



The bridge to possible

# Tři způsoby segmentace DC

Martin Diviš, Technical Solution Engineer

**Microsegmentation** is an approach that enables security architects to construct network **security zones** boundaries **per machine** in data centres and cloud deployments to **segregate** and secure workloads **independently**.

It is now also used on the client network as well as the data center network.

# Segmentace – o čem budeme mluvit?

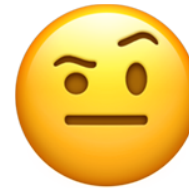
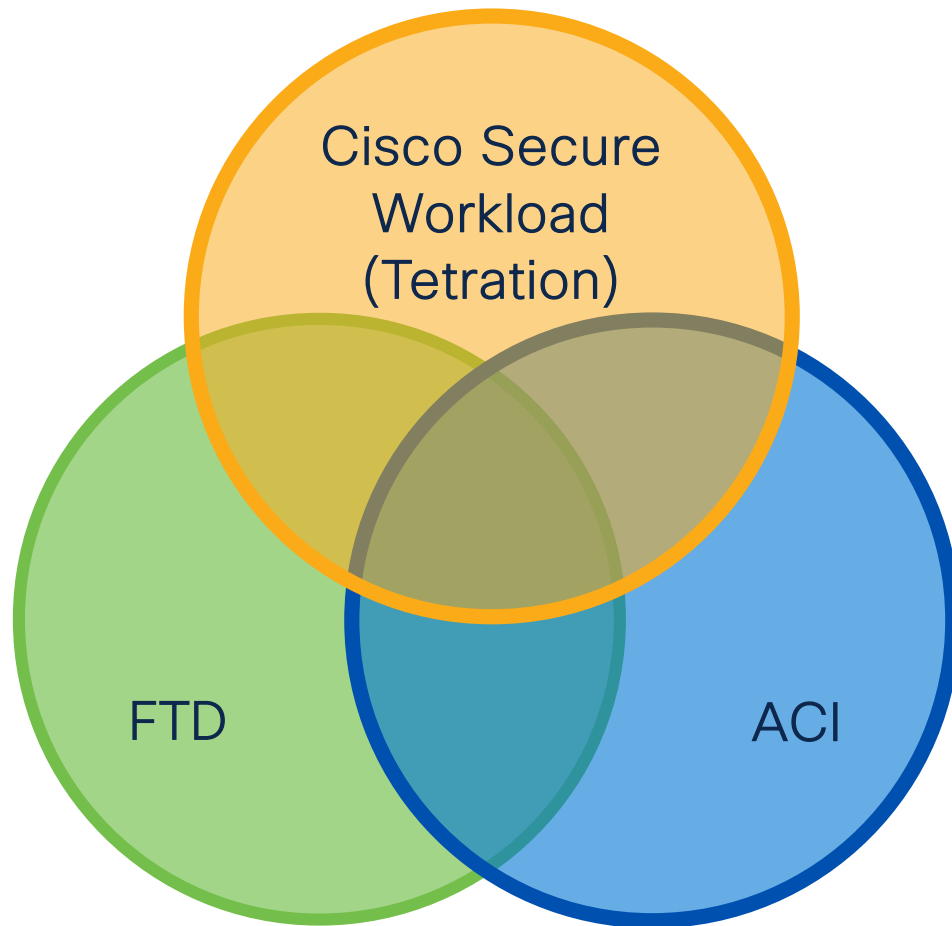
## Policy

- Test  Prod
- any:any  192.168.1.10:443
- Orders  IT Management
- any  any

## Enforcement

- ACLs
- ACI contracts
- FW rules
- Linux IP tables
- Windows FW rules

# Na čem budeme stavět?

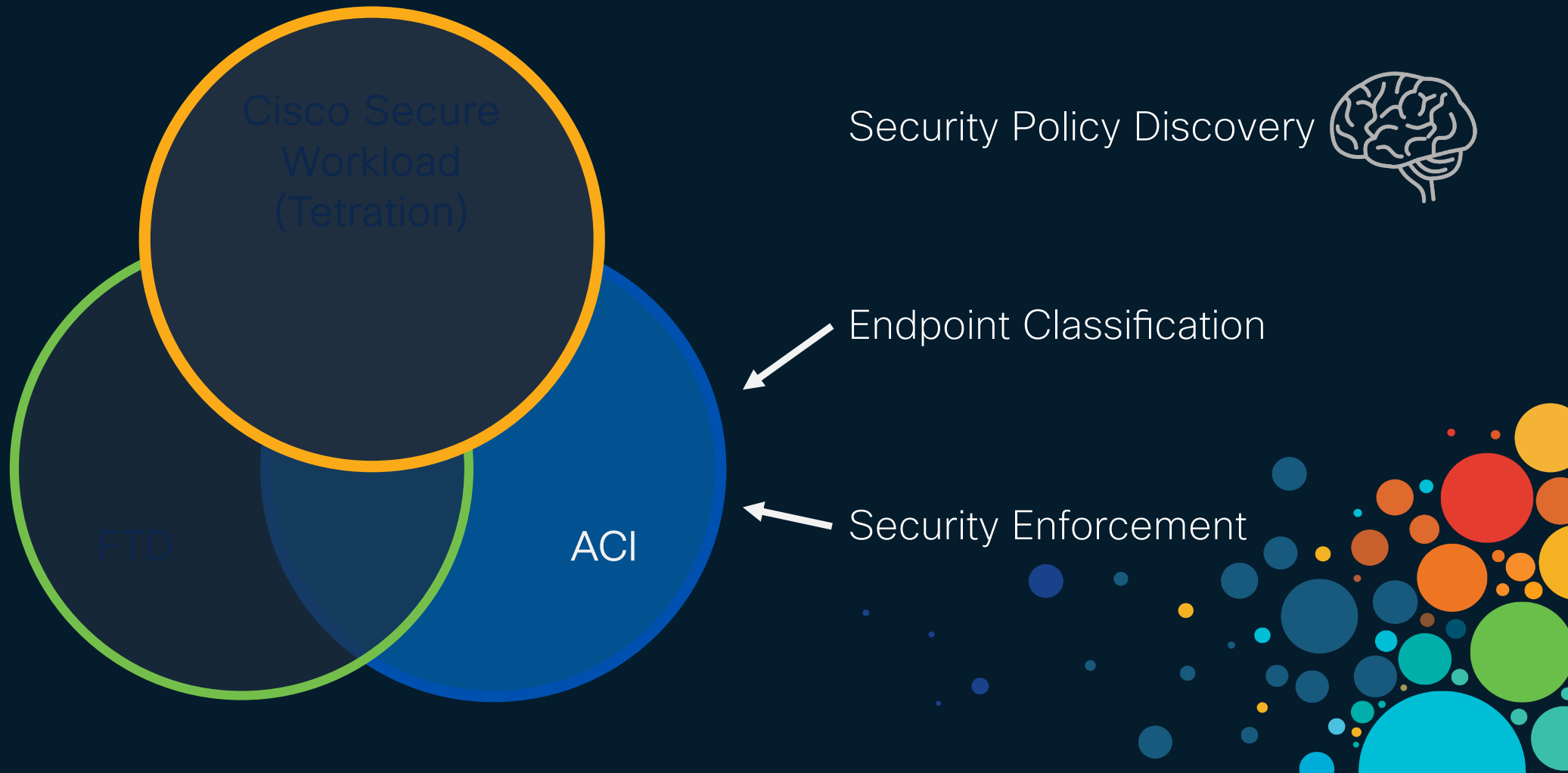


Tohle všechno potřebuju?

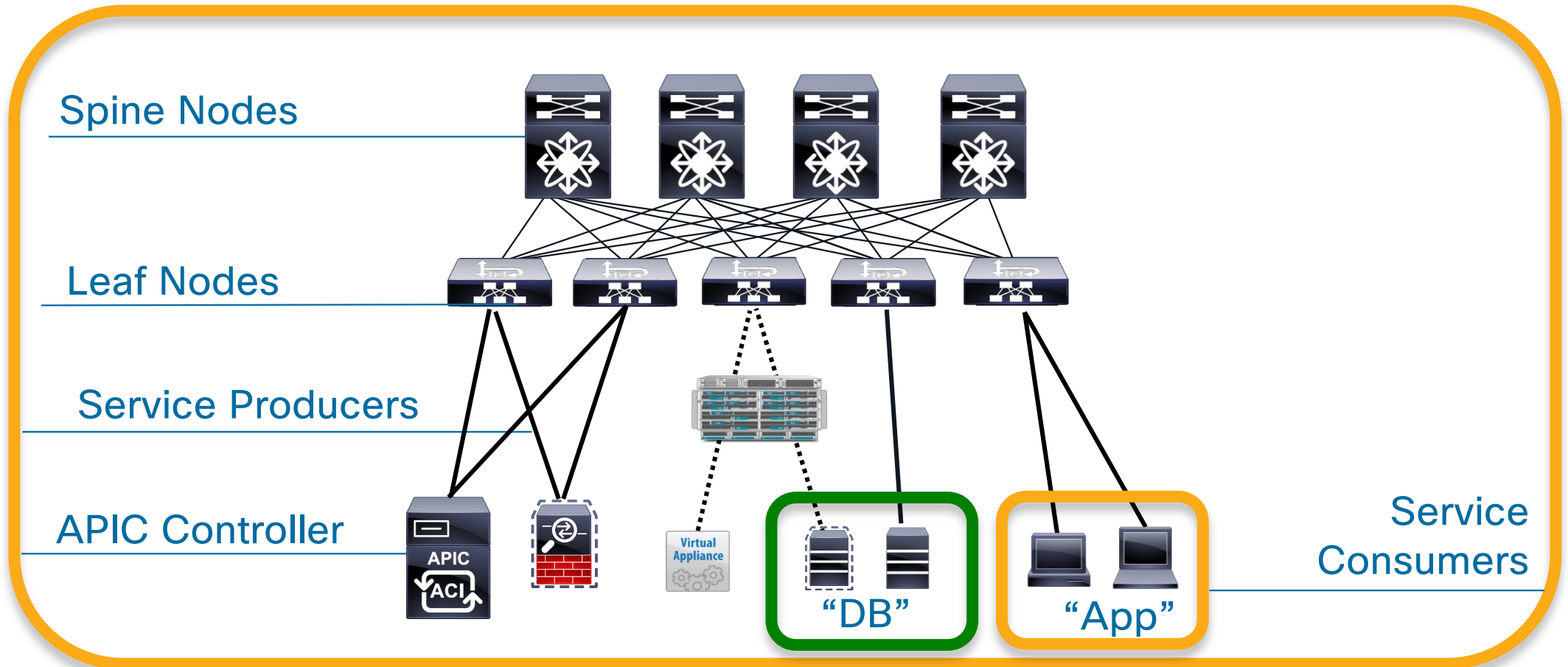


Ne, jen to, co mi dává smysl

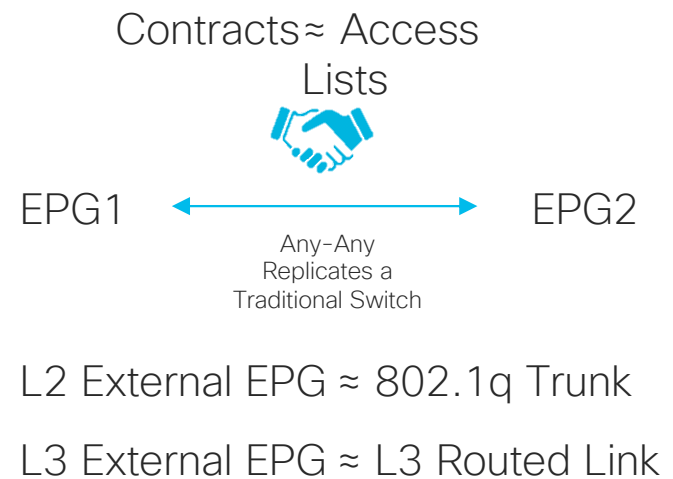
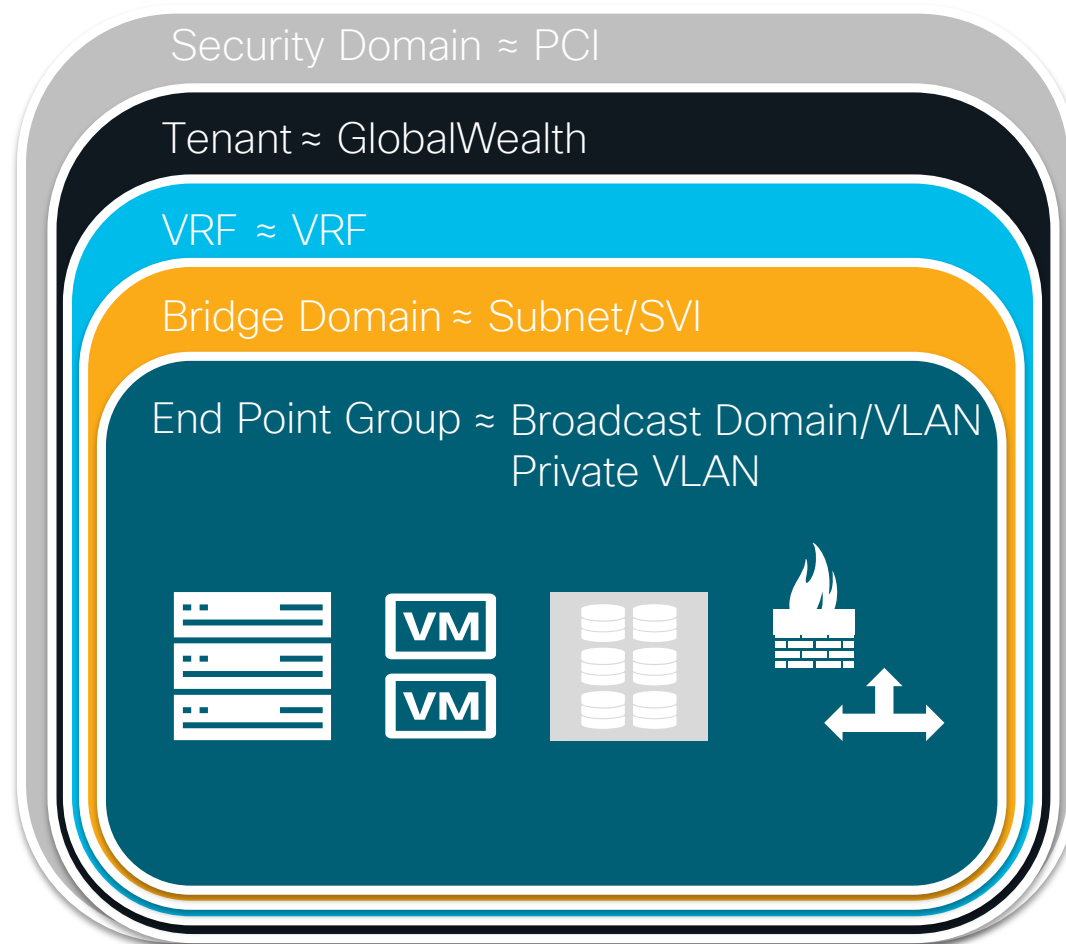
# Secure Network with ACI



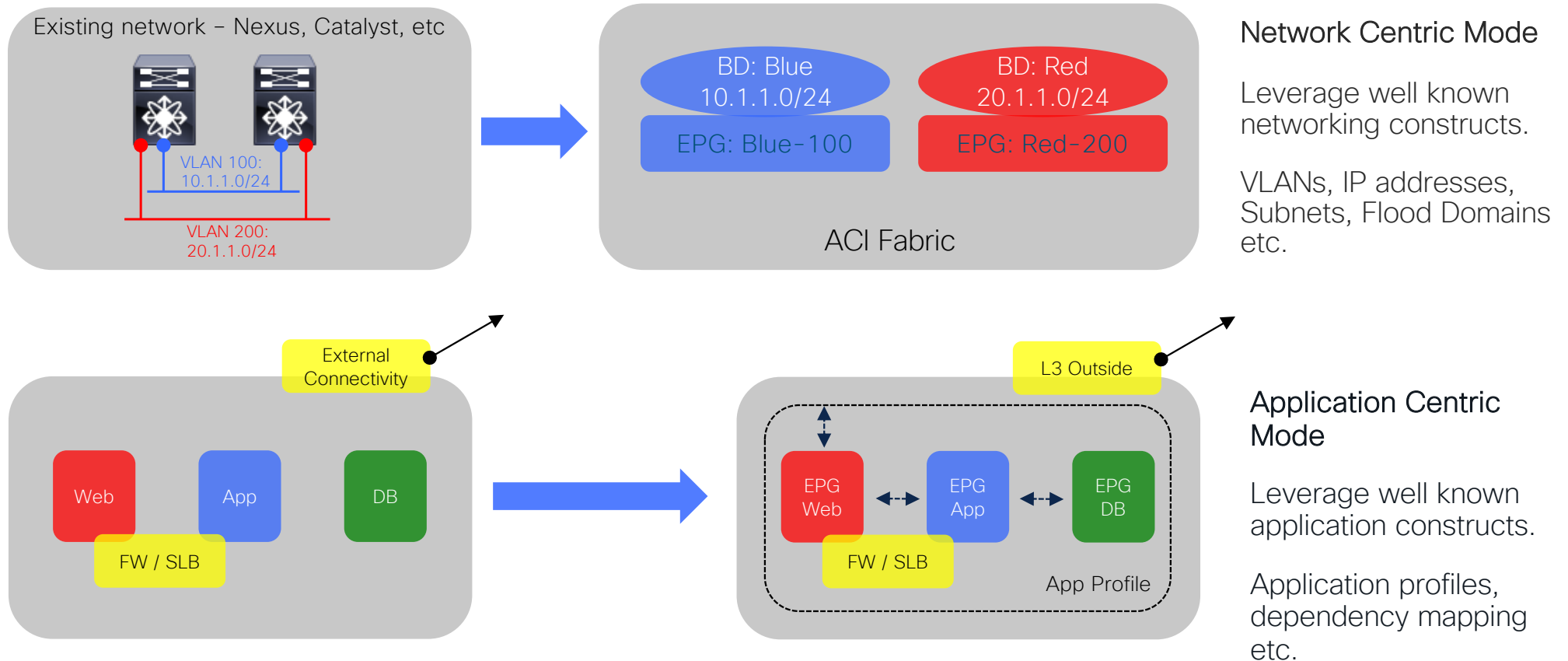
# ACI Devices Role



# The ACI Policy Model



# ACI Fabric – Two Deployment Models

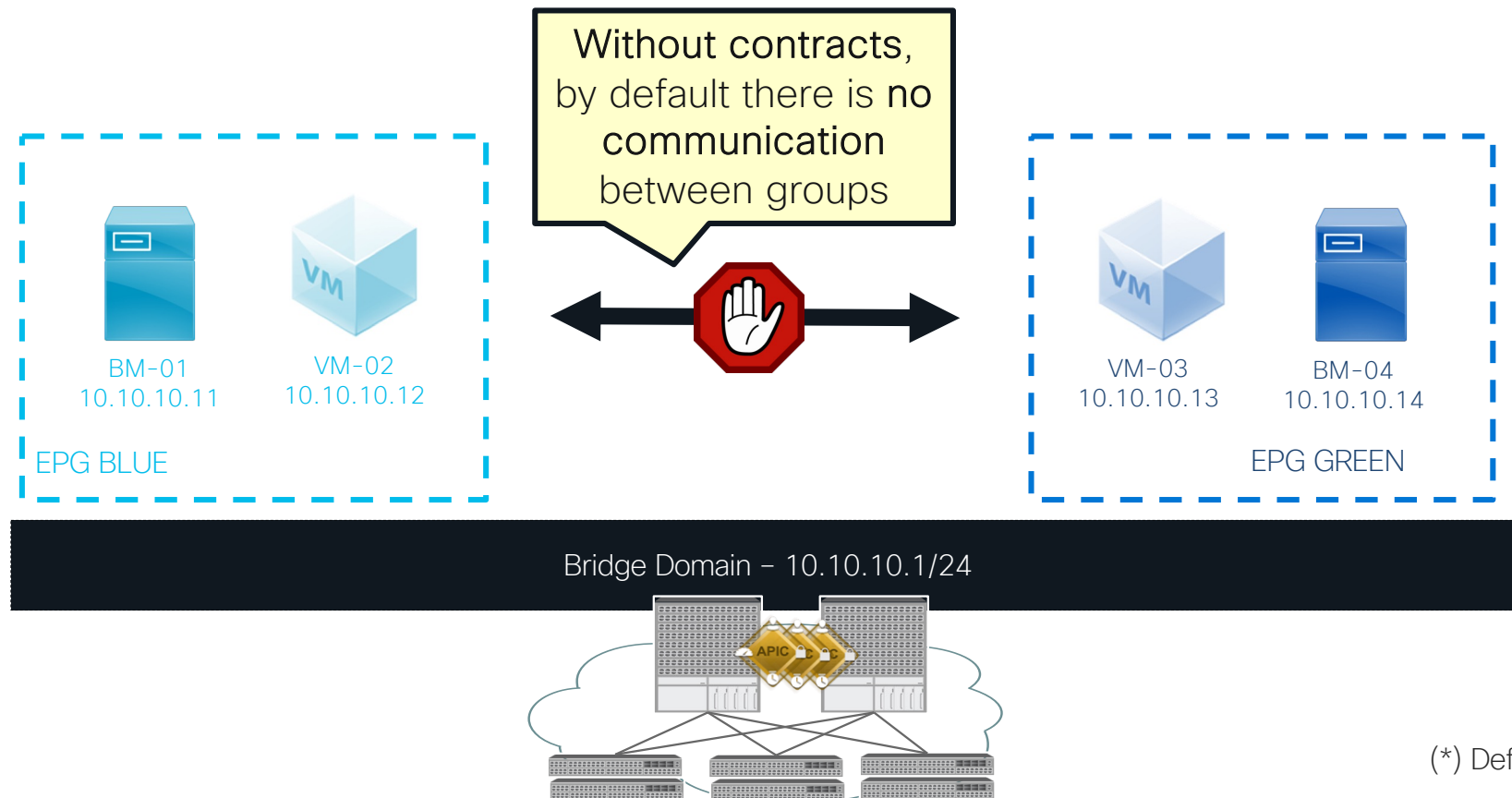


You can mix both network centric and application centric -> typical customer transition path!



# Admins Define EPGs Relationship with Contracts

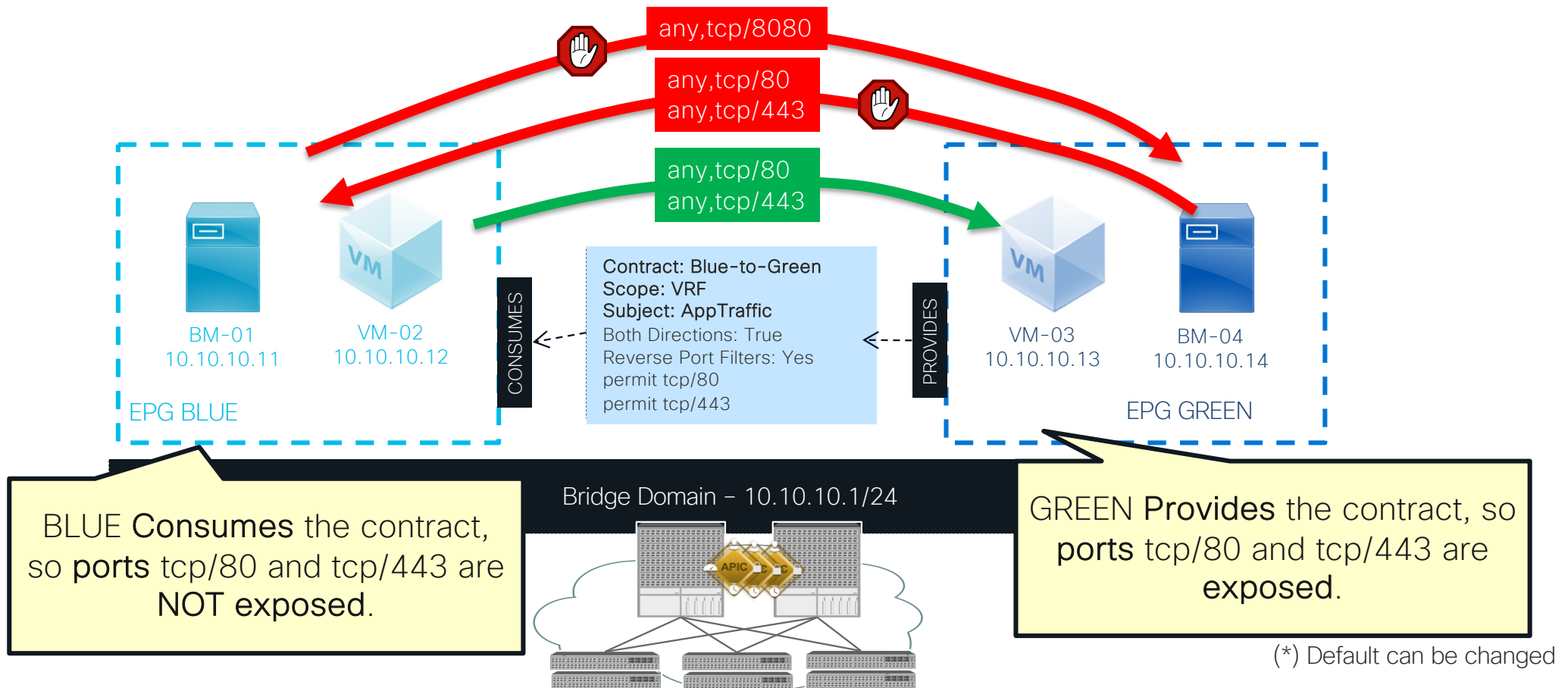
White-List Model (\*): No Contract, No Communication



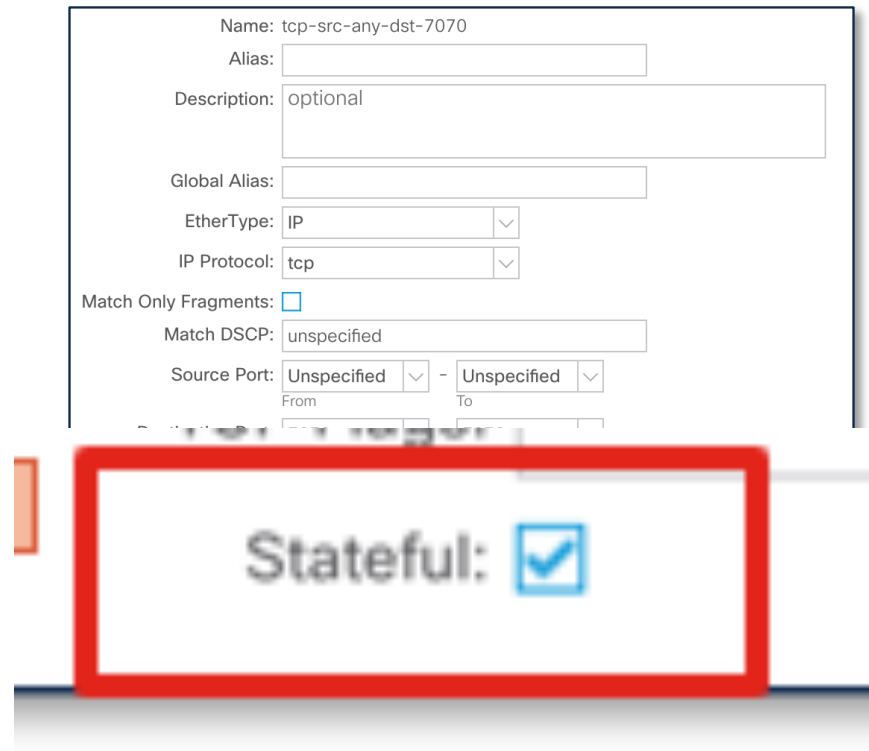
(\*) Default can be changed

# EPGs Will Have Relationships with Contracts

White-List Model (\*): Contract Determines Communication



# Did you say Stateless ?



Name: tcp-src-any-dst-7070

Alias:

Description: optional

Global Alias:

EtherType: IP

IP Protocol: tcp

Match Only Fragments: ☐

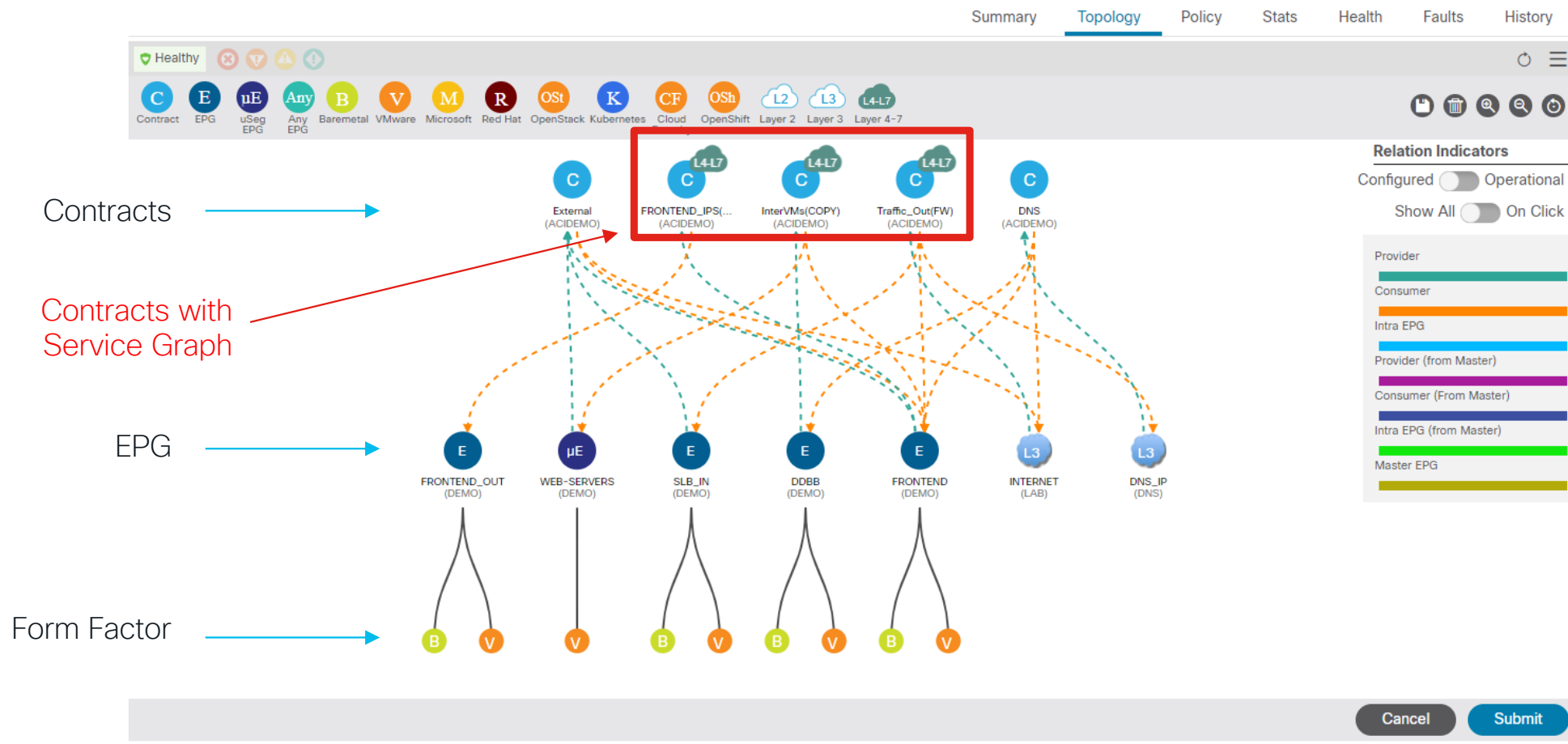
Match DSCP: unspecified

Source Port: Unspecified  - Unspecified   
From To

**Stateful: ☒**

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

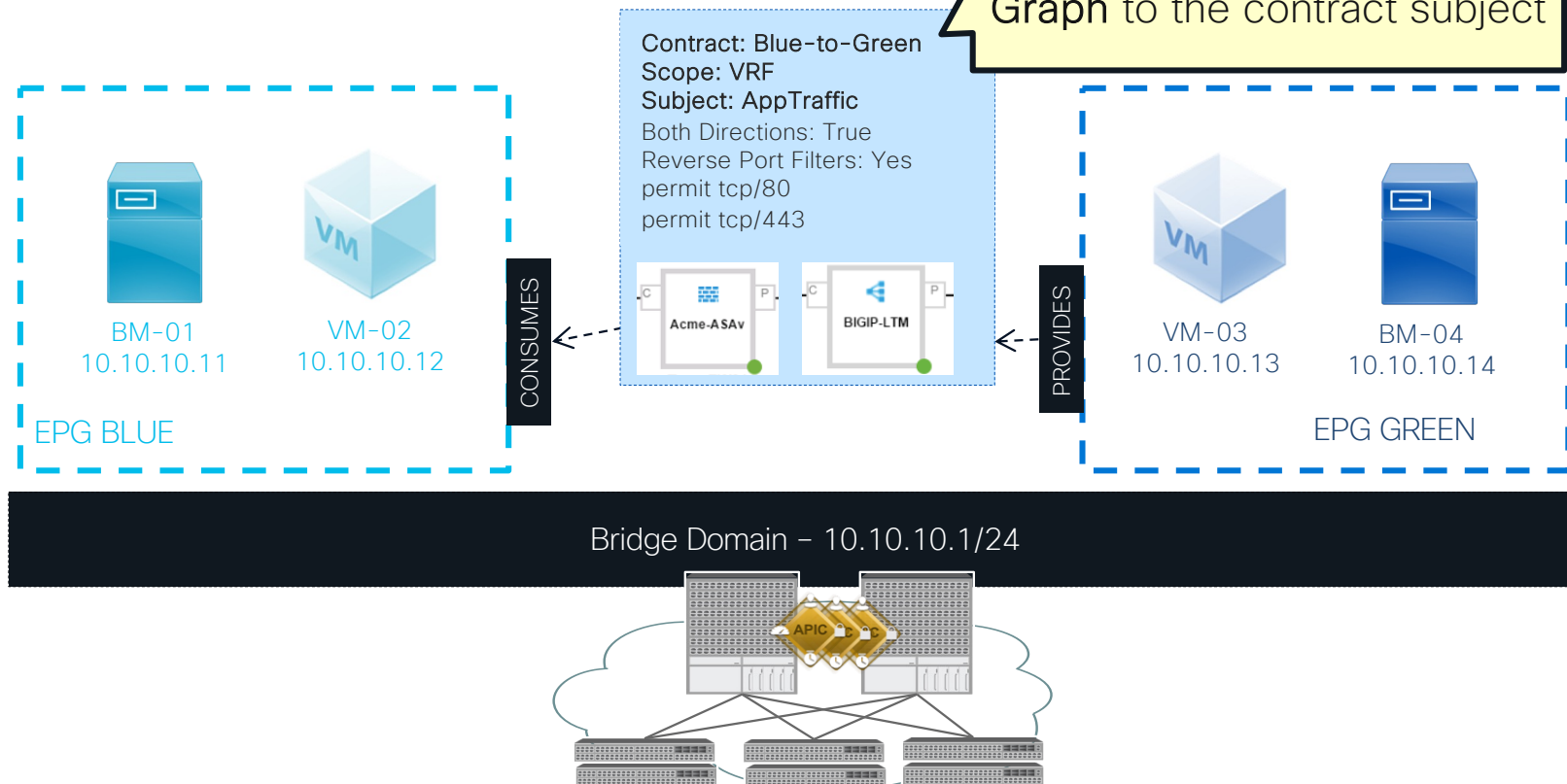
# Application Policy with Contract



# Contracts Also Allow Inserting Services

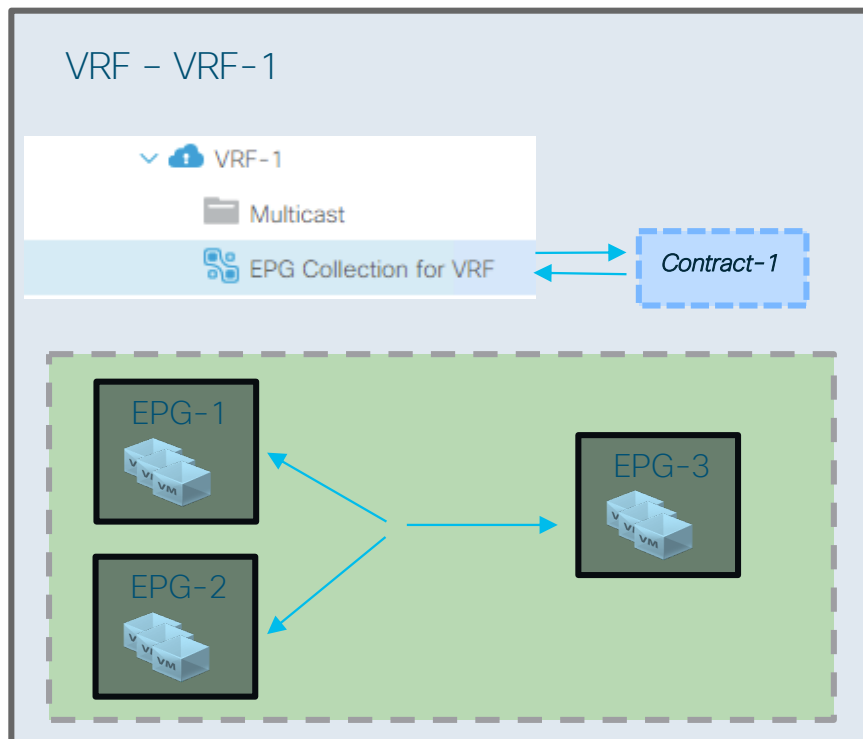
Next Generation Firewall, ADC, IDS/IPS, etc.

You can **insert** an NGFW, or a LB by attaching a **Service Graph** to the contract subject



# vzAny Can be Used to Permit all Traffic Between EPGs

- A contract defined for vzAny includes all the EPGs under the VRF and the L3Out also
- vzAny can provide and consume one contract: permit any any for instance



How Policy-cam is programmed

Source	Destination	Filter	Action
any	any	Contract-1	permit

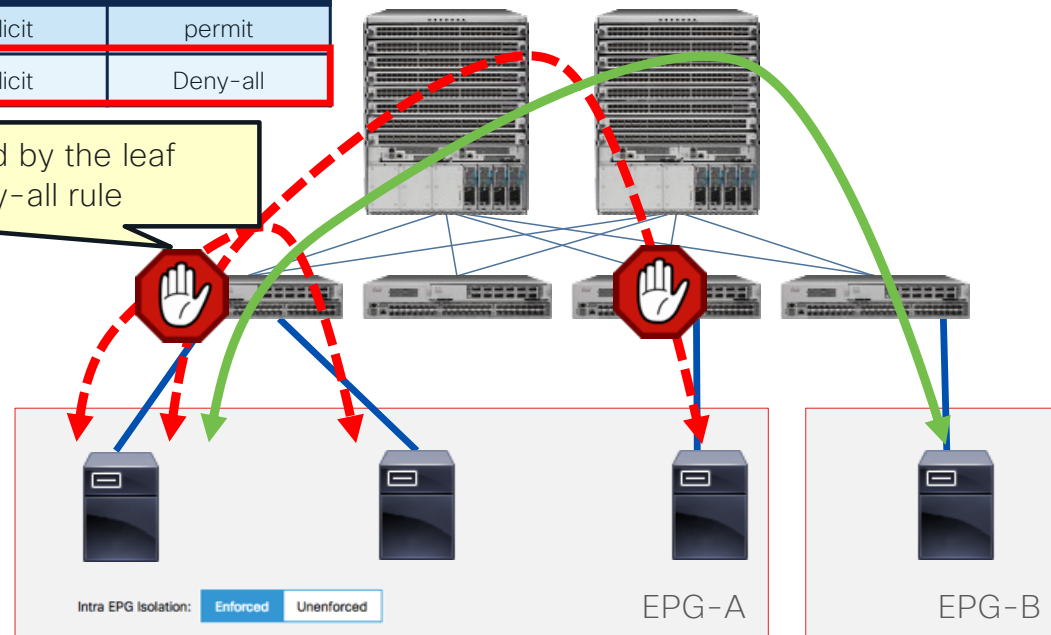
Which is equivalent to:

Source	Destination	Filter	Action
EPG-1	EPG-2	contract-1	permit
EPG-2	EPG-1	contract-1	permit
EPG-1	EPG-3	contract-1	permit
EPG-3	EPG-1	contract-1	permit
EPG-2	EPG-3	contract-1	permit
EPG-3	EPG-2	contract-1	permit

# Intra EPG Isolation – Zoning Rules

Source	Destination	Filter	Action
EPG-A	EPG-B	implicit	permit
EPG-A	EPG-A	implicit	Deny-all

Intra EPG traffic will be dropped by the leaf because of the implicit deny-all rule

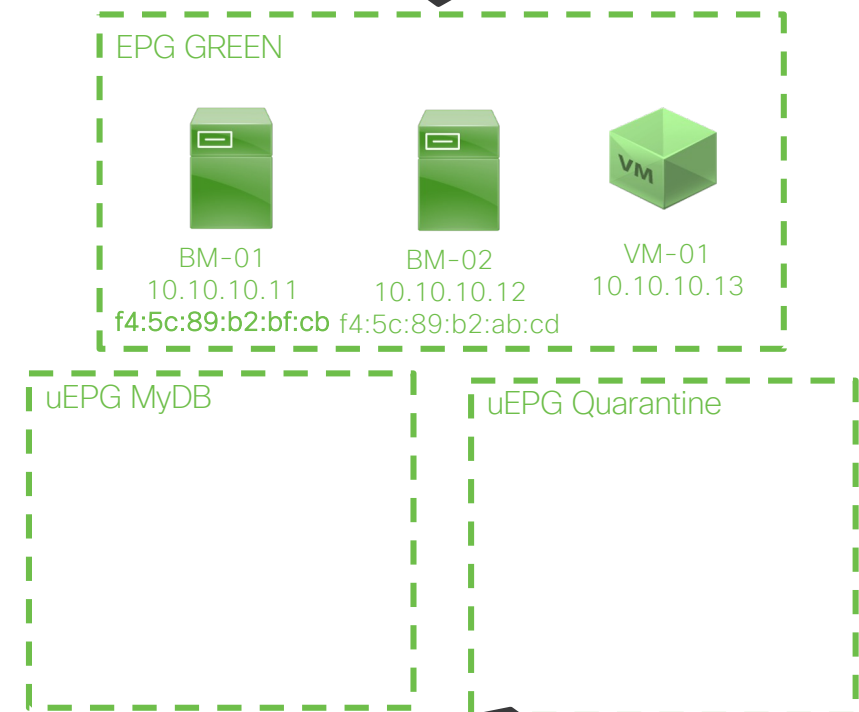


# Understanding Micro EPGs

- A MicroEPG (uEPG) is equivalent to a regular EPG for all purposes, but classification is based on endpoint attributes (and dynamic in nature)
- Endpoints assigned to the uEPG regardless of the encapsulation/port
- The endpoint must be first known to a regular EPG, called “**base EPG**”

Define uEPG based on MAC Address or IP Address.  
Select MAC=f4:5c:89:b2:bf:cb  
Select IP=10.10.10.11

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



Define uEPG based on VM attributes.  
VM-name=VM-01  
Hypervisor-identifier=ESXi-host-01



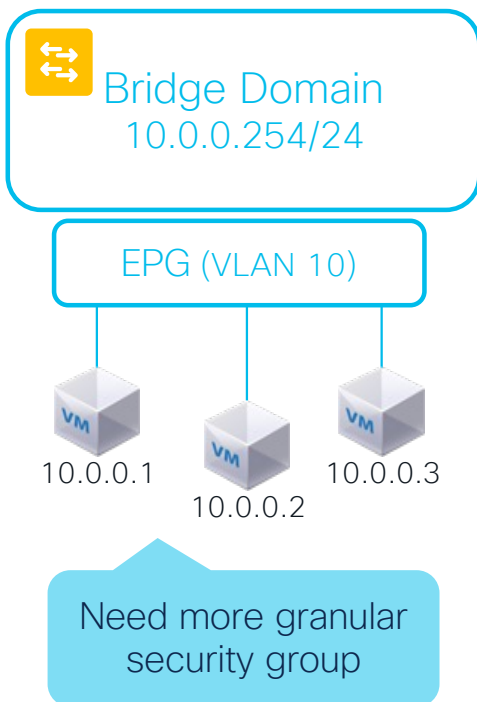
# Leveraging Endpoint Security Groups (ESG)



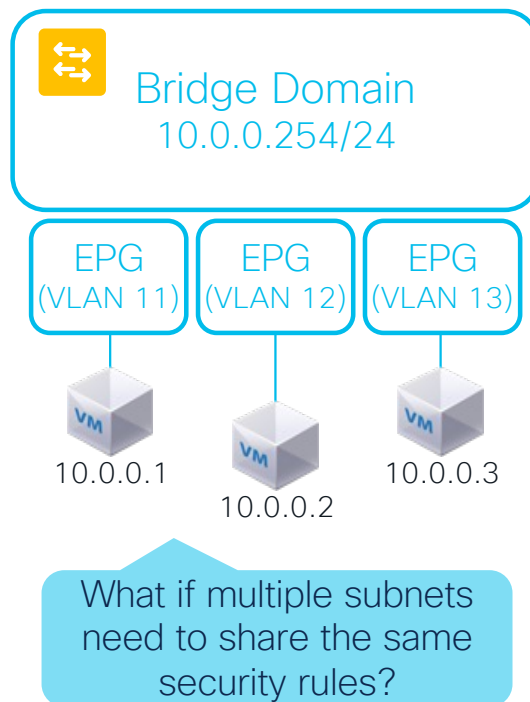
# Network Centric & Application Centric Design

## Network Centric

A security group in 1 subnet

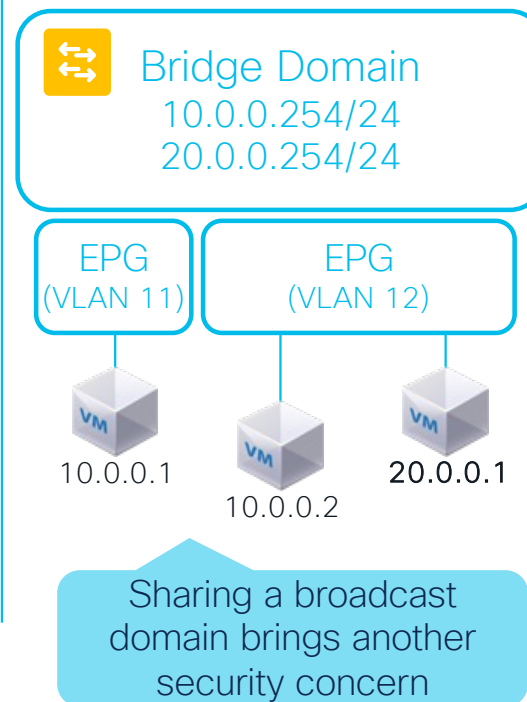


Multiple security groups in 1 subnet



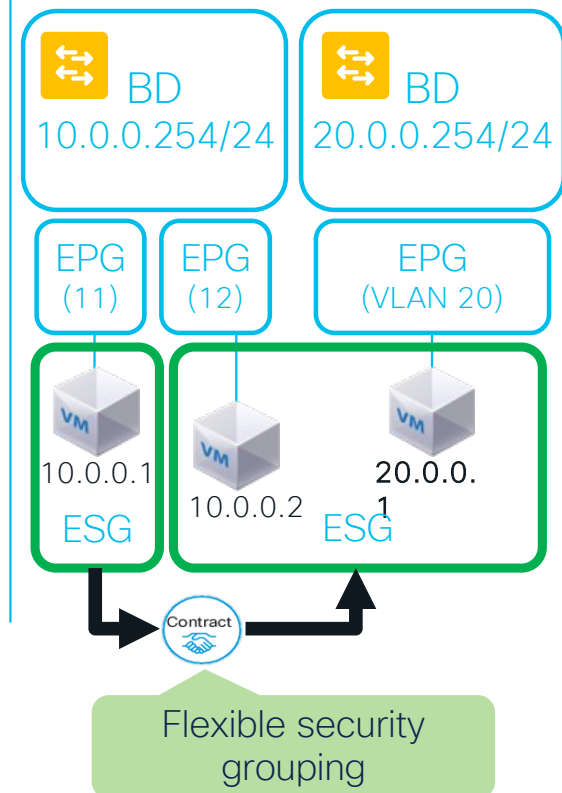
## Application Centric

Security groups across subnets

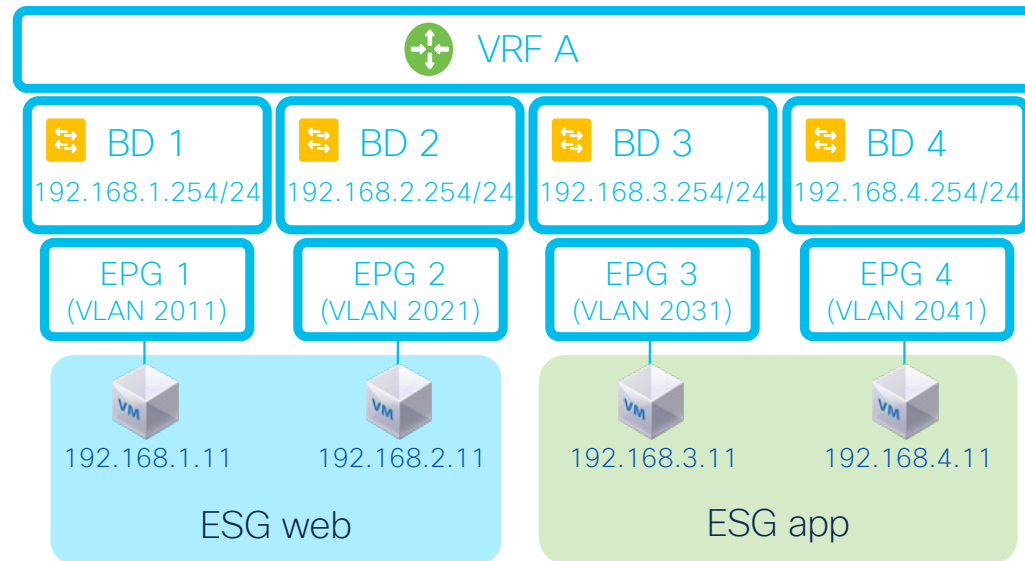


5.0 = Endpoint Security Group (ESG)

Security groups **across** bridge domains



# What is End Point Security Group (ESG)?



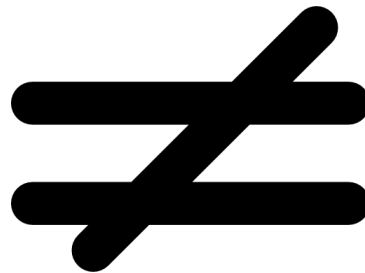
- ESG is a security group across BDs (EPG was across VLANs but within one BD)
- Configure “EP Selector” to classify endpoints into each ESG
- EPG becomes merely a “VLAN – path” binding component.

# Selectors for use with ESG

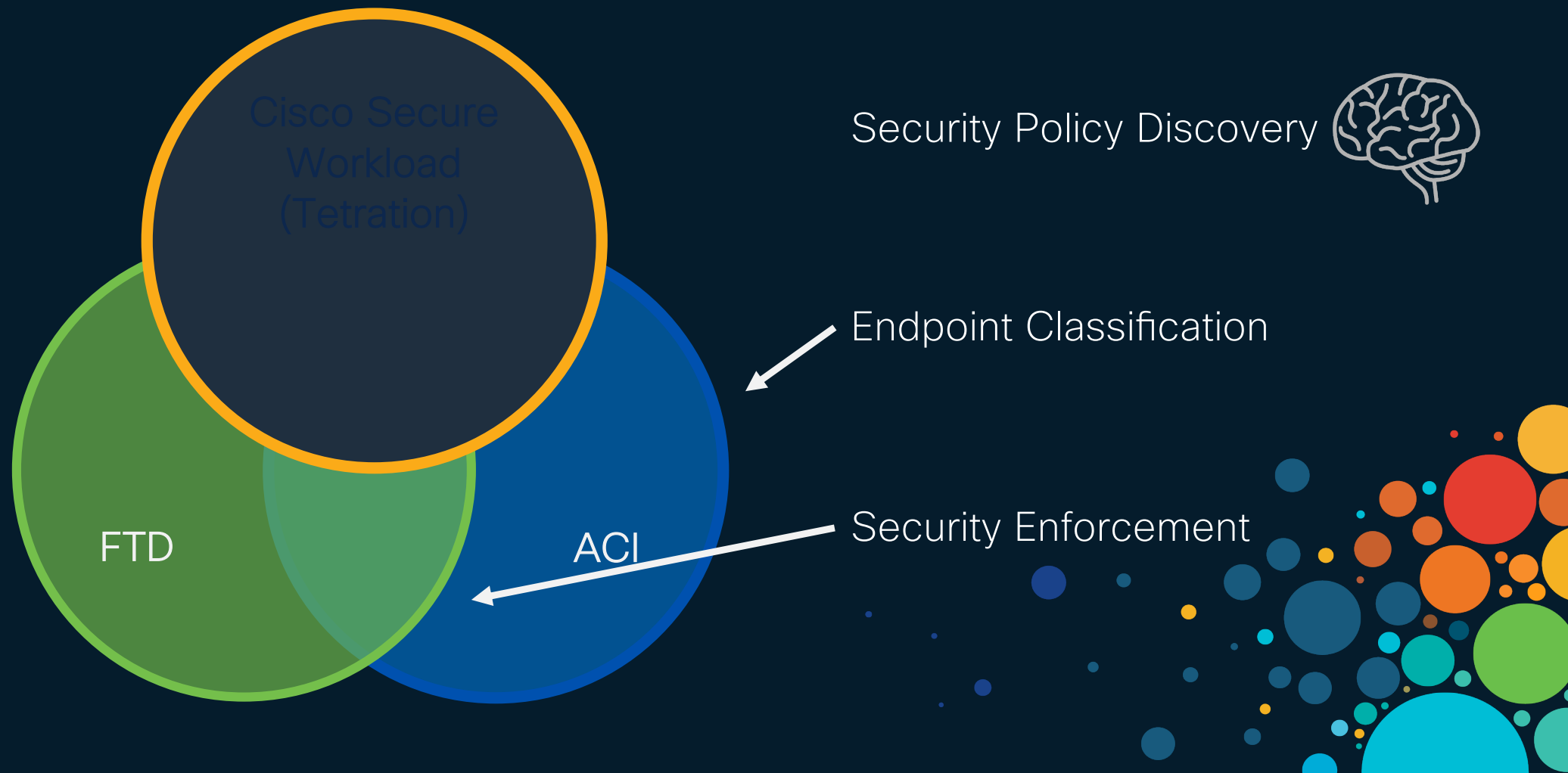
- IP Subnet Selector 5.0(1)
- Service EPG Selector 5.2(4)
  - For exceptions with service graphs vzAny - vzAny
- Tag Selector 5.2(1)
  - Classify endpoints based on Policy Tags (tagTag).
  - Various supported objects to attach Policy Tags
  - Easy to change the ESG of multiple endpoints at once via tag
- EPG Selector 5.2(1)
  - Classify the entire EPG to an ESG
  - The ESG inherits the contracts configured under the EPG
    - The solution to provide contracts between ESG and EPG
    - The solution for seamless migration from EPG to ESG

But...

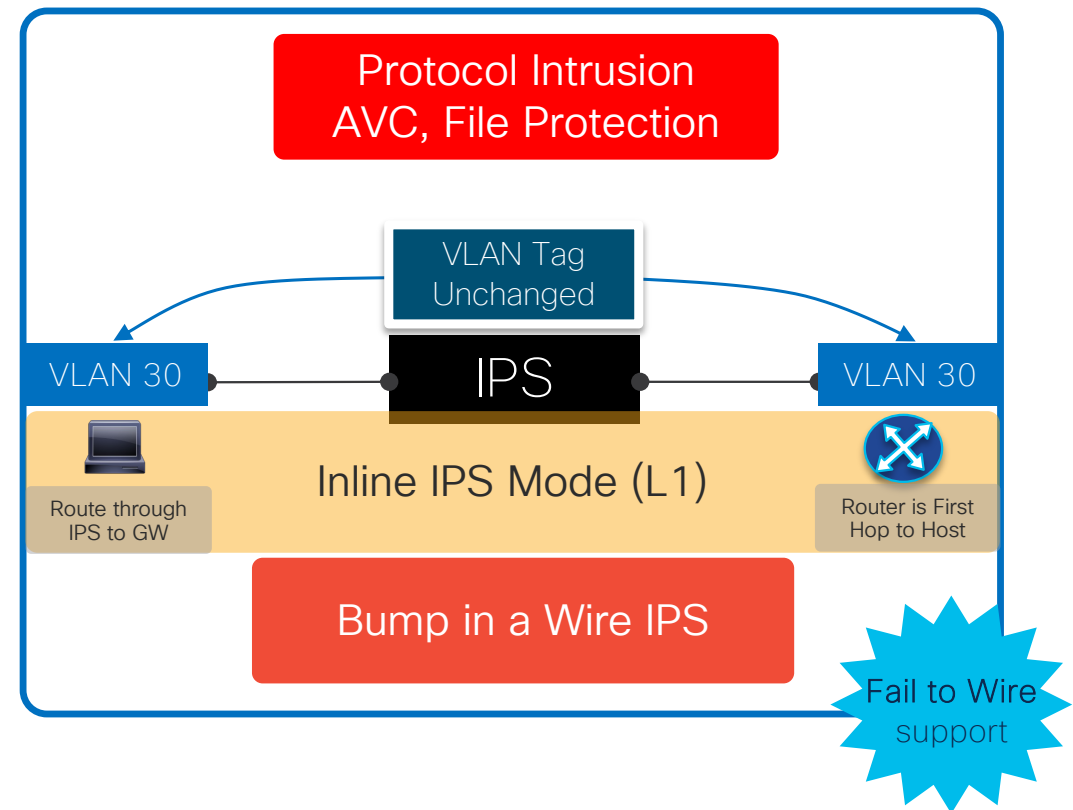
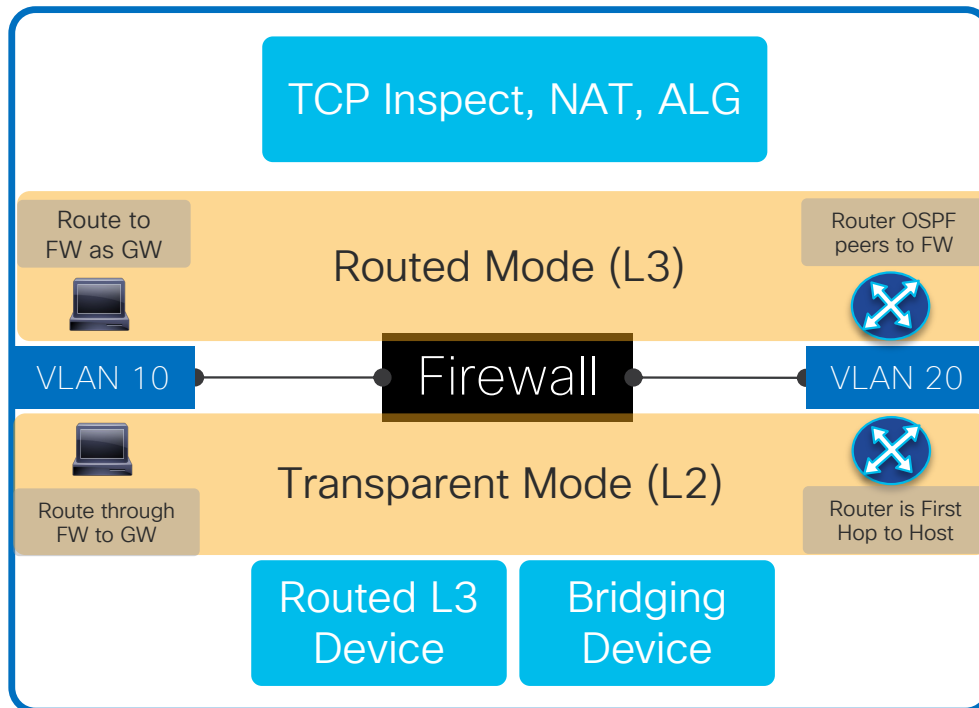
ACI IS NOT A FIREWALL



# FTD with ACI

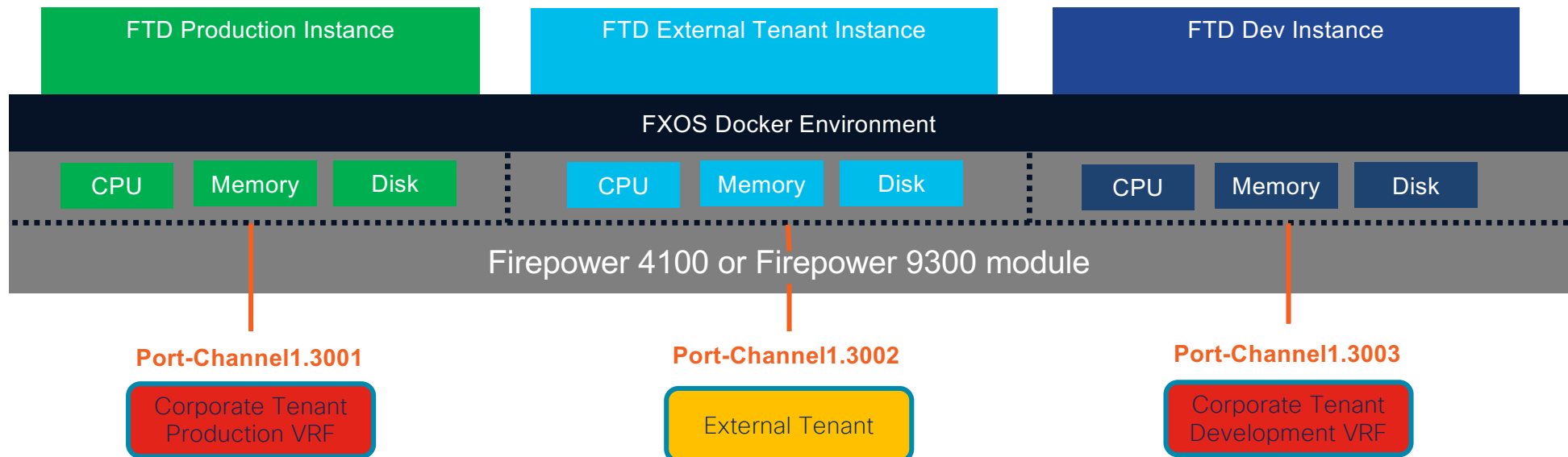


# Cisco Secure Firewall Modes of Operation



# 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



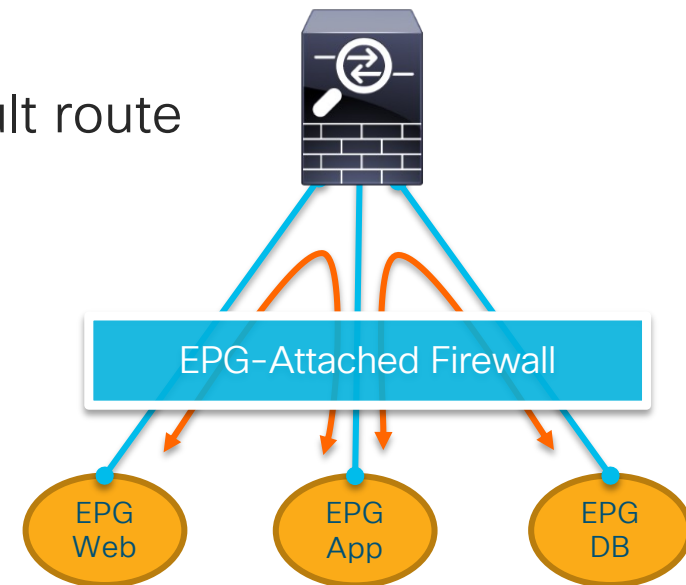


# Secure Firewall Insertion



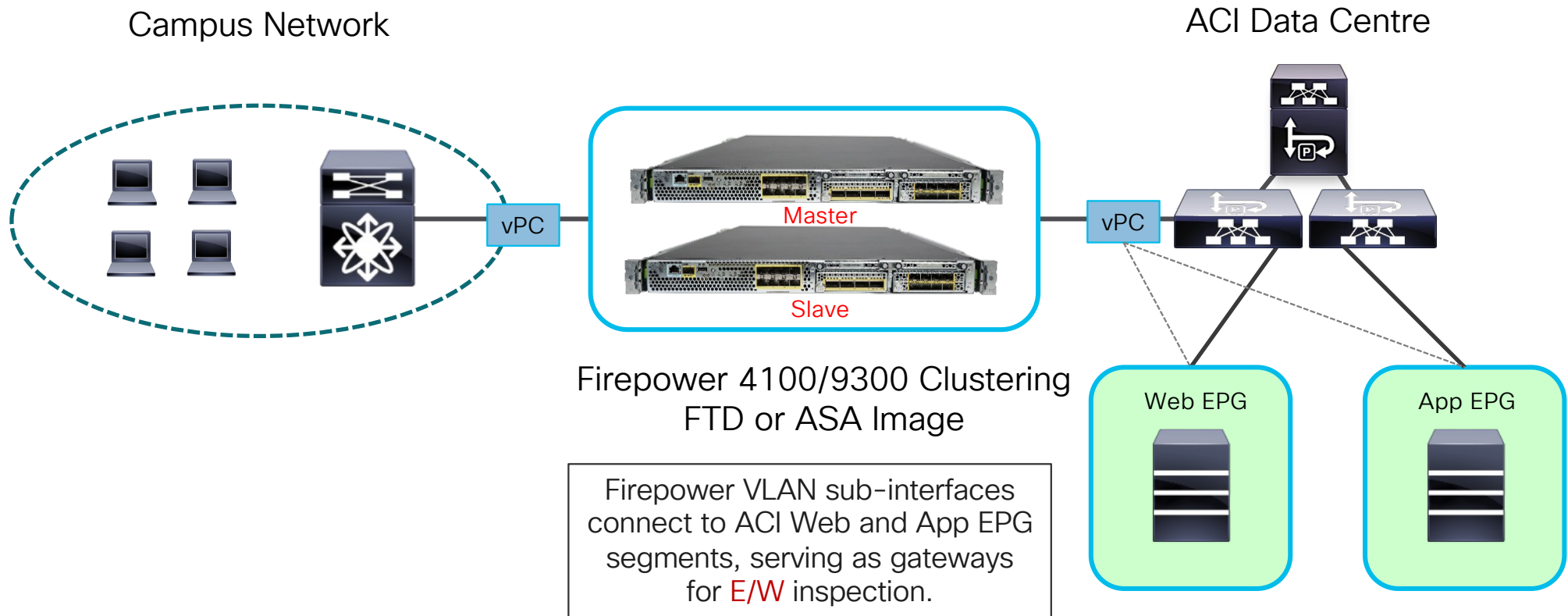
# Network-Centric ACI Fabric

- 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



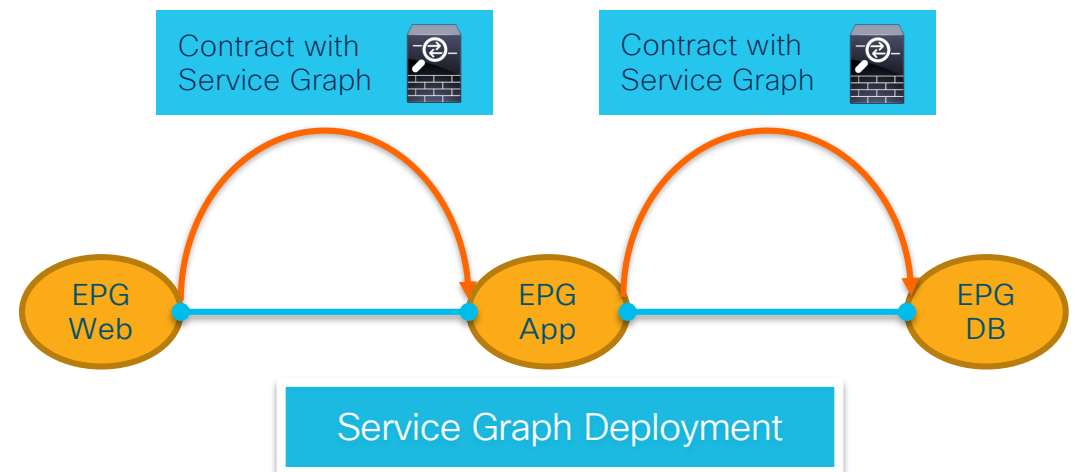
# Firepower Cluster at Perimeter to ACI Fabric

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

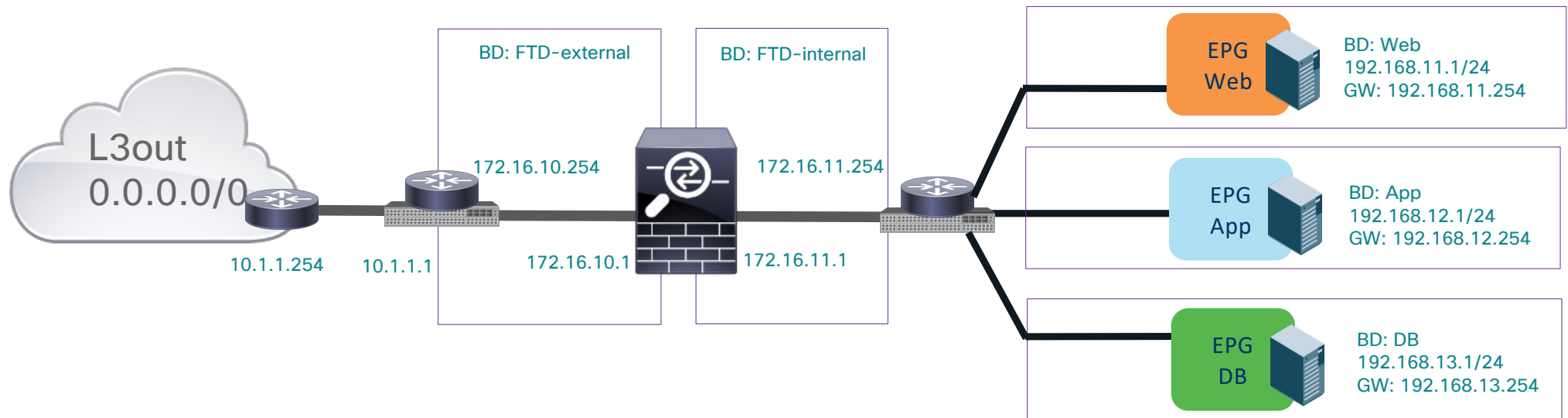


# App-Centric ACI Fabric

- 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

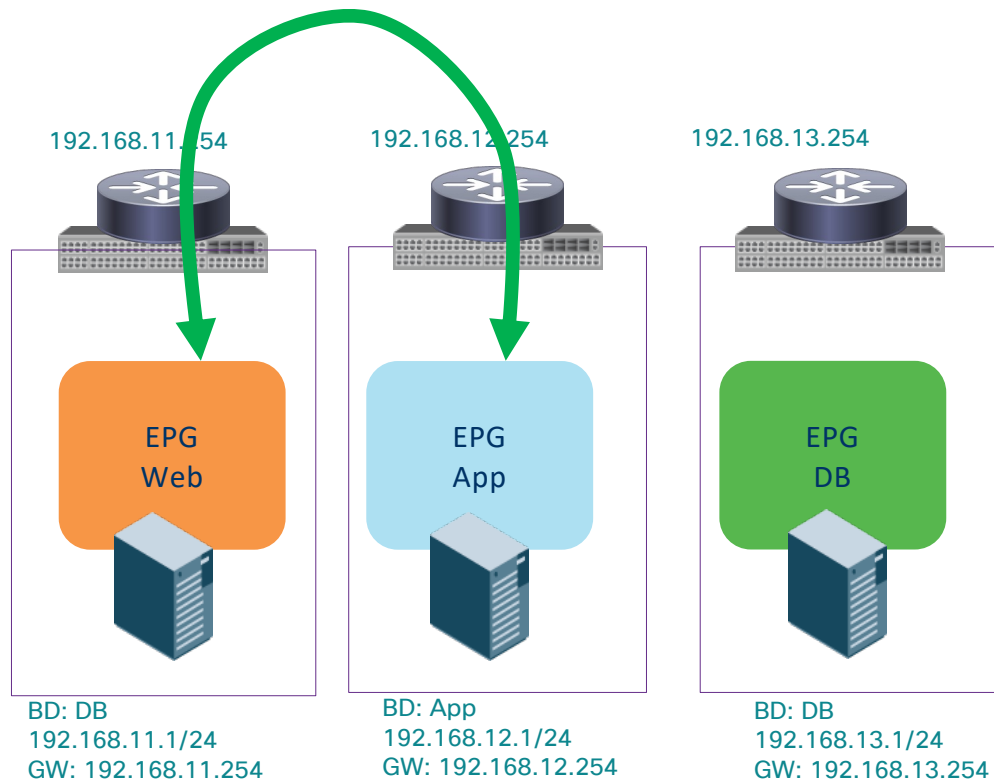


# Topology



# Policy Based Redirect is your Best Friend

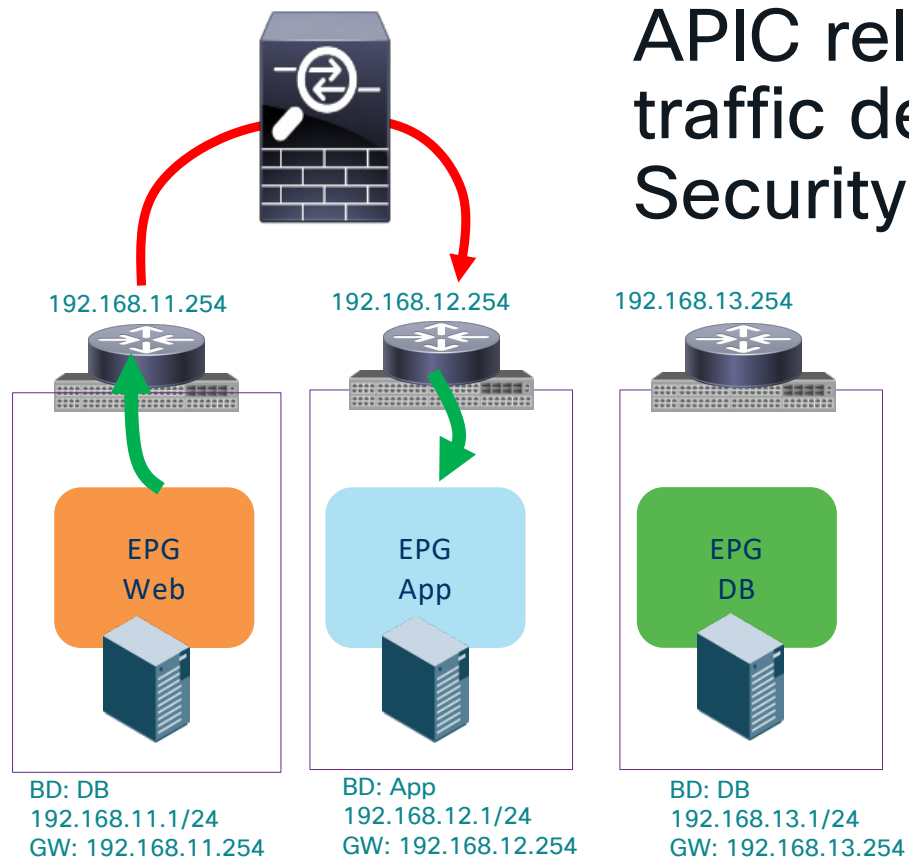
Before Service graph is deployed



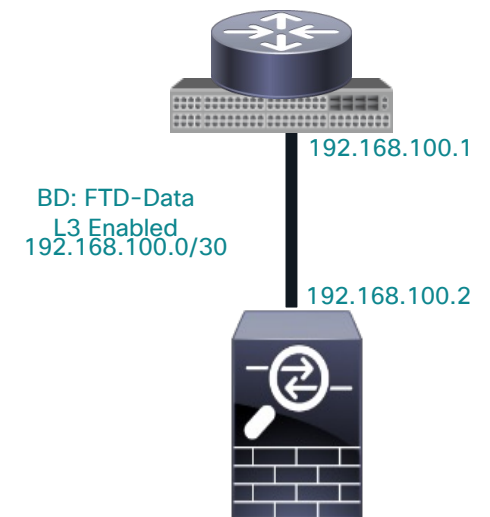
APIC relies on **Routing** to forward traffic from Server in EPG WEB to Server in EPG APP based on contract

# Policy Based Redirect is your Best Friend

With PBR Service Graph

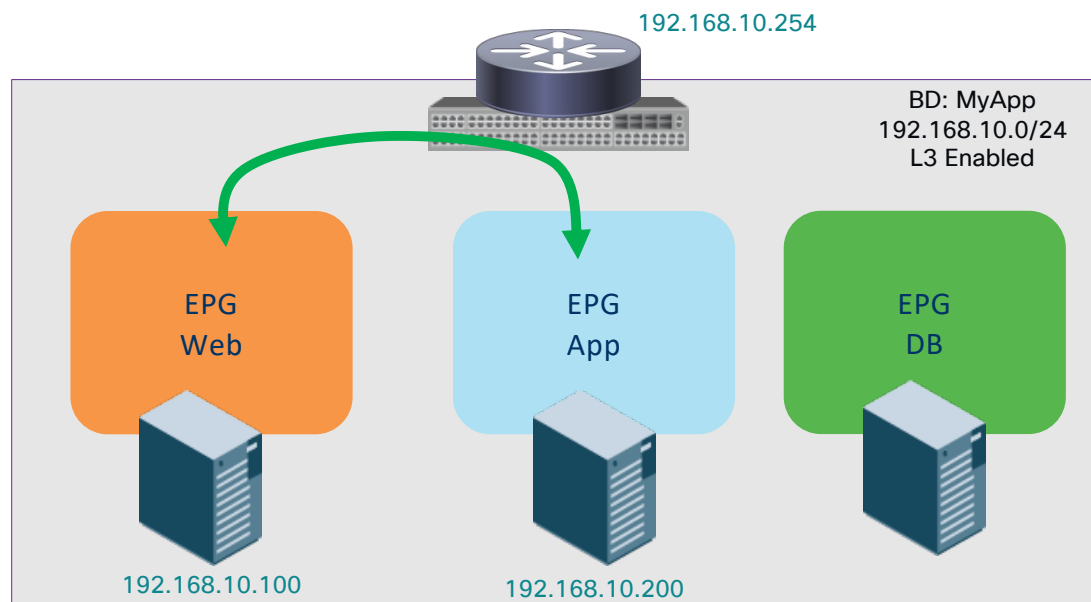


APIC relies on **PBR** to redirect the traffic defined in the contract to the Security Service



# PBR for micro-Segmentation

Based only on Contract



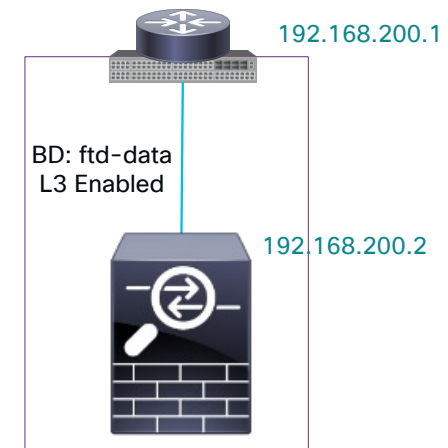
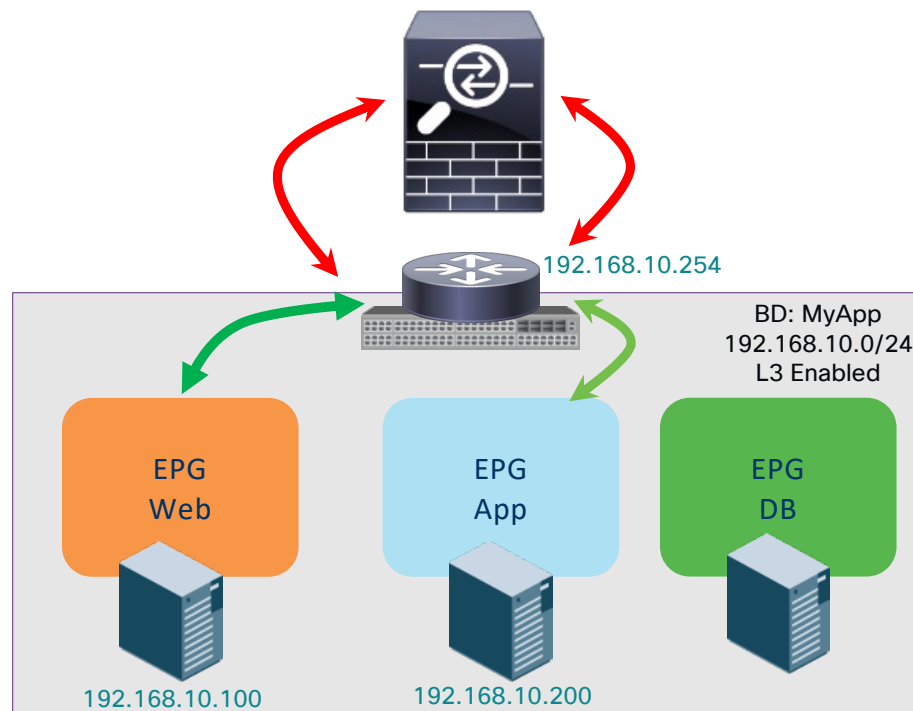
Because this is a communication between two End-points in different EPG, the forwarding decision is made in the leaf switch



# 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.

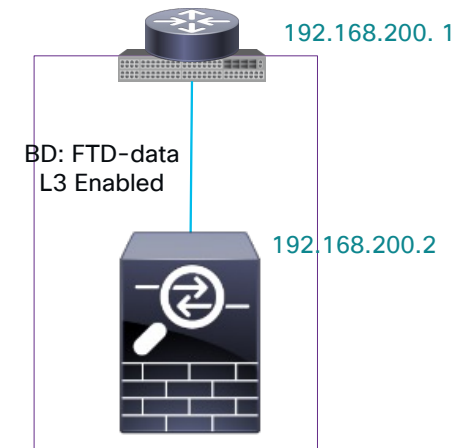
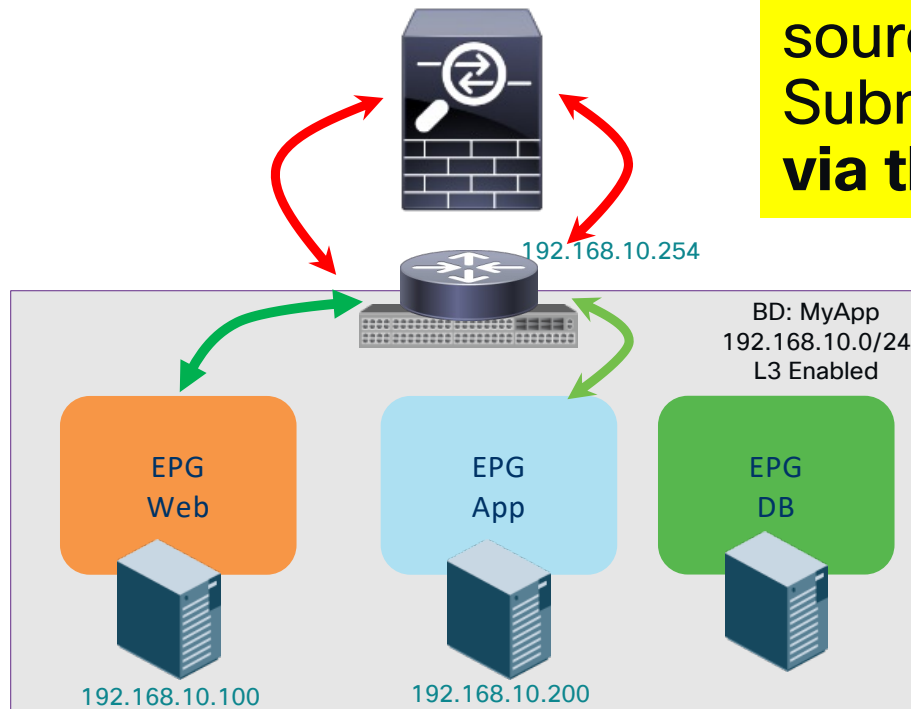


# PBR for micro-Segmentation

## Leveraging PBR



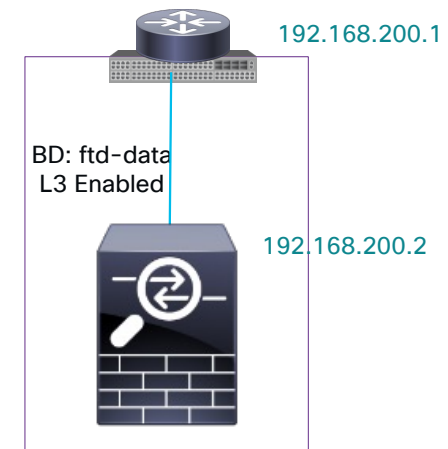
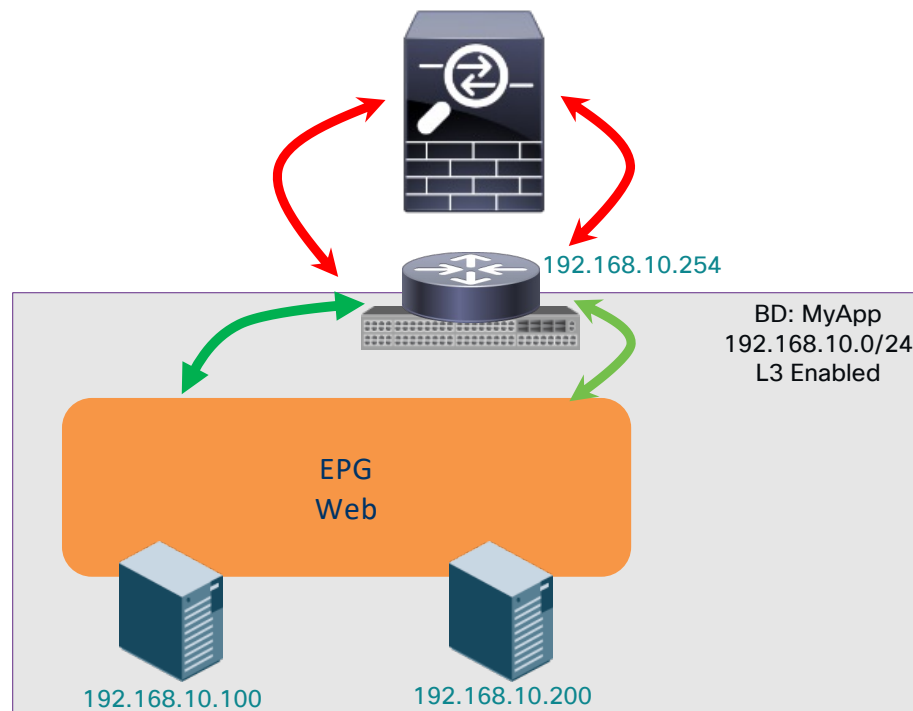
The Firewall must be in **ONE ARM** as source and destination are in the same Subnet. It must **allow traffic in and out via the same interface**.



# Redirecting traffic within an EPG/ESG

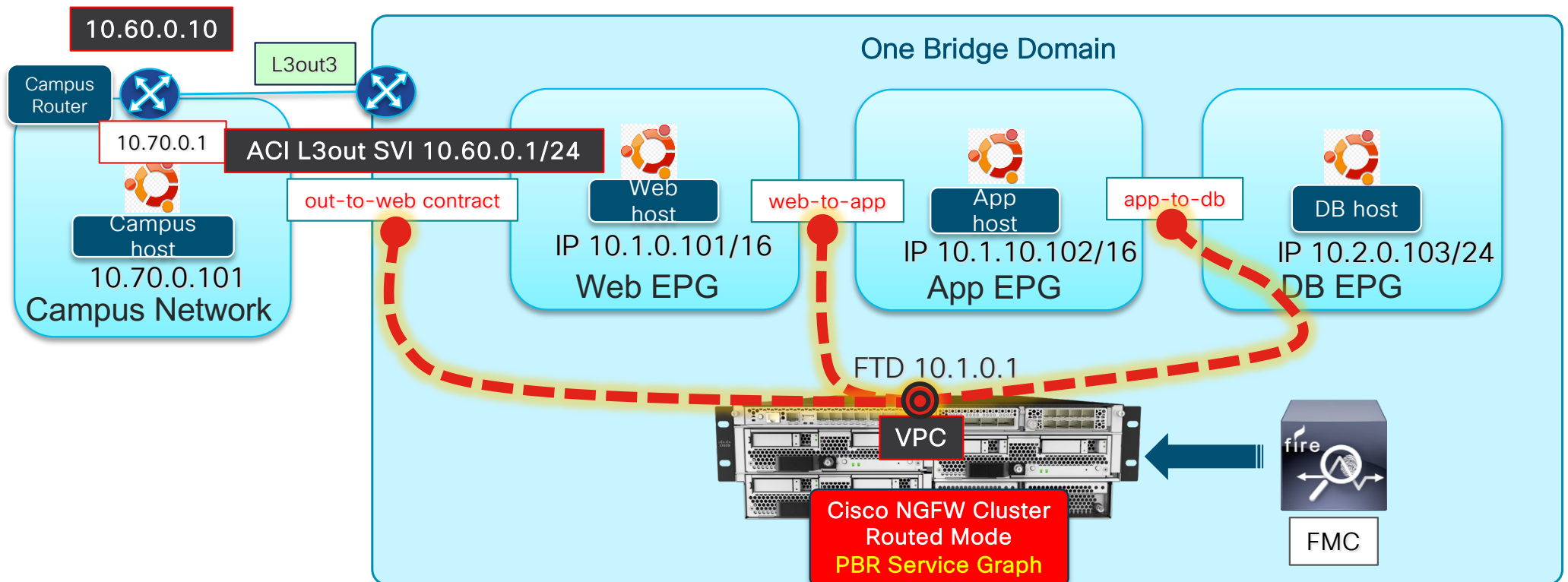
Leveraging PBR

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.

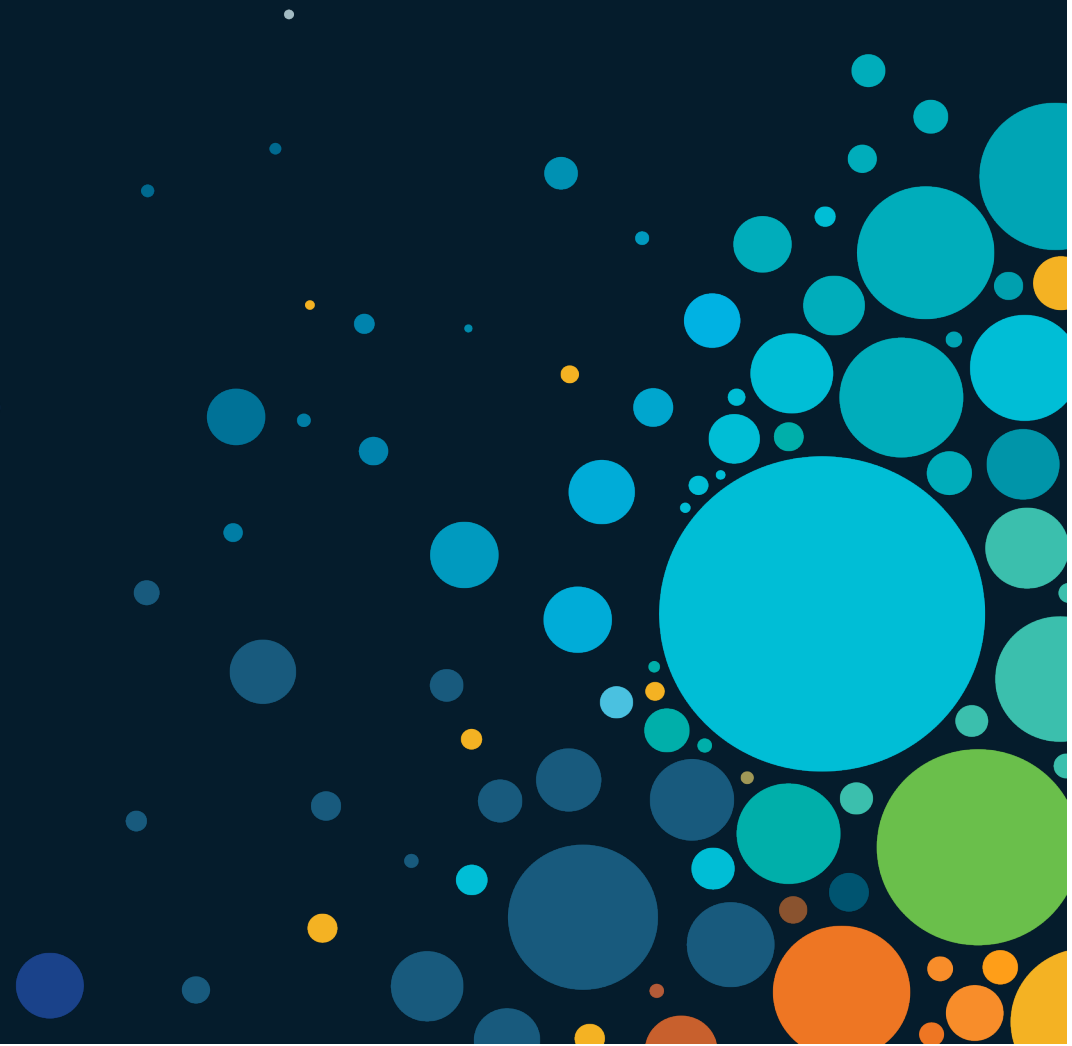


## Rapid Threat Containment

Automatic network threat containment using the network as an enforcer

Threat-centric network access determines network access based on IoCs

# Dynamic Attributes



# The Problem Statement

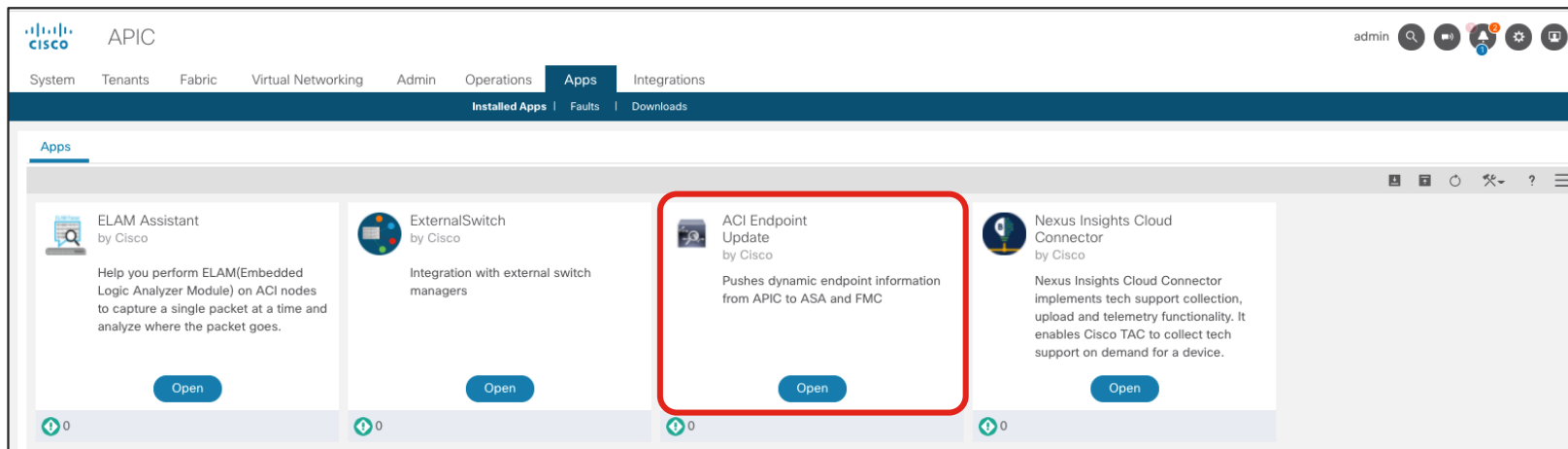
 How to build a policy based on intent instead of static IPs ?

 How to reduce changes on enforcement point?

 How to build a policy with cross security Domain ?

# 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

The screenshot displays the Cisco Secure Firewall Management Center (FMC) interface. On the left, the 'fgandola' tenant is selected under the 'Tenants' tab. The 'firewalls' section is expanded, showing 'Application EPGs' and 'Endpoint Security Groups'. A green box highlights 'ALL\_EPGs', 'development', and 'production' under 'Application EPGs'. An orange box highlights 'ftd-HA-link' and 'ftd-mgmt' under 'Application EPGs'. On the right, the 'Dynamic Objects' page is shown. A modal window titled 'APIC\_FGANDOLA\_FIREWALLS\_FTD-MGMT' is open, displaying a list of mapped IPs: 10.237.100.22, 10.237.100.23, 10.237.100.24, and 10.237.100.25. The modal also shows a 'Download' button and an 'OK' button. The background table lists various dynamic objects, including 'APIC\_FGANDOLA\_APPLICATIONS\_ESG-ALL\_EPGS', 'APIC\_FGANDOLA\_APPLICATIONS\_ESG-DEVELOPMENT', 'APIC\_FGANDOLA\_APPLICATIONS\_ESG-PRODUCTION', 'APIC\_FGANDOLA\_FIREWALLS\_FTD-HA-LINK', and 'APIC\_FGANDOLA\_FIREWALLS\_FTD-MGMT'. A green arrow points from the 'ALL\_EPGs' box to the 'APIC\_FGANDOLA\_APPLICATIONS\_ESG-ALL\_EPGS' row. An orange arrow points from the 'ftd-mgmt' box to the 'APIC\_FGANDOLA\_FIREWALLS\_FTD-MGMT' row. A yellow arrow points from the 'Mapped IPs' list in the modal to the 'Number of Mapped IPs' column in the table.

APIC (aci-dev-01)

System Tenants Fabric

ALL TENANTS | Add Tenant | Tenant Search: name of

fgandola

Quick Start

fgandola

Application Profiles

applications

Application EPGs

uSeg EPGs

Endpoint Security Groups

ALL\_EPGs

development

production

firewalls

Application EPGs

ftd-HA-link

ftd-mgmt

uSeg EPGs

Endpoint Security Groups

network-segments

Networking

Contracts

Policies

Services

Security

Secure Firewall Management Center

Objects / Object Management

Overview Analysis Policies Devices Objects Integration Deploy

Dynamic Objects

Filter

Name Description Number of Mapped IPs

APIC\_DEMO\_APPLICATIONS\_ESG-DEMO-APP 1

APIC\_DEMO\_NETWORK-SEGMENTS\_192.168.150.X\_24 1

APIC\_FGANDOLA\_APPLICATIONS\_ESG-ALL\_EPGS 2

APIC\_FGANDOLA\_APPLICATIONS\_ESG-DEVELOPMENT 1

APIC\_FGANDOLA\_APPLICATIONS\_ESG-PRODUCTION 1

APIC\_FGANDOLA\_FIREWALLS\_FTD-HA-LINK 1

APIC\_FGANDOLA\_FIREWALLS\_FTD-MGMT 4

APIC\_FGANDOLA\_NETWORK-SEGMENTS\_192.168.151.... 1

APIC\_FGANDOLA\_NETWORK-SEGMENTS\_192.168.152.... 2

APIC\_FGANDOLA\_NETWORK-SEGMENTS\_192.168.153.... 1

APIC\_FGANDOLA\_FIREWALLS\_FTD-MGMT

Mapped IPs

Filter

4 Mapped IPs

10.237.100.22

10.237.100.23

10.237.100.24

10.237.100.25

Download OK

# 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

Q 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

Add a Location IP Address

Add

Selected Destination Attributes (2)

Security Group Tags

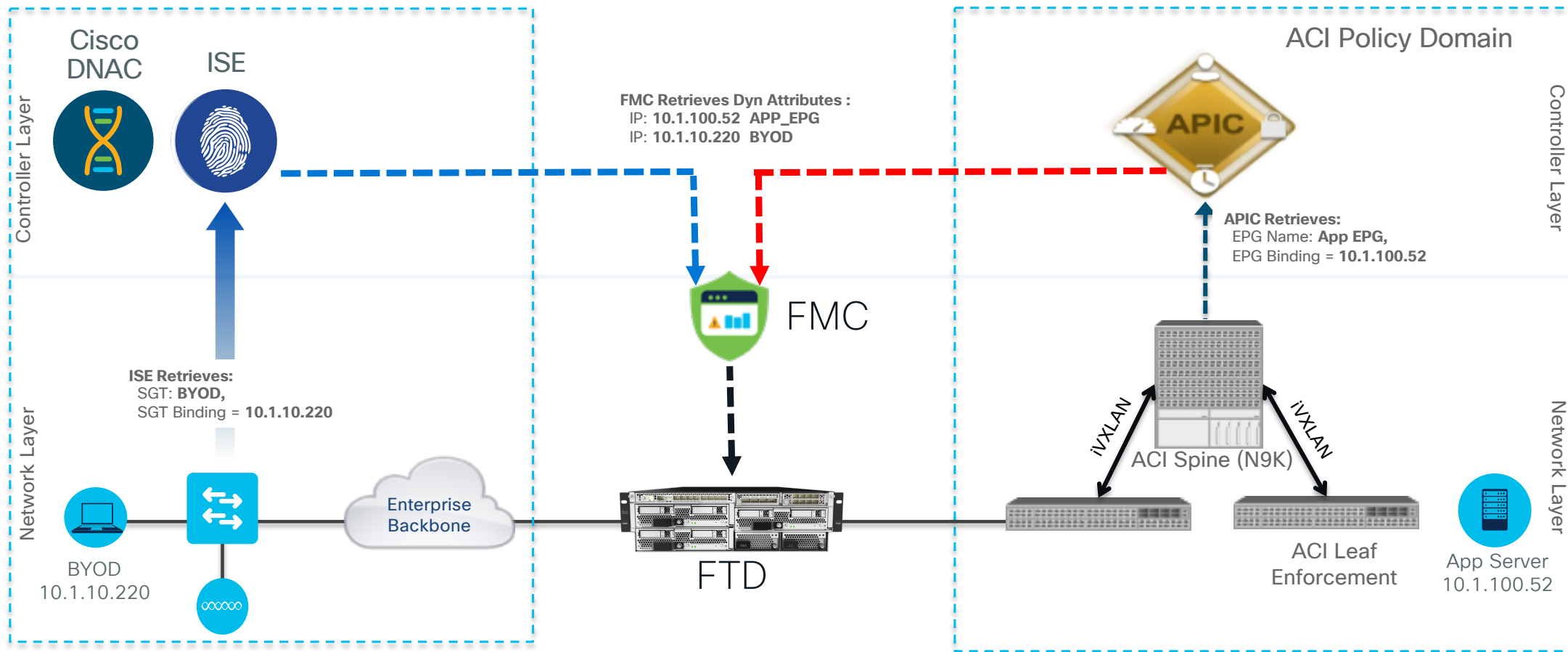
PCI\_Servers

Point\_of\_Sale\_Systems

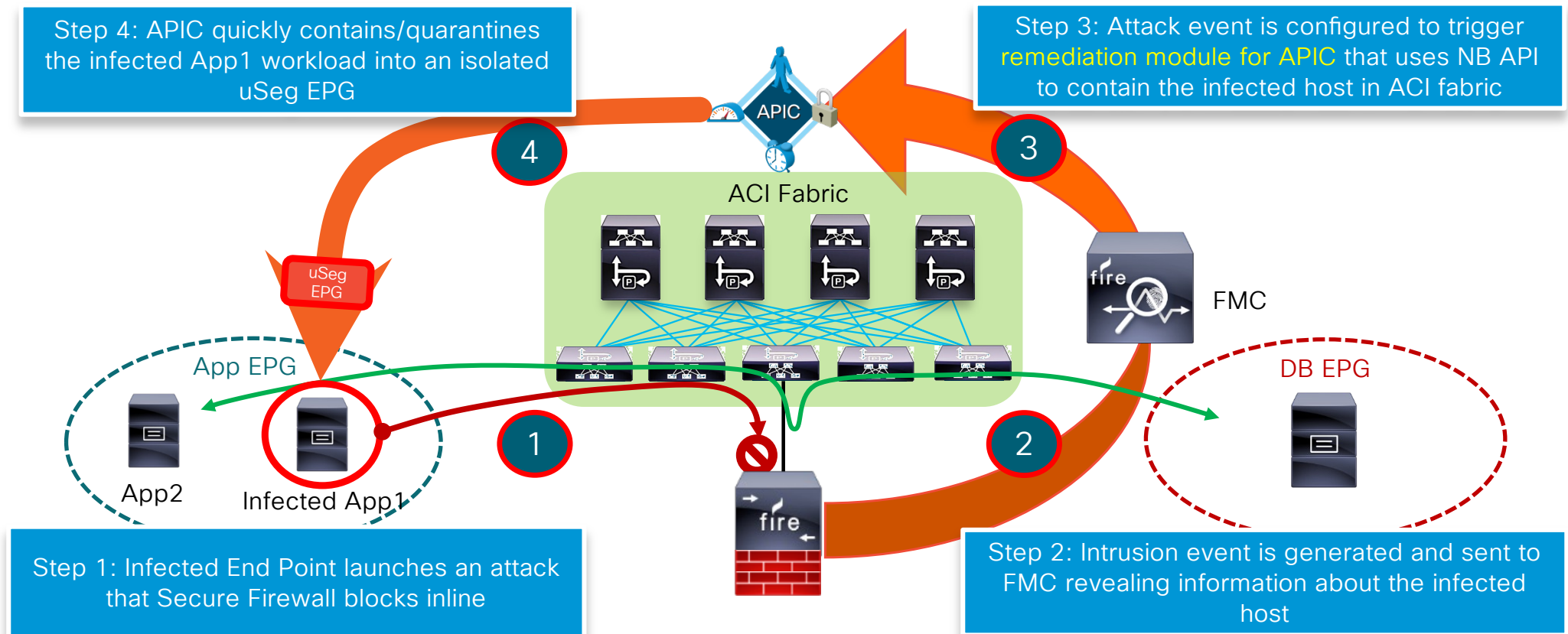
Attributes of the same type (for example, SGT) match the rule if any attribute is matched.

Attributes of different types match the rule only if all attributes are matched. [More info](#)

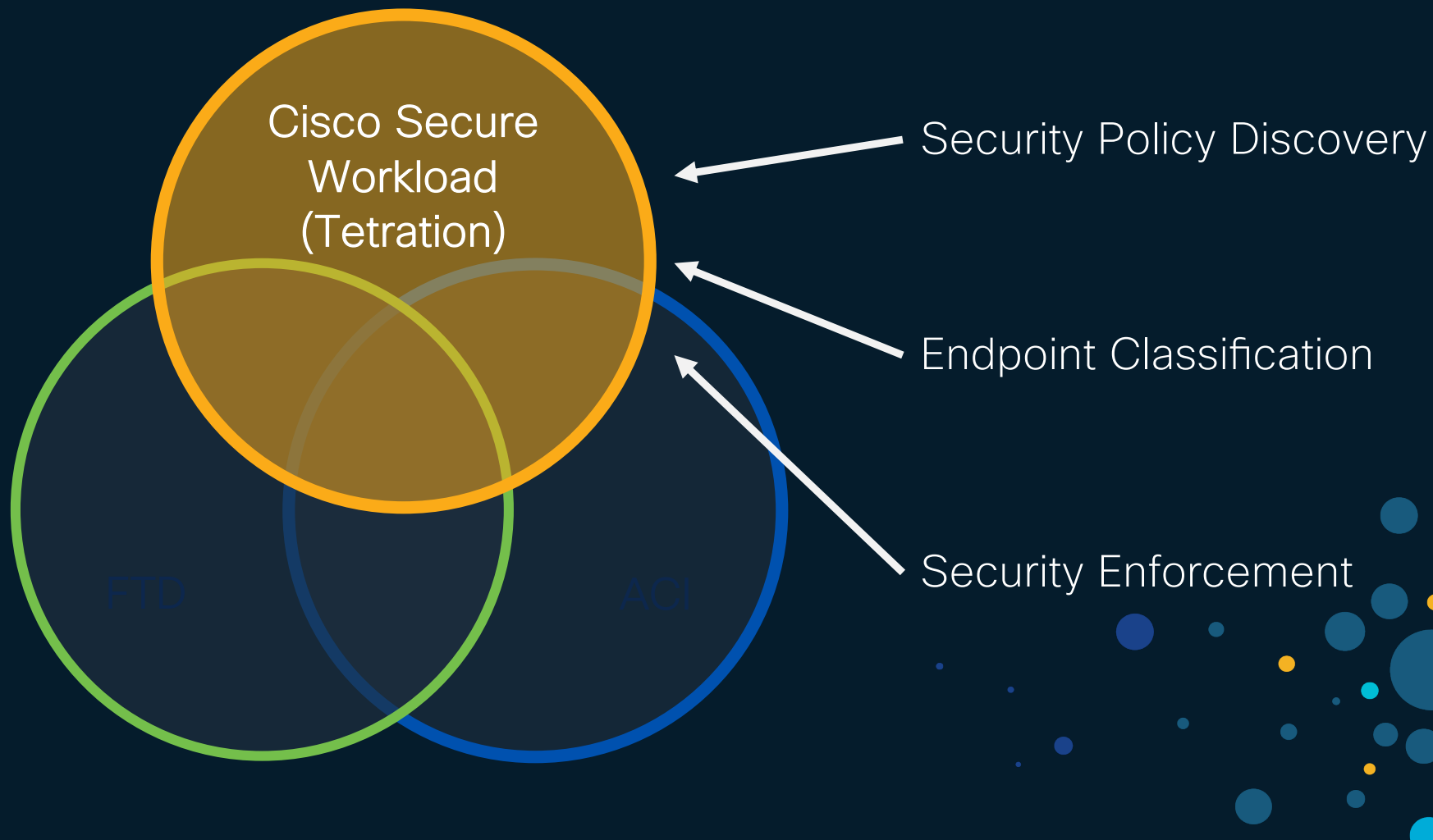
# SGT/ACI Firepower Integration



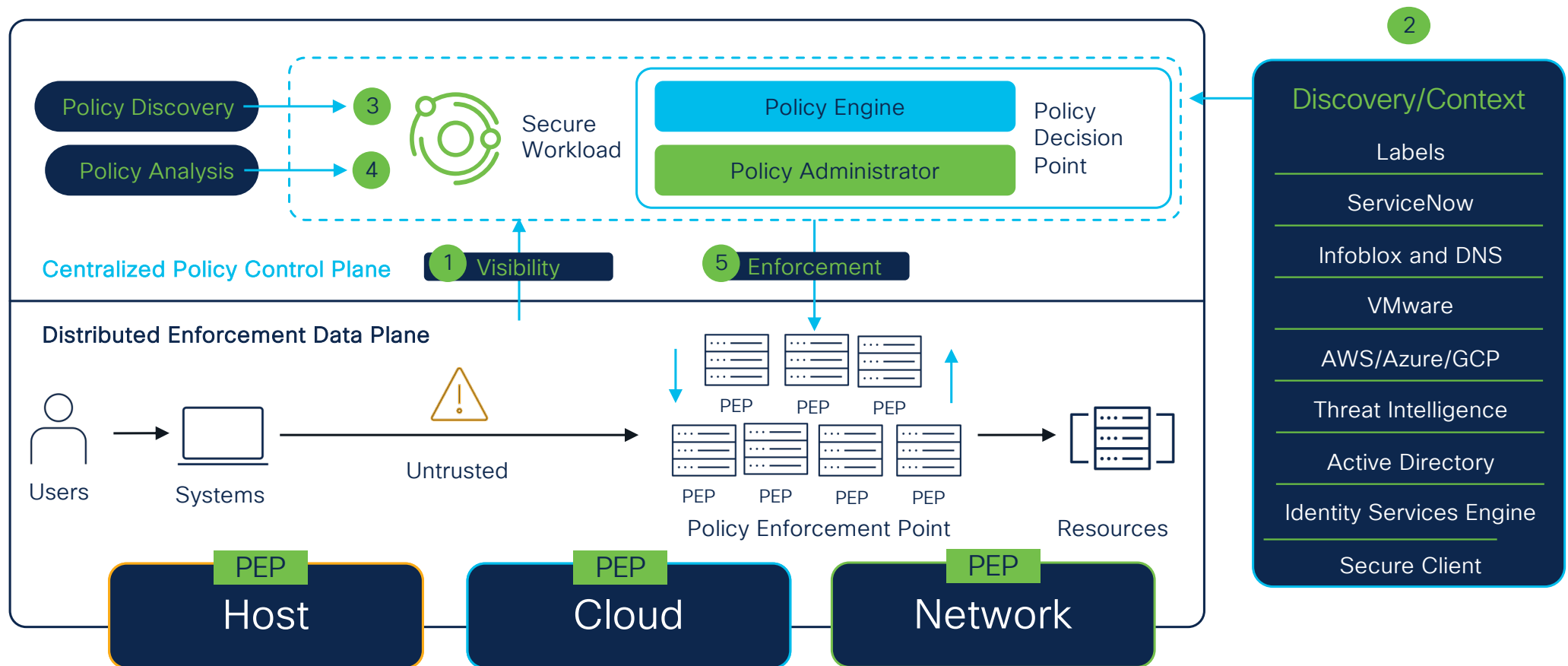
# FMC to APIC Rapid Threat Containment



# Cisco Secure Workload



# Secure Workload – Zero Trust Segmentation



# Secure Workload Use-Cases

Microsegmentation



Behavioral detection  
and protection

Vulnerability detection  
and protection

# Host-Based Agent - Features

## Lightweight

- **Doesn't sit on Datapath**
  - Runs on host OS
  - No kernel modification
  - Single process
- **Minimal resource footprint**
  - CPU 3%, 256MB Ram
- **Easy to install**
  - Script
  - Package
  - Template/Golden Image

## Configurable

- **Flow Visibility**
  - Detailed or Conversation
  - Process lookup/Users
- **Packages/Process visibility**
  - Vulnerable processes/packages
- **Forensics**
  - Process snapshot tree and TTP
- **Enforcement**
  - Enable/Disable
  - L3/L4/DNS/IP Reputation
  - Preservation of existing rules

## Resilient

- **Centralized upgrade**
  - Automatic or manual
- **Easy migration**
  - On-prem to SaaS rehomming
- **Protected communications**
  - Secured communication with Secure Workload Management (TLS 1.2 and 1.3)
  - Tampering protection
  - Telemetry buffering for network failures (up to 16GB or 7days)



# Host-Based DPU - Features

## Transparent

- No Guest OS agent install
  - Agent installed on DPU
- Minimal/Neglectable Performance Impact
- Minimal DPU config requirements
  - DOCA SDK
  - Network interface on DPU for agent communication
- Installer script for agent

## Feature-Set

- Hypervisor agnostic
- Minimal requirements
  - SR-IOV support
  - Guest OS SR-IOV virtual interface
- Baremetal support
- Flow visibility
- Enforcement

# Network-Based Agentless - Features

## Visibility

- **Common telemetry protocols**
  - NetFlow v9
  - IPFIX
  - NSEL (Secure Firewall/ASA)
- **ERSPAN**
- **Flow-Stitching**
  - NAT
  - VIPs and SNAT

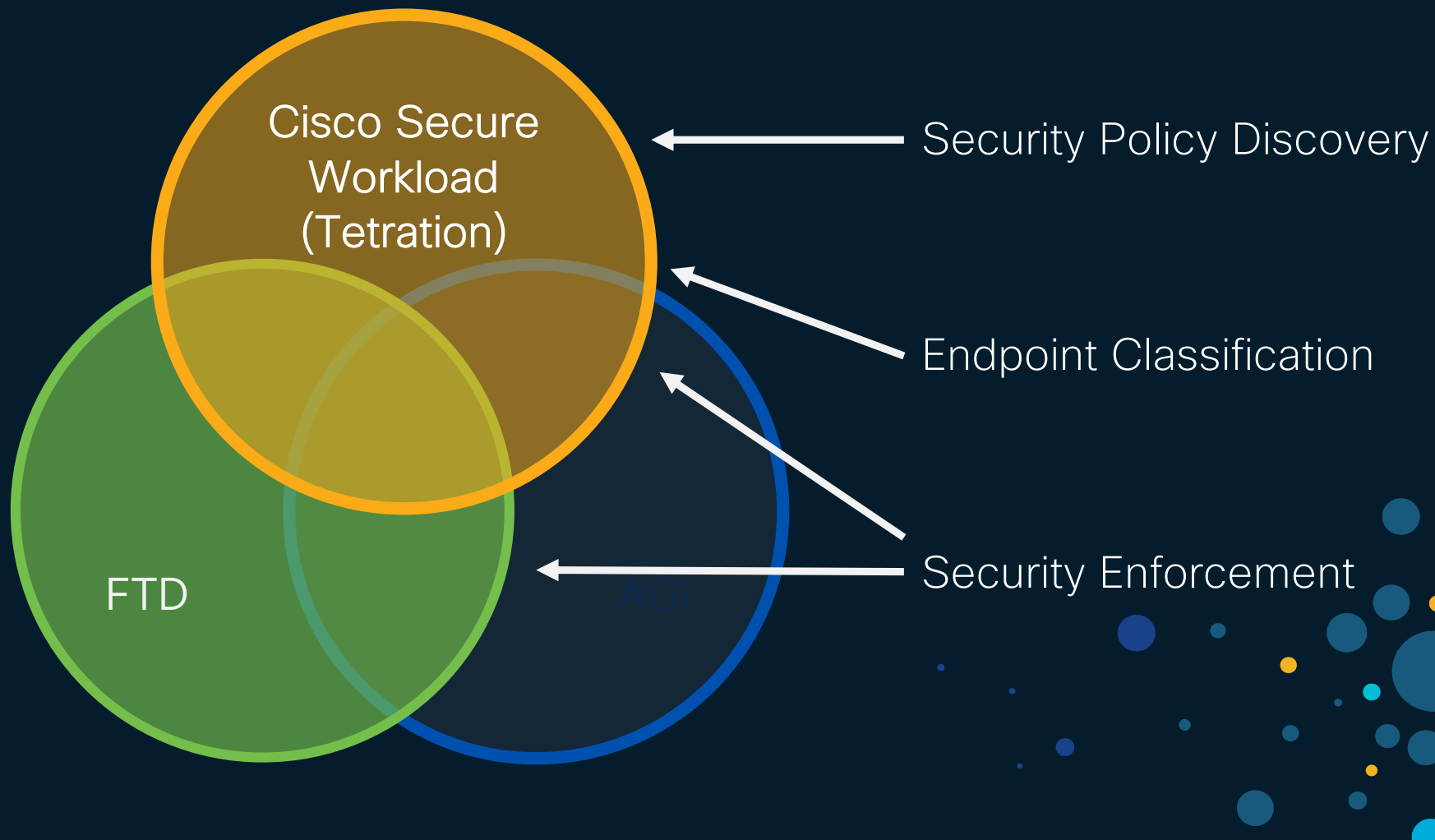
## Enforcement

- **Secure Firewall**
- **Load-Balancers**
  - F5 BIG-IP
  - Citrix NetScaler
- **ACI (3.9 patch 2)**
  - Visibility via Agents\*

## Scalability

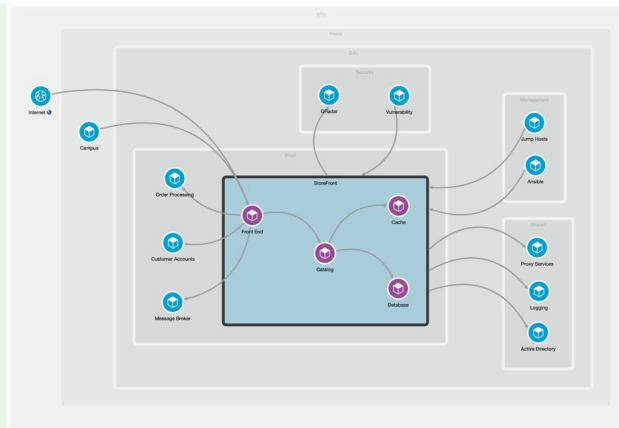
- **Ingest Appliance**
  - 3 connectors per appliance
  - 2 appliances in total
- **Up to 135k fps per appliance**
  - 45k fps per connector

# Cisco Secure Workload with FTD



# Secure Firewall & Secure Workload: better together

✓ Visibility and Enforcement



Cisco Secure Firewall  
Management Center

Native Integration

NSEL Records for ADM  
Policy

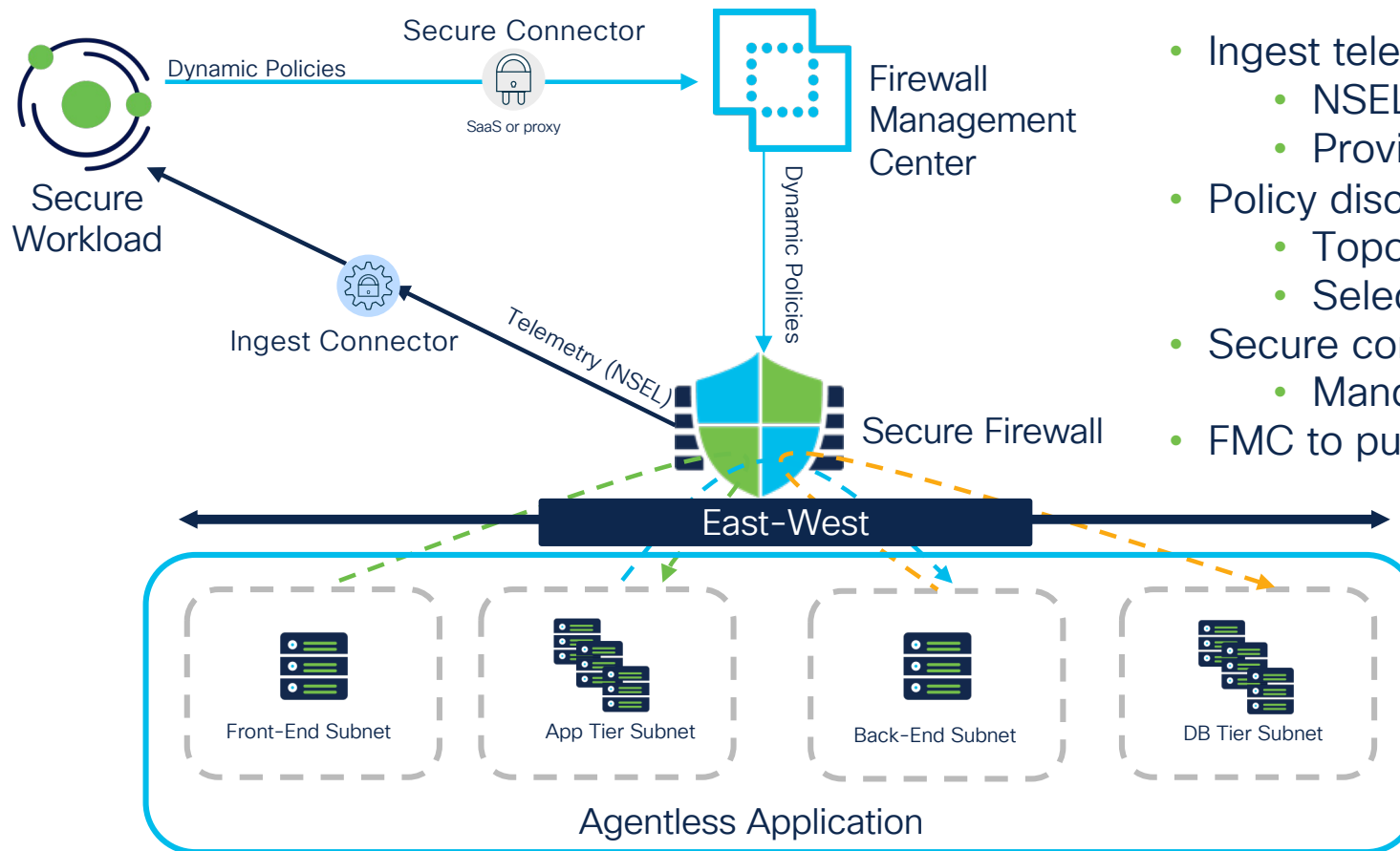
Access Control Policy  
(Dynamic Objects)

FMC Domain Awareness

Meaningful Dynamic Object  
names

Rule Ordering

# Secure Firewall – High Level Architecture



- Ingest telemetry information
  - NSEL via Secure Firewall connector
  - Provides End-to-End visibility
- Policy discovery and enforcement
  - Topology awareness via FMC connector
  - Selective rule pushing
- Secure connector if behind proxy
  - Mandatory with SaaS
- FMC to push policies to Secure Firewalls

Segmentation policies enforcement at firewall

# 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

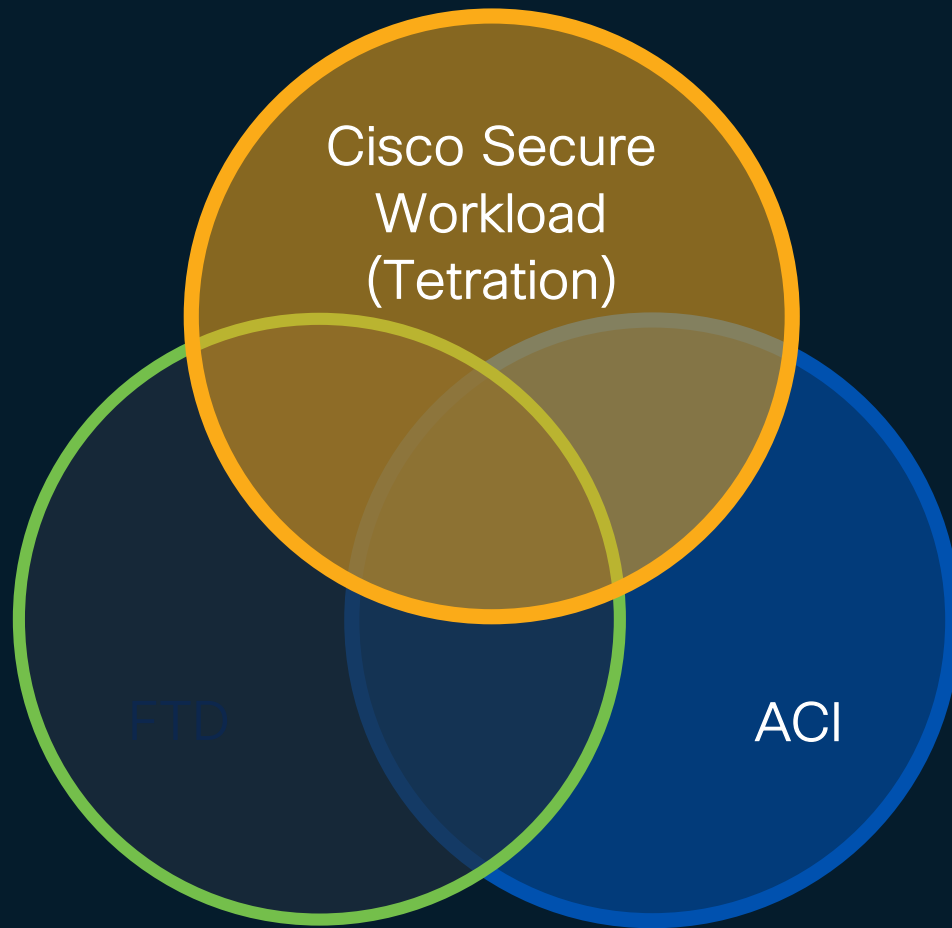


- Defense In-Depth
  - Attribute-Based hierarchical policies for agentless workloads
  - Rapid Threat Containment for agent and agentless workloads with FMC Remediation Module
- Policy Lifecycle Automation
- Enforce zero trust microsegmentation policies to applications where agent installation is not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

# End-to-end protection



# Cisco Secure Workload with ACI ?







The bridge to possible

# Thank you

