cisco Live!

Let's go

The bridge to possible

Application Centric Design

How to get there with Cisco ACI

Robert Burns – Technical Solutions Architect, CISG COE
CCIE #37856

BRKDCN-2658

Cisco Webex App

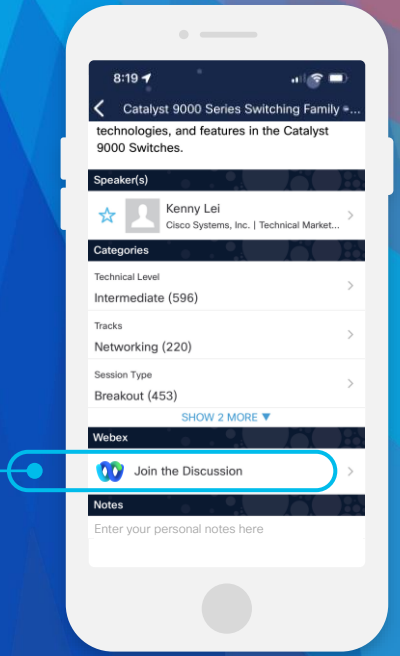
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2658

Companion Sessions – Week at a Glance

ACI General

Monday

- BRKDCN-2626 ACI Troubleshooting with Nexus Insights (2:30pm-3:30pm)
- BRKDCN-1601 Introduction to ACI (8am-9am)

Tuesday

- BRKDCN-2984 ACI: The Foundation of an Internal Private Cloud (10:30am-12pm)
- BRKDCN-2949 ACI Multi-Pod Design and Deployment (1pm-2:30pm)

Wednesday

- BRKDCN-3930 Defense in Depth Security for Multi-Cloud Data Centers (3pm-4:30pm)
- BRKDCN-3900 A Network Engineer's Blueprint for ACI Forwarding (1pm-2:30pm)

Thursday

- BRKDCN-3678 ACI Troubleshooting: Advanced L3out Features (8am-9am)
- DEVNET-3005 Application-Driven Networking with Consul-Terraform-Sync and Cisco ACI (10am-10:45am)

Security Related

Monday

- BRKAPP-1624 New Innovations in Application Security (9:30am-10:30am)
- BRKSEC-1773 How to Build Secure Mult-Cloud with Secure Workload (2:30pm-3:30pm

Tuesday

- BRKSEC-1139 Application Security – The Final Frontier (10:30am-11:30am)
- BRKDCN-3982 ACI L4-L7 PBR Deep Dive and Tips 3pm-4:30pm

Wednesday

- BRKSEC-2008 Zero Trust -Theory to Implementation (10:30am-12pm)
- BRKDCN-2938 Secure Firewall in ACI (1pm-2:30pm)

Thursday

- BRKSEC-2176 Keeping up with Zero Trust (8:30am-10am)
- BRKDCN-2127 Making Secure Firewall Threat Defense with Attribute Based Policy (9:30am-10:30am)

whoami

In 2022, there were an average of 7 breach notices issued each business day

Source: ITRC 2022 Data Breach Report

Session Objectives

- Understand the Need for Increased Security in the Data Center
- Differentiate between Network & Application Centric Design
- Review some of the Security Tools available with Cisco ACI
- Share some tips to advance the journey towards App Centric Design

- Hidden Slides included in downloaded presentation

  denoted with FOR REFERENCE ONLY

Acronym Decoder

FOR REFERENCE ONLY

EP - Endpoint

EPG – Endpoint Group

ESG – Endpoint Security Group

ExG - General reference for both EPG and ESG

uSeg - MicroSegment

uEPG - MicroSegment Endpoint Group

BD – Bridge Domain

VMM – Virtual Machine Manager (ie. vCenter, SCVMM)

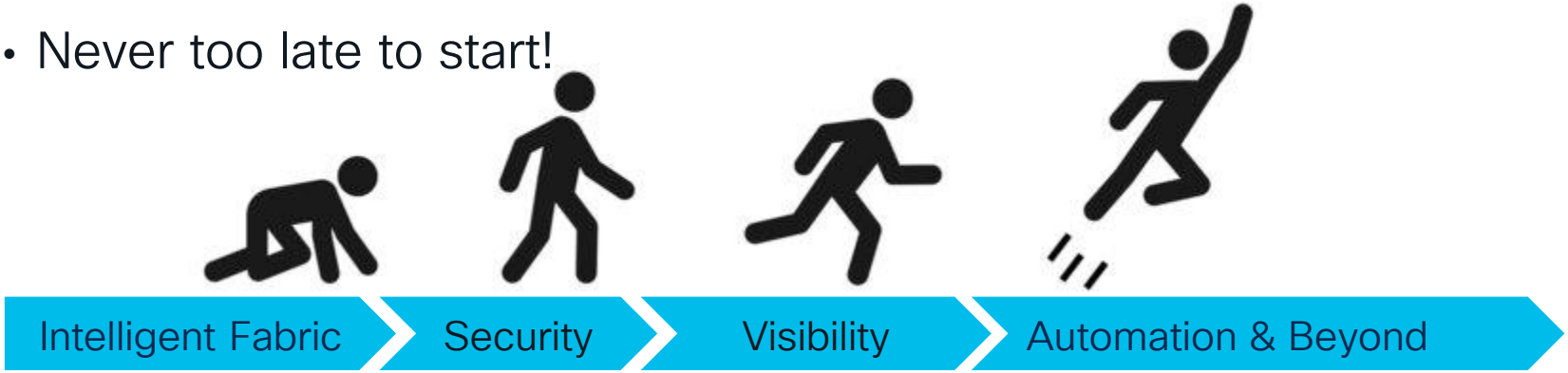
Agenda

- What and Why – App Centric Design & Zero Trust
- Challenges/Obstacles
- Available ACI Security Features
- Application Segmentation & Putting it all Together
- Recommendations & Case Study

App Centric Design

Its about Continuous Improvement

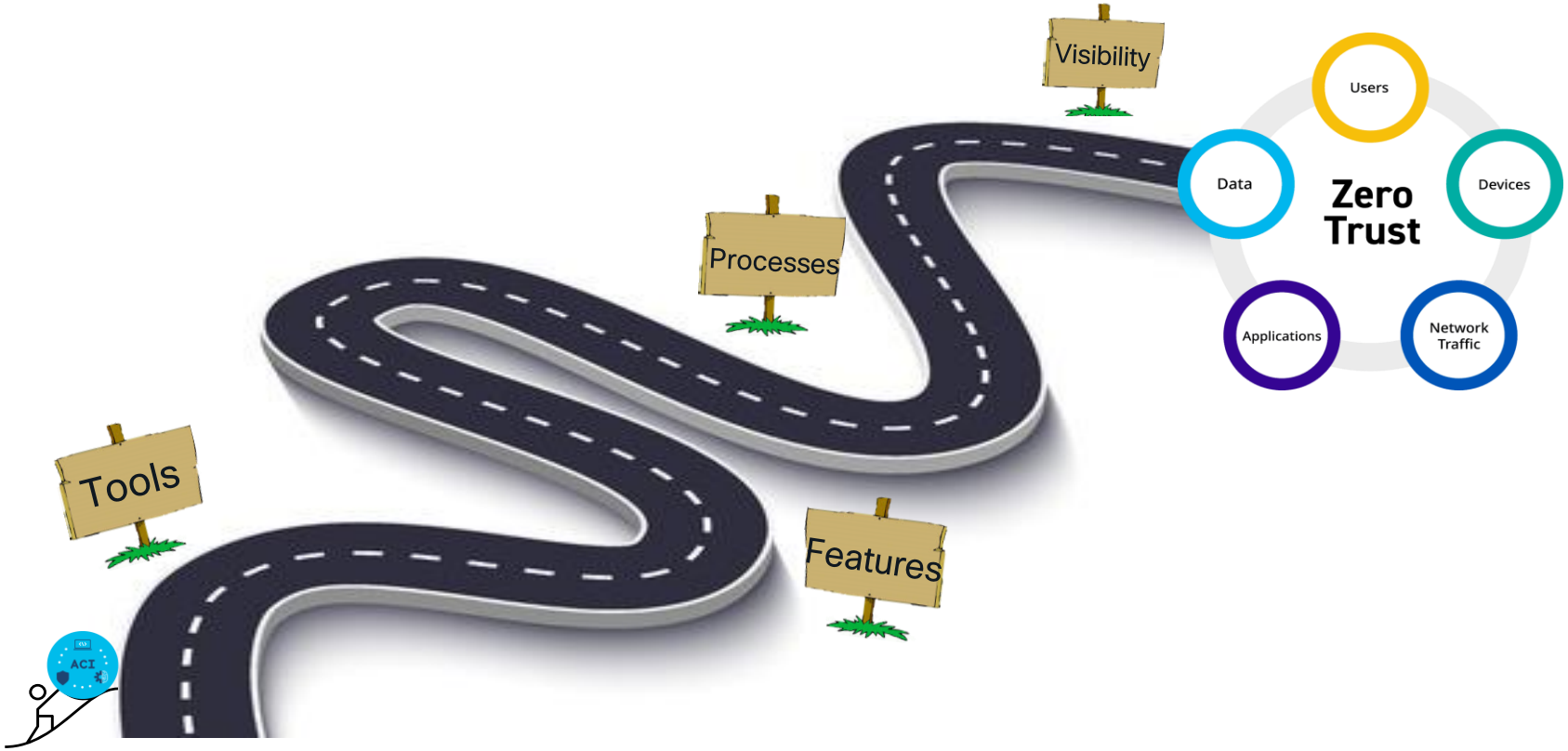
- Zero Trust is a journey
- Different Environments have different requirements
- Few Customers go all-in from Day1
- Any level of improved security is beneficial
- Never too late to start!



Importance of Application Segmentation

- Perimeter security is not enough
  - If breached, lateral movement can allow attackers to compromise additional assets
- Segmentation **improves security** inside the DC
- Micro-Segmentation **can minimize the size of the segments** and provide lesser exposure for lateral attacks

ACI's Path to Improved Security



Application Security 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, , Agent-based

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

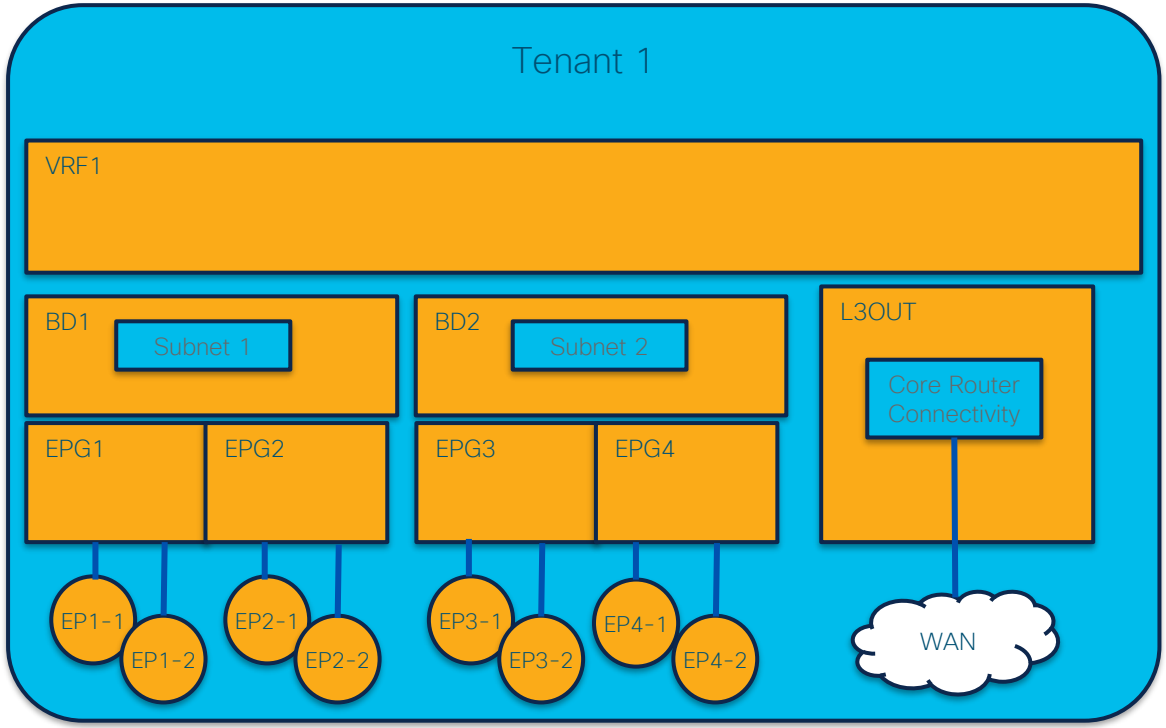
- Pros: distributed, guest independent, agent-less, group-based policies for best scale, endpoint-level visibility and correlation
- Cons: requires network hardware resources (memory, TCAM, etc) for policy

Review: Logical Policy in ACI

Routing Domain (IP forwarding)

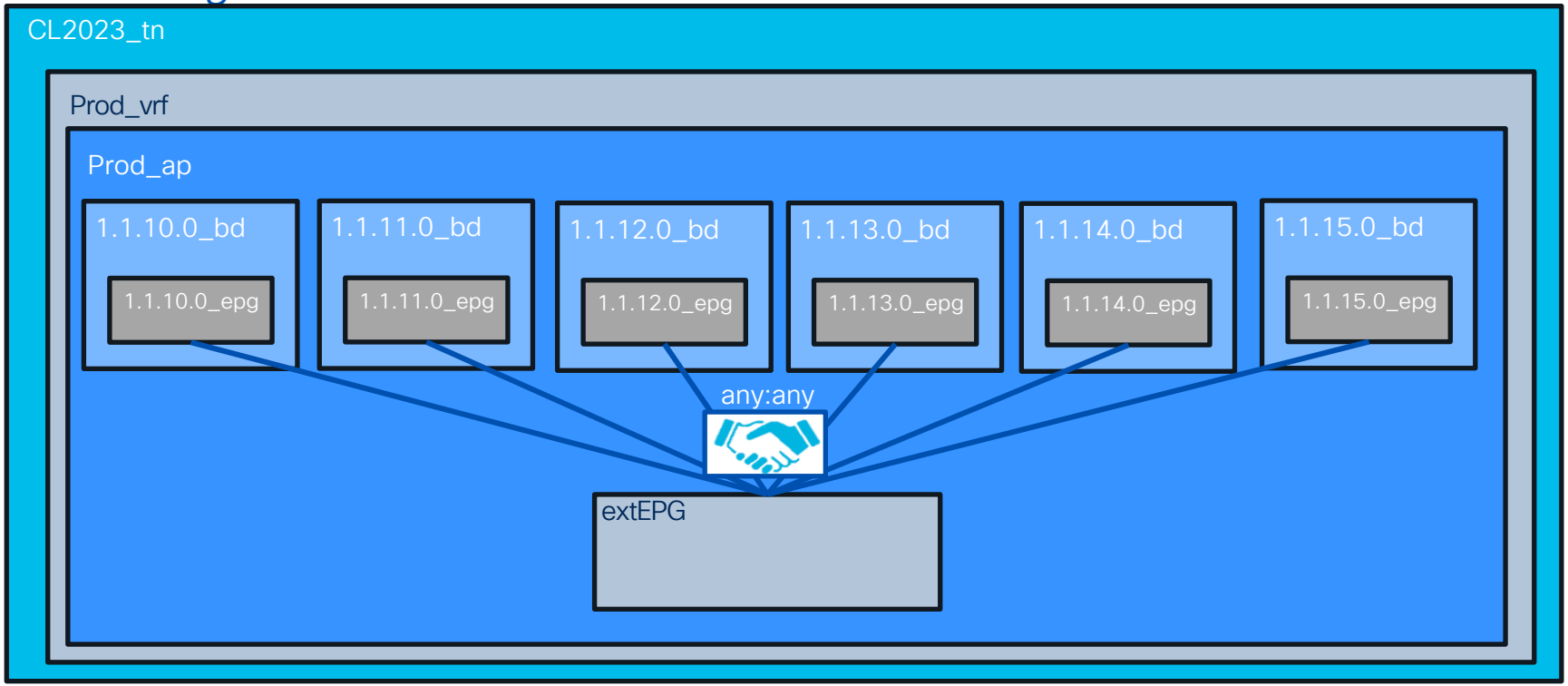
Switching Domain (MAC forwarding)

Security Domain



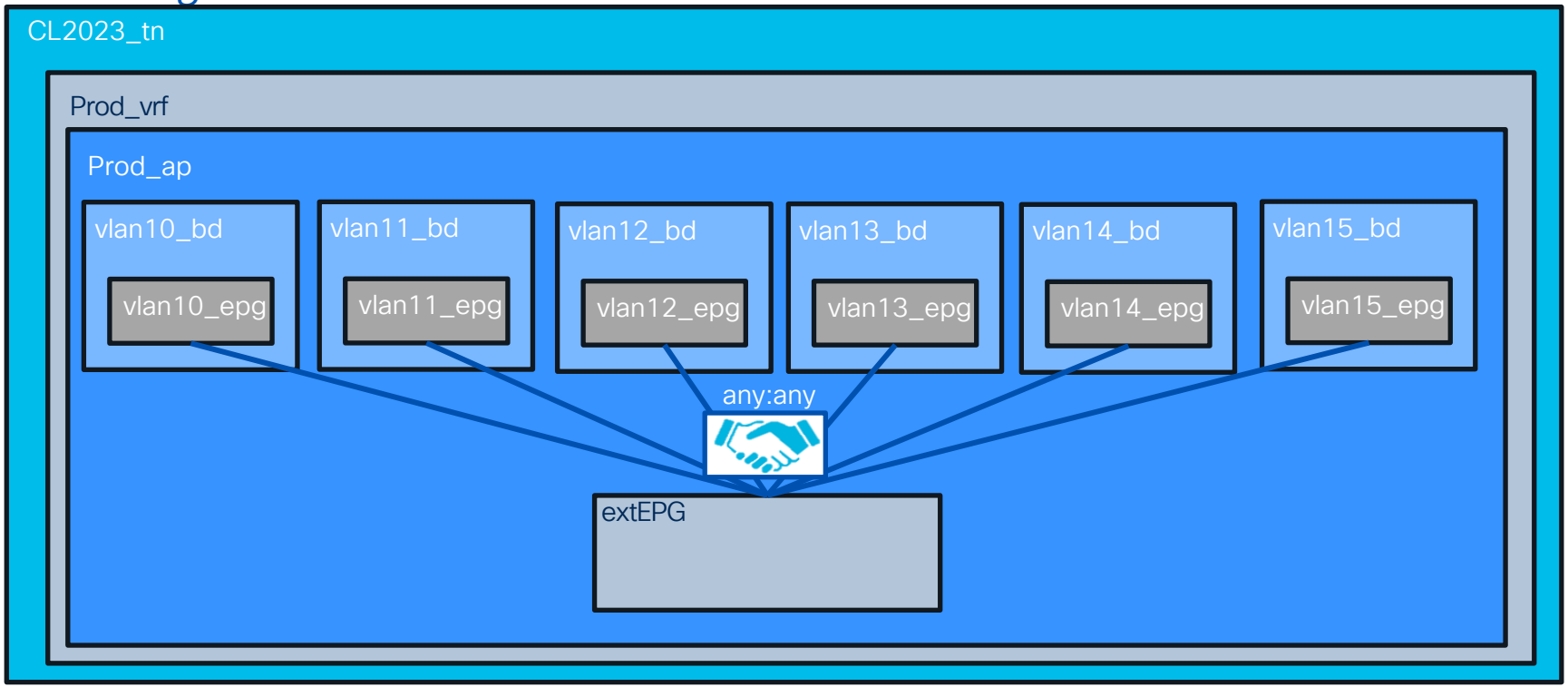
Do your ACI Policies look like this?

Subnet Aligned



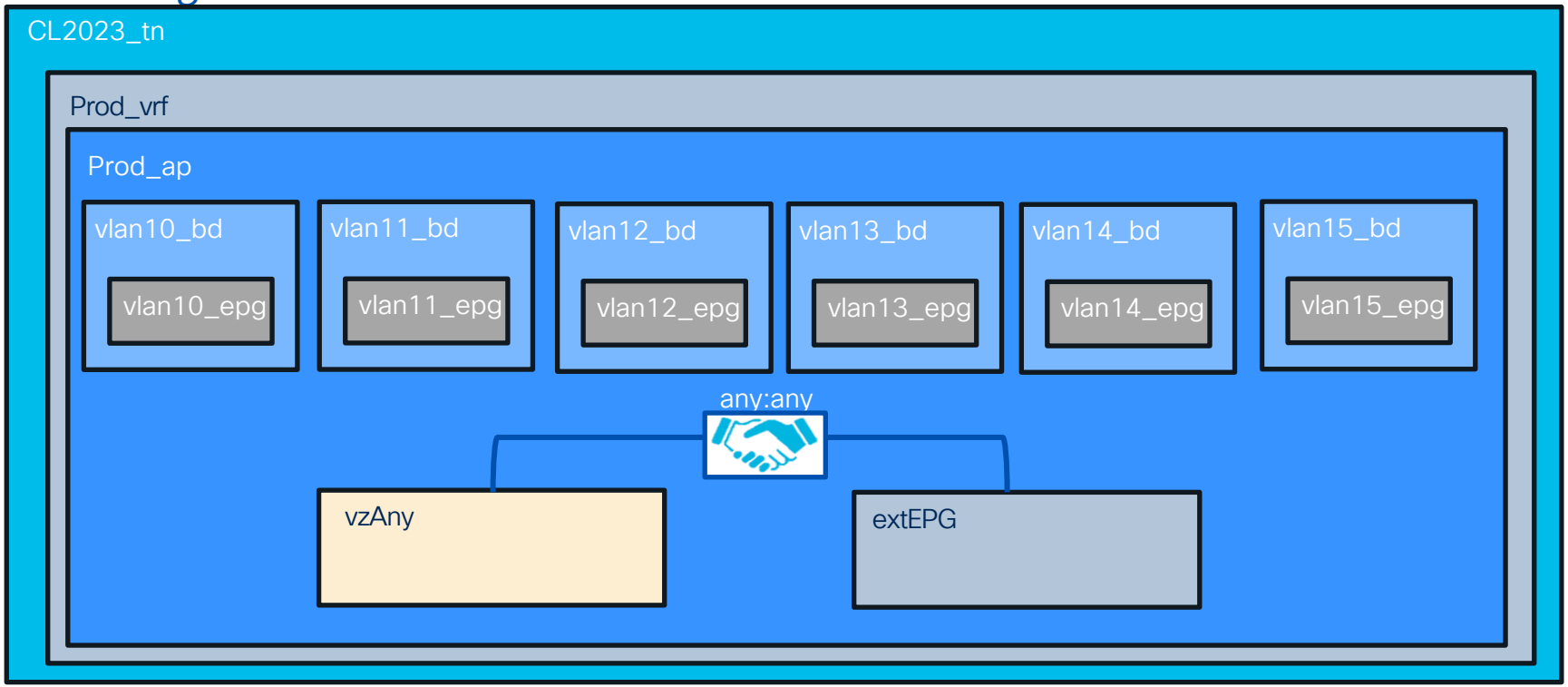
Or this?

VLAN Aligned



Or perhaps like this?

VLAN Aligned



Different Approaches to EPG Design in ACI

EPG/BD = VLAN/Subnet

- EPG and BD for each VLAN/Subnet
- Most Commonly Deployed
- Ease of Legacy Migration, Limited Segmentation
- VLANs/Subnets define security groupings

EPG = App Tier

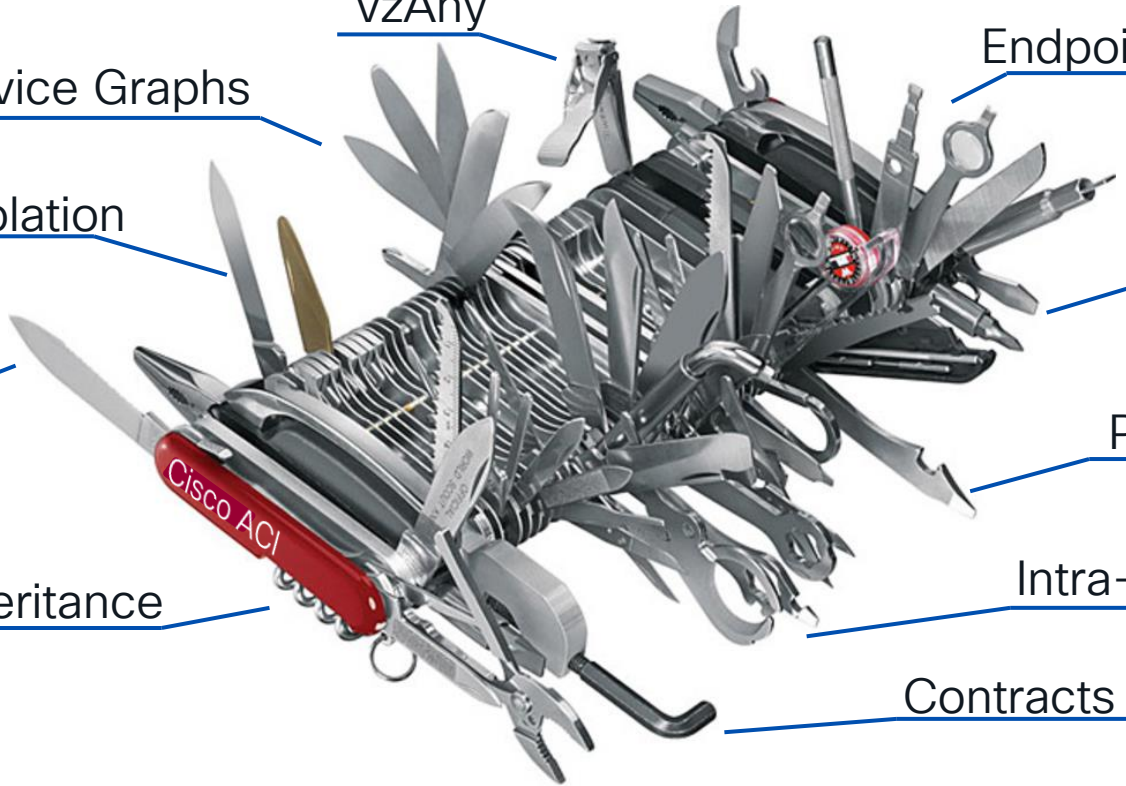
- EPG per Application Tier, sharing common BD
- Ideal for well-understood Apps and/or Flat Network deployments
- Works well with automation tools
- Most Flexible & Granular Security
- Increases operational complexity

Hybrid

- Combination Approach
- Supports both Legacy & New Apps on same fabric
- Introduces a path to an Improved Security Model
- Limited increase operational complexity

ACI Security Features Toolbox

What's in our ACI toolbox



vzAny

L4-7 Service Graphs

Intra-EPG Isolation

Filters

Contracts Inheritance

Endpoint Security Groups

ExGs

Endpoint Groups

Preferred Groups

Intra-EPG Contracts

Contracts

Endpoint Group

Endpoint Group (EPG)

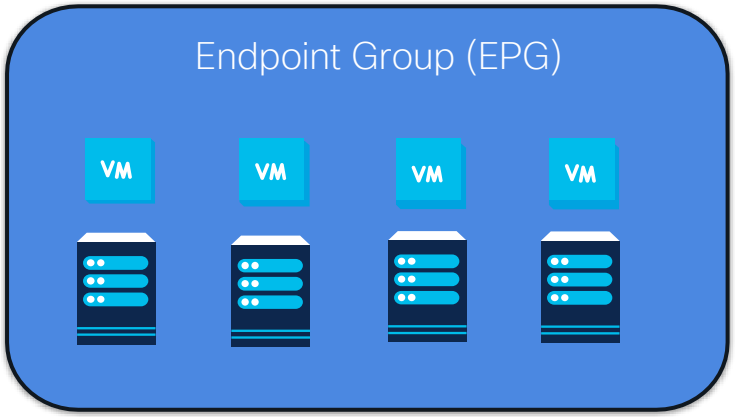
Collection of endpoints, such as VMs, hosts, servers, physical devices

Internally represented by pcTag

Use contracts to communicate to other EPGs

Can represent:

- Subnet/VLAN
- VMware port-group
- Application Tier
- Security zone



Contracts ≈ Access Lists

Endpoint Group Classification

Static Attachment (EPG)

- Physical Domain (Port/VLAN Instance)
- VMM Domain (i.e. Port-Group/VM Network)

Dynamic Attachment (uEPG)

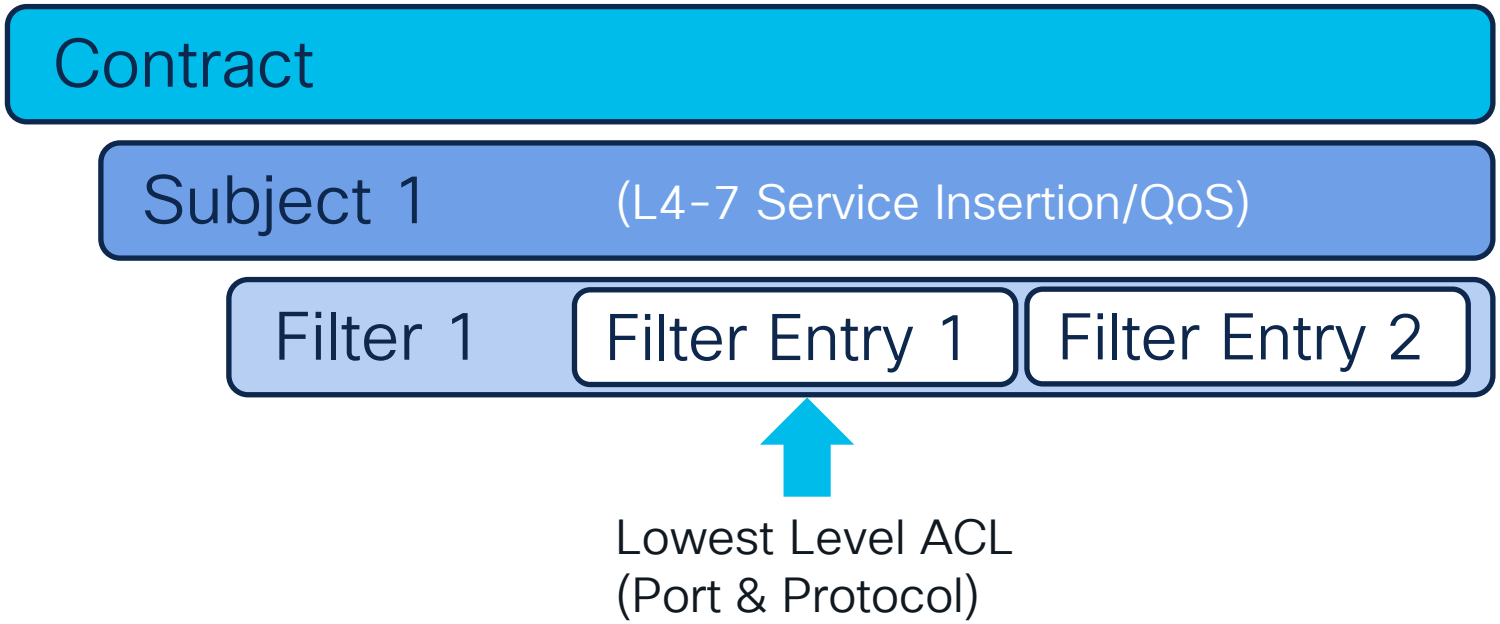
- Physical Domain (IP/MAC)
- VMM Domain (IP/MAC/VM ATTRTRIBUTE)

Contracts

Contracts Review

- Traditional access lists are built between subnets, hosts, VLANs, MACs, and applied to interfaces in a particular direction.
- ACI applies security to Endpoint Groups (EPGs) or Endpoint Security Groups (ESGs)
- Contracts use a Provider/Consumer model
- ACI is a whitelist model by default. That is, only communication which is explicitly defined will be allowed.
- Any endpoint (EP) in an ExG can communicate by default with any other endpoint inside the same ExG.
- When an EP needs to communicate to something outside of its ExG, a contract is required

Contract Structure



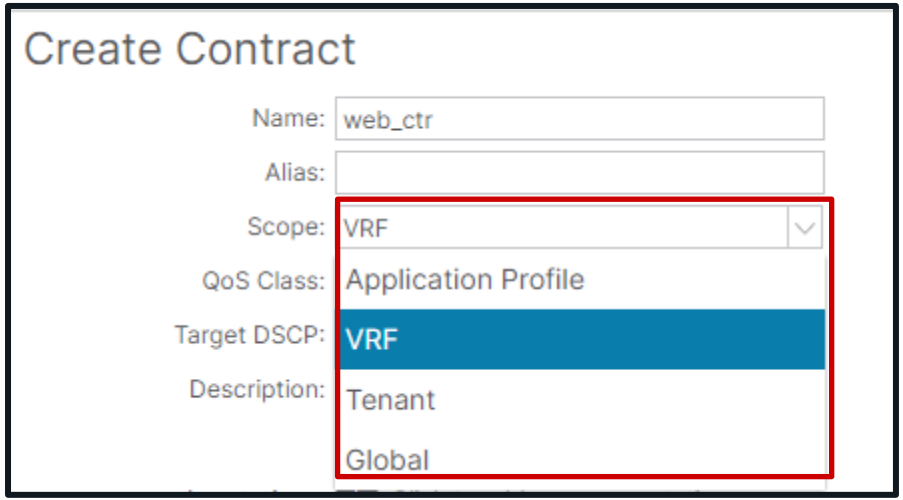
Contract Scope

- **Global** – Provider/Consumer Relationships apply across all tenants
  (required for cross-tenant communication)

- **Tenant** – Provider/Consumer Relationships restricted within tenant

- **VRF** – Provider/Consumer Relationships restricted to specific VRFs of tenants

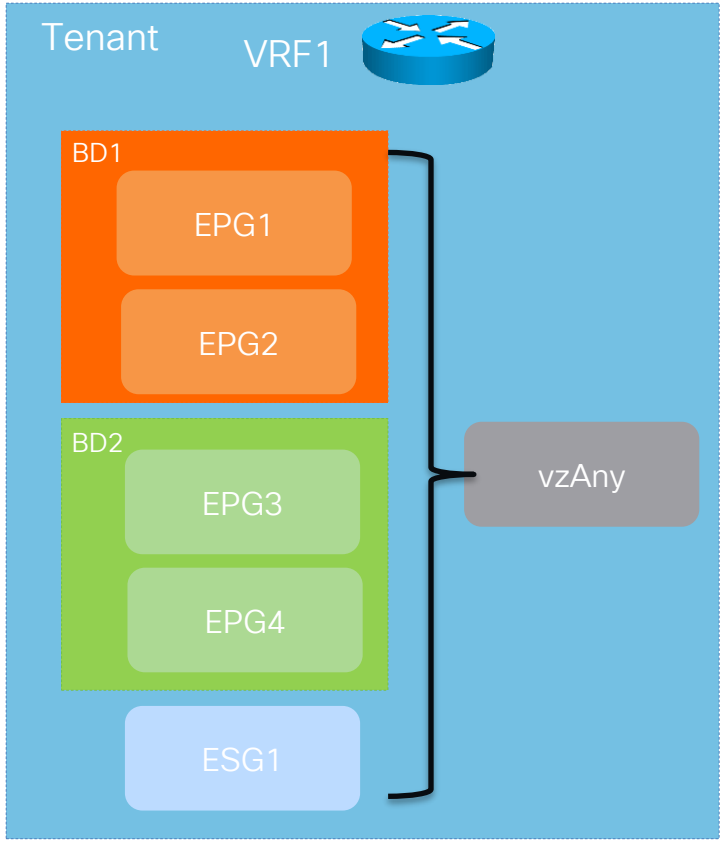
- **Application Profile** – Provider/Consumer Relationships restricted to specific AP within tenants



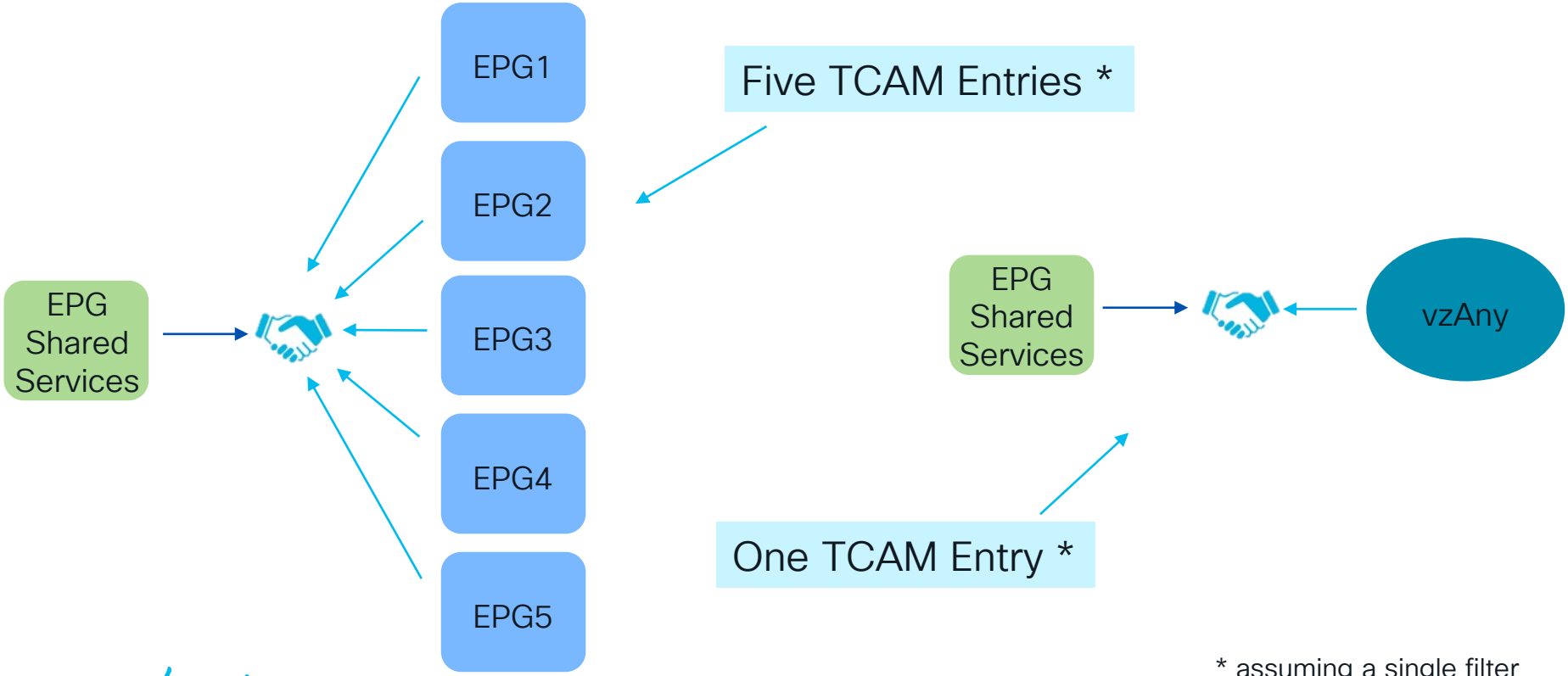
vzAny

Any ExG in VRF = vzAny

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



vzAny Example - Simplicity and TCAM Savings



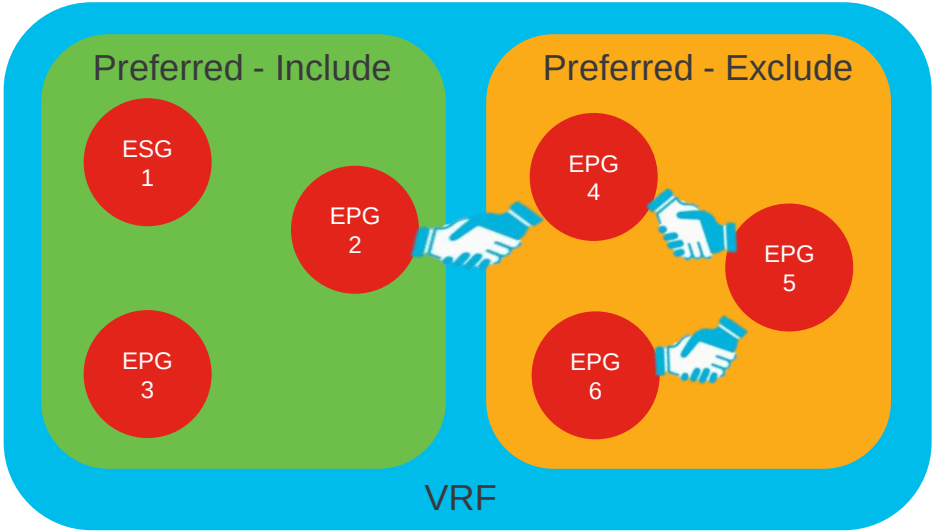
* assuming a single filter

Preferred Groups

Preferred Groups

- Allows multiple different ExGs to freely communicate without the need for contracts

ExGs in PG can talk to other ExGs in PG without requiring a contract

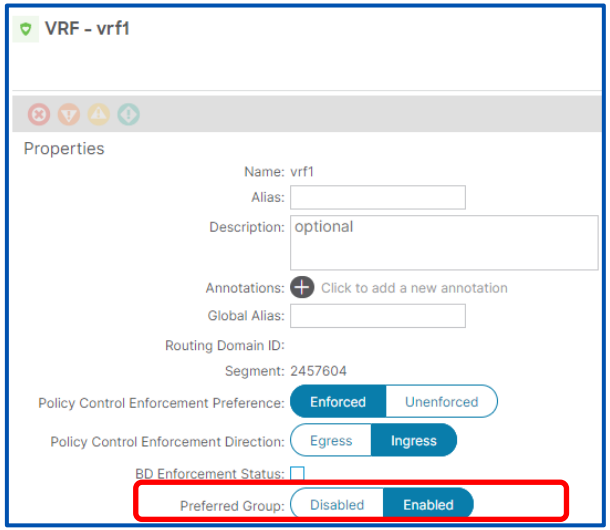


ExGs out of PG require contracts to talk to others ExG (either in or out PG)

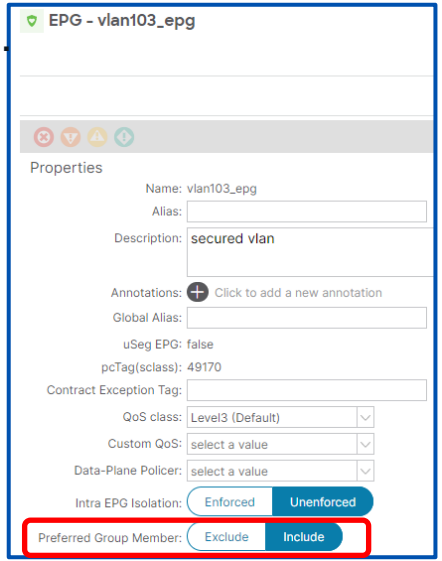
Preferred Group - Config

- Enable Preferred Group under VRF
- Include any EPG/ESG as a Preferred Group Member

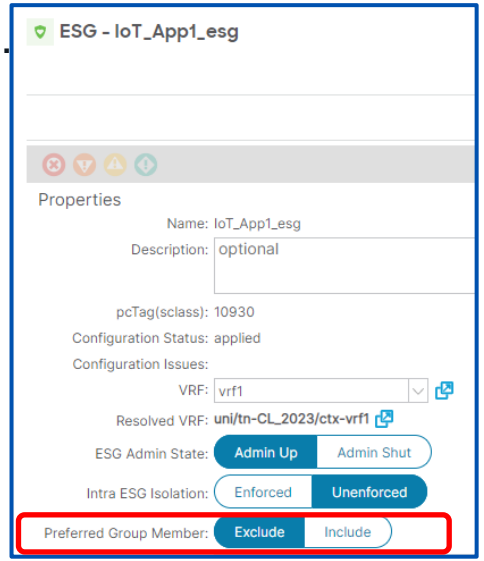
1.



2a.



2b.

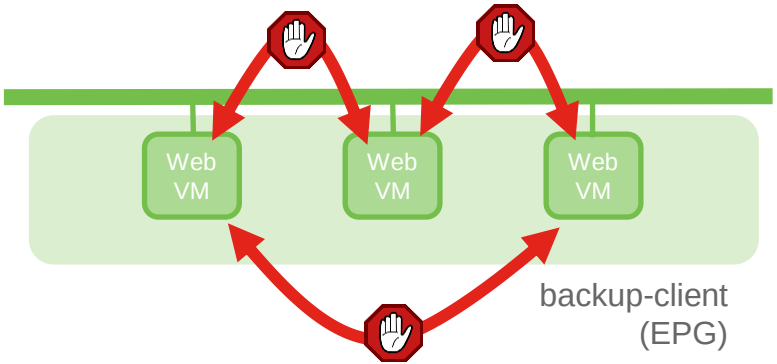


Intra-Group Isolation (ESG/EPG)

Intra-ExG isolation & Intra-ExG Contract

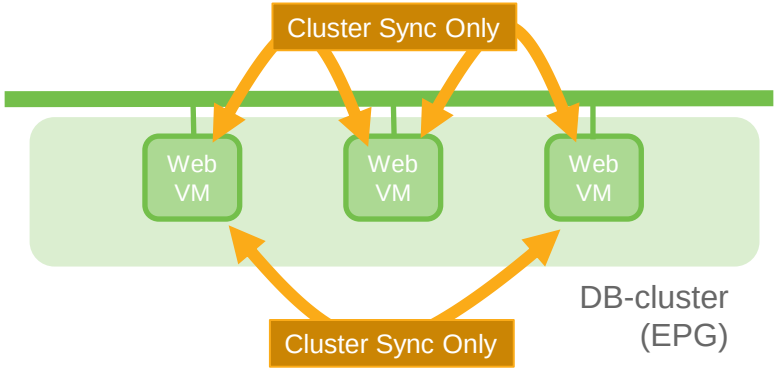
Intra Isolation

- Communication between EPs within an EPG/ESG not permitted.



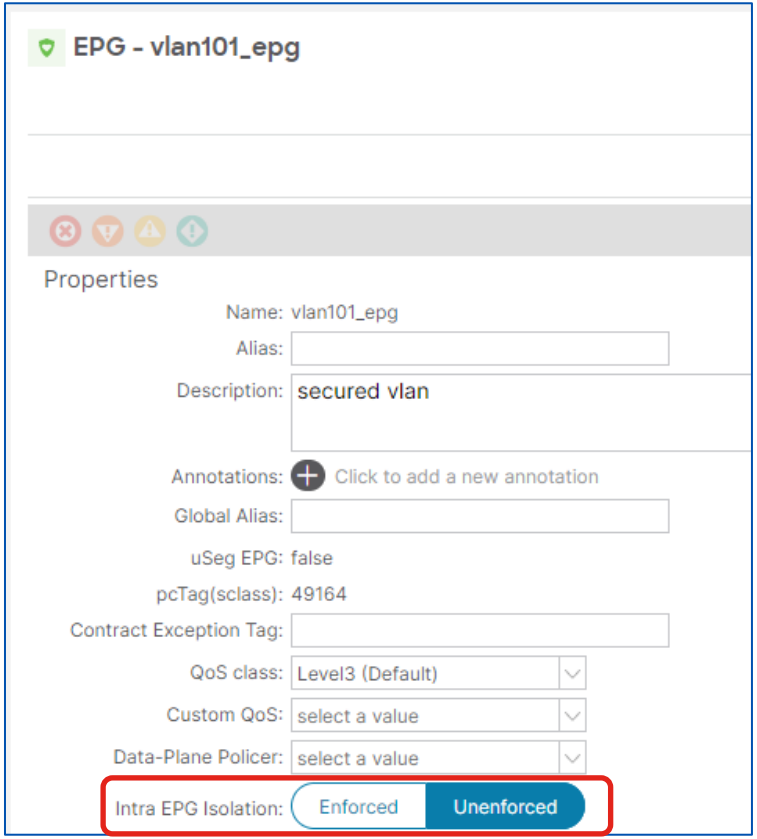
Intra Contract

- Only flows allowed in the contract are allowed between EP in EPG/ESG



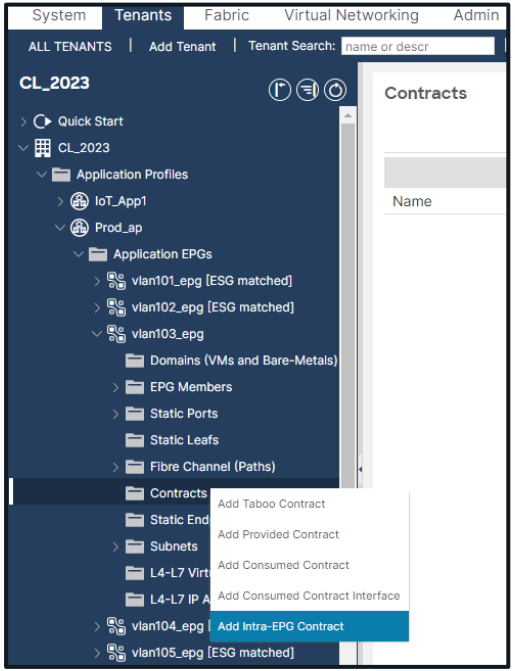
Intra-EPG Isolation

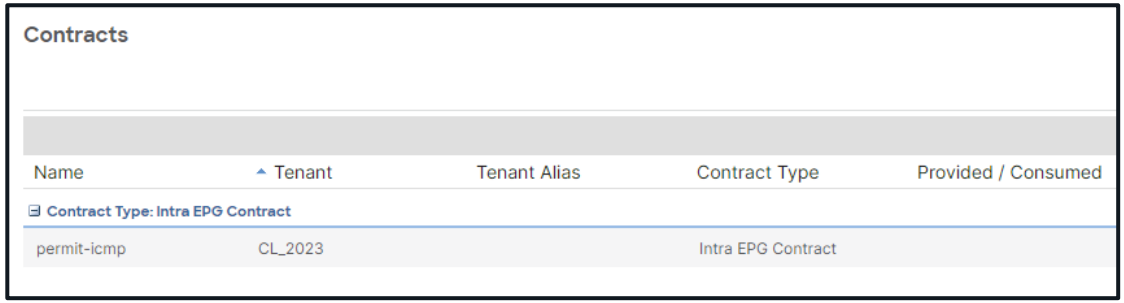
- Go to the EPG/ESG and select “Intra ExG Isolation” as enforced



Intra-EPG Contracts

- Right-click the EPG and add an “Intra-EPG Contract”





Intra-ExG Isolation & Intra-ExG Contracts

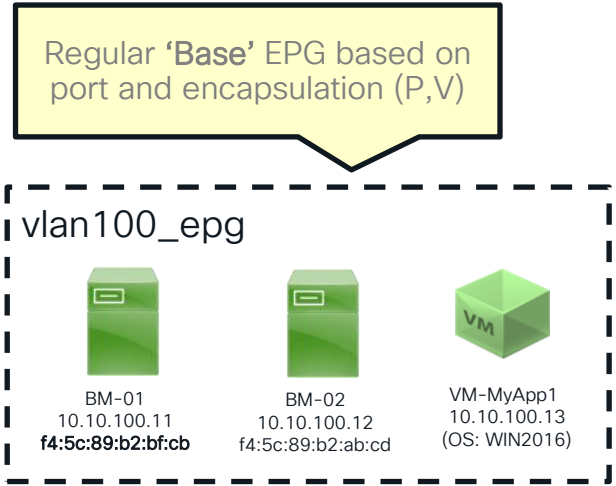
- Considerations:
  - Requires Gen2+ HW & proxy-arp
  - Supported on:
    - Physical Domains (Baremetal Endpoints)
    - VMware VMM vDS
    - Microsoft Hyper-V VMM
  - For VMM, PVLANs are leveraged
    - Same applies for baremetal with intermediate switch

    (External Switch App can automate this if using UCSM)

uSeg EPG
(Micro EPG / Microsegment EPG)

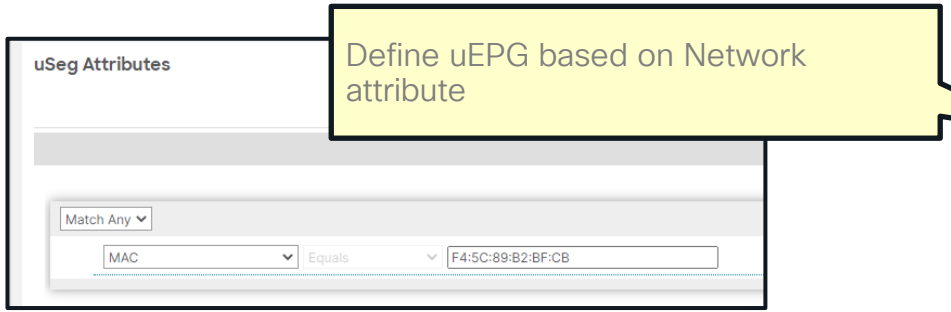
Understanding Micro EPGs

- 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**”

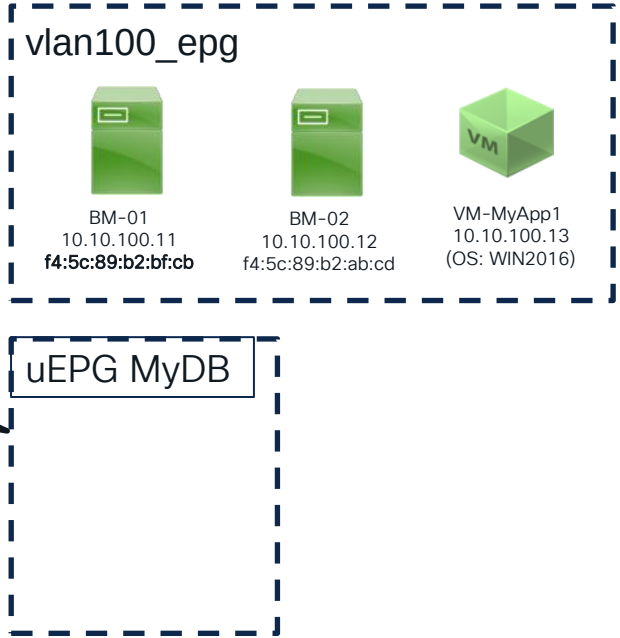


Understanding Micro EPGs

- 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**”

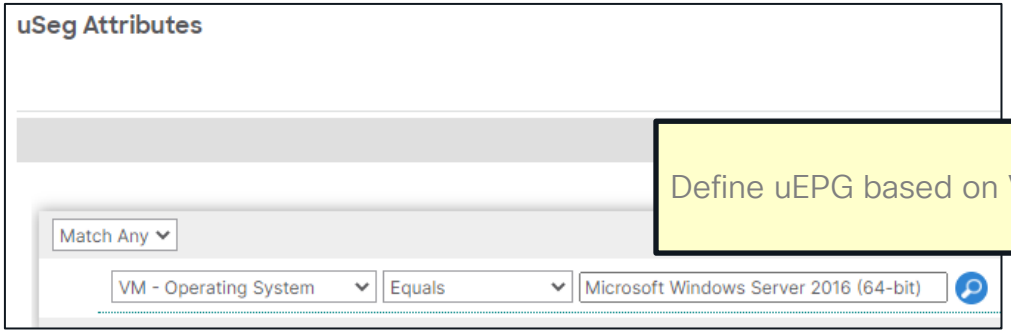


Define uEPG based on Network attribute

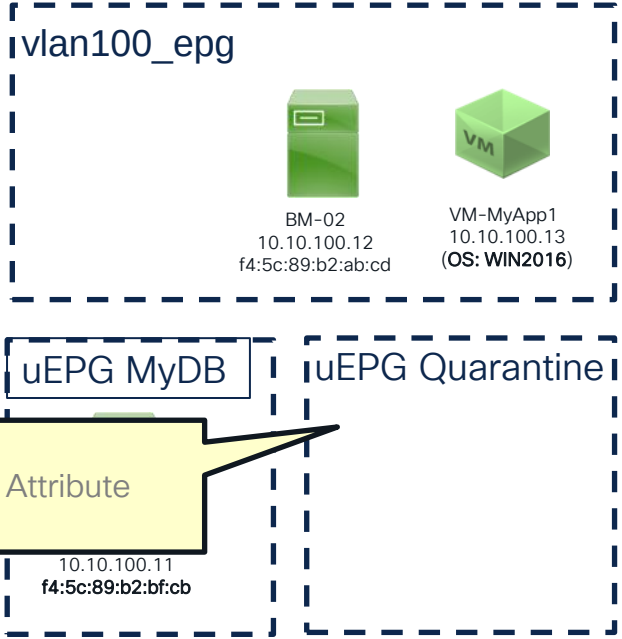


Understanding Micro EPGs

- 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 Attribute



Attributes for Micro-Segmentation

- Network-based attributes are applicable to both baremetal and VM workloads
- VM-based attributes are applicable to VM workloads only, and requires VMM integration

Network-Based
▪ IP ▪ MAC

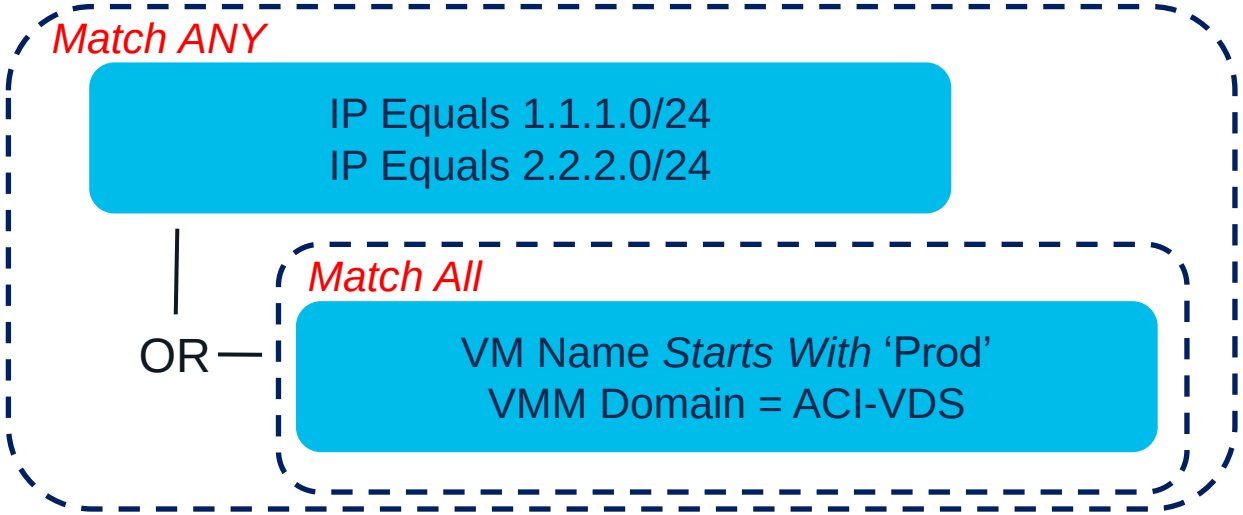
VM-Based
▪ VMM Domain ▪ Operating System ▪ Hypervisor Identifier ▪ Datacenter ▪ VM Identifier ▪ VM Name ▪ VM Folder / Folder Path ▪ vNIC DN ▪ Custom Attribute ▪ Tag

Logical Operators

- Logical operators OR/AND enable multiple rules to match various attributes.
- Rules can be combined into blocks.
- Blocks are sequentially matched using Logical Operators.

Logical Operators – Example

- Any endpoints within either subnet will be matched
- VMs within the VMM domain called ACI-VDS and who's name is prefixed with 'Prod'



Attribute Precedence

FOR REFERENCE ONLY

Attribute	Precedence
IP Sets	1
MAC Sets	2
VNIC (DN)	3
VM (ID)	4
VM Name	5
Hypervisor	6
Domain (DVS)	7
Datacenter	8
Custom Attribute	9
Guest OS	10
Tag	11

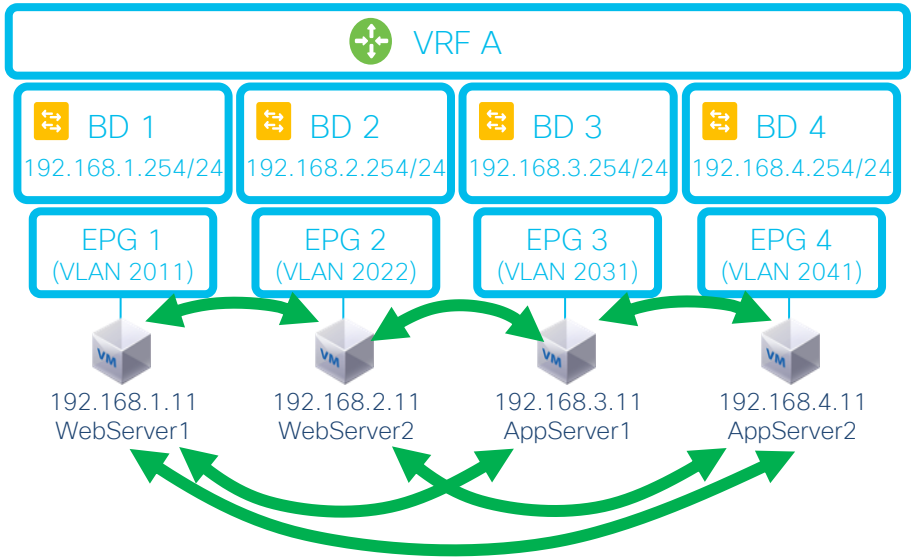
Operator	Precedence
Equals	1
Contains	2
Starts With	3
Ends With	4

- These precedence rules can be overwritten using the **EPG Match Precedence** attribute in the uEPG
  - Higher order wins

Endpoint Security Group

What is an ESG (Endpoint Security Group)?

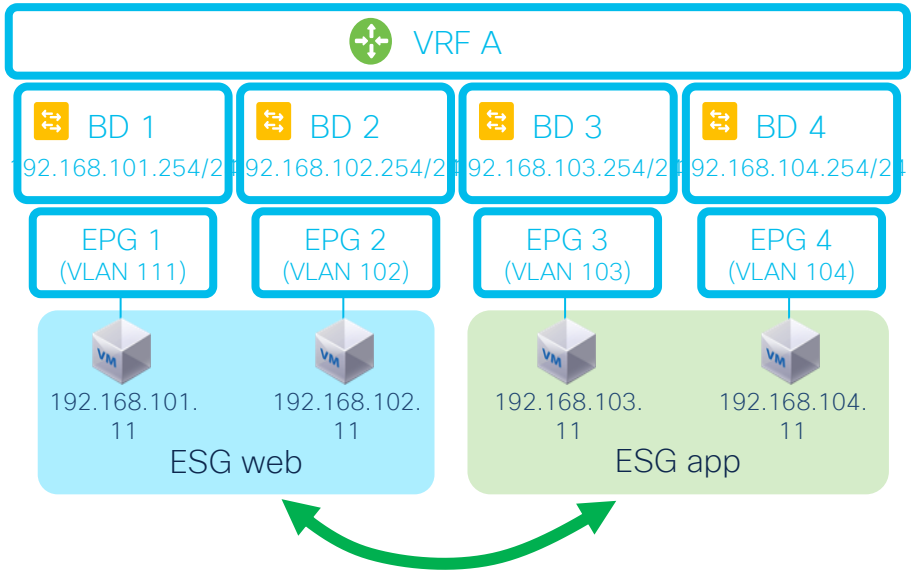
- Introduced with ACI version 5.0
- ESG is a Security Group across BDs (EPG is across VLANs, within one BD)
- Uses “EP Selectors” to classify endpoints into each



Policies Needed: 6

EPG vs. ESG

- ESG is a Security Group construct that can span BDs



Policies Needed: 1

ESG Matching

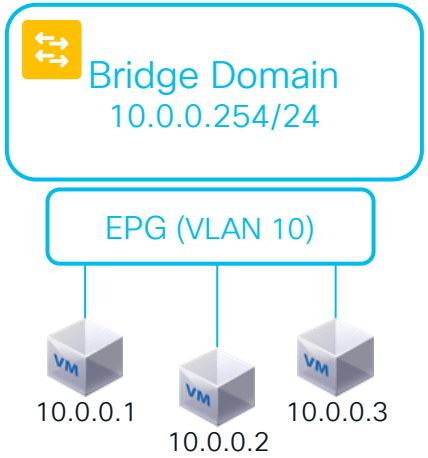
Endpoints can be classified into ESGs using a variety of attributes:

- IPv4/v6 Address or Subnets
- EPG Selector
- Policy Tags (MACs, VM tags, VM Names, Static Endpoint)

Example Design using ESGs

Network Centric

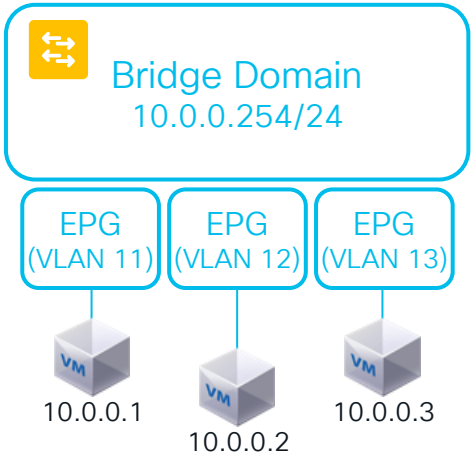
A security group in 1 subnet



Need more granular security group

Hybrid

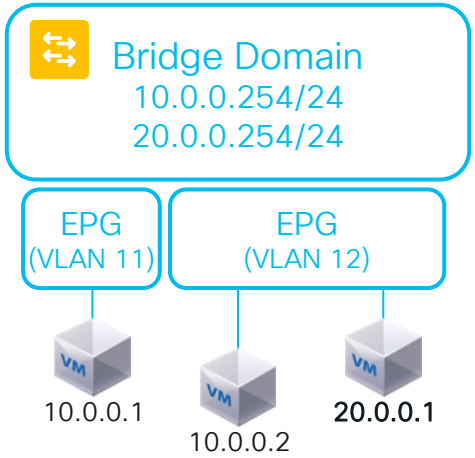
Multiple security groups in 1 subnet



What if multiple subnets need to share the same security rules?

Application Centric

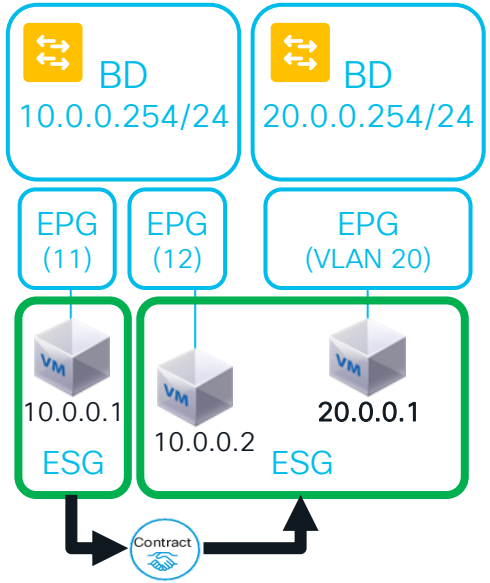
Security groups across subnets



Sharing a broadcast domain brings another security concern

Security Group (ESG)

Security groups across bridge domains



Flexible security grouping

ESG Considerations

- Security can SPAN BDs (within VRF)
  - Simpler than EPGs (i.e. per BD)
  - Great for Network Centric Deployments
- EPG is still used to bind VLANs and interfaces
  - No changes in VRF/BD/EPG from network perspective
- ESG contracts and BD subnets are deployed on all nodes where the VRF is deployed
- No automatic route leaking based on contracts
  - No more subnets under a provider EPG
  - Manual but simple route leaking config

ESG Considerations cont'd

- Only IP selector in 6.0. (/32, /128 or LPM such as /24)
  - ESG can be applied only for routed traffic
  - To prevent L2 traffic to bypass ESG security, Allow Micro-Segmentation, Intra EPG Isolation with Proxy-ARP, or Intra EPG Contract needs to be enabled on each EPG where the endpoints originally belonged to.

- No ESG <-> EPG contract/communication
  - Includes no ESG <-> uSeg EPGs as well

- vzAny or Preferred Group can be used for ESG-EPG communication

- ESG <-> L3Out_EPGs contracts are supported

ESG Contract Support Summary

FOR REFERENCE ONLY

Supported

- Contracts between:
  - ESG ⇔ ESG
  - ESG ⇔ L3Out EPG
  - ESG ⇔ inband-EPG
  - ESG ⇔ vzAny
  - ESG ⇔ service-EPG (internally created shadow EPG)

- Preferred Group
- Intra ESG Contract
- Contract Inheritance

Not Supported

- Contracts between:
  - ESG ⇔ EPG
  - ESG ⇔ uSeg EPG
  - ESG ⇔ Cloud EPG - ESGs not yet supported in NDO

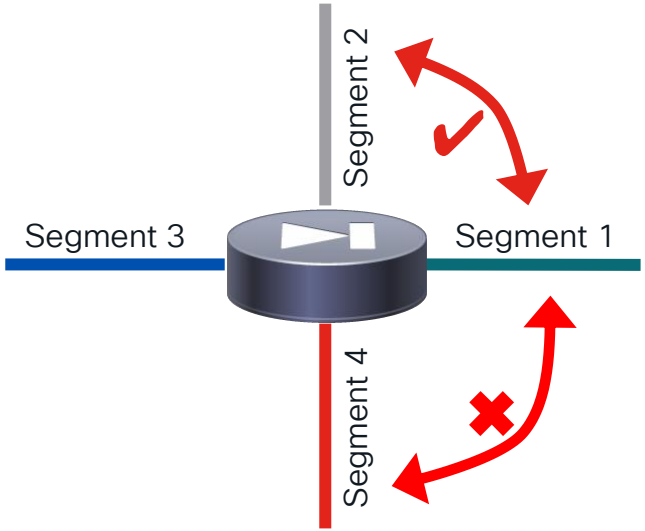
- Taboo Contracts

Note:
Any contract features that are supported in uSeg EPG are supported in ESG unless it's explicitly mentioned as not supported on the right

Application Segmentation & Putting it all together

Segmentation vs. Micro-Segmentation

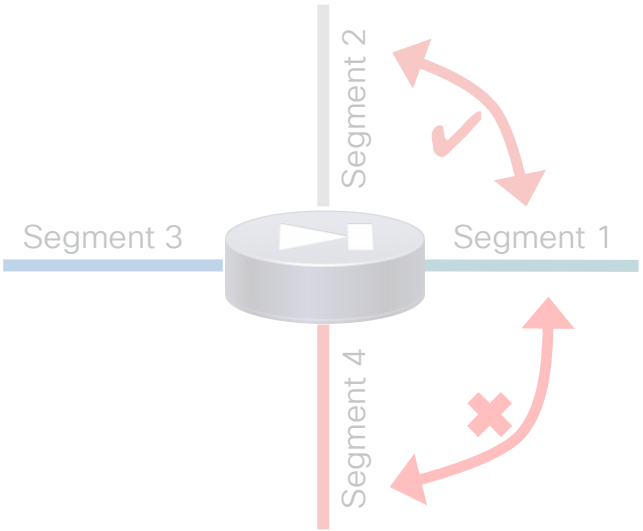
Segmentation



Segment = Broadcast domain / VLAN / Subnet

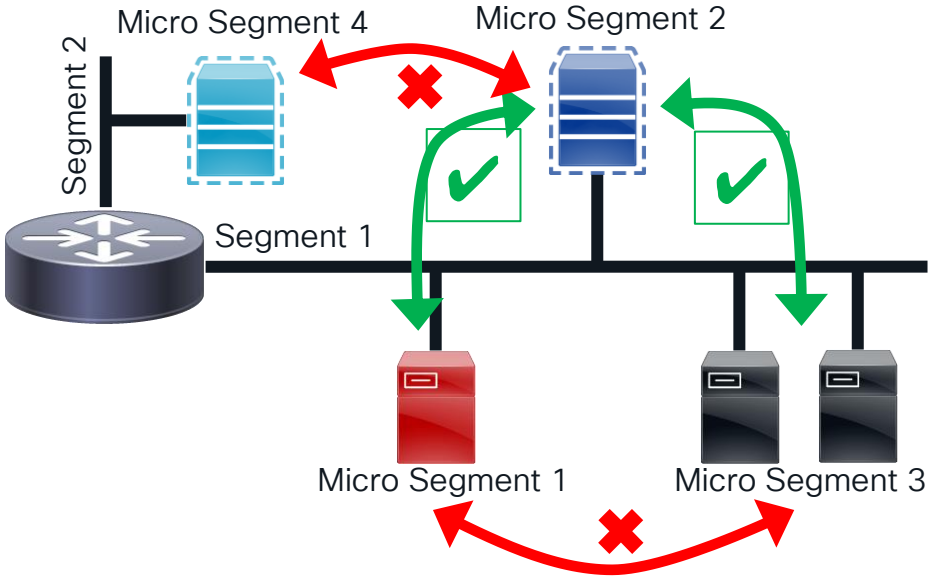
Segmentation vs. Micro-Segmentation

Segmentation



Segment = Broadcast domain / VLAN / Subnet

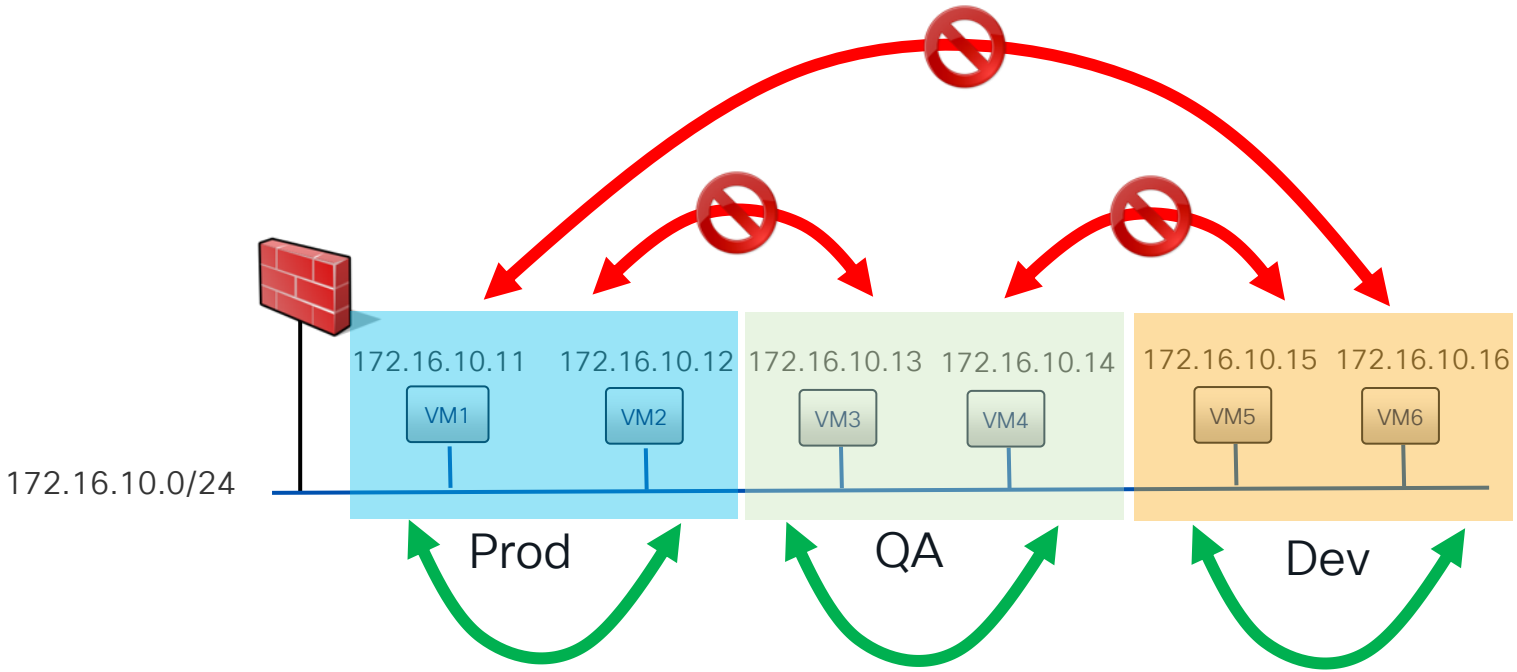
Micro Segmentation



Micro Segment = Endpoint or Group of Endpoints

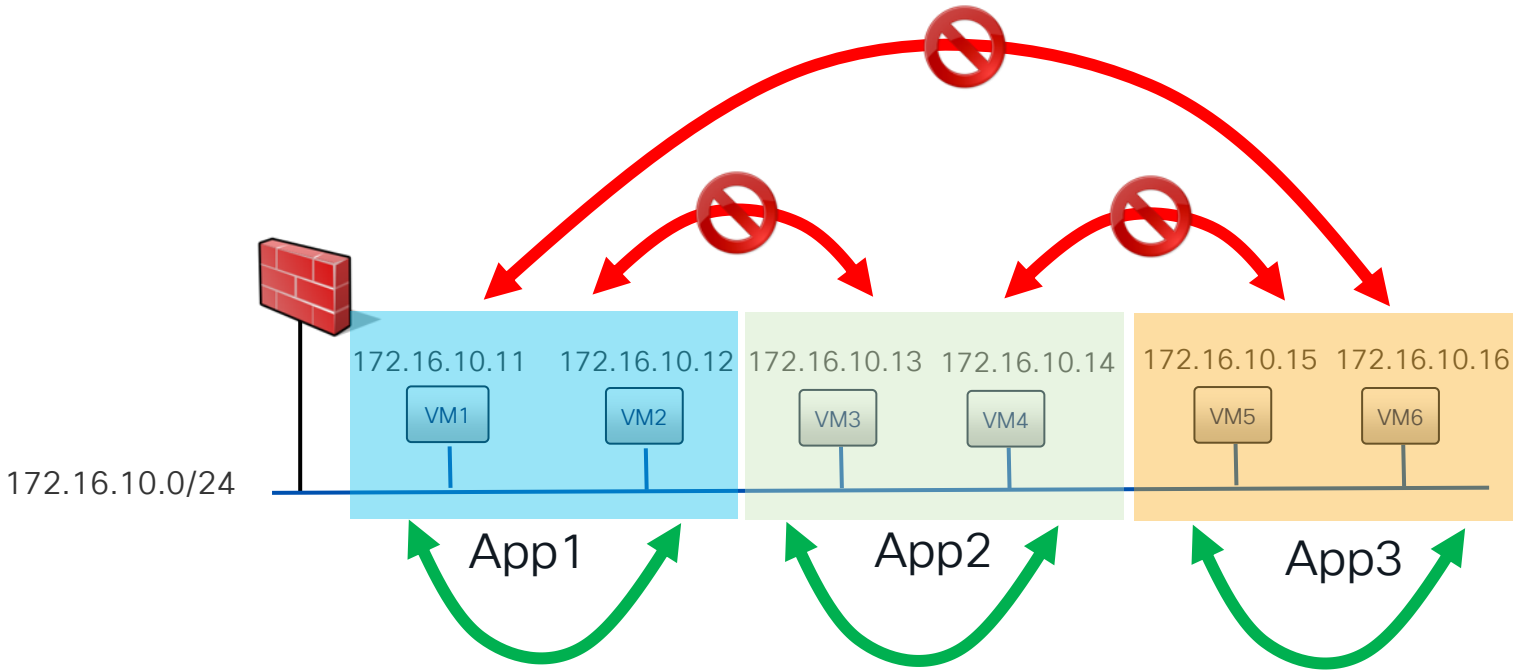
Zone Micro Segmentation

Segmentation Level: Low



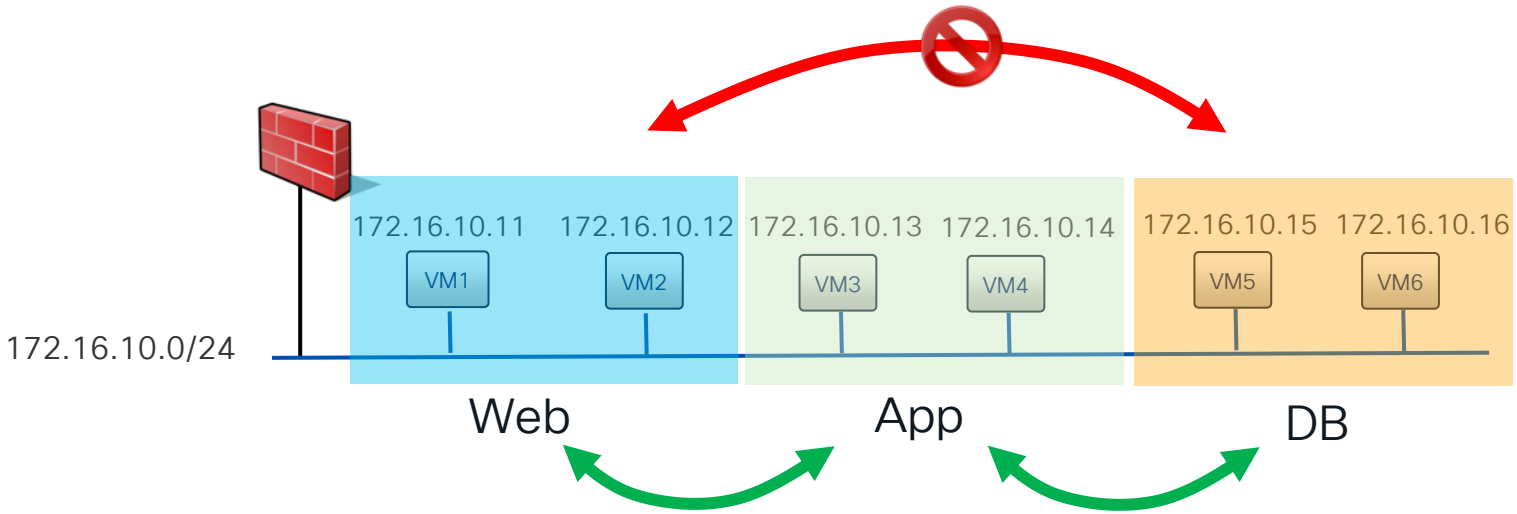
Application Segmentation

Segmentation Level: Medium

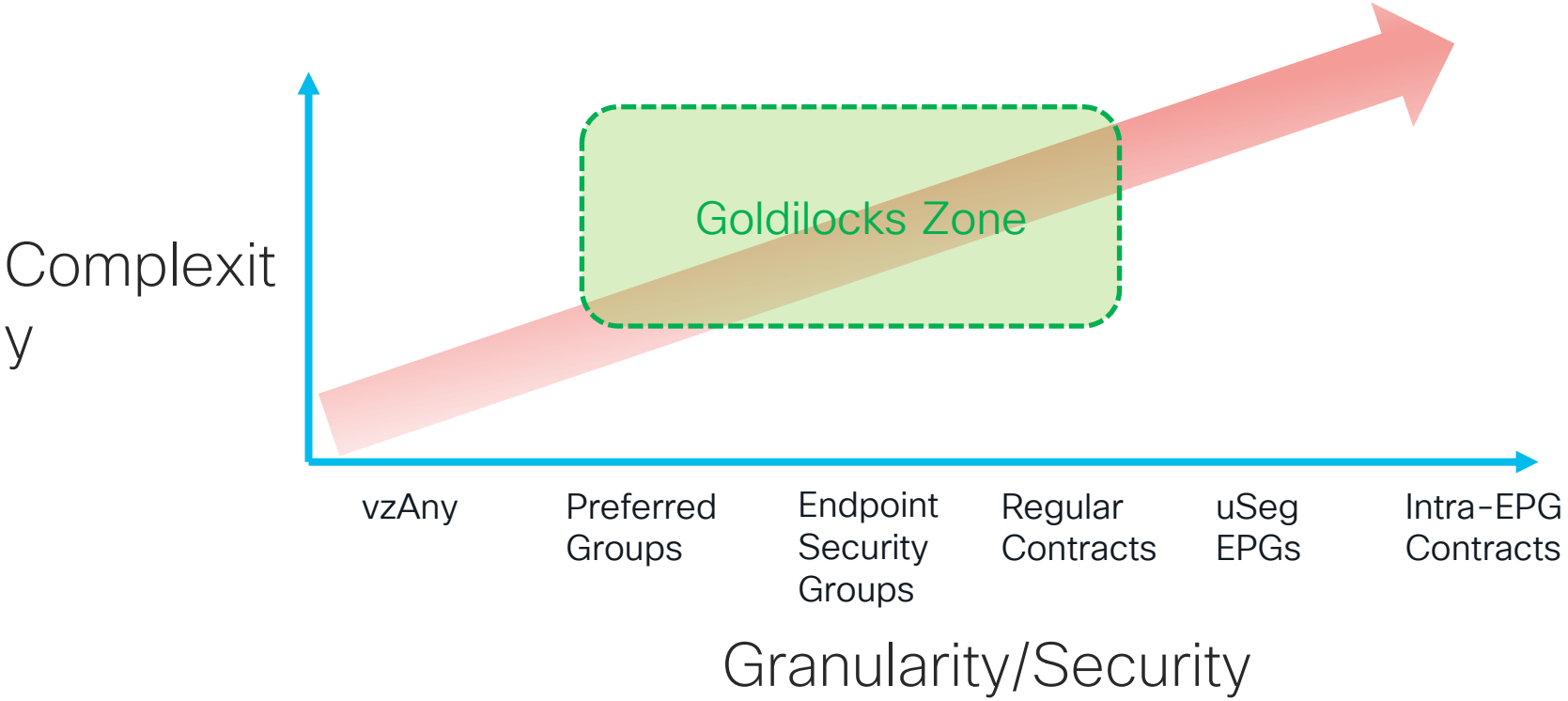


Application Tier Segmentation

Segmentation Level: High



Balancing App Segmentation vs. Complexity



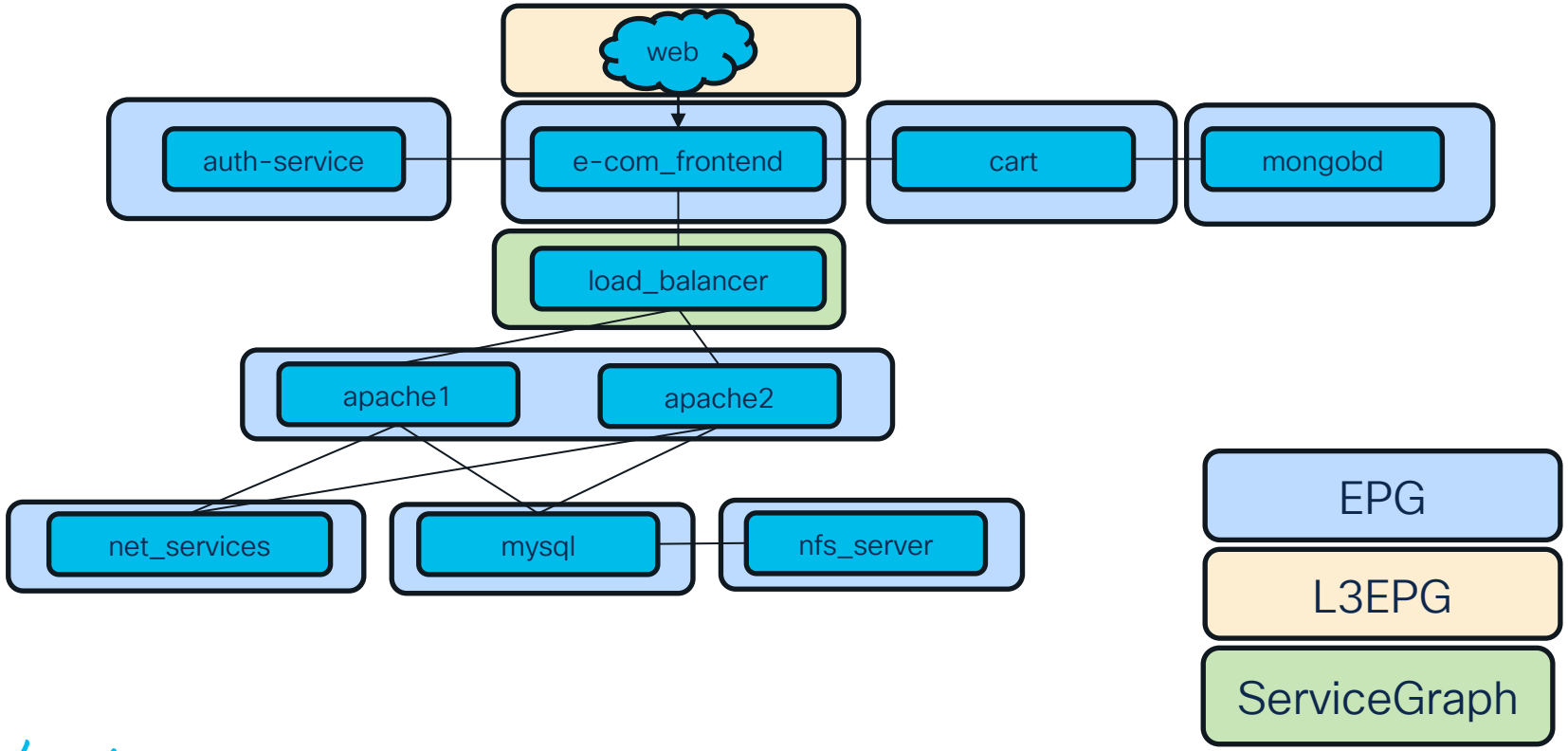
Sample Case Study

Greenfield

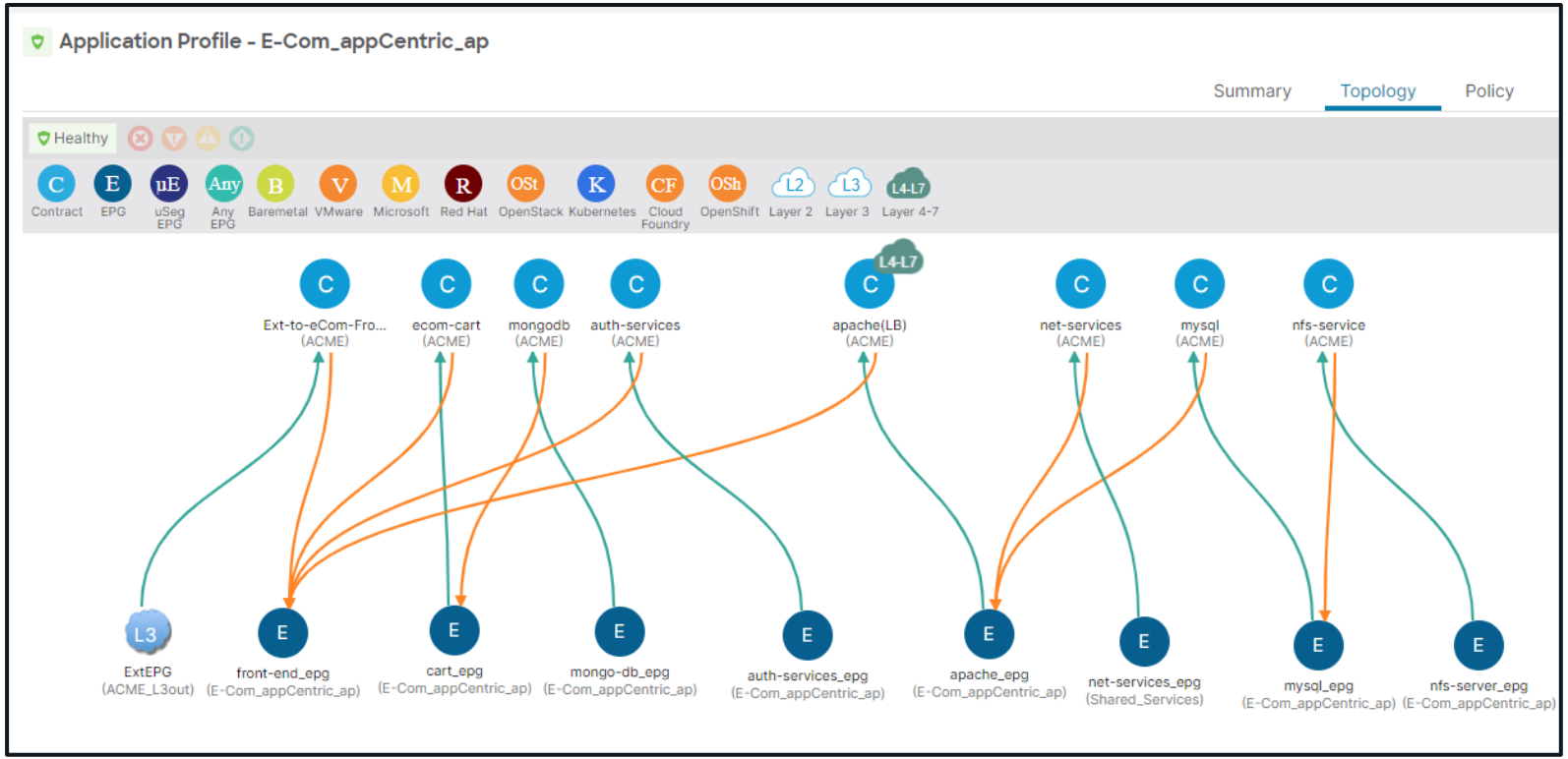
Greenfield Case Study – Acme Inc.

- Acme Inc the industry leading seller of Anvils
- They are planning on deploying a net-new Application for their e-commerce site and wish to do so using an Application Centric approach.
- The application tiers are well understood as are the communication requirements between the tiers.
- The CIO has requested a maximum focus on Segmentation & Security
- New IPs/Subnets will be allocated for the new application endpoints which will be a mix of baremetal & virtual endpoints.

Acme Inc. e-Com Application – EPG Deployment



Acme Inc. e-Com Application – EPG Deployment

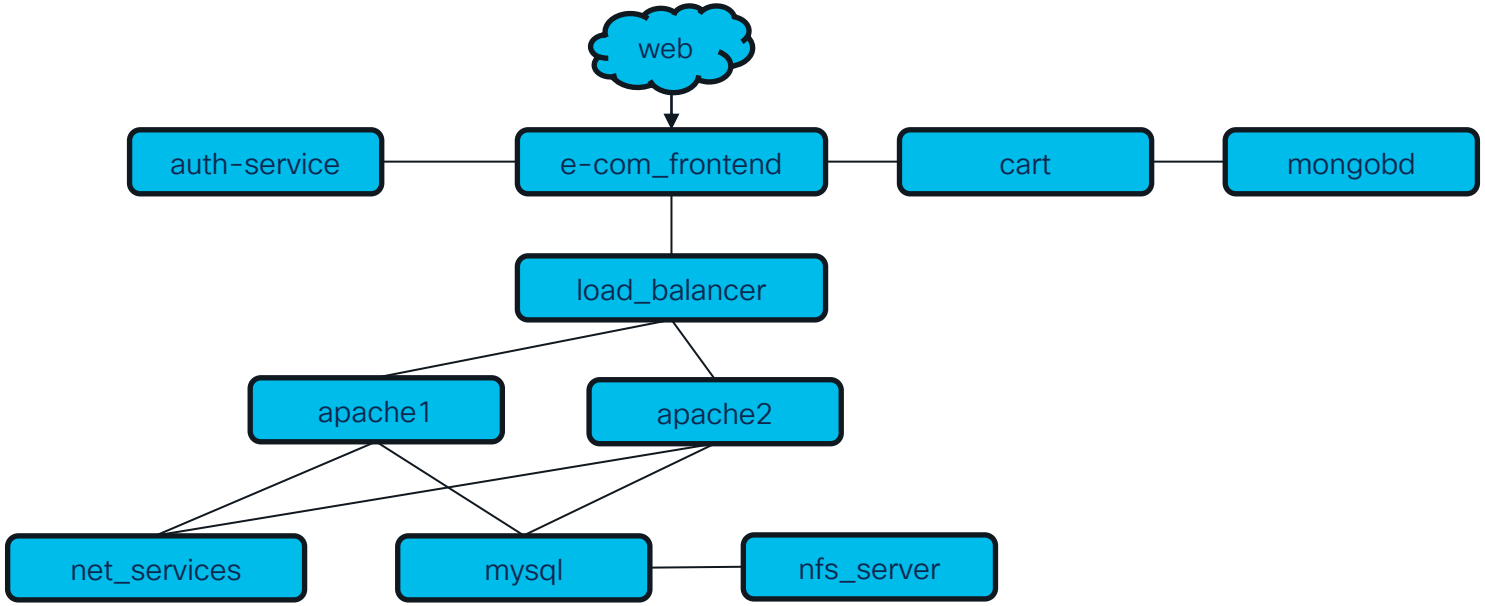


Brownfield

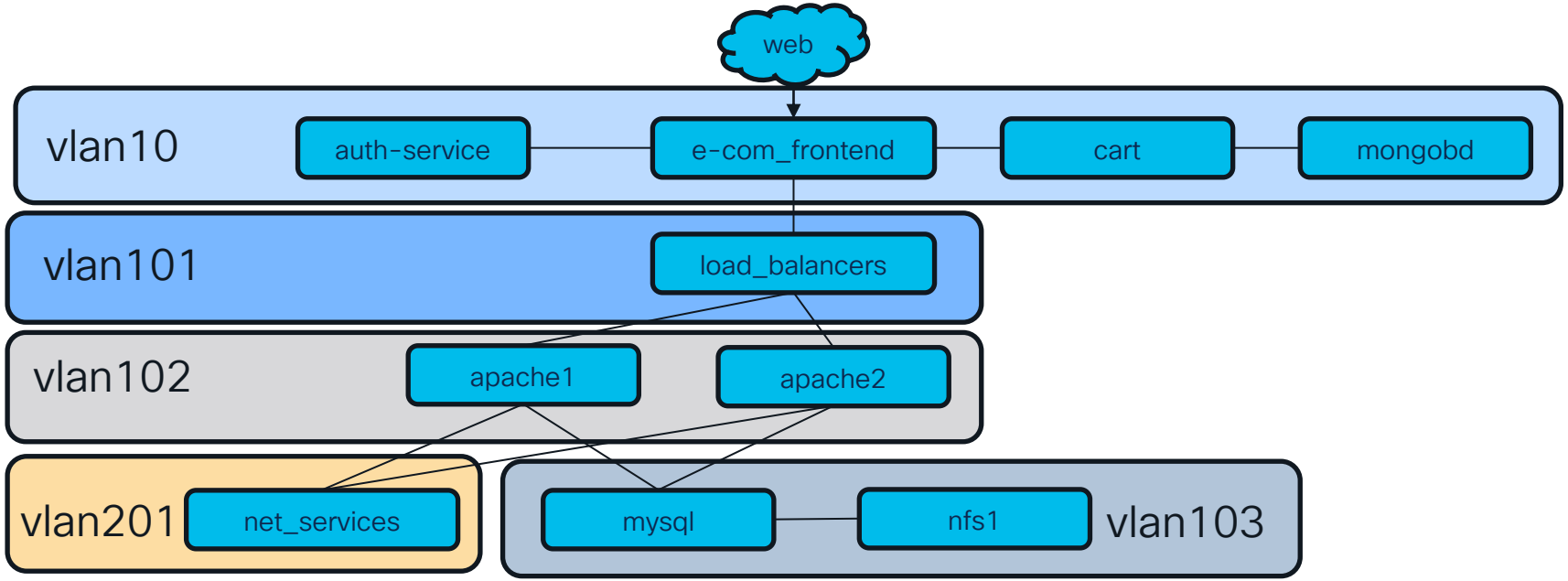
Brownfield Case Study – Acme Inc.

- Acme Inc the industry leading seller of Anvils
- They have deployed ACI in a network Centric manner and wish to apply better security starting with their e-Com application
- The application tiers are well understood, but the specific communication rules between the tiers are not.
- ACME's Ops team have limited cycles and wish to limit any increased complexity any design changes may involve.
- They must not impact any existing applications

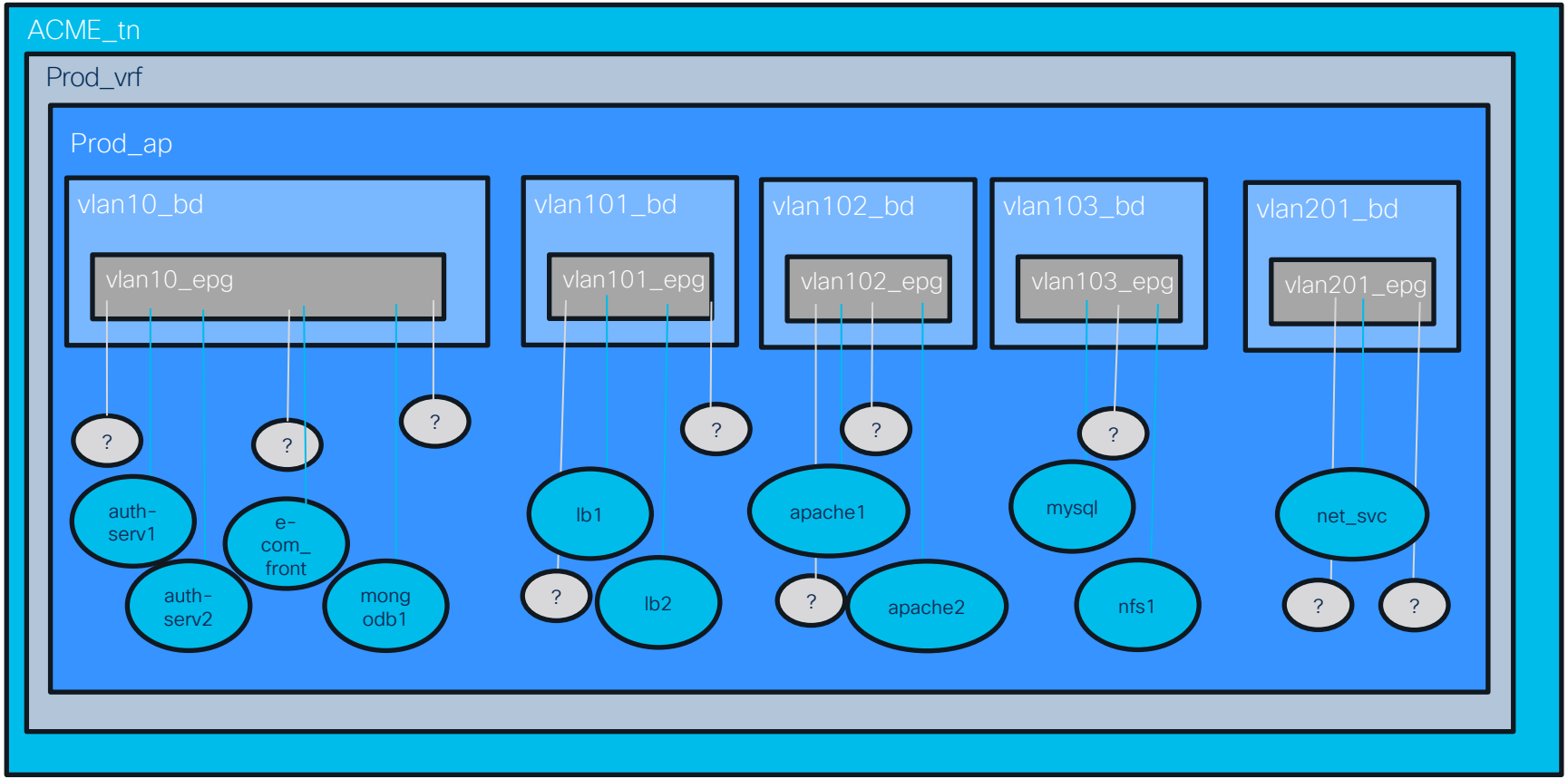
Acme Inc. e-Com Application Summary



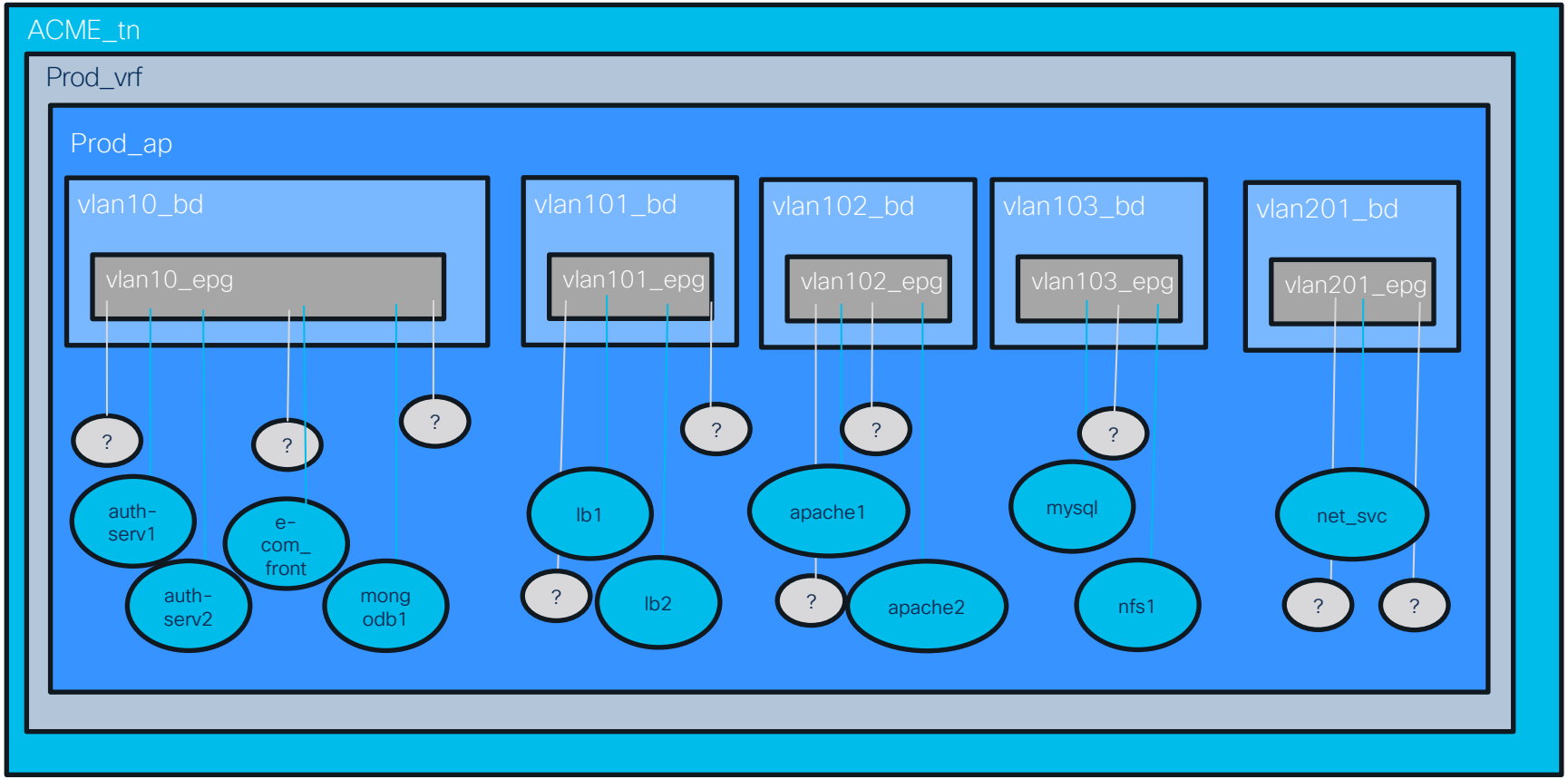
Acme Inc. e-Com Application Summary



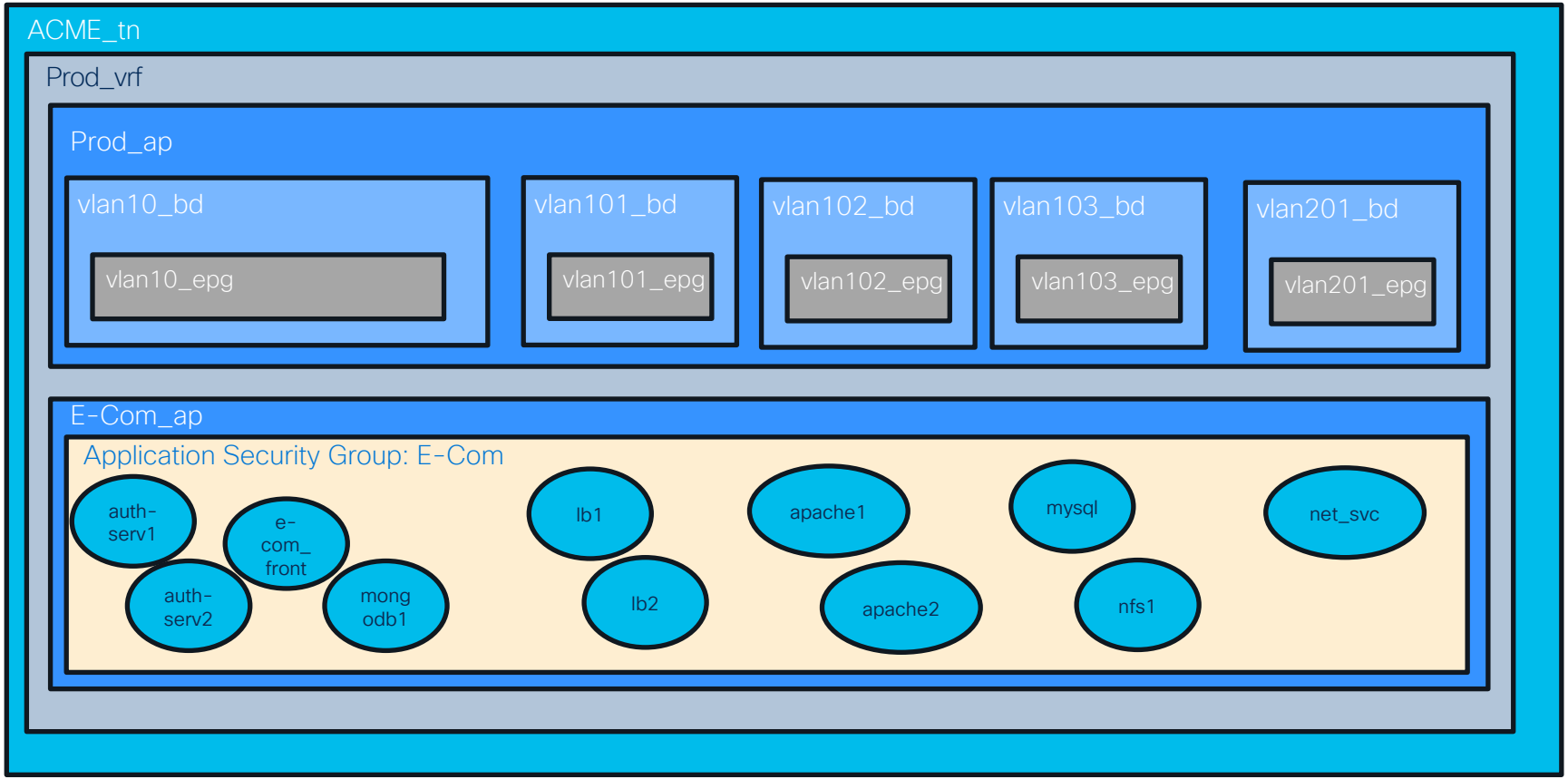
Acme Inc. e-Com App on ACI



Acme Inc. e-Com App on ACI



Acme Inc. e-Com App on ACI

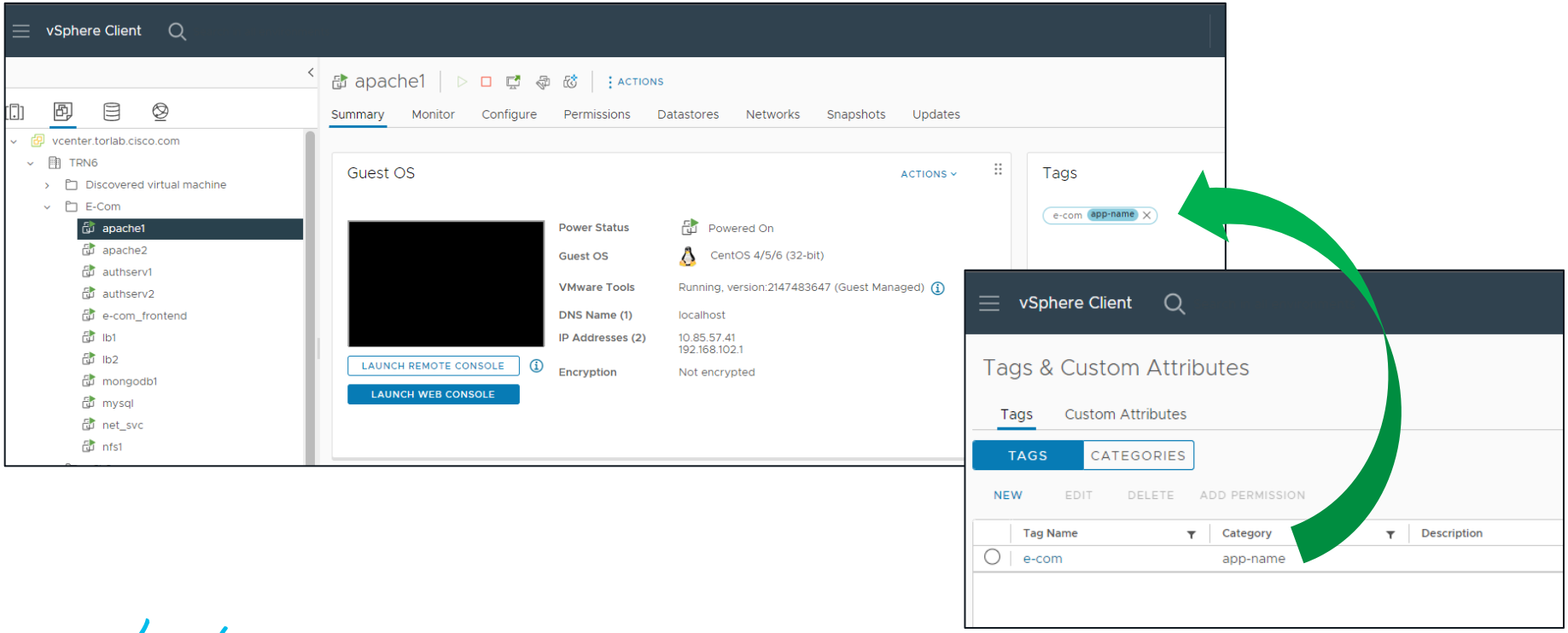


Brownfield Migration of Net-Centric Apps to ESGs

1. Create new application-specific App Profile
2. Create ESG named as App, bind to appropriate VRF
3. Apply Contract between ESG and L3out (for external connectivity)
4. Create Selectors for ESG
   - For VMs, you can use VM Tags, VM Names, VM Folders etc
   - For baremetal & VMs you can use MAC or IP (LPM) selectors
5. Enable “Allow for uSeg” on Base EPG VMM Domain binding

vCenter View

Tag & Category Assignment



ACI View 1 of 5

VMM Domain – Tag Collection

APIC (DCVLab-ACI-Fab1)

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

Kubernetes | Rancher RKE | OpenShift | OpenStack | Microsoft | Red Hat | VMware | VMware SDN

VMware

- VMware
  - ACI_vDS
    - Controllers
      - DCVLab_VC
        - Tags
        - Hypervisors
        - DVS - ACI_vDS
    - Custom Trunk Port Groups
    - Trunk Port Groups

Domain - ACI_vDS

Properties

Name: ACI_vDS

Virtual Switch: Distributed Switch

Associated Attachable Entity Profiles: Name

lab_aep

Encapsulation: VLAN

Configure Infra Port Groups: ☐

To configure port groups for virtual apic

Delimiter:

Enable Tag Collection: ☑

Enable VM folder Data Retrieval (Beta): ☑

Access Mode: Read Only Mode | Read Write Mode

Endpoint Retention Time (seconds): 0

VLAN Pool: DCVLab_VMM(dynamic)

APIC (DCVLab-ACI-Fab1)

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

Kubernetes | Rancher RKE | OpenShift | OpenStack | Microsoft | Red Hat | VMware | VMware SDN

VMware

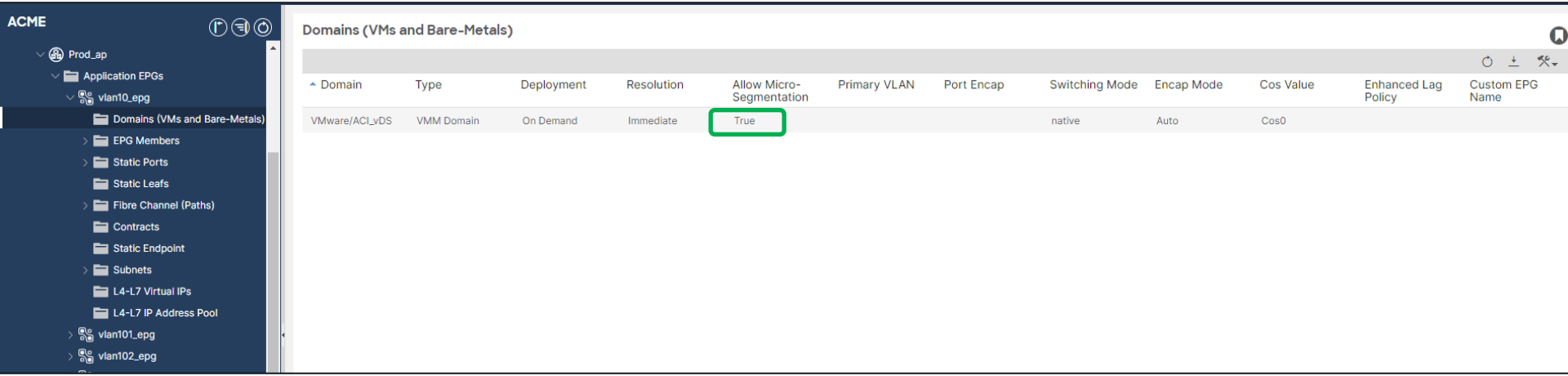
- VMware
  - ACI_vDS
    - Controllers
      - DCVLab_VC
        - Tags
        - Hypervisors
        - DVS - ACI_vDS
    - Custom Trunk Port Groups
    - Trunk Port Groups

Categories and Tags

Name
app-name
e-com

ACI View 2 of 5

Base EPGs VMM Domain Binding



ACI View 3 of 5

ESG – Tag Selector

ACME

- Quick Start
- ACME
  - Application Profiles
    - E-Com_ap
      - Application EPGs
      - uSeg EPGs
      - Endpoint Security Groups
        - E-Com_esg
          - Contracts
          - Selectors
            - Tag Selectors
            - EPG Selectors
            - IP Subnet Selectors
            - Service EPG Selectors
    - Prod_ap
      - Application EPGs
        - vlan10_epg
          - Domains (VMs and Bare-Metals)

Tag Selectors

Tag Key	Value Operator	Tag Value
app-name	Contains	e-com

vSphere Client

Tags & Custom Attributes

Tags | Custom Attributes

TAGS | CATEGORIES

NEW | EDIT | DELETE | ADD PERMISSION

Tag Name	Category	Description
e-com	app-name	

ACI View 4 of 5

Base EPG – Learned Endpoints

ACME

- Prod_ap
  - Application EPGs
    - vlan10_epg
      - Domains (VMs and Bare-Metals)
      - EPG Members
      - Static Ports
      - Static Leafs
      - Fibre Channel (Paths)
      - Contracts
      - Static Endpoint
      - Subnets
      - L4-L7 Virtual IPs
      - L4-L7 IP Address Pool
    - vlan101_epg
    - vlan102_epg
    - vlan103_epg
    - vlan201_epg
  - uSeg EPGs
  - Endpoint Security Groups
- Networking

EPG - vlan10_epg

Summary | Policy | Operational | Stats | Health | Faults | History | Policy Viewer

Client Endpoints | Configured Access Policies | Contracts | Controller End-Points | Deployed Leaves

Healthy

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface (learned)	Encap	ESG	Policy Tags
00:50:56:A4:19:22	authserv1	learned vmm	hxafm5-esx-2.torlab.cisco....	DCVLab_VC	Pod-1/Node-101-102/UCS-FIB (learned)	vlan-236(P) vlan-237(S)	ACME:E-Com_ap:E-Com_esg	__vmm::vmname authserv1 app-name e-com
192.168.10.1							ACME:E-Com_ap:E-Com_esg	
00:50:56:A4:32:0F	mongodb1	learned vmm	hxafm5-esx-3.torlab.cisco....	DCVLab_VC	Pod-1/Node-101-102/UCS-FIA (learned)	vlan-236(P) vlan-237(S)	ACME:E-Com_ap:E-Com_esg	__vmm::vmname mongodb1 app-name e-com
192.168.10.4							ACME:E-Com_ap:E-Com_esg	
00:50:56:A4:43:8E	e-com_frontend	learned vmm	hxafm5-esx-2.torlab.cisco....	DCVLab_VC	Pod-1/Node-101-102/UCS-FIA (learned)	vlan-236(P) vlan-237(S)	ACME:E-Com_ap:E-Com_esg	__vmm::vmname e-com_front app-name e-com
192.168.10.3							ACME:E-Com_ap:E-Com_esg	
00:50:56:A4:89:84	authserv2	learned vmm	hxafm5-esx-2.torlab.cisco....	DCVLab_VC	Pod-1/Node-101-102/UCS-FIB (learned)	vlan-236(P) vlan-237(S)	ACME:E-Com_ap:E-Com_esg	__vmm::vmname authserv2 app-name e-com
192.168.10.2							ACME:E-Com_ap:E-Com_esg	

ACI View 5 of 5

ESG – Matched Endpoints

ACME

- Quick Start
- ACME
  - Application Profiles
    - E-Com_ap
      - Application EPGs
      - uSeg EPGs
      - Endpoint Security Groups
        - E-Com_esg
          - Contracts
          - Selectors
            - Tag Selectors
            - EPG Selectors
            - IP Subnet Selectors
            - Service EPG Selectors
    - Prod_ap
  - Networking
  - Contracts
  - Policies

ESG - E-Com_esg

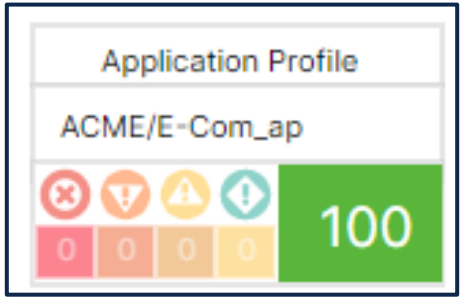
Summary | Policy | Operational | Health | Faults | History

Client Endpoints | Contracts | Deployed Leaves | Tag Selectors

Healthy

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface (learned)	Encap	Base EPG	Policy Tags
00:50:56:A4:2C:24	mysql	vmm	hxafm5-esx-2.torlab.cisco.com	DCVLab_VC	---	vlan-241(P) vlan-244(S)	ACME:Prod_ap:vlan103_epg	__vmm::vmname **mysql** app-name **e-com**
00:50:56:A4:4C:3E	lb2	vmm	hxafm5-esx-2.torlab.cisco.com	DCVLab_VC	---	vlan-235(P) vlan-243(S)	ACME:Prod_ap:vlan101_epg	__vmm::vmname **lb2** app-name **e-com**
00:50:56:A4:6C:8A		learned vmm			Pod-1/Node-101-102/UCS-FIA ...	vlan-213(P) vlan-214(S)	ACME:Prod_ap:vlan102_epg	__vmm::vmname **apache1** app-name **e-com**
192.168.102.1							ACME:Prod_ap:vlan102_epg	
00:50:56:A4:6D:F3	net_svc	learned vmm	hxafm5-esx-2.torlab.cisco.com	DCVLab_VC	Pod-1/Node-101-102/UCS-FIB ...	vlan-238(P) vlan-239(S)	ACME:Prod_ap:vlan201_epg	__vmm::vmname **net_svc** app-name **e-com**
192.168.201.1							ACME:Prod_ap:vlan201_epg	
00:50:56:A4:7E:D5	lb1	vmm	hxafm5-esx-3.torlab.cisco.com	DCVLab_VC	---	vlan-235(P) vlan-243(S)	ACME:Prod_ap:vlan101_epg	__vmm::vmname **lb1** app-name **e-com**
00:50:56:A4:19:22	authserv1	learned vmm	hxafm5-esx-2.torlab.cisco.com	DCVLab_VC	Pod-1/Node-101-102/UCS-FIB ...	vlan-236(P) vlan-237(S)	ACME:Prod_ap:vlan10_epg	__vmm::vmname **authserv1** app-name **e-com**
192.168.10.1							ACME:Prod_ap:vlan10_epg	

Result



- Application-Level Health Visibility
- Application Segmentation – Increased Security
- No changes to legacy EPG mappings/VM Port Groups
- Optimized Policy TCAM
- Potential reduction of load on external FWs
- Ability to further segment Application into ‘tiers’

Key Takeaways

- Better Segmentation of Applications will reduce exposure to lateral attacks
- ACI offers varying degrees and options for securing applications
- Any level of improved security is invaluable
- Application Centric Design is a journey, get started today!

In 2022, there were an average of 7 breach notices issued each business day

Let’s ensure your business never has to issue one

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

cisco Live!

Let's go