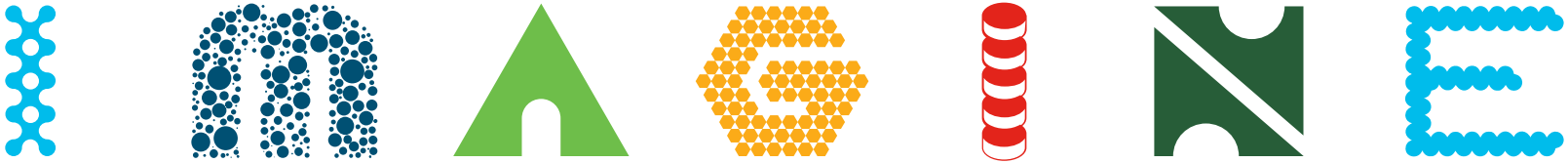
Cisco live!

January 28 - February 1, 2019 - Barcelona

cisco



INTUITIVE

BRKACI-2301

Practical Applications of Cisco ACI Micro Segmentation

Andy Sholomon

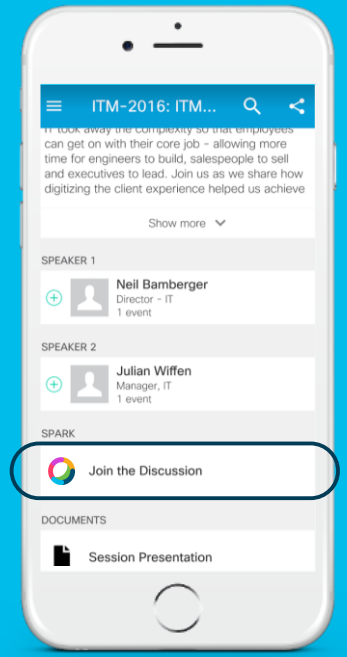
@asholomon, Principal Engineer – DC Switching

Session Objectives

- Provide an overview of what we mean when we talk about implementing Micro Segmentation
- Describe the ACI features that help deploying Micro Segmentation
- Deep dive on what you can do with Micro EPGs and ACI contracts
- Provide ideas of how to use these features
- Show these features working on simple yet practical examples
- Show an example of Tetration and explain how it can work with ACI

Some comments about this deck

- We will cover some of the topics via examples and showing demos
- In the deck there are links to the code and videos of the demos
- Some slides are provided for your reference only, we may not talk through them.



cs.co/ciscolivebot#BRKACI-2301

Cisco Webex Teams

Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

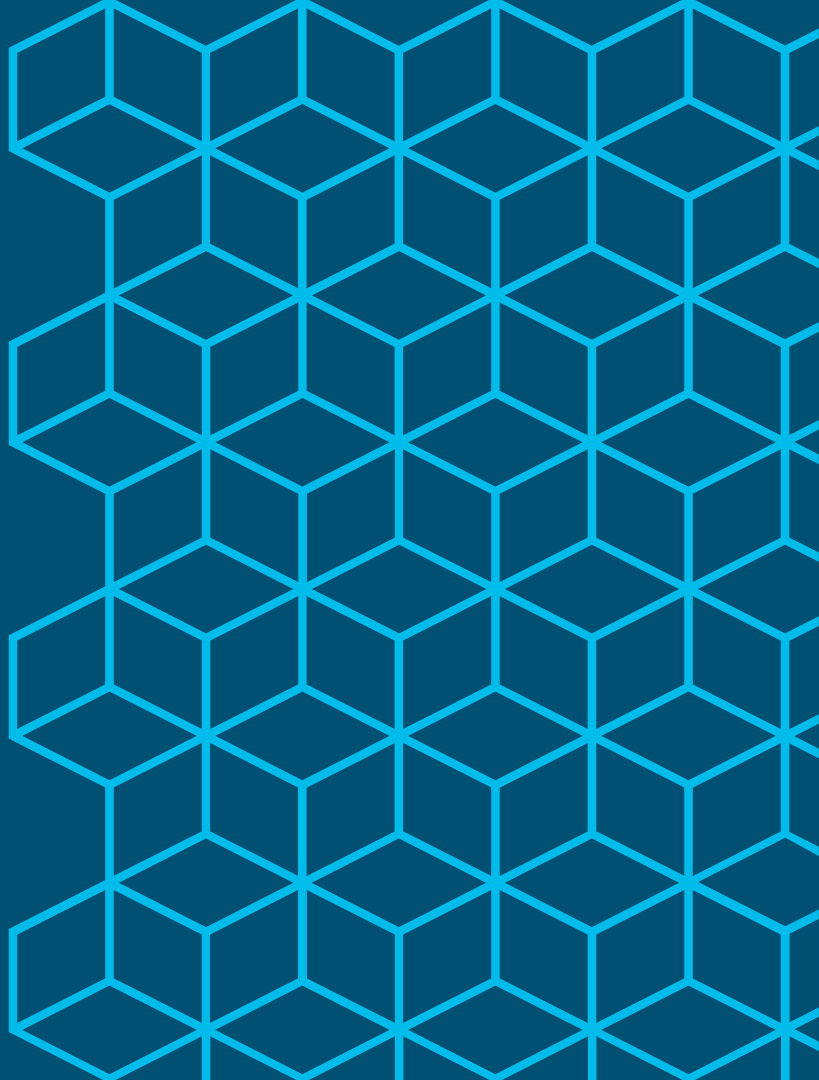
How

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

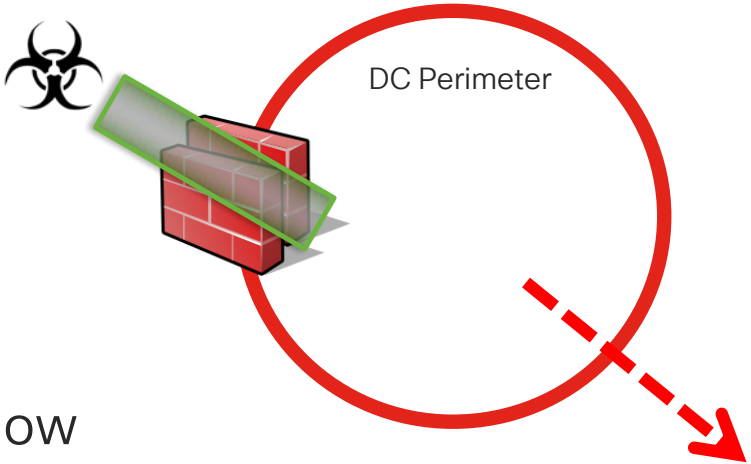
Agenda

- Micro Segmentation Fundamentals
- Endpoint Identity Using EPGs and Micro EPGs (uEPG)
- ACI Contracts for Policy Definition
- Improvements in Hardware Utilization
- ACI and Hybrid Cloud Security
- Demo

What do we mean by Micro Segmentation?

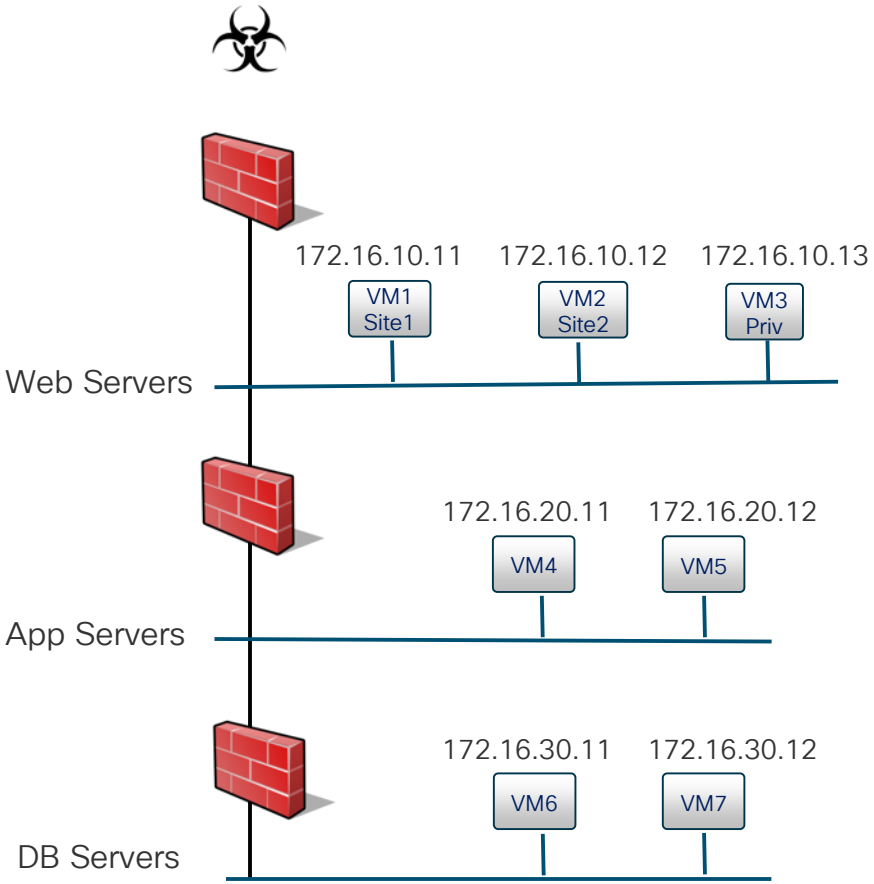


Why Micro Segmentation?

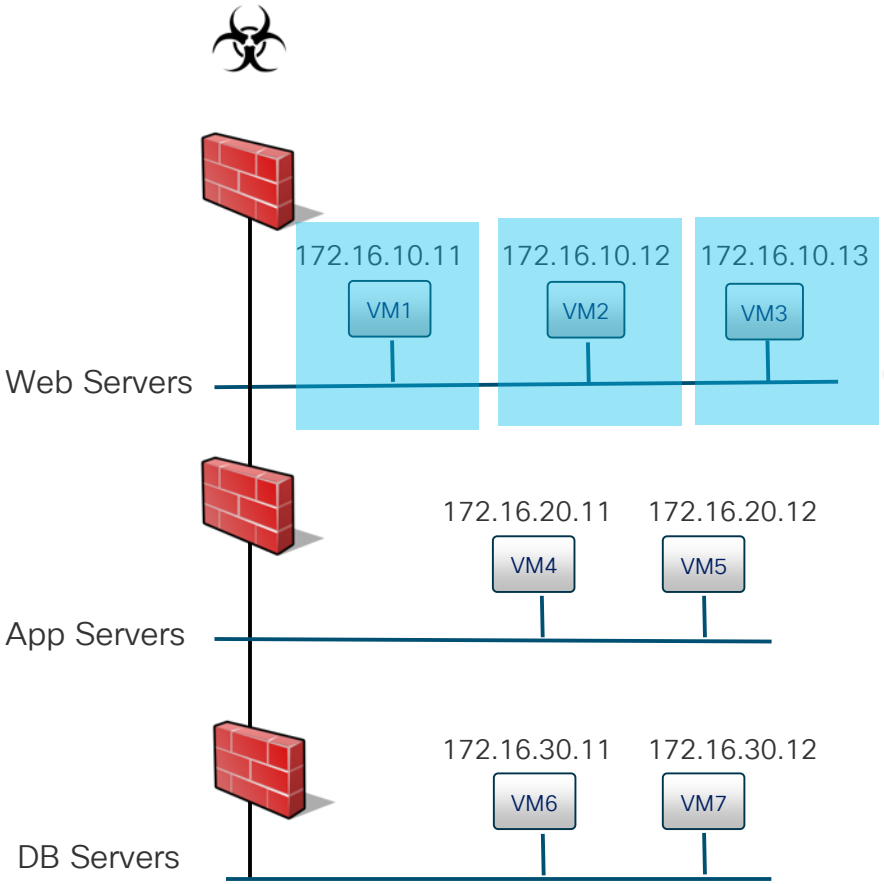


- Perimeter security is not enough: once it is breached, lateral movement can allow attackers to compromise more assets
- Micro Segmentation can improve the security posture inside the Data Center
- Micro Segmentation can minimize segment size and provide lesser exposure for lateral movement

Security Risk: VMs or Servers on a Single Subnet

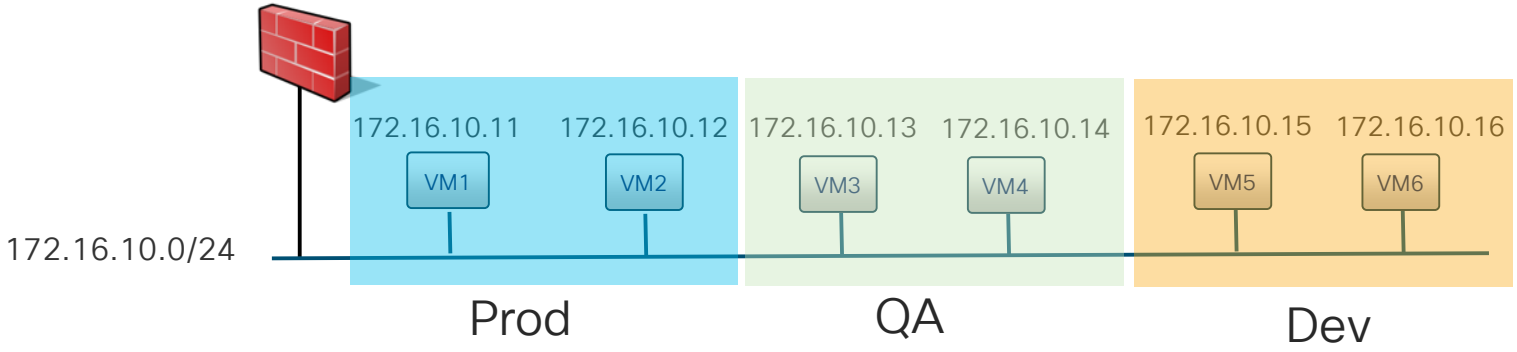


Security Risk: VMs or Servers on a Single Subnet

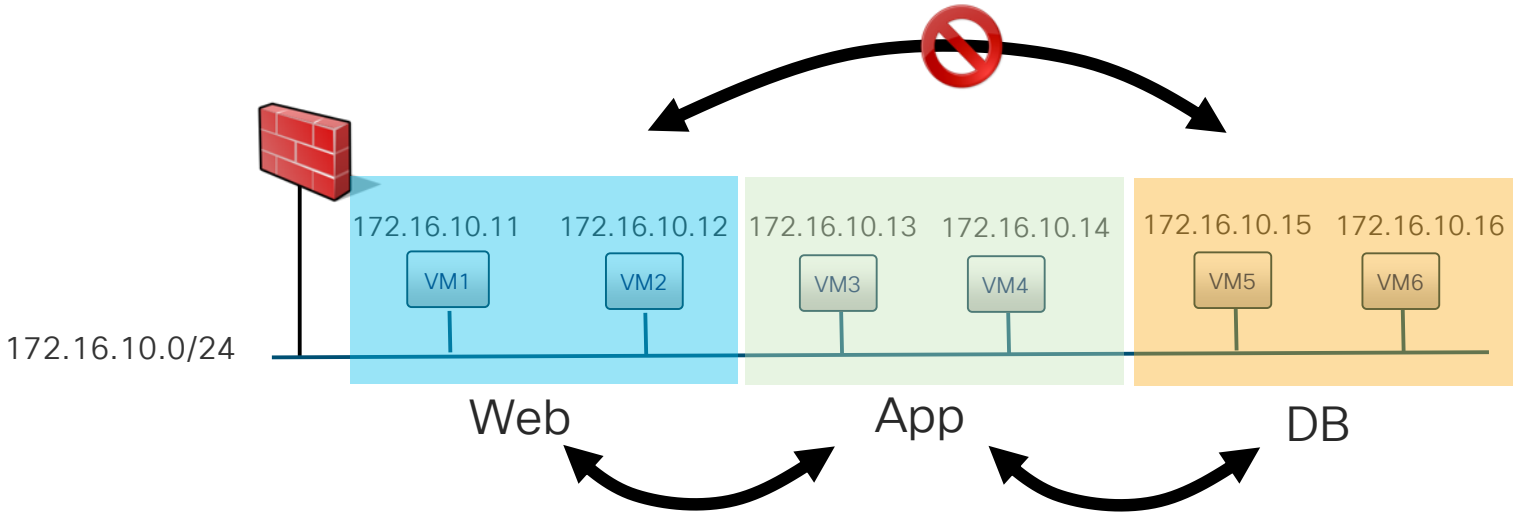


Very simple Micro Segmentation use case

A Micro Segmentation Use Case



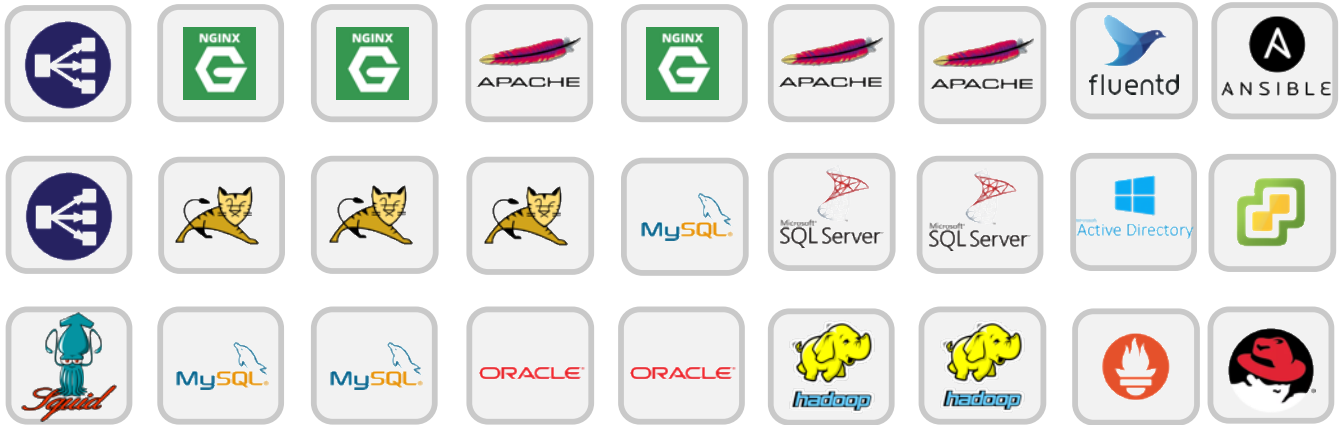
Another Micro Segmentation Use Case



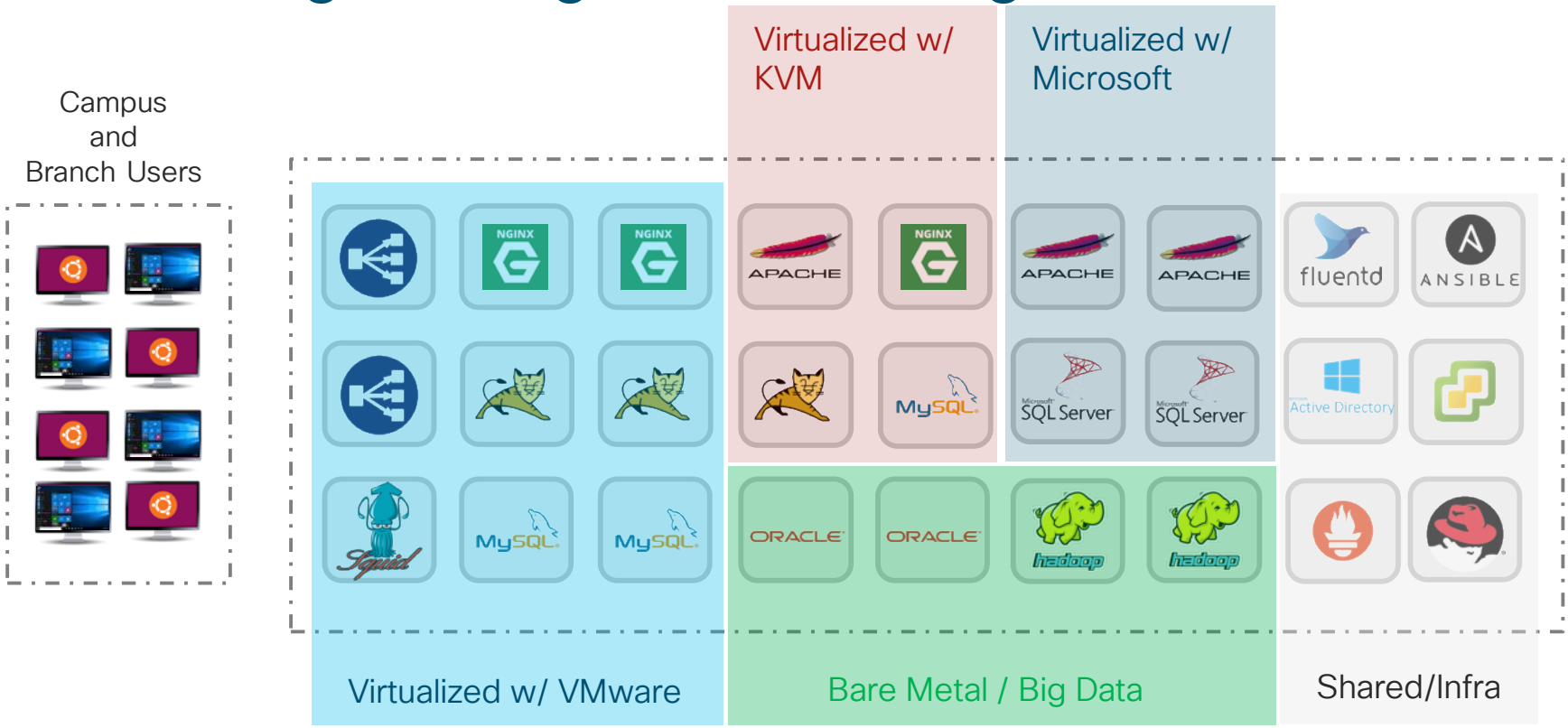
Micro Segmenting in an Heterogeneous Data Center

Campus
and
Branch Users

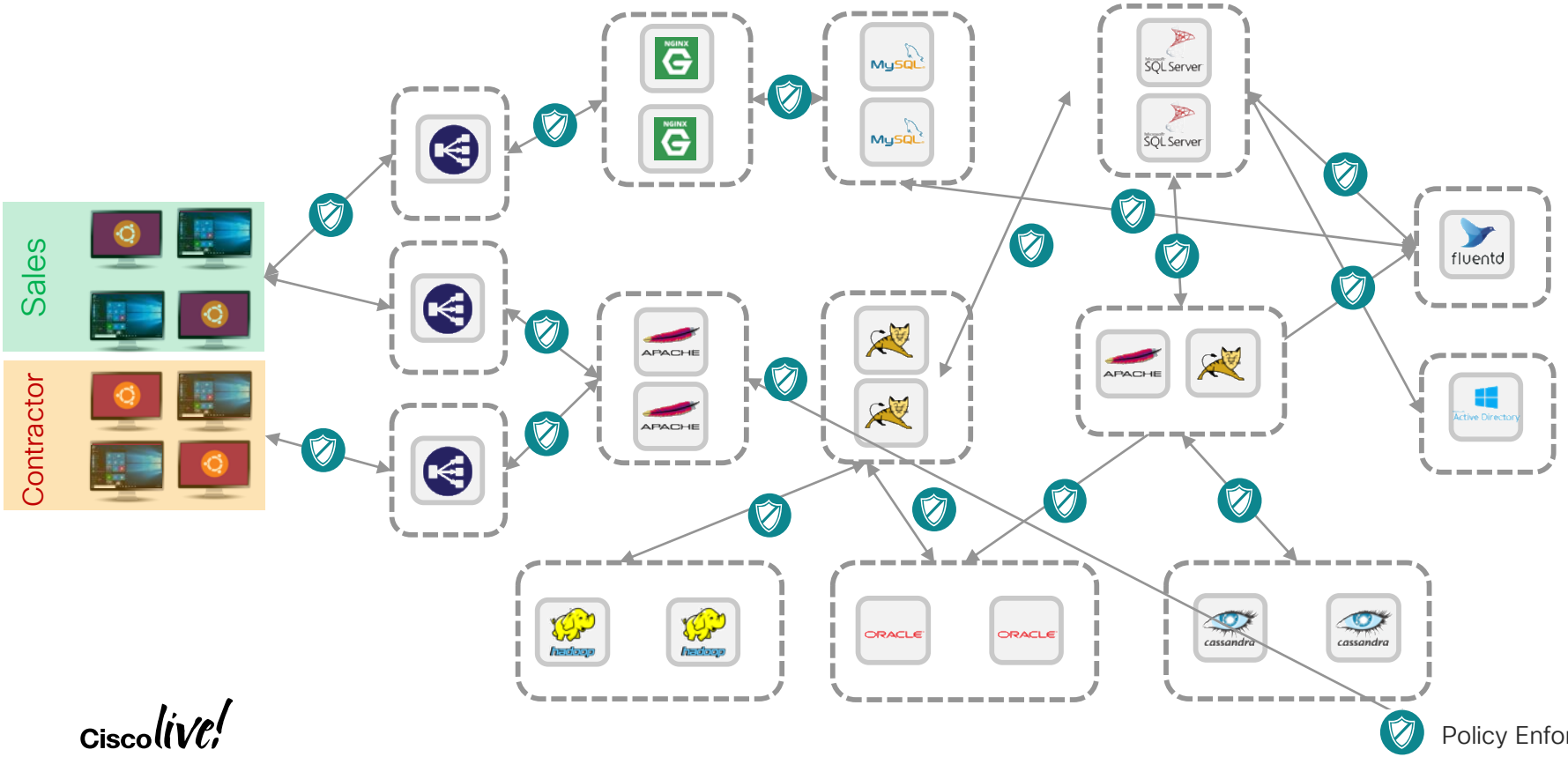
Many different types of workloads running in a Data Center



Micro Segmenting in an Heterogeneous Data Center



Micro Segmenting requires granularly grouping endpoints, and defining and enforcing policy between them



Key Functions to Achieve Micro Segmentation

Endpoint Identity

Classify endpoints into groups:

- Network identity (IP/MAC/VLAN)
- Meta-data: VM attributes, labels, tags, etc.
- DNS
- User Authentication (i.e. from ISE)

Policy Definition

Determine what policy to configure between groups:

- Application Dependency Mapping
- White-List vs. Black-List
- Policy Simulation
- Dynamic vs. pre-defined

Verify and Refine

Verify policy enforcement, lifecycle management:

- Policy visibility
- Logging and log analysis
- Alerts, remediation
- Constant updates

Enforcement Points

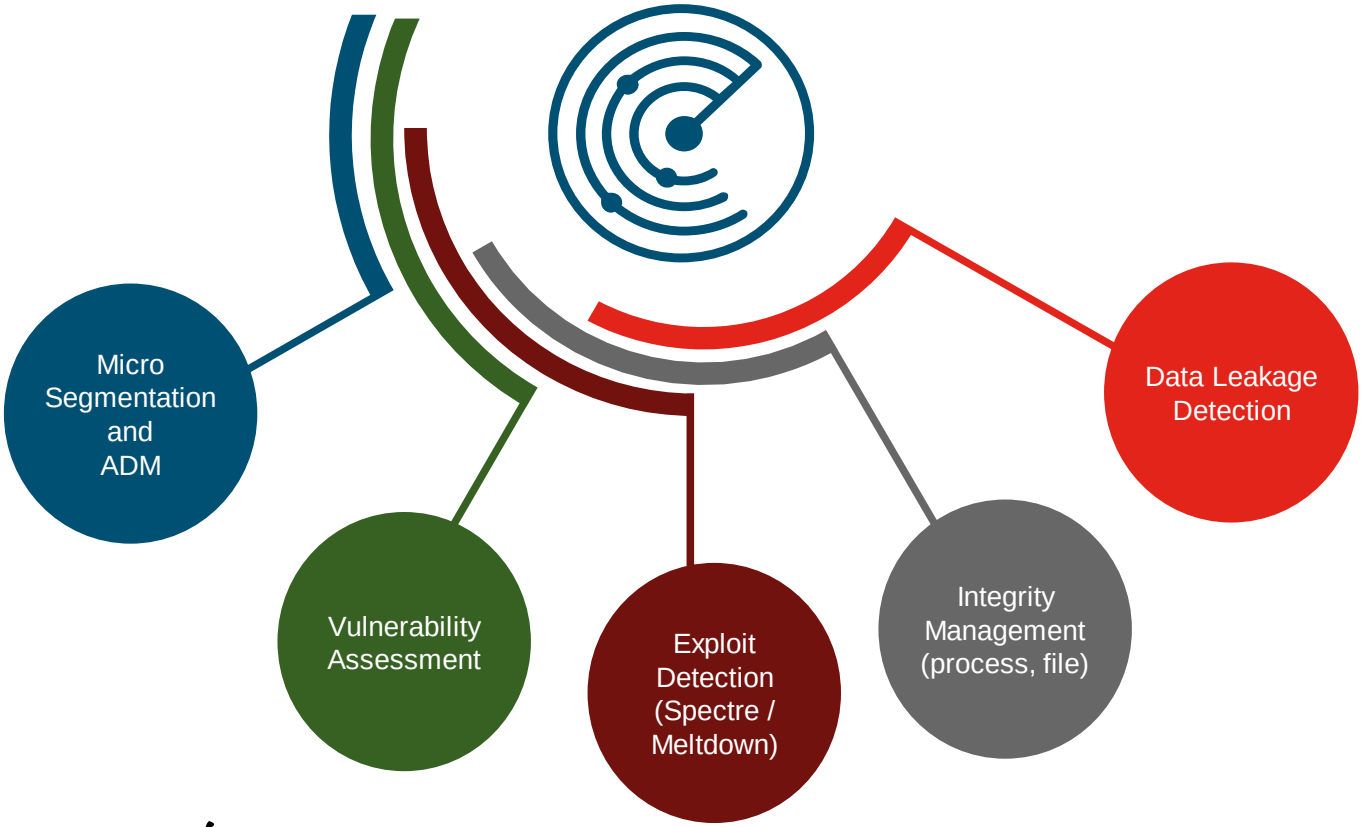
Host-based - Centrally manage host-based firewalls

- Pros: distributed, network independent, very granular policies possible, process-level visibility and correlation
- Cons: Guest-OS dependent

Network-based - Centrally manage access rules at the network edge (Virtual Switch, Physical Switch or both)

- Pros: distributed, guest independent, group based policies for best scale, endpoint-level visibility and correlation
- Cons: requires network hardware resources (memory, TCAM, etc) for policy

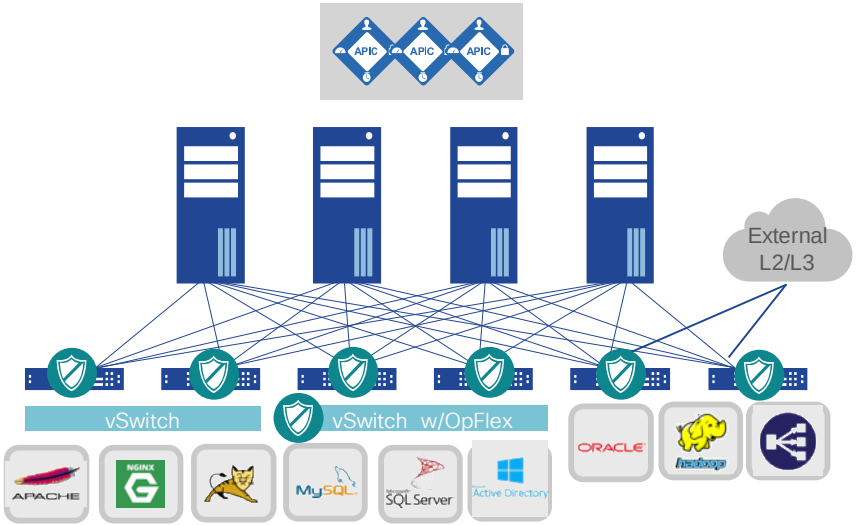
Cisco Tetration – cloud workload protection



- ✓ Real time
- ✓ Thousands of workloads
- ✓ On premises and public cloud
- ✓ All types of workloads from mainframes to containers

ACI implements distributed network policies

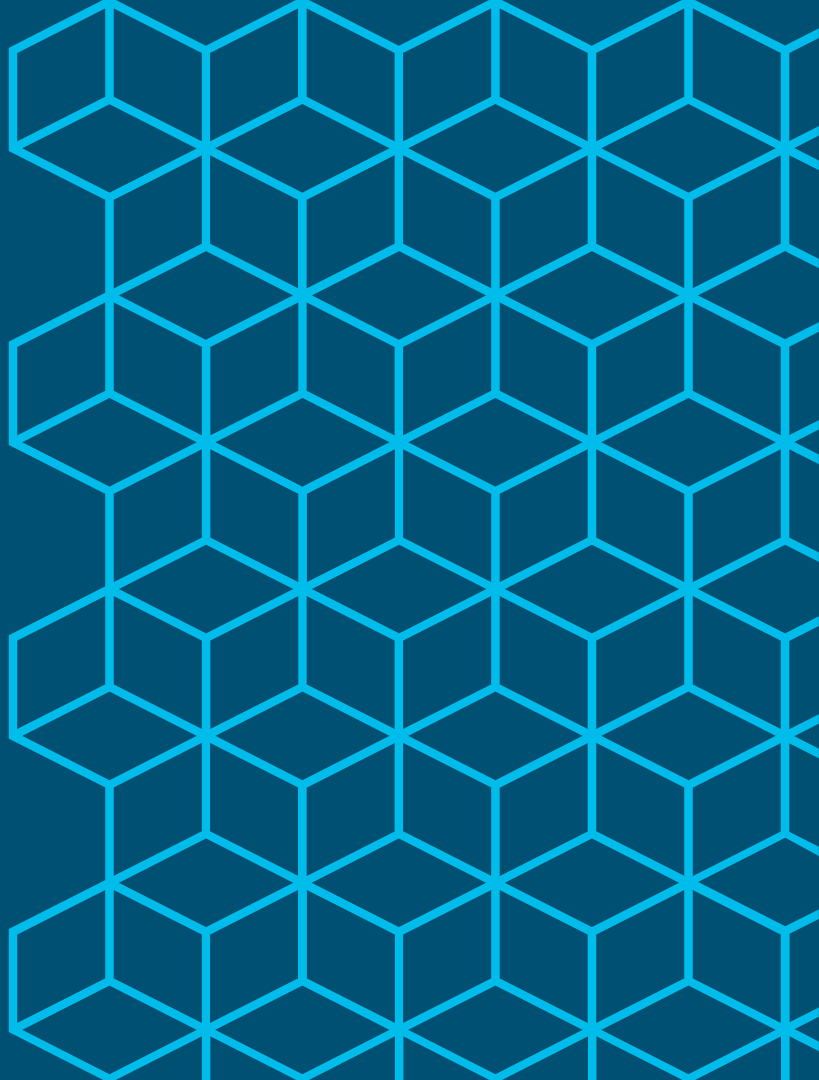
- Contracts define Layer2-Layer4 security policies.
- ACI distributed security policies are implemented at different enforcement points:
  - Leaf: hardware based, no performance penalty.
  - vSwitch (i.e. OVS, AVE): closest to VM, stateful connection tracking



You can combine **both host-based and network-based** for tiered-security and operational reasons (SecOps vs. NetOps vs. DevOps).

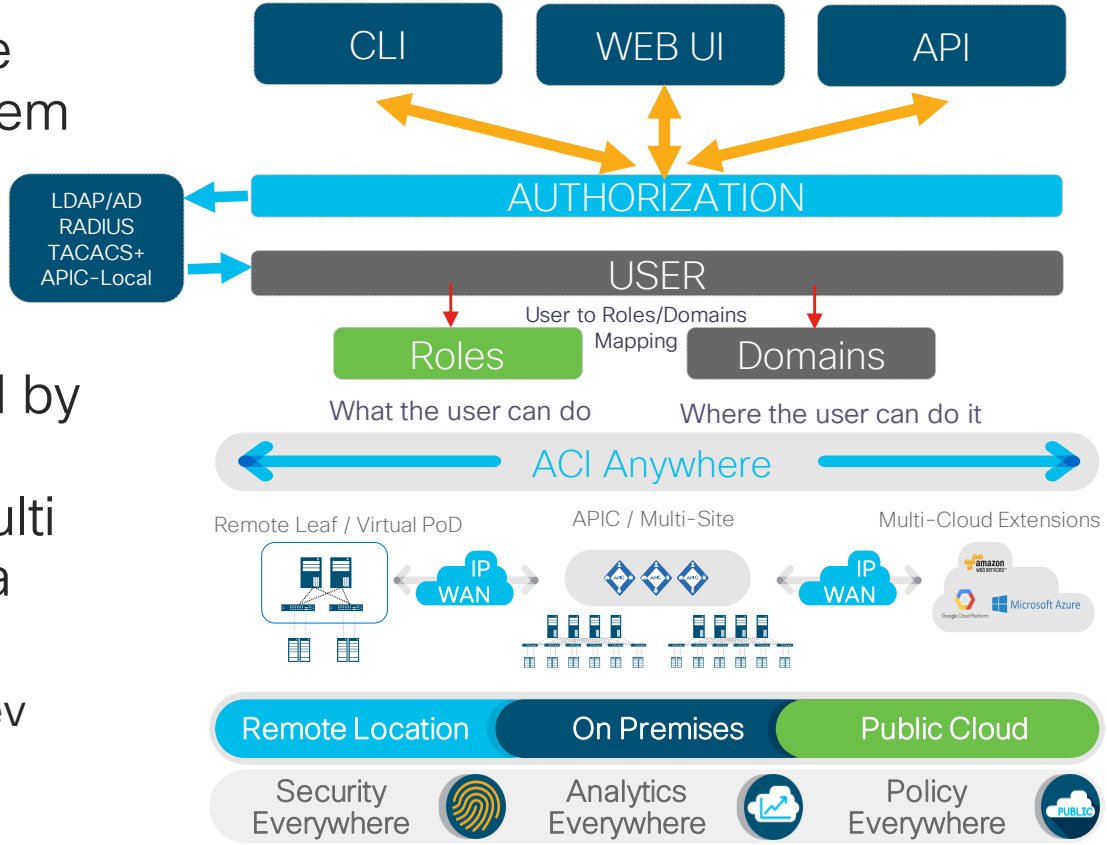
Learn more: BRKACI-2010 – Tetration and ACI: Better Together

ACI RBAC

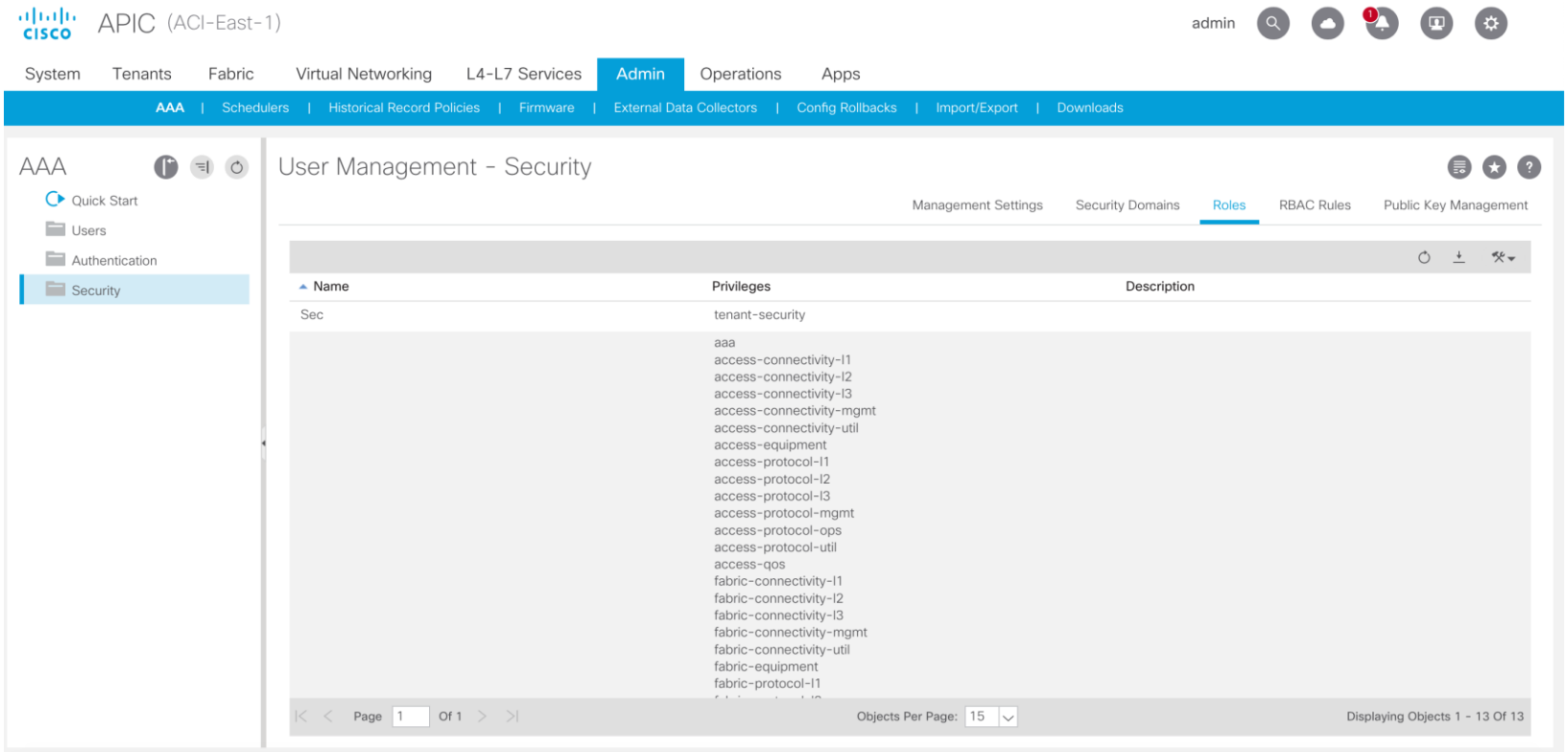


ACI Configuration Management

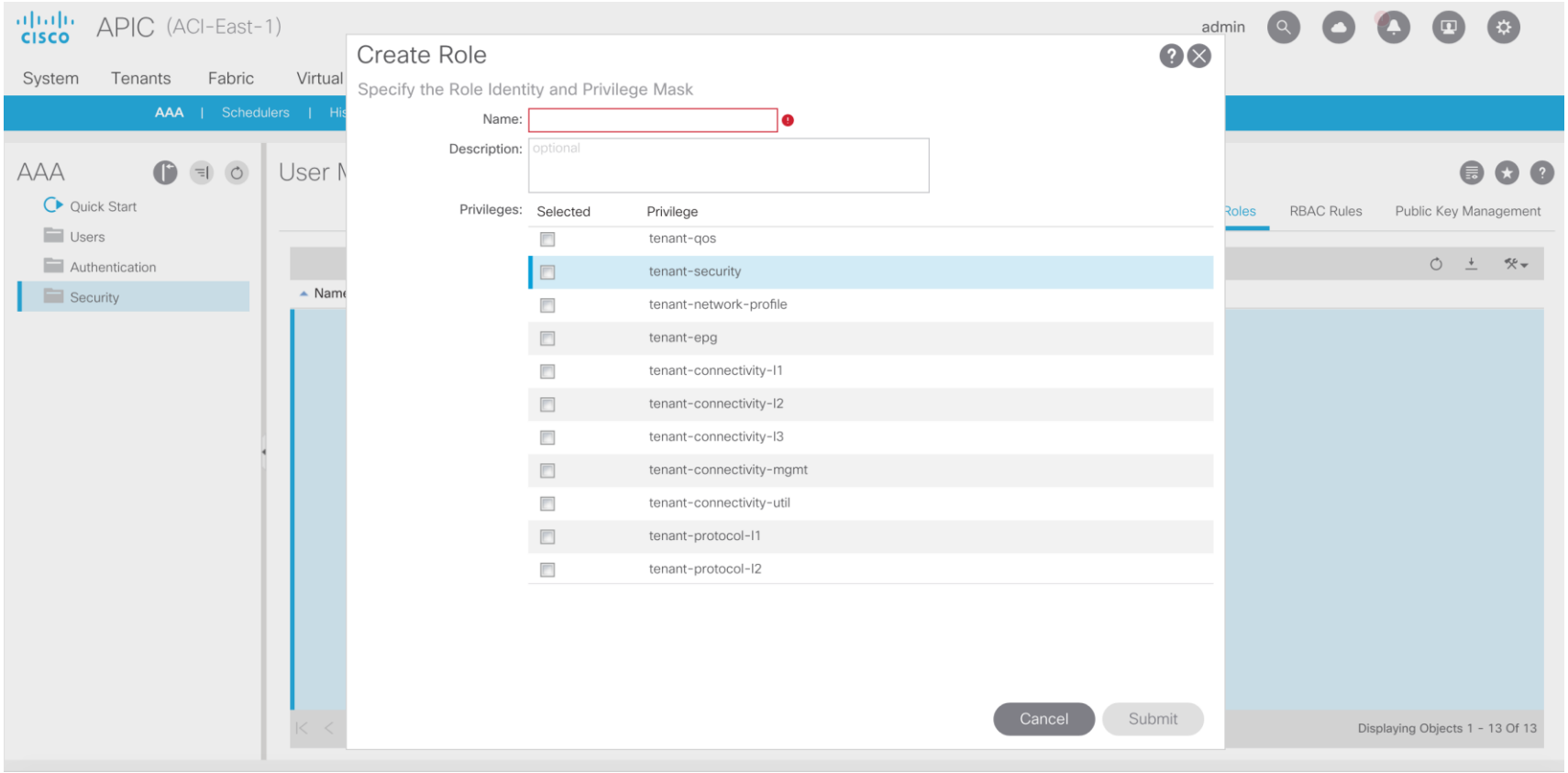
- ACI has 3 ways to manage the entire DC fabric; on and off prem
  1. Web UI
  2. CLI
  3. API
- All three methods are secured by RBAC (Role Based Access Control) and allow granular multi tenancy configuration for extra flexibility
  - For example, if desired, your “Dev Tenant” admin cannot see or configure your “Prod tenant”



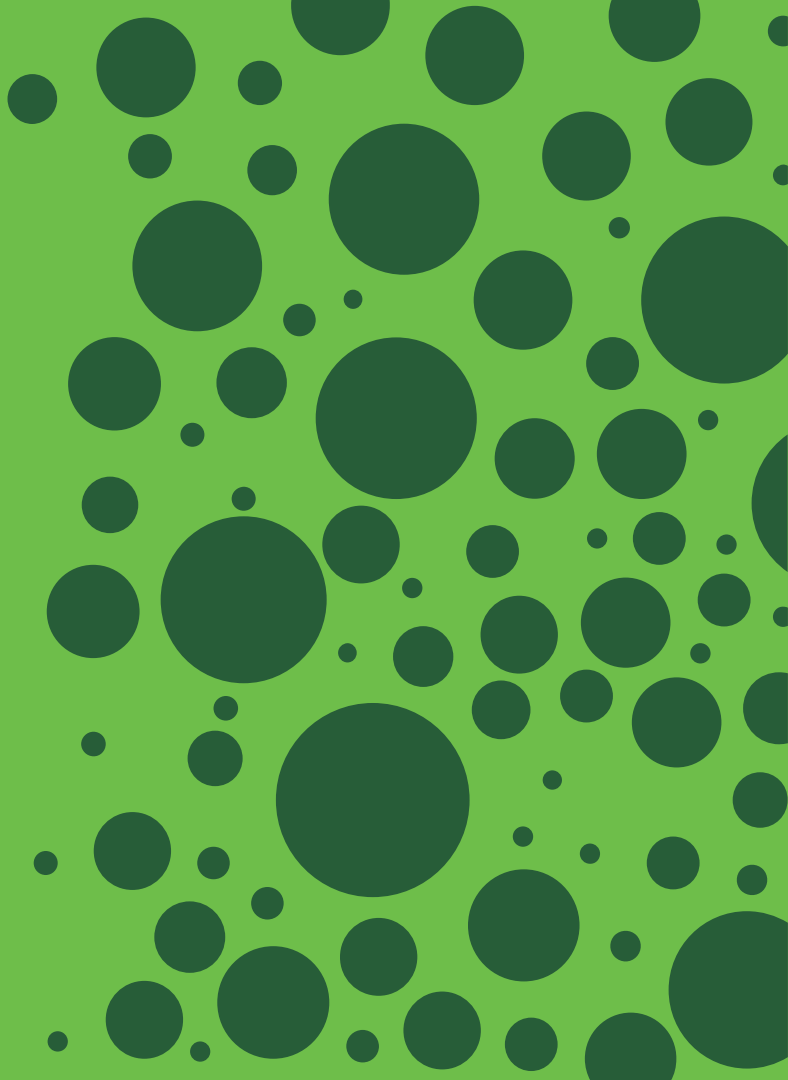
ACI RBAC Roles are very granular



ACI RBAC Roles are very granular



With the granular RBAC capabilities there is a capacity to split roles/responsibilities for users



Agenda

- Micro Segmentation Fundamentals
- Endpoint Identity using EPGs and Micro EPGs (uEPG)
- ACI Contracts for Policy Definition
- Improvements in Hardware Utilization
- ACI and Hybrid Cloud Security

But before we talk about Micro EPGs … a quick refresher on the ACI policy model and endpoint domains

So What's an Endpoint Group (EPG)?

Endpoints are "grouped" to attach them to the fabric.

An **Endpoint Group (EPG)** is a set of devices (or VMs) that share the same policy requirements.

Communication Between EPGs

By default:

Endpoints inside an EPG can talk to each other

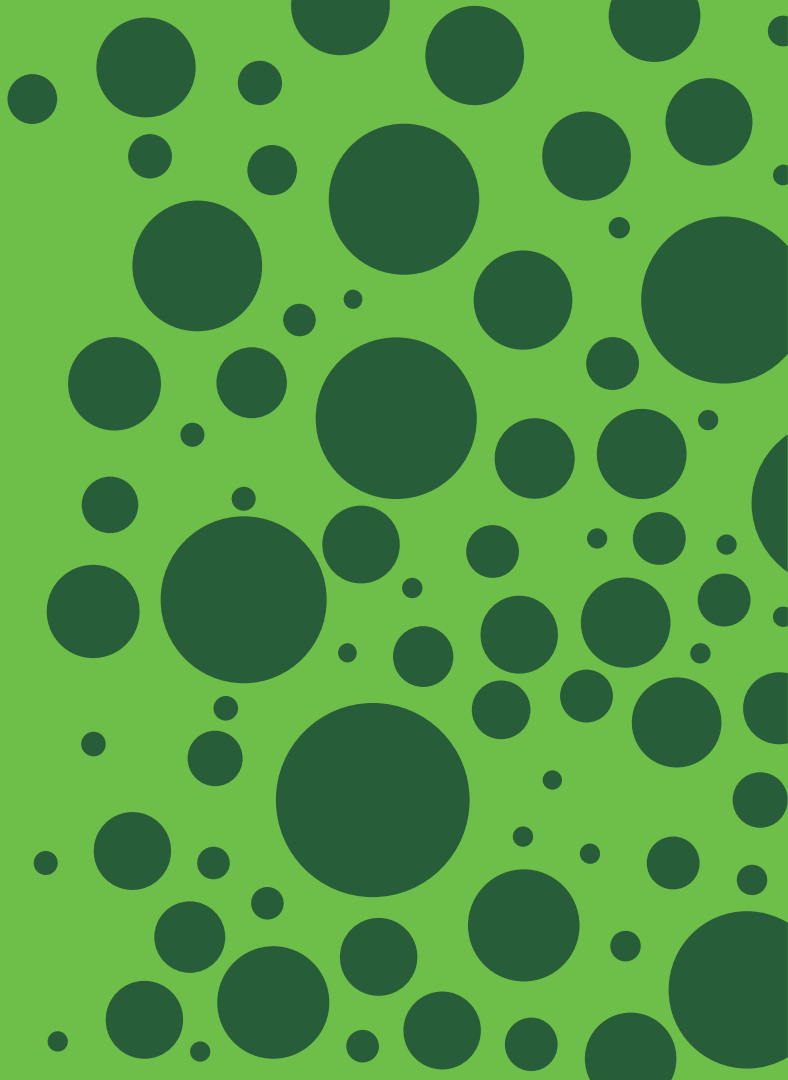
Endpoint Groups (EPGs) cannot communicate with each other.

To allow EPGs to speak with each other we connect them using **contracts**

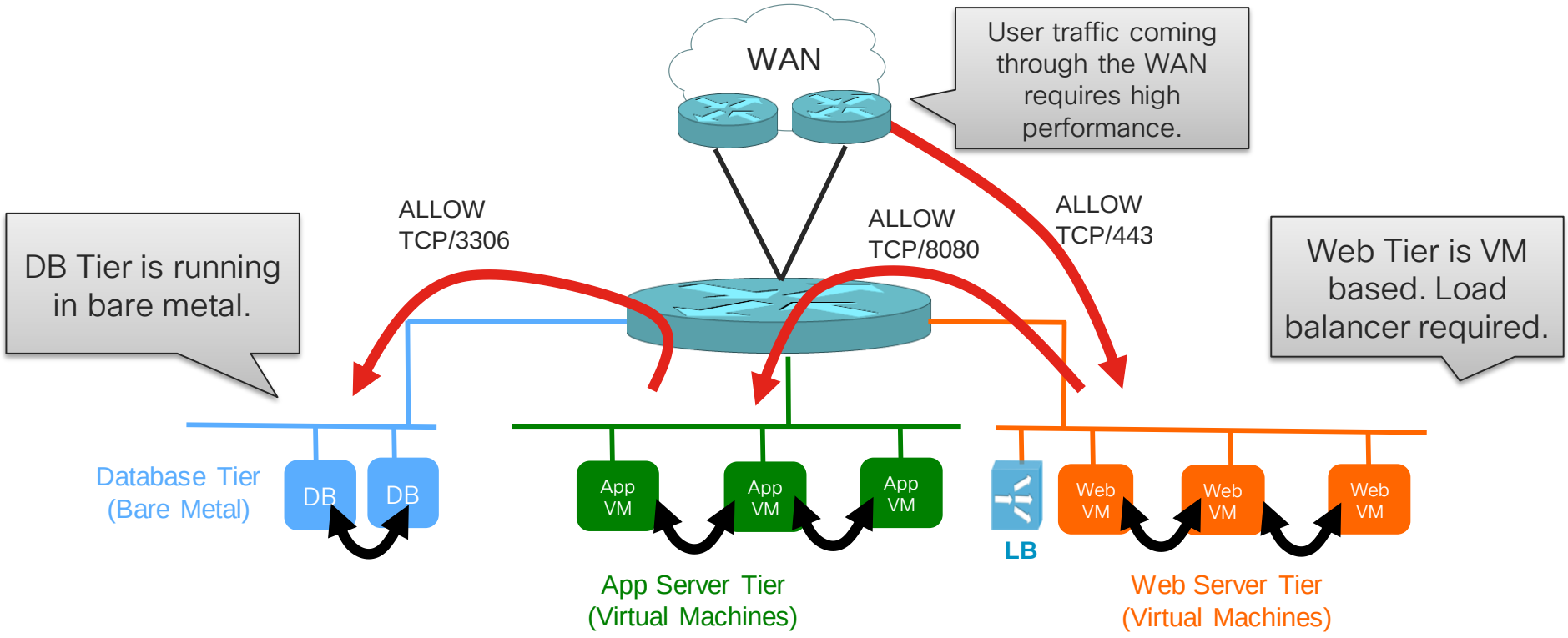
ACI uses a "white list model."

Remember...that's the default behavior. It can be changed.

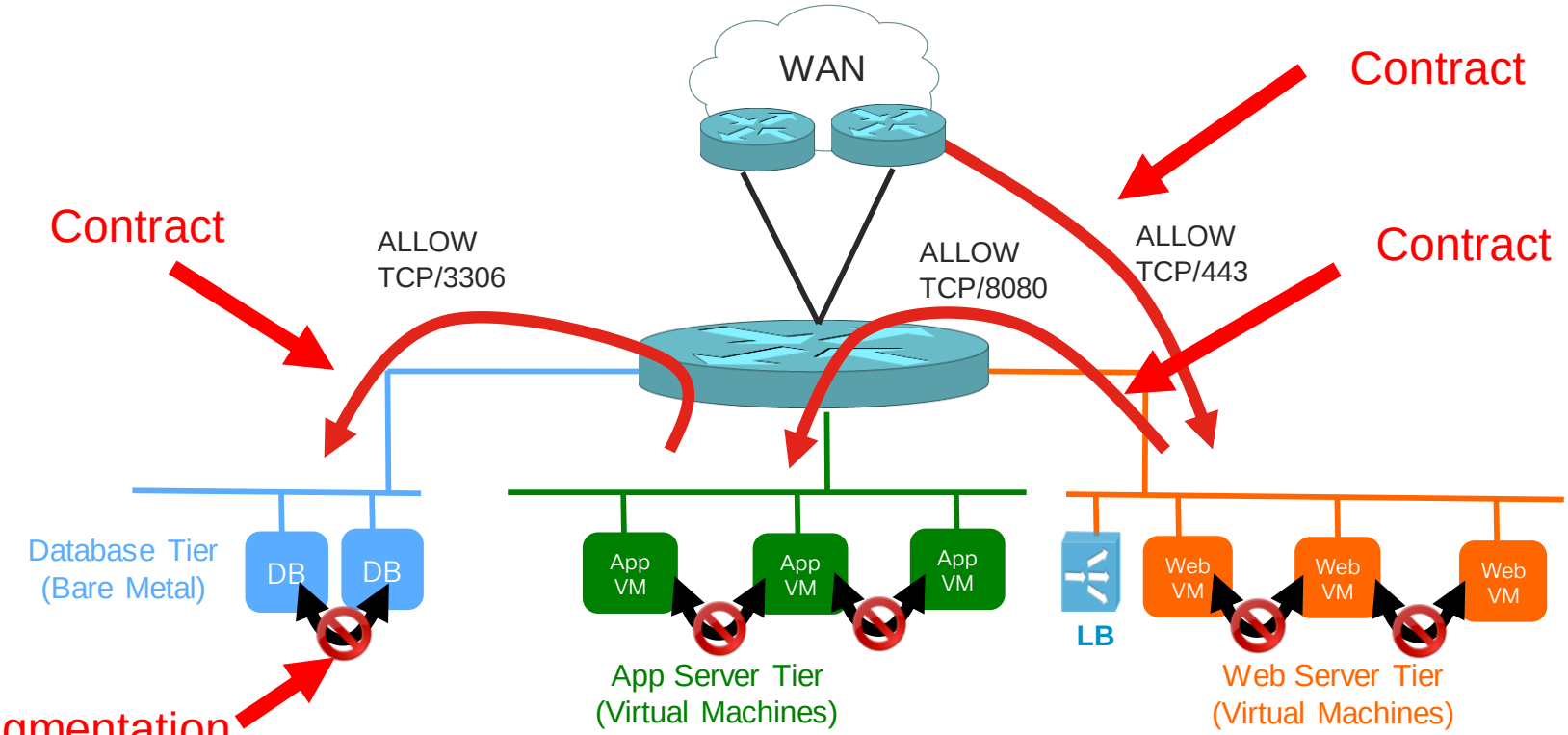
Now let's talk about contracts.



A typical 3-tier application with a non-virtualized database



Contracts



A contract can use a Service Graph

Understanding Fabric Domains

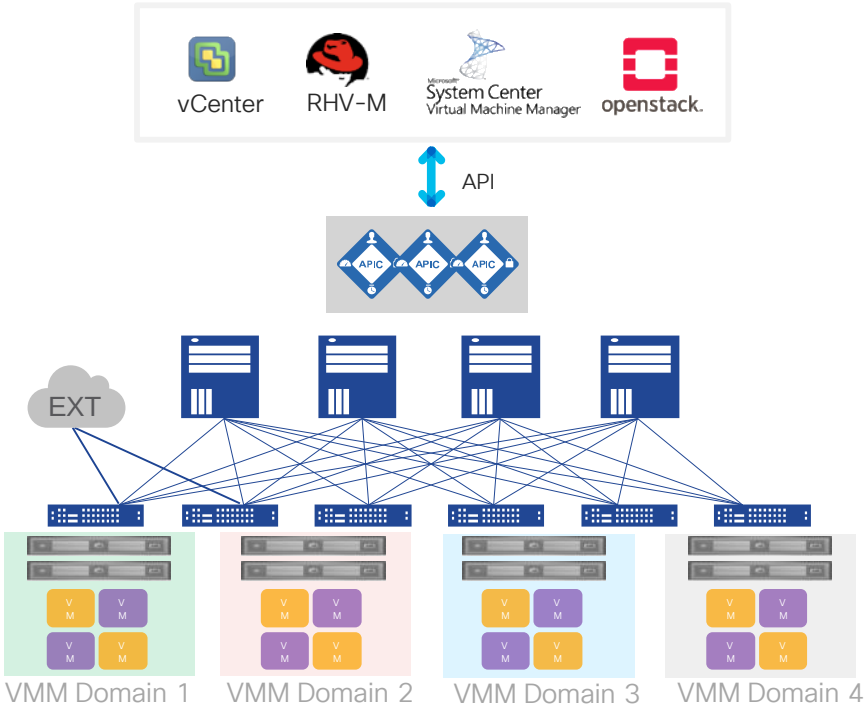
Fabric Domains represent the connectivity type for a physical port:

- Physical Domains (PhysDoms) – any type of endpoint (Bare Metal, IP Storage, etc.)
- External Bridge Domains – endpoints that are on an external L2 fabric
- External Routed Domains – IP endpoints external to the fabric
- FibreChannel Domains – FC endpoints
- Virtual Network Domains (VMM Domains) – VM or Container endpoints connected to the fabric via a domain manager that provides virtual network information.

Understanding Fabric Domains (contd.)

- Fabric domains also help APIC manage the allocation of certain resources for different types of endpoints:
  - Encapsulation pools: VLAN and VXLAN
  - Address pools: IP Multicast address pools
  - Security Domains
- Ports associate to the Domains via **Attachable Entity Profile (AEP)**

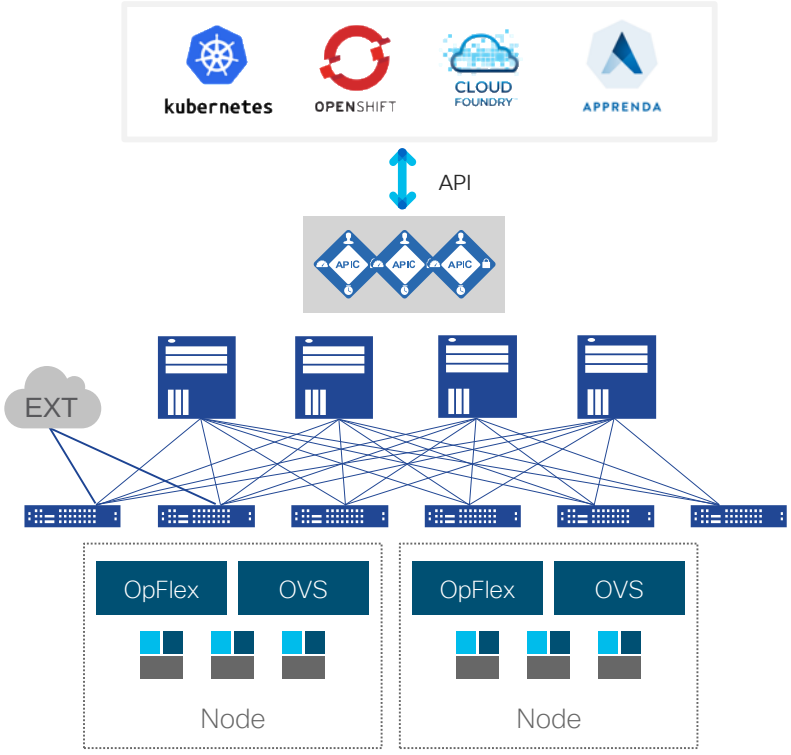
Virtual Machine Manager (VMM) Domains for Hypervisor Integration



- API Relationship is formed between APIC and Virtual Machine Manager (VMM)
- APIC obtains virtualization inventory, performs virtual and physical correlation

  APIC has visibility of hypervisor hosts, Virtual Machines, vNICs and more.
- APIC manages the hypervisor virtual switch (VDS, OVS, AVE, etc …) via either API or Opflex
- Multiple VMMs supported on a single ACI Fabric simultaneously

Containers / PaaS Integration with ACI CNI Plugin



- Integration with kubeapi server, APIC obtains inventory of nodes and Kubernetes objects.
- ACI CNI Plugin Implements:

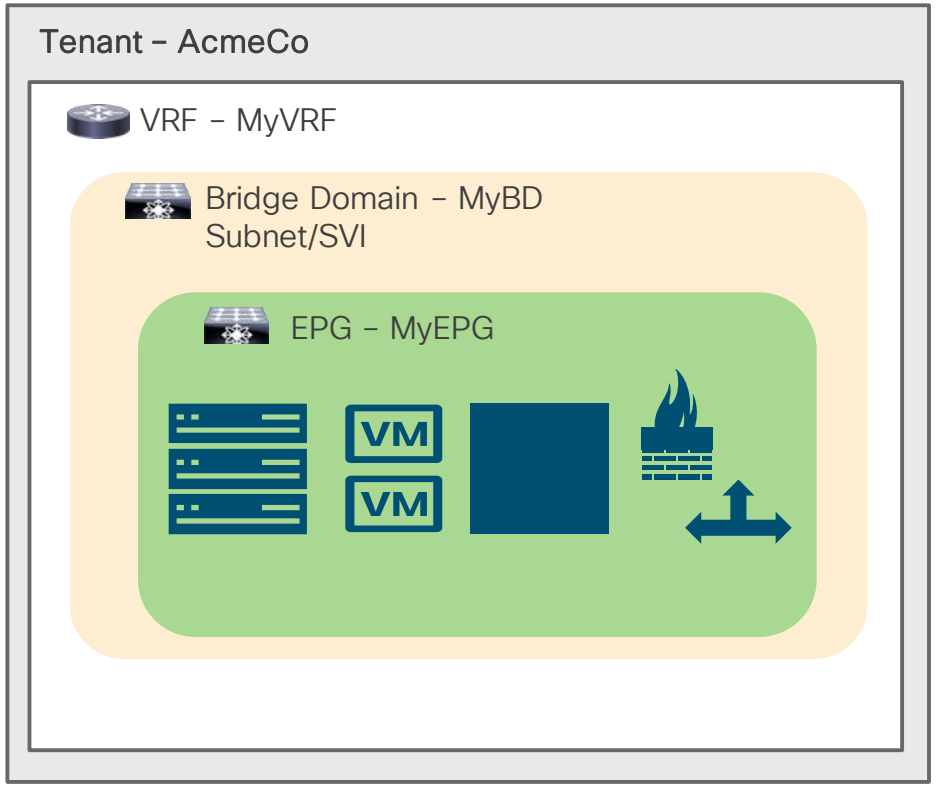
  Distributed OVS Load Balancer for *ClusterIP* services.

  Distributed HW Load Balancer for *LoadBalancer* services.

  Distributed Kubernetes Network Policies
- Secure multi-tenancy and ACI policies
- Visibility: Live statistics in APIC per container, health metrics

Learn more: BRKACI-2505- Deploying Kubernetes in the Enterprise with Cisco ACI
BRKACI-3330 - Openshift and Cisco ACI Integration

The ACI Network and Policy Model in one slide



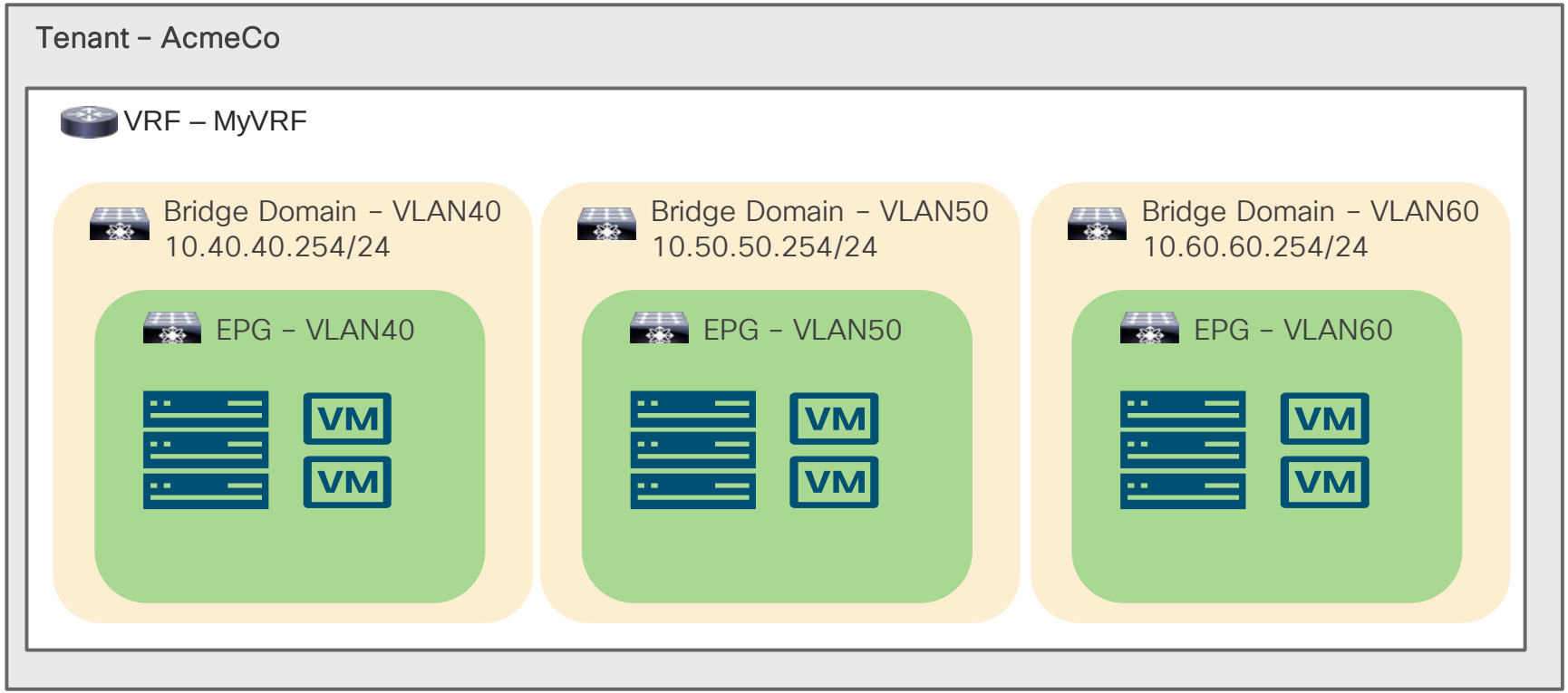
L2 External EPG ≈ 802.1q Trunk

L3 External EPG ≈ L3 Routed Link

Three approaches to using EPGs in ACI

EPG/BD = VLAN	EPG = App Tier	Hybrid (Combination)
Create a BD and one EPG for each existing VLAN. Common strategy to lift-and-shift traditional configurations. Simpler for migration, complex for Micro Segmentation.	Create one EPG for each application Tier. Flat-network design, many apps can share a single BD. Fantastic for GreenField and automated deployments.	New Apps and Legacy Apps share the same Fabric. Tenant and VRF sharing. or Dedicated Tenant/VRF and leaking.

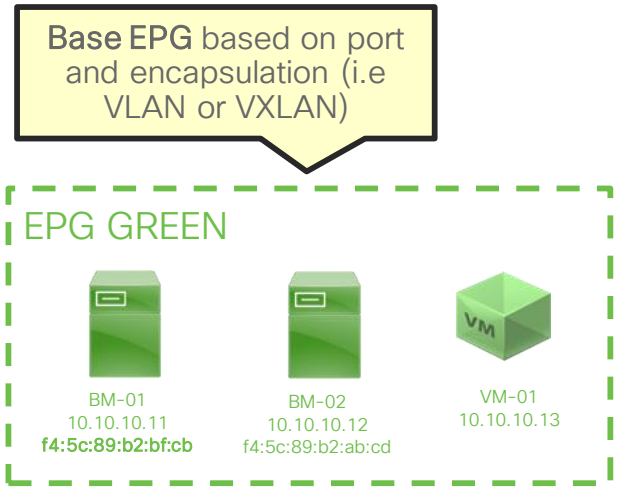
A common network-centric example with BD/EPG = VLAN



Micro EPGs allow the fabric administrator to **group** endpoints **based on** their **attributes**.

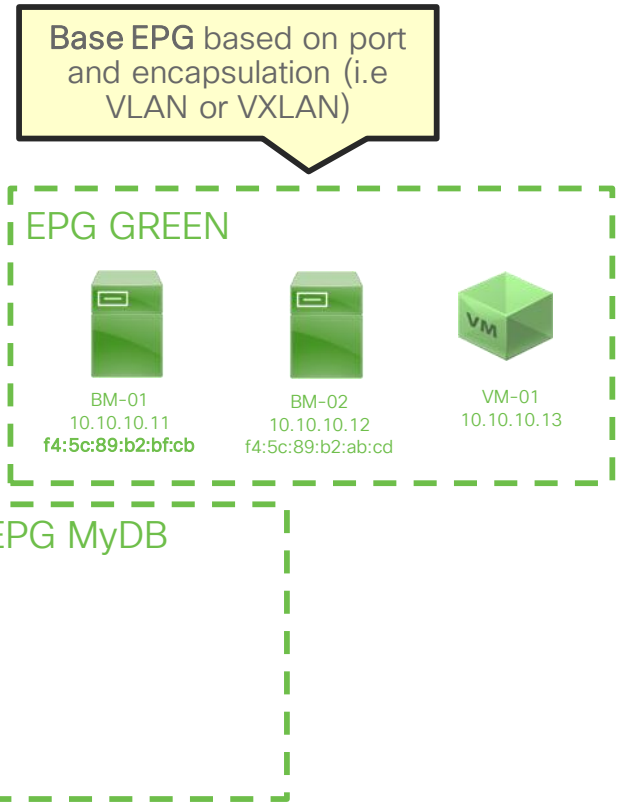
Understanding Micro EPGs

- 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**”



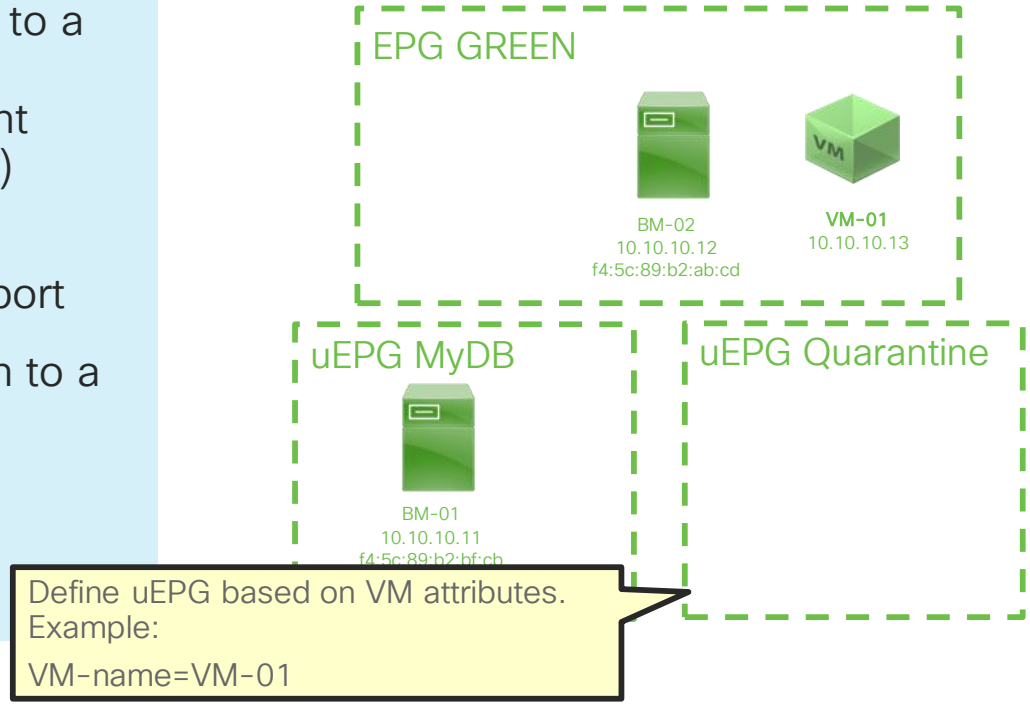
Understanding Micro EPGs

- 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**”



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**”



The actual classification possibilities depend on the **type of endpoint Domain**.

For endpoints connected to **Physical Domains** (bare metal) you can classify based on **IP or MAC** addresses.

Example: PhysDom (Bare Metal) with IP Address uEPG

IP Micro EPGs considerations on PhysDoms

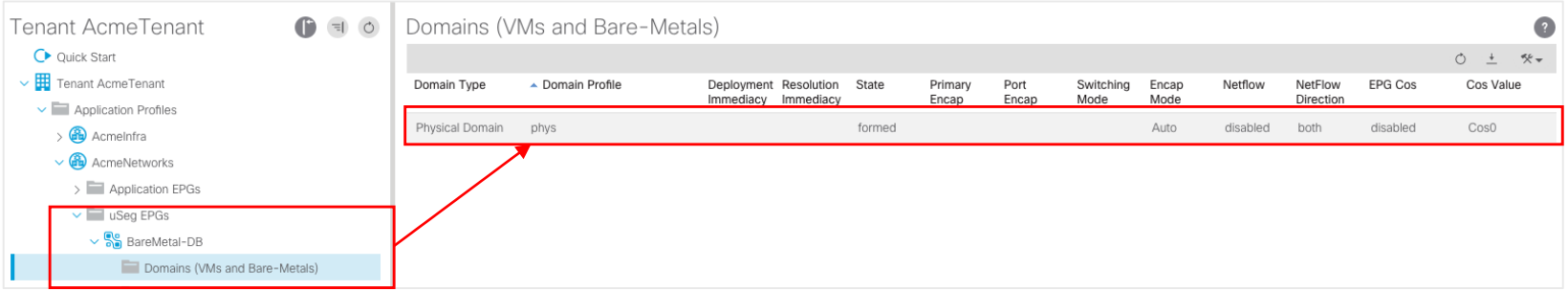
- **Base EPG must be configured** and deployed to program VLANs on leaf host ports
- Base EPG & IP uEPG must associate with **same BD and the BD MUST have an IP subnet configured**.
- IP uEPG must be deployed an all the nodes where the BD is deployed by using node attachment
- Deployment Immediacy must be “Immediate”
- You can specify individual **IP addresses and/or subnets** (i.e. 10.10.10.1, 10.10.10.0/24)

Software Dependency: 1.2(x)
Hardware Dependency: E-Series or newer
Caveat: bridged traffic will NOT be enforced based on the IP-EPG classification

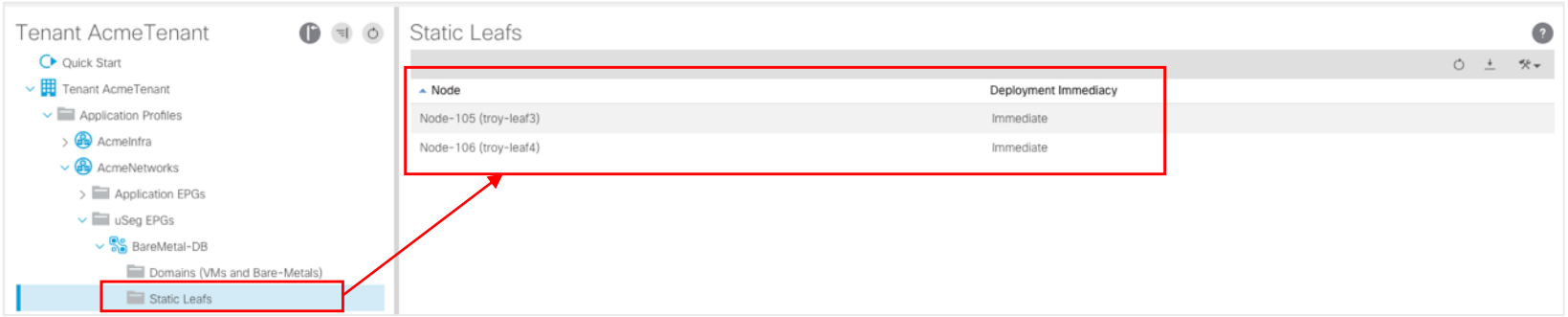
PhysDom (Bare Metal) with IP Address uEPG – Configuration [1/2]

For Your Reference

1. Define uEPG and map to the same PhysDom and BD as Base EPG



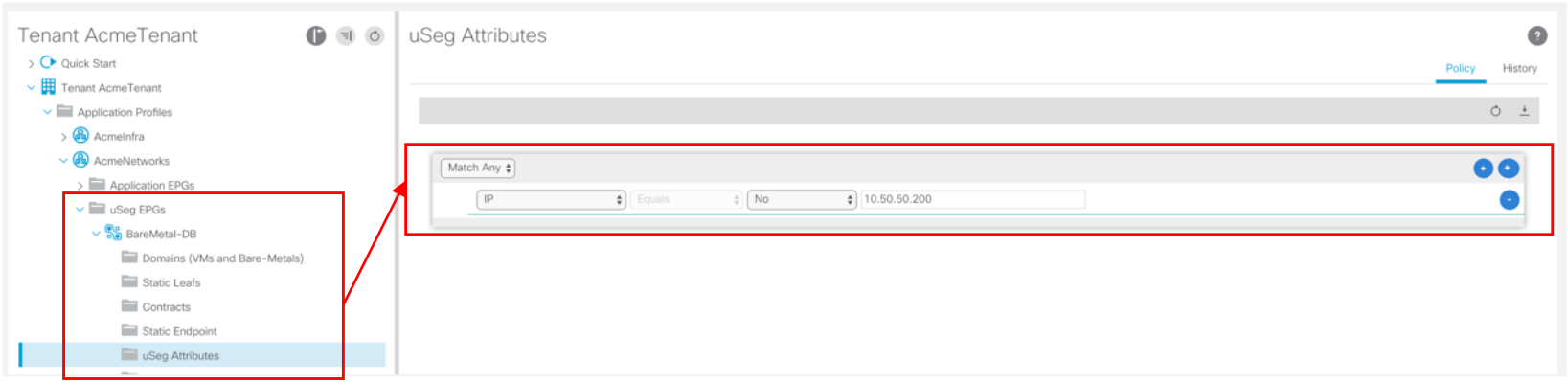
2. Map the uEPG to the required leaf switches



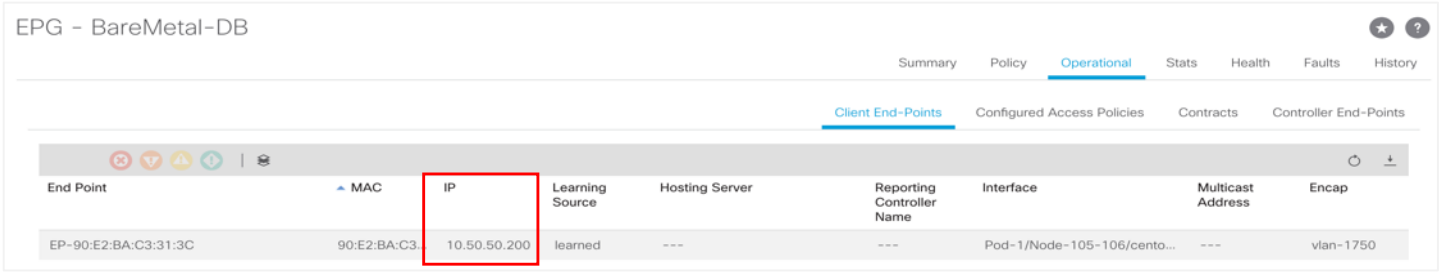
PhysDom (Bare Metal) with IP Address uEPG – Configuration [2/2]

For Your Reference

3. Define the IP address and/or list of IP addresses to match on

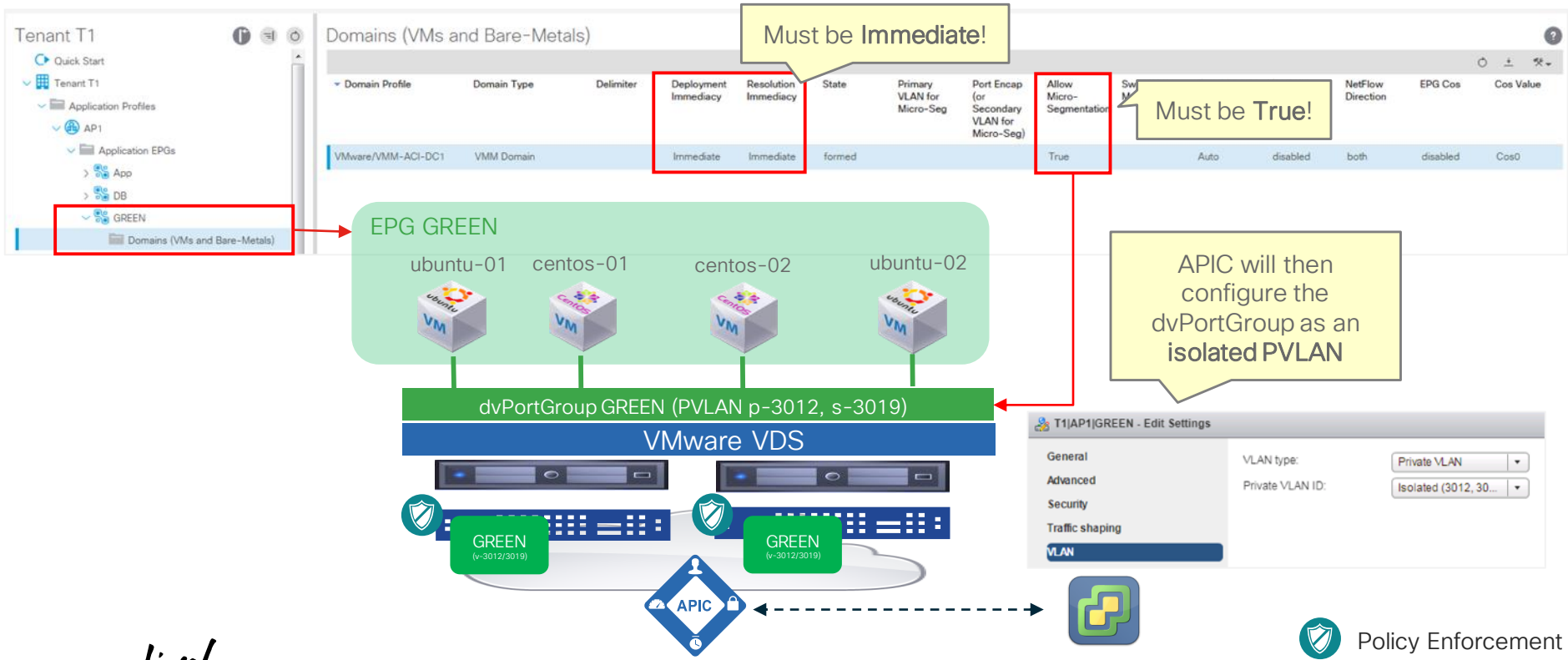


4. Review the result



For endpoints connected to
VMware and Microsoft VMM Domains you can use the **IP, MAC or VM-attributes.**

Micro EPG Support with vSphere VDS
1. Start with Base EPG, enable MicroSeg



Policy Enforcement

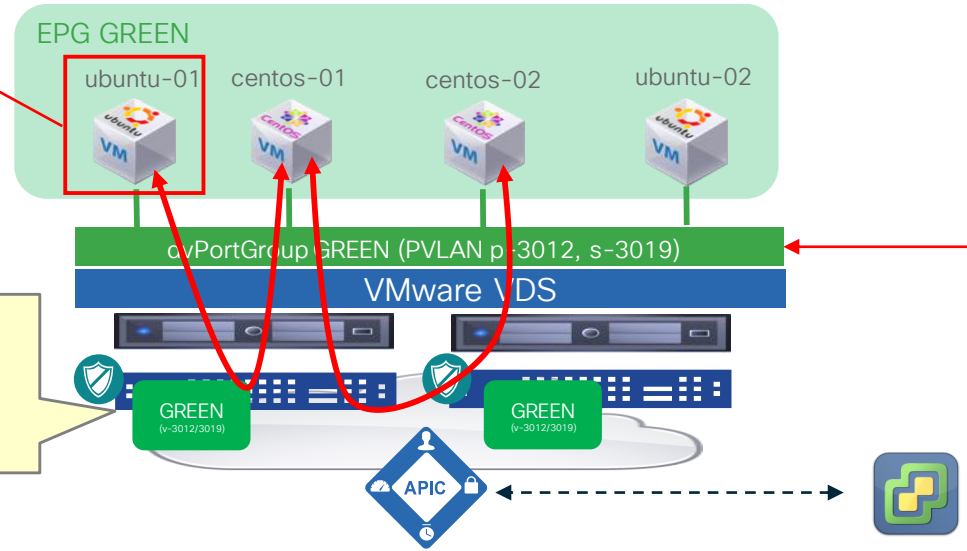
Micro EPG Support with vSphere VDS 1.1 Base EPG is working as normal EPG

EPG - GREEN

Policy | Operational | Stats | Health | Faults | History

Client End-Points | Configured Access Policies | Contracts | Controller End-Points

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
ubuntu-01	00:50:56:AD:15:2E	0.0.0.0	vmm	esx10.nillo.net	vcenter6-app-07.nillo.net	Pod-1/Node-101-102/ESX05-vPC-1-41 (v... Pod-1/Node-101-102/ESX10-vPC-1-44 (v...	---	vlan-3012(P) vlan-3019(S)

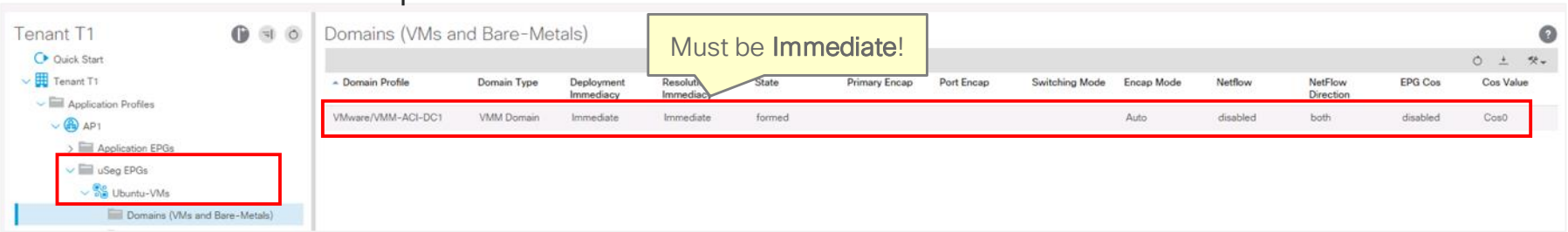


Communication between endpoints inside the EPG is allowed at the Leaf. **Proxy-ARP** enabled.

Policy Enforcement

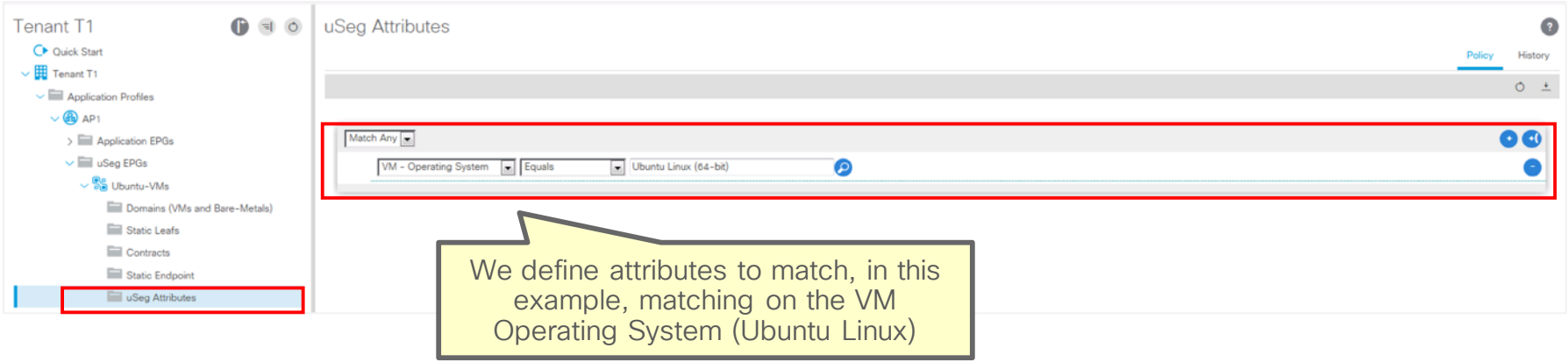
Micro EPG Support with vSphere VDS
2. Configure uEPG based on attributes

1. Define uEPG and map to the same VMM Domain and BD as Base EPG

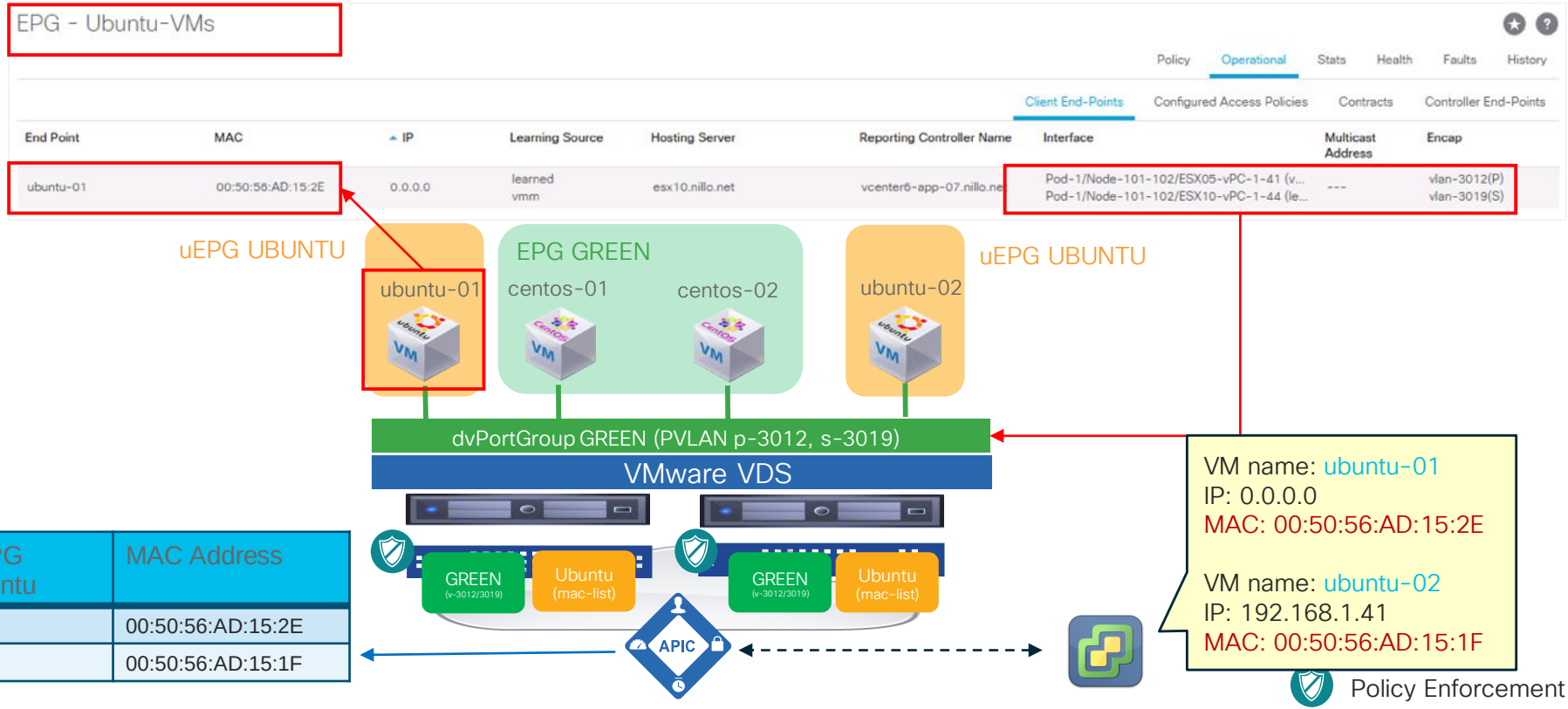


Micro EPG Support with vSphere VDS
2. Configure uEPG based on attributes

2. Configure the required attributes



Micro EPG Support with vSphere VDS
3. VM is classified according to attributes



uEPG Ubuntu	MAC Address
vm-1	00:50:56:AD:15:2E
vm-2	00:50:56:AD:15:1F

A quick demo of using VM attributes for uSEG

Micro EPG Support with vSphere VDS – Summary

For Your Reference

Micro EPG Considerations on vSphere VDS

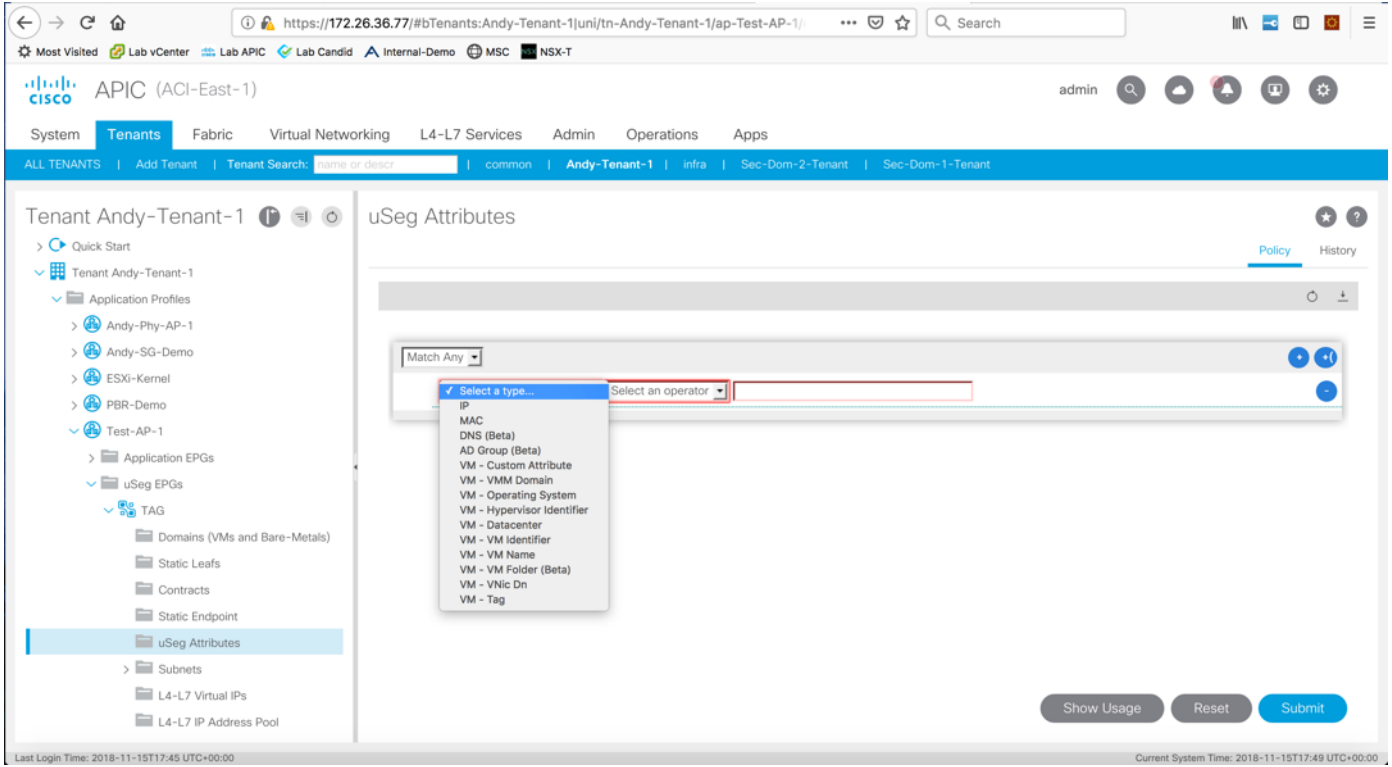
- Under base EPG you must enable micro segmentation for vDS. This is only required if using uSeg with VDS.
  - When EPG is mapped to VMM domain, it will change vDS and port-group configuration: PVLAN will be enabled.
  - Port-group uses secondary VLAN (isolated), which is same with intra-EPG isolation.
  - Proxy-ARP is automatically enabled on base EPG (this is only supported in EX-models)
  - PVLAN configuration is only to force all traffic to flow through Leaf.

- Some considerations when using uEPG with VDS:
  - Proxy-ARP is required
  - SPAN/ERSPAN work at the leaf level, but operate on the Base EPG
  - Traffic stats are kept for the Base EPG, not per uEPG

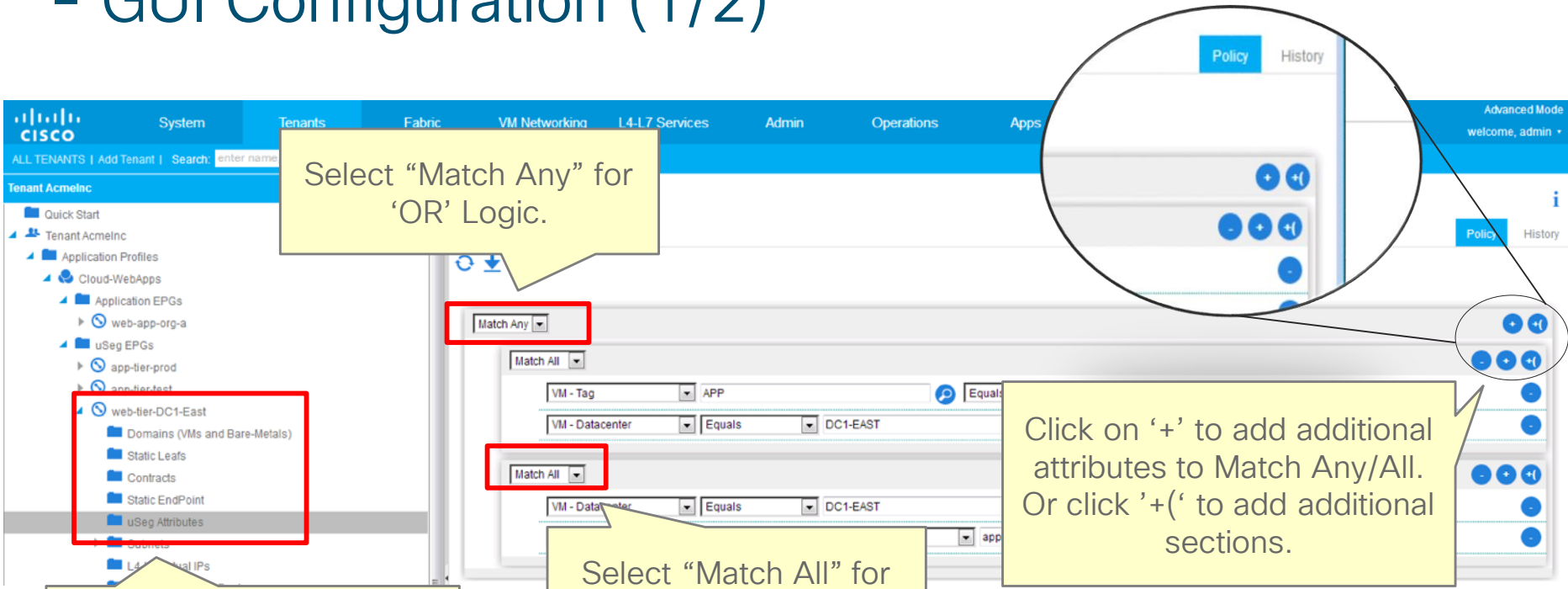
- Software Dependency: 1.3(1g)
- Hardware Dependency: EX-Series or newer

When using VMM Domains, you can configure **multiple attributes** to select endpoints for a Micro EPG using **Logical Operators** (since APIC release 2.3)

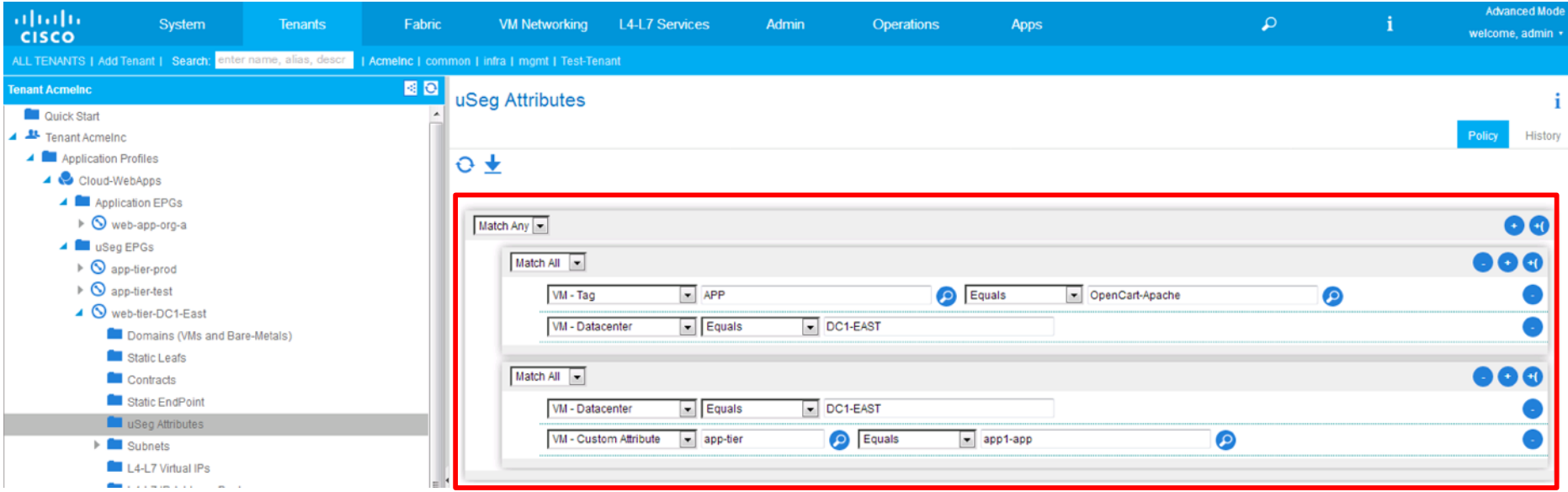
ACI Doing Segmentation With Attributes



uEPGs with Attributes and Logical Operators – GUI Configuration (1/2)



uEPGs with Attributes and Logical Operators – GUI Configuration (2/2)



Selects VMs with Tag 'APP:OpenCart-Apache', or VMs with 'Custom Attribute app-tier=app1-app' as long as they are running on vCenter DC1-EAST datacenter


What about Containers?

With **Kubernetes Domains** classification does not use micro EPG.

We use regular EPGs selected using native semantics (Kubernetes annotations).

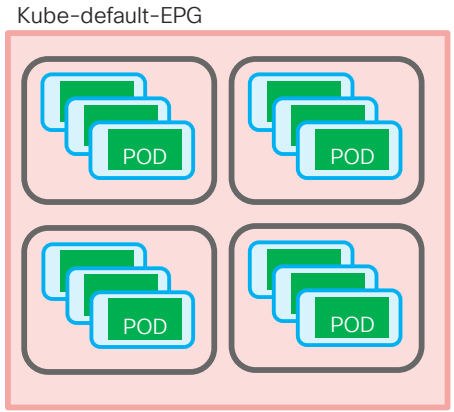
Using annotations to specify the EPG for a set of Kubernetes PODs

- Provide isolation beyond using Kubernetes Network Policies
- Opflex annotation can be applied at POD, Deployment or namespace level
- Priority of annotations goes from less specific to more specific
  1. Pod annotation
  2. Deployment annotation
  3. Namespace annotation
  4. Namespace group mapping from controller config file
  5. Global default group from controller config file

ACI allows flexible POD to EPG mapping

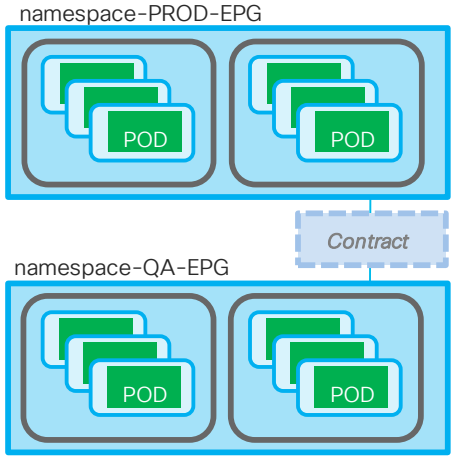
K8s Network Policy

Cluster Isolation



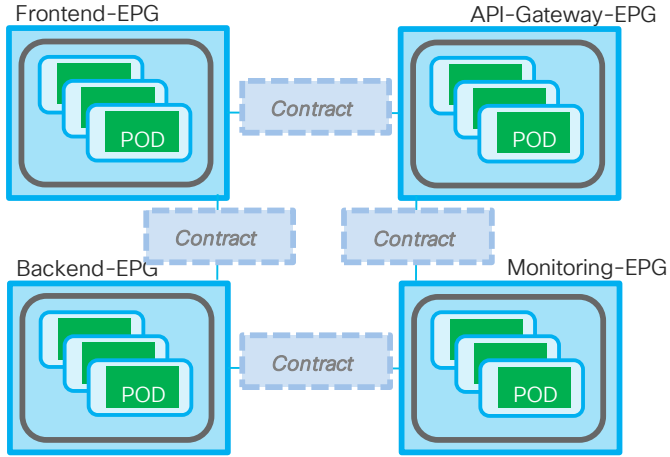
- Default behavior: single EPG for entire cluster user PODs
- No need for internal contracts

Namespace Isolation



- Each namespace mapped to an EPG
- Contracts for inter-namespace traffic are required

Deployment Isolation

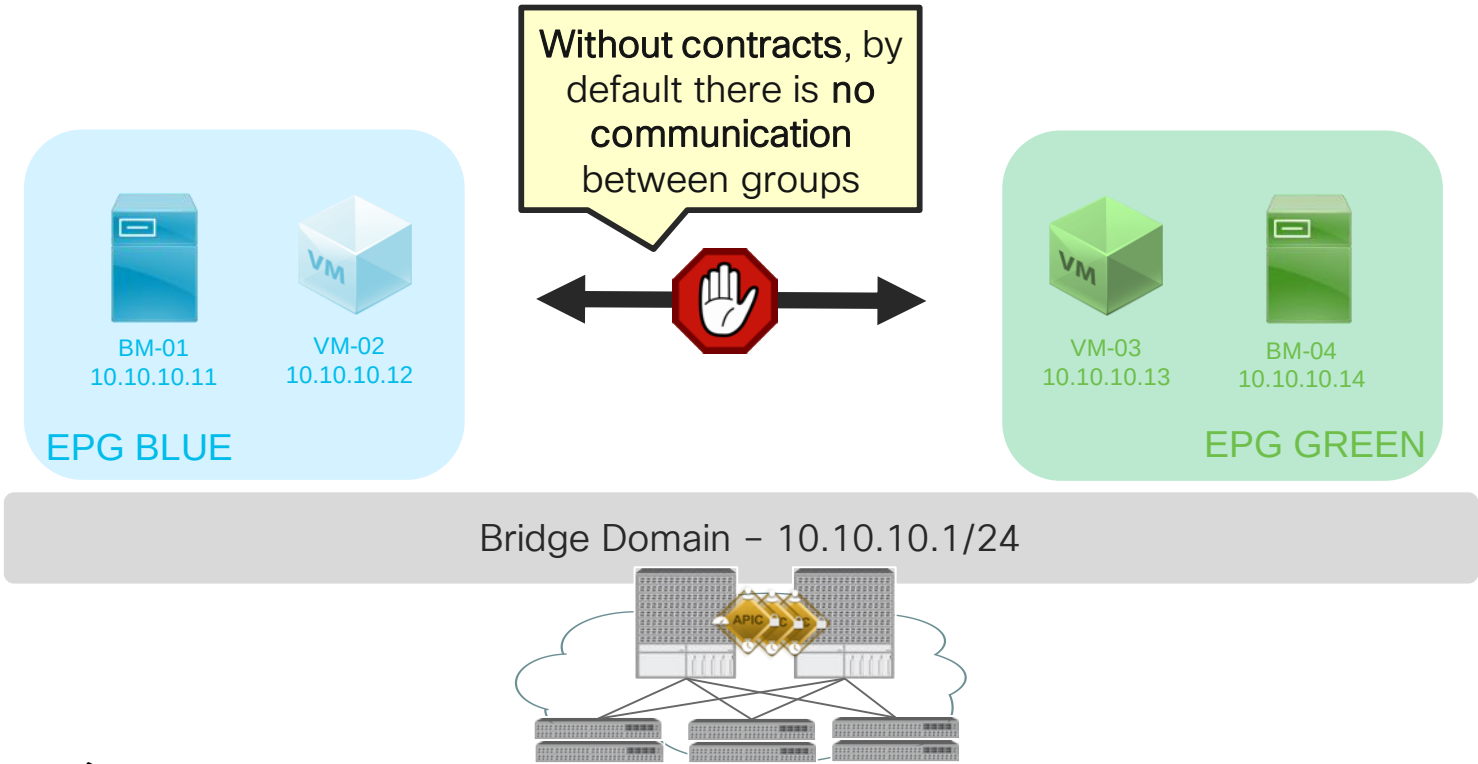


- Each deployment mapped to an EPG
- Contracts control traffic between microservice tiers

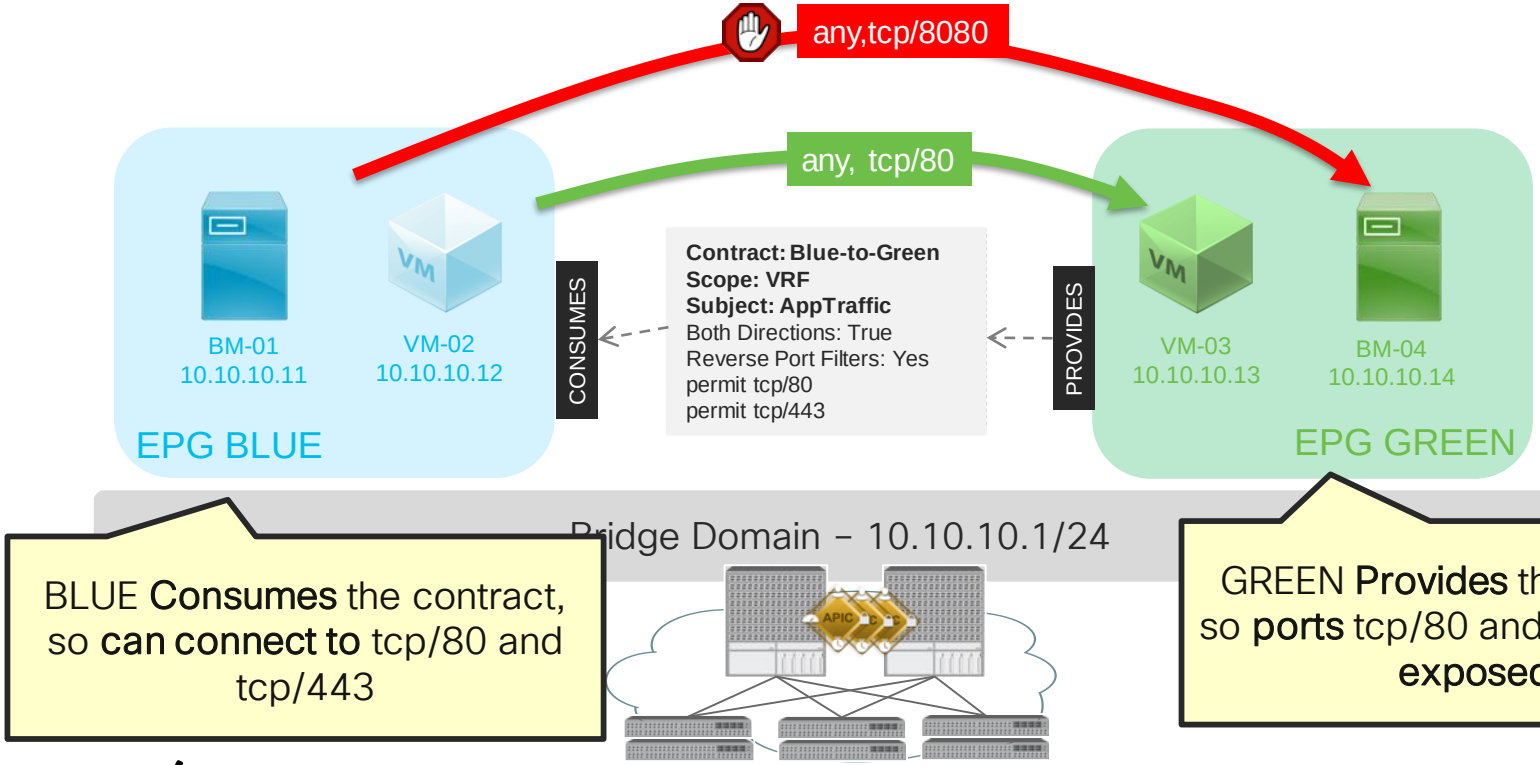
Agenda

- Micro Segmentation Fundamentals
- Endpoint Identity using EPG and micro EPG (uEPG)
- ACI Contracts for Policy Definition
- Improvements in hardware utilization
- ACI and Hybrid Cloud Security

By default communication between EPGs is not allowed in absence of contracts

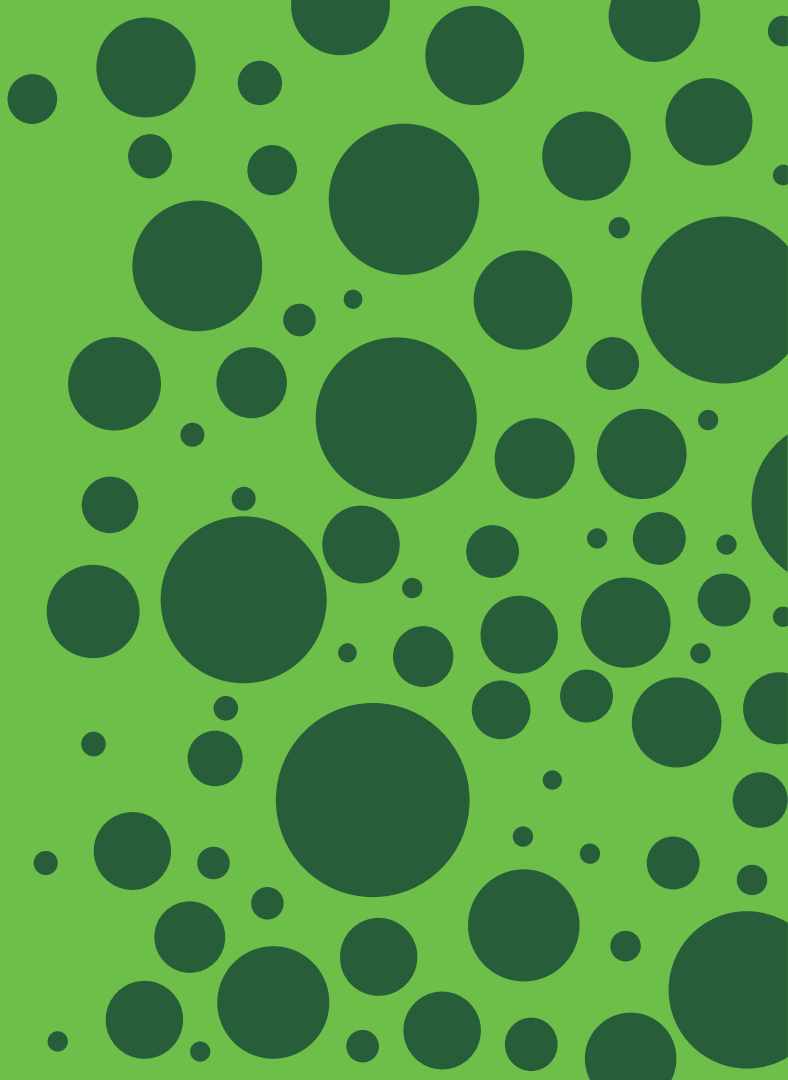


By default communication between EPGs is not allowed in absence of contracts

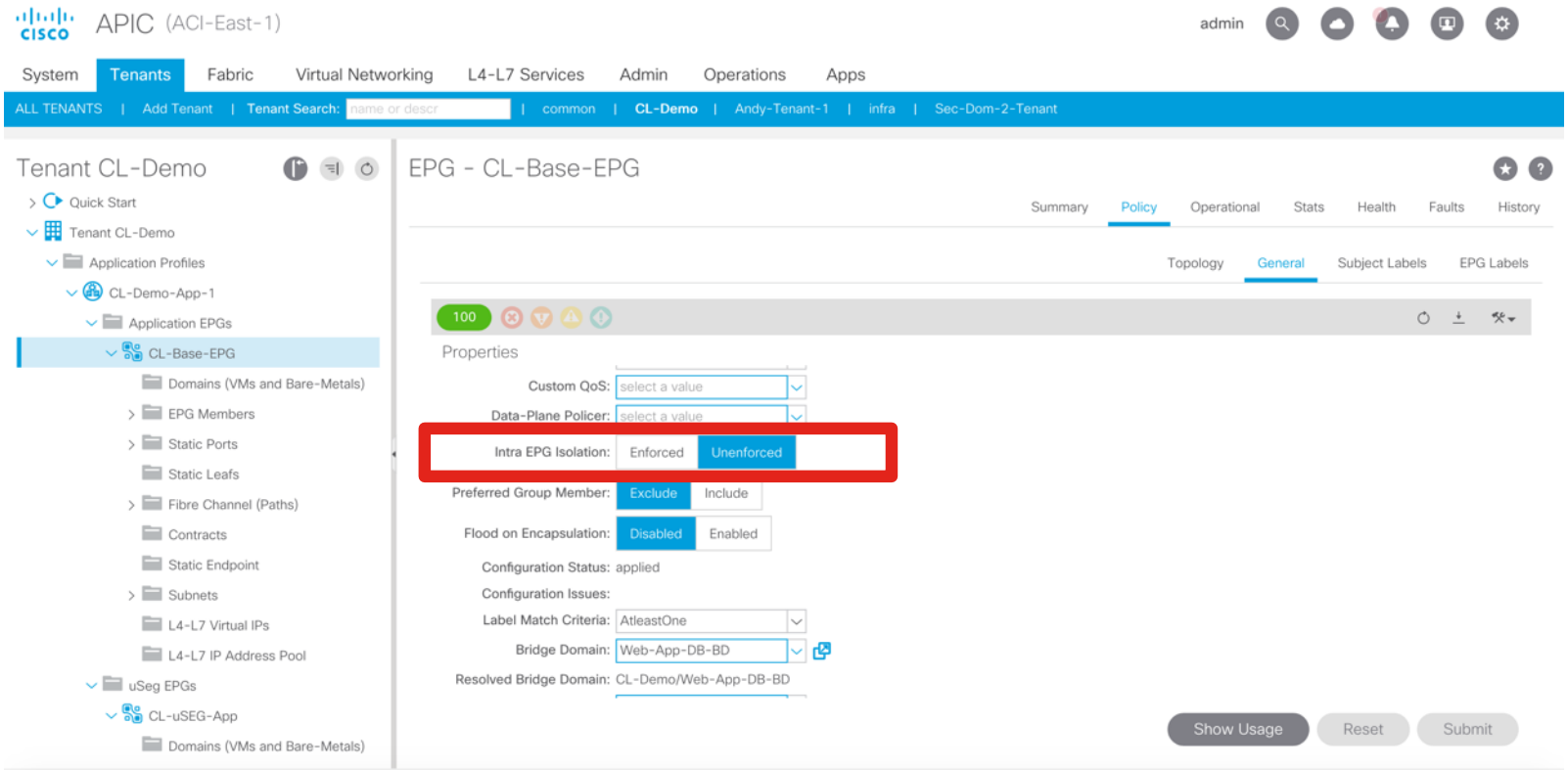


Demo: Creating a filter and contract

What about applying policy within an EPG.



Denying all traffic between EPs in the same EPG is easy

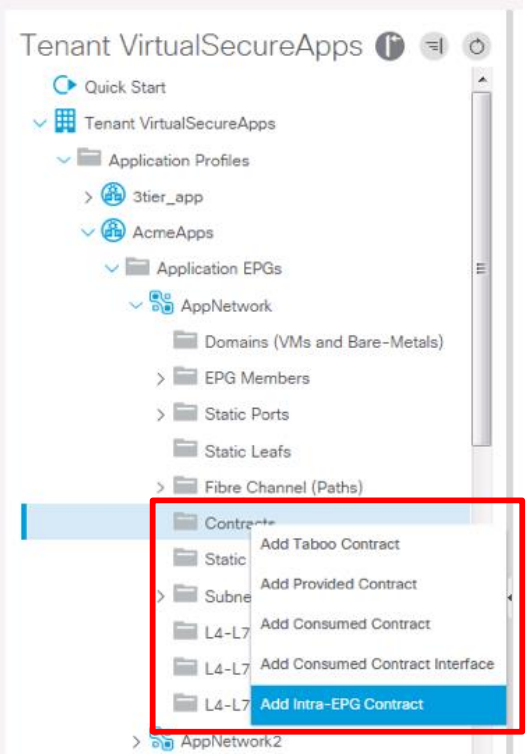


You can restrict all traffic inside a group using Intra EPG isolation

- Supported on PhysDoms, VMware VMM domain using VDS (it also works with AVS, AVE) (*)
- Since ACI 3.0 Microsoft VMM domain also supports intra EPG isolation.
- Can be configured on EPG and uEPG (**)
- It's supported with EX and FX, and later, leaf models.
  - We use Proxy-ARP – required to reach other EPG in the same subnet
  - We utilize PVLAN integration already present for VDS intra EPG isolation.

Contracts can also apply for Intra-EPG communications (since ACI 3.0)

- It is possible to assign contracts to restrict traffic internal to an EPG
- It can be enabled on both EPG and uEPG
- It supported with PhysDoms and VMware VMM Domains
- IntraEPG contracts require using proxy-arp. This means it is only supported on EX/FX switches or newer.



Intra EPG Security Feature Overview
How does it work for 2 VMs on the same ESXi Host?

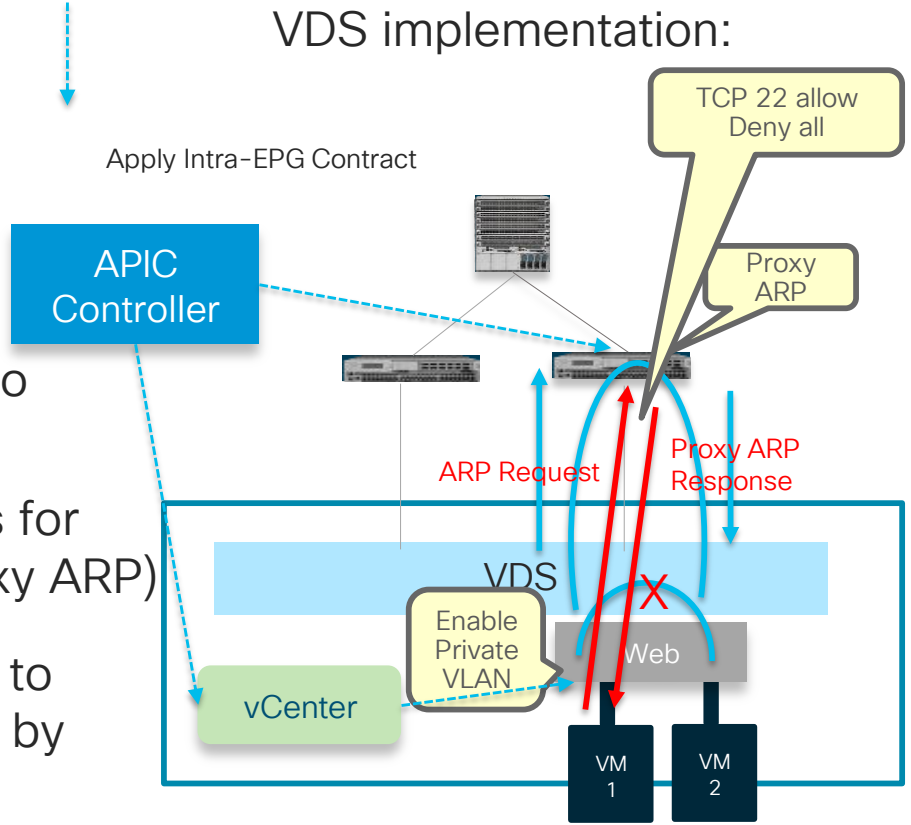
1- We enable Intra-EPG Security

2- APIC configures a PVLAN for the EPG/portgroup on vCenter with the TOR setup as the promiscuous port

3- The VMs in the portgroup can only talk to the TOR

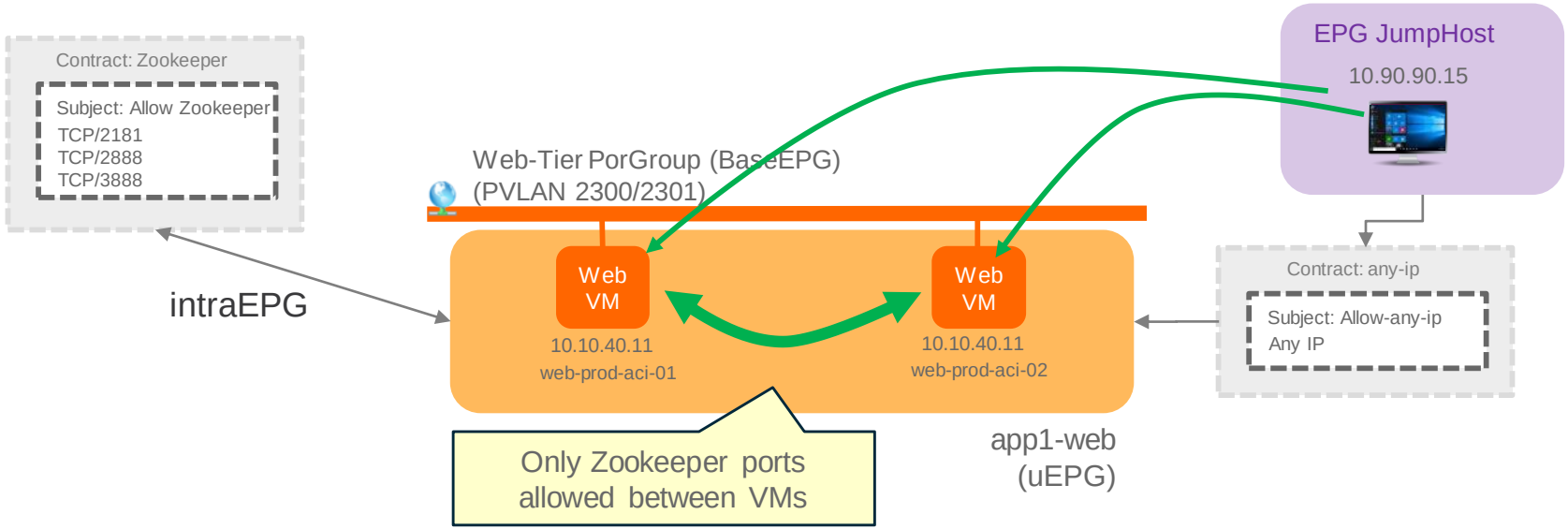
4- When VM1 wants to talk to VM2 it ARPs for it and the TOR responds with its MAC (proxy ARP)

5- All the traffic between the VMs is pulled to the TOR which allows only traffic permitted by the contract applied for Intra-EPG security



IntraEPG Contract Use Case – service vNIC used for mgmt in a clustered App

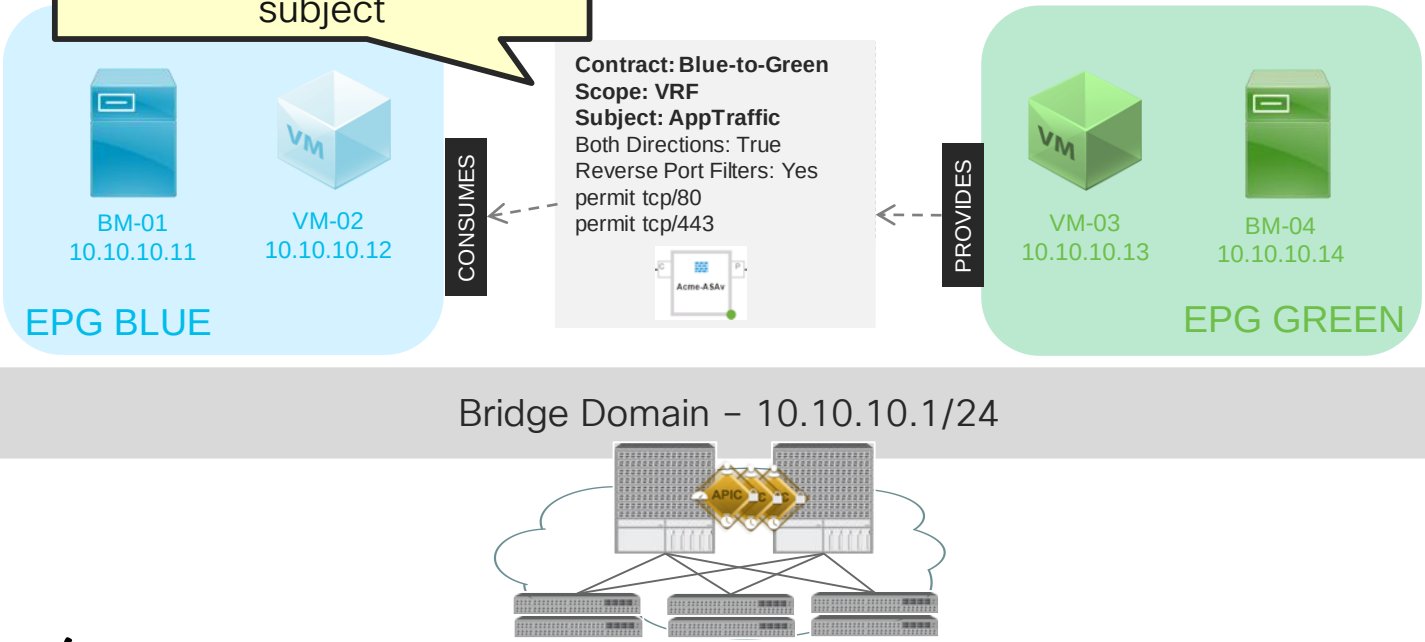
Example: a clustered web application. The jump host must be able to access all endpoints and you cannot use IntraEPG Isolation because the required protocols must be allowed between the VM inside the dvPortGroup.



Contracts also allow inserting services, like Next Generation Firewalls, ADC, IPS/IDS, etc.

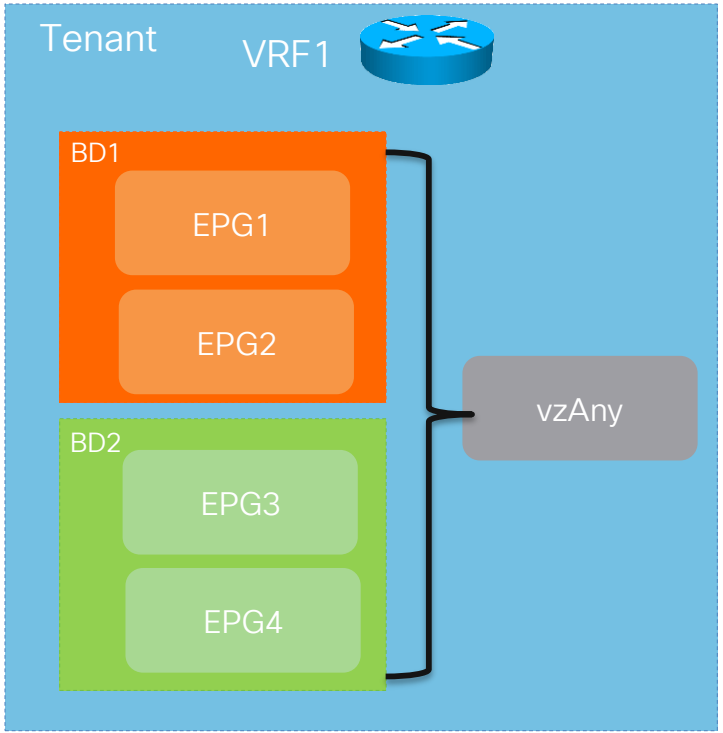
You can **insert** an NGFW, or a LB by attaching a **Service Graph** to the contract subject

Note: Service Graph between Micro EPGs requires 3.2 or higher



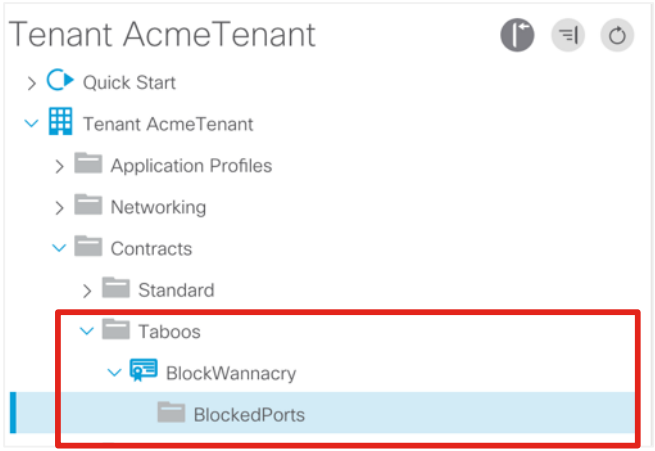
vzAny allows you to configure contracts that apply for all EPG in a VRF

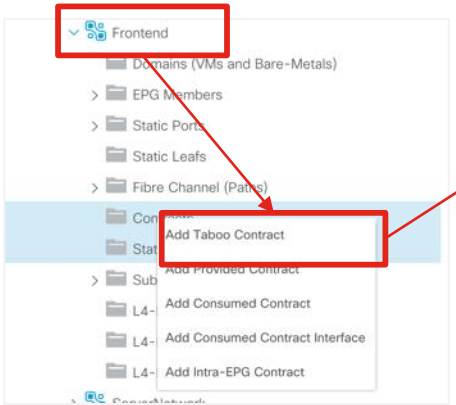
- vzAny represents the collection of EPGs that belong to the same VRF, including L3 external.
- Instead of associating contracts to each individual EPG you can configure a contract to the vzAny
- With cross-VRF contracts, vzAny can be a consumer, not provider
- Since ACI 3.2 it can also be used with Service Graphs

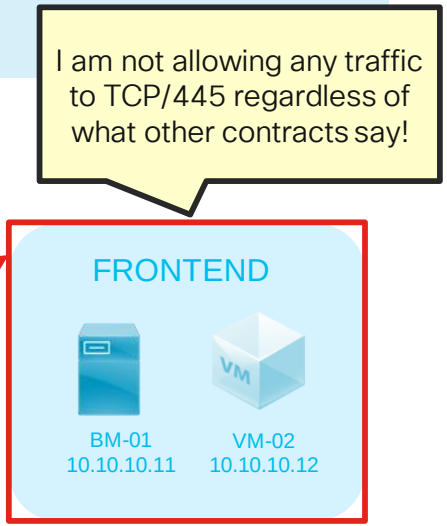


Taboo Contracts

- Taboo are special type of contracts that will be applied to individual EPGs
- They deny a set of ports on the EPG to which the taboo contract is applied
- For instance you can say EPG Frontend does not allow tcp/445
- Taboo filters will override regular contract filters







Blacklist (Deny) Contracts – Introduced with ACI 3.2

- Representing policy with a whitelist model is complicated: it requires complete understanding of application communication logic (every protocol and port required).
- Since ACI 3.2 we are introducing the possibility of implementing blacklist contracts.
- Blacklist contracts can apply to consumer/provider as well as intraEPG configurations
- For instance, now you can:
  - configure a contract that allows everything
  - then deny specific ports and protocols.

Blacklist Contracts implement Deny Filter Rules

- Since 3.2, the subject filter attachment has one additional attribute action
  - Action = **permit**, default to keep existing behavior
  - Action = **deny**, causes rules for these filters to switch to deny (drop)
- Now subject filters will have different priorities to determine precedence:
  - Default Values:
    - Level 1 – lowest priority corresponding to any-to-any filter rules
    - Level 2 – medium, corresponds to src-to-any/any-to-dst filter rules
    - Level 3 – highest, corresponding to src-to-dst filter rules

  Or to put it more simply…the most specific rule has highest priority
- Administrator is given a choice to override default priorities.

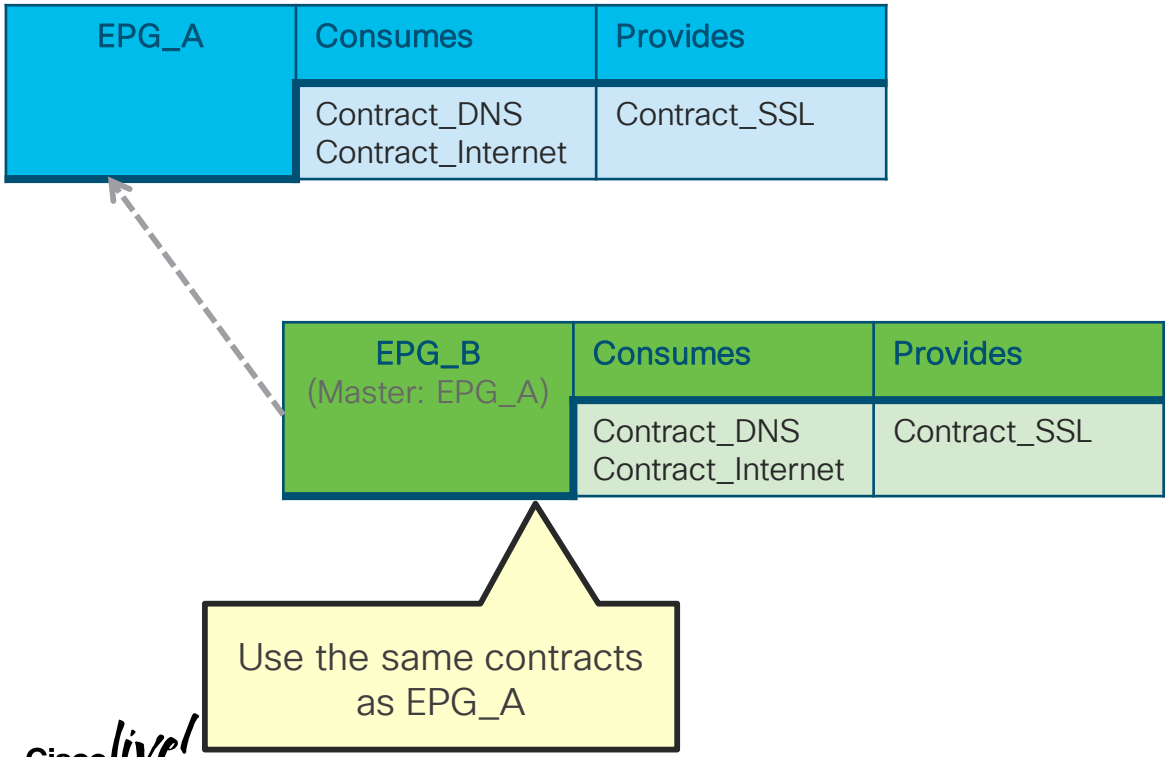
Simplifying Contract Configurations with EPG Contract Inheritance

- Objective: simplify policy configuration
- Contract Inheritance will help:
  - Establish a **relation between EPGs**, so that one **EPG can inherit the contract relations** of other EPGs
  - When new contract relations are added to the higher EPG, those with inheritance relation will automatically get those same contract associations
- Considerations:
  - does NOT apply to VzAny and also does NOT replace use of VzAny
  - does NOT reduce number of contracts or TCAM utilization
  - EPGs can only inherit contracts from EPGs under the same Tenant

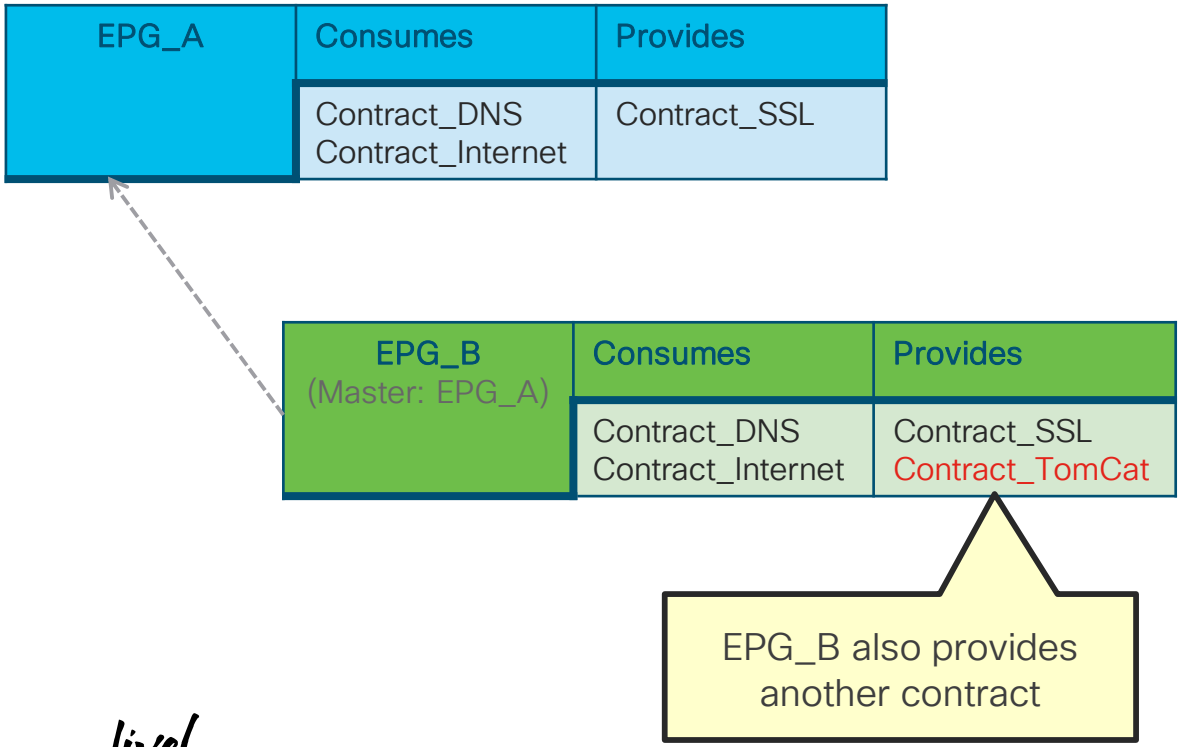
Example: EPG_A has three contract relations

EPG_A	Consumes	Provides
	Contract_DNS Contract_Internet	Contract_SSL

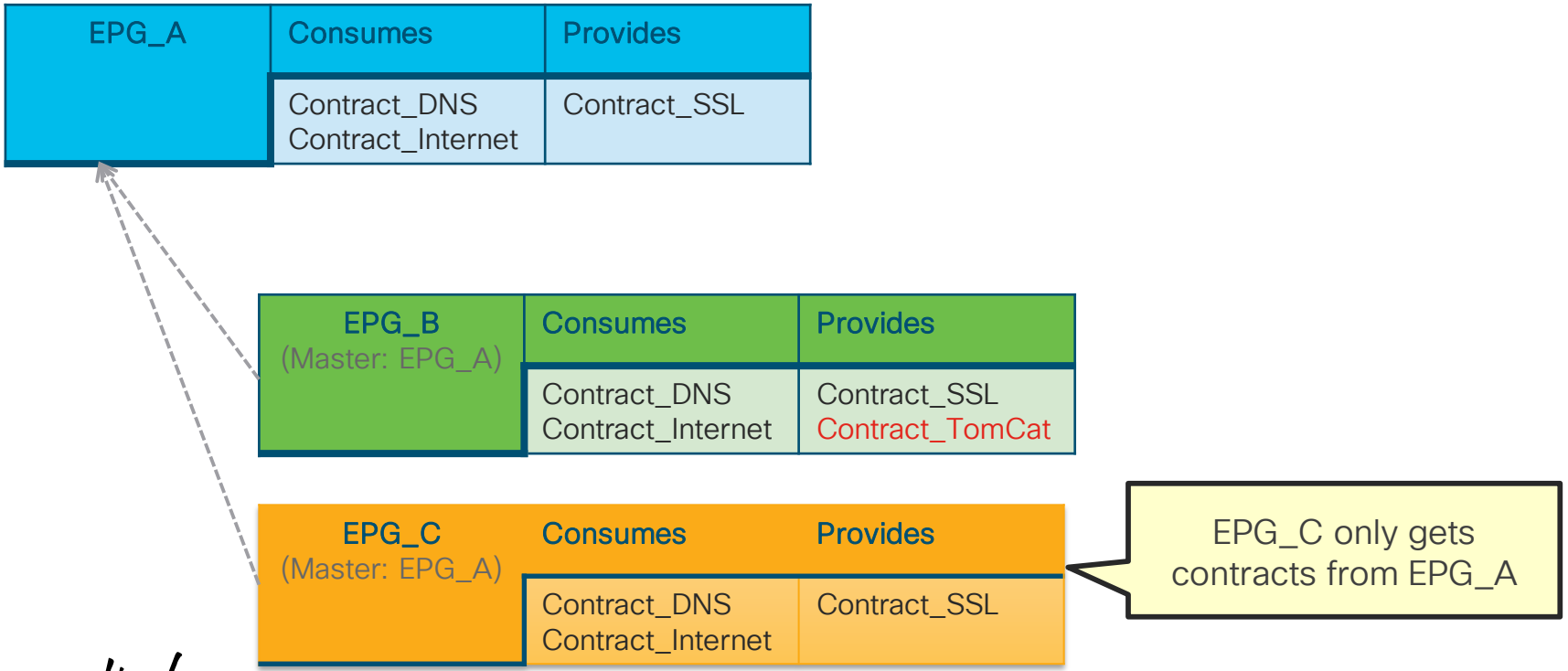
EPG_B is configured to inherit from EPG_A



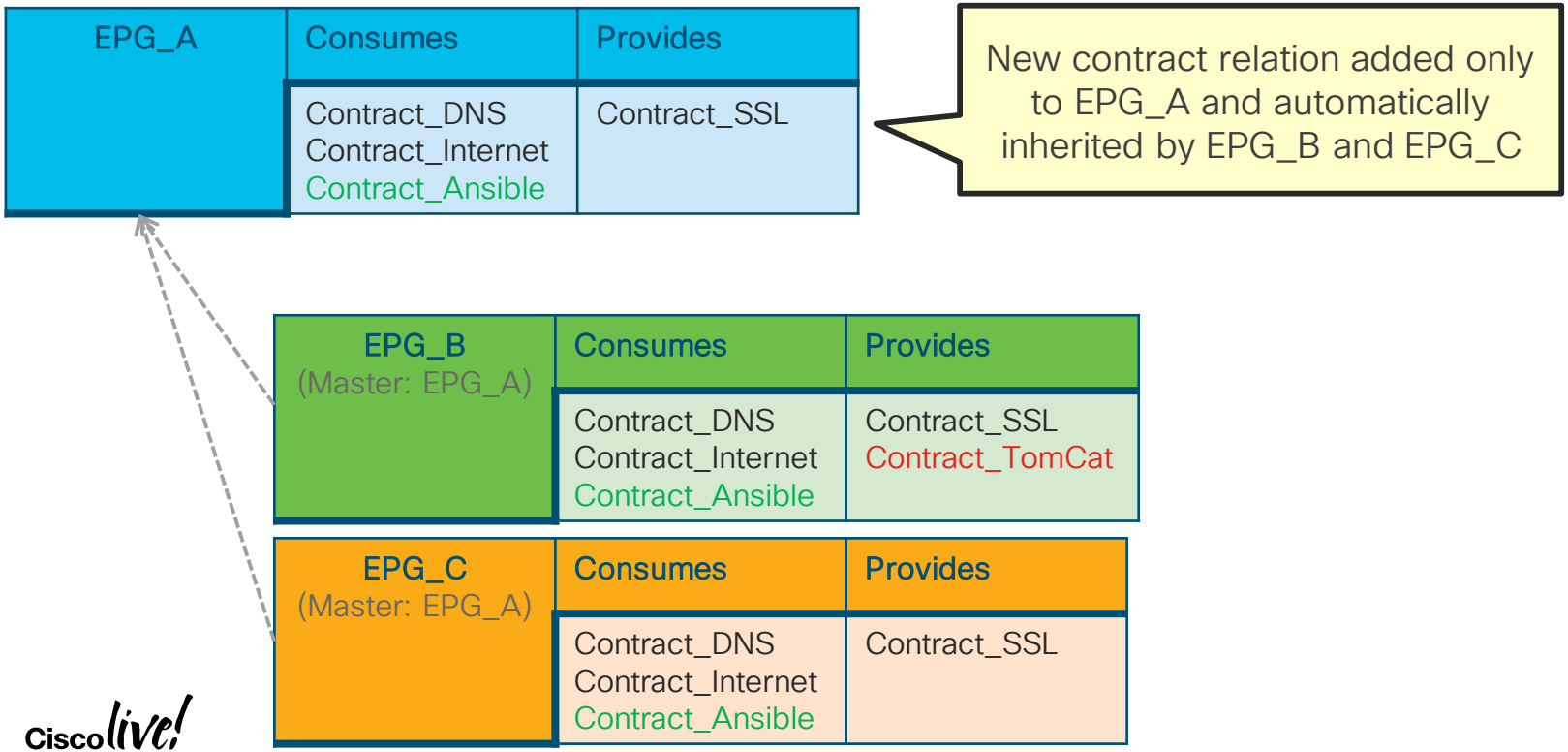
EPG_B is configured to inherit from EPG_A - can now add specific contracts to “child”



EPG_C is configured to inherit from EPG_A

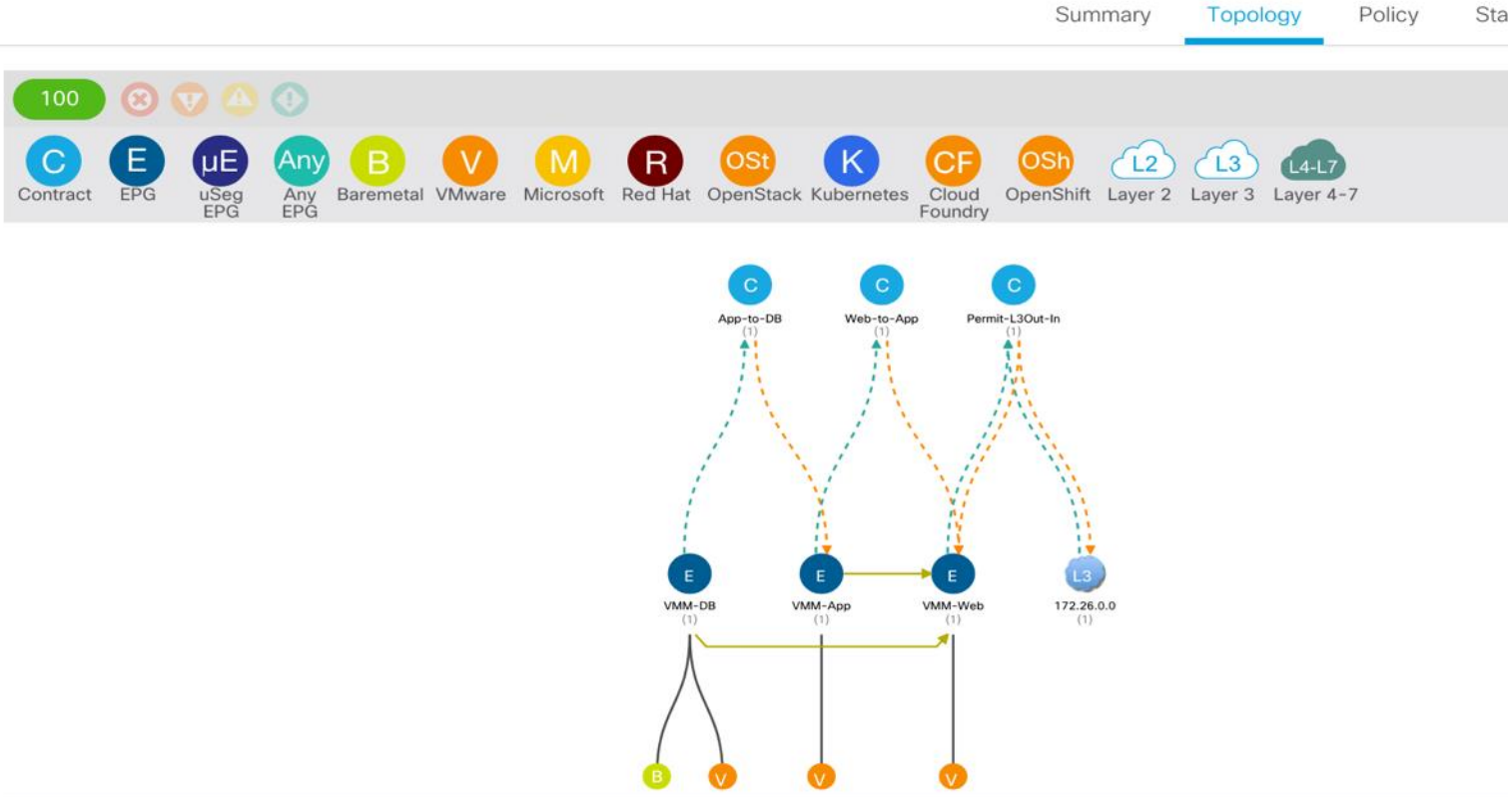


Changes to contract relations on EPG_A are inherited by EPG_B and EPG_C



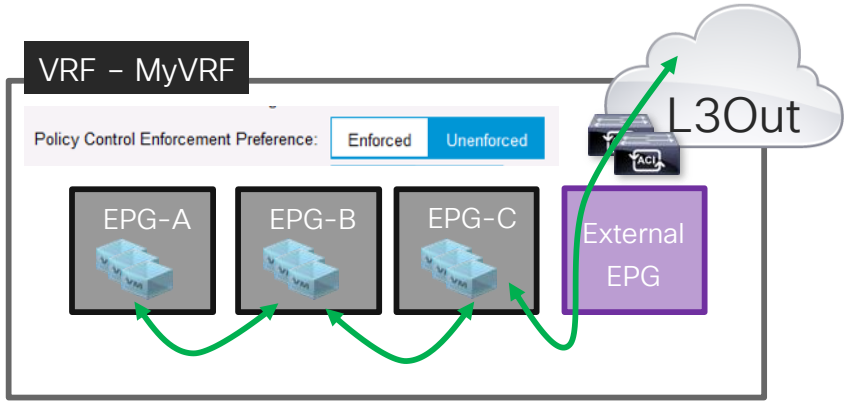
Adding Contract Inheritance

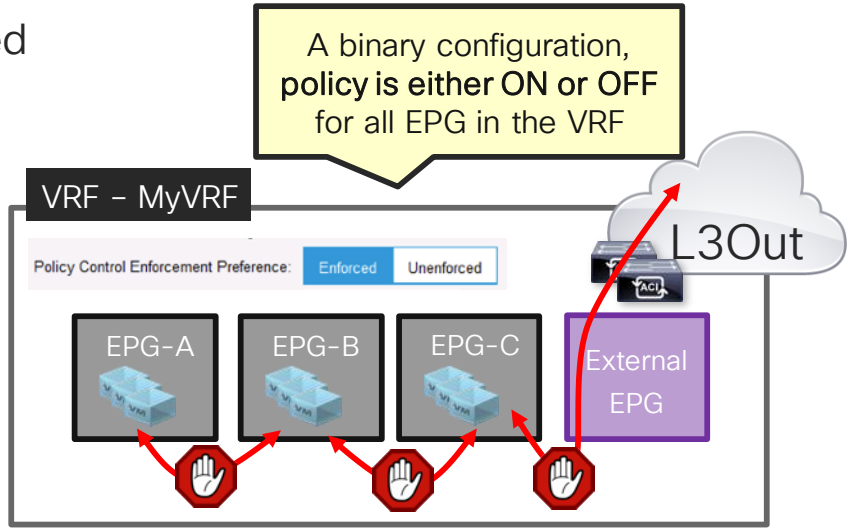
Application Profile - Test-AP-1



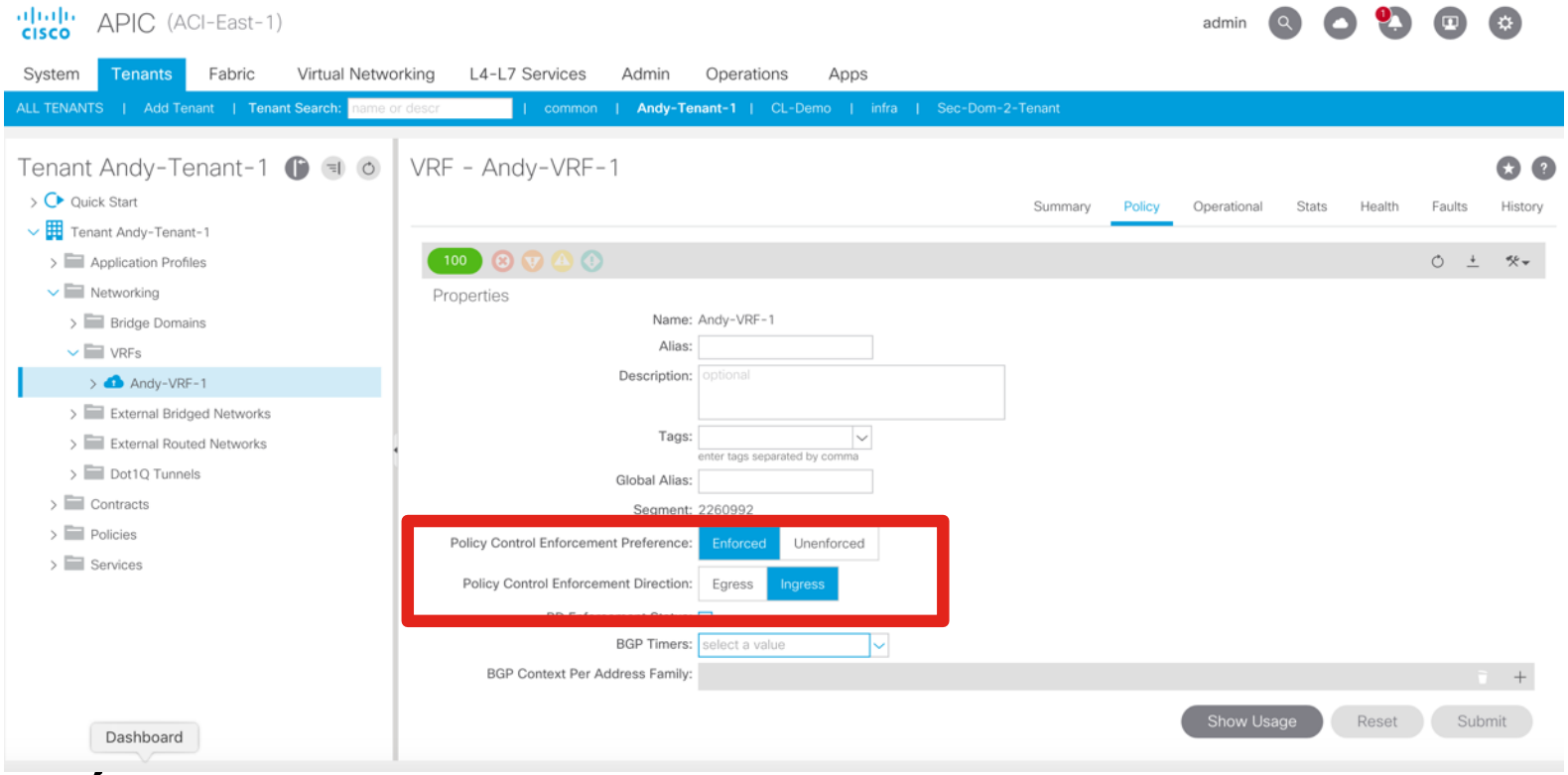
Contract Policy Enforcement can be enabled or disabled at VRF level

- Policy Enforce: no communication without contracts
- Policy Unenforced: all communication allowed

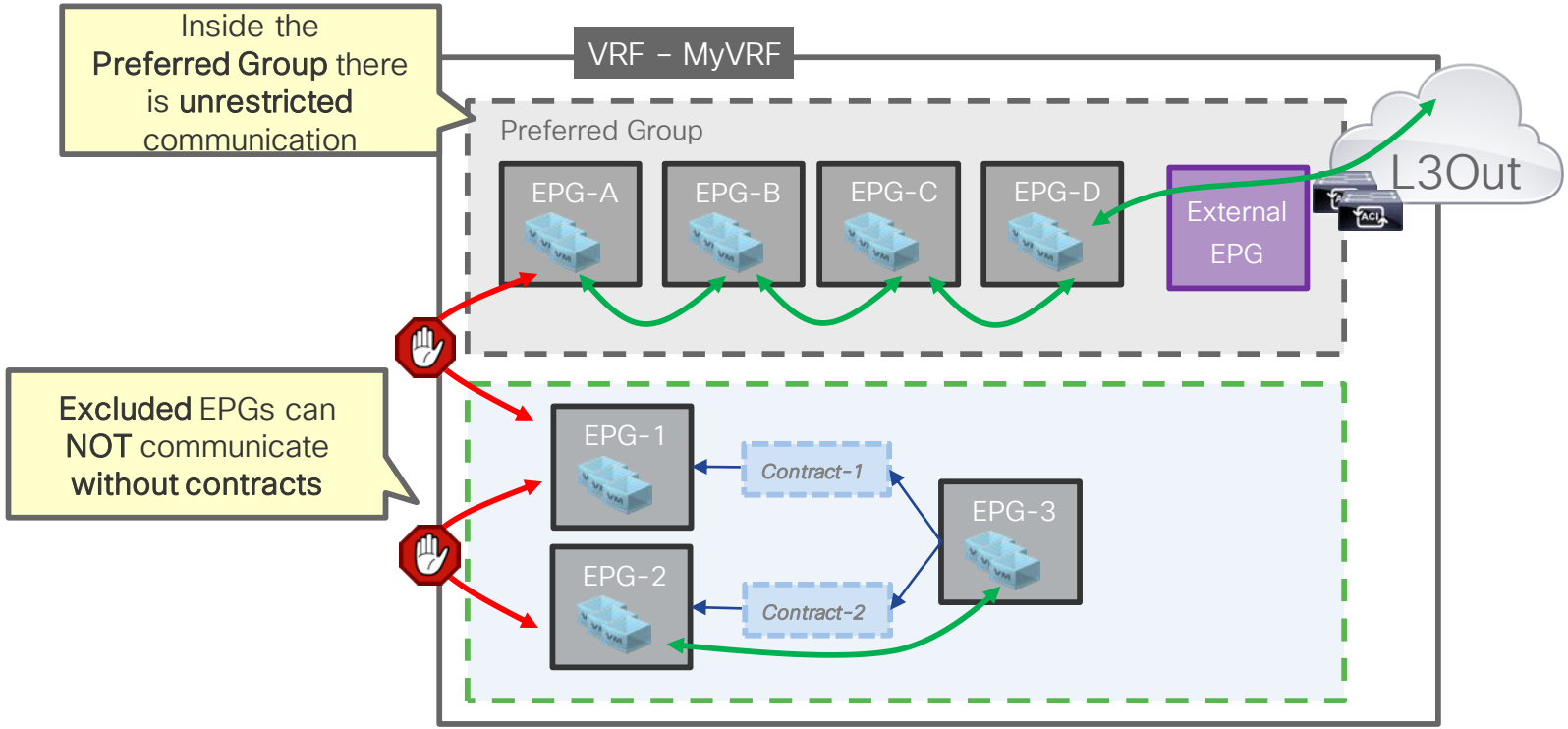




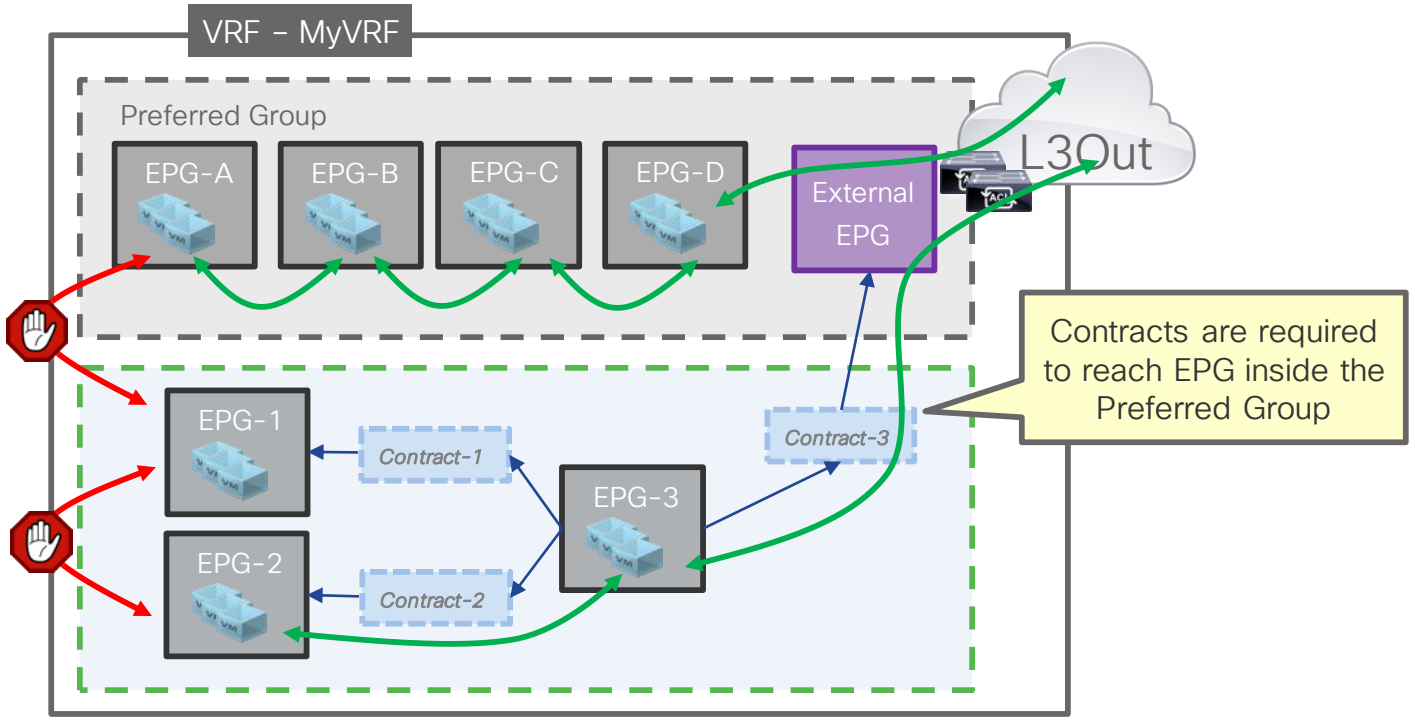
Enabling Enforcement at VRF Level



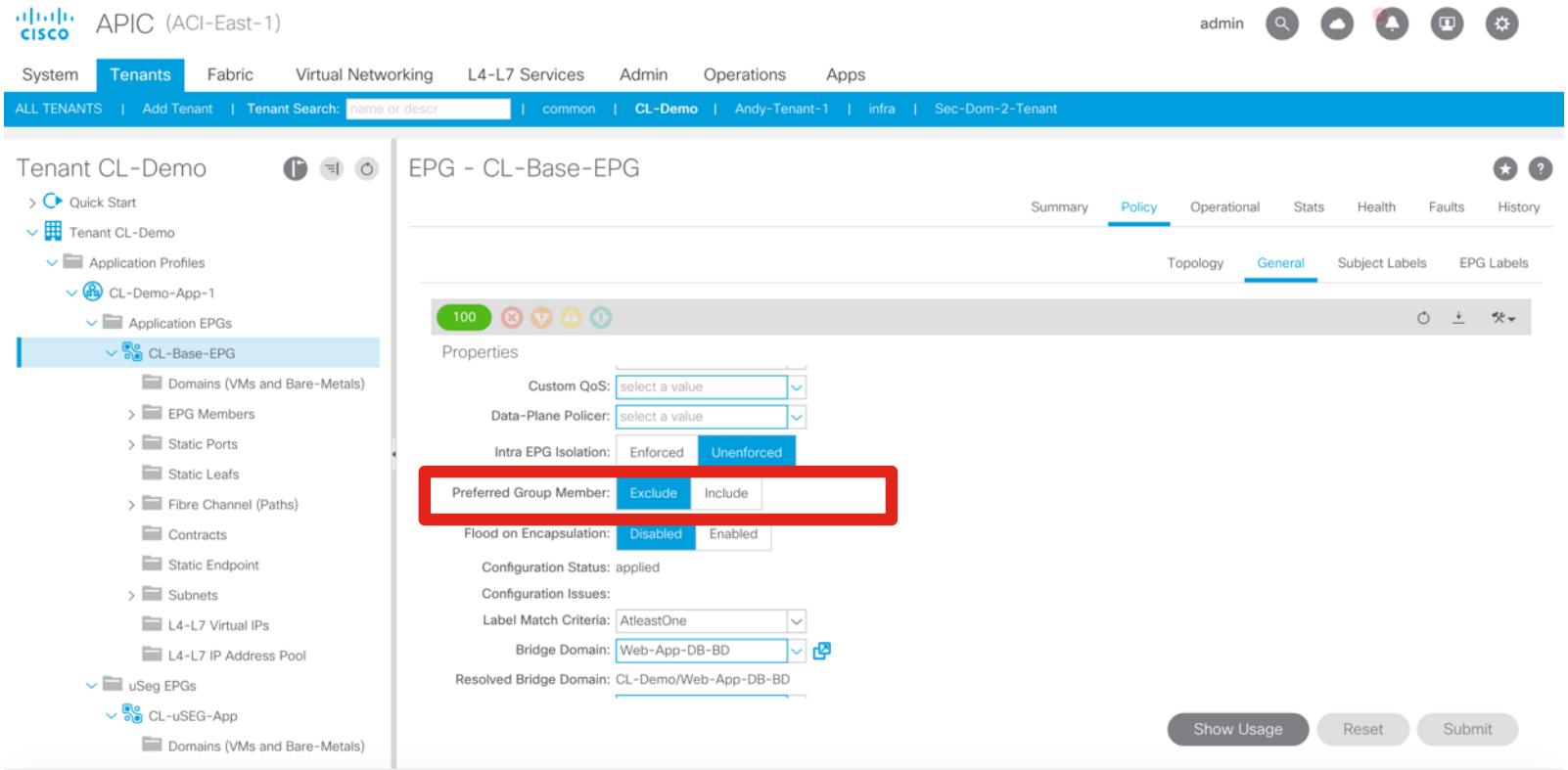
Contract Preferred Group Example



Contract Preferred Group Example



Enabling Preferred Groups Is Easy



Contract Logging – Denied Packets

For Your Reference

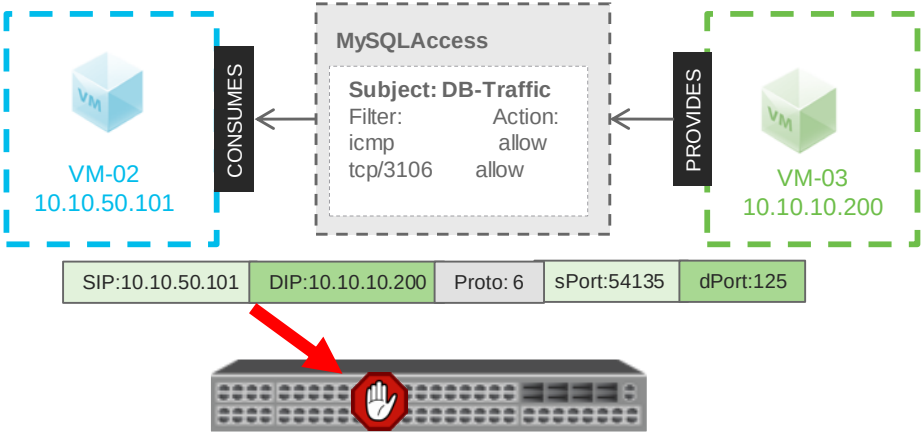
Logging Deny

- ACI can **log implicit deny hits**
  - For Bare Metal, VMware VDS and MSFT Domains logs generated by Leaf
  - For AVS logs may be generated on Leaf or vLeaf
  - For OpenStack ML2 mode, logs configured external to the fabric at the host
- Syslog is exported according to monitoring policies and configured External Data Collectors
- Logs **include Tenant/VRF, EPG VLAN encap, ingress interfaces** and offending packet details

- **Software Dependency: supported on all software releases**
- **Hardware Dependency: supported on all hardware models**

ACL deny not logged by default:

Fabric -> Fabric Policies -> Policies -> Monitoring -> Common Policy -> Syslog Message Policies -> Default -> Change 'default' to 'info'



Feb 04 10:26:54 troy-leaf1 %LOG_LOCAL7-6-SYSTEM_MSG [E4204936][transition][info][sys] %ACLLOG-5-ACLLOG_PKTLOG_DENY: CName: Test-Tenant:Test-Tenant-VRF(VXLAN: 2162689), VlanType: FD_VLAN, Vlan-Id: 21, SMac: 0x00505690b43a, DMac:0x0022bdf819ff, SIP: 10.10.50.101, DIP: 10.10.10.200, SPort: 54135, DPort: 125, Src Intf: port-channel2, Proto: 6, PktLen: 74

Contract Logging – Permitted Packets

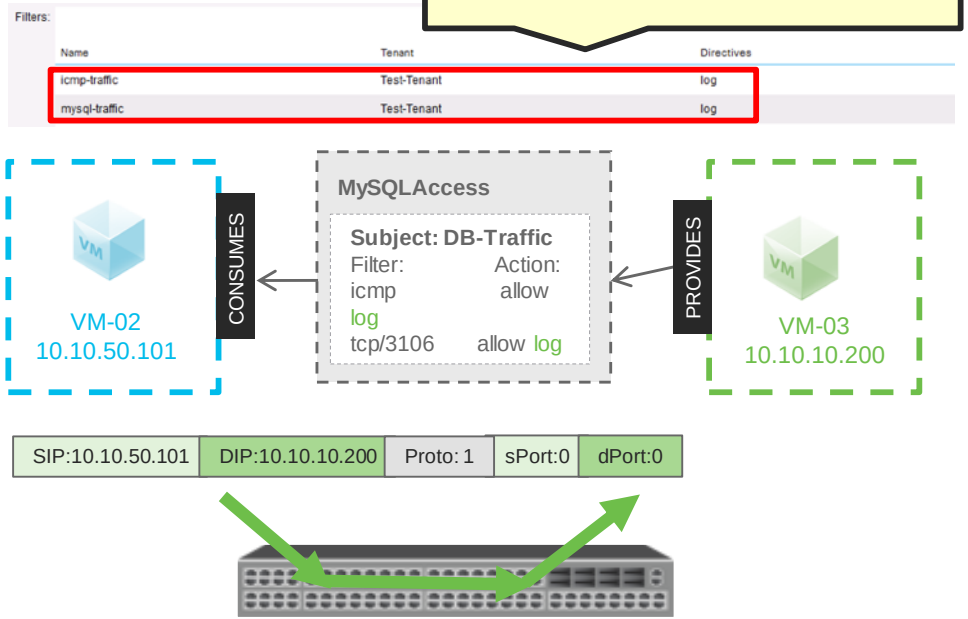
For Your Reference

Permit log configured at the subject on a per filter basis.

Logging Permit

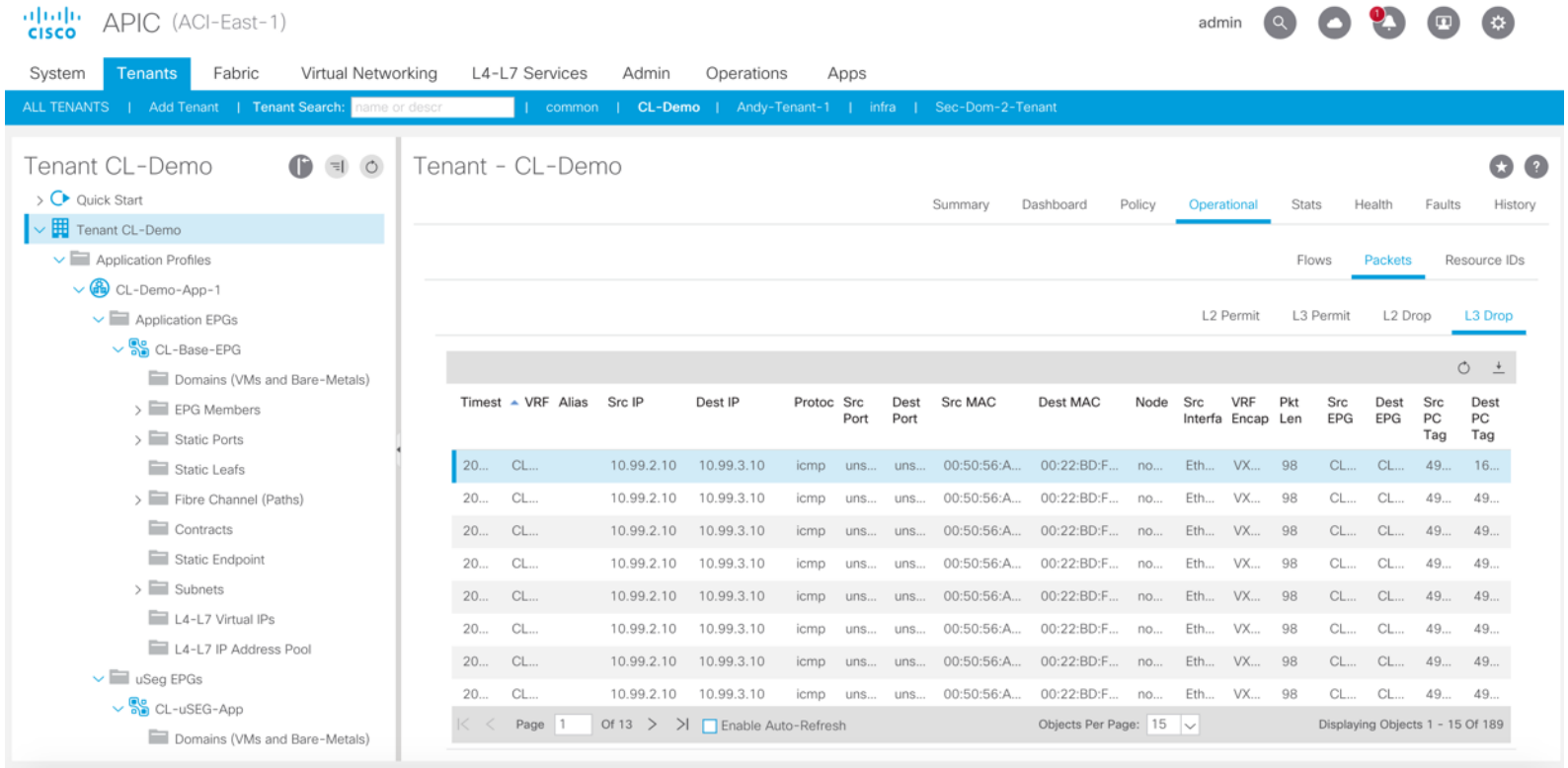
- Permit logging is configured per Filter
  - For Bare Metal, VDS and MSFT Domains logs generated by Leaf
  - For AVS logs may be generated on Leaf or vLeaf
  - For OpenStack ML2 mode, logs configured external to the fabric at the host
- Syslog is exported according to monitoring policies and configured External Data Collectors
- Logs include Tenant/VRF, EPG VLAN encap, ingress interfaces and offending packet details

- **Software Dependency: 2.2(1n) or higher**
- **Hardware Dependency: requires EX models or newer**

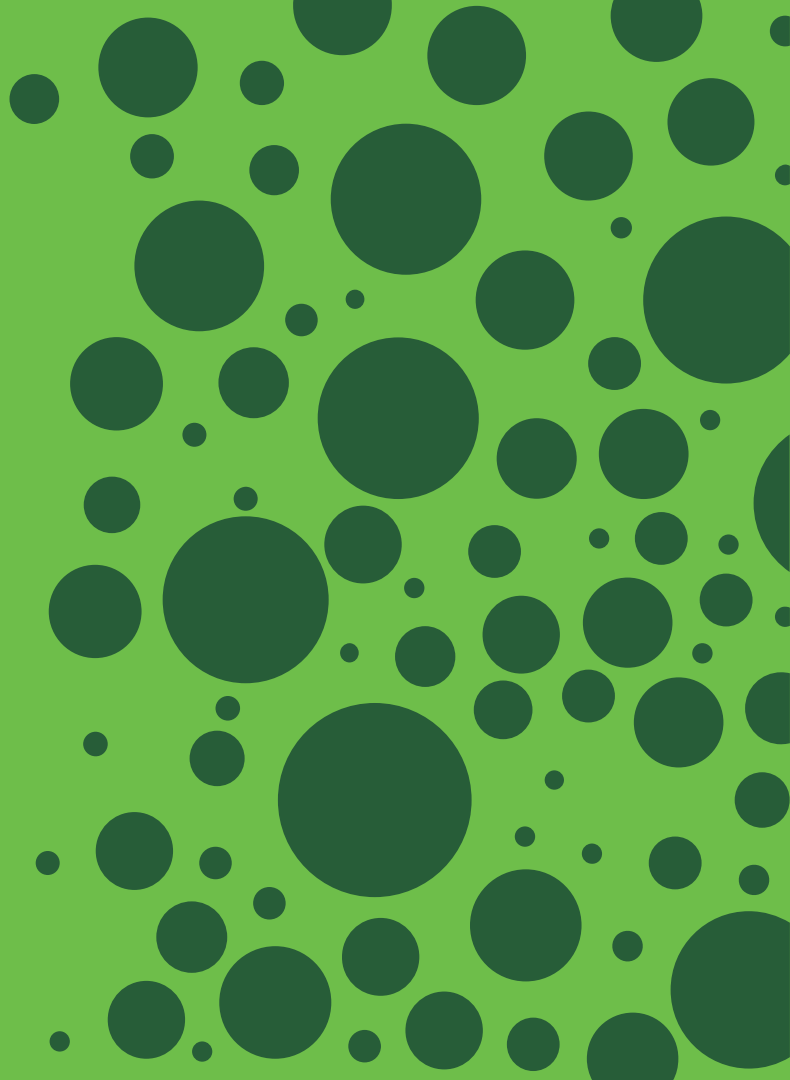


Feb 04 10:14:44 troy-leaf1 %LOG_LOCAL7-6-SYSTEM_MSG [E4204936][transition][info][sys] %ACLLOG-5-ACLLOG_PKTLOG_PERMIT: CName: Test-Tenant:Test-Tenant-VRF(VXLAN: 2162689), VlanType: FD_VLAN, Vlan-Id: 21, SMac: 0x00505690b43a, DMac:0x0022bdf819ff, SIP: 10.10.50.101, DIP: 10.10.10.200, SPort: 0, DPort: 0, Src Intf: port-channel2, Proto: 1, PktLen: 98

You can also see logs under the tenant

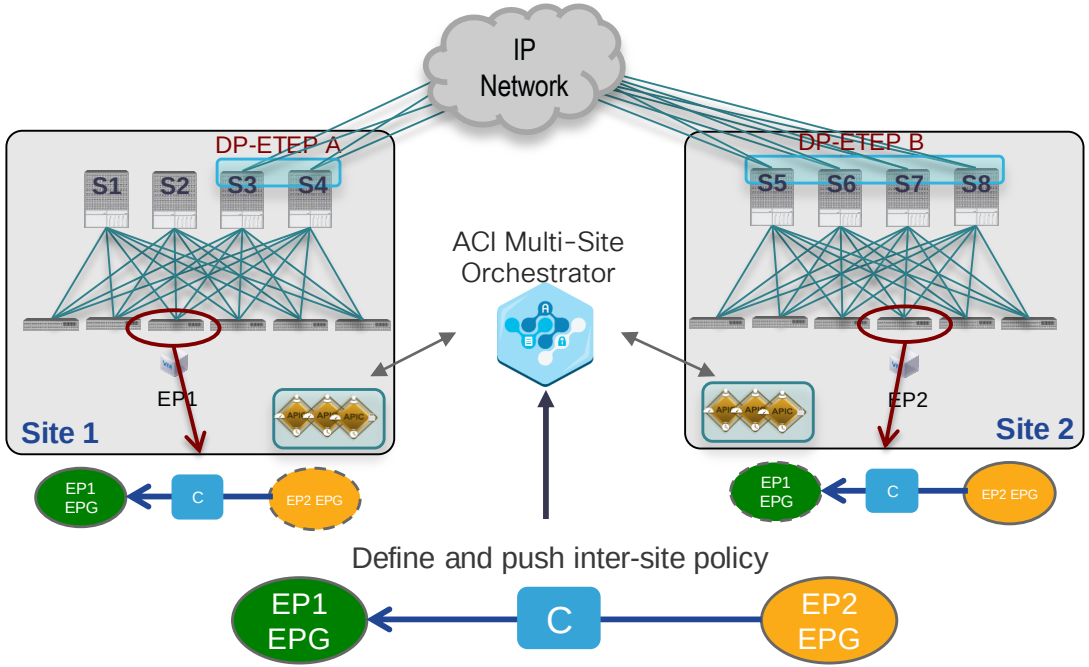


A quick work about contracts in ACI Multi-Site



ACI Multi-Site
Inter-Site Policies and 'Shadow Objects'

- Inter-Site policies defined on the Multi-Site manager are pushed to the respective APIC domains
- 'Shadow Objects' are created (for non stretched objects) in each APIC domain to be able to enforce policy locally
  - Requires namespace translation function performed by the spines



Agenda

- Micro Segmentation Fundamentals
- Endpoint Identity using EPG and micro EPG (uEPG)
- ACI Contracts for Policy Definition
- Improvements in hardware utilization
- ACI and Hybrid Cloud Security

While for most use cases hardware resource exhaustion for policy enforcement is never going to be a worry...you can have 128K policy TCAM entries on a single FX* switch.

We have added a few new features for the very heavy policy users.

*Amount of TCAM depends on the switch type

Bi-Directional Compression added in ACI Release 3.2

- Before 3.2 release, if the same contract was consumed and provided between the same EPGs, that would result in 2 TCAM entries being programmed in HW. One for consumer to provider and the other for provider to consumer

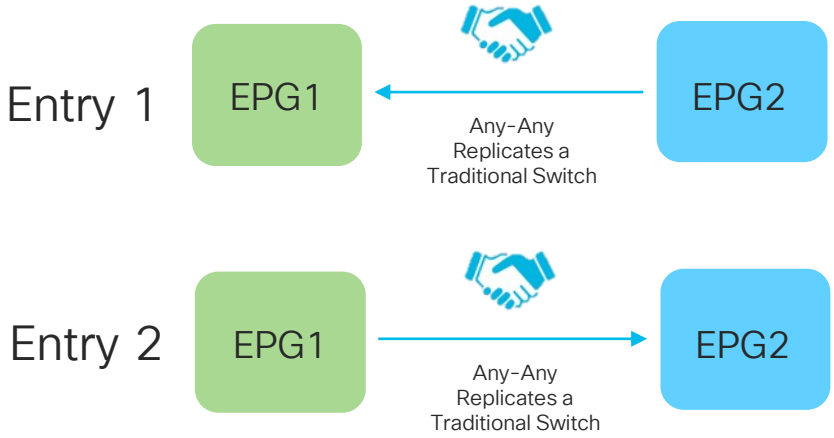
- After the introduction of the bi-directional compression feature in 3.2, if the same contract is consumed and provided between two EPGs. It could be represented in HW using a single TCAM entry with direction bit masked. This would mean TCAM savings of 50%.

- When rules are compressed they lose per direction statistics. Given that, the user has a choice to configure compression (TCAM savings) at the cost of statistics.

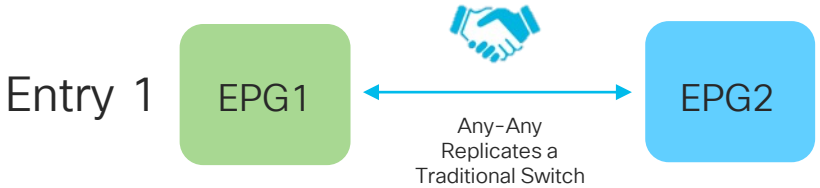
Oversimplified Look

Actual Contract Relationship

TCAM Entries Before 3.2



TCAM Entries After 3.2

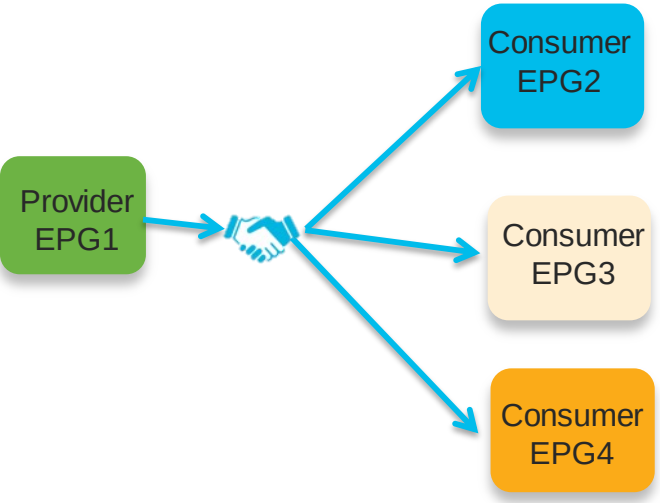


Criteria for Bi-directional TCAM Compression

- Only the contracts which follow the below guidelines will become candidates of bi-directional compression.
  - Contract->subject->apply-both-direction
  - Contract->subject->reverse-filter-ports
  - Contract->subject->filter-group->no-stats
  - Fully qualified rules
  - Action: permit or permit+log

Policy Compression via Indirection In ACI 4.0

- All provider-consumer EPG pair refer to same set of rules in the policy CAM
- No statistics for these compressed rules
- This built-in HW support allows improving zonerule scale.



1st Stage: Policy Group Label Lookup

sclass	dclass	PG-Label
EPG1	EPG2	10
EPG1	EPG3	10
EPG1	EPG4	10

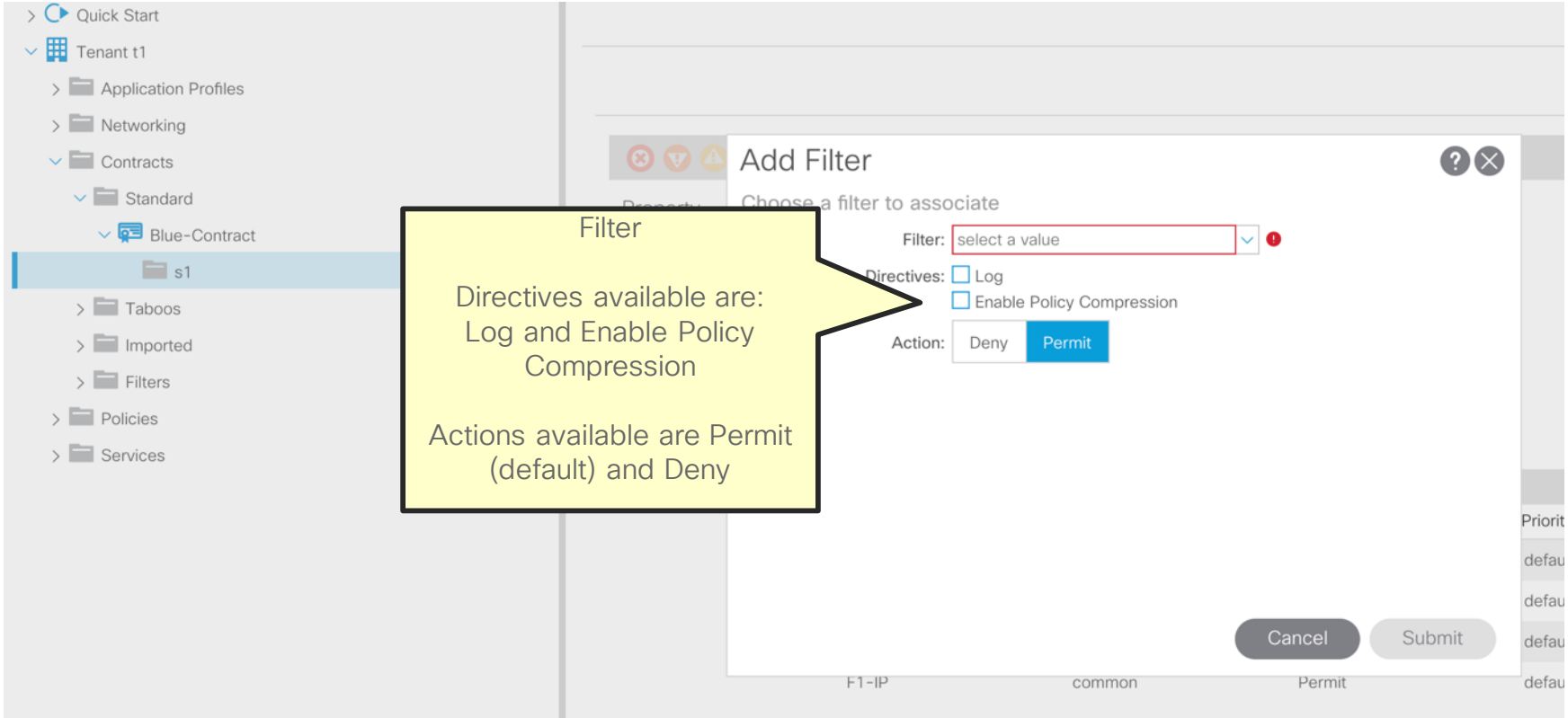
2nd Stage: Policy Hash TCAM Lookup

PG-Label	Protocol	sport	dport
10	tcp	*	443
10	tcp	*	80

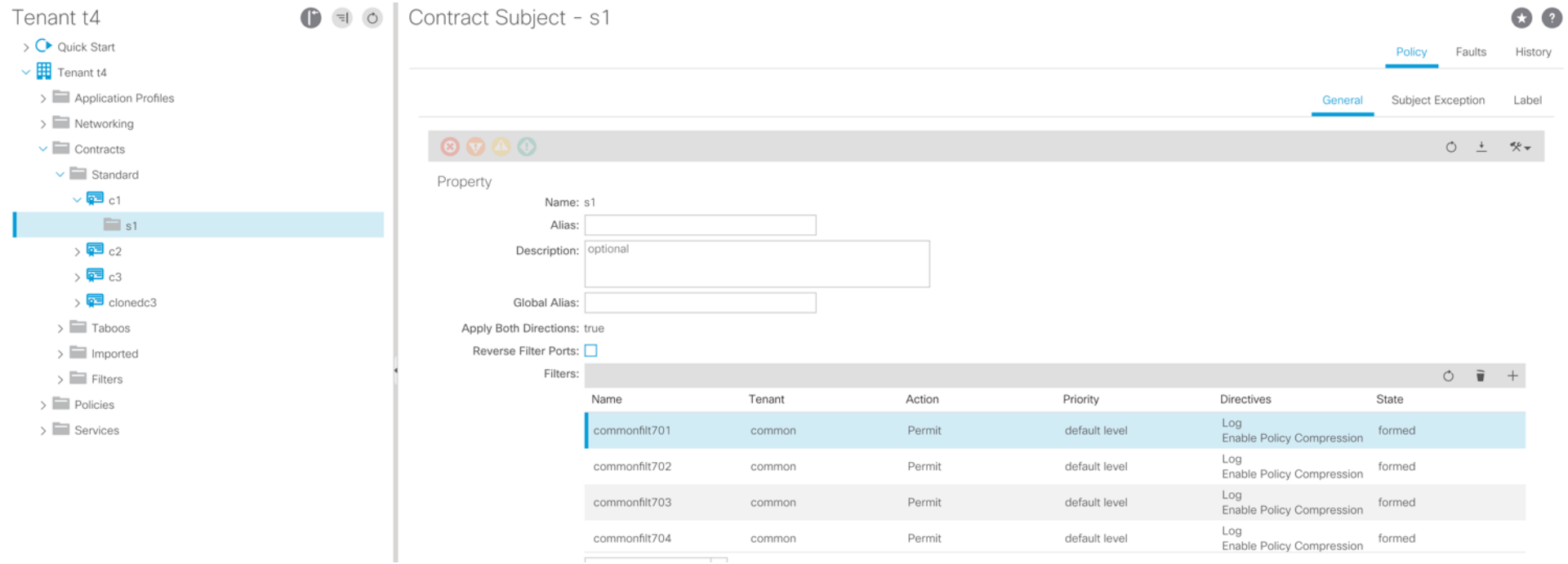
One copy of contract rules for all consumer EPG

Policy compression requires FX and later hardware

Enabling Policy Compression

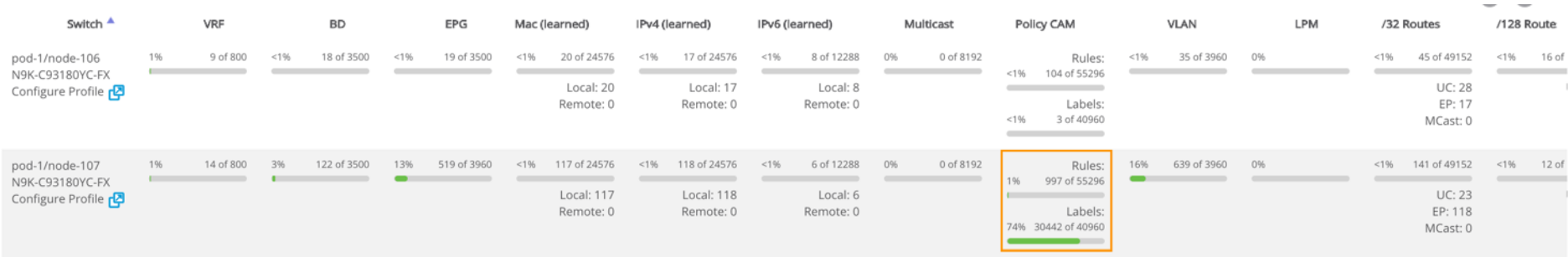


Contract Configuration Snapshot



Checking Filter/Contract Capacity on the Dashboard

Operations->Capacity Dashboard->Leaf Capacity



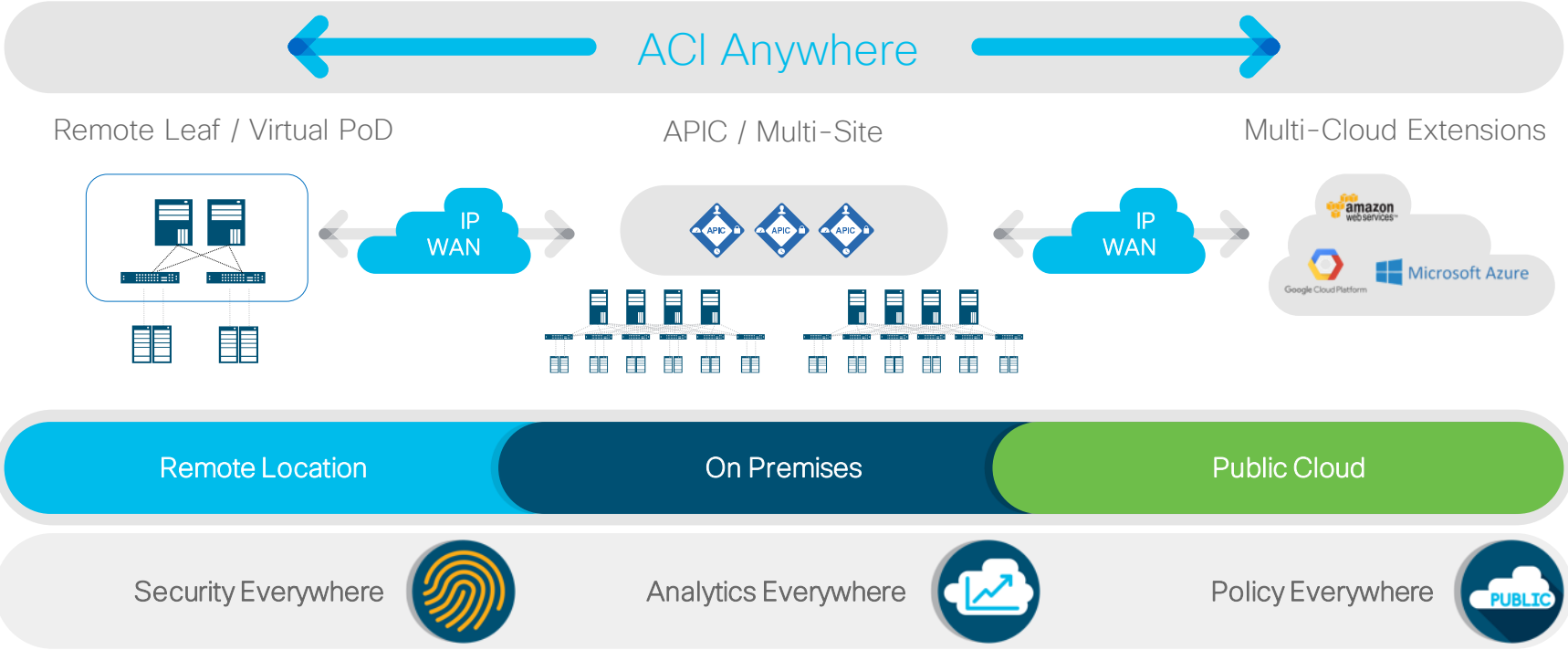
Switch	VRF	BD	EPG	Mac (learned)	IPv4 (learned)	IPv6 (learned)	Multicast	Policy CAM	VLAN	LPM	/32 Routes	/128 Route
pod-1/node-106 N9K-C93180YC-FX Configure Profile	1% 9 of 800	<1% 18 of 3500	<1% 19 of 3500	<1% 20 of 24576 Local: 20 Remote: 0	<1% 17 of 24576 Local: 17 Remote: 0	<1% 8 of 12288 Local: 8 Remote: 0	0% 0 of 8192	Rules: <1% 104 of 55296 Labels: <1% 3 of 40960	<1% 35 of 3960	0%	<1% 45 of 49152 UC: 28 EP: 17 MCast: 0	<1% 16 of
pod-1/node-107 N9K-C93180YC-FX Configure Profile	1% 14 of 800	3% 122 of 3500	13% 519 of 3960	<1% 117 of 24576 Local: 117 Remote: 0	<1% 118 of 24576 Local: 118 Remote: 0	<1% 6 of 12288 Local: 6 Remote: 0	0% 0 of 8192	Rules: 1% 997 of 55296 Labels: 74% 30442 of 40960	16% 639 of 3960	0%	<1% 141 of 49152 UC: 23 EP: 118 MCast: 0	<1% 12 of

Agenda

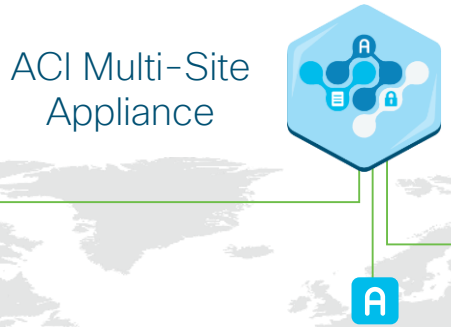
- Micro Segmentation Fundamentals
- Endpoint Identity using EPG and micro EPG (uEPG)
- ACI Contracts for Policy Definition
- Improvements in hardware utilization
- ACI and Hybrid Cloud Security

ACI Anywhere - Vision

Any Workload, Any Location, Any Cloud

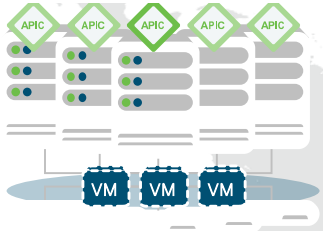


ACI Hybrid-Cloud Deployment Model

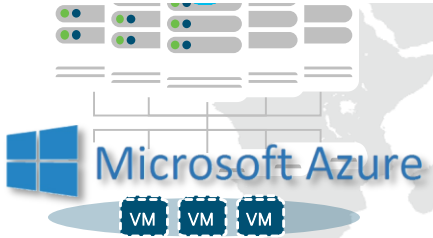


Hybrid Cloud:
- AWS in Q2-CY19
- Azure in Q3-CY19

AWS Integration is in EFT with several customers today

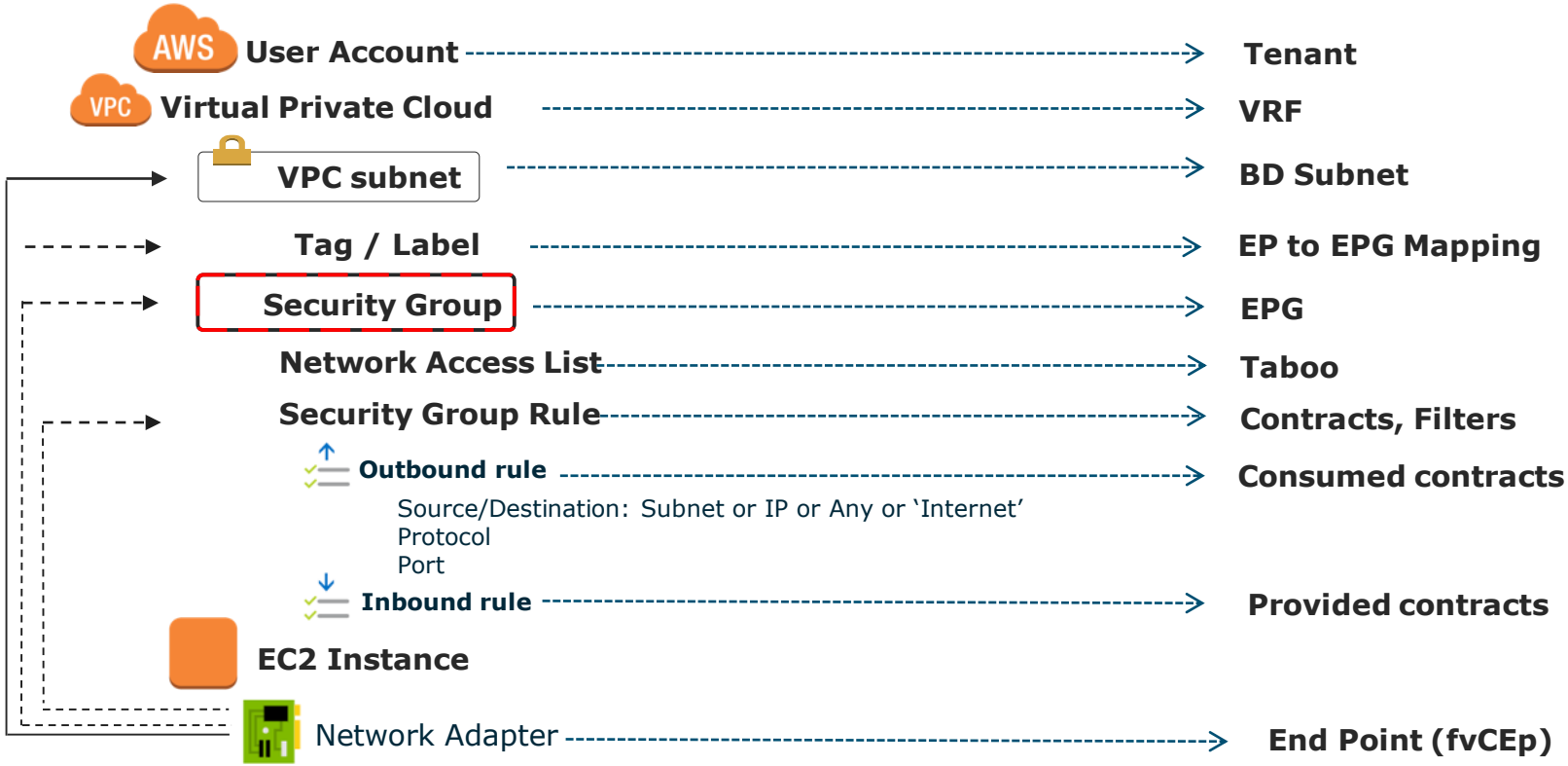


ACI – On Premise



Common Governance	Discovery & Visibility	Policy Translation	Monitoring & Troubleshooting	Single Point Of Orchestration	Operational Consistency

Policy and Resource Mapping - AWS



Policy Mapping – AWS

Identity and Access Management (IAM)

Region

Availability Zone (AZ)

Infra VPC

VPC Peering

Internet Gateway,

VPN Gateway,

Direct Connect,

CSR1000V

Inter Region VPC Peering
Direct Connect Gateway

AAA Users, Security Domains

Pod

Path/Node Attachment

Overlay-1 VRF (ACI Infra)

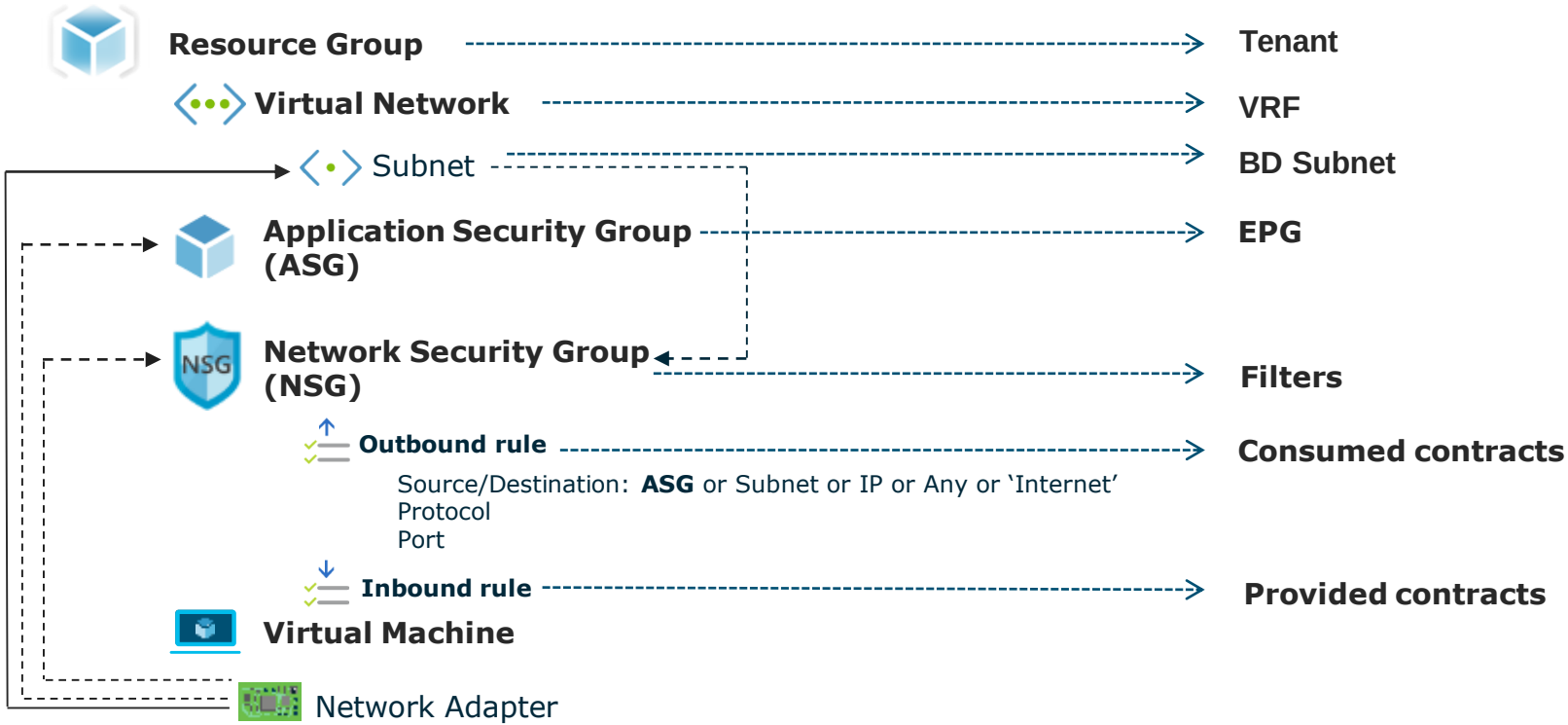
Shared Services / Common

Border Leaf, Spine (Internal and External connectivity)

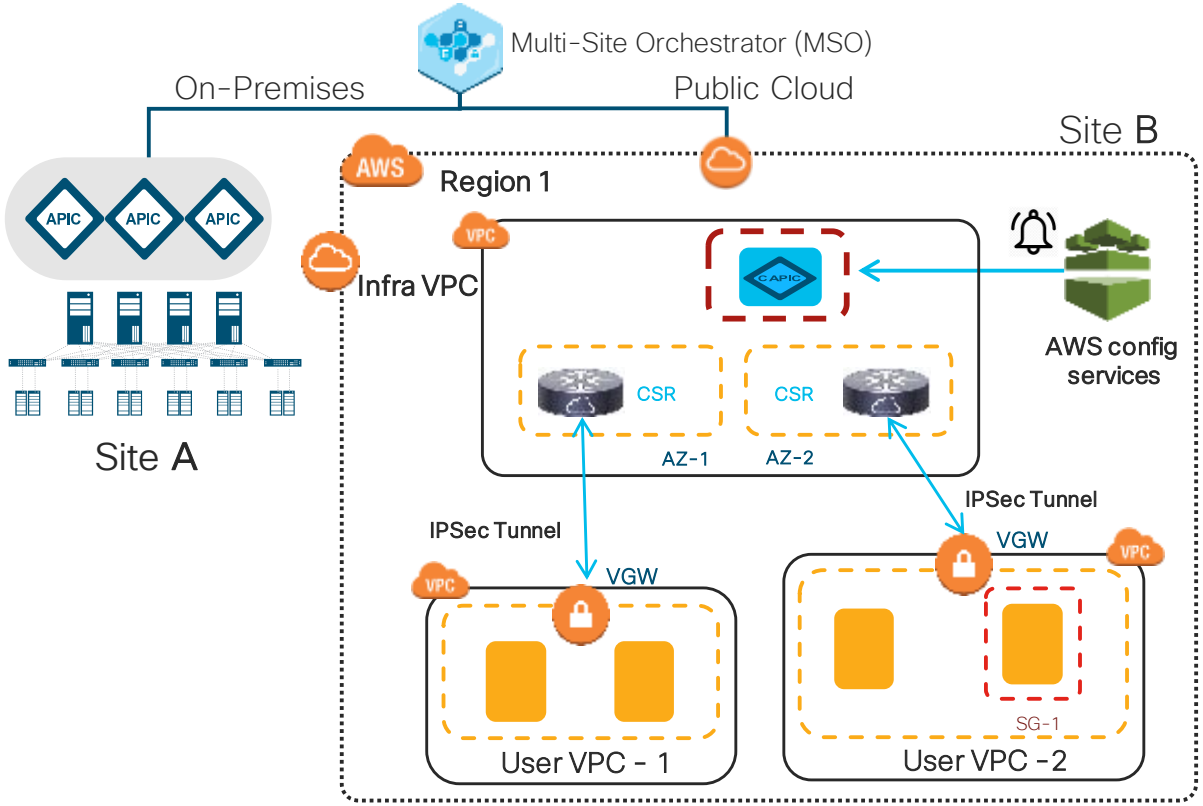
Inter POD Connectivity

For your info & reference

Policy Mapping – Azure



End Point Learning on AWS



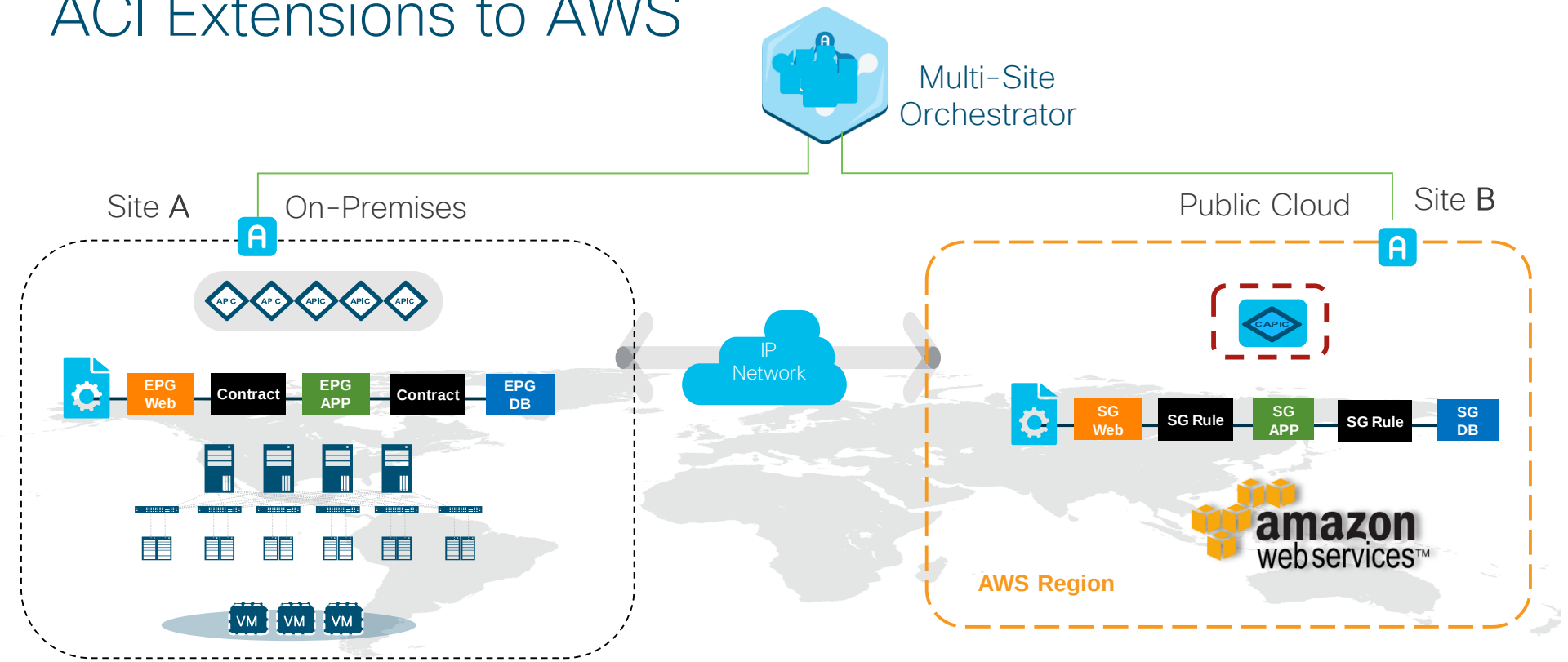
- User deploys a new instance in AWS
- AWS config services notifies the event to cAPIC
- cAPIC learns the endpoint and registers it
- Based on the policies (EPG's and Contracts) the correct security group (SG) is attached to the instance

Security Group (SG) | Availability Zone (AZ)

CSR-1000V | AWS Internet Gateway (IGW)

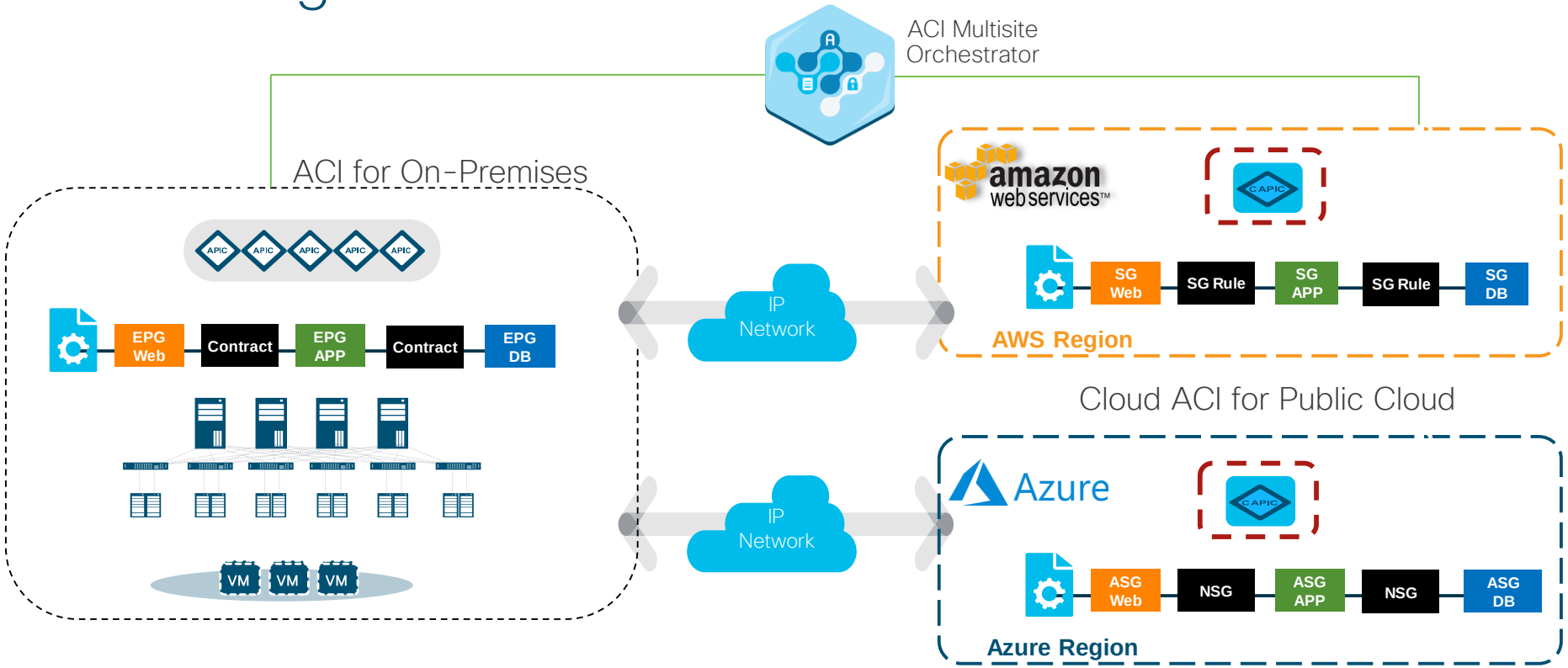
Cloud APIC | AWS Virtual Private Gateway (VGW)

ACI Extensions to AWS



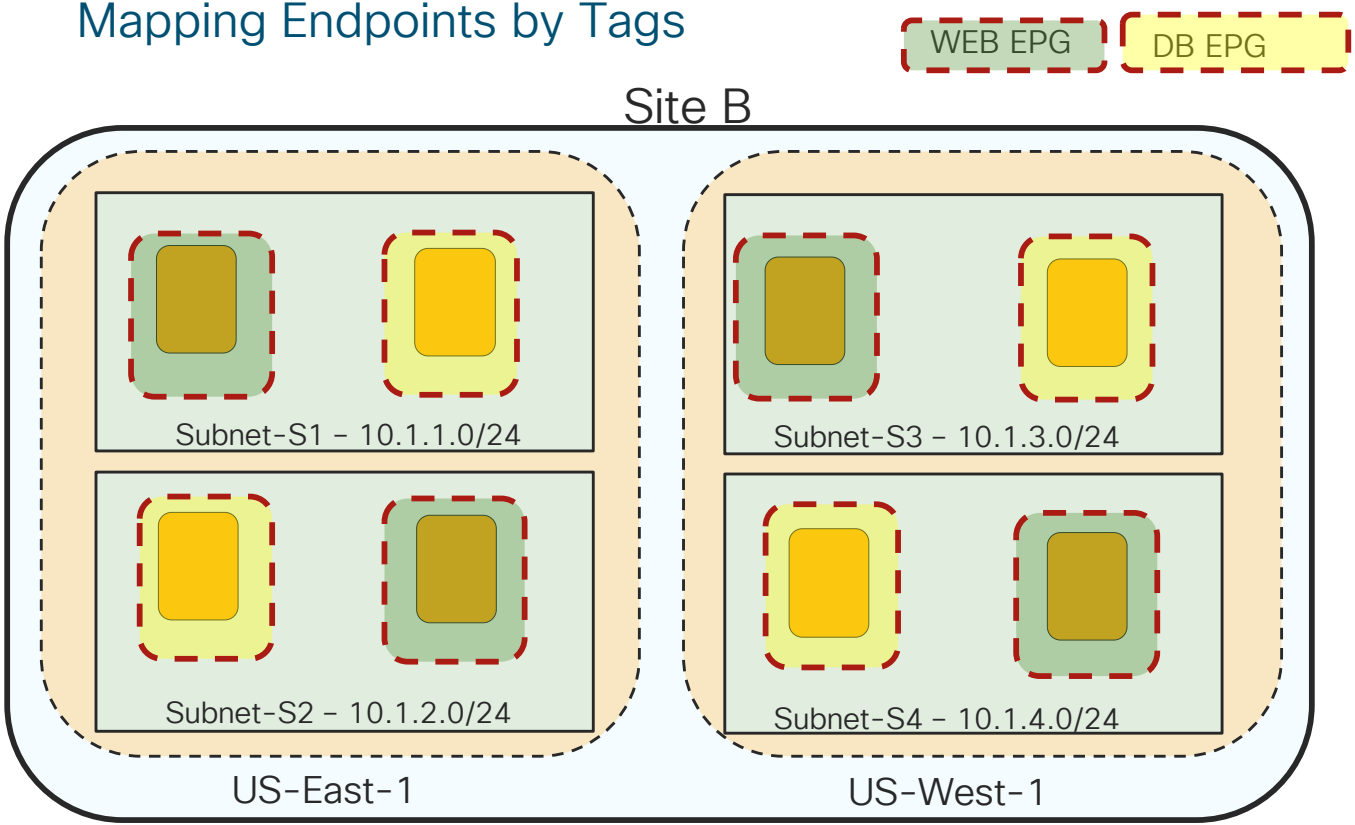
Common Governance | Discovery & Visibility | Policy Translation | Monitoring & Troubleshooting | Single Point Of Orchestration | Operational Consistency

Extending ACI to the Cloud



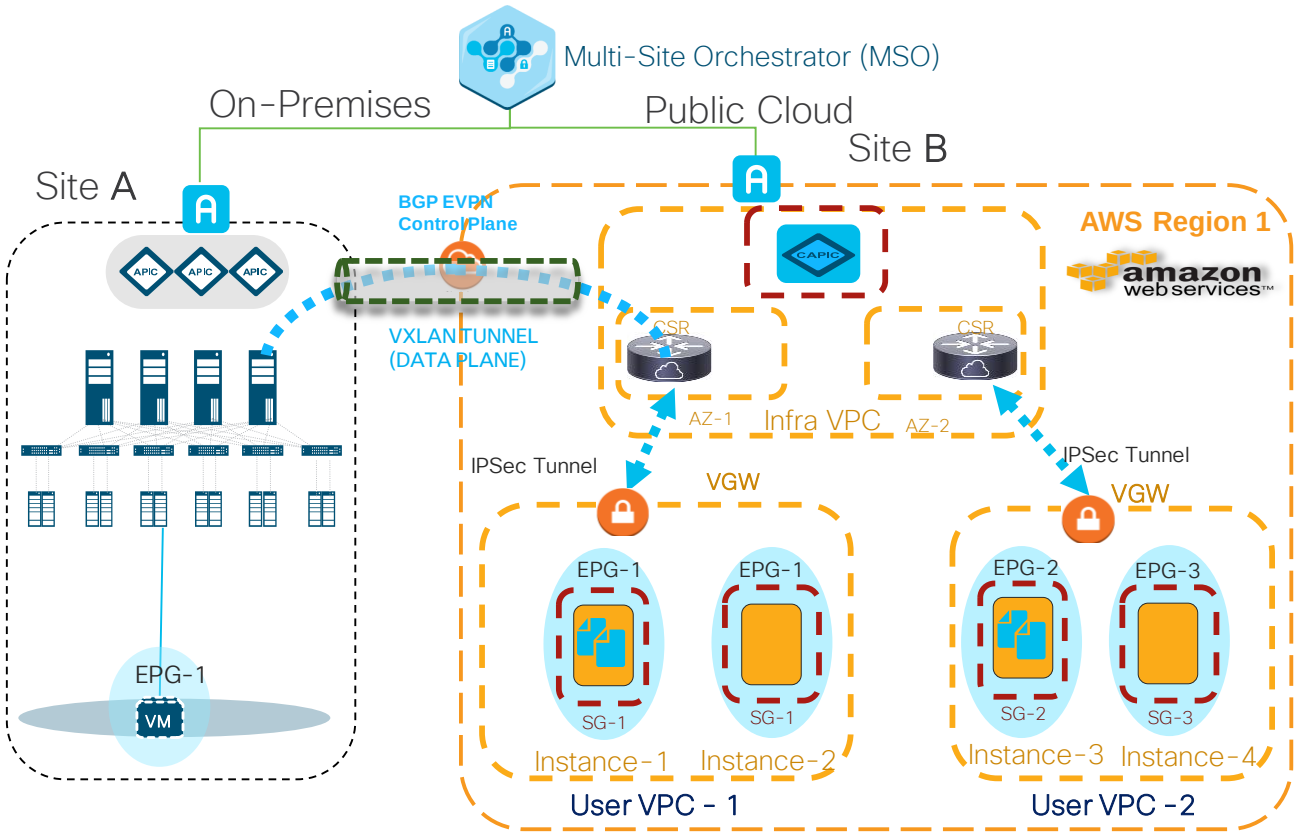
Common Governance | Discovery & Visibility | Policy Translation | Monitoring & Troubleshooting | Single Point Of Orchestration | Operational Consistency

Cloud EPG
Mapping Endpoints by Tags



- Web-EPG associated to tag: “EPG: WEB”
- Web-EPG has endpoints across Us-East-1 & Us-West-1 regions and multiple subnets
- DB-EPG associated to tag: “EPG:DB”
- DB-EPG has endpoints across Us-East-1 & Us-West-1 regions and multiple subnets

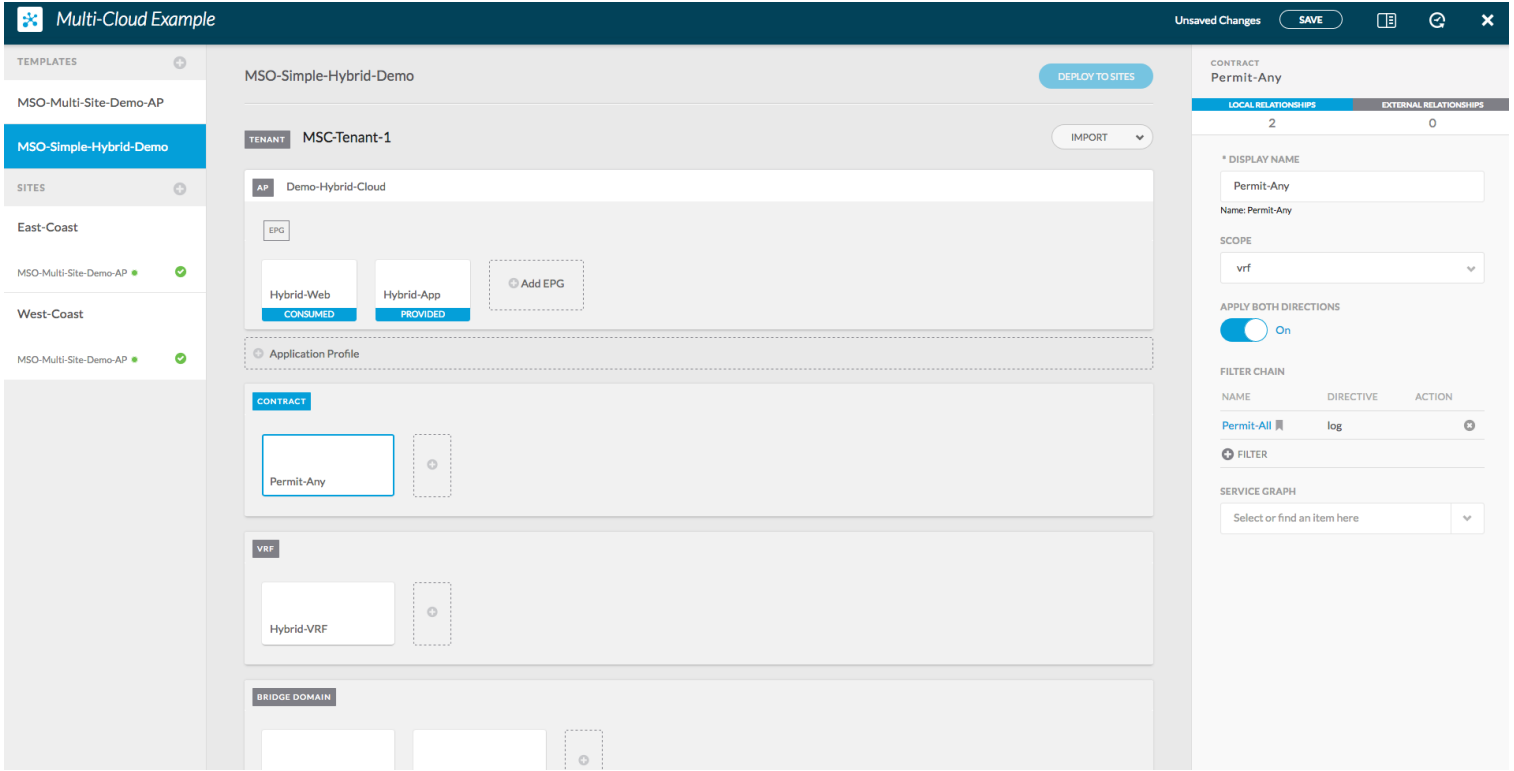
Instances in a VPC and on-Premises



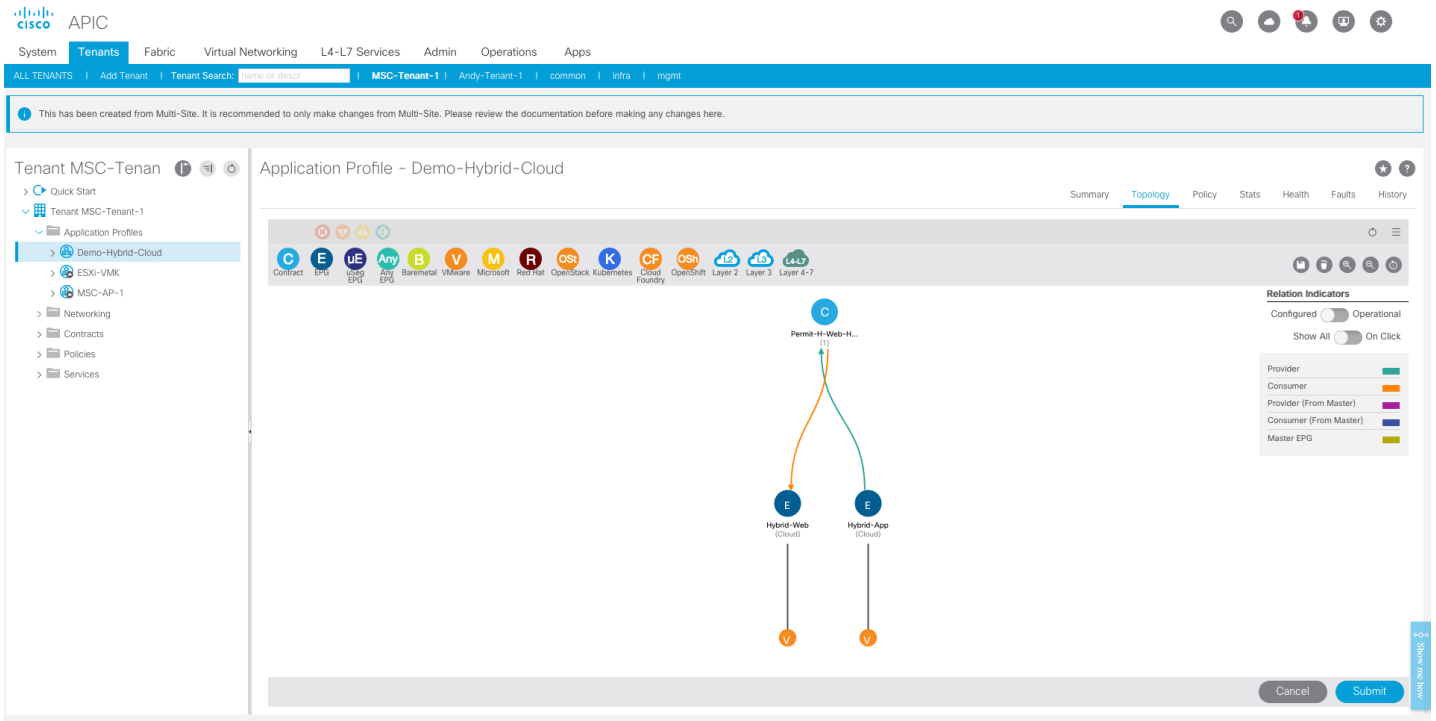
For traffic from Instances in a VPC to on-premises, traffic reaches CSR in Infra VPC and goes over the VXLAN tunnel to the ACI spines on-premises

Spine forwards the traffic to the corresponding leaf on which the EP is located

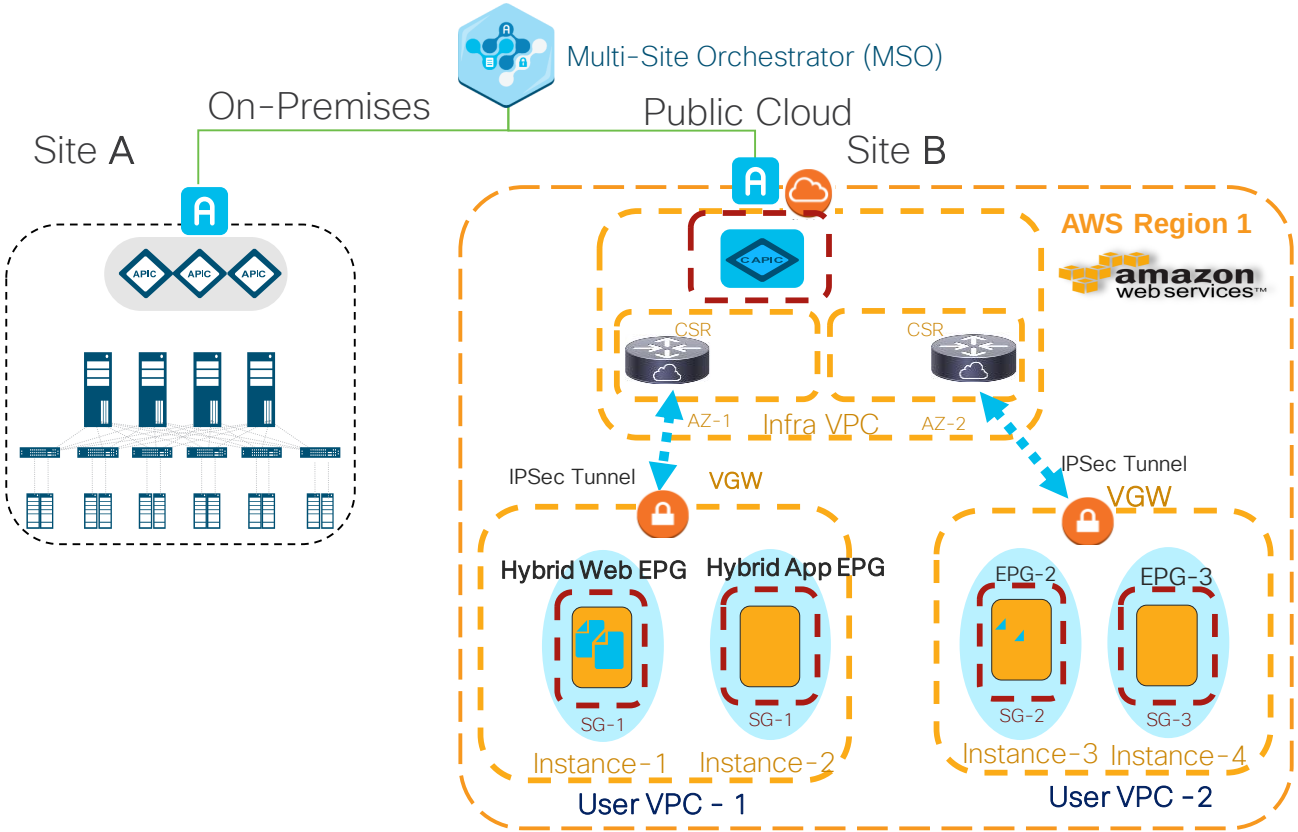
Creating an Application Using MSO



Traffic Allowed Between Two EPGs

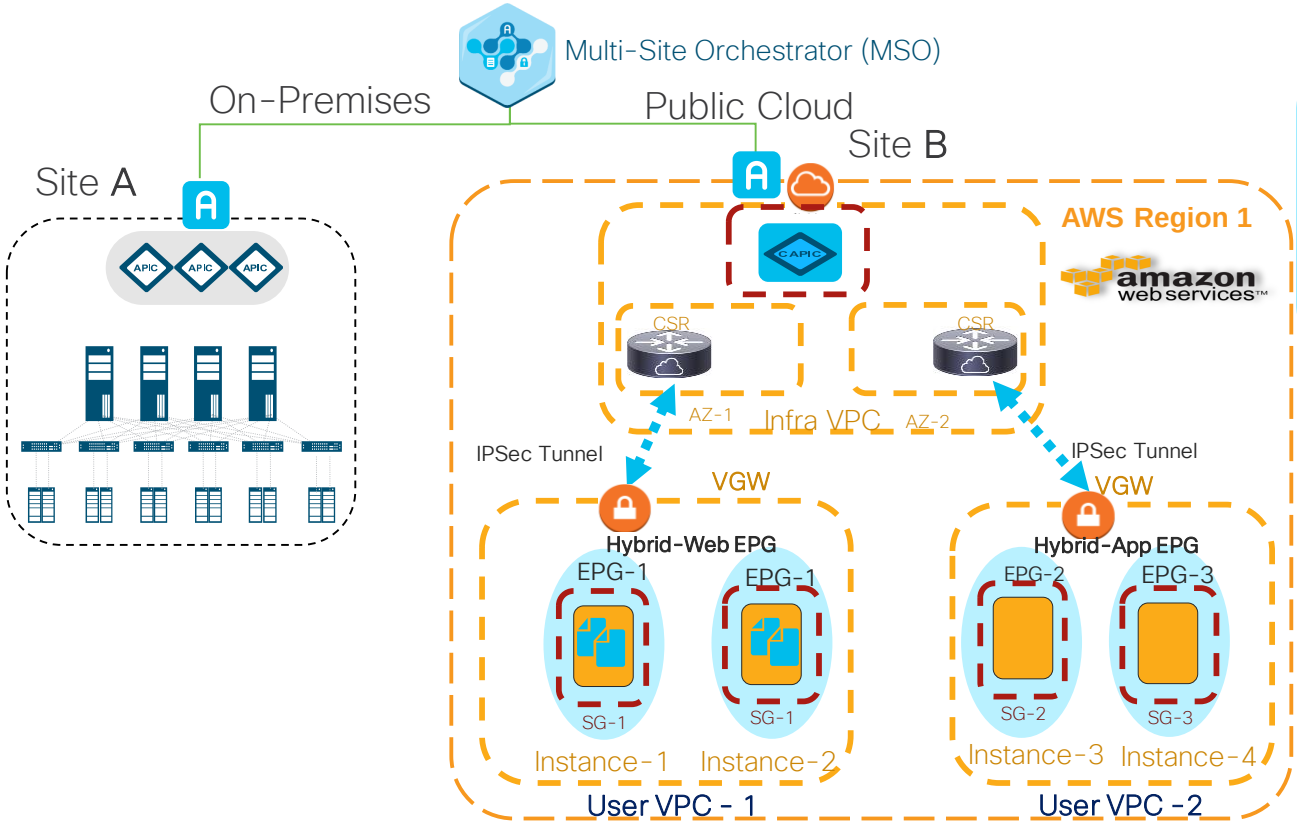


Instances within a VPC



All traffic between instances within the same VPC, can directly communicate to each other based on the respective security group policies programmed by cAPIC

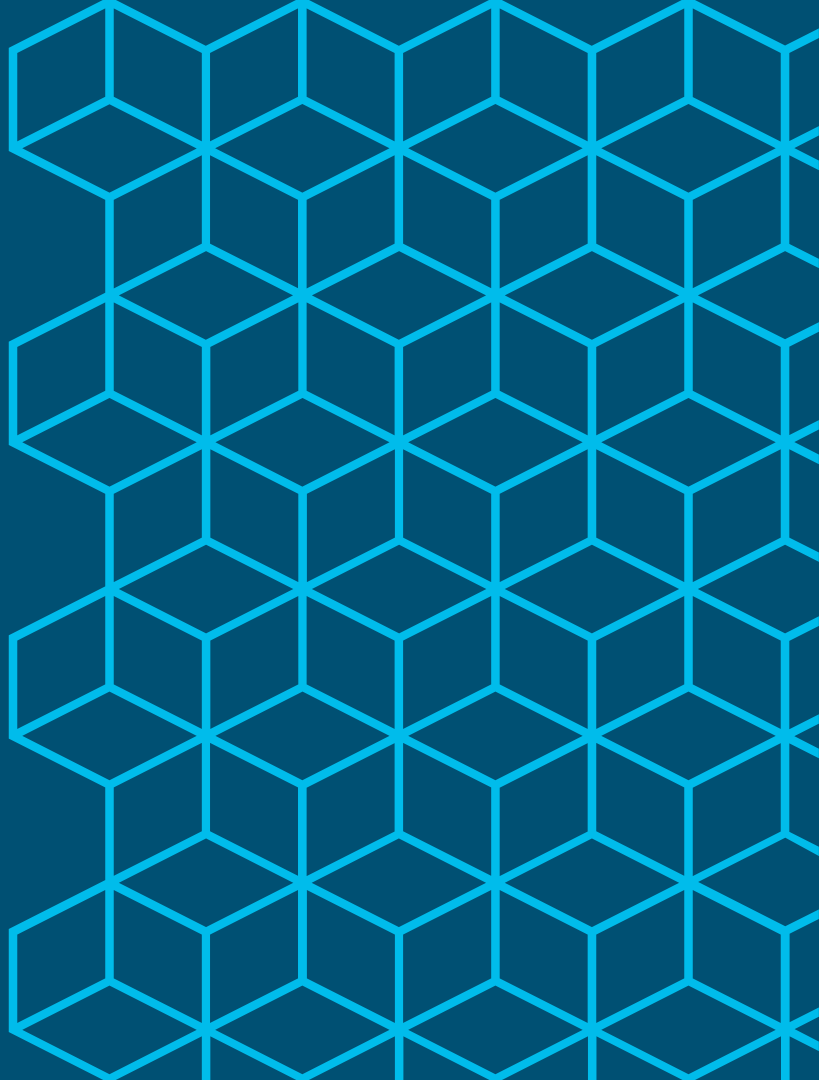
Instances across VPCs



For instances in two different VPCs communicating to each other, the traffic has to exit the VPC either via VGW of the user VPC and reach CSR in infra VPC.

Once the traffic reaches the CSR in infra VPC, packets are routed to the destination based on the configured policies

Demo



Demo

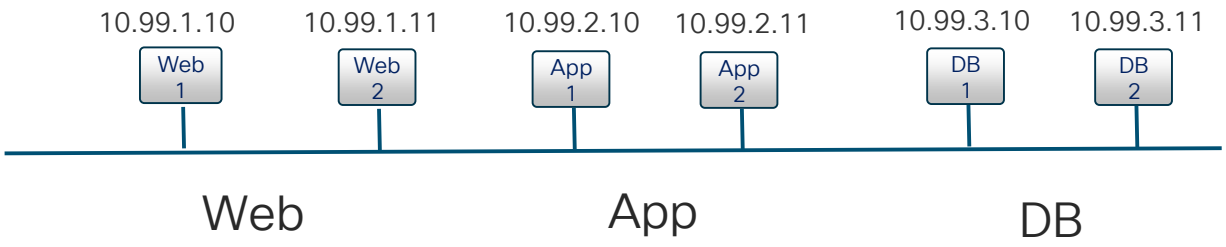
Tenant: CL-Demo

App: CL-Demo-App-1

EPG: CL-Base-EPG

CL-Base-EPG

Web-App-DB-BD
10.99.1.1/24
10.99.2.1/24
10.99.3.1/24



Demo

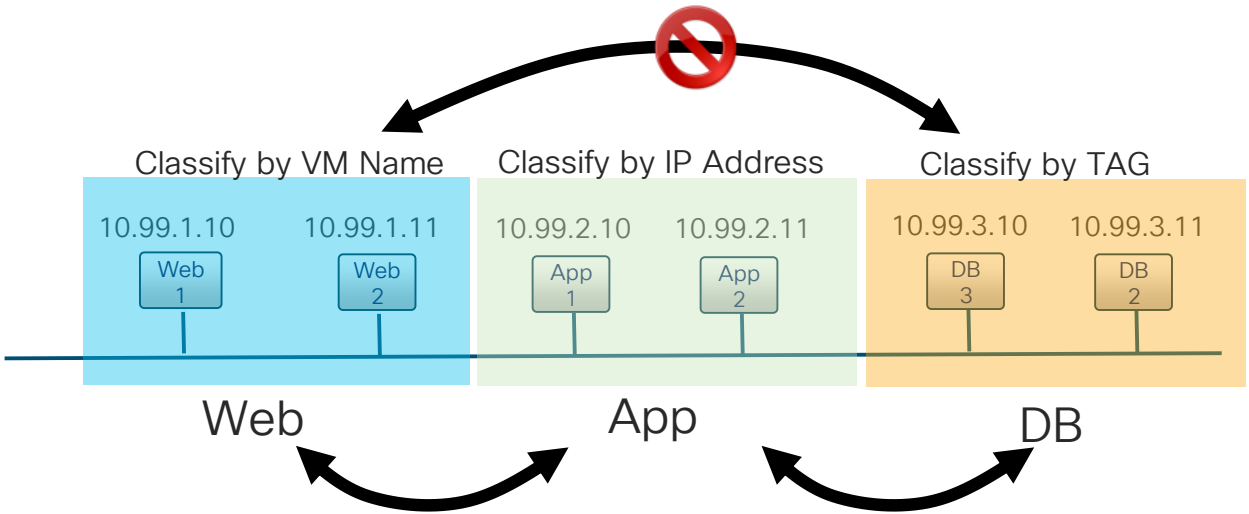
Tenant: CL-Demo

App: CL-Demo-App-1

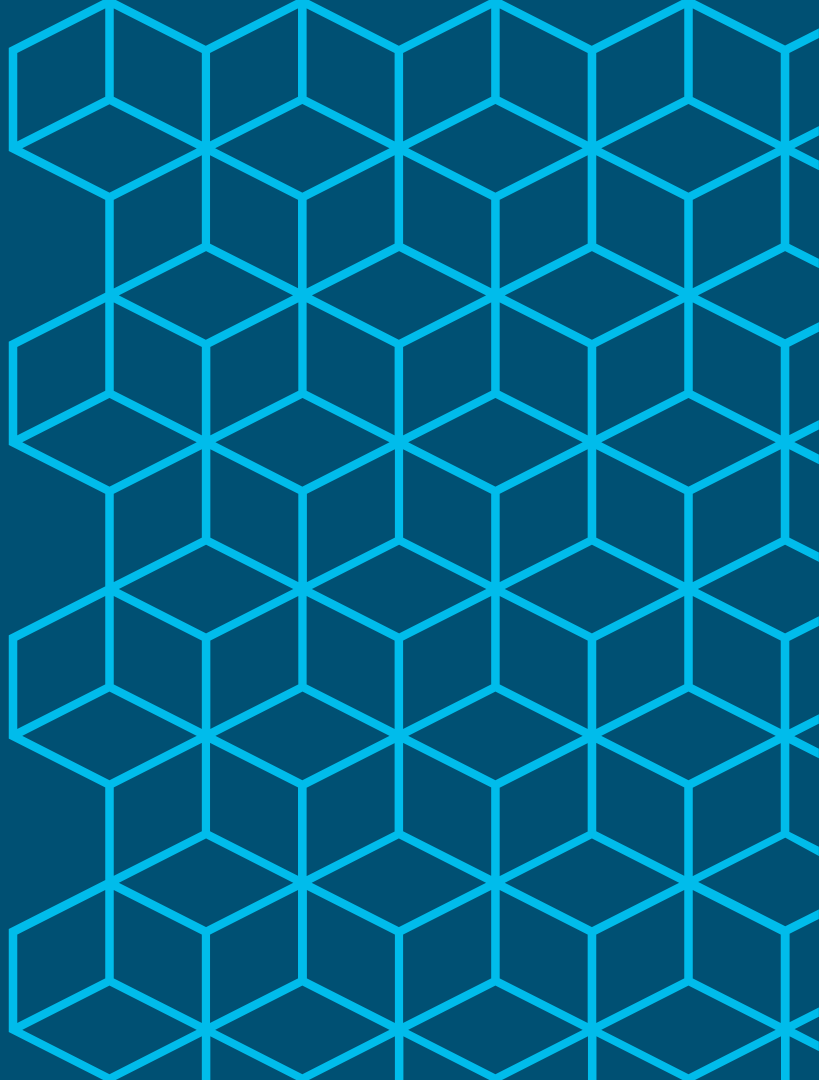
EPG: CL-Base-EPG

CL-Base-EPG

Web-App-DB-BD
10.99.1.1/24
10.99.2.1/24
10.99.3.1/24



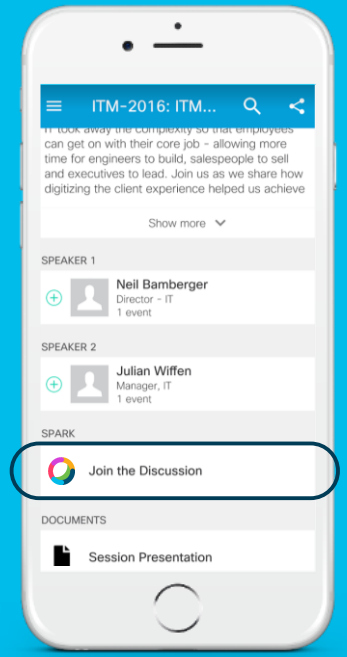
Summary



ACI enables micro segmentation that you can deploy in a gradual and flexible way. Use the right tool or feature for your use case...

You can use static configurations using the GUI or the NX-OS CLI …

... and you can use orchestration or configuration management tools...



cs.co/ciscolivebot#BRKACI-2301

Cisco Webex Teams

Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

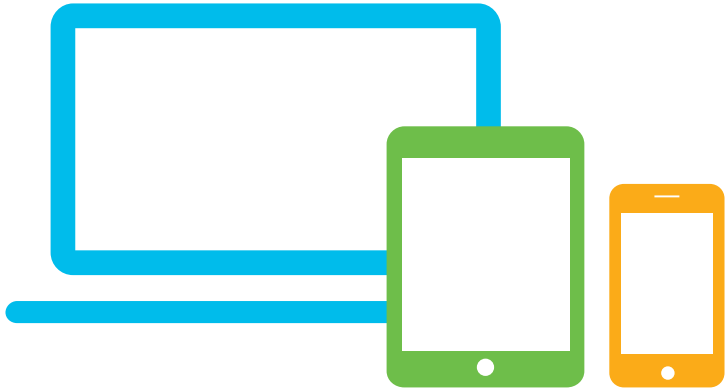
How

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

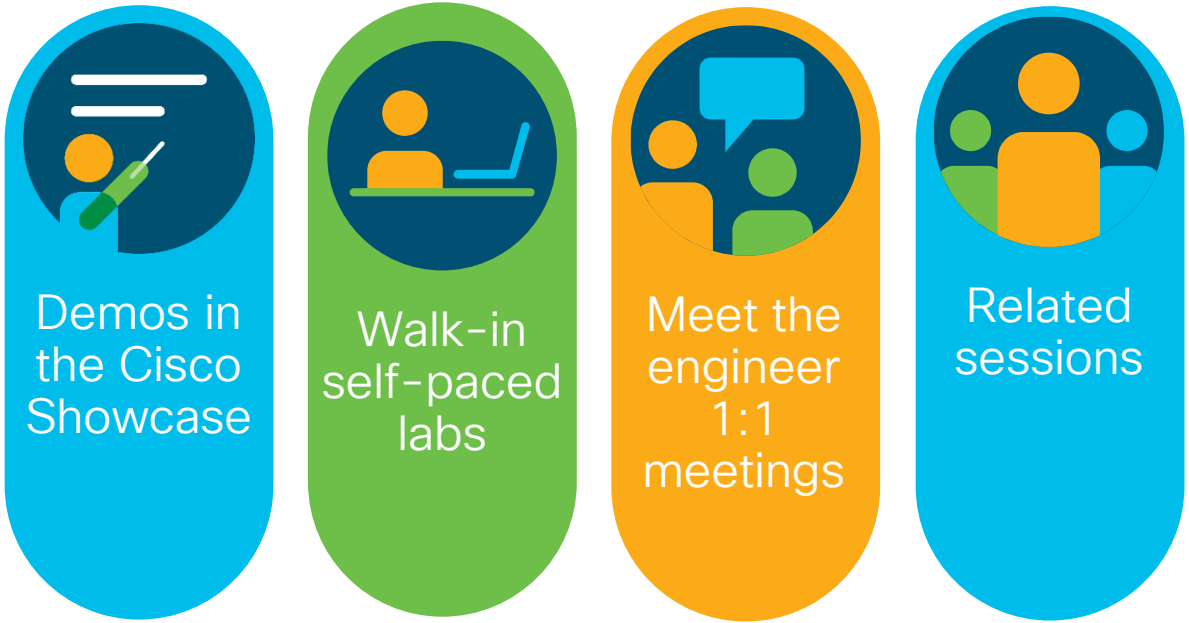
Complete your online session survey

- Please complete your Online Session Survey after each session
- Complete 4 Session Surveys & the Overall Conference Survey (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Events Mobile App or the Communication Stations

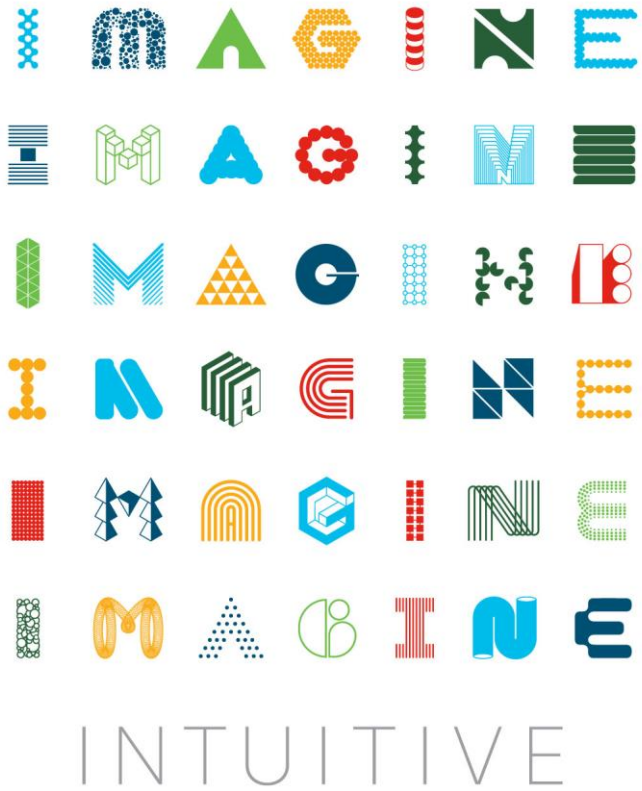
Don't forget: Cisco Live sessions will be available for viewing on demand after the event at ciscolive.cisco.com



Continue Your Education



Thank you



INTUITIVE