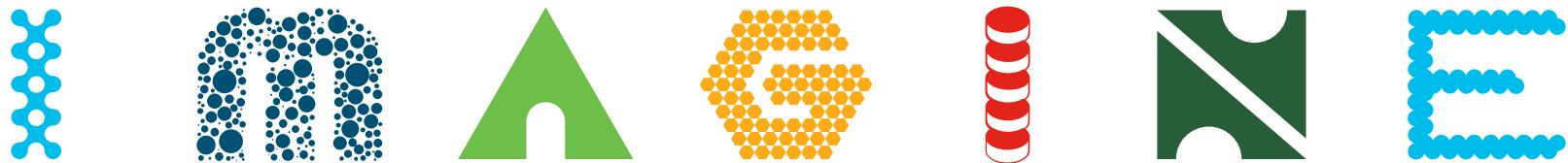




January 28 - February 1, 2019 • Barcelona



INTUITIVE



BRKACI-2301

Practical Applications of Cisco ACI Micro Segmentation

Andy Sholomon

@asholomon, Principal Engineer – DC Switching

Cisco *live!*



INTUITIVE

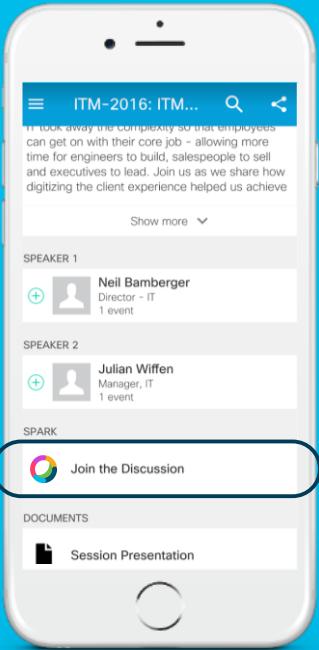
Session Objectives

- 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.





Cisco Webex Teams



Questions?

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

How

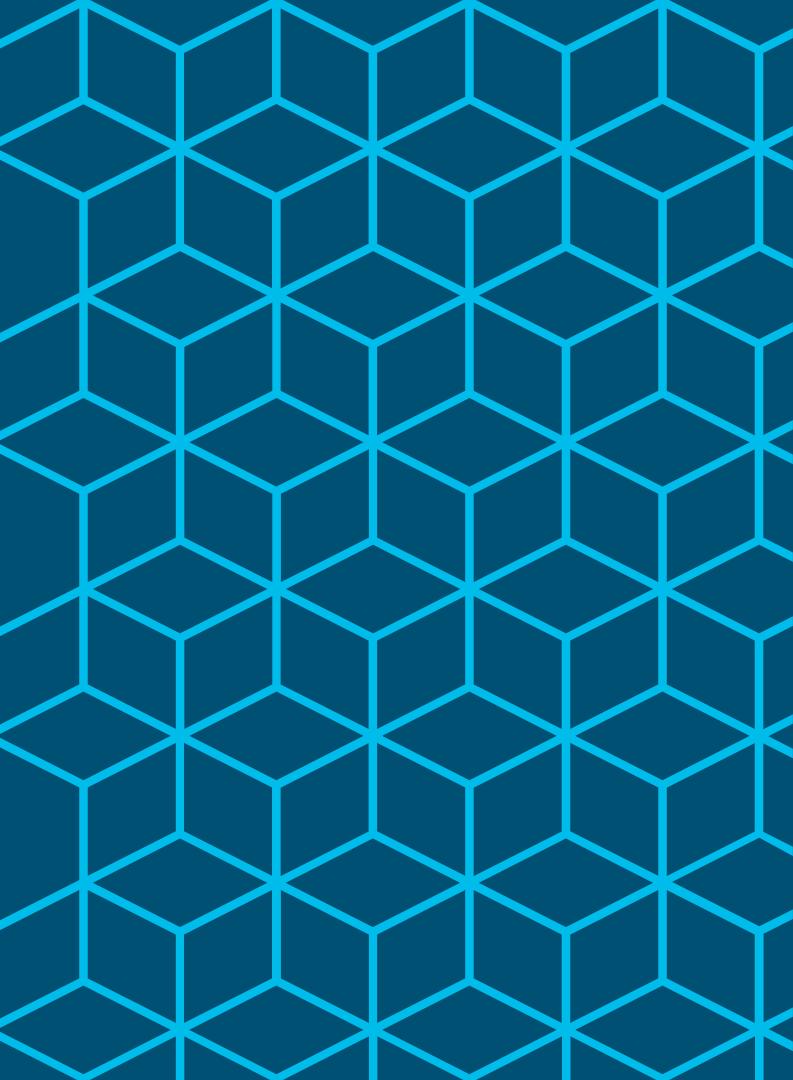
- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space

cs.co/ciscolivebot#BRKACI-2301

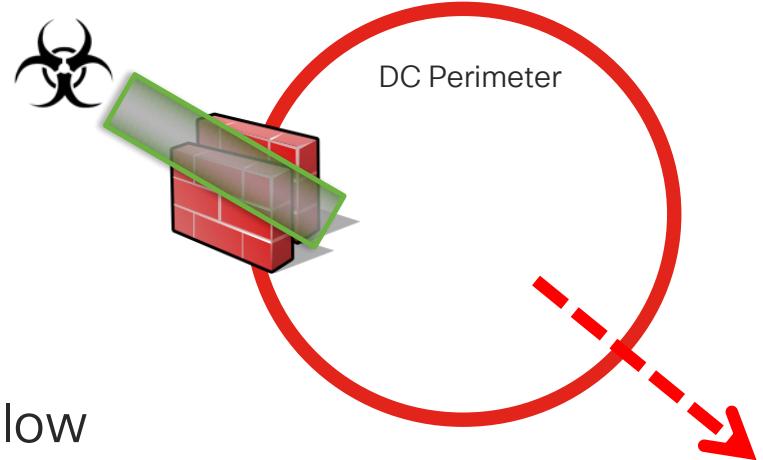
Agenda

- 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?

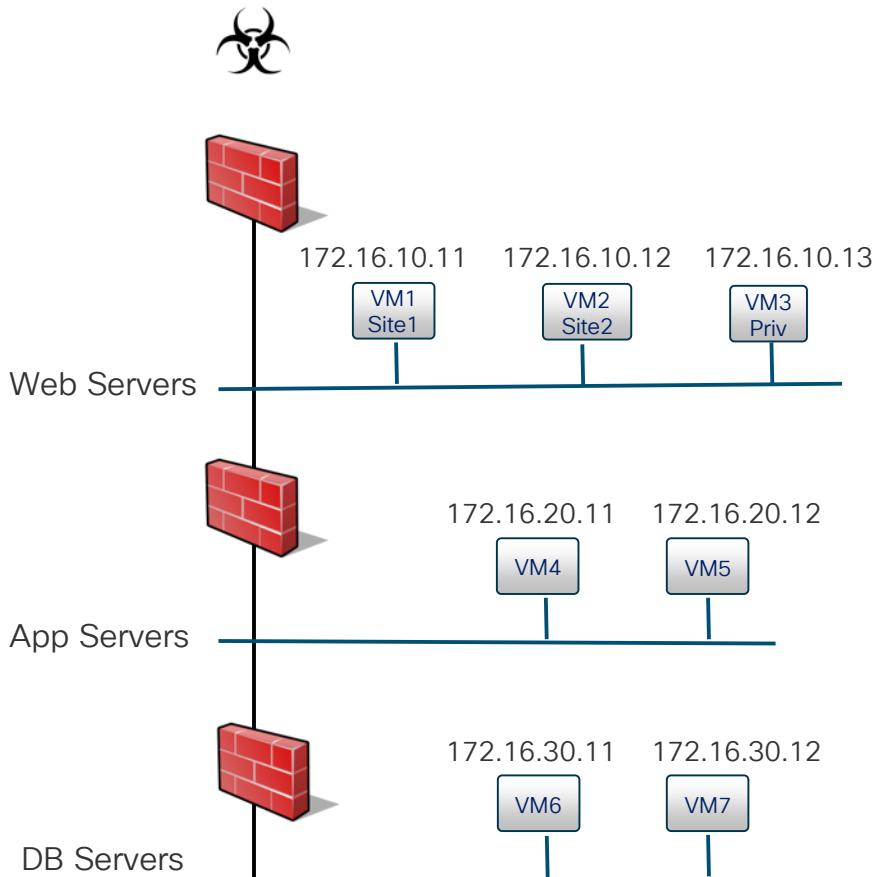


Why Micro Segmentation?

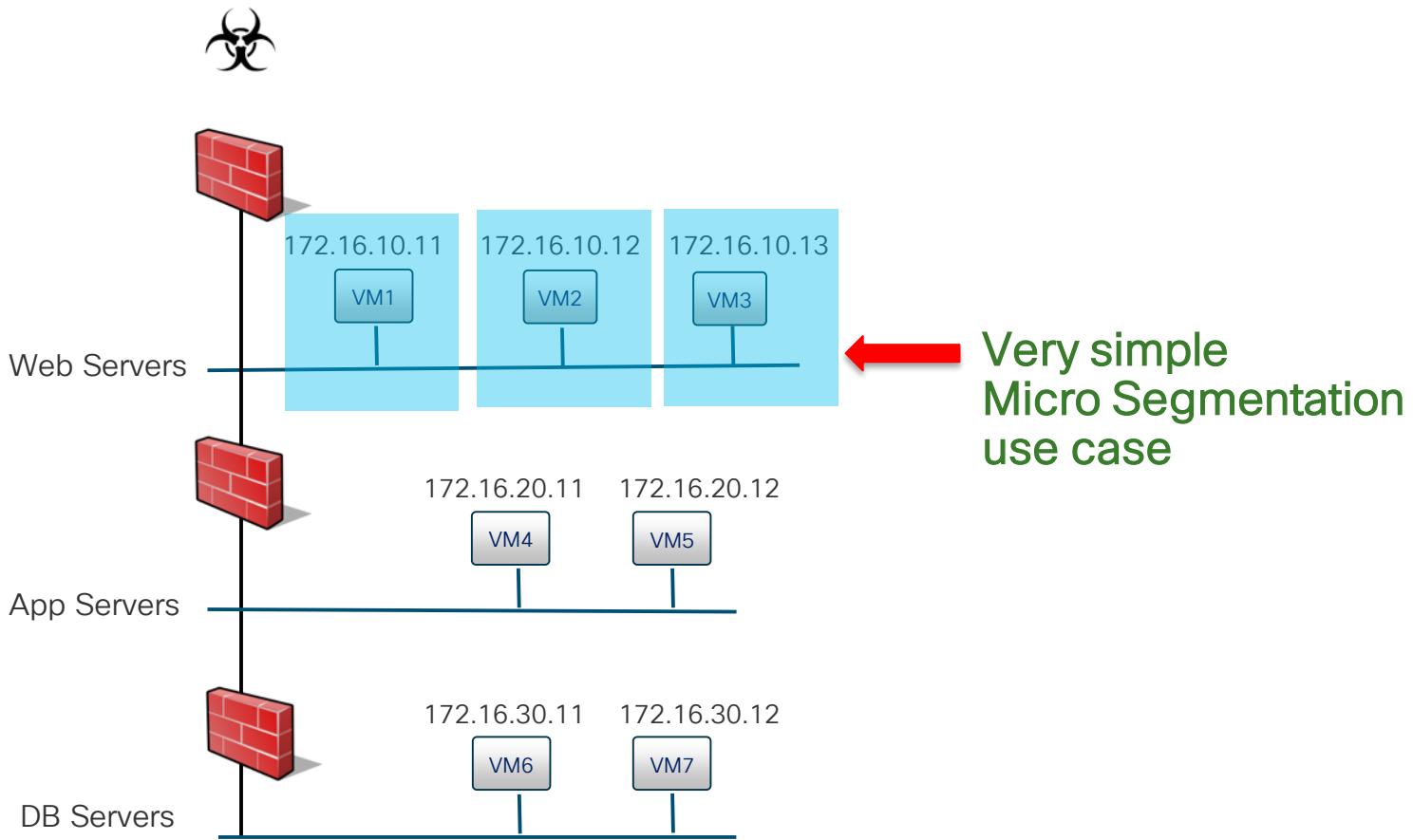


- Perimeter security is not enough: once it is breached, lateral movement can allow attackers to compromise more assets
- Micro Segmentation can improve the security posture inside the Data Center
- Micro Segmentation can minimize segment size and provide lesser exposure for lateral movement

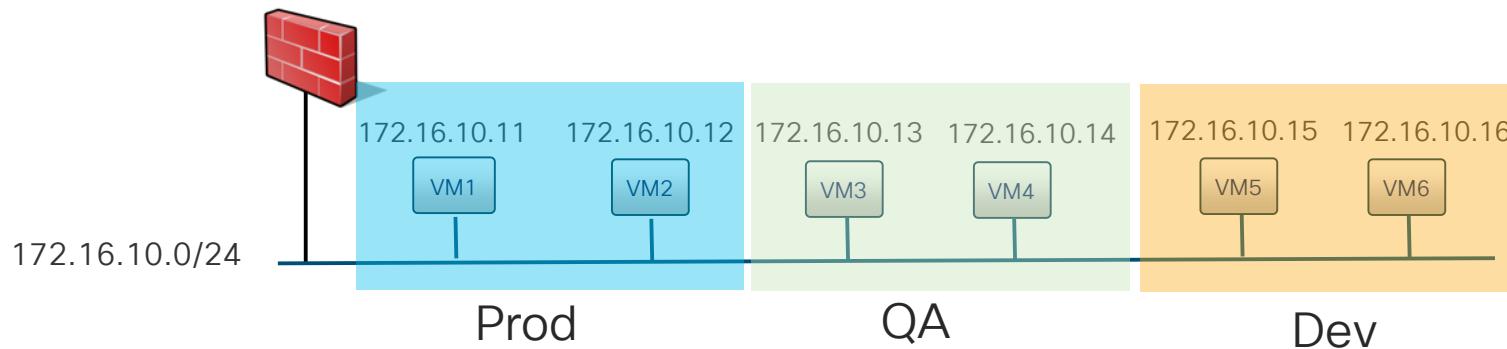
Security Risk: VMs or Servers on a Single Subnet



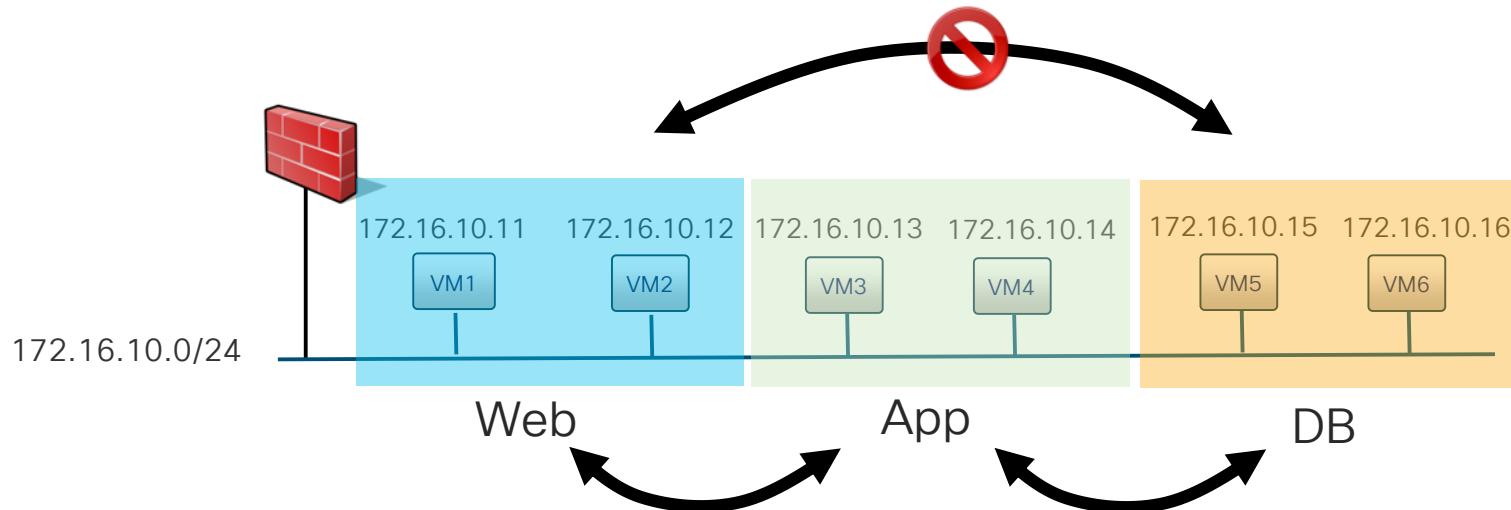
Security Risk: VMs or Servers on a Single Subnet



A Micro Segmentation Use Case



Another Micro Segmentation Use Case

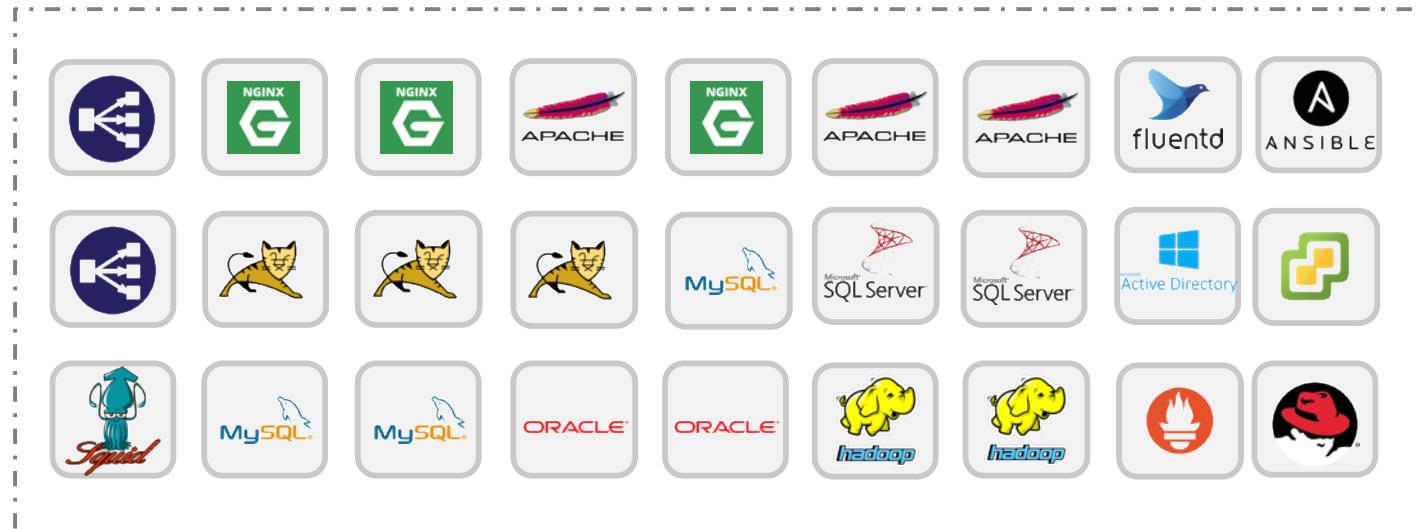


Micro Segmenting in an Heterogeneous Data Center

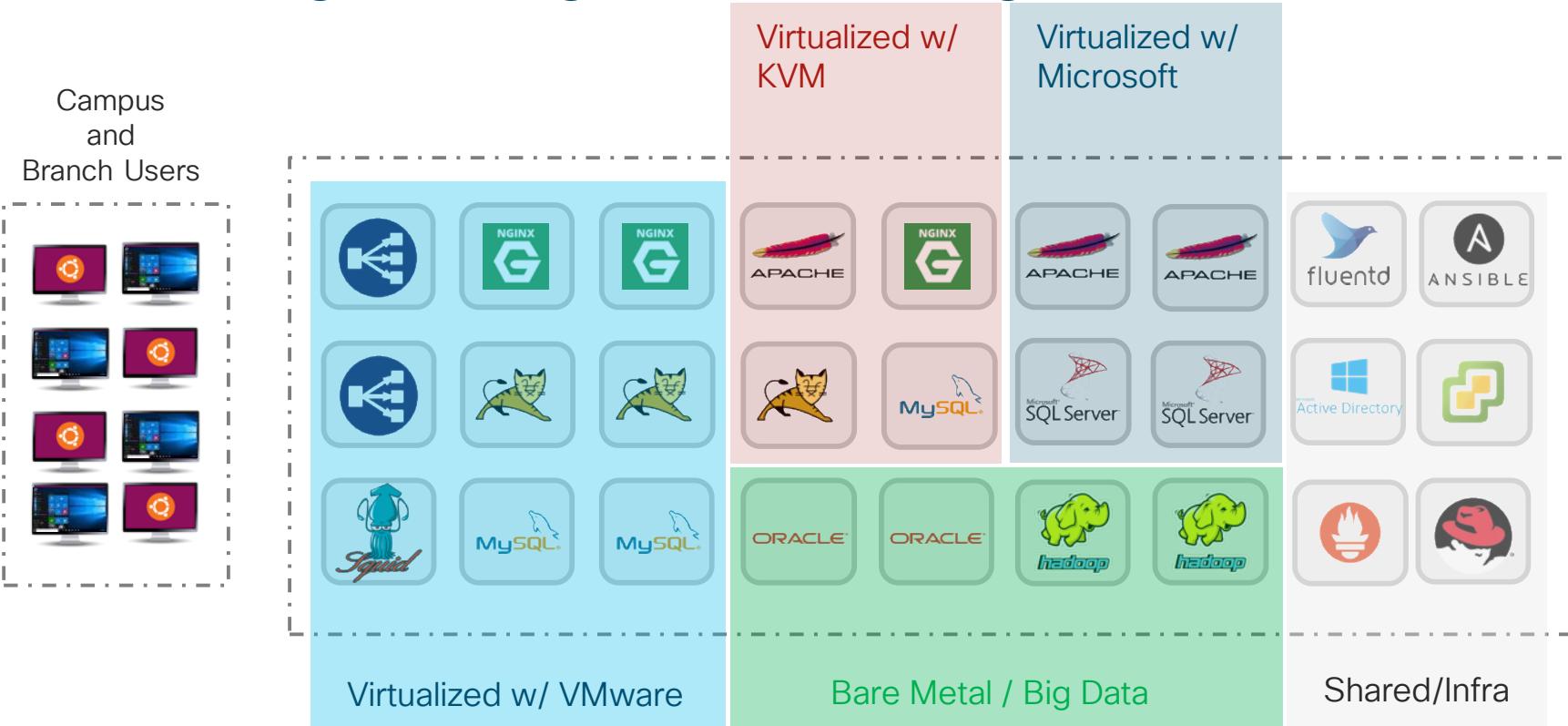
Campus
and
Branch Users



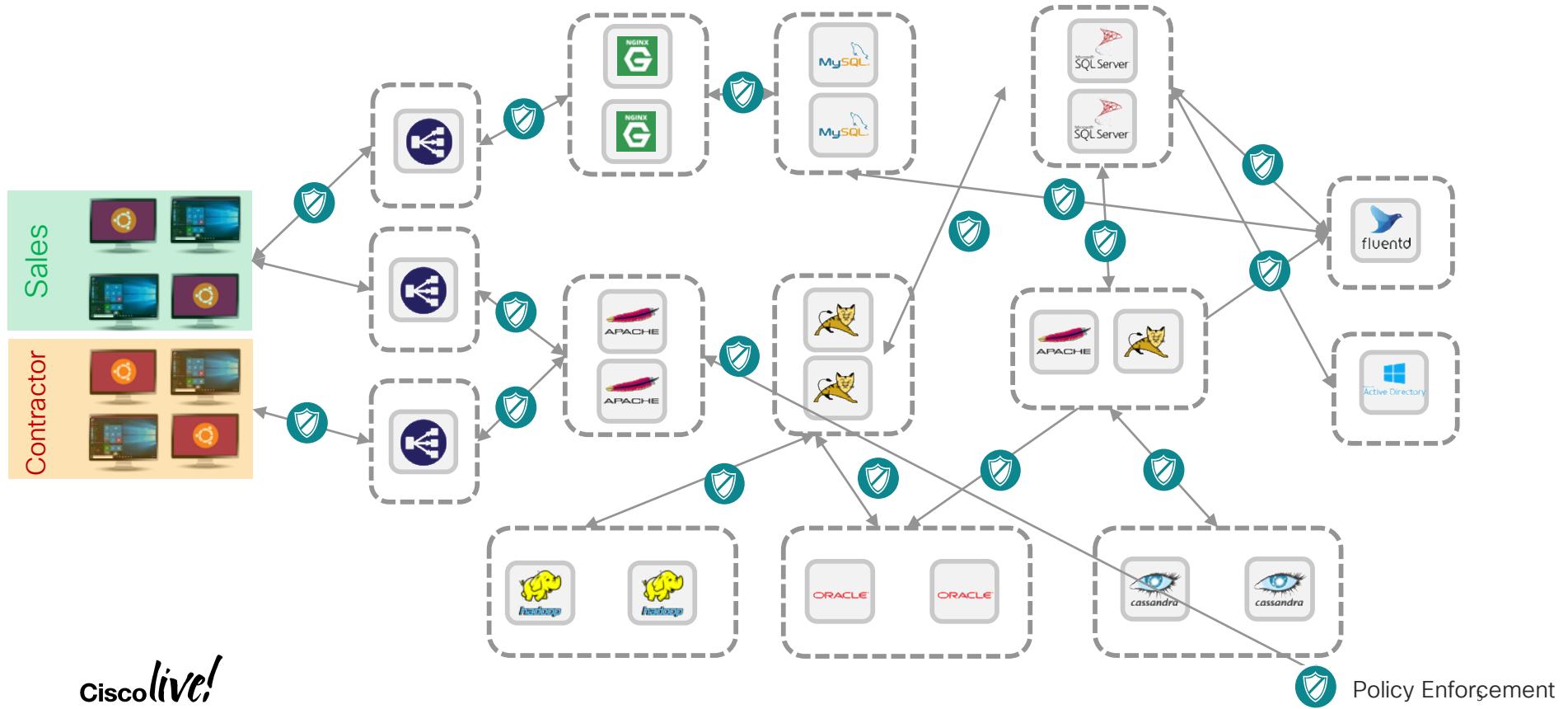
Many different types of workloads running in a Data Center



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

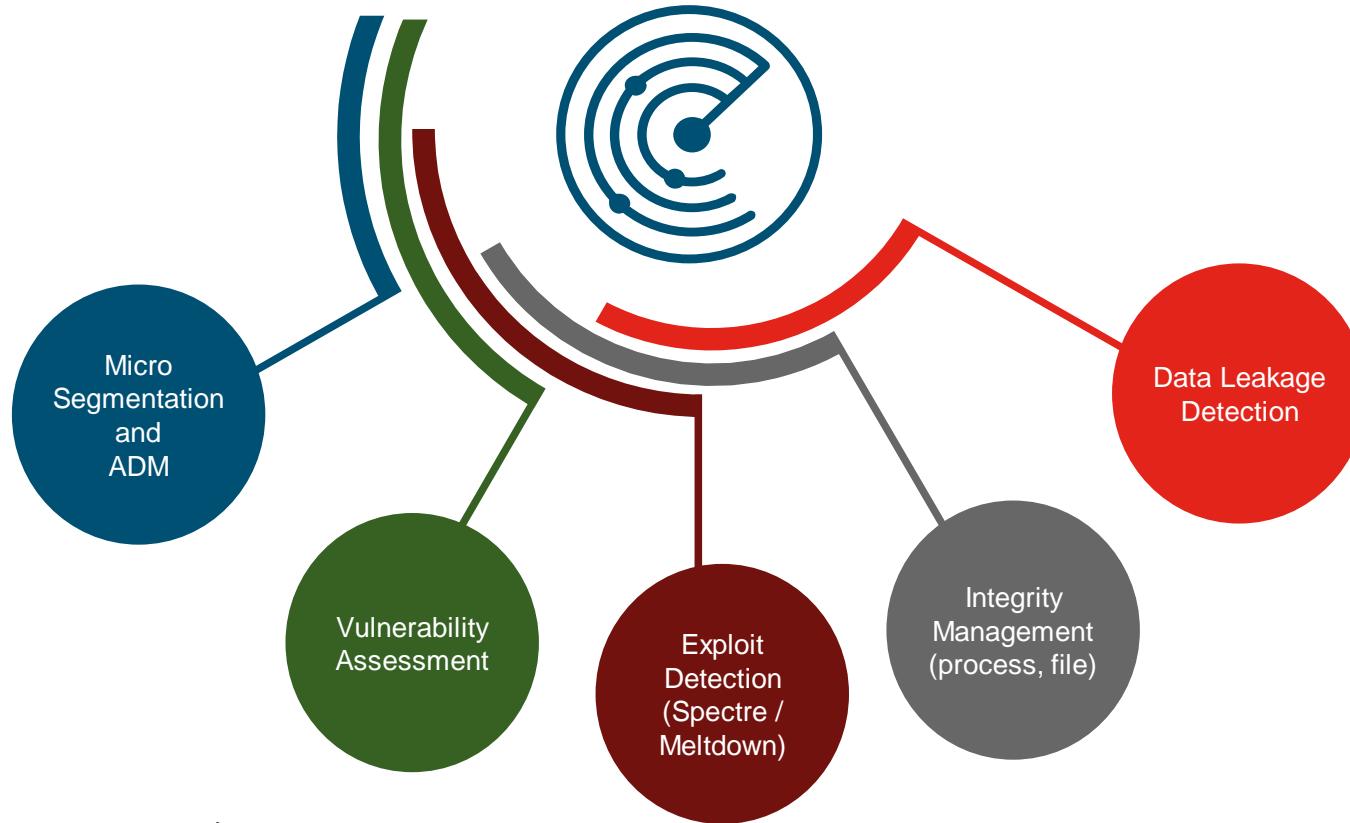
Host-based - Centrally manage host-based firewalls

- 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

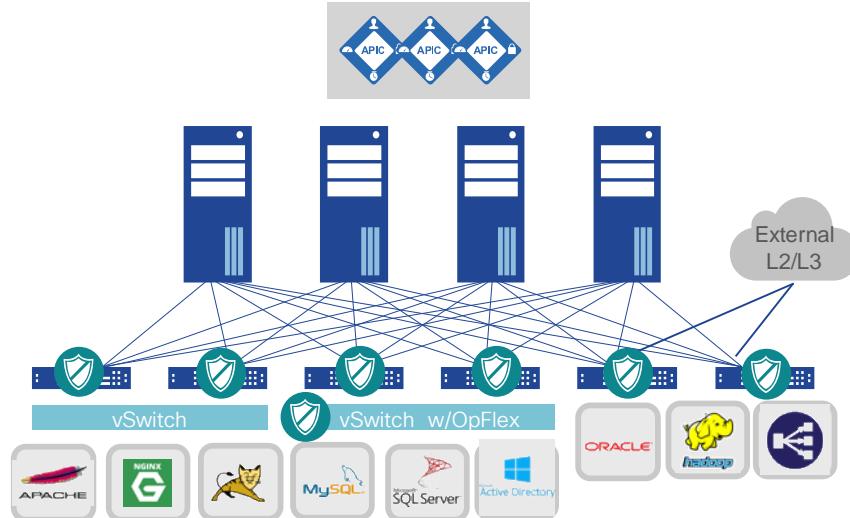
Cisco Tetration – cloud workload protection



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

ACI implements distributed network policies

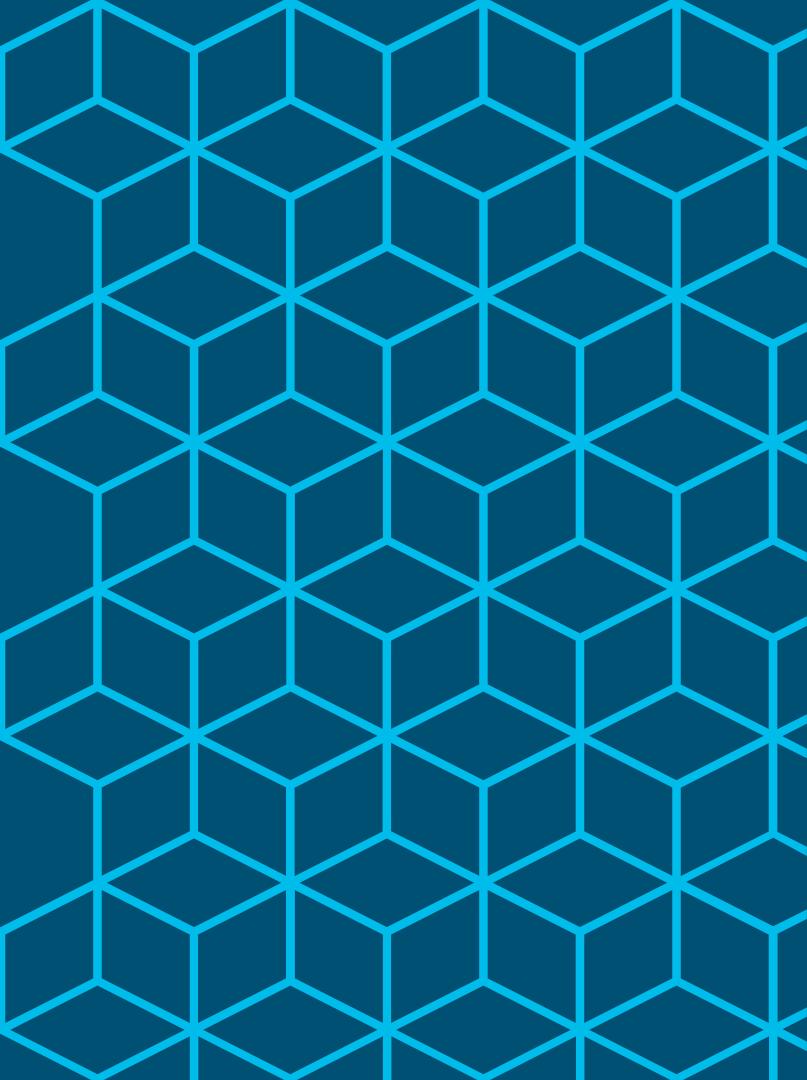
- Contracts define Layer2-Layer4 security policies.
- ACI distributed security policies are implemented at different enforcement points:
 - Leaf: hardware based, no performance penalty.
 - vSwitch (i.e. OVS, AVE): closest to VM, stateful connection tracking



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



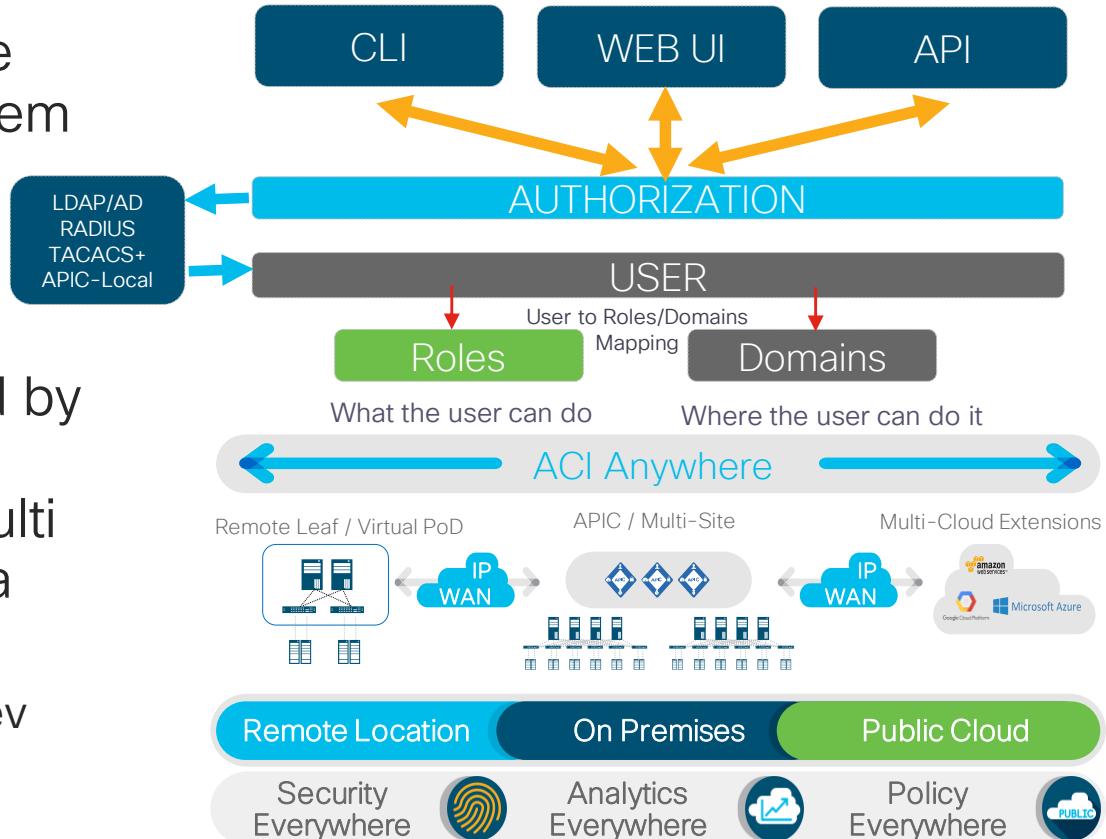
ACI Configuration Management

- 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

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin (which is selected), Operations, and Apps. Below the navigation is a secondary menu with links for AAA, Schedulers, Historical Record Policies, Firmware, External Data Collectors, Config Rollbacks, Import/Export, and Downloads.

The main content area is titled "User Management - Security". On the left, there's a sidebar under the "AAA" heading with options for Quick Start, Users, Authentication, and Security (which is currently selected). The main pane displays a table titled "Roles" with the following data:

Name	Privileges	Description
Sec	aaa access-connectivity-i1 access-connectivity-i2 access-connectivity-i3 access-connectivity-mgmt access-connectivity-util access-equipment access-protocol-i1 access-protocol-i2 access-protocol-i3 access-protocol-mgmt access-protocol-ops access-protocol-util access-qos fabric-connectivity-i1 fabric-connectivity-i2 fabric-connectivity-i3 fabric-connectivity-mgmt fabric-connectivity-util fabric-equipment fabric-protocol-i1 fabric-protocol-i2	

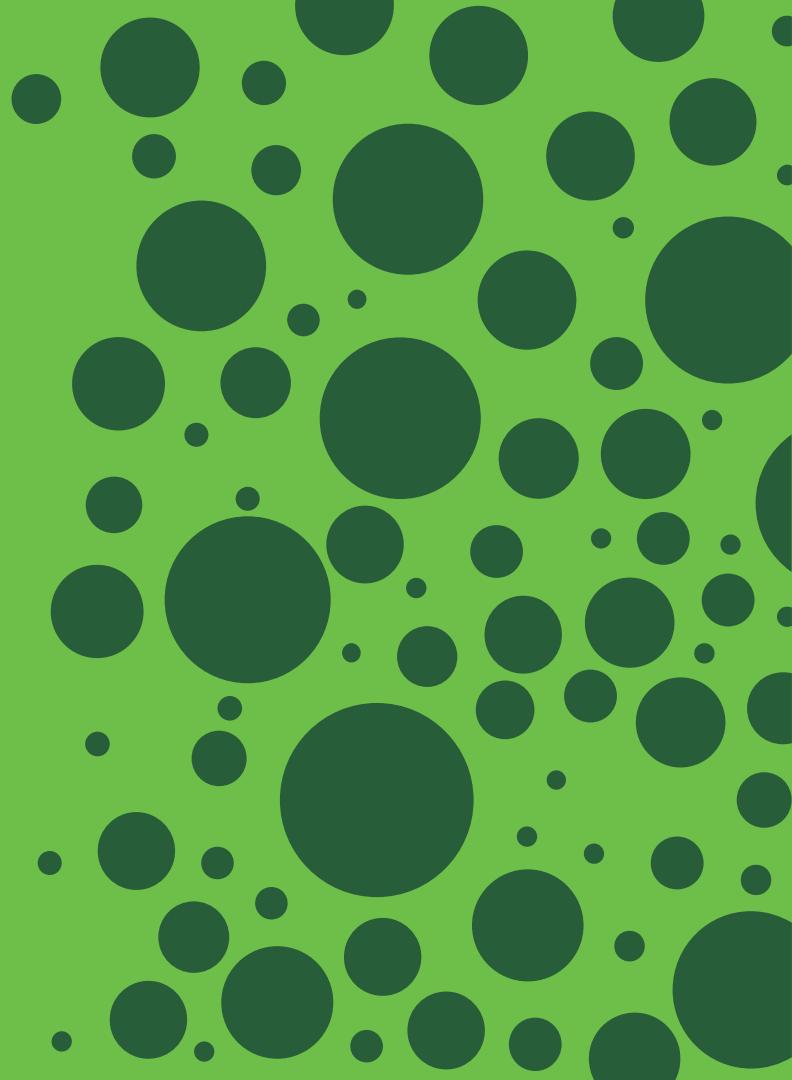
At the bottom of the table, there are navigation controls for Page 1 of 1, objects per page (15), and a message indicating 13 objects displayed.

ACI RBAC Roles are very granular

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface for the 'ACI-East-1' cluster. The left sidebar navigation includes 'System', 'Tenants', 'Fabric', 'Virtual', 'AAA' (selected), 'Users', 'Authentication', and 'Security'. The main content area is titled 'Create Role' with the sub-instruction 'Specify the Role Identity and Privilege Mask'. It features fields for 'Name' (with a red border and an exclamation mark icon) and 'Description' (labeled 'optional'). A table lists 'Privileges' under 'Selected' and 'Privilege' columns. The 'tenant-security' privilege is selected, highlighted with a blue background. Other privileges listed include tenant-qos, tenant-network-profile, tenant-epg, tenant-connectivity-l1, tenant-connectivity-l2, tenant-connectivity-l3, tenant-connectivity-mgmt, tenant-connectivity-util, tenant-protocol-l1, and tenant-protocol-l2. At the bottom are 'Cancel' and 'Submit' buttons, and a footer note 'Displaying Objects 1 - 13 Of 13'.

Privileges:	Selected	Privilege
	<input type="checkbox"/>	tenant-qos
	<input checked="" type="checkbox"/>	tenant-security
	<input type="checkbox"/>	tenant-network-profile
	<input type="checkbox"/>	tenant-epg
	<input type="checkbox"/>	tenant-connectivity-l1
	<input type="checkbox"/>	tenant-connectivity-l2
	<input type="checkbox"/>	tenant-connectivity-l3
	<input type="checkbox"/>	tenant-connectivity-mgmt
	<input type="checkbox"/>	tenant-connectivity-util
	<input type="checkbox"/>	tenant-protocol-l1
	<input type="checkbox"/>	tenant-protocol-l2

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.

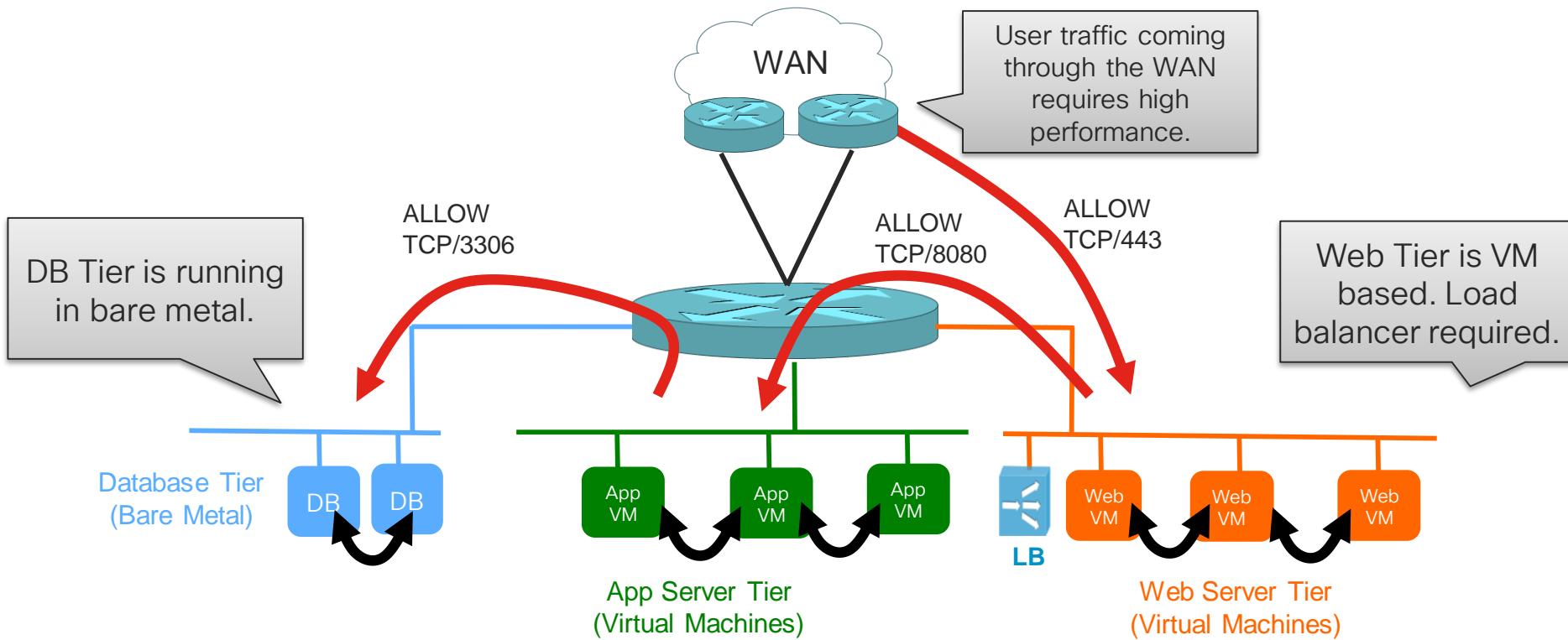
To allow EPGs to speak with each other we connect them using **contracts**

ACI uses a “white list model.”

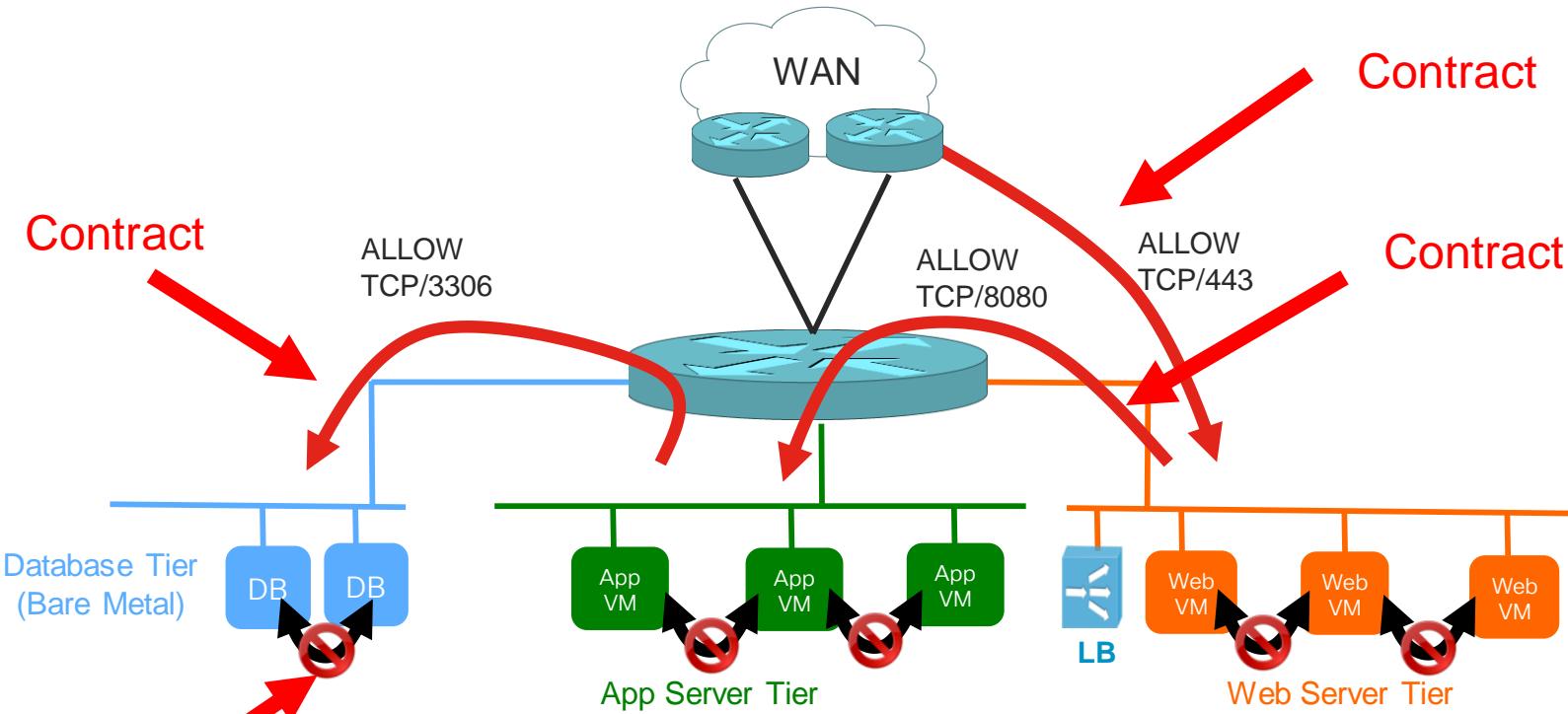
Remember...that's the default behavior. It can be changed.

Now let's talk about contracts.

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



Contracts



uSegmentation
For Physical and Virtual

A contract can use a Service Graph

Understanding Fabric Domains

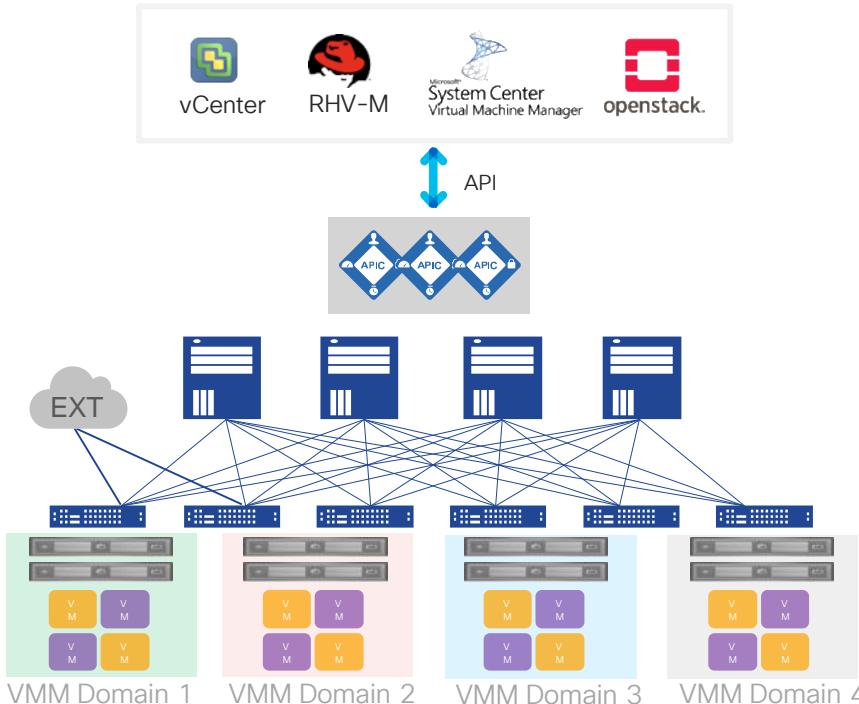
Fabric Domains represent the connectivity type for a physical port:

- 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.)

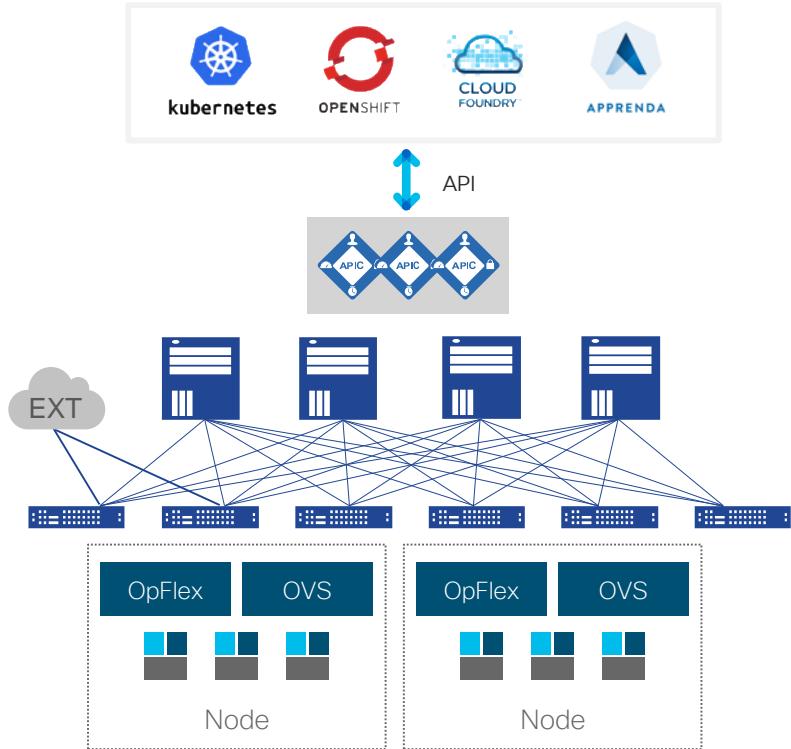
- Fabric domains also help APIC manage the allocation of certain resources for different types of endpoints:
 - Encapsulation pools: VLAN and VXLAN
 - Address pools: IP Multicast address pools
 - Security Domains
- Ports associate to the Domains via **Attachable Entity Profile (AEP)**

Virtual Machine Manager (VMM) Domains for Hypervisor Integration



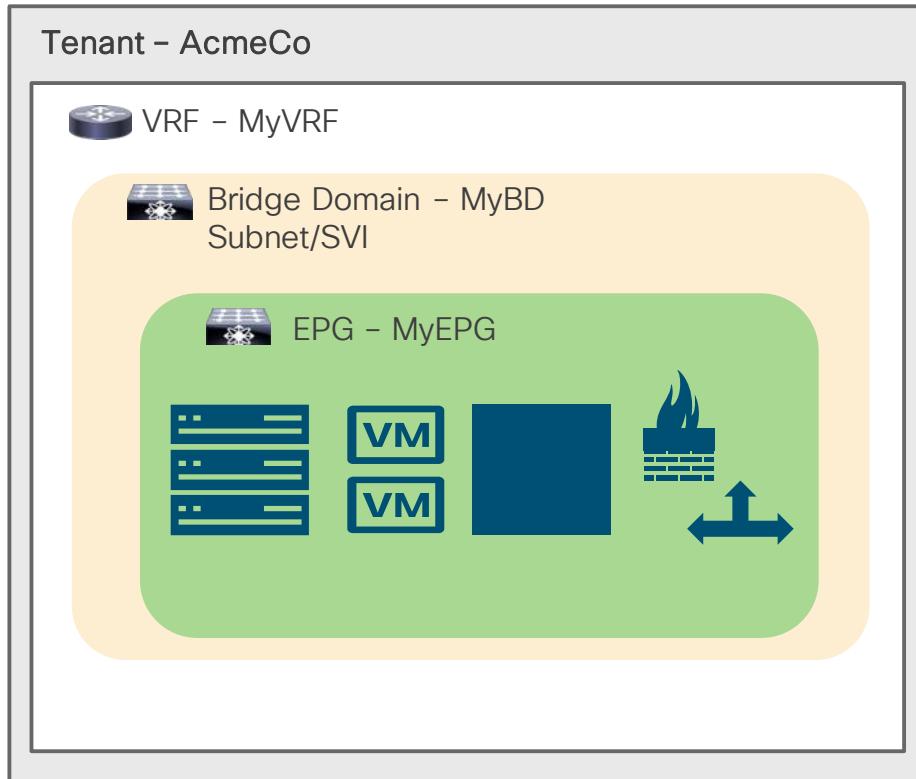
- API Relationship is formed between APIC and Virtual Machine Manager (VMM)
- APIC obtains virtualization inventory, performs virtual and physical correlation
 - APIC has visibility of hypervisor hosts, Virtual Machines, vNICs and more.
- APIC manages the hypervisor virtual switch (VDS, OVS, AVE, etc ...) 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

The ACI Network and Policy Model in one slide



L2 External EPG \approx 802.1q Trunk

L3 External EPG \approx L3 Routed Link

Three approaches to using EPGs in ACI

EPG/BD = VLAN

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.

EPG = App Tier

Create one EPG for each application Tier.

Flat-network design, many apps can share a single BD.

Fantastic for GreenField and automated deployments.

Hybrid (Combination)

New Apps and Legacy Apps share the same Fabric.

Tenant and VRF sharing.

or

Dedicated Tenant/VRF and leaking.

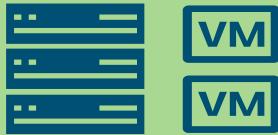
A common network-centric example with BD/EPG = VLAN

Tenant – AcmeCo

VRF – MyVRF

Bridge Domain – VLAN40
10.40.40.254/24

EPG – VLAN40



Bridge Domain – VLAN50
10.50.50.254/24

EPG – VLAN50



Bridge Domain – VLAN60
10.60.60.254/24

EPG – VLAN60

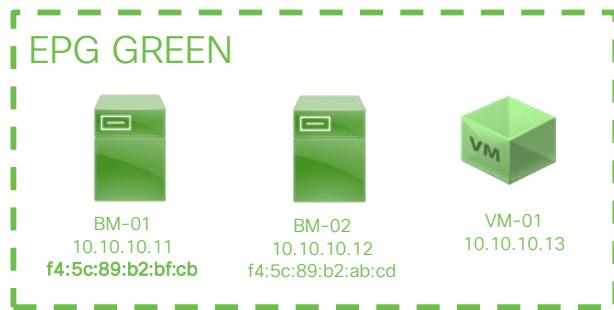


Micro EPGs allow the fabric administrator to **group endpoints based on their attributes**.

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**”

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



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.
Example:
Select MAC=f4:5c:89:b2:bf:cb

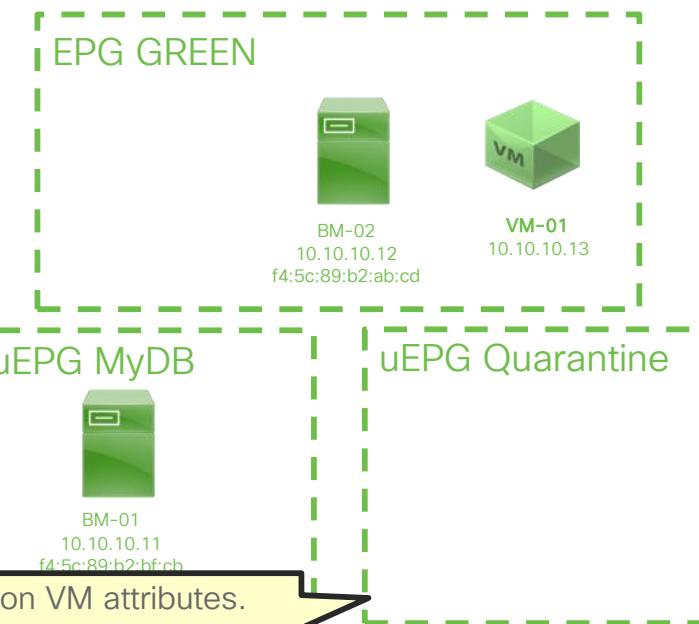
Base EPG based on port and encapsulation (i.e VLAN or VXLAN)



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 VM attributes.
Example:
VM-name=VM-01



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 on 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]



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

Domain Type	Domain Profile	Deployment Immediacy	Resolution Immediacy	State	Primary Encap	Port Encap	Switching Mode	Encap Mode	Netflow	Netflow Direction	EPG Cos	Cos Value
Physical Domain	phys			formed			Auto	disabled	both	disabled	Cos0	

2. Map the uEPG to the required leaf switches

Node	Deployment Immediacy
Node-105 (troy-leaf3)	Immediate
Node-106 (troy-leaf4)	Immediate

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



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

The screenshot shows the 'uSeg Attributes' configuration page. On the left, a navigation tree under 'Tenant AcmeTenant' shows 'Application EPGs' expanded, with 'uSeg EPGs' and 'BareMetal-DB' selected. A red box highlights this section. On the right, the 'uSeg Attributes' tab is active, showing a search bar with 'Match Any' dropdown set to 'IP', operator 'Equals' set to 'No', and value '10.50.50.200'. A red box highlights this search bar area.

4. Review the result

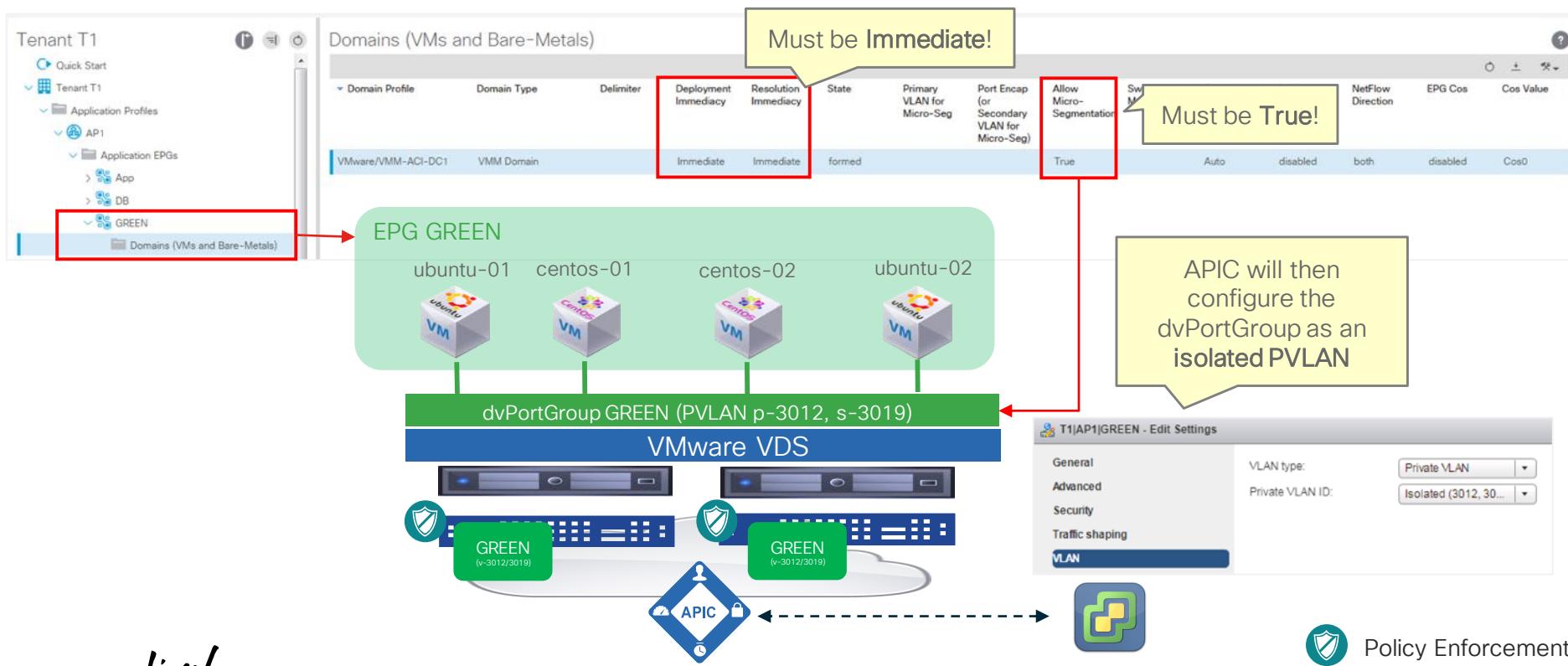
The screenshot shows the 'Operational' view for the 'BareMetal-DB' EPG. At the top, tabs include 'Summary', 'Policy', 'Operational' (which is selected), 'Stats', 'Health', 'Faults', and 'History'. Below, the 'Client End-Points' table is displayed. A red box highlights the 'IP' column for the first row. The table data is as follows:

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
EP-90:E2:BA:C3:31:3C	90:E2:BA:C3	10.50.50.200	learned	---	---	Pod-1/Node-105-106/cento...	---	vlan-1750

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



Micro EPG Support with vSphere VDS

1.1 Base EPG is working as normal EPG

EPG - GREEN

		Operational							
End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Configured Access Policies	Contracts	Controller End-Points
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)

EPG GREEN

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

Legend: GREEN (v-3012/3019)

APIC

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

The screenshot shows the Cisco ACI Controller interface for Tenant T1. On the left, under Application EPGs, a red box highlights the 'uSeg EPGs' section, which contains an entry for 'Ubuntu-VMs'. On the right, the 'Domains (VMs and Bare-Metals)' table lists a single row:

Domain Profile	Domain Type	Deployment Immediacy	Resolution Immediacy	State	Primary Encap	Port Encap	Switching Mode	Encap Mode	Netflow	Netflow Direction	EPG Cos	Cos Value
VMware/VMM-ACI-DC1	VMM Domain	Immediate	Immediate	formed			Auto	disabled	both	disabled	Cos0	

A yellow box with the text 'Must be Immediate!' is overlaid on the 'Resolution Immediacy' column header.

Micro EPG Support with vSphere VDS

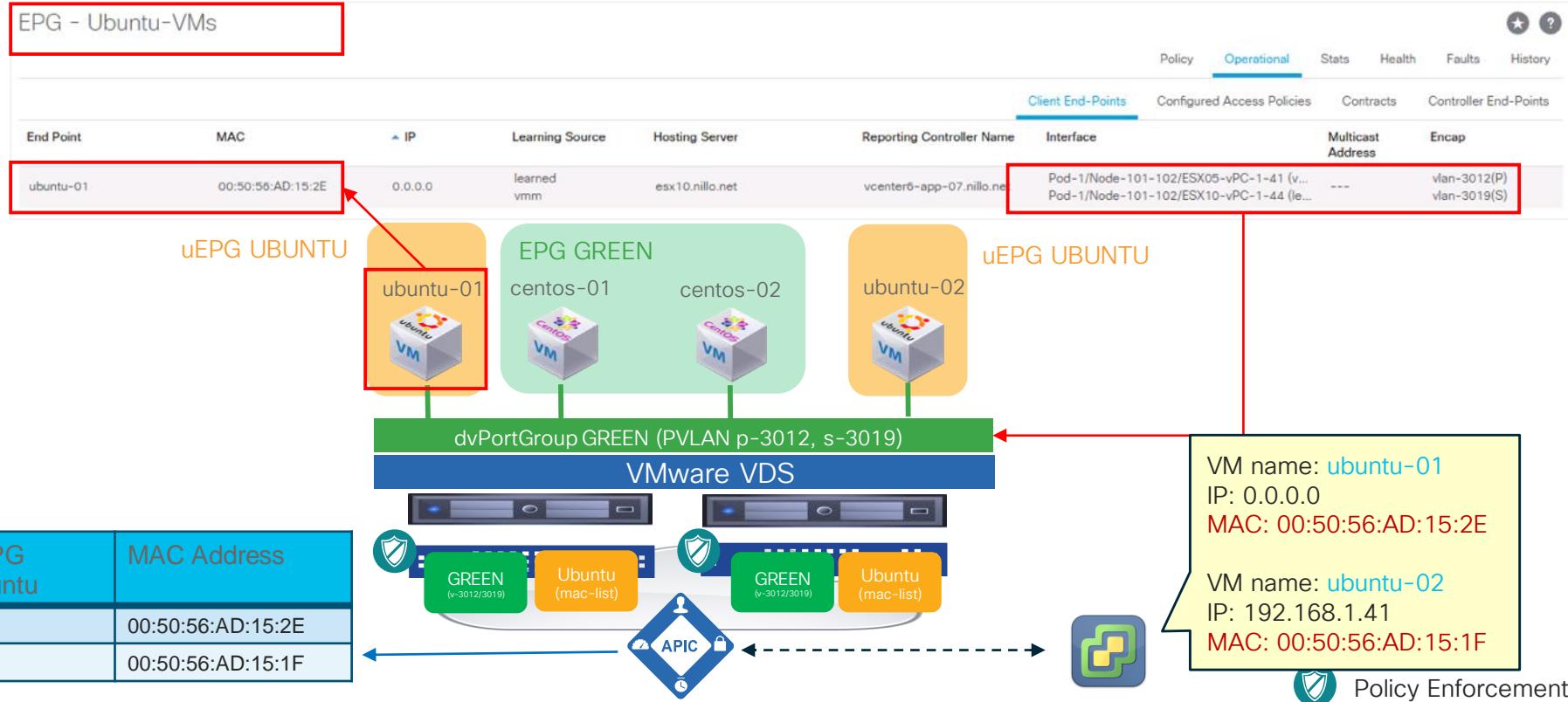
2. Configure uEPG based on attributes

2. Configure the required attributes

The screenshot shows the Cisco ACI Policy Manager interface. On the left, the navigation pane for Tenant T1 is visible, with 'uSeg Attributes' selected. The main pane is titled 'uSeg Attributes' and contains a search bar with the query 'VM - Operating System Equals Ubuntu Linux (64-bit)'. A red box highlights this search bar. A callout bubble points to the search bar with the text: 'We define attributes to match, in this example, matching on the VM Operating System (Ubuntu Linux)'. The top right of the interface has tabs for 'Policy' (which is selected) and 'History', along with other standard UI elements.

Micro EPG Support with vSphere VDS

3. VM is classified according to attributes



A quick demo of using VM attributes for uSEG

Micro EPG Support with vSphere VDS – Summary

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

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The URL is <https://172.26.36.77/#bTenants:Andy-Tenant-1/untn-Andy-Tenant-1/ap-Test-AP-1/>. The navigation bar includes links for Lab vCenter, Lab APIC, Lab Candid, Internal-Demo, MSC, and NSX-T. The main menu has tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. The current view is under the Tenants tab, showing the ALL TENANTS page with Tenant Search: `name or descr` and filters for common, **Andy-Tenant-1**, infra, Sec-Dom-2-Tenant, and Sec-Dom-1-Tenant.

The left sidebar shows the Tenant structure:

- Tenant Andy-Tenant-1
 - Application Profiles
 - Andy-Phy-AP-1
 - Andy-SG-Demo
 - ESXi-Kernel
 - PBR-Demo
 - Test-AP-1
 - Application EPGs
 - uSeg EPGs
 - TAG
 - Domains (VMs and Bare-Metals)
 - Static Leafs
 - Contracts
 - Static Endpoint
 - uSeg Attributes
 - Subnets
 - L4-L7 Virtual IPs
 - L4-L7 IP Address Pool

The "uSeg Attributes" section is selected in the sidebar. A modal dialog is open, titled "Match Any", showing a dropdown menu for "Select a type..." with the following options:

- IP
- MAC
- DNS Group (Beta)
- AD Group (Beta)
- VM - Custom Attribute
- VM - VMM Domain
- VM - Operating System
- VM - Hypervisor Identifier
- VM - Datacenter
- VM - VM Identifier
- VM - VM Name
- VM - VM Folder (Beta)
- VM - VNic Dn
- VM - Tag

At the bottom of the dialog are buttons for "Show Usage", "Reset", and "Submit".

At the bottom of the screen, status bars show "Last Login Time: 2018-11-15T17:45 UTC+00:00" and "Current System Time: 2018-11-15T17:49 UTC+00:00".

uEPGs with Attributes and Logical Operators

- GUI Configuration (1/2)

The screenshot shows the Cisco ACI GUI interface for Tenant AcmeInc. The left sidebar lists various application profiles, and a specific uSeg EPG named 'web-tier-DC1-East' is selected and highlighted with a red box. A yellow callout box points to this selection with the text: "Select new ‘uSeg Attributes’ folder under each specific uEPG". The main workspace displays two Match dropdown menus. The top one is set to "Match Any" and has a yellow callout box with the text: "Select ‘Match Any’ for ‘OR’ Logic.". The bottom one is set to "Match All" and has a yellow callout box with the text: "Select ‘Match All’ for ‘AND’ Logic.". Both dropdowns have a red border around them. To the right, a large circular callout highlights the '+' button in the toolbar, with the text: "Click on ‘+’ to add additional attributes to Match Any/All. Or click ’+(‘ to add additional sections." The top right corner of the slide shows a user interface snippet with "Policy" and "History" tabs.

Select “Match Any” for ‘OR’ Logic.

Select new “uSeg Attributes” folder under each specific uEPG

Match Any

Match All

VM - Tag APP Equals VM - Datacenter Equals DC1-EAST

VM - Datacenter Equals DC1-EAST

Match All

Click on ‘+’ to add additional attributes to Match Any/All. Or click ’+(‘ to add additional sections.

uEPGs with Attributes and Logical Operators

- GUI Configuration (2/2)

The screenshot shows the Cisco ACI GUI interface for Tenant AcmeInc. The left sidebar lists various tenant components like Application Profiles, uSeg EPGs, and Subnets. The main panel is titled "uSeg Attributes" and displays a configuration window with a red border around the logical operator section. This section contains two "Match All" conditions separated by a logical OR operator ("Match Any"). The first condition checks for "VM - Tag" equals "APP" and "Equals" "OpenCart-Apache". The second condition checks for "VM - Datacenter" equals "DC1-EAST". Below these, there is another "Match All" condition for "VM - Custom Attribute" equals "app-tier" equals "app1-app".

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

A grayscale photograph showing a dense stack of shipping containers. The containers are stacked in several layers, filling the frame. Some have markings like 'CAR' and 'DA' visible.

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

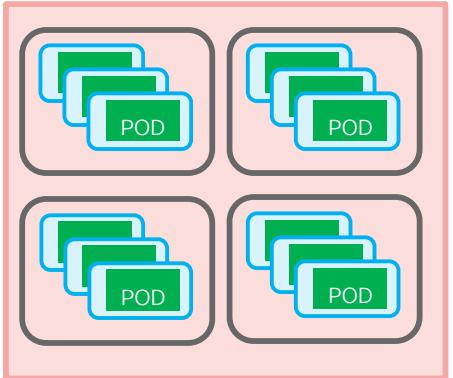
- Provide isolation beyond using Kubernetes Network Policies
- Opflex annotation can be applied at POD, Deployment or namespace level
- Priority of annotations goes from less specific to more specific
 1. Pod annotation
 2. Deployment annotation
 3. Namespace annotation
 4. Namespace group mapping from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

ACI allows flexible POD to EPG mapping

K8s
Network
Policy

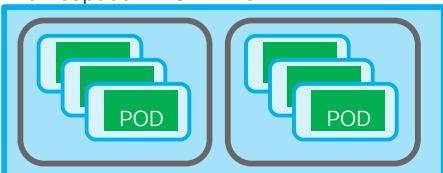
Cluster Isolation

Kube-default-EPG

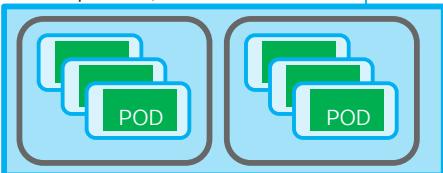


Namespace Isolation

namespace-PROD-EPG



namespace-QA-EPG



Deployment Isolation

Frontend-EPG



Backend-EPG



API-Gateway-EPG



Monitoring-EPG



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

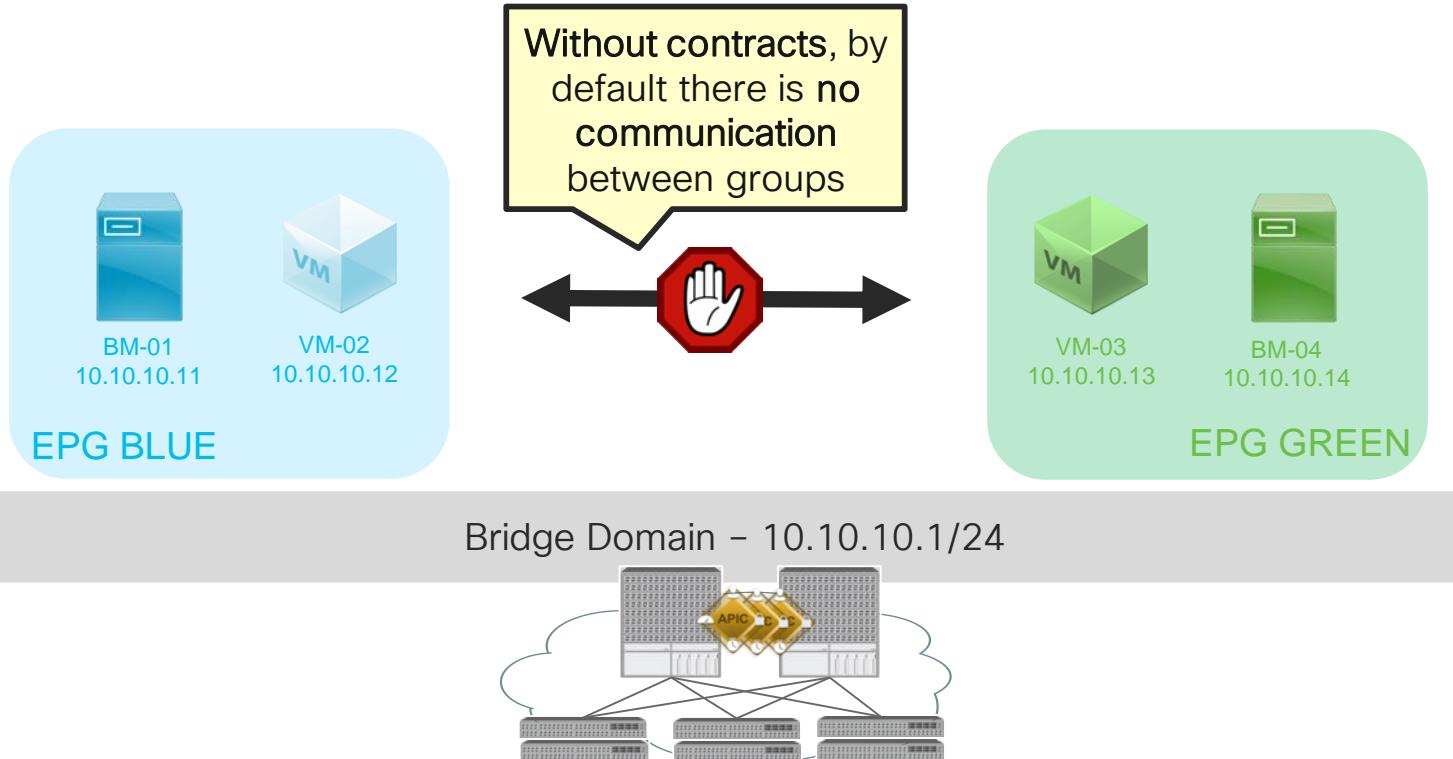
- Each namespace mapped to an EPG
- Contracts for inter-namespace traffic are required

- 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

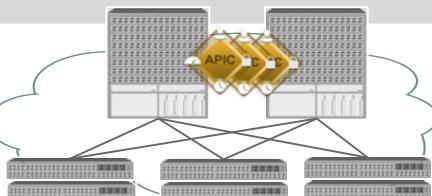


By default communication between EPGs is not allowed in absence of contracts



BLUE Consumes the contract,
so can connect to tcp/80 and
tcp/443

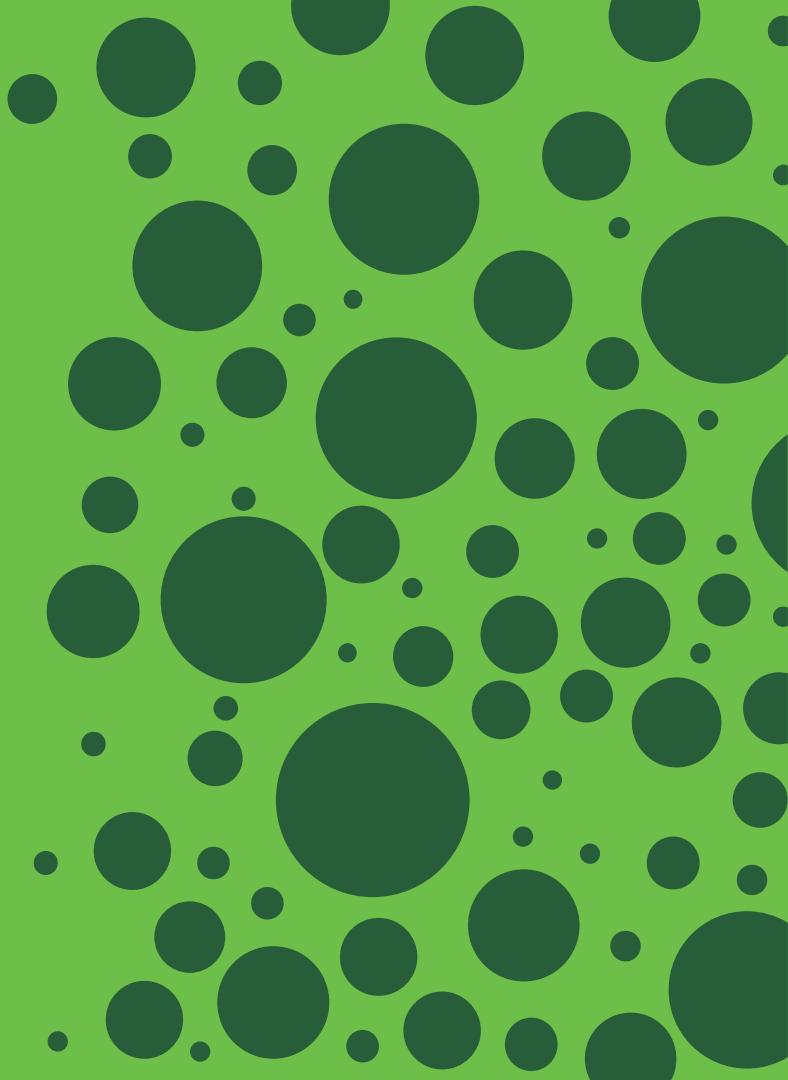
Bridge Domain - 10.10.10.1/24



GREEN Provides the contract,
so ports tcp/80 and tcp/443 are
exposed.

Demo: Creating a filter and contract

What about applying
policy within an EPG.



Denying all traffic between EPs in the same EPG is easy

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The top navigation bar includes the Cisco logo, the title "APIC (ACI-East-1)", and user authentication ("admin"). Below the title, there are tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. The "Tenants" tab is selected.

The main content area displays the "ALL TENANTS" view, with the "CL-Demo" tenant selected. A search bar at the top of the tenant list allows searching by name or description. Other visible tenants include "common", "Andy-Tenant-1", "infra", and "Sec-Dom-2-Tenant".

On the left, a sidebar shows the structure of the "CL-Demo" tenant, including "Application Profiles", "Application EPGs" (with "CL-Base-EPG" selected), and "uSeg EPGs".

The right panel shows the configuration for the "CL-Base-EPG". The "Policy" tab is selected. The "Properties" section contains the following settings:

- Custom QoS: Select a value
- Data-Plane Policer: Select a value
- Intra EPG Isolation: Enforced (highlighted with a red box)
- Preferred Group Member: Exclude
- Flood on Encapsulation: Disabled

Below these, the "Configuration Status" is listed as "applied". The "Label Match Criteria" is set to "AtleastOne", and the "Bridge Domain" is set to "Web-App-DB-BD". The "Resolved Bridge Domain" is shown as "CL-Demo/Web-App-DB-BD".

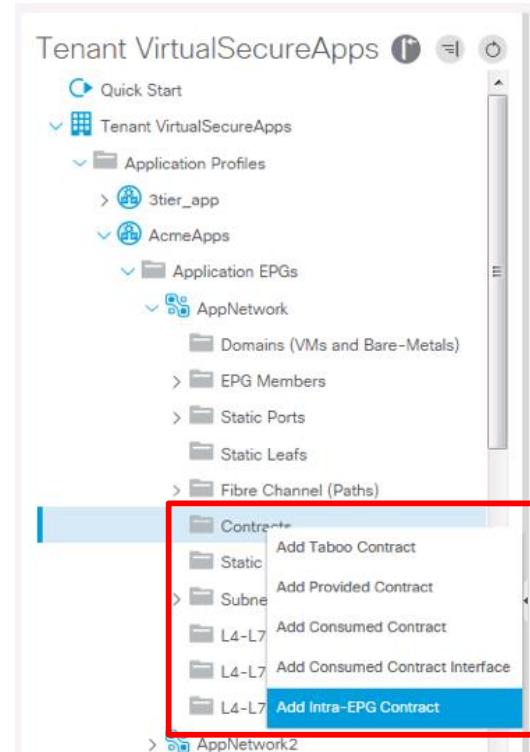
At the bottom of the right panel are three buttons: "Show Usage", "Reset", and "Submit".

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)

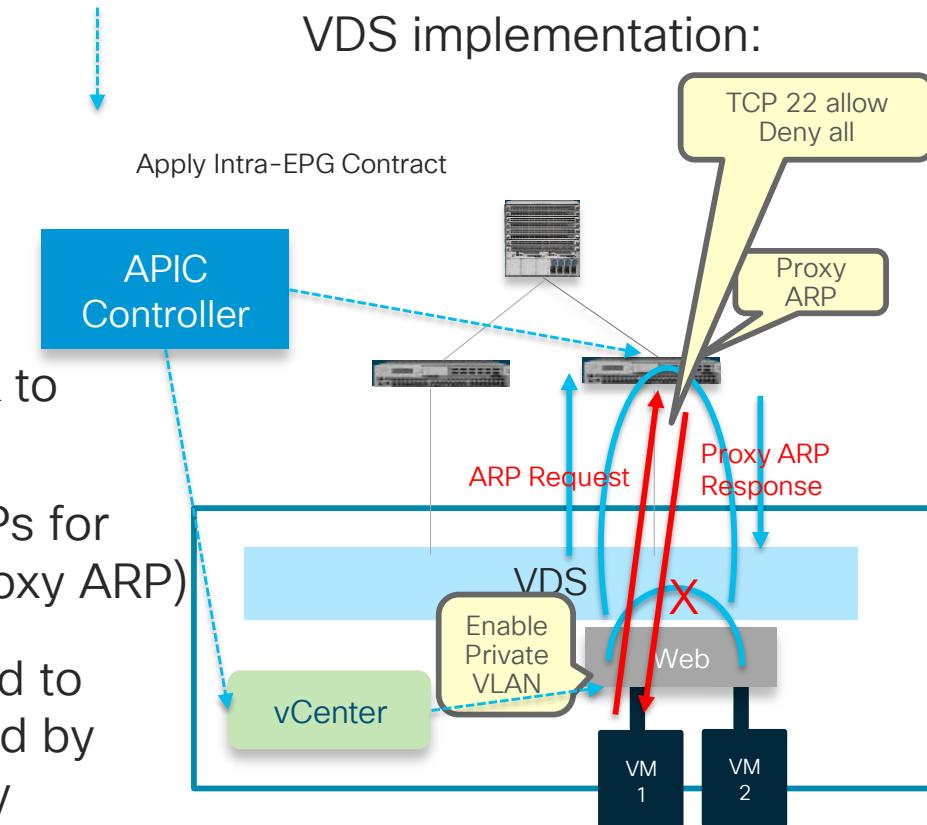
- It is possible to assign contracts to restrict traffic internal to an EPG
- It can be enabled on both EPG and uEPG
- It supported with PhysDoms and VMware VMM Domains
- IntraEPG contracts require using proxy-arp. This means it is only supported on EX/FX switches or newer.



Intra EPG Security Feature Overview

How does it work for 2 VMs on the same ESXi Host?

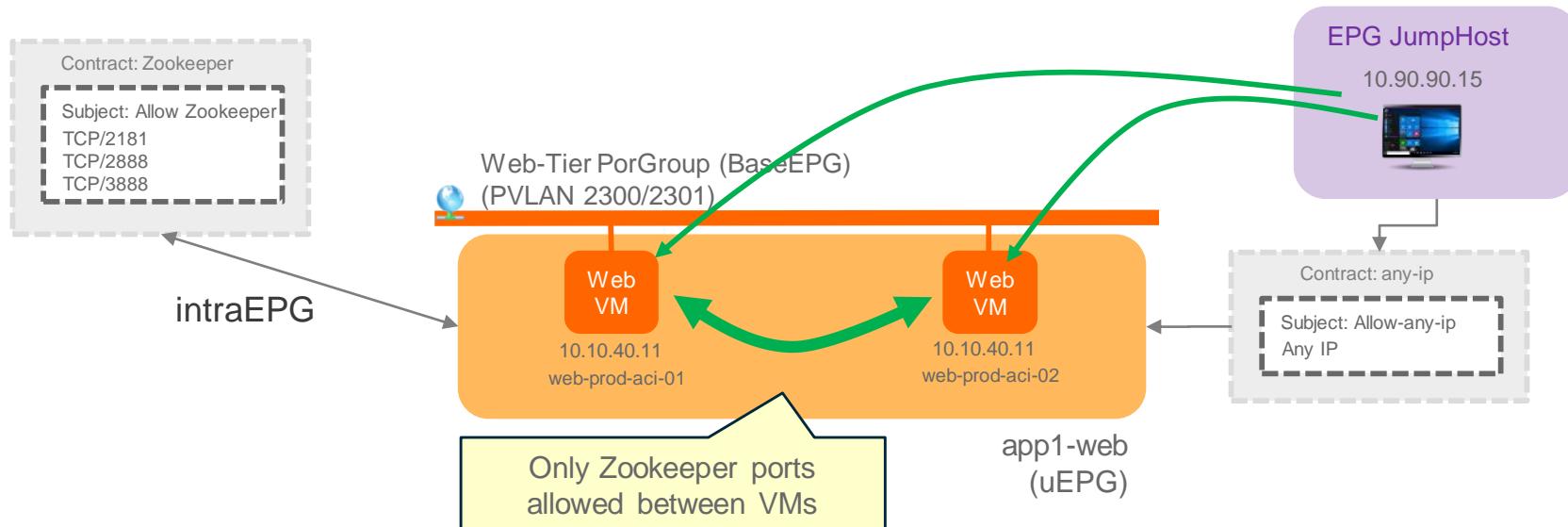
- 1- We enable Intra-EPG Security
- 2- APIC configures a PVLAN for the EPG/portgroup on vCenter with the TOR setup as the promiscuous port
- 3- The VMs in the portgroup can only talk to the TOR
- 4- When VM1 wants to talk to VM2 it ARPs for it and the TOR responds with its MAC (proxy ARP)
- 5- All the traffic between the VMs is pulled to the TOR which allows only traffic permitted by the contract applied for Intra-EPG security



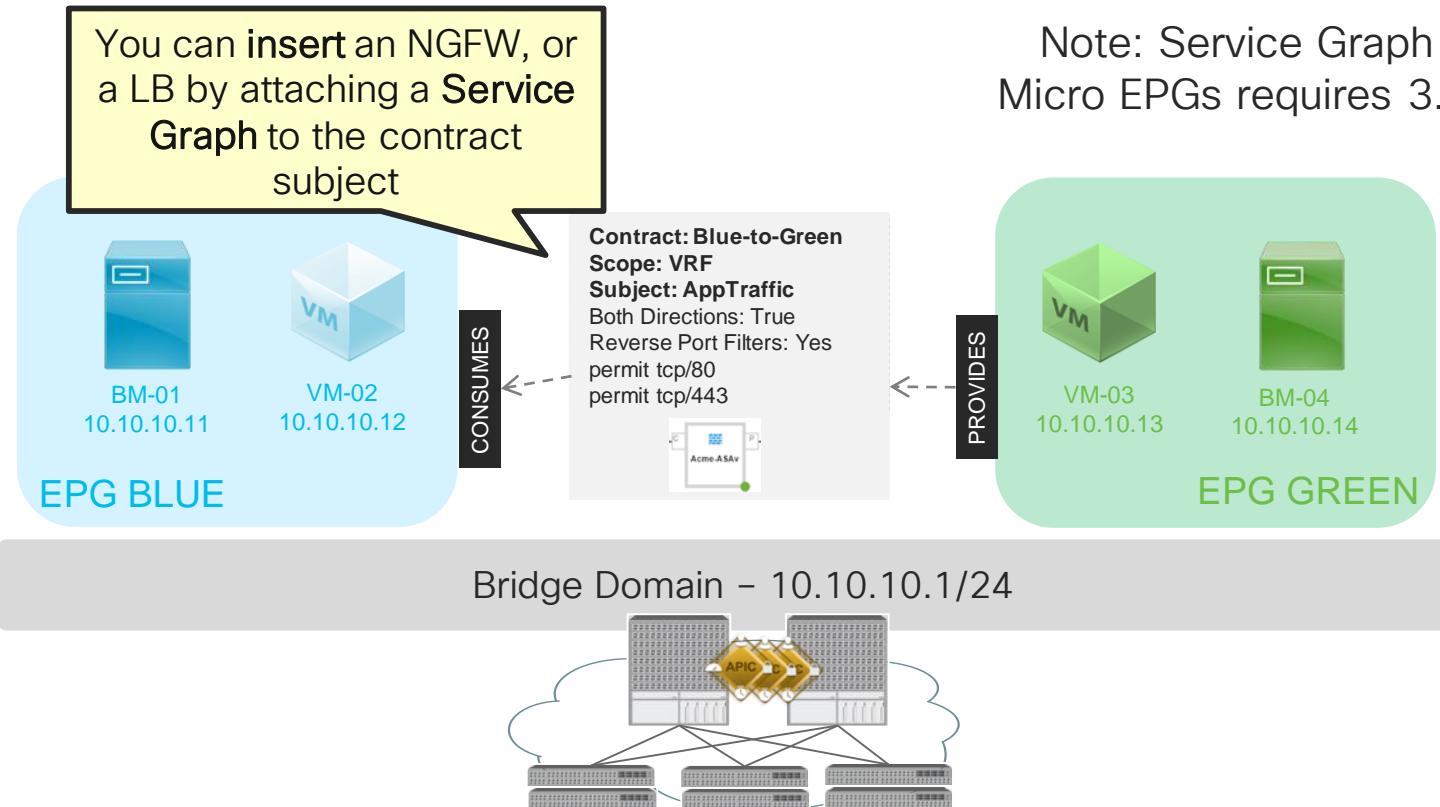
IntraEPG Contract Use Case

- 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.



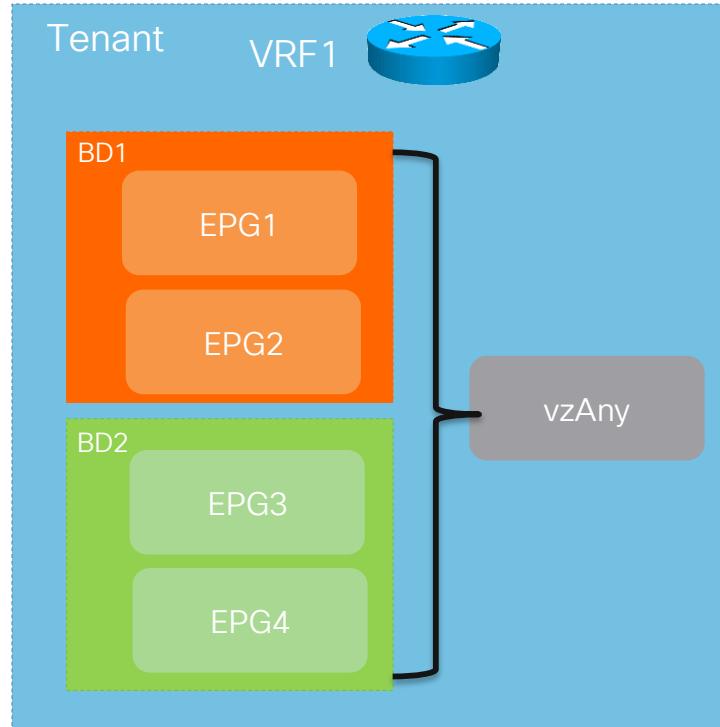
Contracts also allow inserting services, like Next Generation Firewalls, ADC, IPS/IDS, etc.



Note: Service Graph between Micro EPGs requires 3.2 or higher

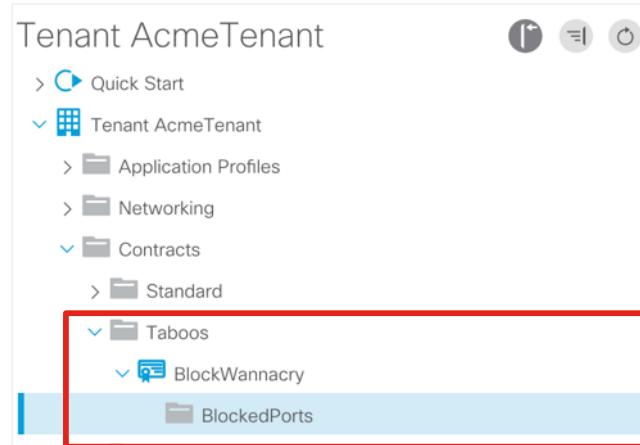
vzAny allows you to configure contracts that apply for all EPG in a VRF

- 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.

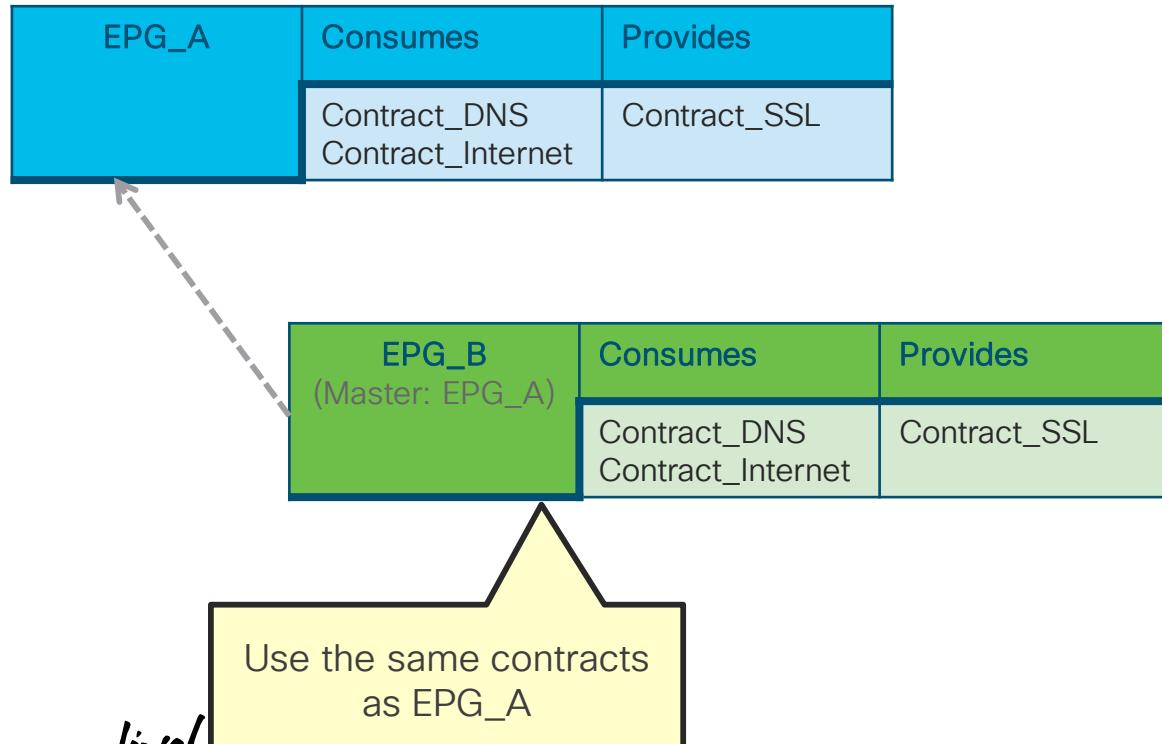
Simplifying Contract Configurations with EPG Contract Inheritance

- 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

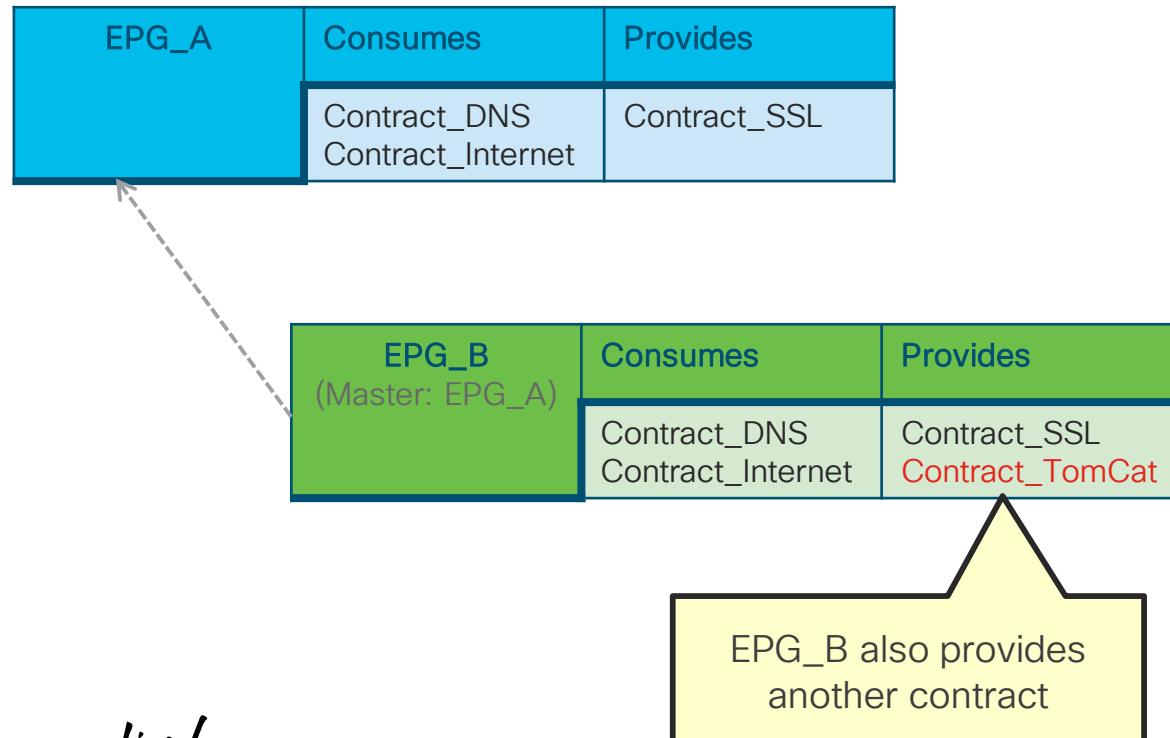
EPG_A	Consumes	Provides
	Contract_DNS Contract_Internet	Contract_SSL

EPG_B is configured to inherit from EPG_A

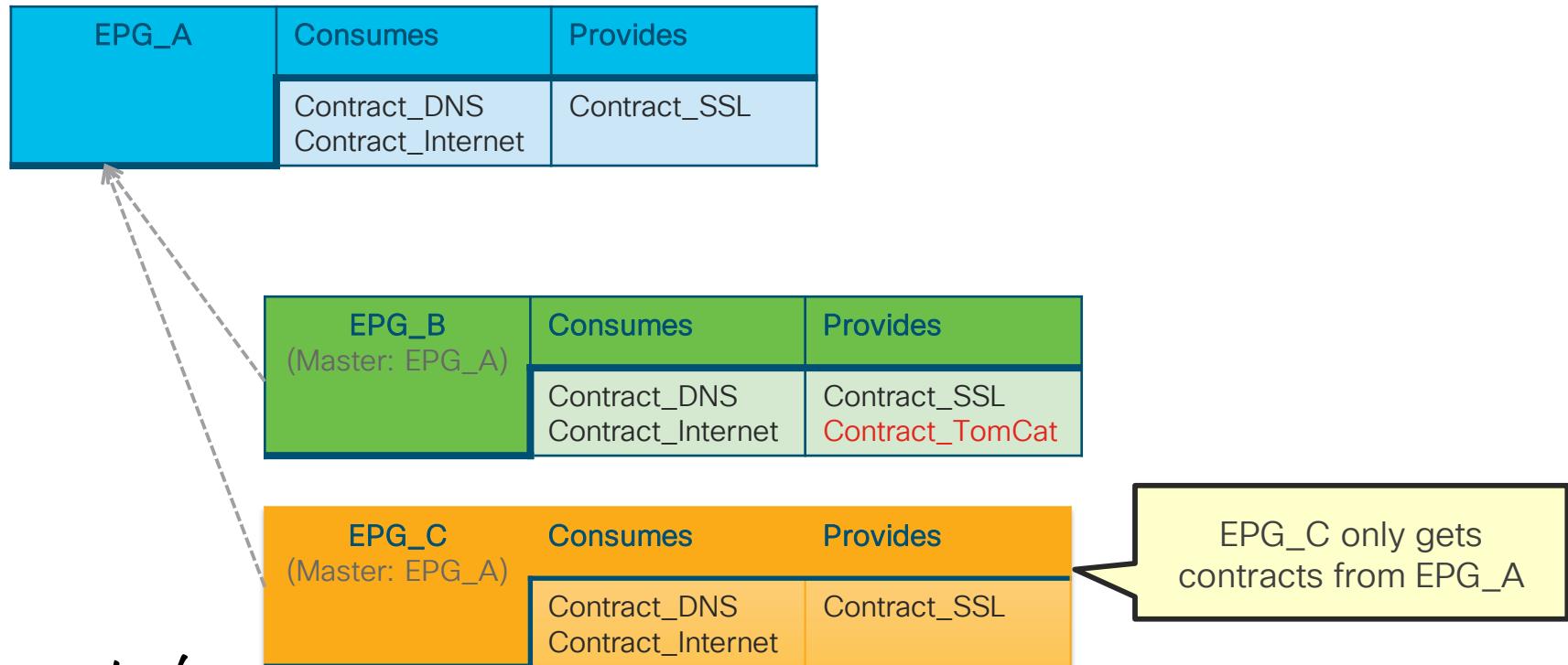


EPG_B is configured to inherit from EPG_A

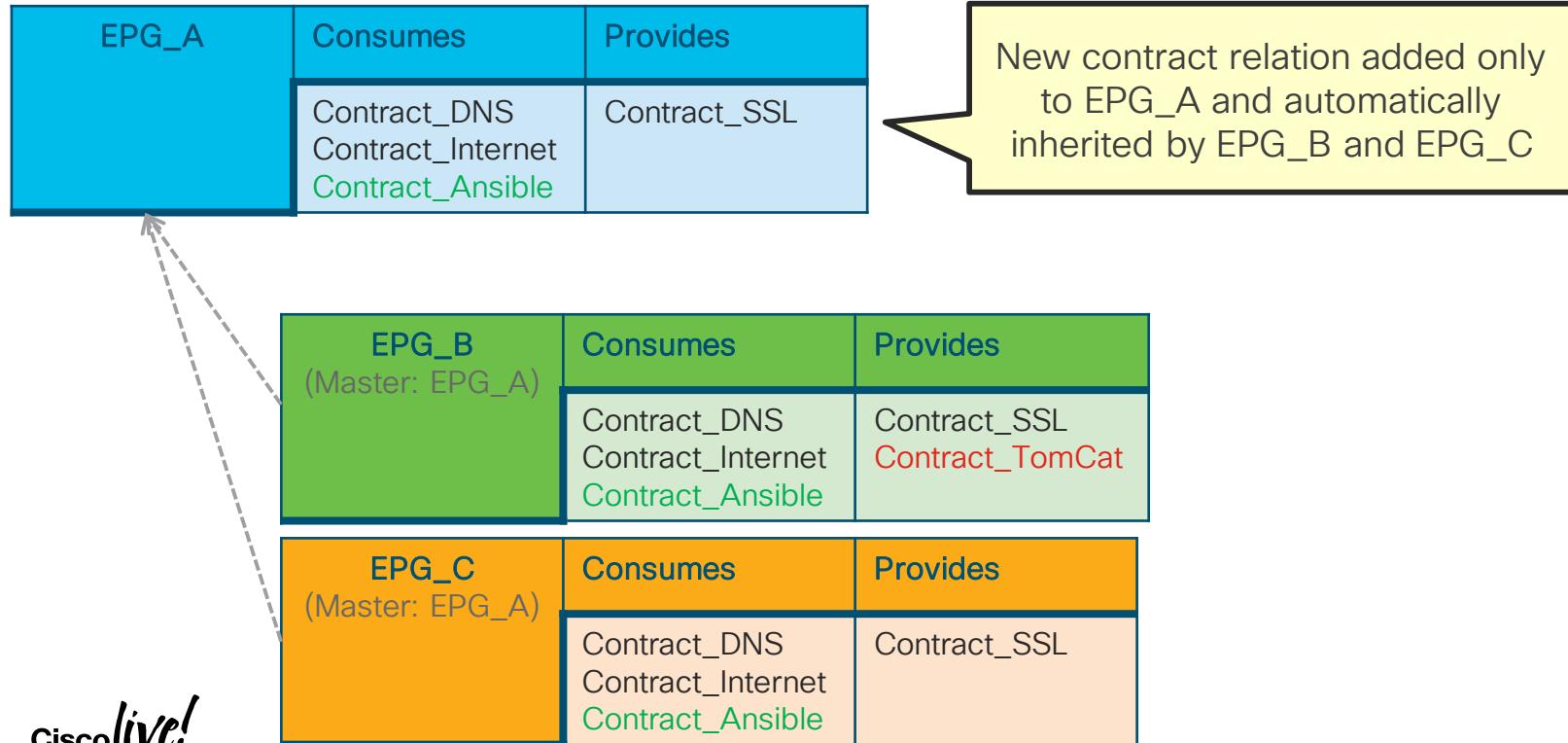
- can now add specific contracts to “child”



EPG_C is configured to inherit from EPG_A



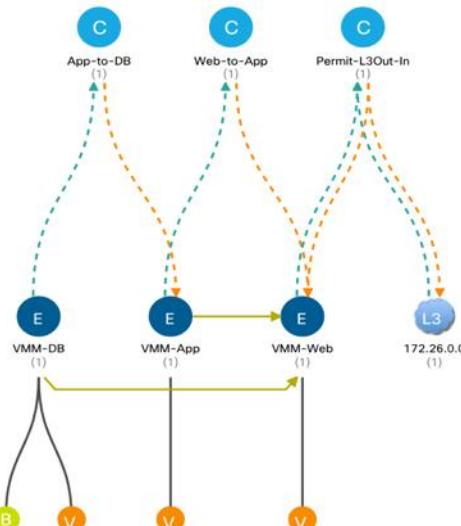
Changes to contract relations on EPG_A are inherited by EPG_B and EPG_C



Adding Contract Inheritance

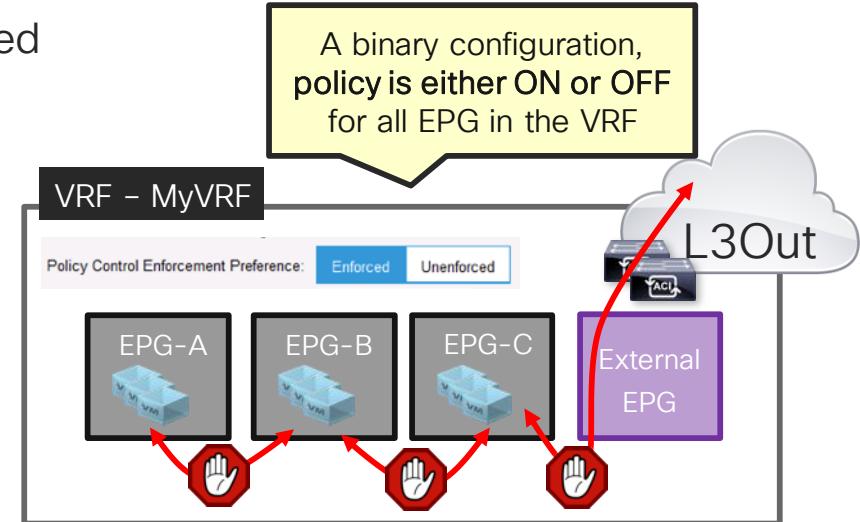
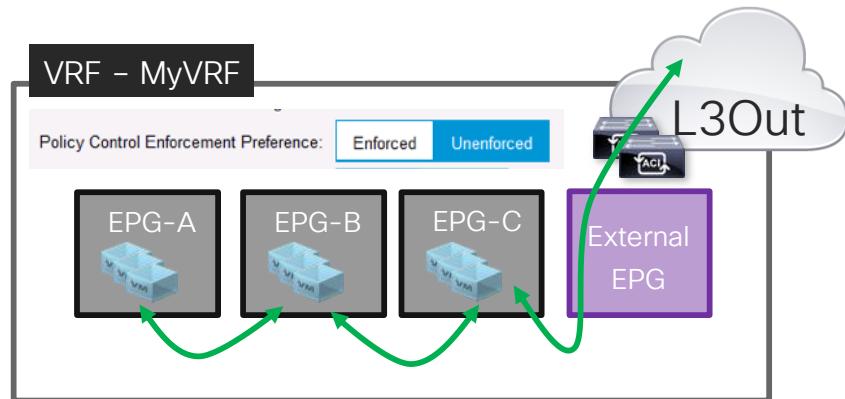
Application Profile - Test-AP-1

Summary Topology Policy Sta



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

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The top navigation bar includes the Cisco logo, the title "APIC (ACI-East-1)", and user authentication ("admin"). Below the title, there are tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. The "Tenants" tab is selected.

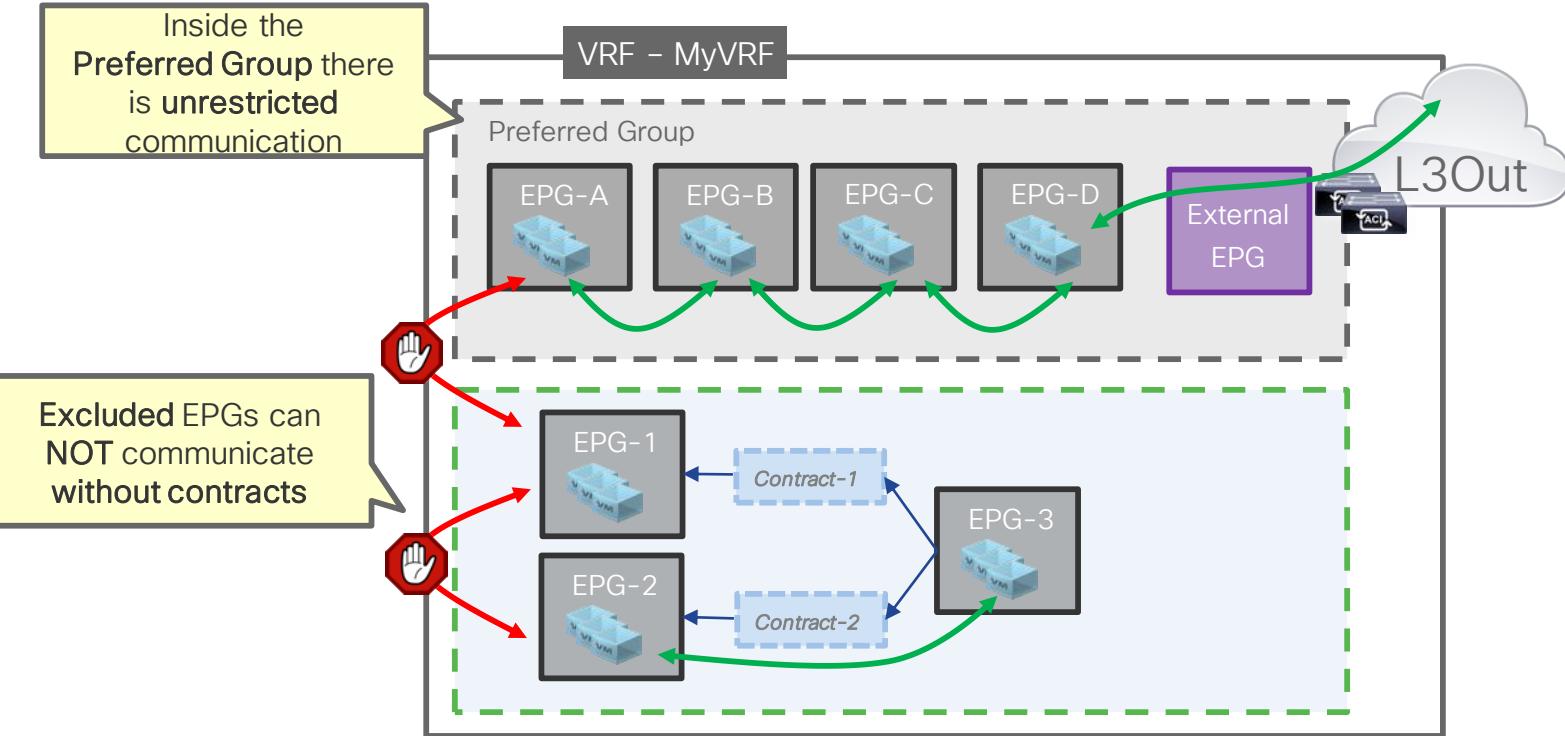
The main content area displays the "Tenant Andy-Tenant-1" configuration. On the left, a sidebar lists tenant components: Application Profiles, Networking (Bridge Domains, VRFs), Contracts, Policies, and Services. Under "Networking", "VRFs" is expanded, and "Andy-VRF-1" is selected, highlighted with a blue background.

The right panel shows the "VRF - Andy-VRF-1" configuration page. The "Policy" tab is active. At the top, there is a summary section with a green button labeled "100" and several status icons. Below this is the "Properties" section, which includes fields for Name (Andy-VRF-1), Alias, Description (optional), Tags (with a placeholder "enter tags separated by comma"), Global Alias, and Segment (2260992).

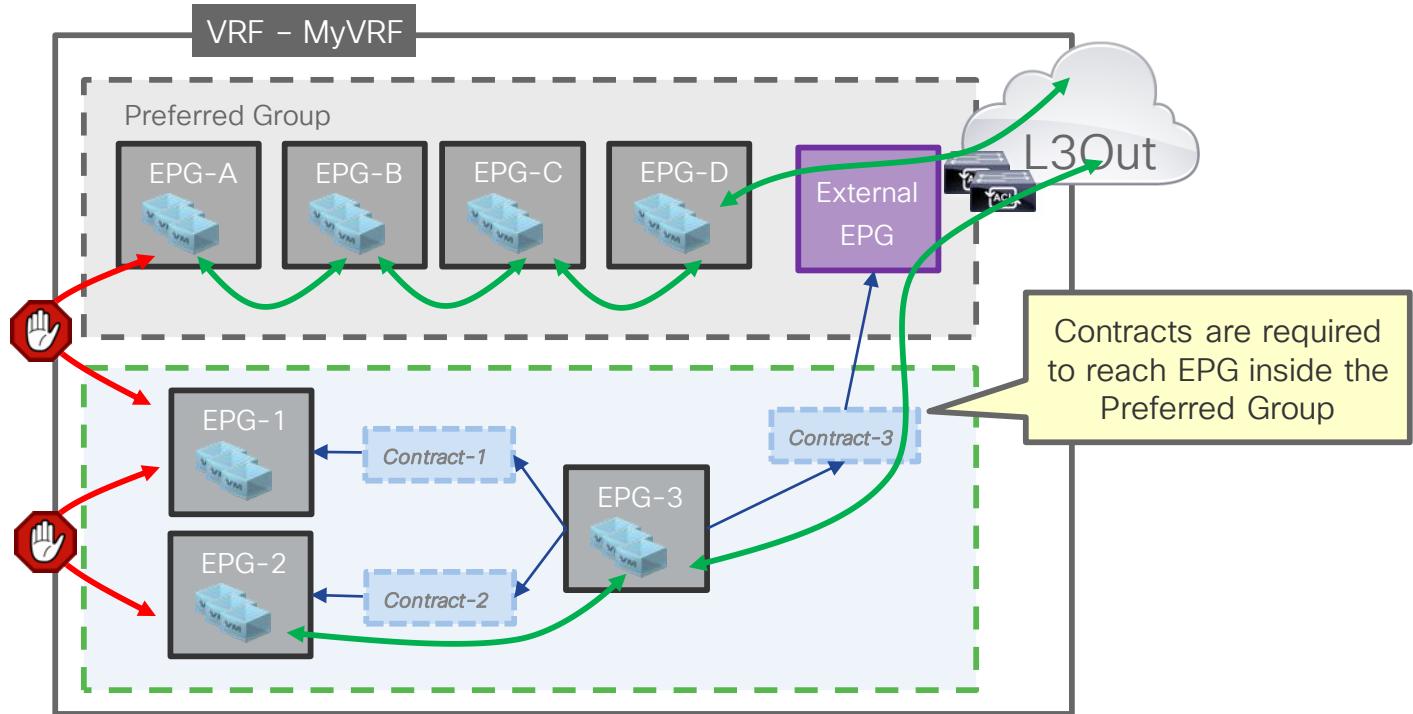
A red box highlights the "Policy Control Enforcement Preference" and "Policy Control Enforcement Direction" sections. The "Policy Control Enforcement Preference" has two options: "Enforced" (selected) and "Unenforced". The "Policy Control Enforcement Direction" has two options: "Egress" (selected) and "Ingress".

At the bottom of the page are buttons for "Show Usage", "Reset", and "Submit".

Contract Preferred Group Example



Contract Preferred Group Example



Enabling Preferred Groups Is Easy

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The top navigation bar includes the Cisco logo, the title "APIC (ACI-East-1)", and user authentication ("admin"). Below the title, there are tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. The "Tenants" tab is selected.

The main content area displays the "ALL TENANTS" view, with a search bar and a list of tenants: common, CL-Demo, Andy-Tenant-1, infra, and Sec-Dom-2-Tenant. The "CL-Demo" tenant is currently selected.

On the left, a sidebar shows the structure of the "CL-Demo" tenant, including Application Profiles, Application EPGs, and uSeg EPGs. The "CL-Base-EPG" under Application EPGs is selected and highlighted with a red box.

The right panel shows the "EPG - CL-Base-EPG" configuration page. The "Policy" tab is selected. The "General" sub-tab is active. The "Properties" section includes fields for Custom QoS (set to "select a value"), Data-Plane Policer (set to "select a value"), and Intra EPG Isolation (set to "Unenforced"). The "Preferred Group Member" field is set to "Exclude" and is also highlighted with a red box. Other settings include Flood on Encapsulation (set to "Disabled") and Configuration Status (set to "applied").

At the bottom of the right panel, there are buttons for "Show Usage", "Reset", and "Submit".

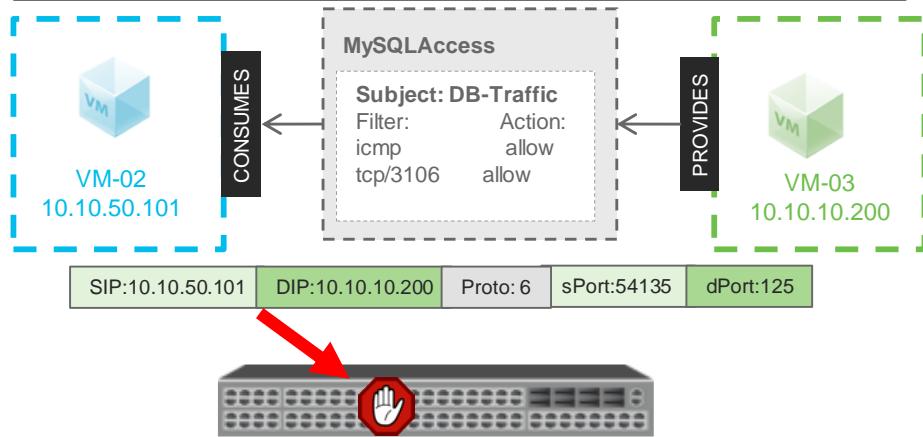
Contract Logging - Denied Packets

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'

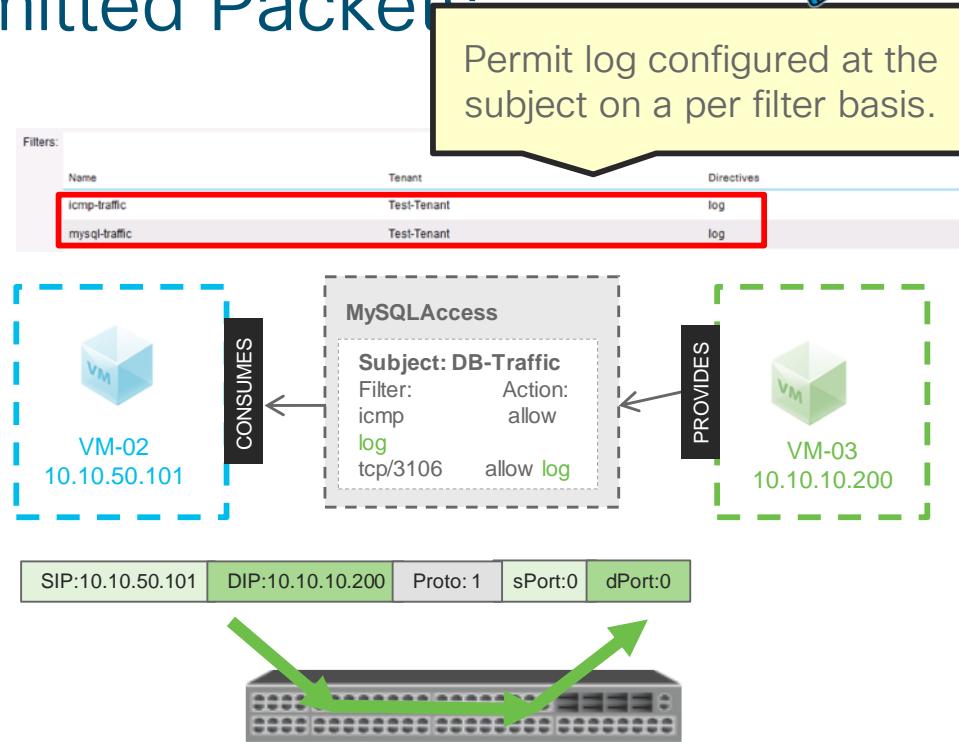


```
Feb 04 10:26:54 troy-leaf1 %LOG_LOCAL7-6-SYSTEM_MSG [E4204936][transition][info][sys] %ACLLOG-5-ACLLOG_PKTLOG_DENY:  
CName: Test-Tenant:Test-Tenant-VRF(VXLAN: 2162689), VlanType: FD_VLAN, Vlan-Id: 21, SMac: 0x00505690b43a,  
DMac:0x0022bdf819ff, SIP: 10.10.50.101, DIP: 10.10.10.200, SPort: 54135,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

Contract Logging – Permitted Packets

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
```

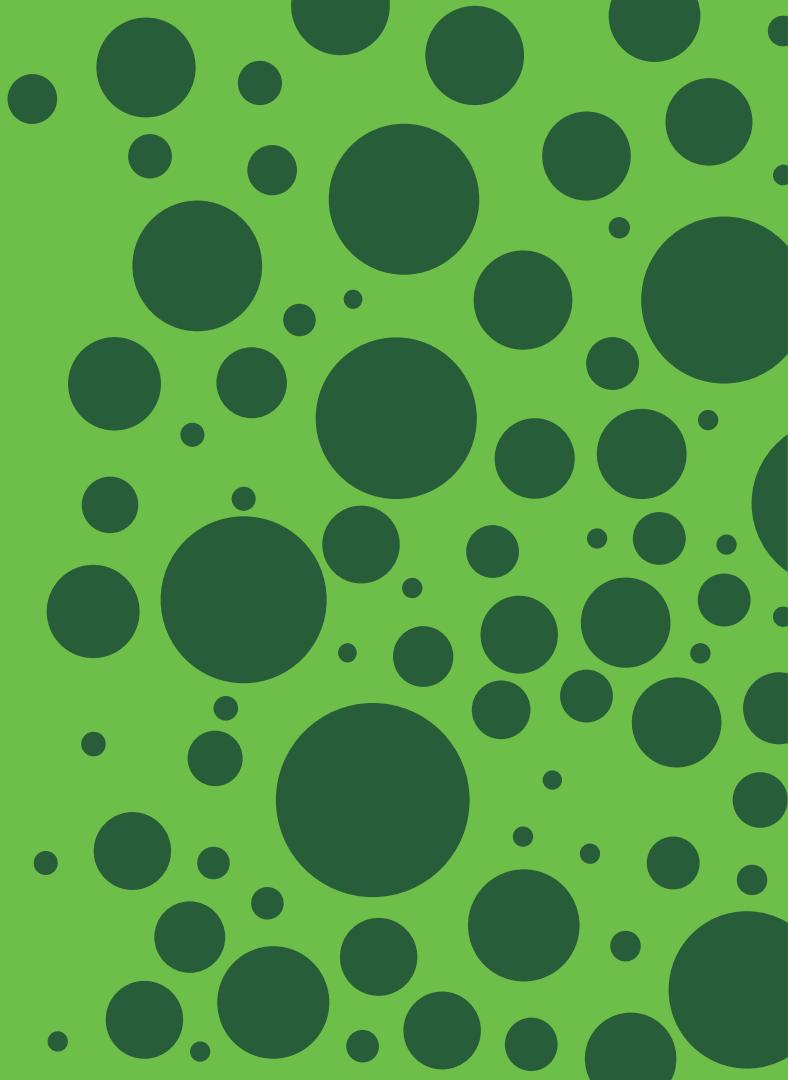
You can also see logs under the tenant

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface for the 'ACI-East-1' cluster. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. The 'Tenants' tab is selected, displaying the 'ALL TENANTS' list with 'CL-Demo' highlighted. Below the navigation is a search bar and a breadcrumb trail: common > CL-Demo > Andy-Tenant-1 > infra > Sec-Dom-2-Tenant.

The main content area is titled 'Tenant - CL-Demo'. It features a sidebar with a tree view of tenant resources, including Application Profiles (CL-Demo-App-1), Application EPGs (CL-Base-EPG, CL-uSEG-App), and uSeg EPGs (CL-uSEG-App). The main pane displays a log table with the following columns: Timest, VRF, Alias, Src IP, Dest IP, Protoc, Src Port, Dest Port, Src MAC, Dest MAC, Node, Src Interfa, VRF Encap, Pkt Len, Src EPG, Dest EPG, Src PC Tag, and Dest PC Tag. The table lists 15 log entries, each showing a timestamp starting from 2023-06-20T10:22:00Z, source IP 10.99.2.10, destination IP 10.99.3.10, protocol ICMP, and various interface and MAC addresses. The last entry shows a destination port of 49... and a destination PC tag of 49... The bottom of the table includes pagination controls (Page 1 of 13), an auto-refresh checkbox, and object filtering options.

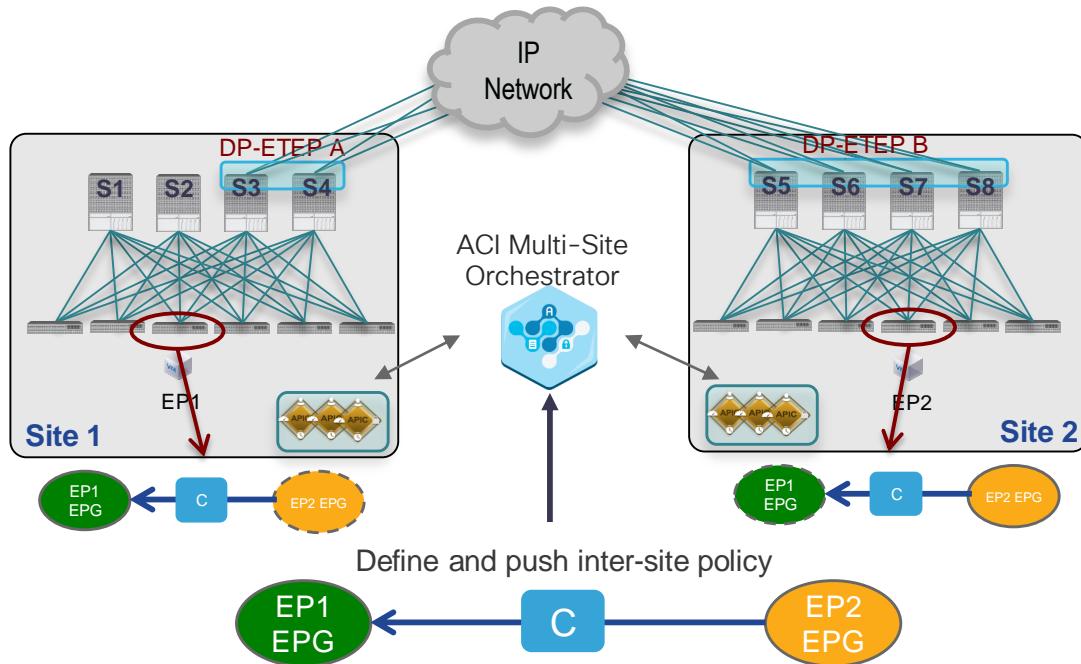
Timest	VRF	Alias	Src IP	Dest IP	Protoc	Src Port	Dest Port	Src MAC	Dest MAC	Node	Src Interfa	VRF Encap	Pkt Len	Src EPG	Dest EPG	Src PC Tag	Dest PC Tag
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	16...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...
2023-06-20T10:22:00Z	CL...		10.99.2.10	10.99.3.10	icmp	uns...	uns...	00:50:56:A...	00:22:BD:F...	no...	Eth...	VX...	98	CL...	CL...	49...	49...

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

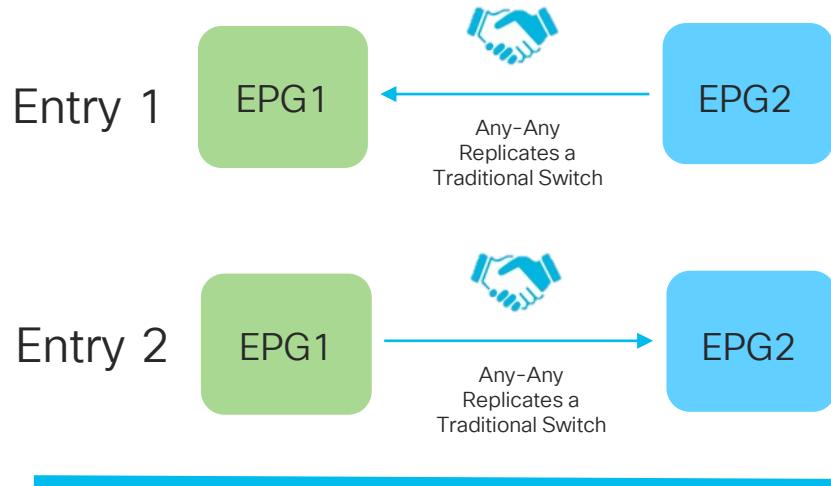
- Before 3.2 release, if the same contract was consumed and provided between the same EPGs, that would result in 2 TCAM entries being programmed in HW. One for consumer to provider and the other for provider to consumer
- After the introduction of the bi-directional compression feature in 3.2, if the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

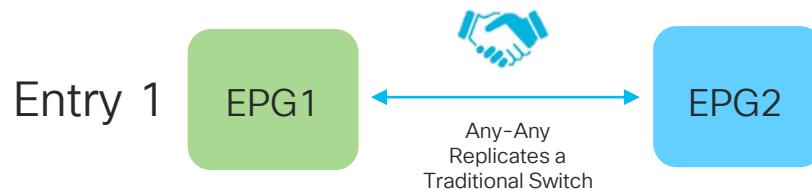
Actual Contract Relationship



TCAM Entries Before 3.2



TCAM Entries After 3.2

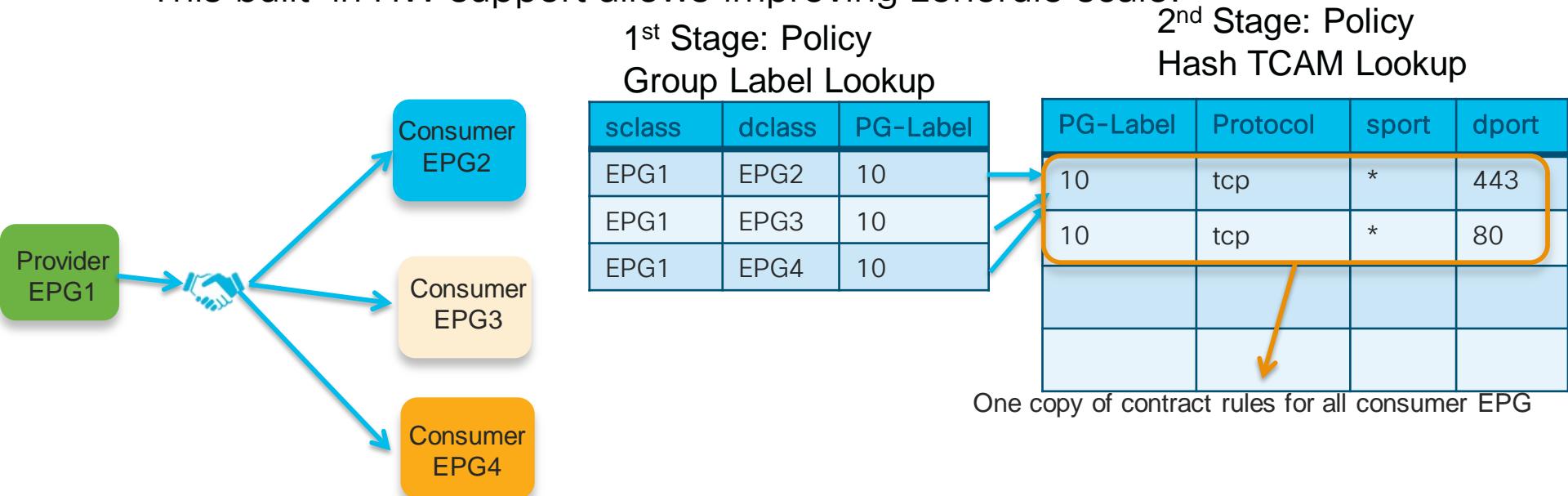


Criteria for Bi-directional TCAM Compression

- 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.



Policy compression requires FX and later hardware

Enabling Policy Compression

The screenshot shows the Cisco Policy Manager interface with a sidebar navigation menu and a central configuration window.

Navigation Sidebar:

- Quick Start
- Tenant t1
 - Application Profiles
 - Networking
 - Contracts
 - Standard
 - Blue-Contract
 - s1
 - Taboos
 - Imported
 - Filters
 - Policies
 - Services

Main Window - Add Filter Dialog:

Filter: Choose a filter to associate

Directives:

- Log
- Enable Policy Compression

Action:

Yellow Callout Box Content:

- Filter**
- Directives available are:
Log and Enable Policy Compression
- Actions available are Permit (default) and Deny

Contract Configuration Snapshot

Tenant t4

- > Quick Start
- > Tenant t4
 - > Application Profiles
 - > Networking
 - > Contracts
 - > Standard
 - > c1
 - s1
 - > c2
 - > c3
 - > clonedc3
 - > Taboos
 - > Imported
 - > Filters
 - > Policies
 - > Services

Contract Subject - s1

Policy Faults History

General Subject Exception Label

Property

Name: s1
Alias:
Description: optional
Global Alias:

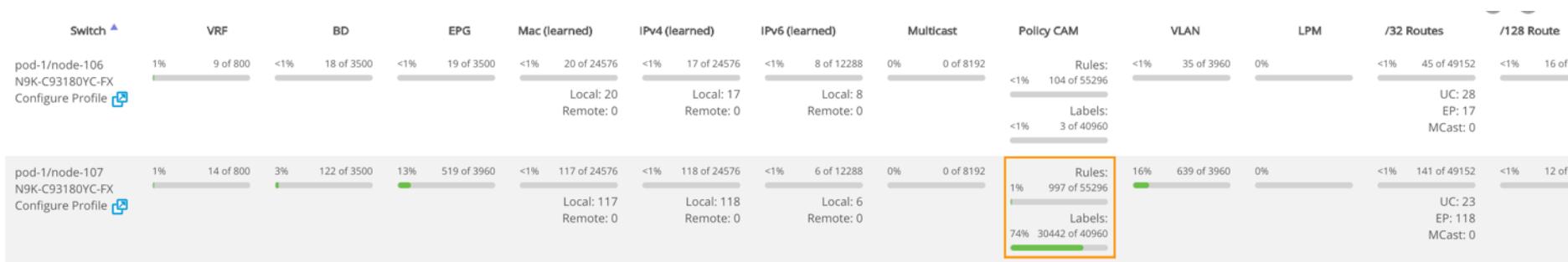
Apply Both Directions: true
Reverse Filter Ports:

Filters:

Name	Tenant	Action	Priority	Directives	State
commonfilt701	common	Permit	default level	Log Enable Policy Compression	formed
commonfilt702	common	Permit	default level	Log Enable Policy Compression	formed
commonfilt703	common	Permit	default level	Log Enable Policy Compression	formed
commonfilt704	common	Permit	default level	Log Enable Policy Compression	formed

Checking Filter/Contract Capacity on the Dashboard

Operations->Capacity Dashboard->Leaf Capacity

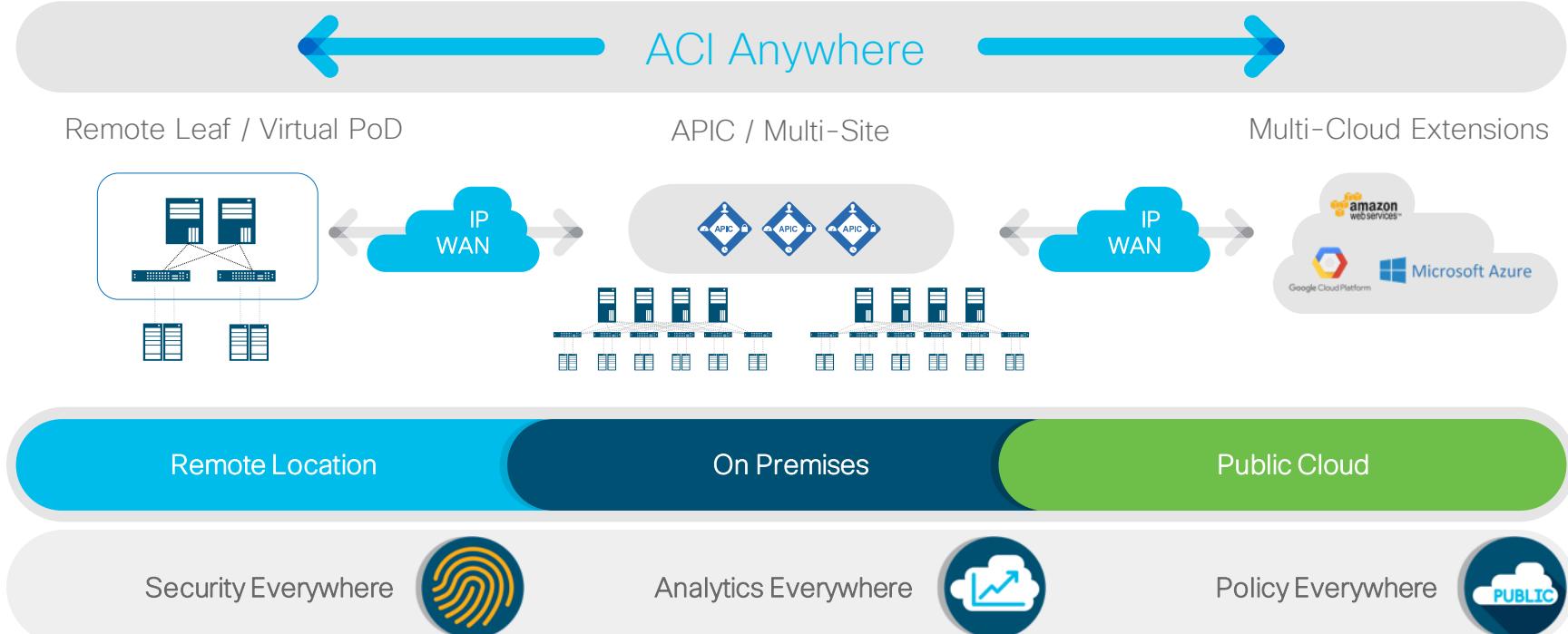


Agenda

- 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

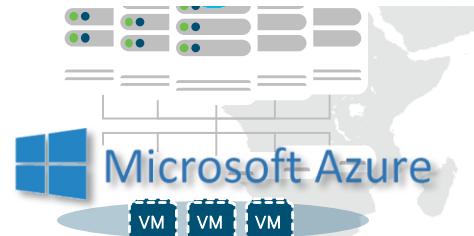
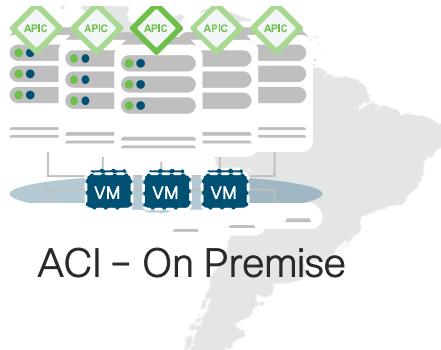
Any Workload, Any Location, Any Cloud



ACI Hybrid-Cloud Deployment Model



AWS Integration is in EFT with several customers today



Common
Governance

Discovery
& Visibility

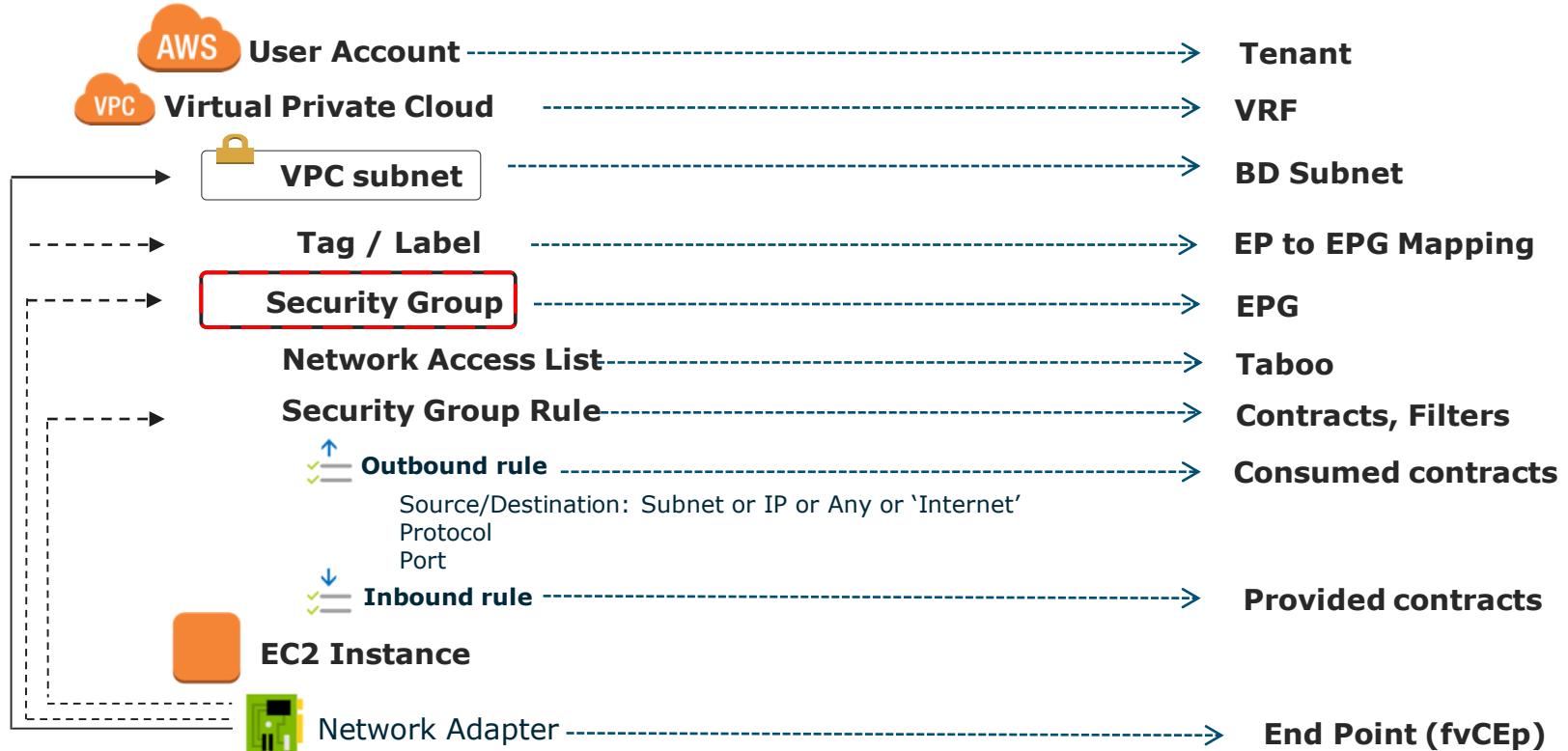
Policy
Translation

Monitoring &
Troubleshooting

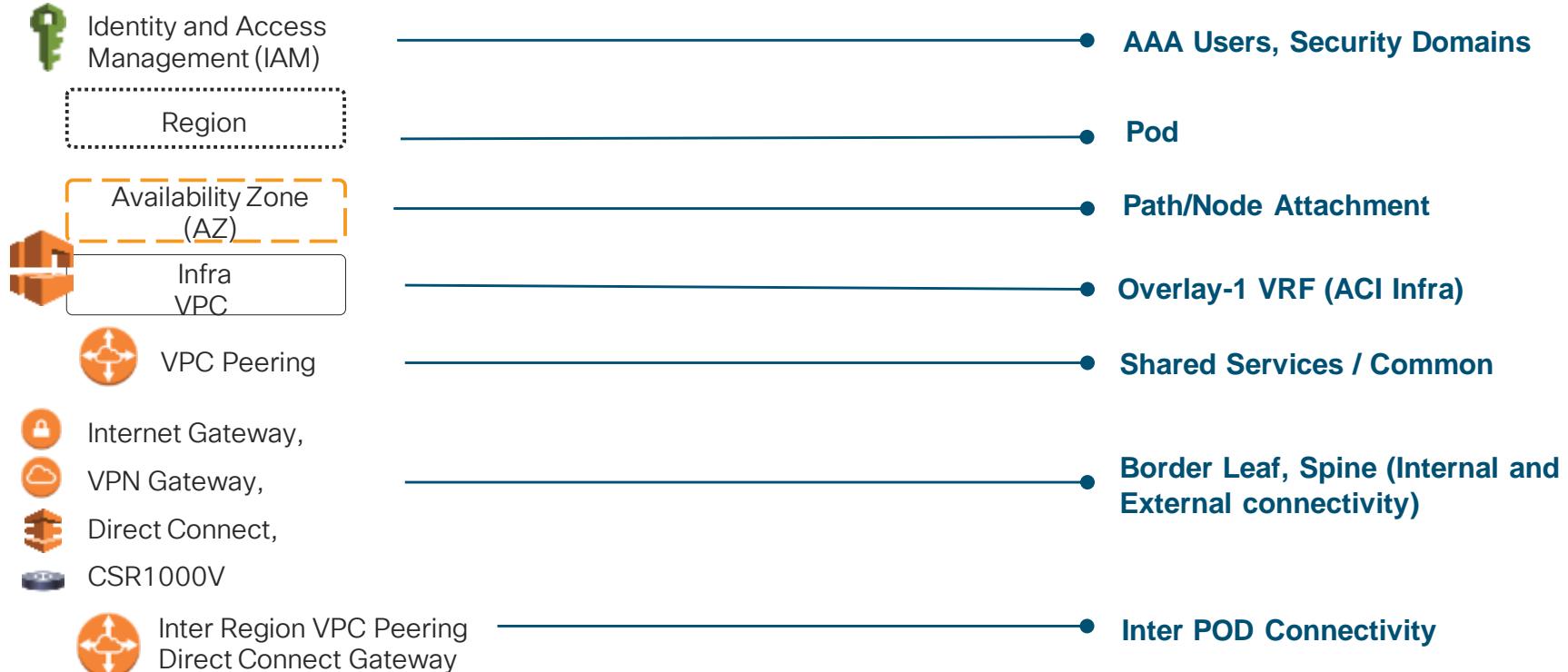
Single Point
Of Orchestration

Operational
Consistency

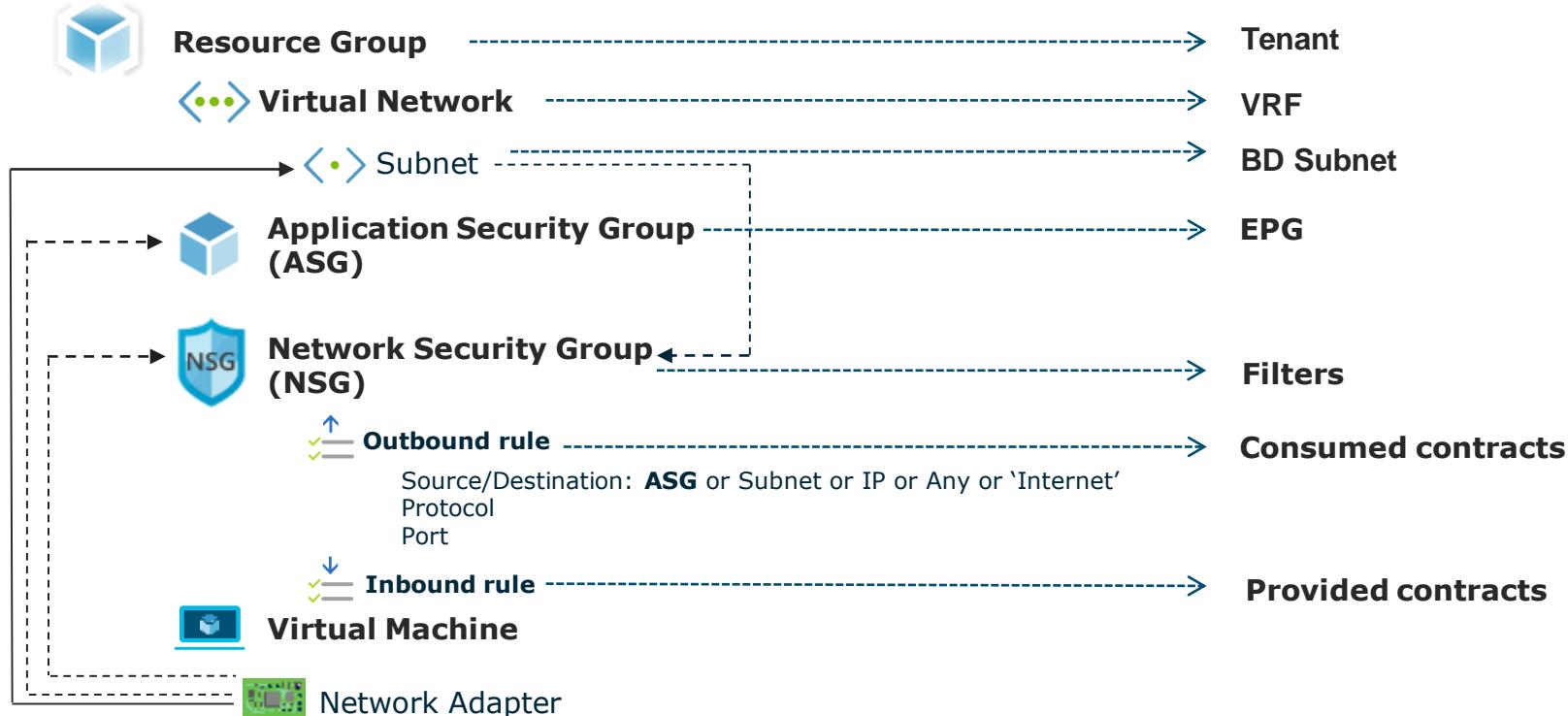
Policy and Resource Mapping - AWS



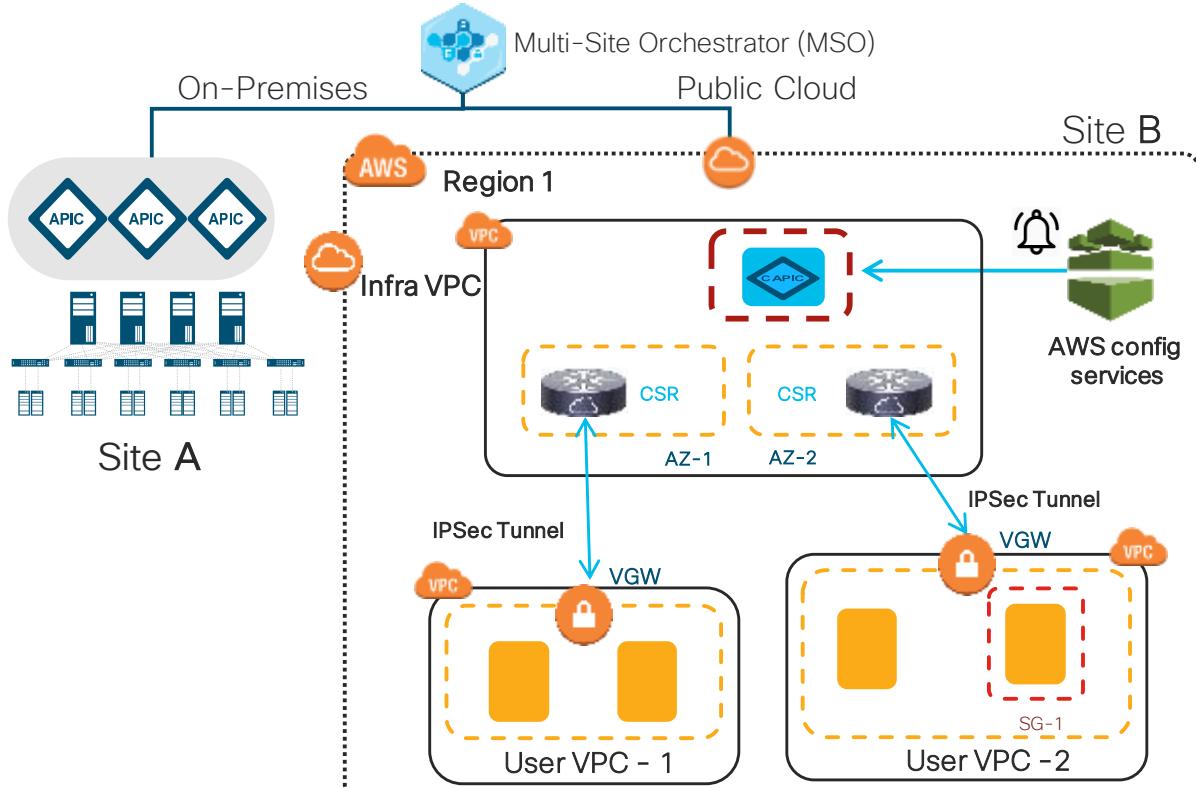
Policy Mapping – AWS



Policy Mapping - Azure



End Point Learning on AWS

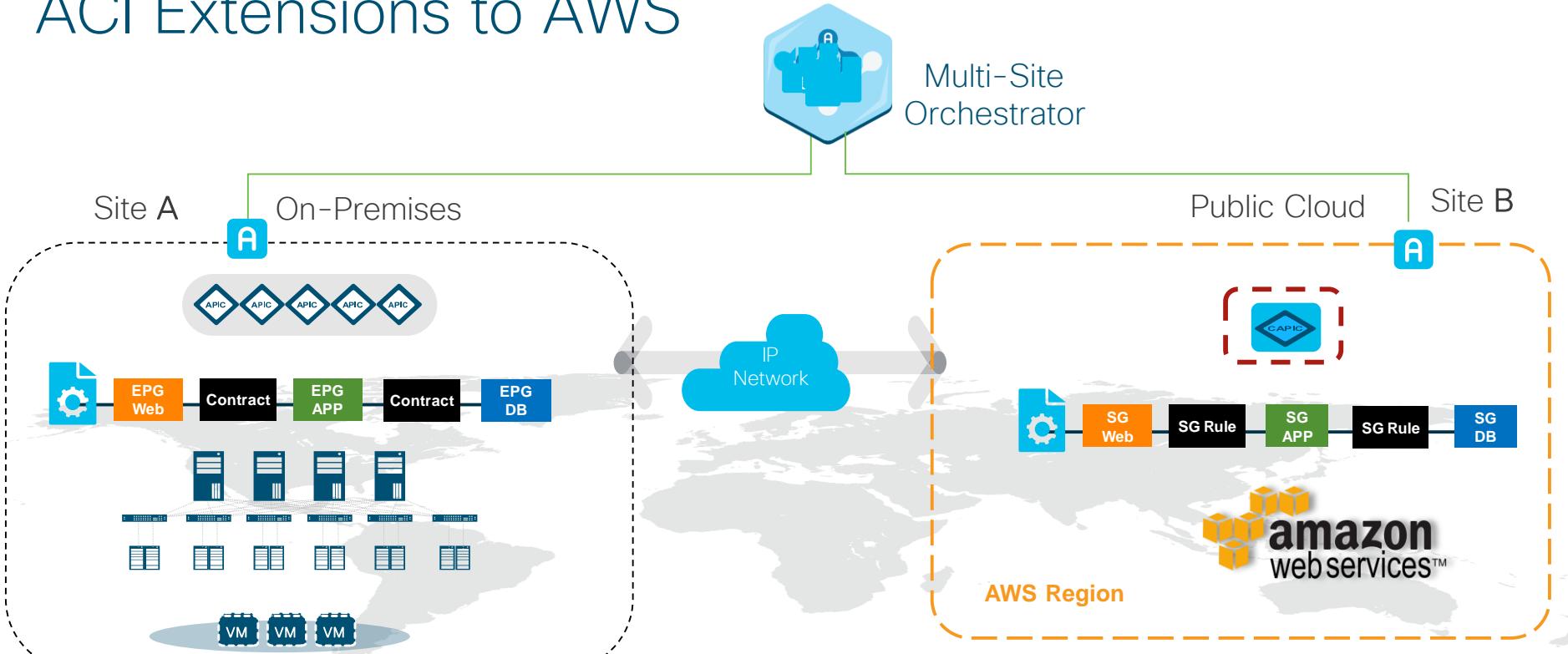


- User deploys a new instance in AWS
- AWS config services notifies the event to cAPIC
- cAPIC learns the endpoint and registers it
- Based on the policies (EPG's and Contracts) the correct security group (SG) is attached to the instance

Legend:

- 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

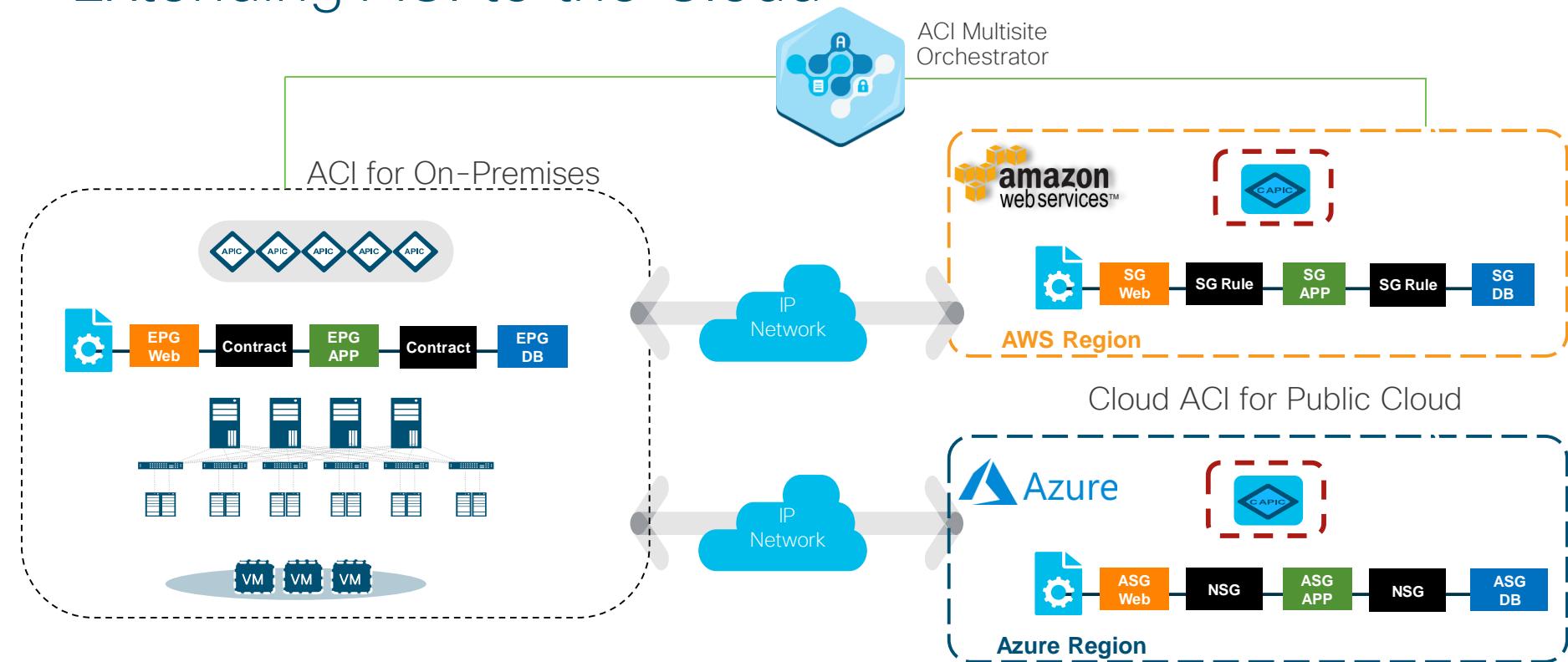
Policy
Translation

Monitoring &
Troubleshooting

Single Point
Of Orchestration

Operational
Consistency

Extending ACI to the Cloud



Common Governance

Discovery & Visibility

Policy Translation

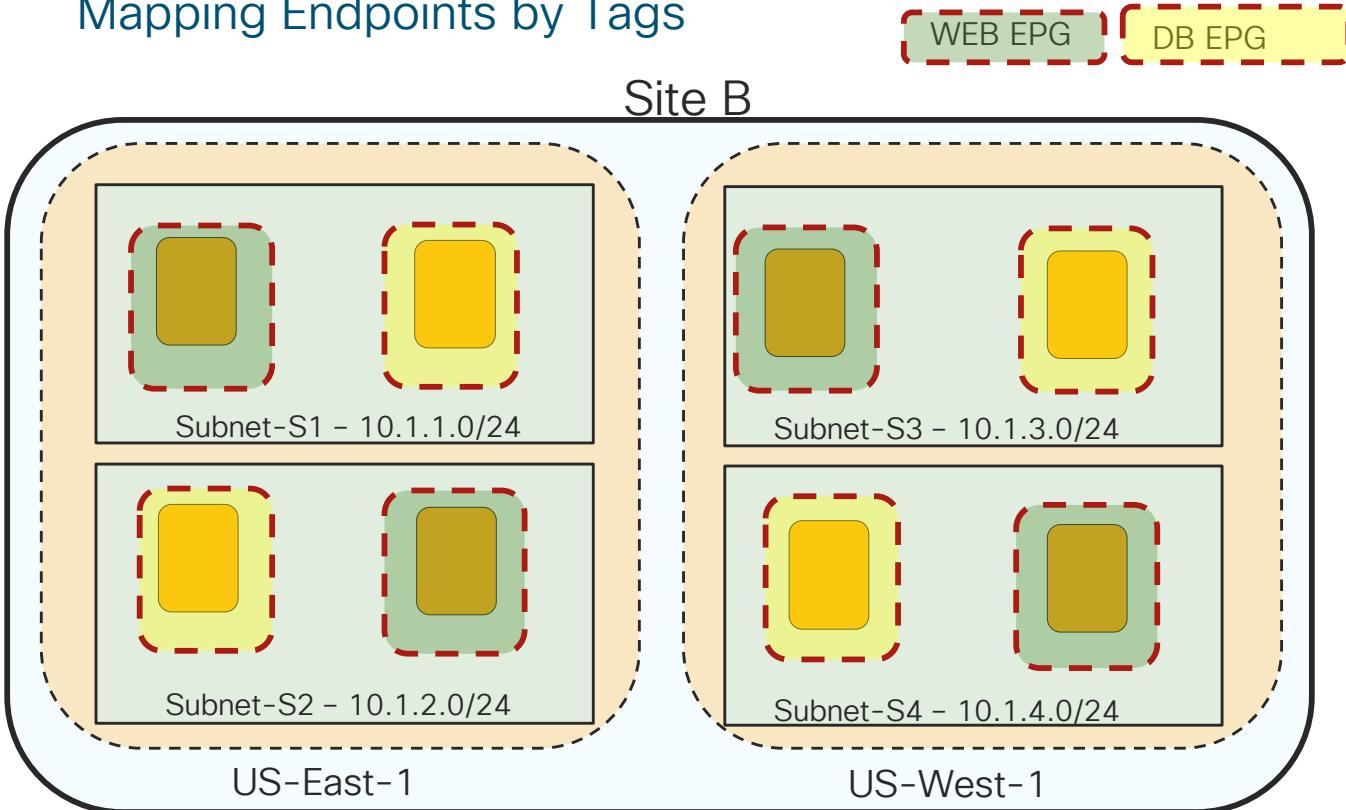
Monitoring & Troubleshooting

Single Point Of Orchestration

Operational Consistency

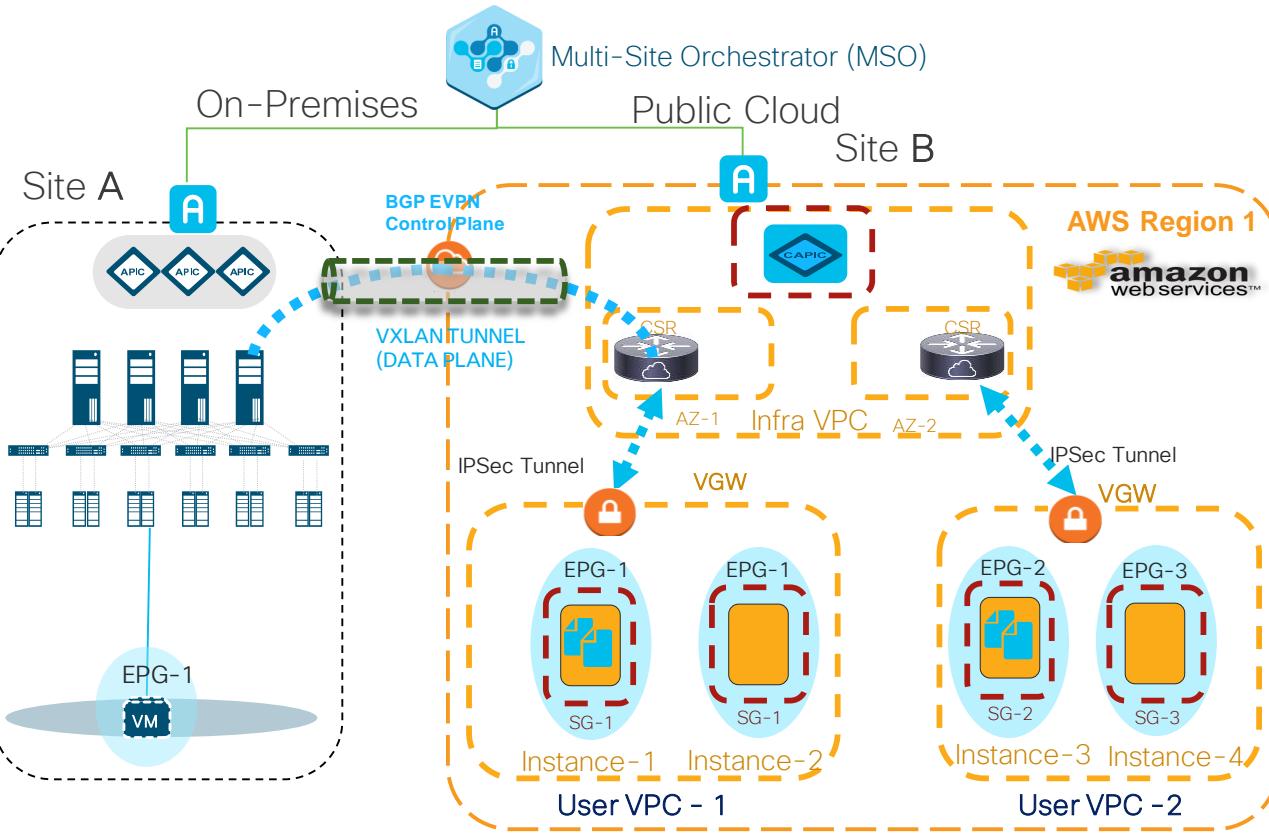
Cloud EPG

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

 Multi-Cloud Example

TEMPLATES

MSO-Multi-Site-Demo-AP

MSO-Simple-Hybrid-Demo

SITES

East-Coast

MSO-Multi-Site-Demo-AP •

West-Coast

MSO-Multi-Site-Demo-AP •

MSO-Simple-Hybrid-Demo

MSC-Tenant-1

AP Demo-Hybrid-Cloud

EPG

Hybrid-Web CONSUMED Hybrid-App PROVIDED Add EPG

Application Profile

CONTRACT

Permit-Any

VRF

Hybrid-VRF

BRIDGE DOMAIN

DEPLOY TO SITES

IMPORT

Unsaved Changes **SAVE**   

CONTRACT
Permit-Any

LOCAL RELATIONSHIPS EXTERNAL RELATIONSHIPS

2 0

* DISPLAY NAME
Permit-Any
Name: Permit-Any

SCOPE
vrf

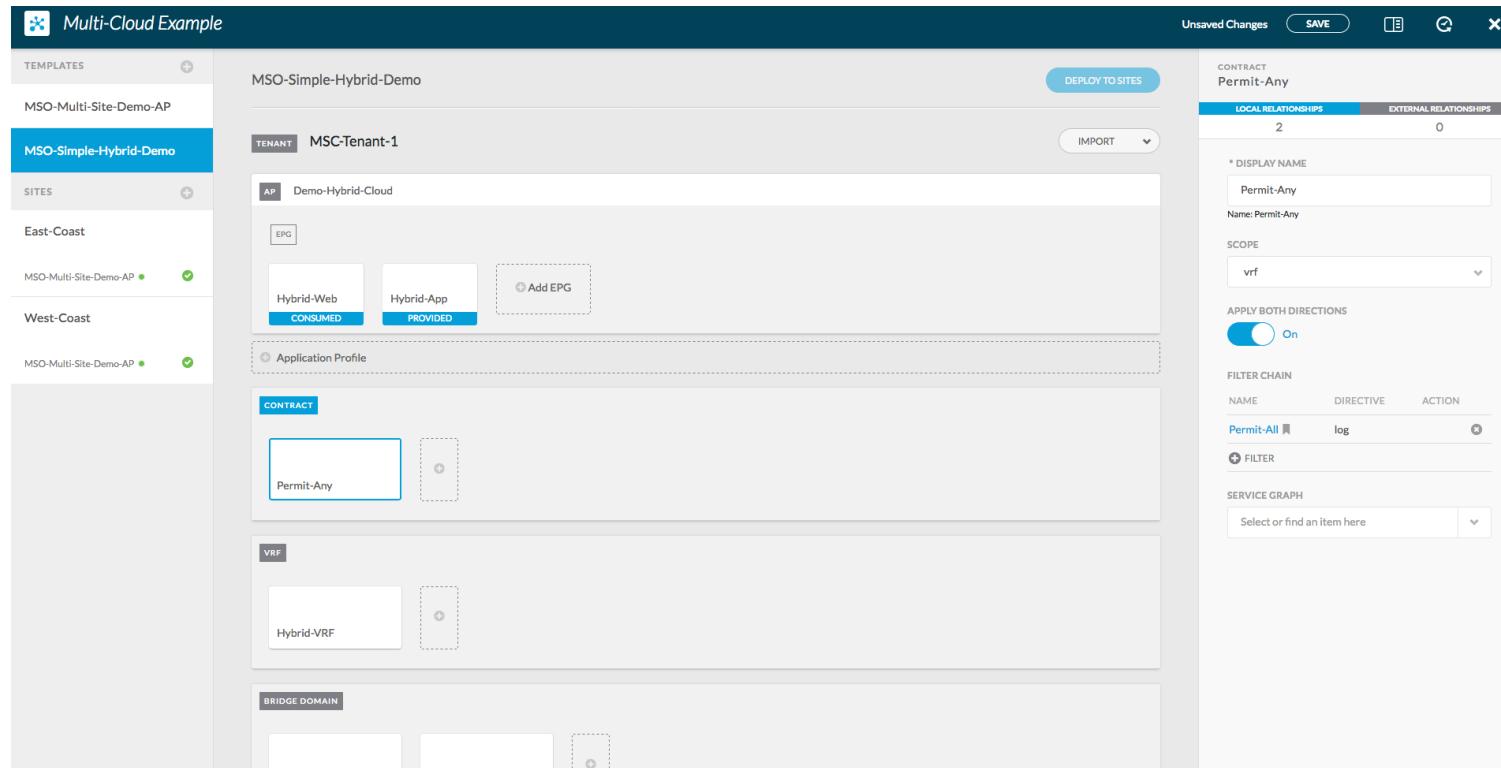
APPLY BOTH DIRECTIONS  On

FILTER CHAIN

NAME	DIRECTIVE	ACTION
Permit-All	log	

+ FILTER

SERVICE GRAPH
Select or find an item here



Traffic Allowed Between Two EPGs

APIC

System **Tenants** Fabric Virtual Networking L4-L7 Services Admin Operations Apps

ALL TENANTS | Add Tenant | Tenant Search: | **MSC-Tenant-1** | Andy-Tenant-1 | common | Infra | mgmt

This has been created from Multi-Site. It is recommended to only make changes from Multi-Site. Please review the documentation before making any changes here.

Tenant MSC-Tenant (F) (E) (O)

Application Profile - Demo-Hybrid-Cloud

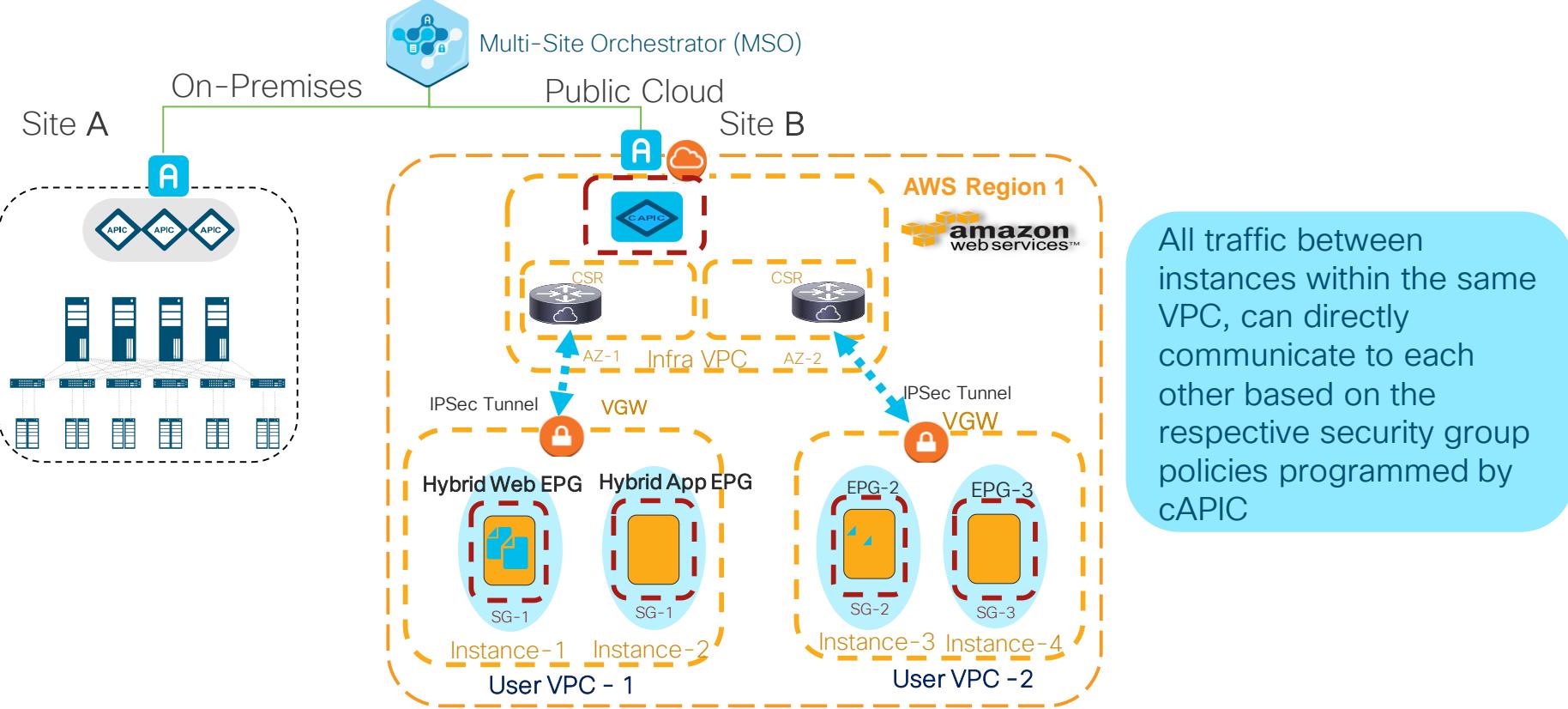
Summary **Topology** Policy Stats Health Faults History

Relation Indicators
Configured Operational
Show All On Click

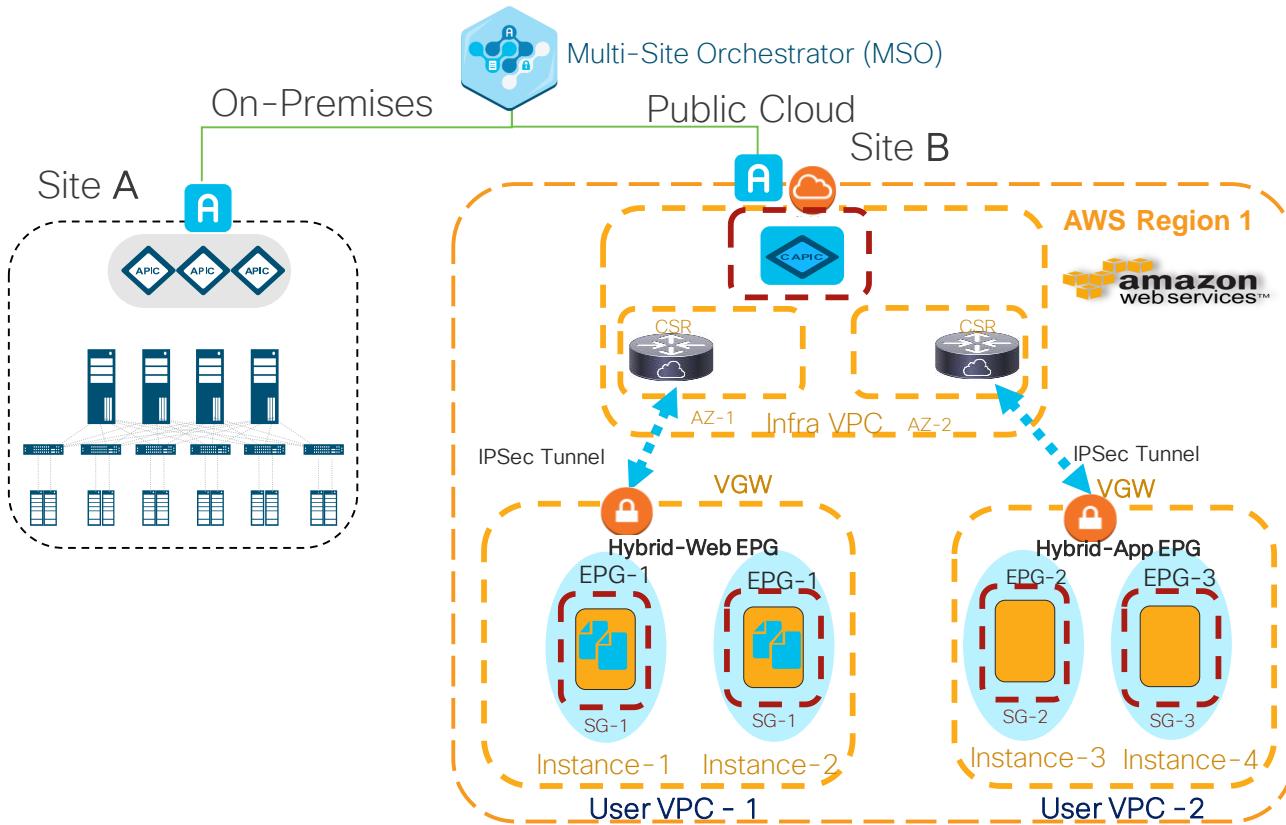
Provider
Consumer
Provider (From Master)
Consumer (From Master)
Master EPG

The diagram illustrates a network topology with three main components: a central node labeled 'C' (Contract), and two peripheral nodes labeled 'E' (EPG). Node 'C' is connected to both 'E' nodes via a green curved line, indicating a bidirectional contract. Each 'E' node is further connected to a specific virtual interface (v) via a straight line, representing a consumer relationship. The interface 'v' is colored orange, corresponding to the 'Consumer' indicator in the legend. The legend also includes icons for Provider, Provider (From Master), Consumer (From Master), and Master EPG.

Instances within a VPC



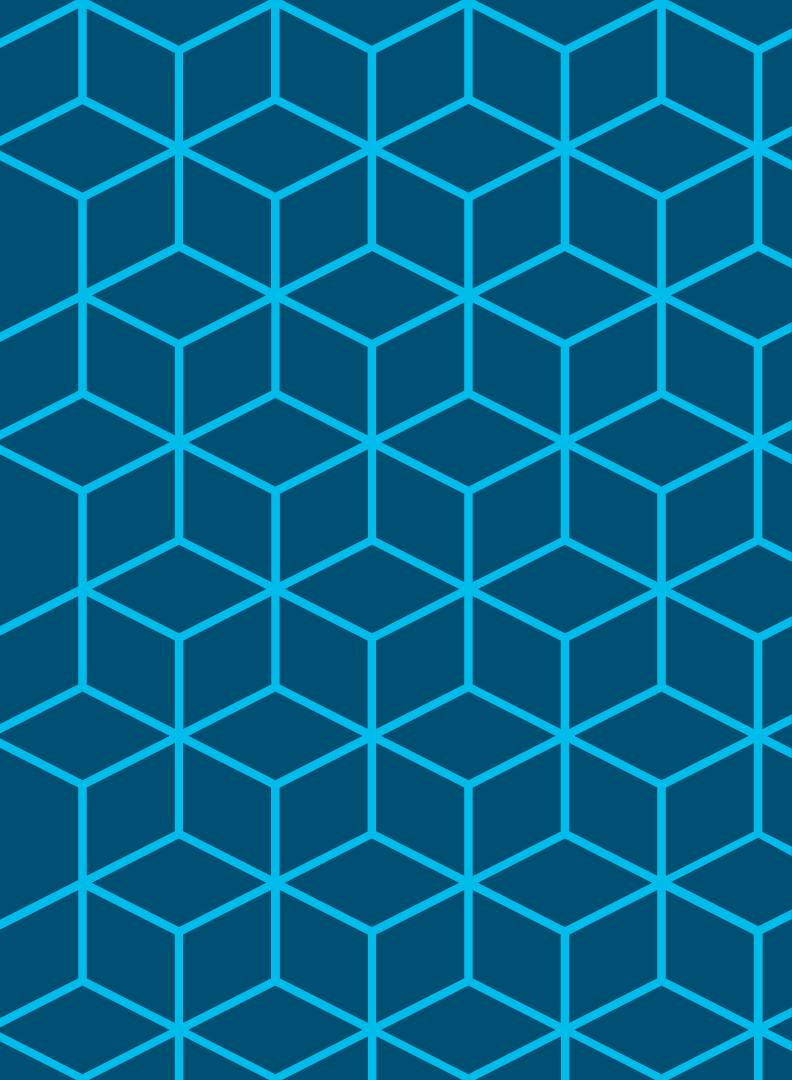
Instances across VPCs



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



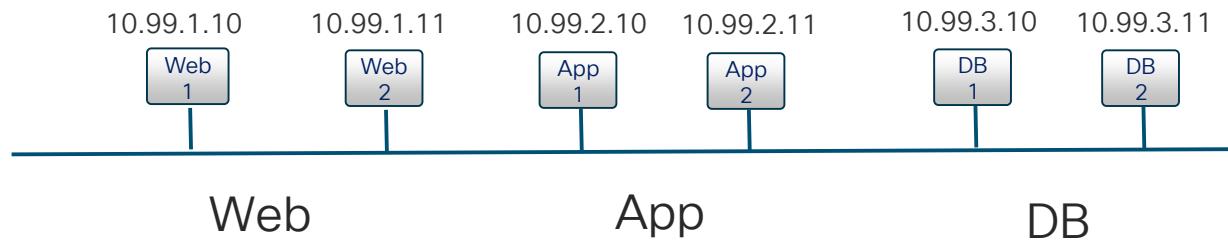
Demo

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

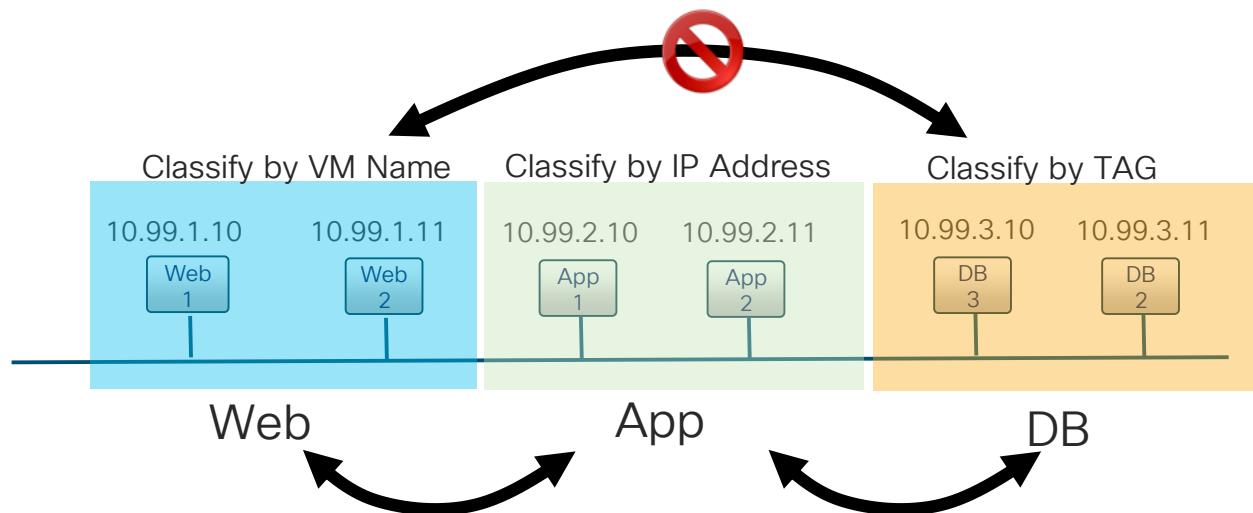
Tenant: CL-Demo

App: CL-Demo-App-1

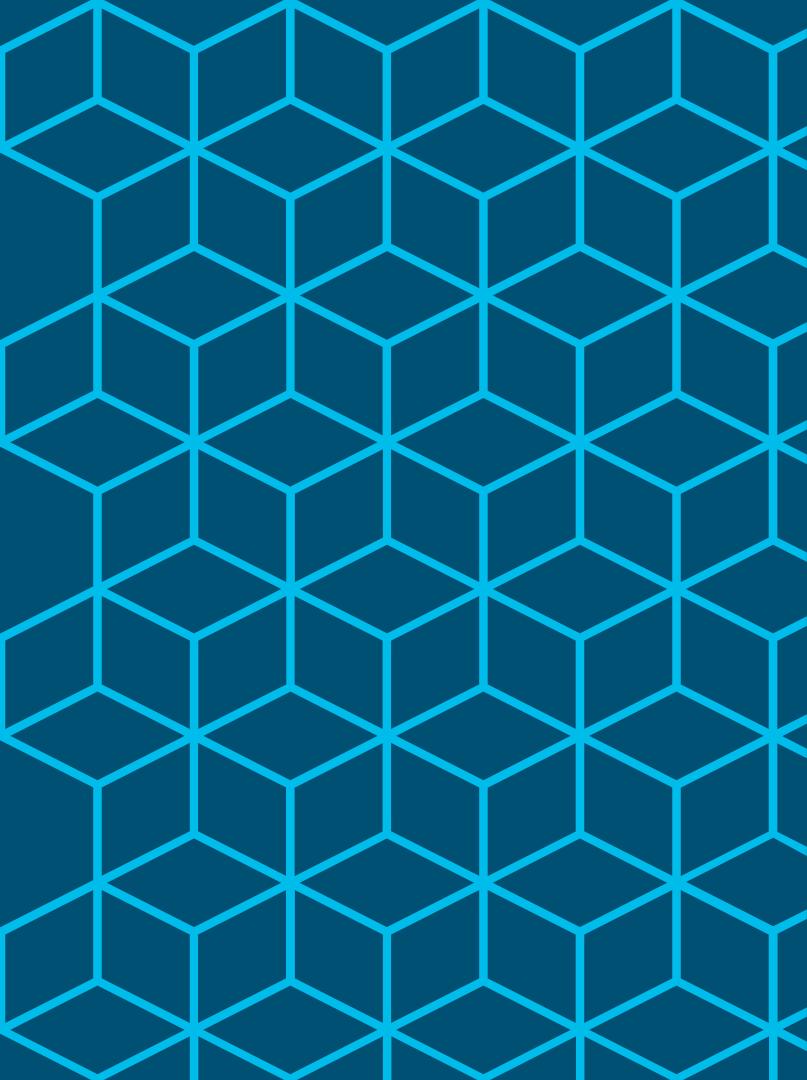
EPG: CL-Base-EPG

CL-Base-EPG

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



Summary

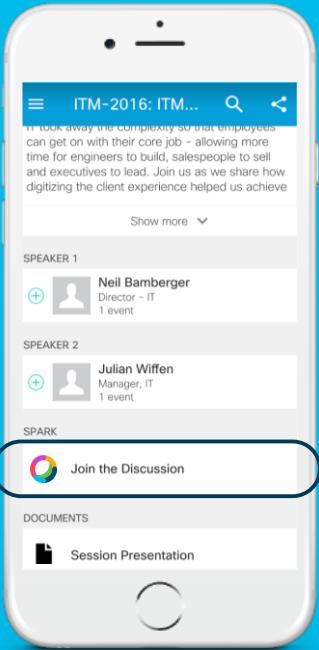


ACI enables micro segmentation that you can deploy in a gradual and flexible way. Use the right tool or feature for your use case...

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

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





Cisco Webex Teams



Questions?

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

How

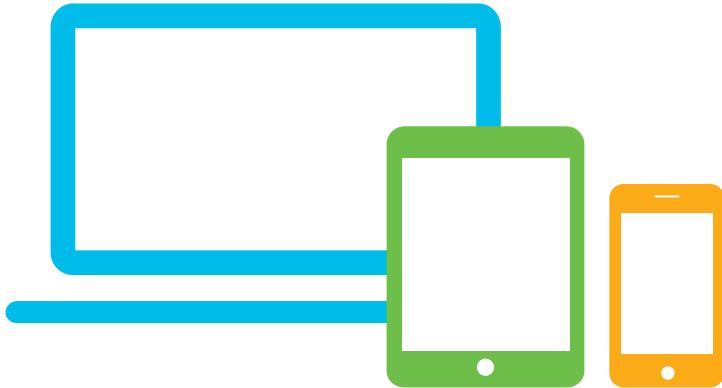
- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space

cs.co/ciscolivebot#BRKACI-2301

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](https://cisco.com/ciscolive)



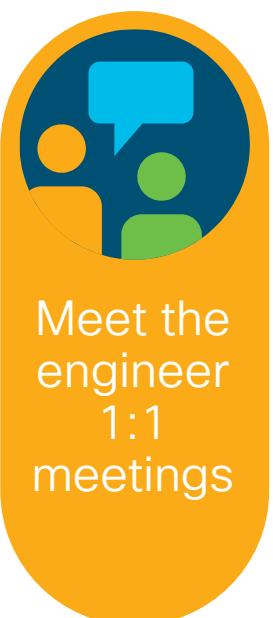
Continue Your Education



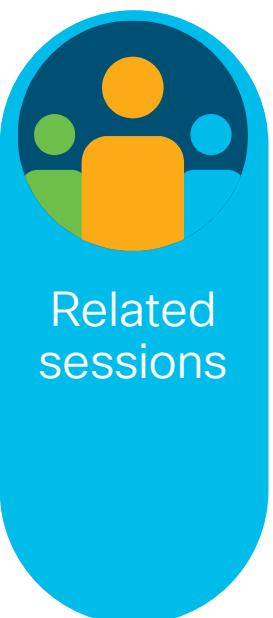
Demos in
the Cisco
Showcase



Walk-in
self-paced
labs



Meet the
engineer
1:1
meetings



Related
sessions



Thank you

Cisco *live!*



INTUITIVE



INTUITIVE