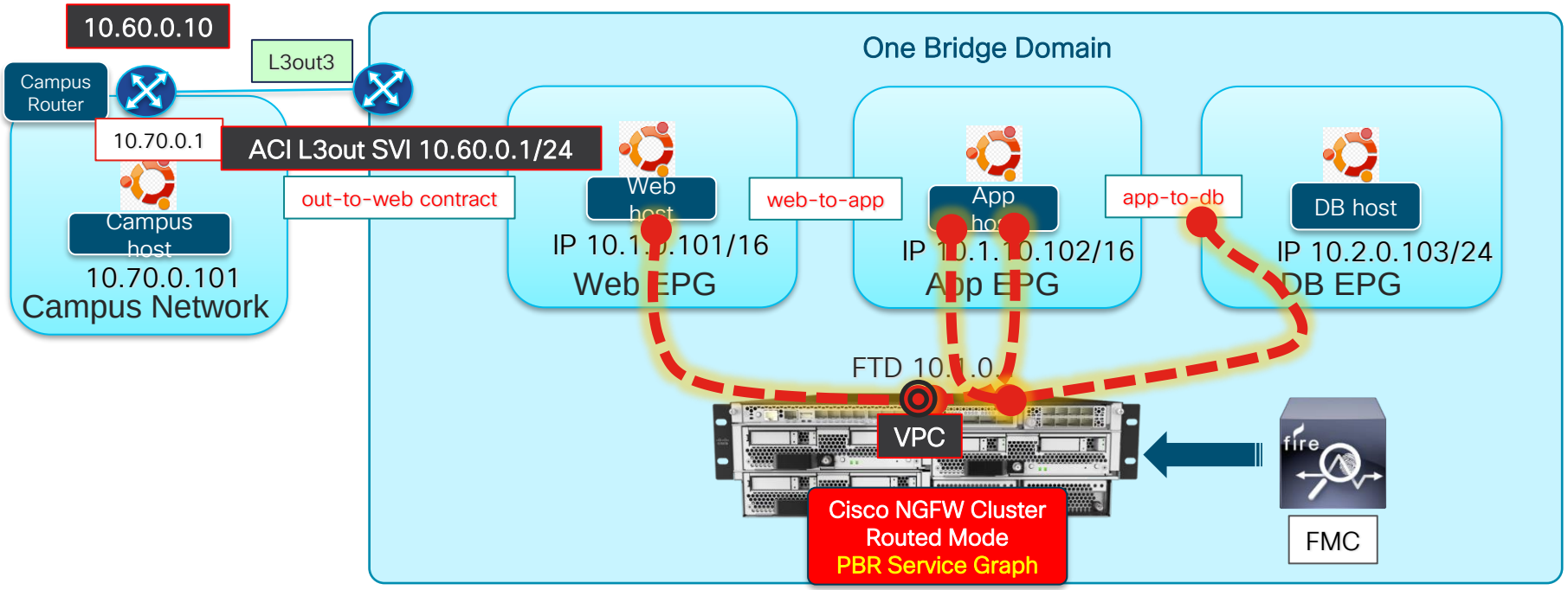
L1/L2/L3 device

- Prior to ACI Release 5.0, a PBR destination must be an L3 routed device (L3 PBR).
- Starting from ACI Release 5.0, L1/L2 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.



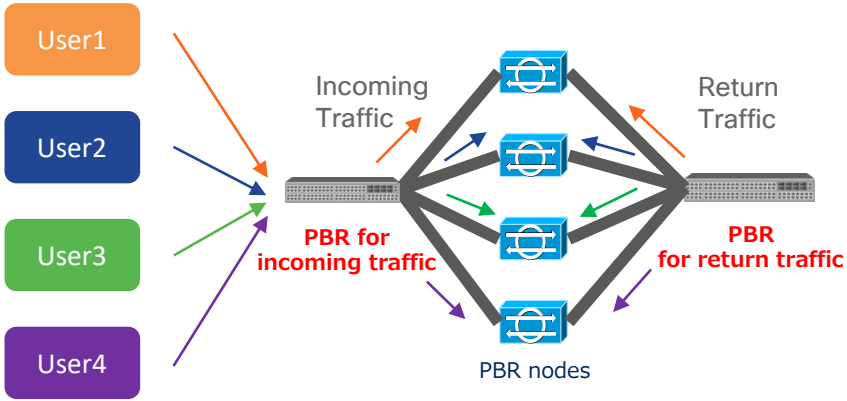
Reuse a PBR Service Graph in Multiple Contracts

Keep the Firewall Network Config Simple

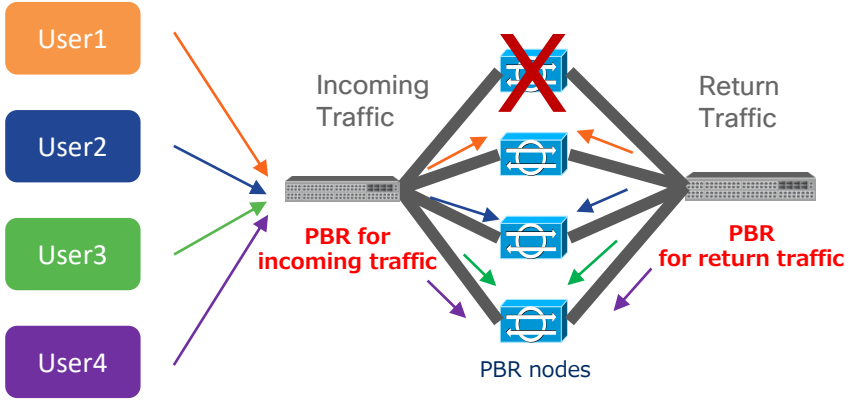


Without Resilient Hash PBR

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



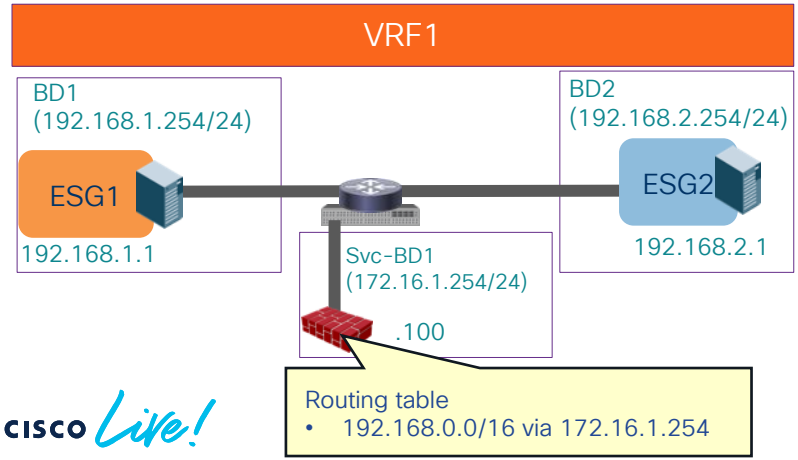
Some traffic could be load-balanced to different PBR nodes that don't have existing connection info.



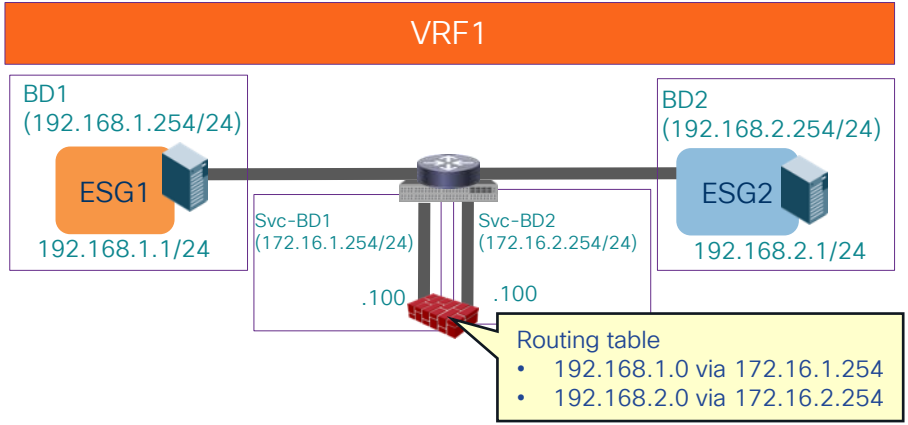
Sessions Green and Blue are impacted.

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.

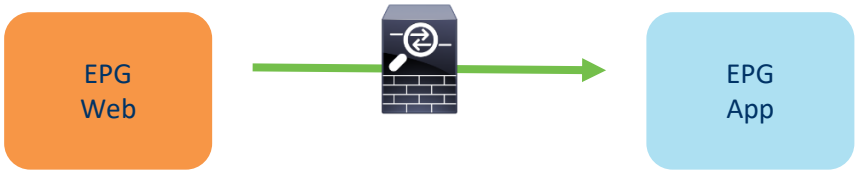


PBR Consideration

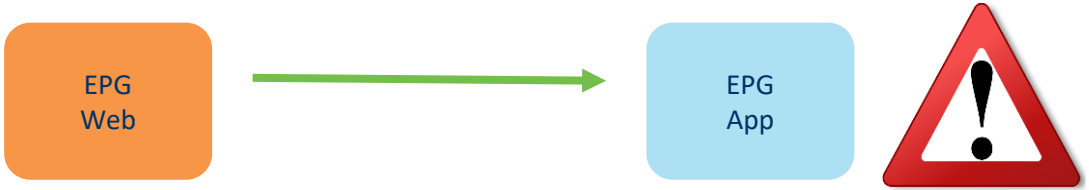
Contract 1: Permit TCP any any → Service Graph Firewall

Contract 2: Permit TCP any any eq HTTP

Contract Filters Precision DOES MATTER



Contract 1: Permit TCP any any → Service Graph Firewall



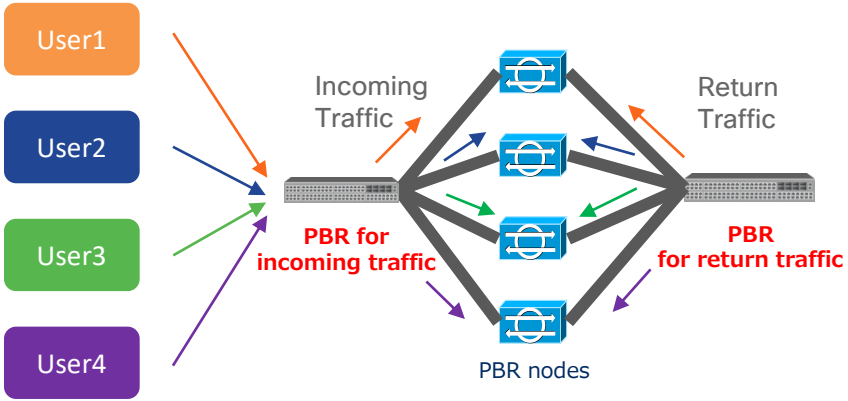
HTTP traffic not sent to FW

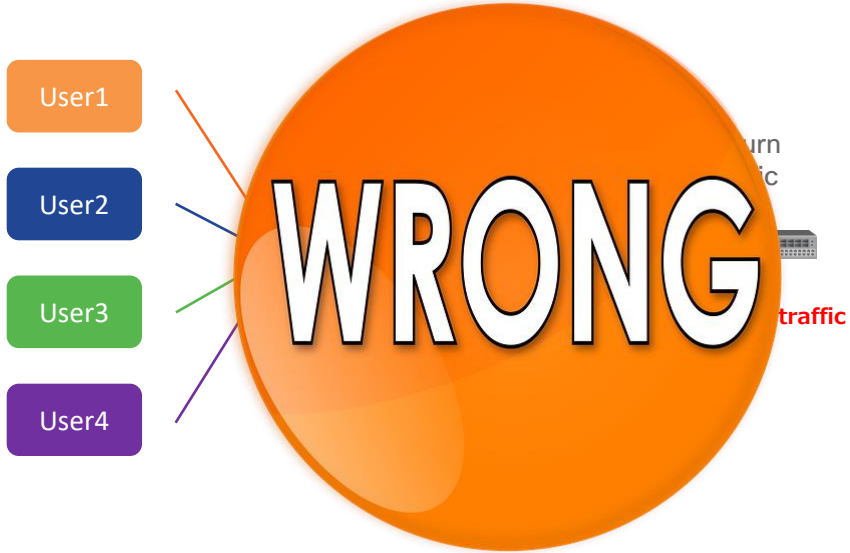
Contract 2: Permit TCP any any eq HTTP

Priority to the most precise contract

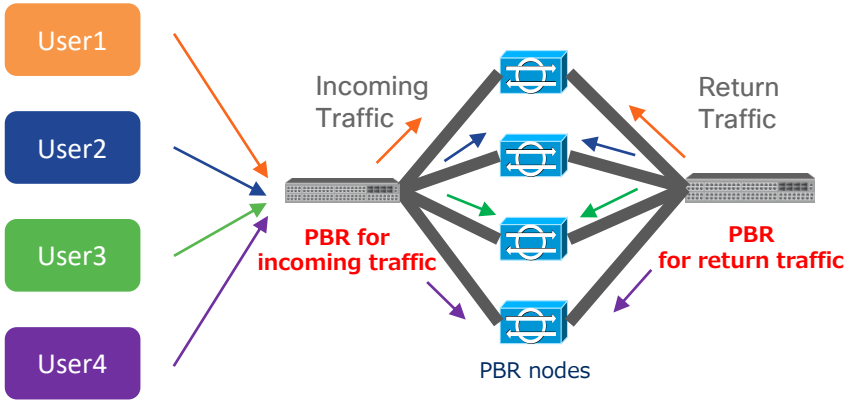
Resilient Hash PBR

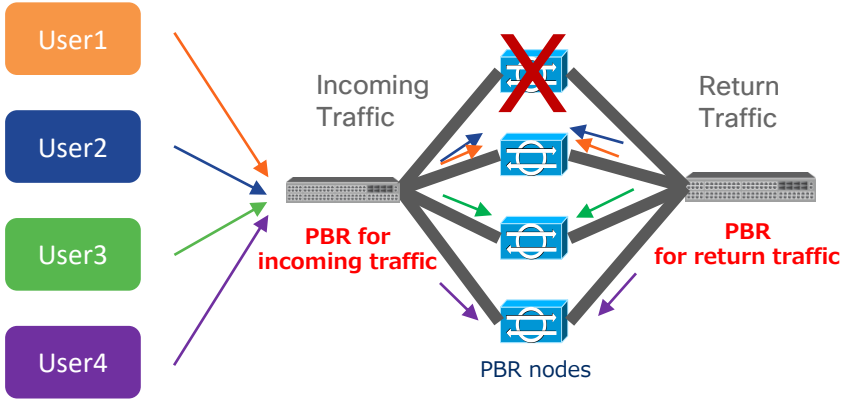
With Resilient Hash PBR, only the traffics that went though failed node will start using different PBR node.





Resilient Hash PBR caveats





Sessions impacted goes to ONE SINGLE different PBR node.

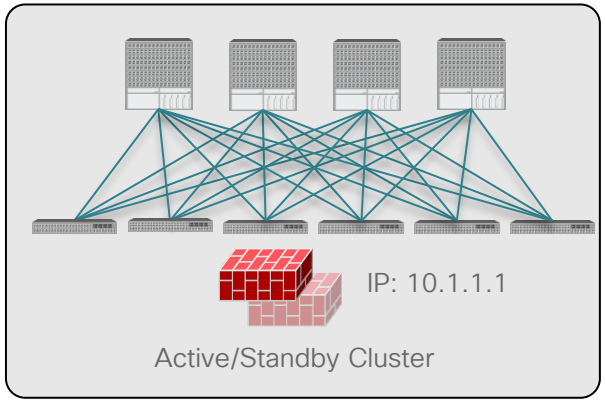
Solutions:

- Implement HA for each PBR node
- Implement PBR backup node
- Implement FTD Clustering and disable Resilient Hash

What are the Stateful HA options ?

One PBR destination IP
One Logical device with two concrete devices

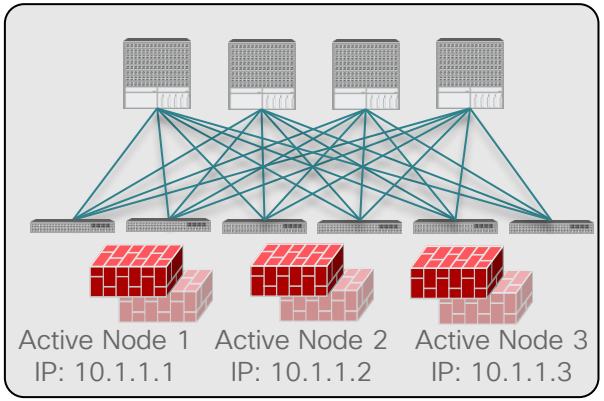
Single A/S Failover Node



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

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

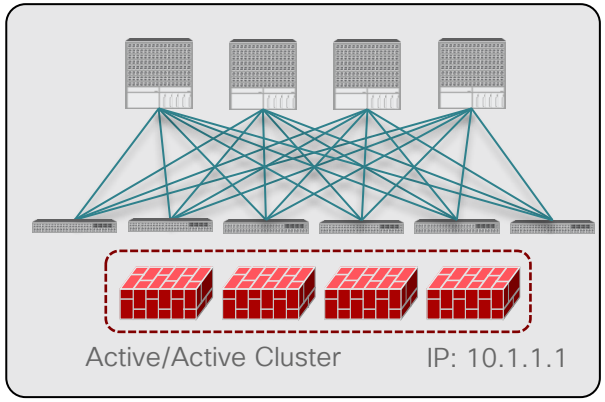
Several A/S Nodes



- 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

One PBR destination IP
One Logical device with one concrete device

Active/Active Cluster



- 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

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

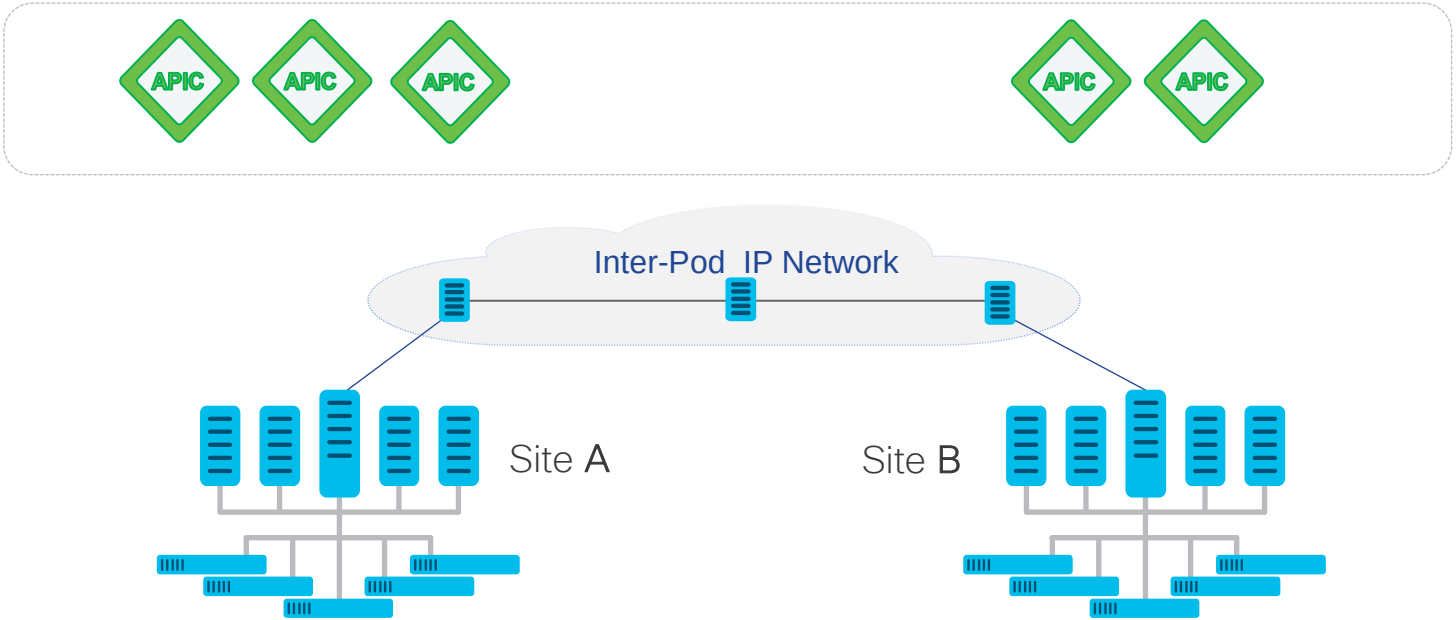
Automatic network threat containment using the network as an enforcer

Threat-centric network access determines network access based on IoCs

Multi-Pod Resilience with FTD Cluster

ACI MultiPod

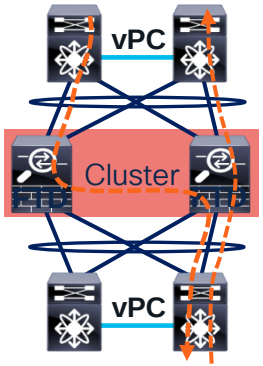
Single APIC Cluster Extends Network Virtualization, Policy, Services to Multiple PODs



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

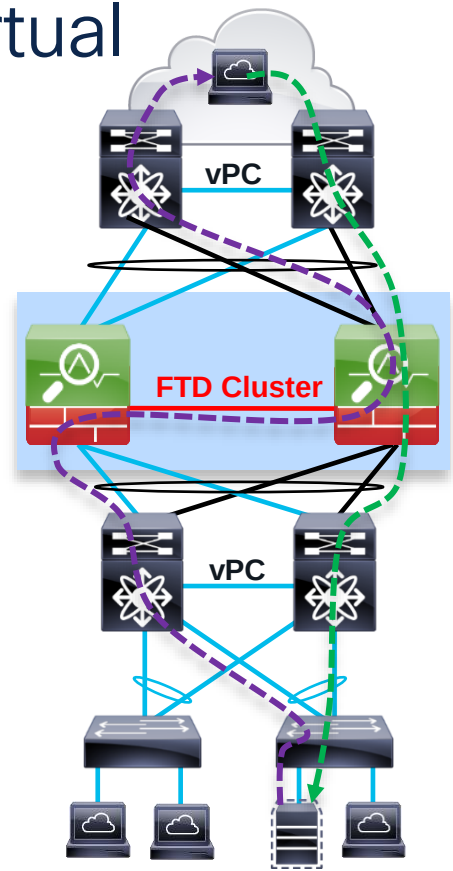
ASA and FTD Clustering

- **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

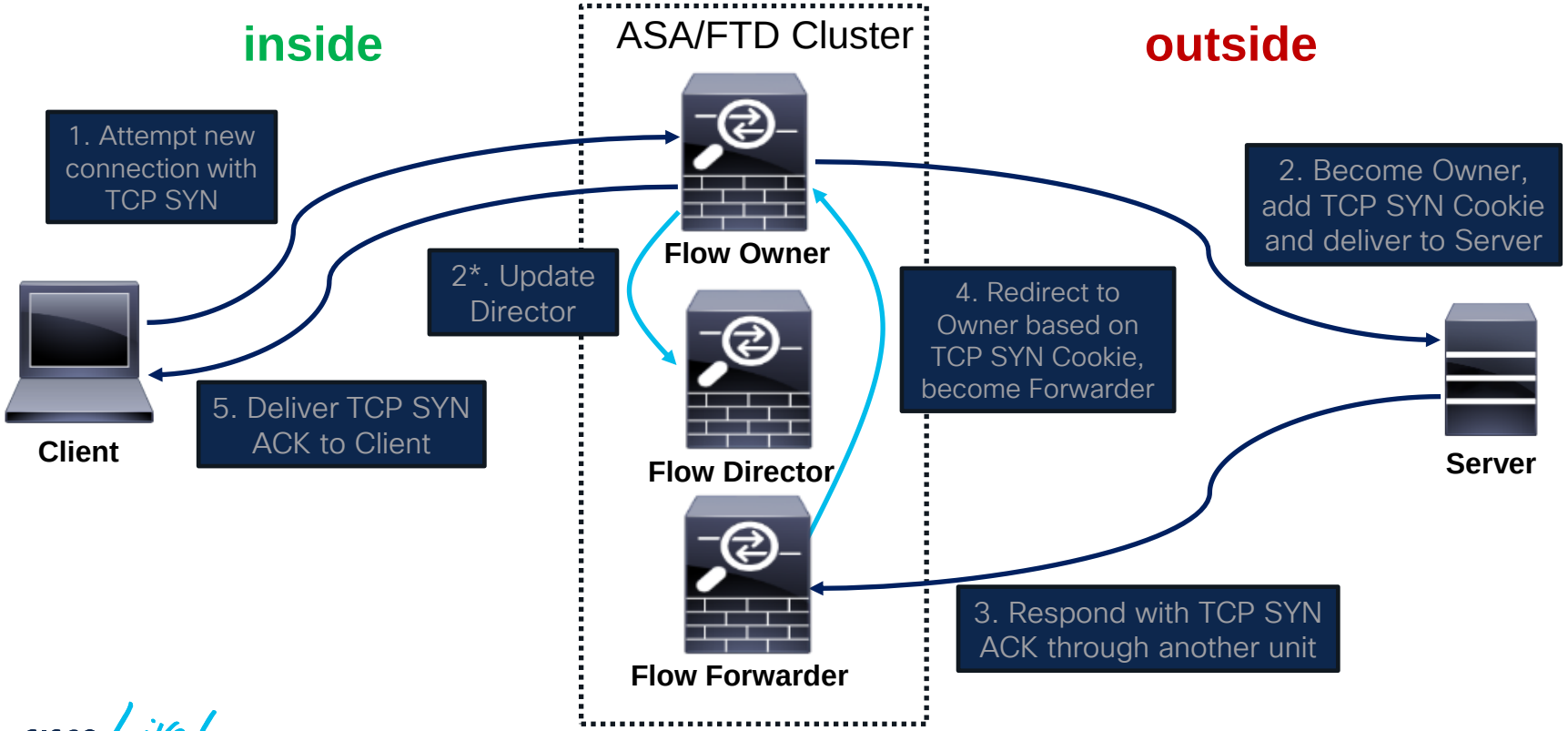


Clustering Concepts – Physical and Virtual

- Cluster roles
  - Control Node – synchronizes cluster configuration
  - Data Node – Cluster member other than the Control Node
- Flow roles
  - 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
  - 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

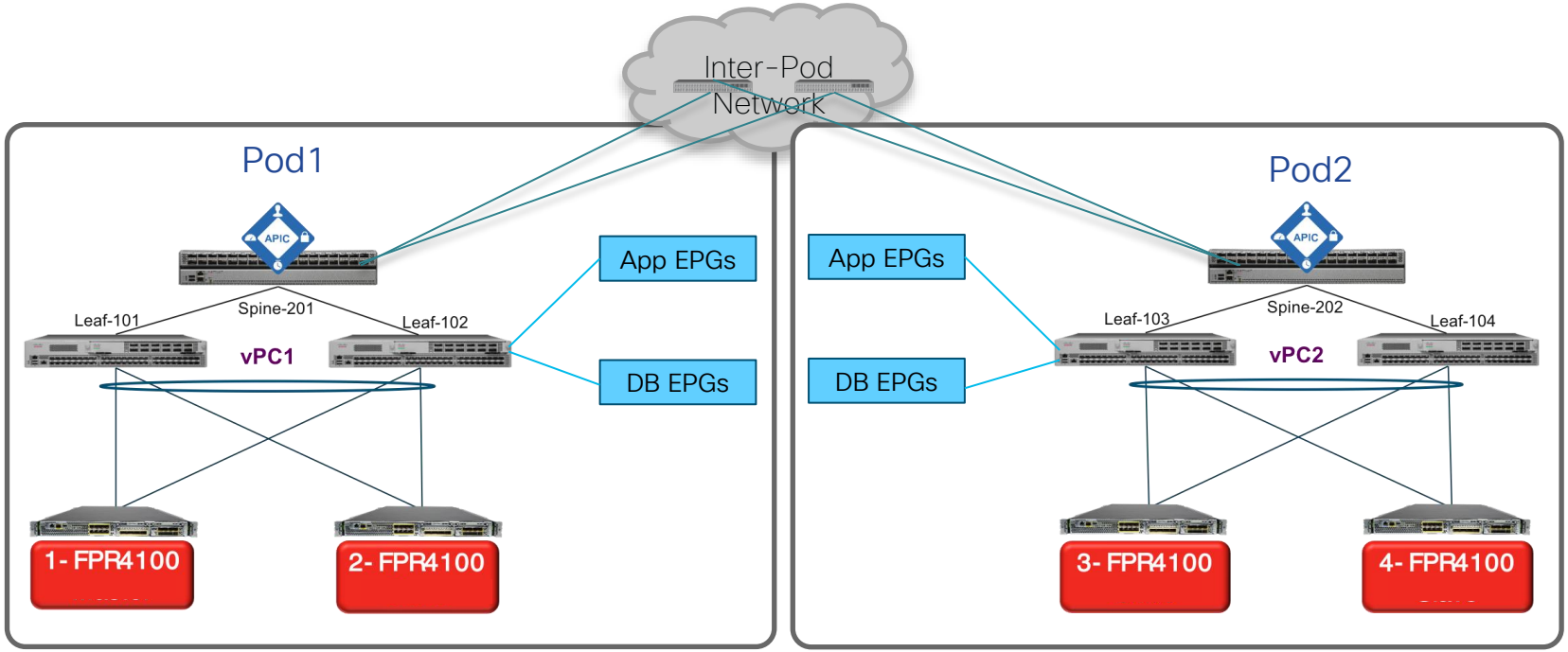
Remove

Add a data node

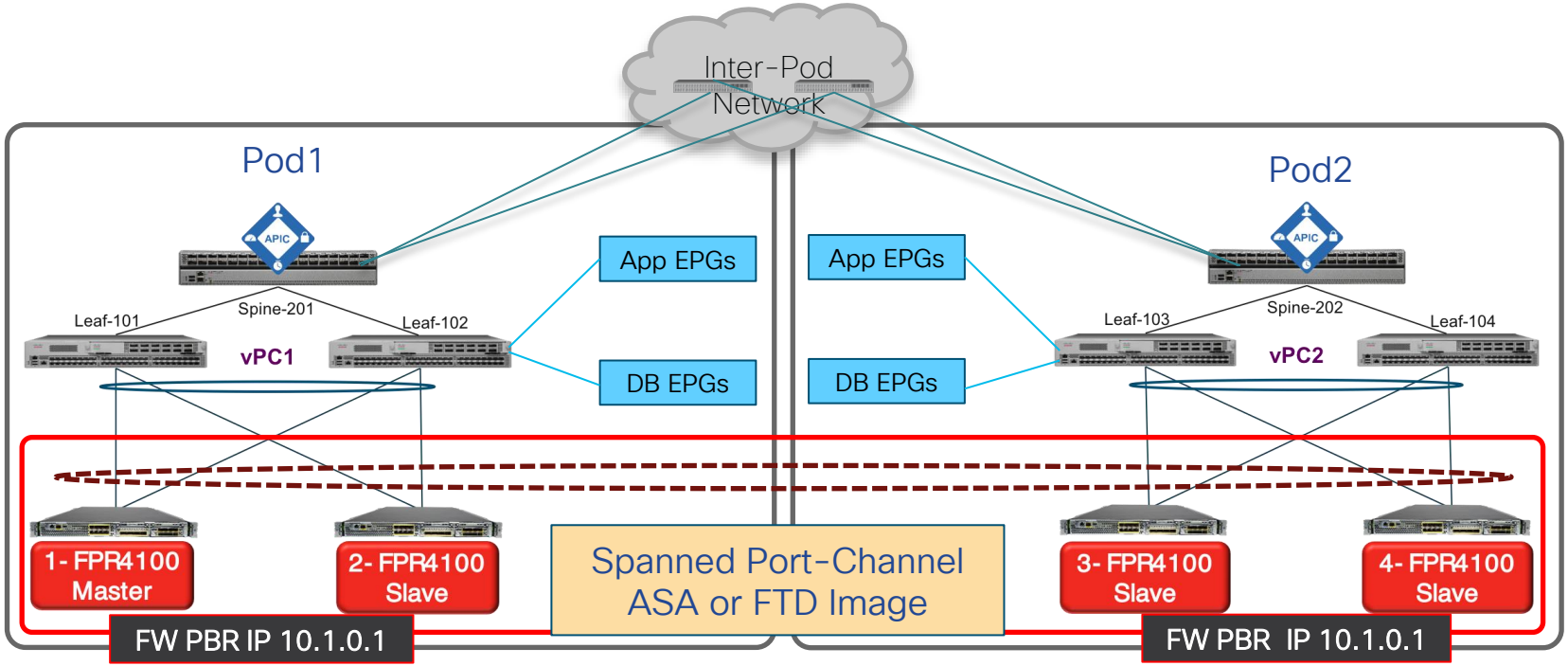
Cancel

Continue

PBR for FTD Cluster in ACI Multi-Pod

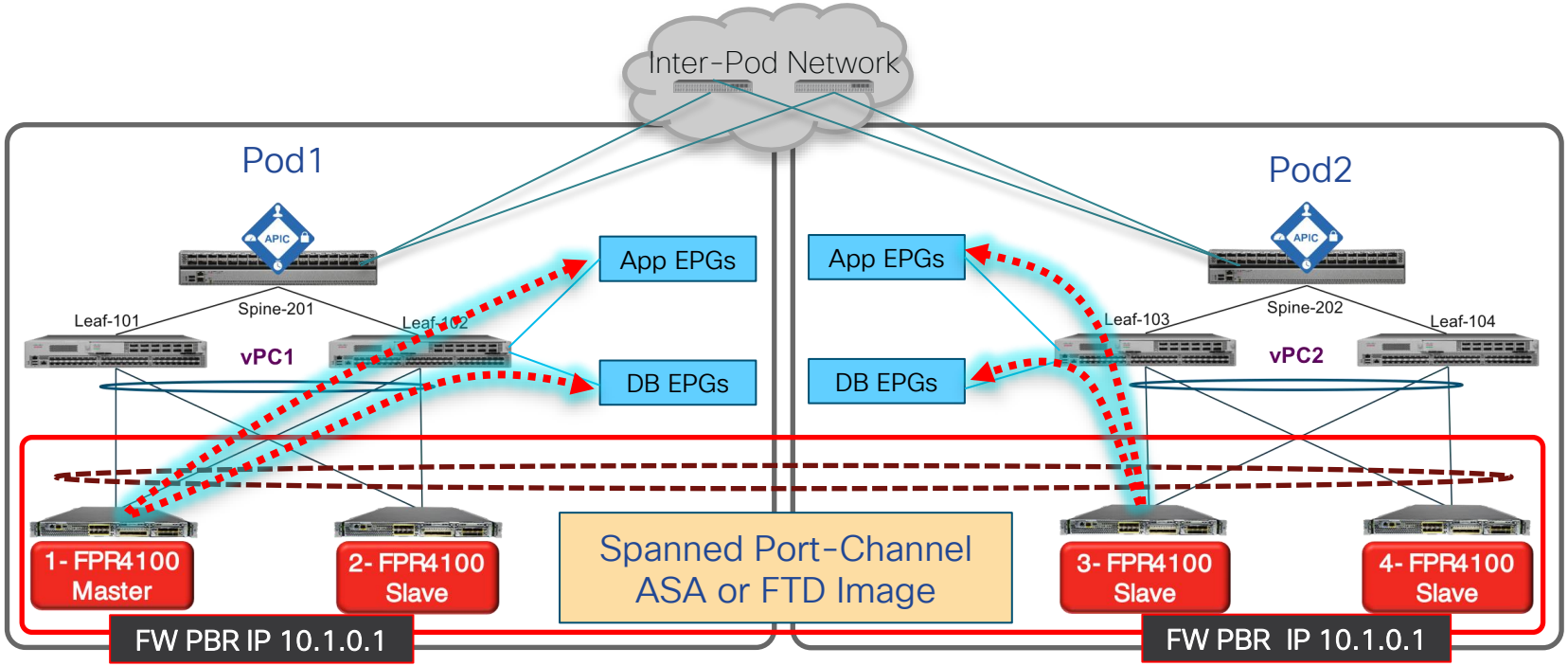


PBR for FTD Cluster in ACI Multi-Pod



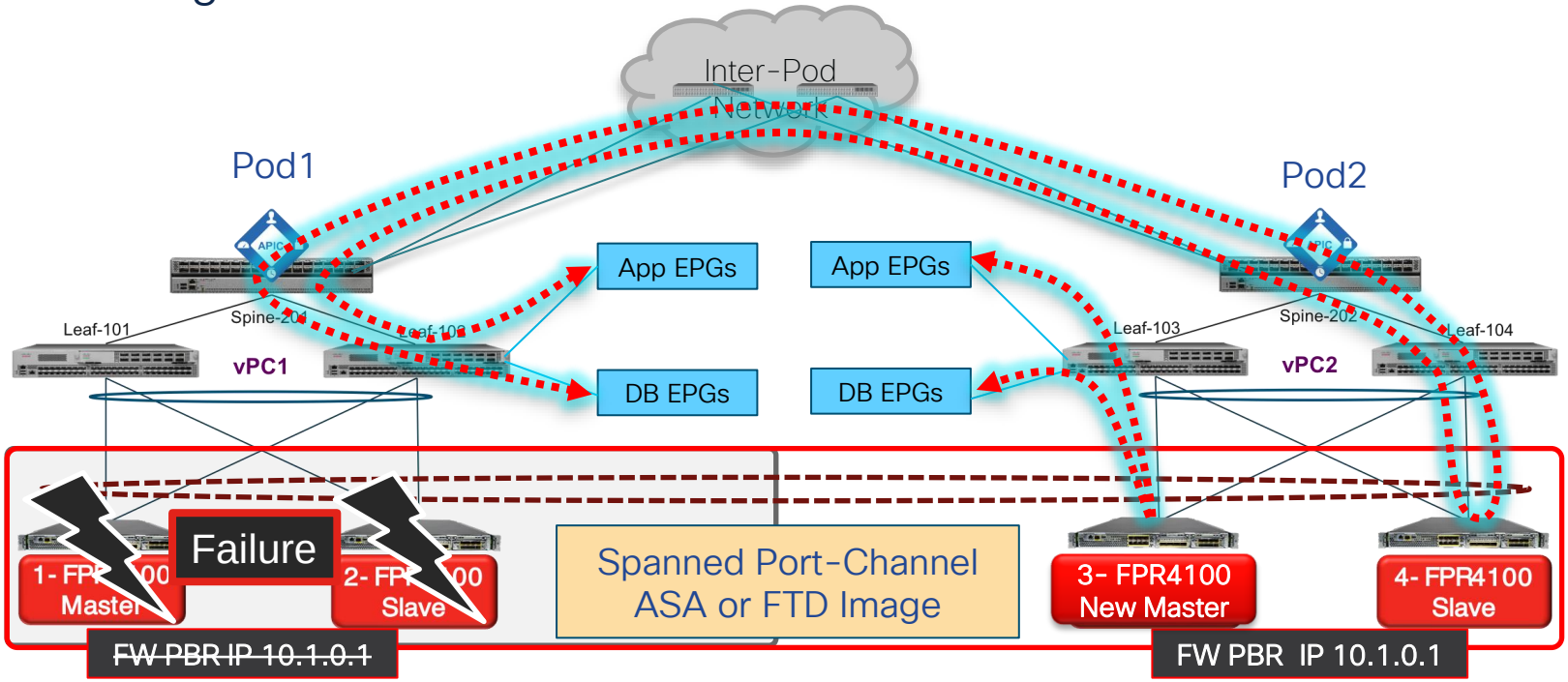
PBR for FTD Cluster in ACI Multi-Pod

Local Cluster member used



Firepower Cluster Resiliency

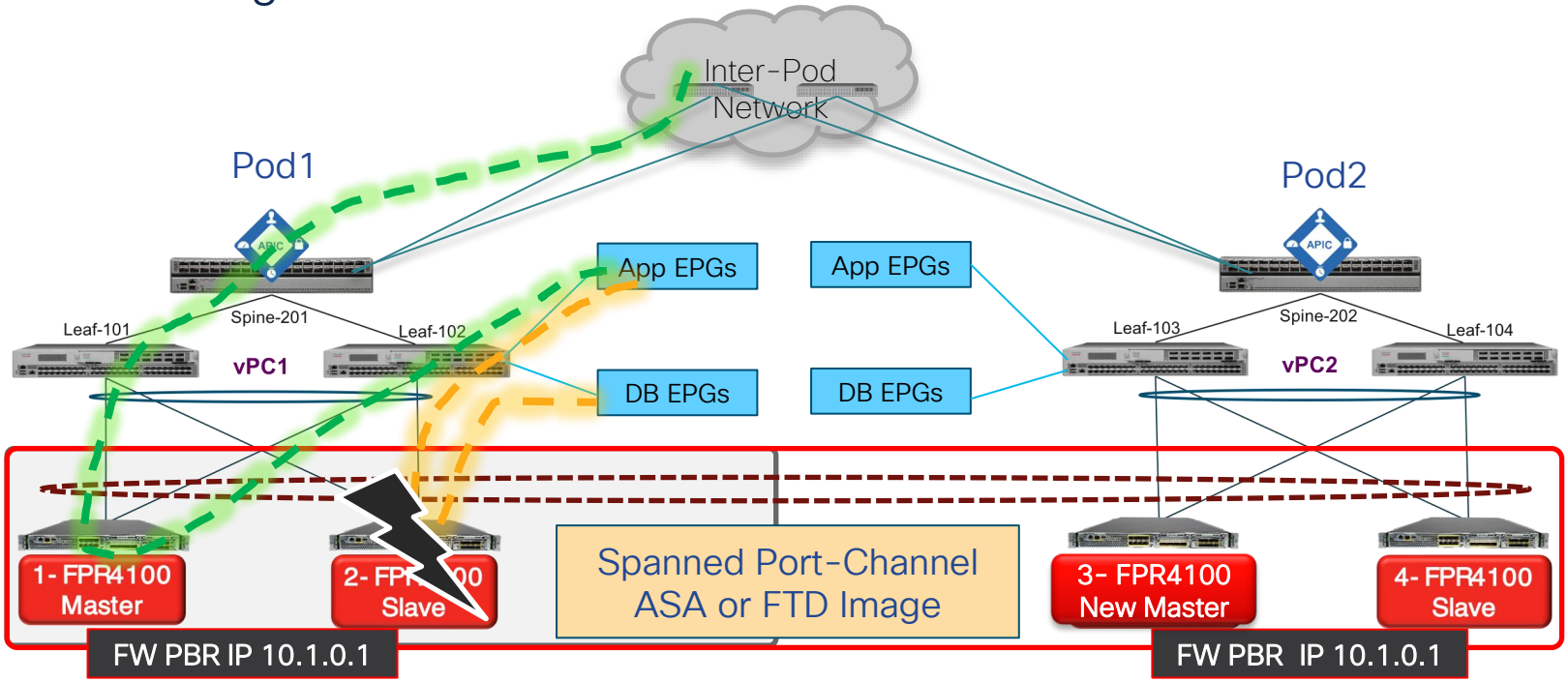
In case of global failure of POD1 cluster members



DEMO

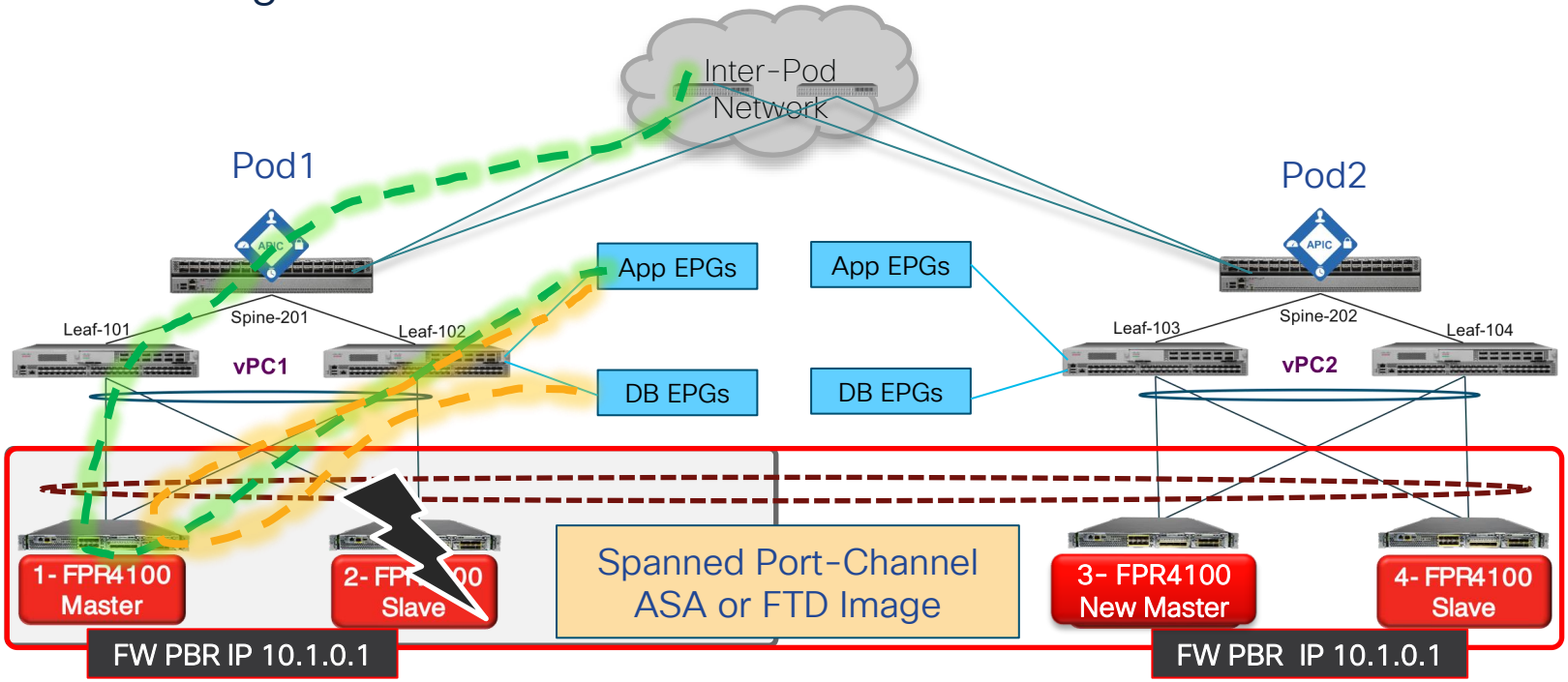
Firepower Cluster Resiliency

In case of single member failure of POD1



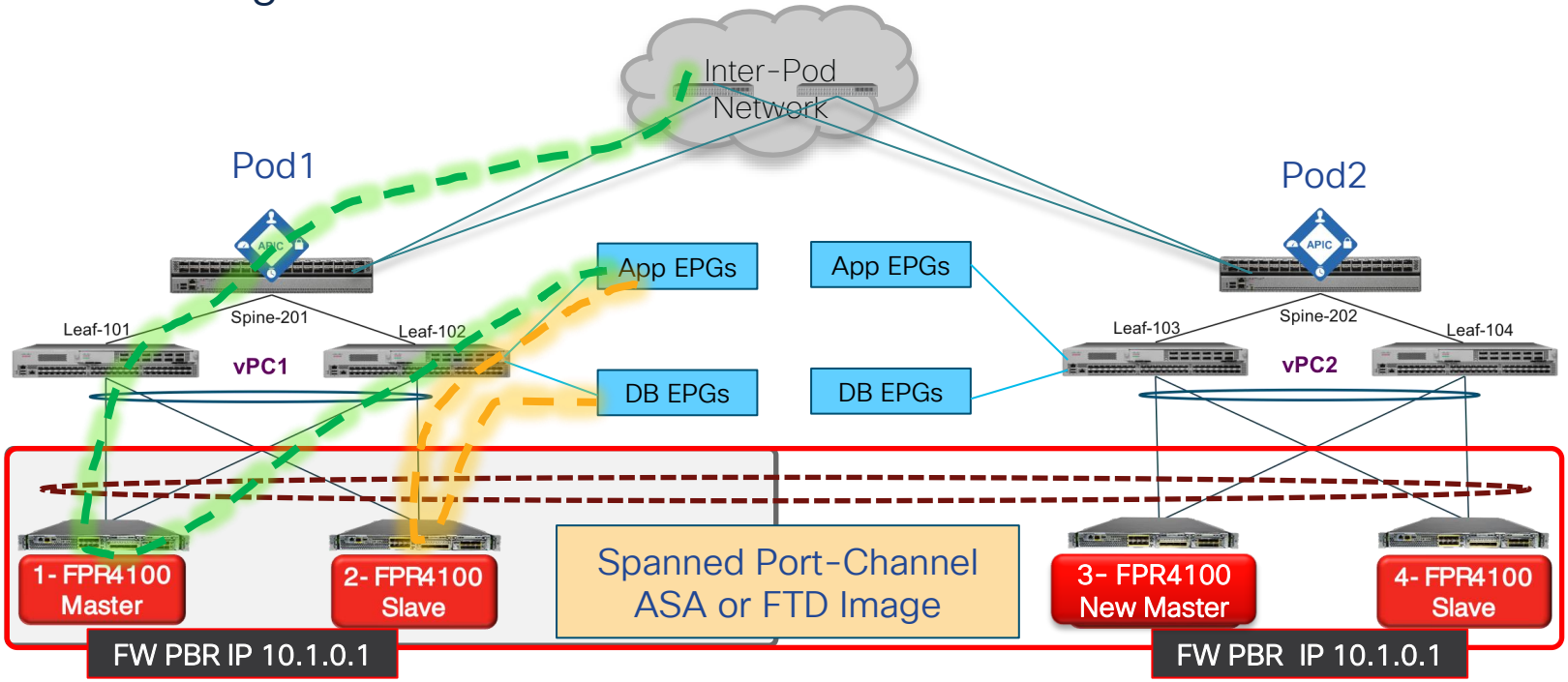
Firepower Cluster Resiliency

In case of single member failure of POD1



Firepower Cluster Resiliency

In case of single member failure of POD1

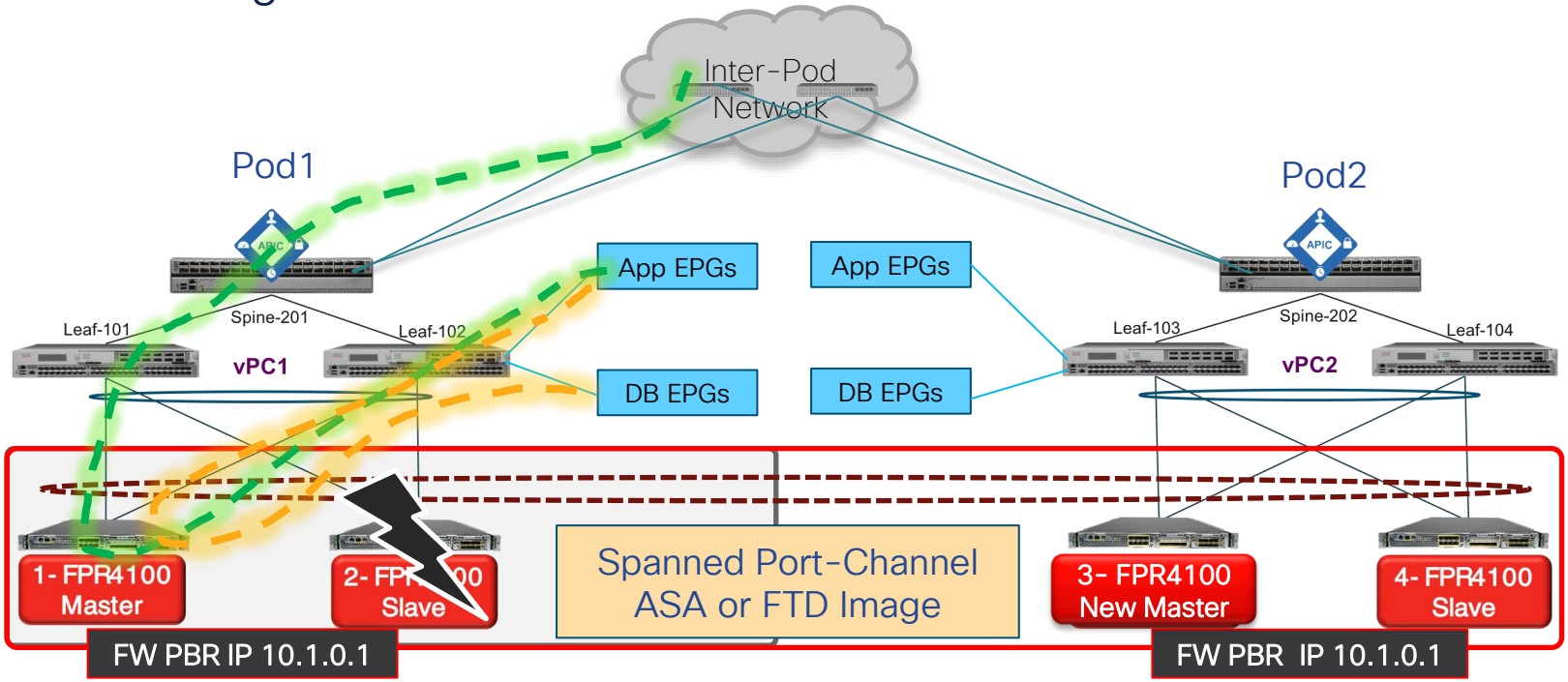


FTD load 60%

FTD load 61%

Firepower Cluster Resiliency

In case of single member failure of POD1

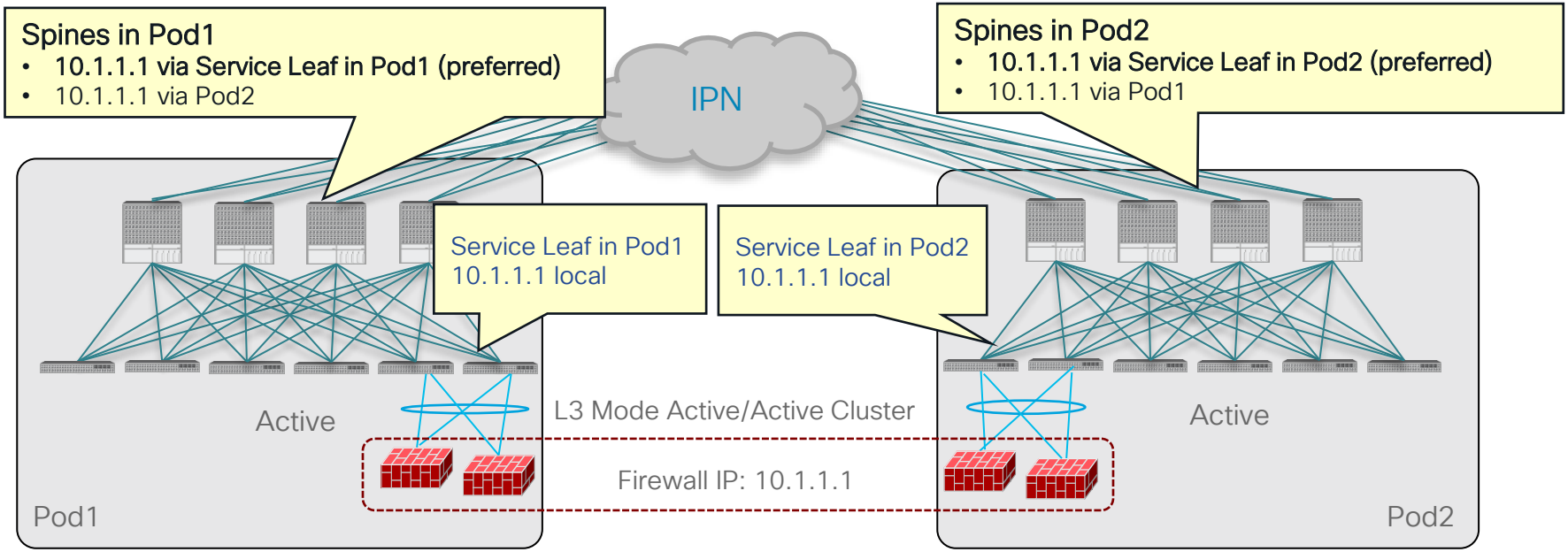


FTD load 121%

FTD load 0%

Active/Active cluster across pods

Anycast service



Should i tick Anycast Endpoint ?

L4-L7 Policy-Based Redirect - ftdv-03-eth5-gig-0-2

Properties

Name: ftdv-03-eth5-gig-0-2

Description: optional

Destination Type: L1 | L2 | L3

Rewrite source MAC: ☐

IP SLA Monitoring Policy: select an option

Oper Status: Enabled

Enable Pod ID Aware Redirection: ☐

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

Anycast Endpoint: ☐

Resilient Hashing Enabled: ☐

L3 Destinations:

IP	Destination Name	MAC	Redirect Health Group	Additional IPv4/IPv6
192.168.56.4		00:50:56:A1:AC:90		0.0.0.0

Should i Enable « Resilient Hashing» ?

L4-L7 Policy-Based Redirect - ftdv-03-eth5-gig-0-2

Properties

Name: ftdv-03-eth5-gig-0-2

Description: optional

Destination Type: L1 | L2 | L3

Rewrite source MAC: ☐

IP SLA Monitoring Policy: select an option

Oper Status: Enabled

Enable Pod ID Aware Redirection: ☐

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

Anycast Endpoint: ☐

Resilient Hashing Enabled: ☐

L3 Destinations:

IP	Destination Name	MAC	Redirect Health Group	Additional IPv4/IPv6
192.168.56.4		00:50:56:A1:AC:90		0.0.0.0

Should i Enable Pod Id Aware Redirection ?

L4-L7 Policy-Based Redirect - ftdv-03-eth5-gig-0-2

Properties

Name: ftdv-03-eth5-gig-0-2

Description: optional

Destination Type: L1 | L2 | L3

Rewrite source MAC: ☐

IP SLA Monitoring Policy: select an option

Oper Status: Enabled

Enable Pod ID Aware Redirection: ☐

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

Anycast Endpoint: ☐

Resilient Hashing Enabled: ☐

L3 Destinations:

IP	Destination Name	MAC	Redirect Health Group	Additional IPv4/IPv6
192.168.56.4		00:50:56:A1:AC:90		0.0.0.0

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

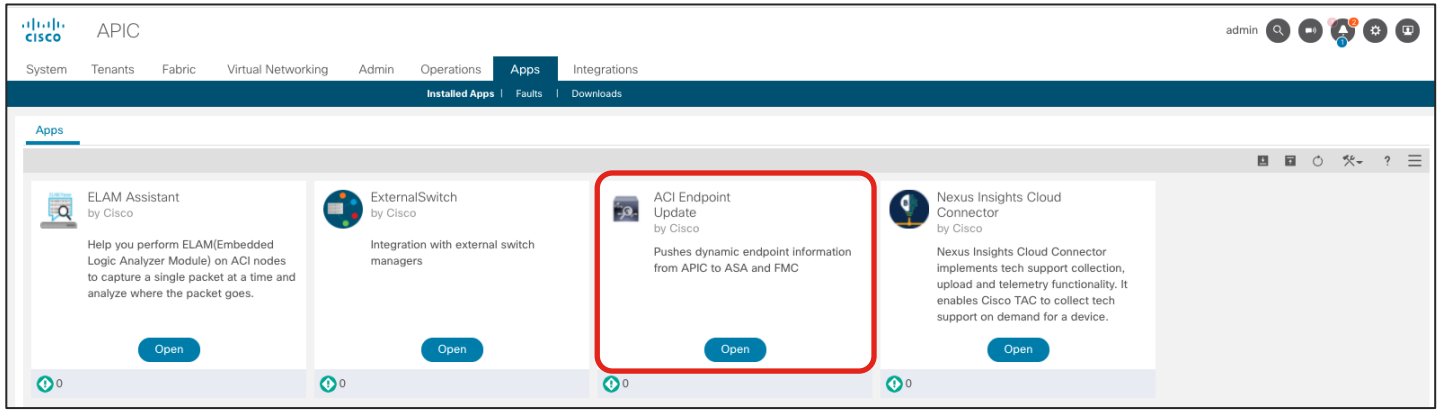
Add a Location IP Address

Add

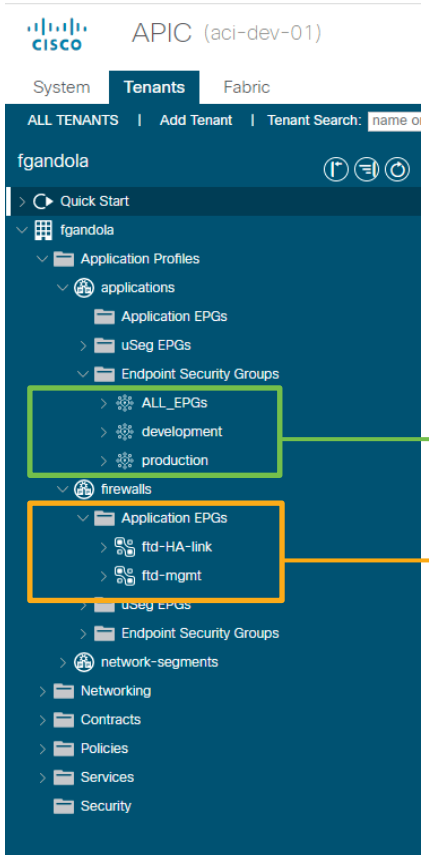
Attributes of the same type (for example, SGT) match the rule if any attribute is matched.
Attributes of different types match the rule only if all attributes are matched. More info

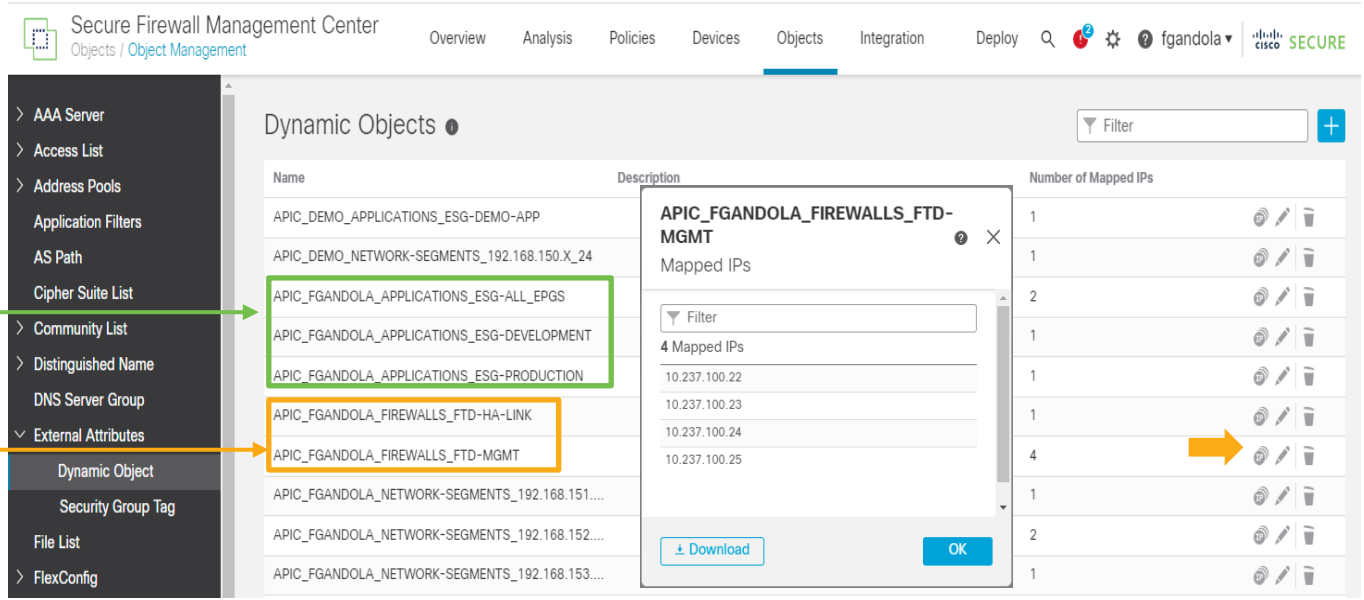
FMC App for APIC – FMC Endpoint Update

- 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

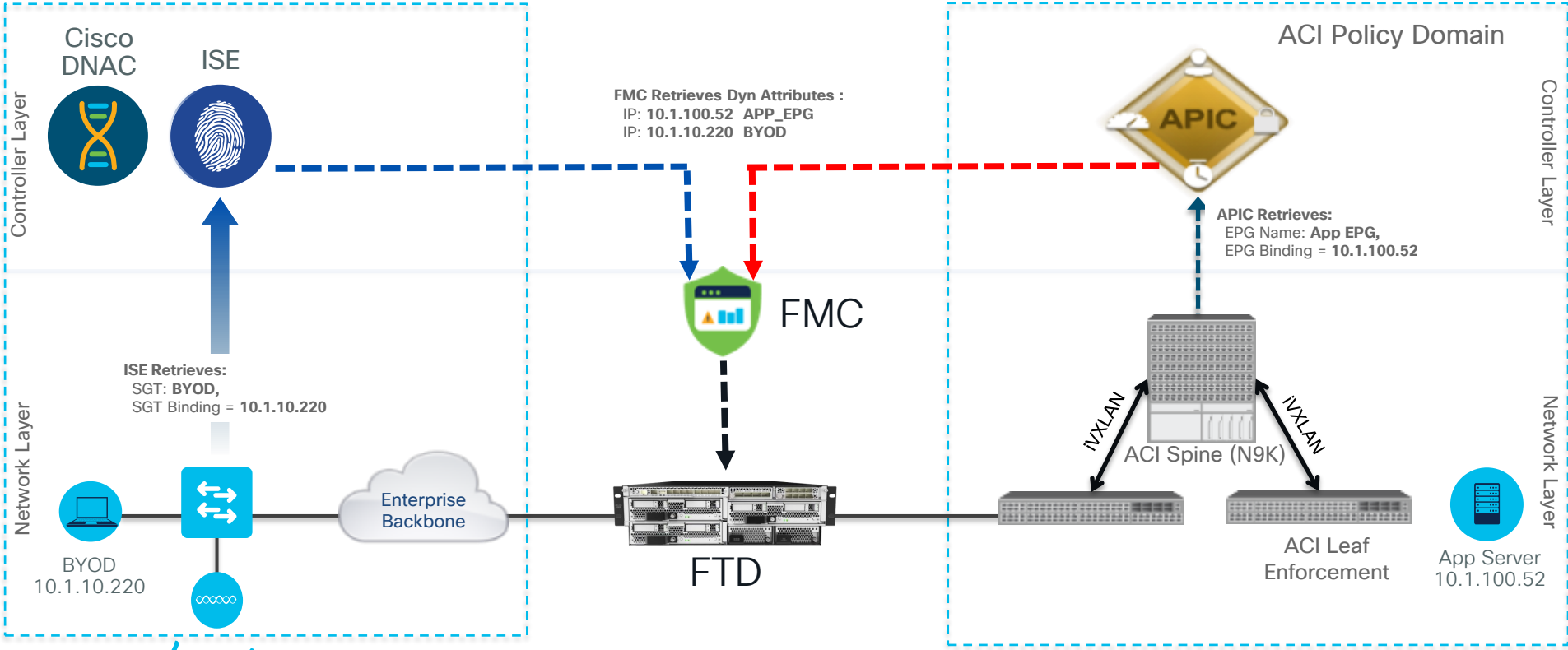


FMC Learns EPGs/ESGs as Dynamic Attributes



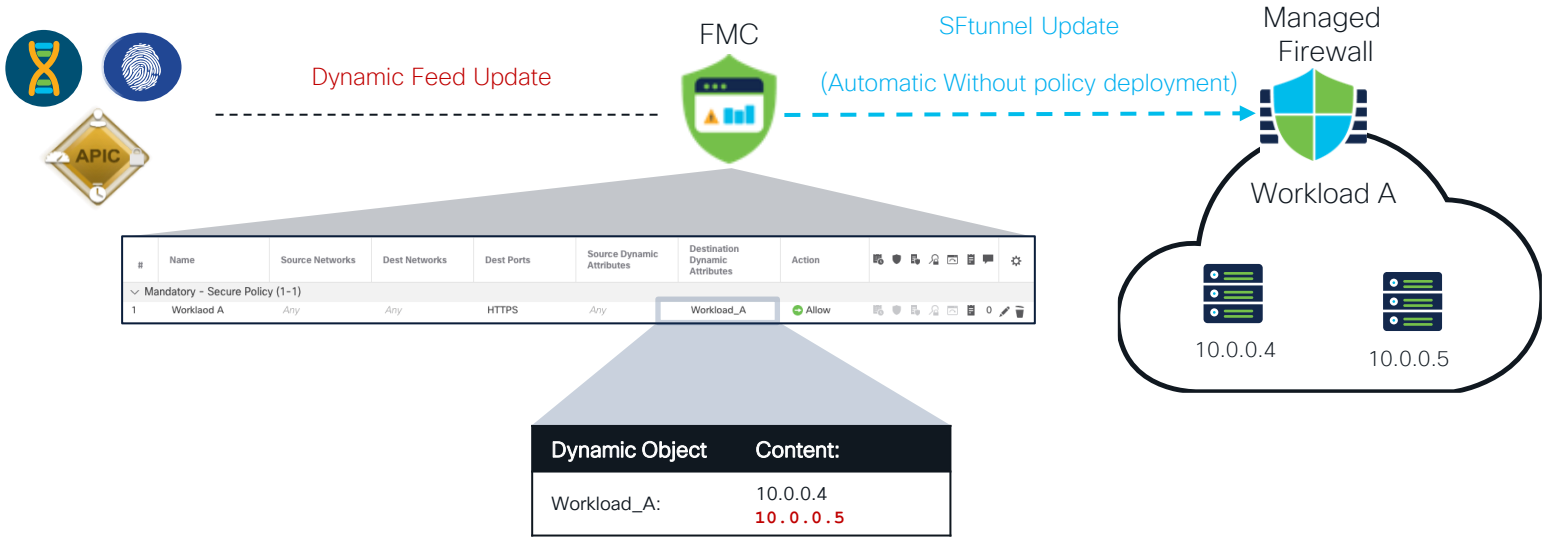


SGT/ACI Firepower Integration



Dynamic Objects in Action

Automatic Without policy deployment



Demo

Policy Editor | Secure Firewall Ma | APIC (10.237.97.182)

Not secure | https://10.237.97.182/#bTenants:fgandola|uni/tn-fgandola/ap-applications

APIC (aci-dev-01) — fgandola

System | Tenants | Fabric | Virtual Networking | Admin | Operations | Apps | Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | mgmt | fgandola | ylouis | ssharman

fgandola

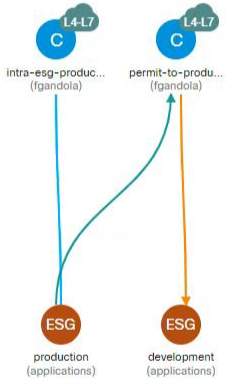
- Quick Start
- fgandola
  - Application Profiles
    - applications
      - Application EPGs
      - uSeg EPGs
      - Endpoint Security Groups
    - firewalls
    - network-segments
  - Networking
  - Contracts
  - Policies
  - Services
  - Security

Application Profile - applications

Summary | Topology | Policy | Stats | Health | Faults | History

Healthy

Contract | EPG | uSeg EPG | Any EPG | Baremetal | VMware | Microsoft | Red Hat | OpenStack | Kubernetes | Cloud Foundry | OpenShift | Layer 2 | Layer 3 | Layer 4-7



Relation Indicators

Configured | Operational

Show All | On Click

Show VRF on EPG:

Provider
Consumer
Intra EPG/ESG
Provider (from Master)
Consumer (From Master)
Intra EPG/ESG (from Master)
Master EPG/ESG

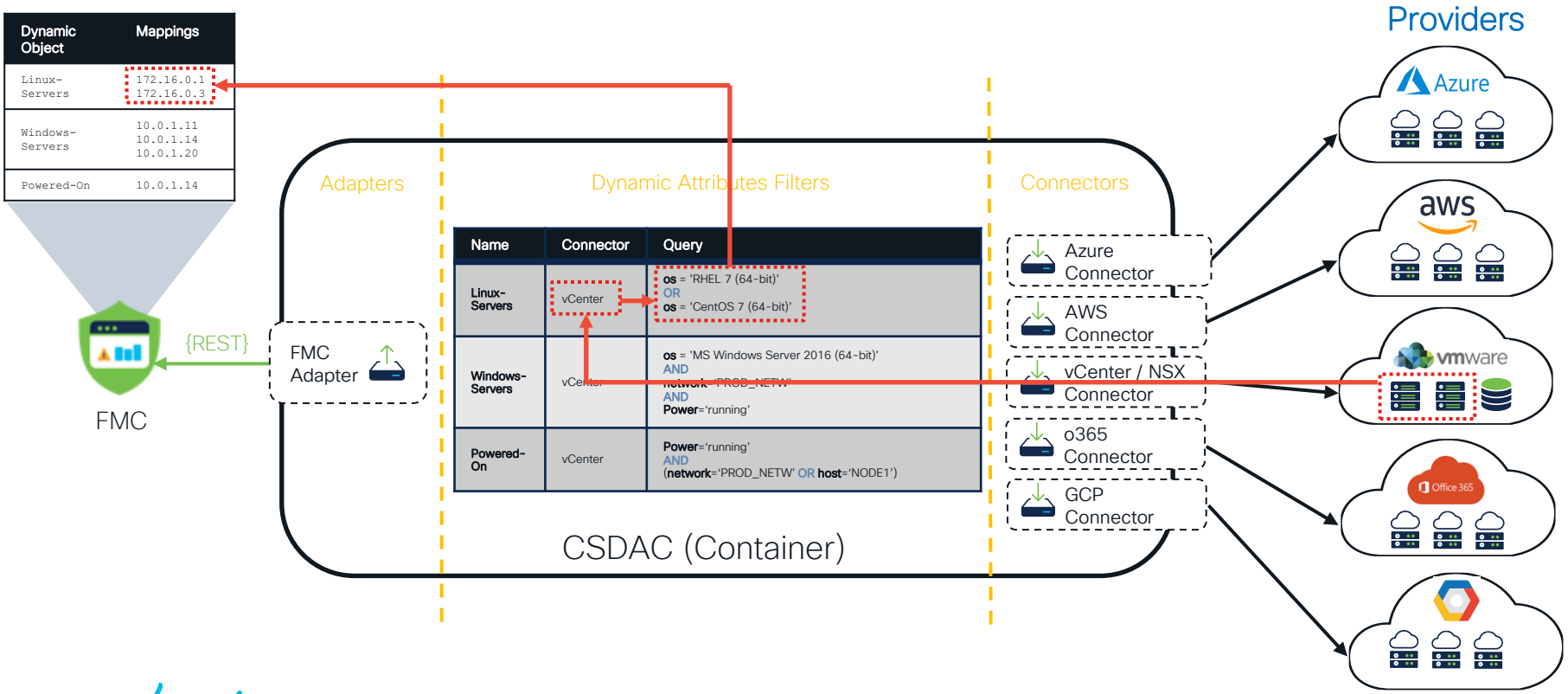
Cancel | Submit

Last Login Time: 2022-06-02T21:49 UTC+01:00

Current System Time: 2022-06-03T08:01 UTC+01:00

Cisco-FMCEndpoin....aci Canceled | Cisco-FMCEndpoin....aci | Show all

Architecture of the Dynamic Attributes Connector

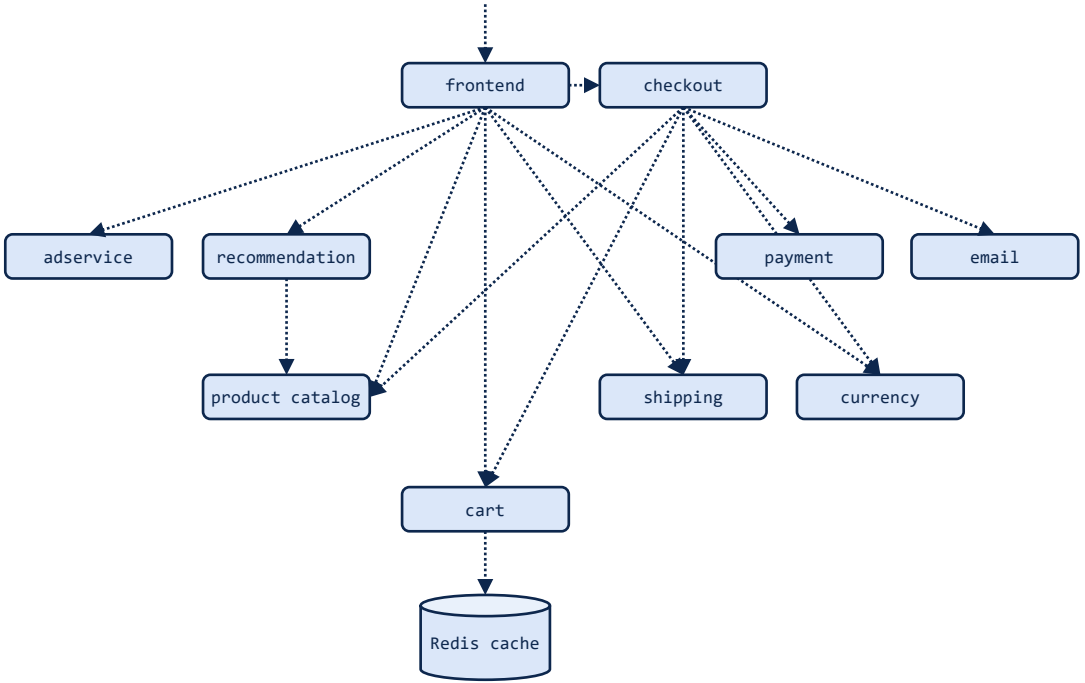


Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
>	Mandatory - Attribute-Based Policy (-)								
⌄	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		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		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

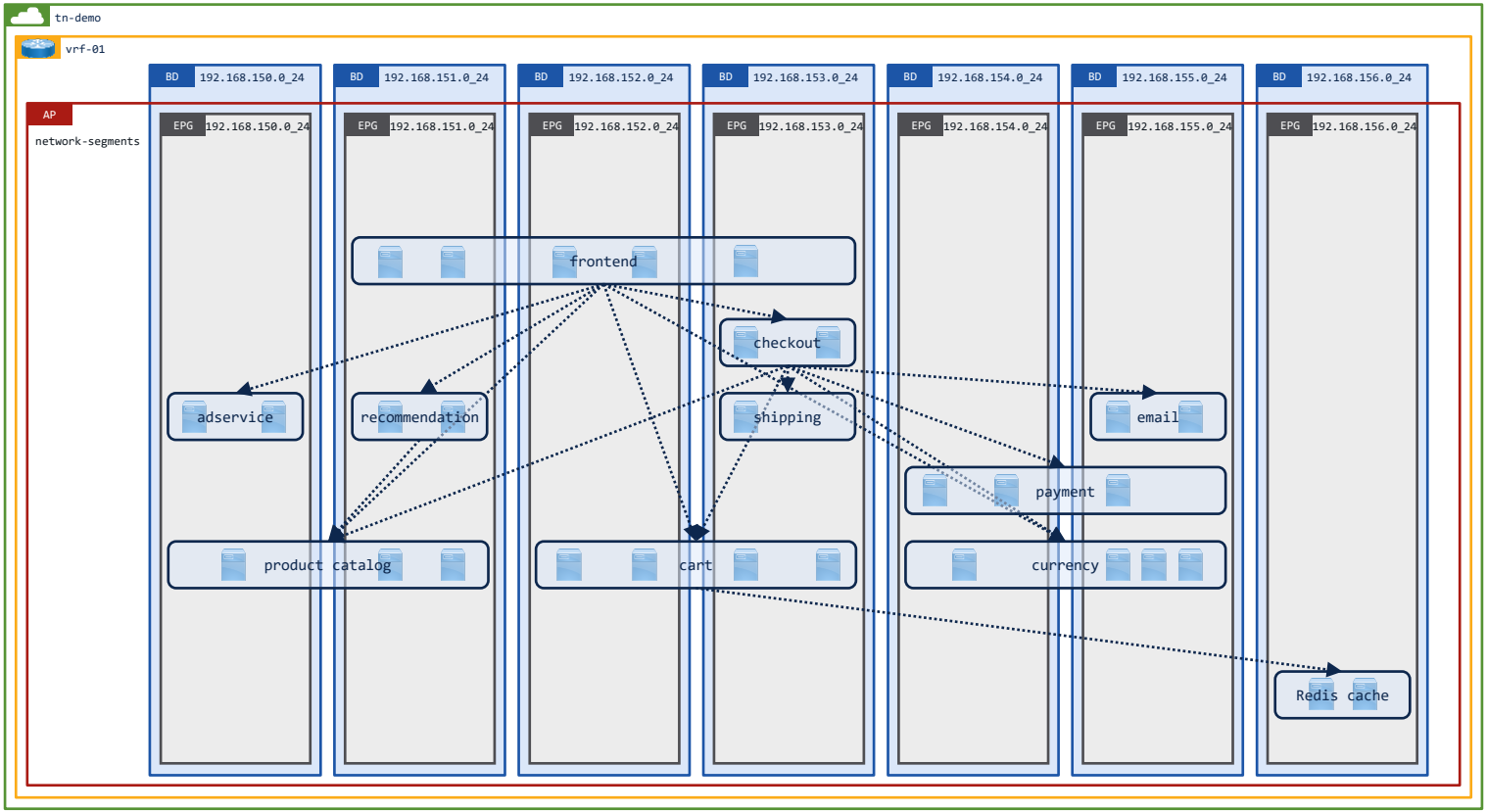
Online Boutique

https://github.com/GoogleCloudPlatform/microservices-demo

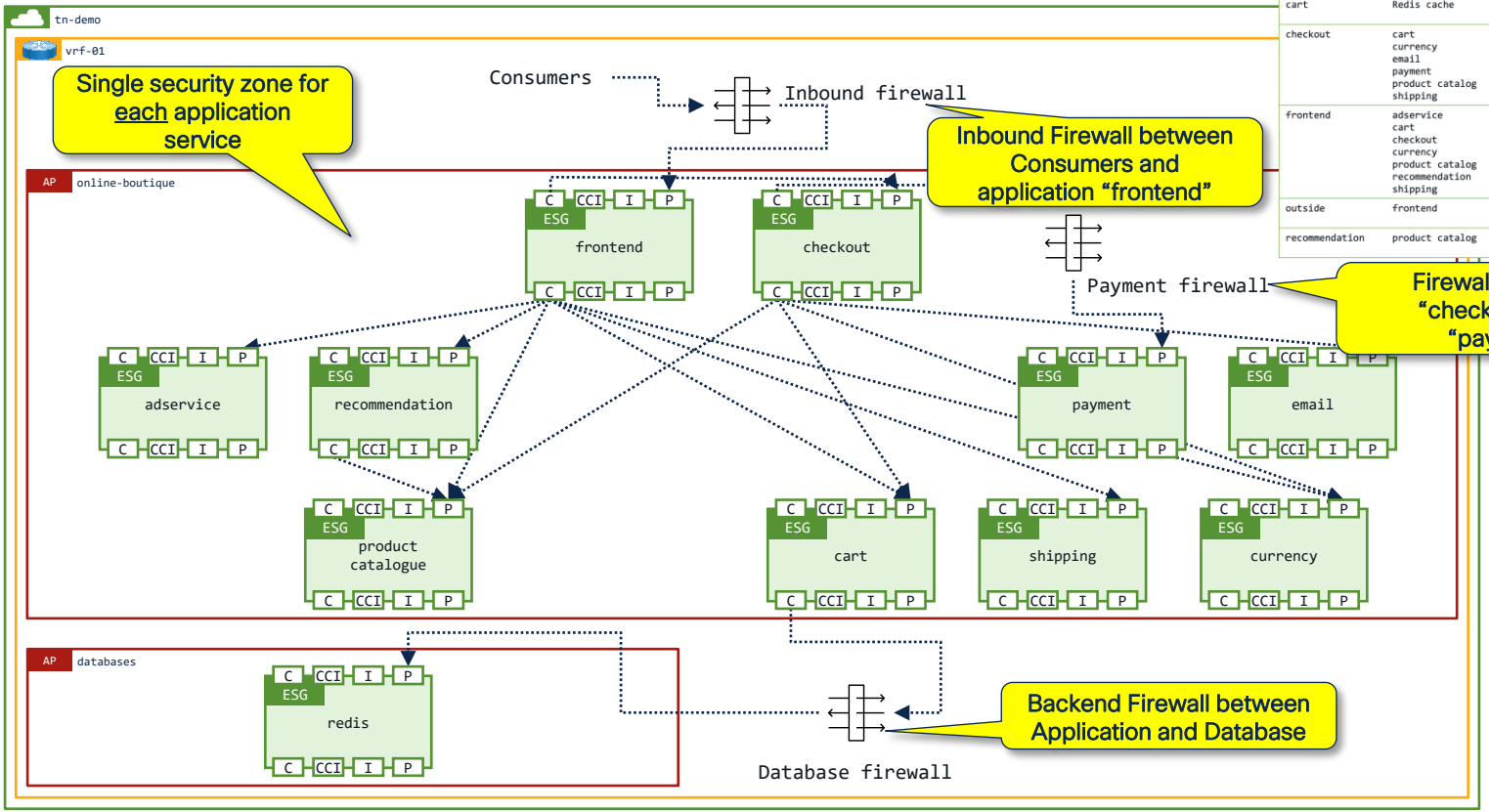


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP 5050 TCP 7000 TCP 3550 TCP 8080 TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Where is our application running…?

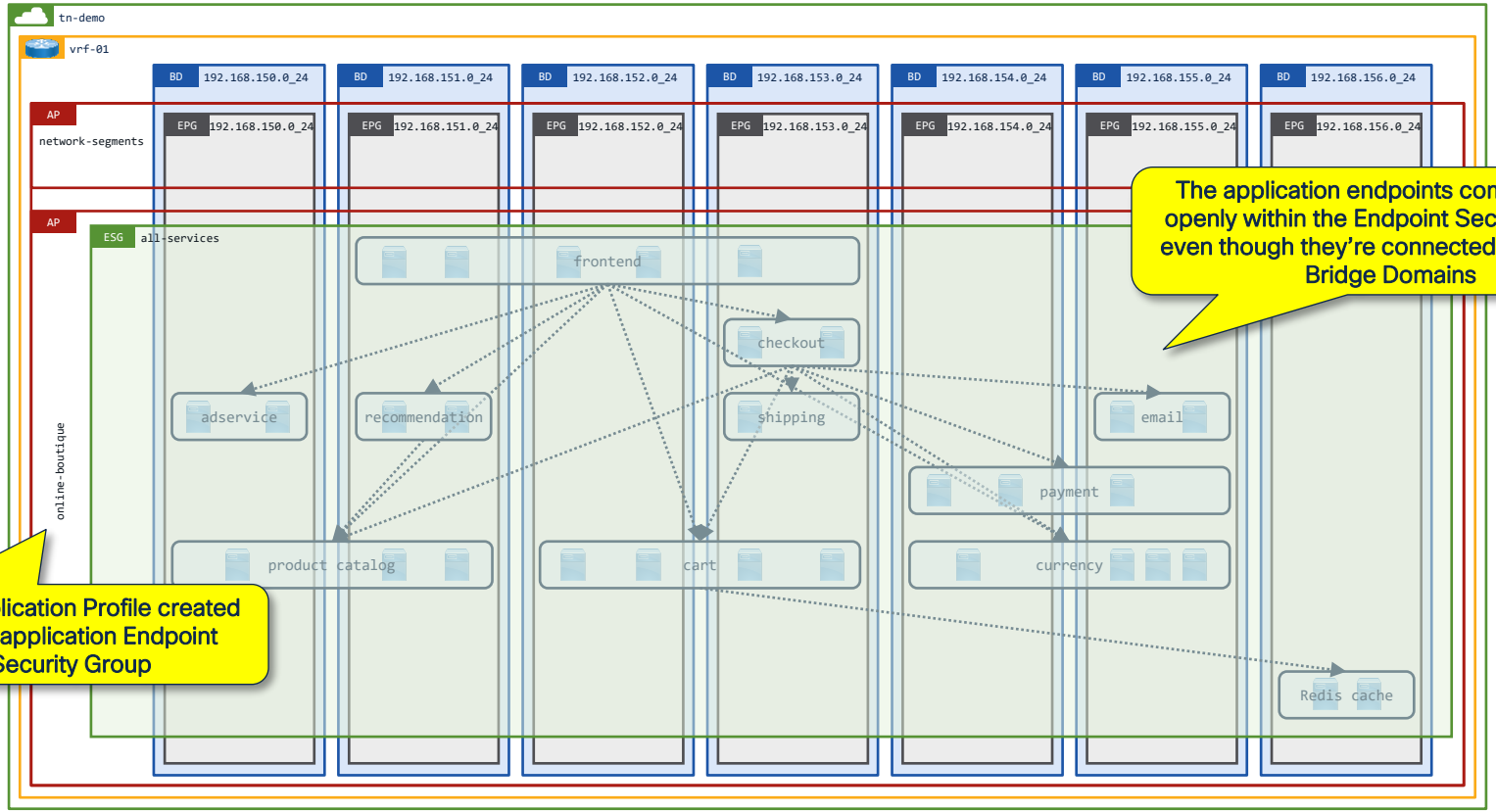


Tiered Security Approach



Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

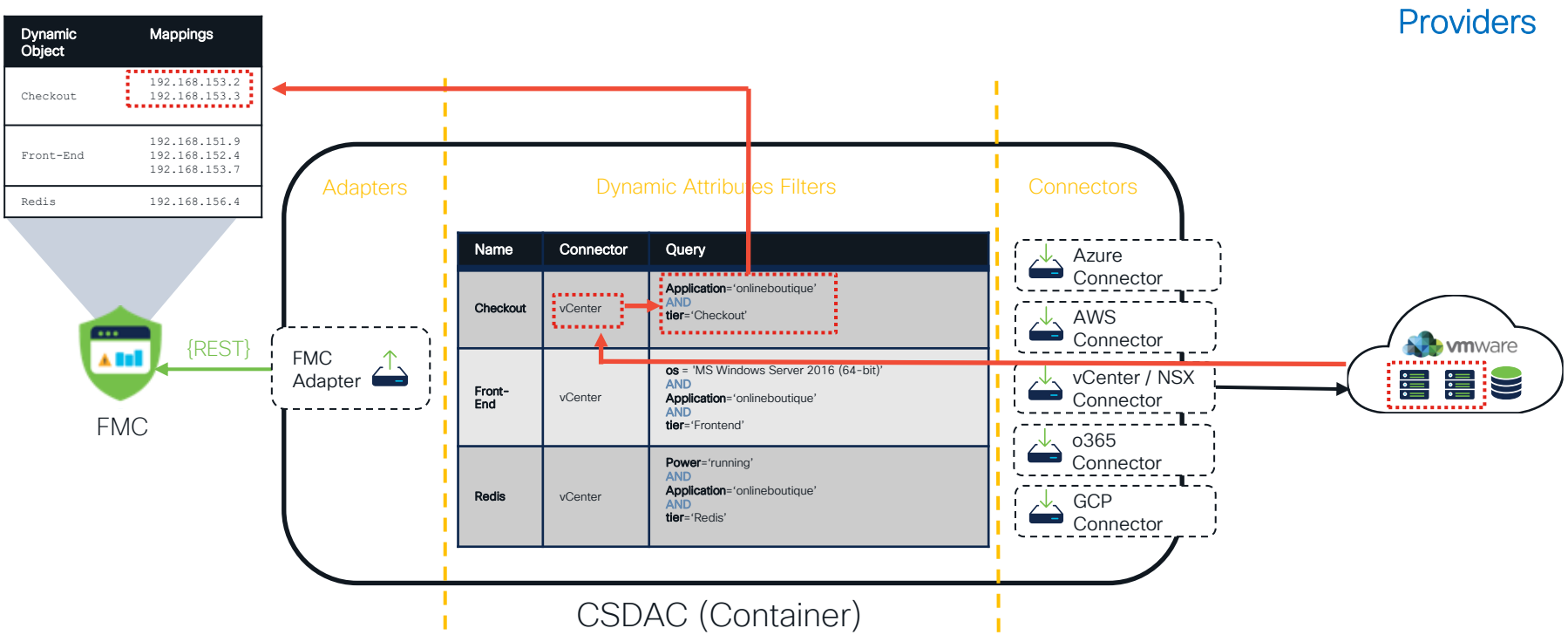
Let’s convert to “Application Centric” mode



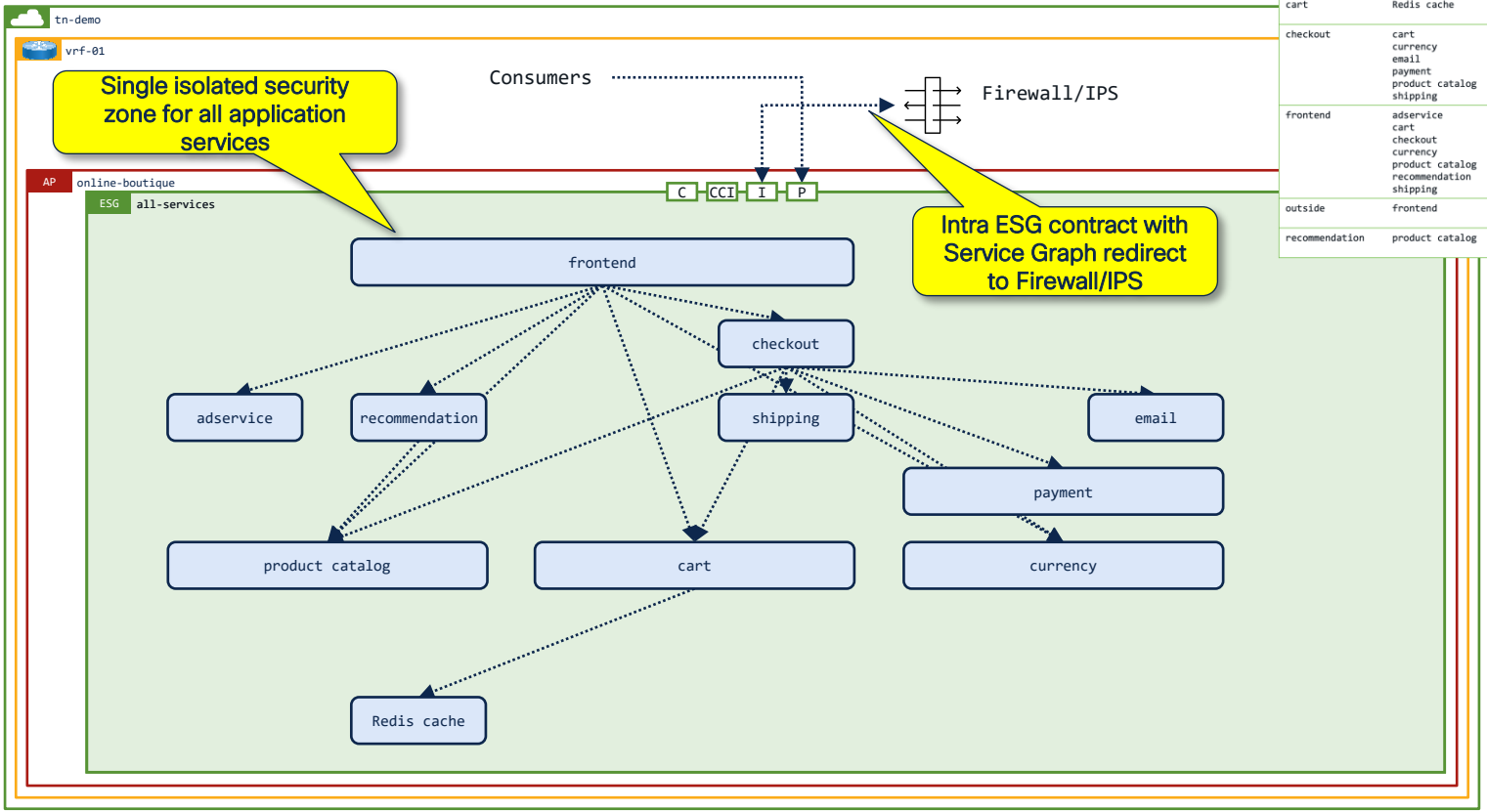
The application endpoints communicate openly within the Endpoint Security Group even though they’re connected to different Bridge Domains

New Application Profile created for the application Endpoint Security Group

Architecture of the Dynamic Attributes Connector



Control North/South Traffic and Intra-ESG

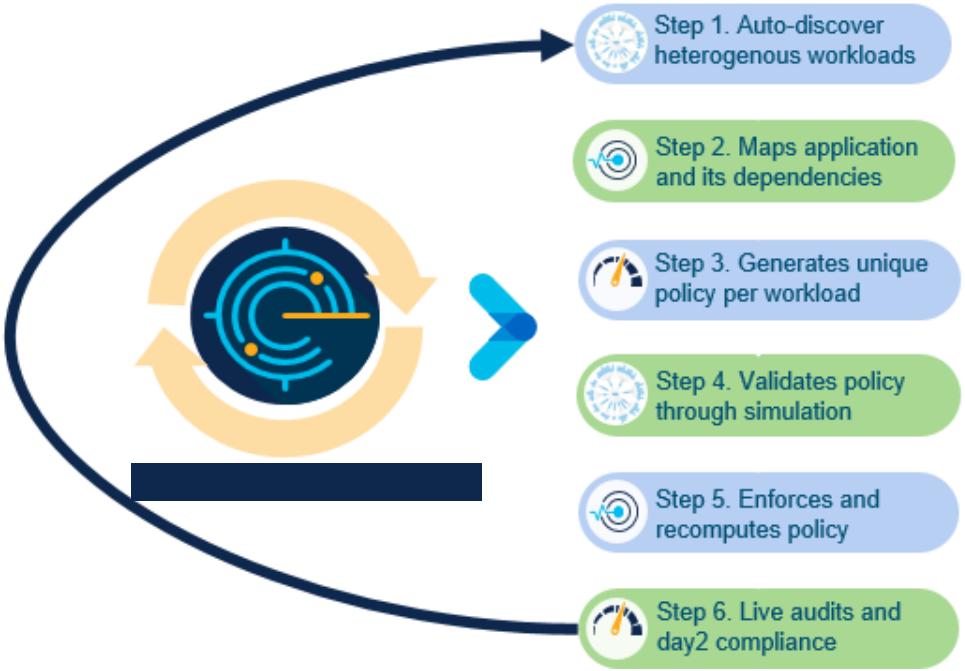


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Integration FTD +CSW (Cisco Secure Workload)

A practical approach to micro-segmentation

Full Life cycle policy Discovery, Management and Enforcement



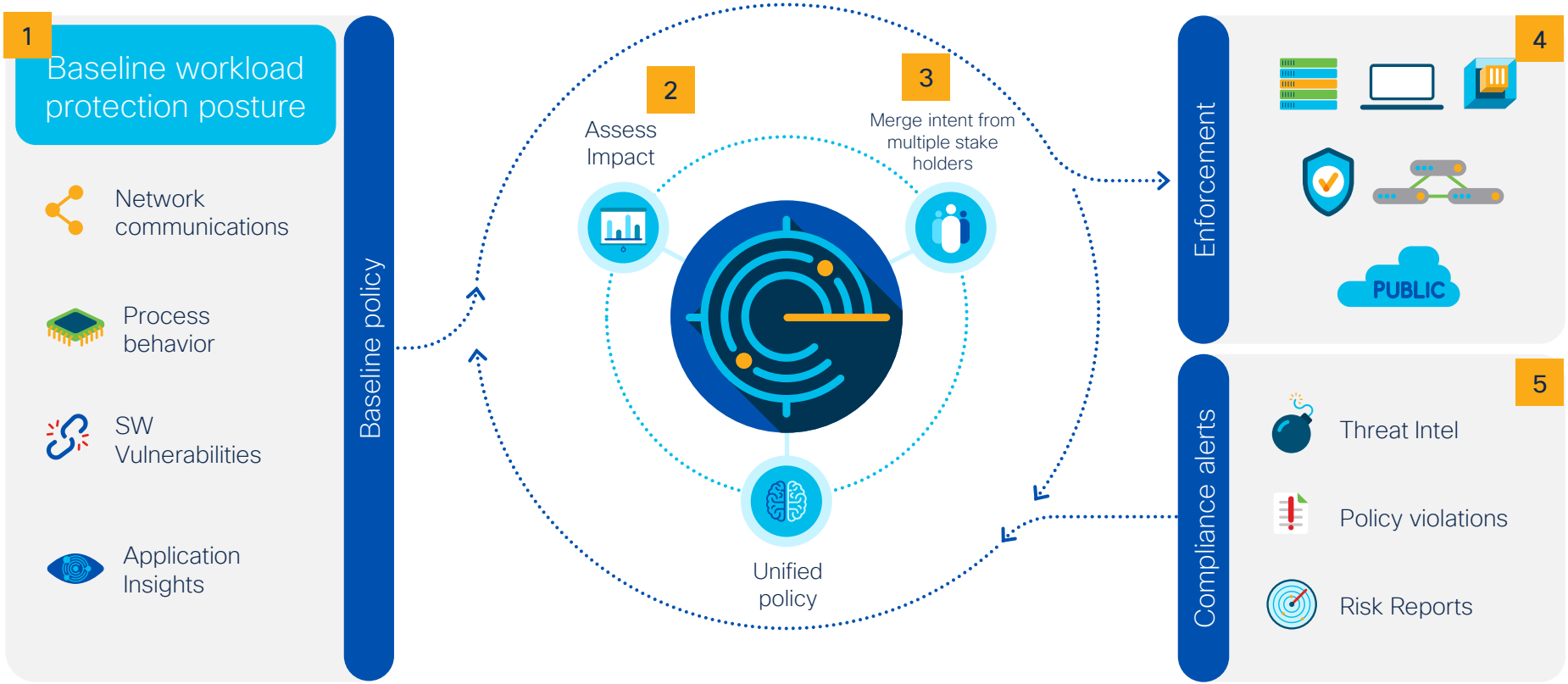
Reduction in Attack Surface

Faster Time to Value

Reduction in Security Rules

Cloud Workload Protection

Dynamic attribute & behavior-based security policy and segmentation

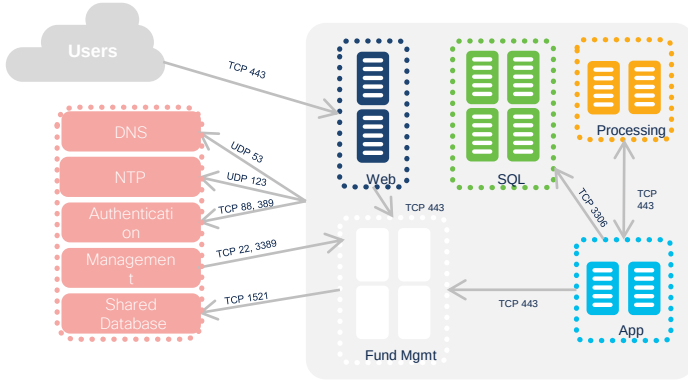


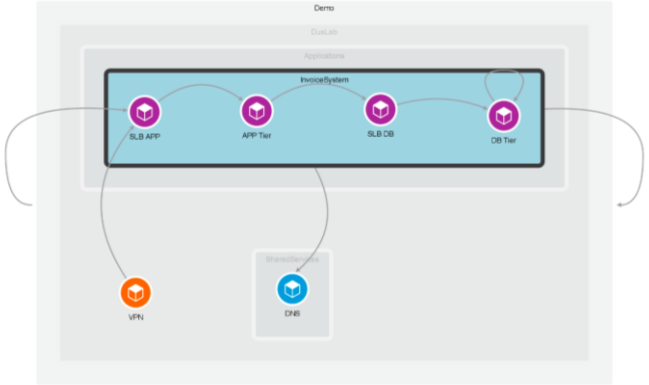
Understand your workloads

Automated discovery, clustering and policy generation

Baseline workload protection posture

- Network communications
- Process behaviour
- Labels



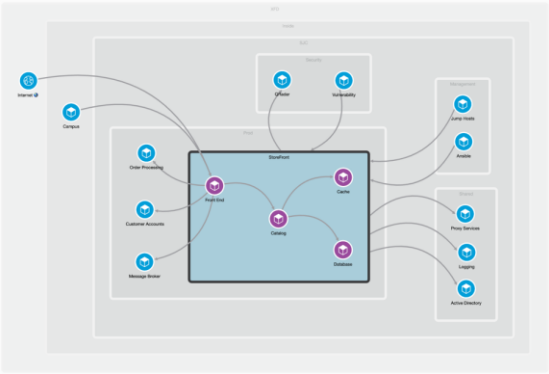


Absolute and Default Policies 13 | Catch All DENY | Grouped | Ungrouped

Rank	Priority	Action	Consumer	Provider	Protocols And Ports
Absolute	100	ALLOW	VPN	SLB APP	TCP : 1936
Default	100	ALLOW	VPN	SLB APP	TCP : 80 (HTTP)
Default	100	ALLOW	SLB DB	DB Tier	TCP : 3306 (MySQL)
Default	100	ALLOW	SLB APP	APP Tier	TCP : 8081
Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo	UDP : 123 (NTP) ...2 more
Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo : DusLab : SharedServices : DNS	UDP : 53 (DNS) ...1 more

Secure Firewall & Secure Workload: better together

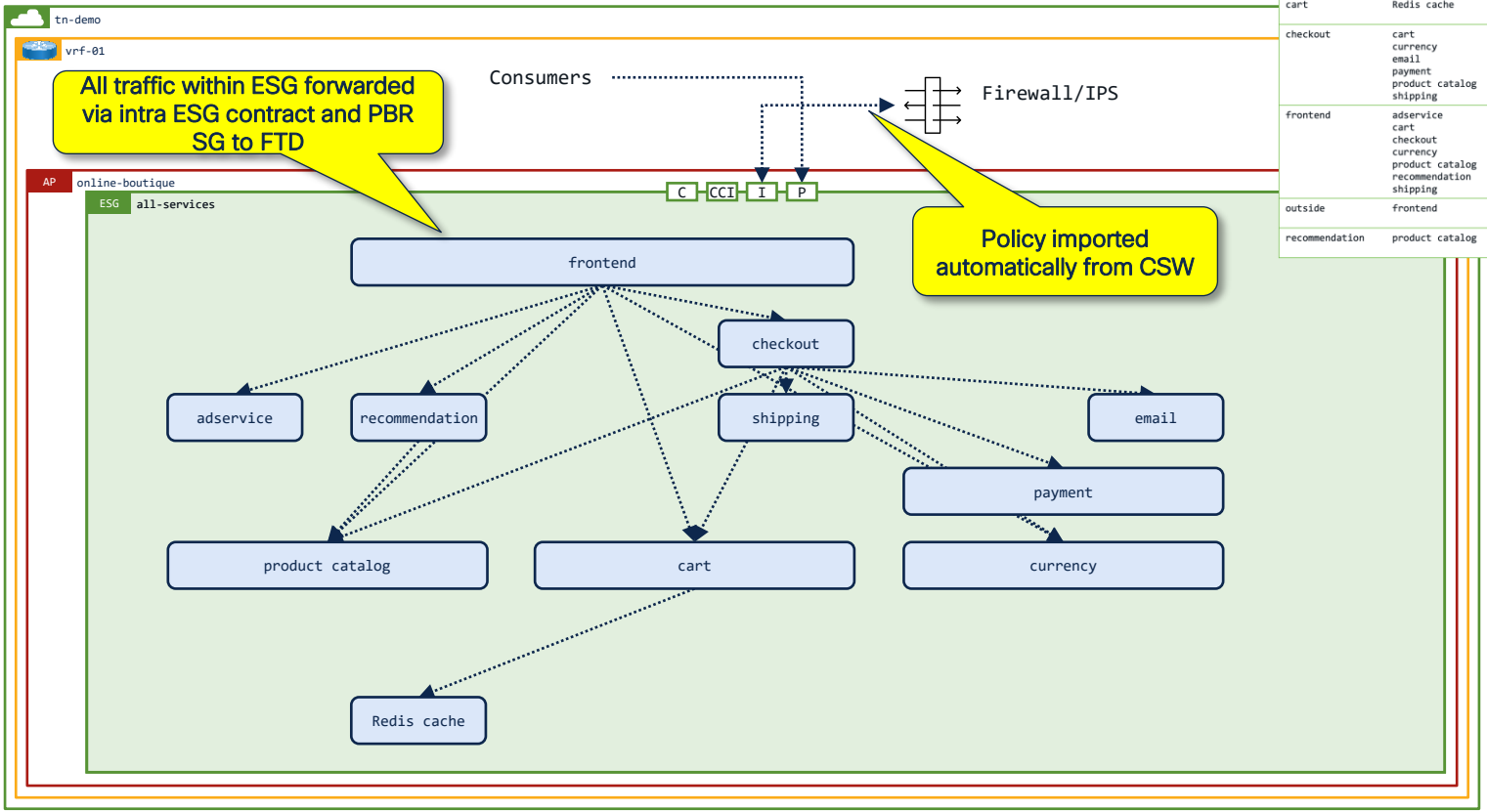
Visibility and Enforcement



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

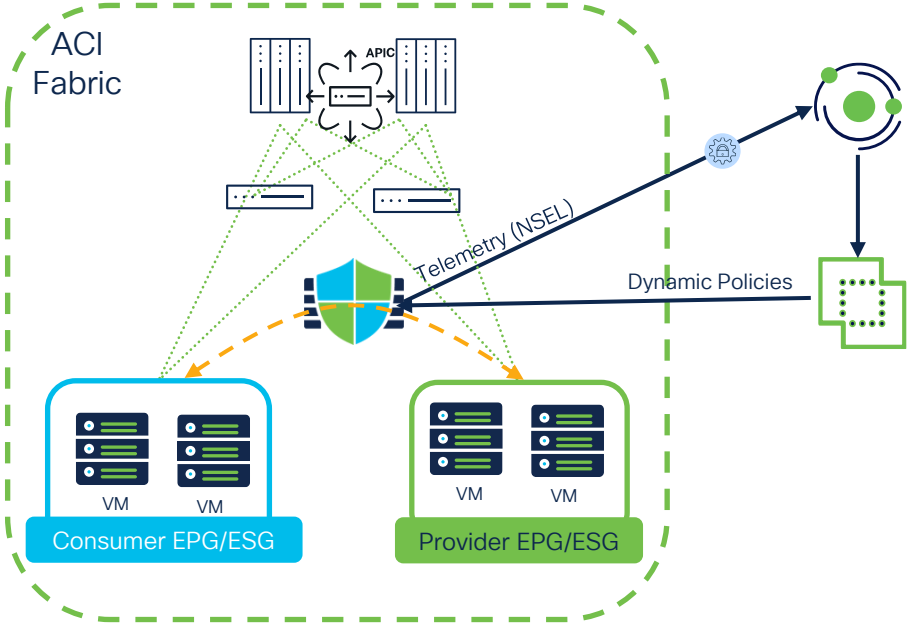
Enforce CSW policy with FTD in ACI



Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

ACI (SDN) Firewall Insertion

Network-Based Agentless Microsegmentation – SDN Insertion with Firewall



Service Graph PBR and Firewall Insertion Protection

- Flexible segmentation for workloads
  - Acceptable fine-grained
  - Reasonable
- Full visibility of flows with NSEL
  - FW inserted in datapath with service graph
  - Intra and inter EPG/ESG
- Protection at network level
  - Intra EPG/ESG (intra-app)
  - Inter EPG/ESG (inter-app)
- Allows policy multi-management
  - CSW owned-policies
  - FMC owned-policies
  - ACI owned-policies
- Convenient for network (ACI) and firewall engineers

Demo

Chrome File Edit View History Bookmarks Profiles Tab Window Help Thu 25. May 16:44

Cisco Secure Workload - Secu | Cisco Secure Workload - Conn | Cisco Secure Workload - Scop | Dashboard | Secure Firewall M | csw-truenas.dus.ciscolabs.co

Not Secure | https://plx.cisco.com/#/security-dashboard?t0=1685019600&filter_workloads=W10-&scope_id=619fccbb755f024e84f43c45

vSphere Web Client | Visibility | Imported | SRC- APJC | SRC- EMEAR | SRC - US | Attendee Resourc... | TSA Opp | Install Python on... | e-tron Charging S... | Miles & More Onli... | Tetration | Security Architect...

Cisco Secure Workload

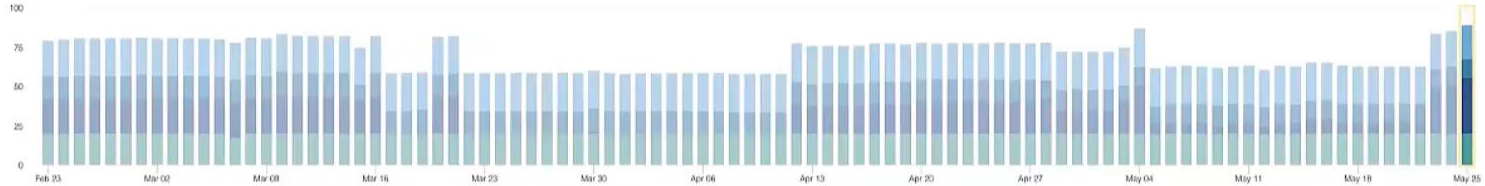
Demo | cisco SECURE

Your license usage is out of compliance. Please login to Cisco Smart Software Manager account for more details.

Security Dashboard

SCOPE SECURITY SCORE | May 25, 2023 | Demo

Filter Workloads | Adjust Weights

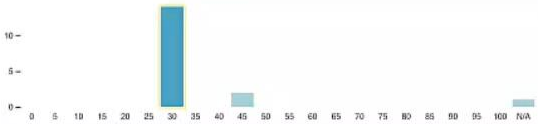


SCORE BREAKDOWN

Vulnerability Score	Process Hash Score	Attack Surface Score	Forensics Score	Network Anomaly Score	Segmentation Compliance Score
32	91	56	99	100	96

Workload Score Distribution

17 total



Workloads	Score
oshift-hnrqf-worker-r4h2c	30
oshift-hnrqf-worker-qk8x4	30

Vulnerability Score

May 25 3:00pm

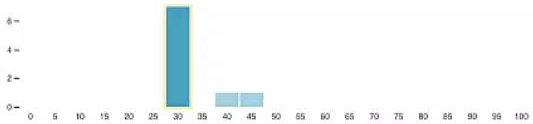
Demo

Average score, 16 workloads (1 N/A)

Hourly scores - May 25, 2023

Child Scope Scores

9 descendants of Demo with scores



Scopes	Score
Demo:DusLab:RHOCP4.9	30
Demo:DusLab:RH Openshift	30

Cisco Secure Workload

Secure Workload

Tetration

Site

Attention: We strongly recommend you register Secure Workload cluster with a Smart Account on Cisco Smart Software Manager. The evaluation period will expire in 90 days. Take action now.

Vulnerabilities

CVSS V2 DISTRIBUTION | Tetration

Access Complexity

Access Vector

Authentication

Availability Impact

Confidentiality Impact

Integrity Impact

Severity

0 Remotely Exploitable Low Complexity

13 Remotely Exploitable Higher Complexity

0 Locally Exploitable Low Complexity

0 Locally Exploitable Higher Complexity

0 Critical Severity

2 High Severity

11 Medium Severity

0 Low Severity

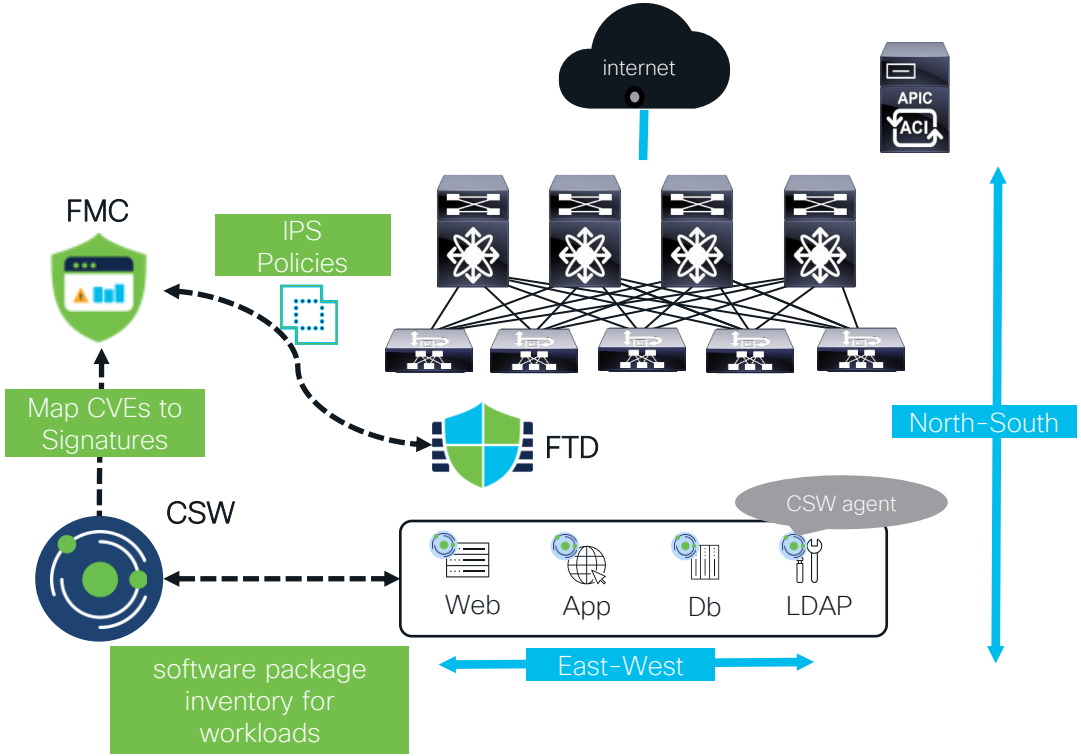
Access Vector (v2) = NETWORK and not Access Complexity (v2) = LOW

Filter

CVEs 13 | Packages 14 | Workloads 15 | Pods 0

CVE	OS	Year	Score (v2)	Score (v3)	Severity (v2)	Base Severity (v3)	Access Vector (v2)	Access Complexity (v2)	Authentication (v2)	Confidentiality Impact (v2)	Integrity Impact (v2)	Availability Impact (v2)
CVE-2017-10784	centos	2017	9.3	5.4	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE
CVE-2017-17405	centos	2017	9.3	6.3	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE
CVE-2019-8324	centos	2019	6.8	7.2	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2020-36385	centos	2020	6.8	7.8	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2017-0902	centos	2017	6.8	7.5	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2020-8625	centos	2020	6.8	8.1	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2018-1000074	centos	2018	6.8	7.8	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2018-16396	centos	2018	6.8	5.9	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL

Virtual patching - Cisco Secure Firewall



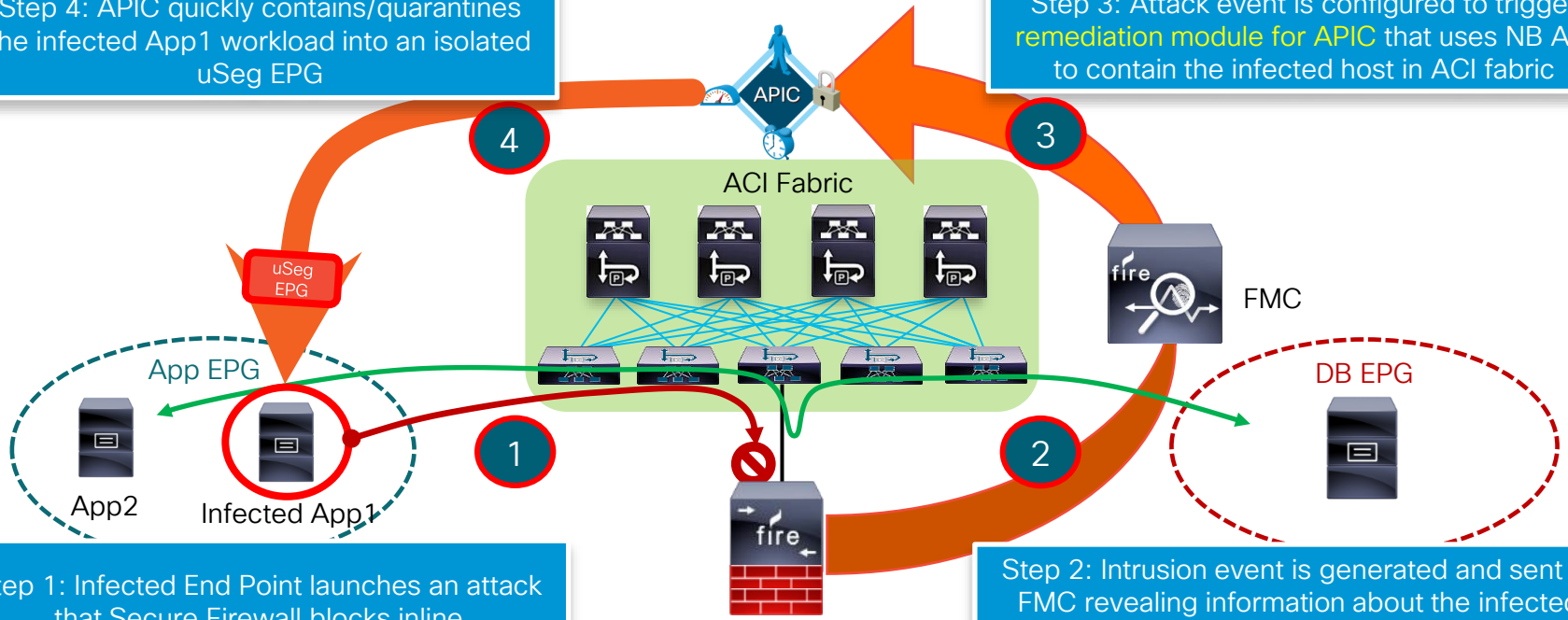
- Secure Workload agents collects CVE data from workloads
- Publish specific CVE data to Firewall Management Center
- Use Firewall recommendations to generate precise IPS policy
- Apply precise IPS policy to protect against CVE exploits

Remediation Module

FMC to APIC Rapid Threat Containment

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

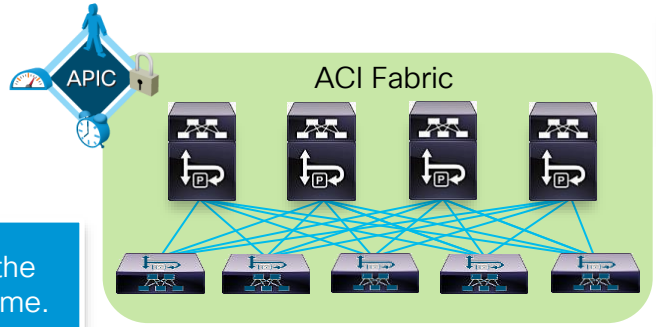
Step 3: Attack event is configured to trigger remediation module for APIC that uses NB API to contain the infected host in ACI fabric



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

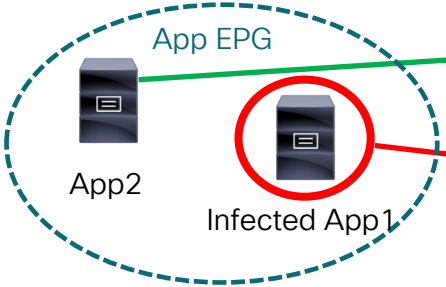
Contract Based Rapid Threat Containment

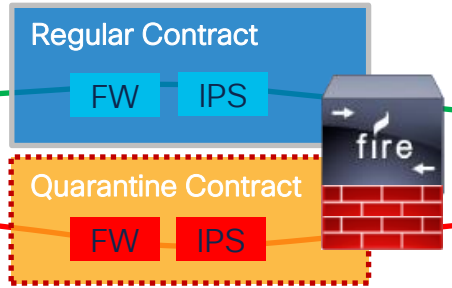


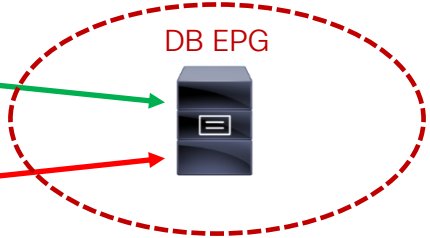
Remediation module for APIC triggers switchover to **quarantine contract**

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

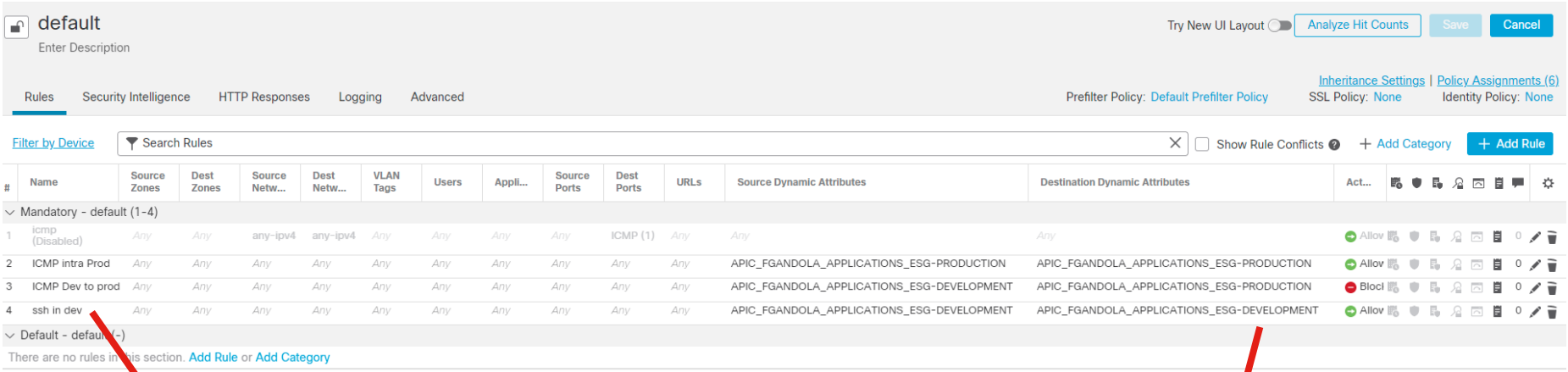
Cancel Save

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

Key Takeways

- Ease of Service Insertion with PBR brings new capabilities for more dynamic security
- Dynamic Groups and CSDAC really helps keeping coherent and consistent enforcement
- Clustering in Multipod offers a real Active-Active stateful solution for environment with potential asymmetric traffic
- Integration with CSW helps separating duty of Security team by automating the creation of dynamic policies

The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go