

The background features a vibrant, multi-colored abstract design. On the left, there are overlapping, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

# Introduction to ACI

Chris Merkel – DC TSA – CCIE 17841  
BRKDCN-1601



#CiscoLive

# 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-1601>

# Agenda

- Fabric Basics
- Policy Model
- Architectural Deployments
- Day 2 and beyond
- Conclusion

# Fabric Basics

# ACI: One Network, any location





## ACI Anywhere

Edge / Remote

Core Data Centers

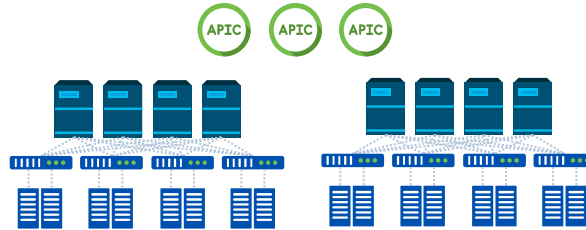
Hybrid Cloud & Multicloud

IP WAN

IP WAN



ACI  
Remote Leaf



ACI  
Single-POD      ACI  
Multi-POD



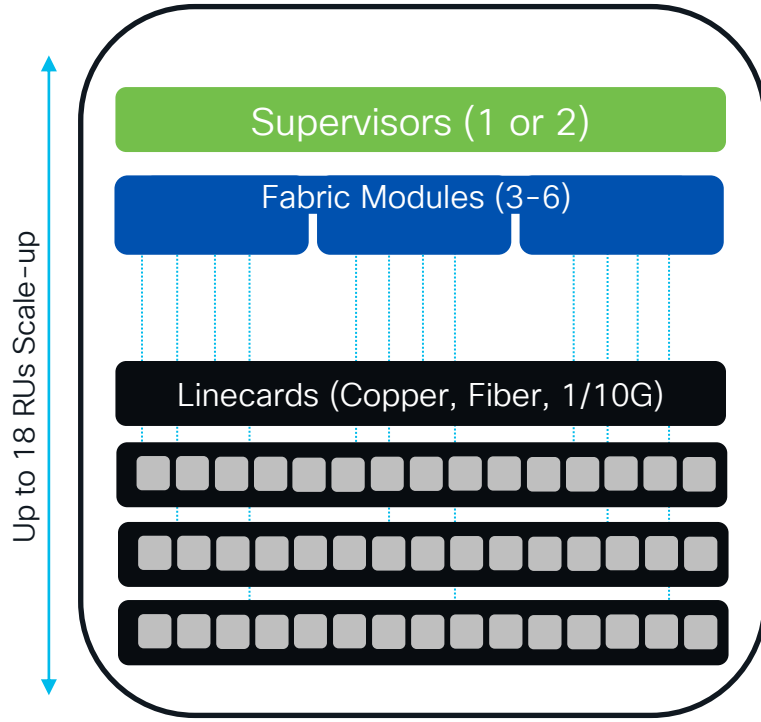
ACI  
Multisite

Cloud  
ACI

The easiest Data Center and Cloud Interconnect Solution in the Market

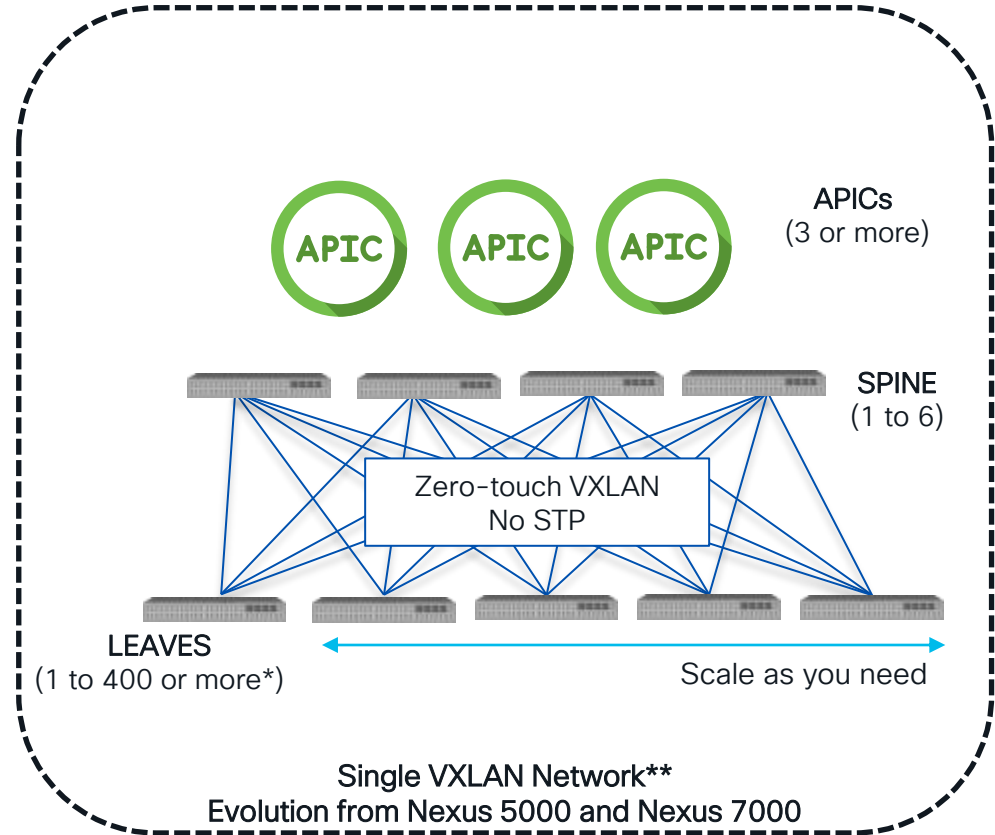
Try it today!

## The DC network before Classic modular switching



Single chassis (e.g. Nexus 7000)

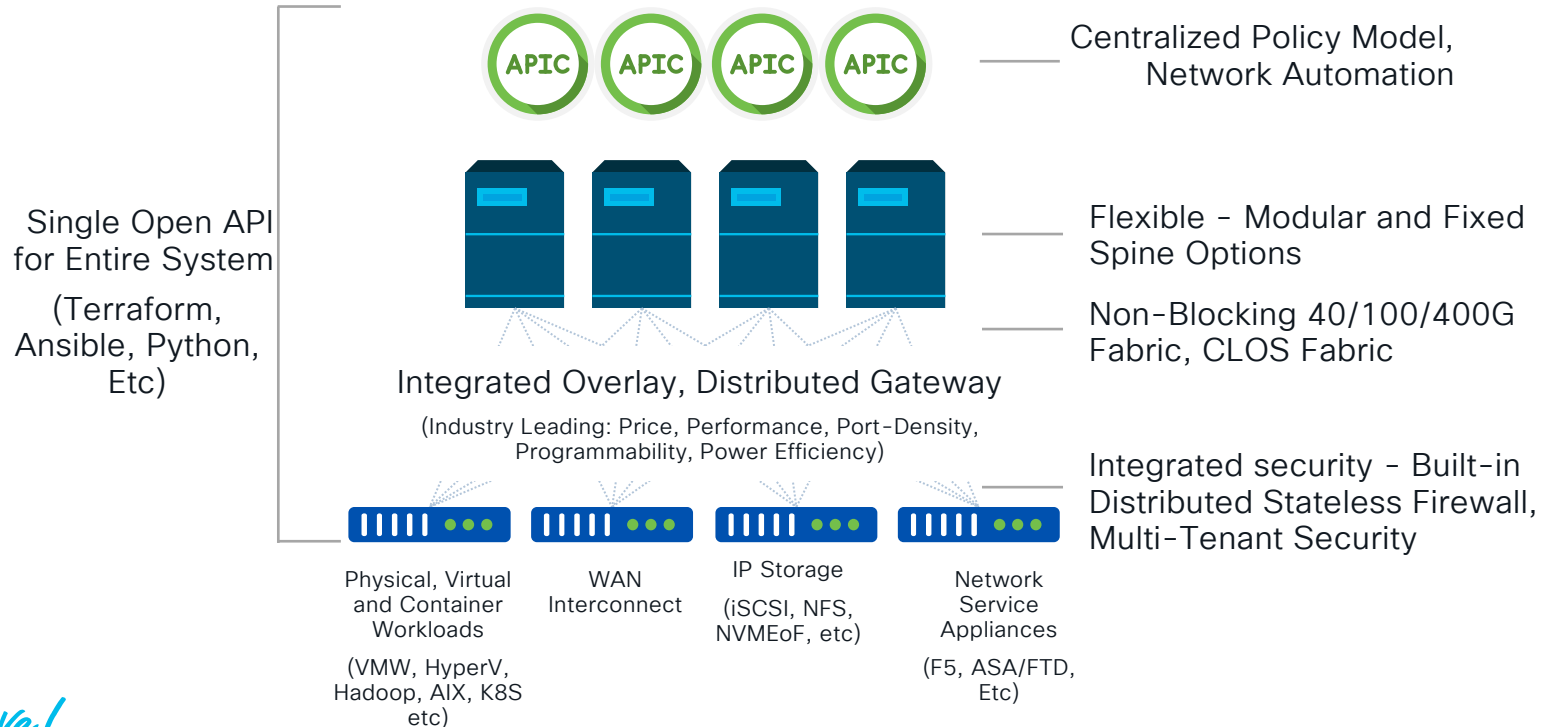
## The DC network NOW ACI





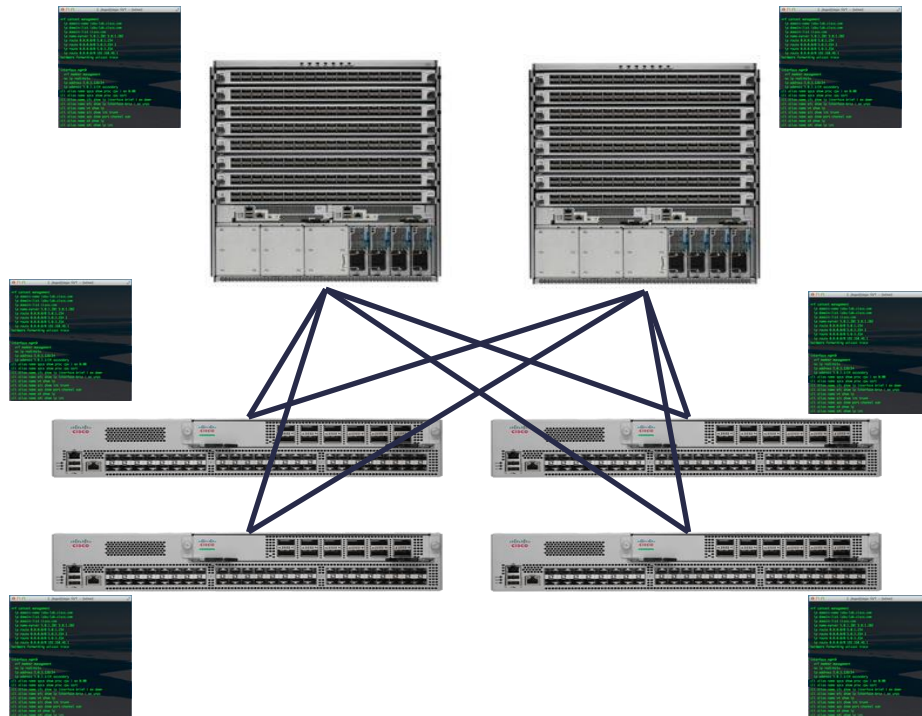
# Application Centric Infrastructure Building Blocks

Built on the Nexus 9000



# All nodes are managed and operated independently, and the actual topology dictates a lot of configuration

- **Device basics:** AAA, syslog, SNMP, PoAP, hash seed, default routing protocol bandwidth ...
- **Interface and/or Interface Pairs:** UDLD, BFD, MTU, interface route metric, channel hashing, Queuing, LACP, ...
- **Fabric and hardware specific design:** HW Tables, ...
- **Switch Pair/Group:** HSRP/VRRP, VLANs, vPC, STP, HSRP sync with vPC, Routing peering, Routing Policies, ...
- **Application specific:** ACL, PBR, static routes, QoS, ...
- **Fabric wide:** MST, VRF, VLAN, queuing, CAM/MAC & ARP timers, COPP, route protocol defaults



# ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

BEFORE

SSH to every switch, Assign IP Address, Enable  
Telnet/SSH, Add users on every switch/Create ACLs  
(optional)

# ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

## BEFORE

### • Nexus 9000 VTEP-1 configuration:

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit

switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

SSH to every switch, Assign IP Address, Enable  
Telnet/SSH, Add users on every switch/Create ACLs  
(optional)

(Times **X** Switches & **Y** VNIs)

# ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

BEFORE

NOW

• Nexus 9000 VTEP-1 configuration:

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nvel
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nvel
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

External to Internal Route redistribution  
& Control Plane (MP-BGP, QoS, etc)

Multicast (BD GIPo Addressing)

Overlay Network (VXLAN)

Underlay Routed Network (IS-IS)

Switch management & Best Practices

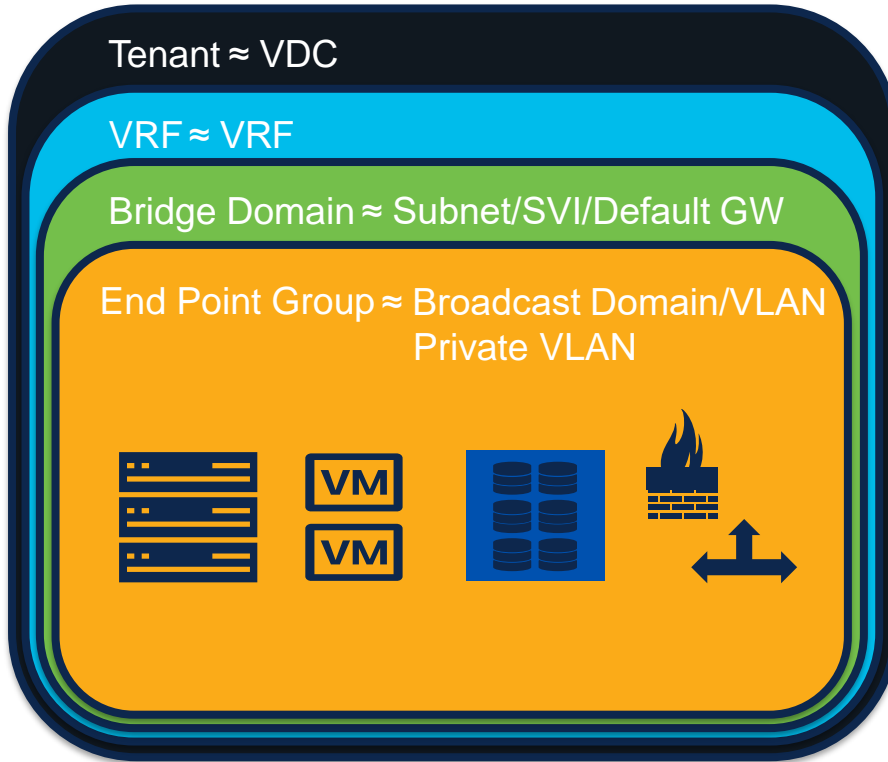
SSH to every switch, Assign IP Address, Enable  
Telnet/SSH, Add users on every switch/Create ACLs  
(optional)

(Times **X** Switches & **Y** VNIs)

ACI Automated tasks  
From HOURS to seconds!

# ACI Policy Model Simplified

# The ACI Policy Model



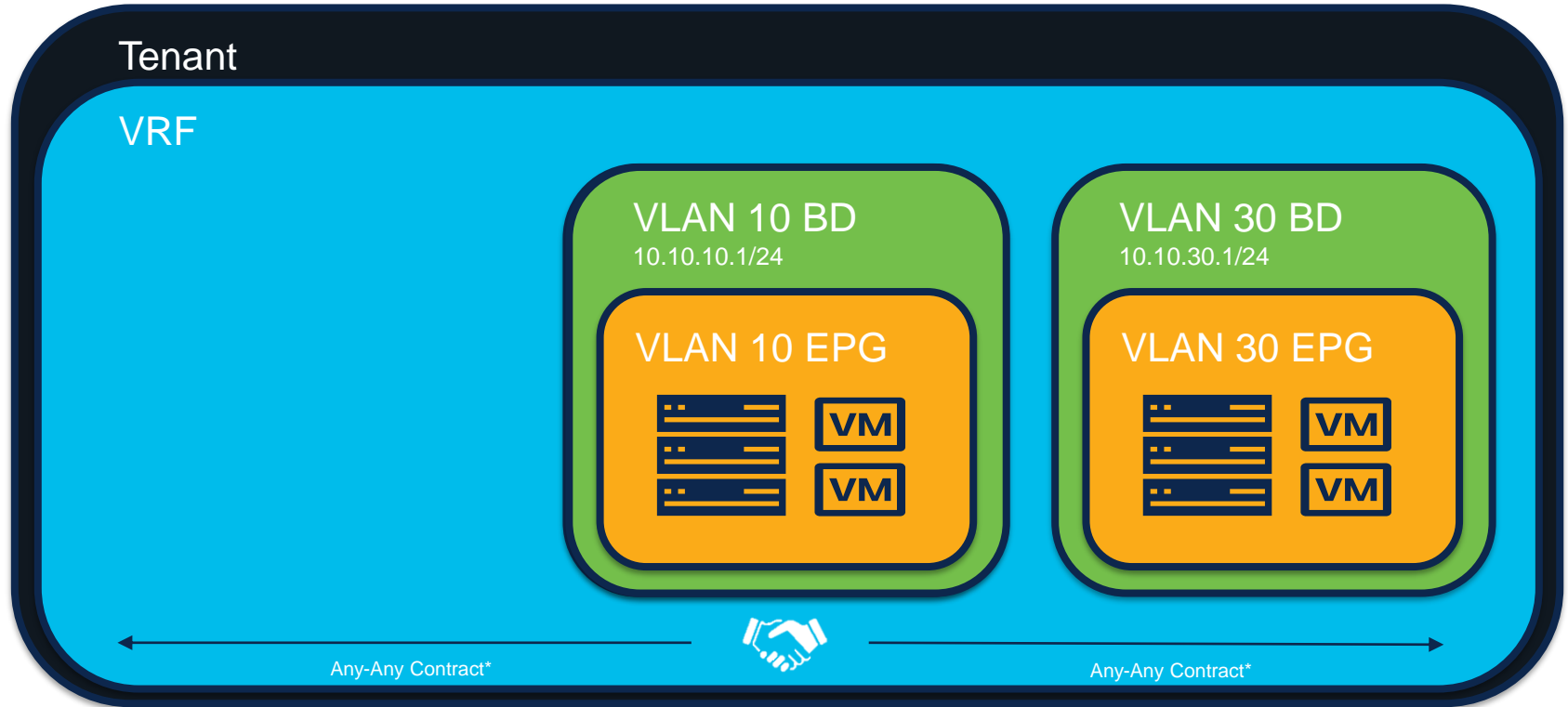
Contracts ≈ Access Lists



L2 External EPG ≈ 802.1q Trunk

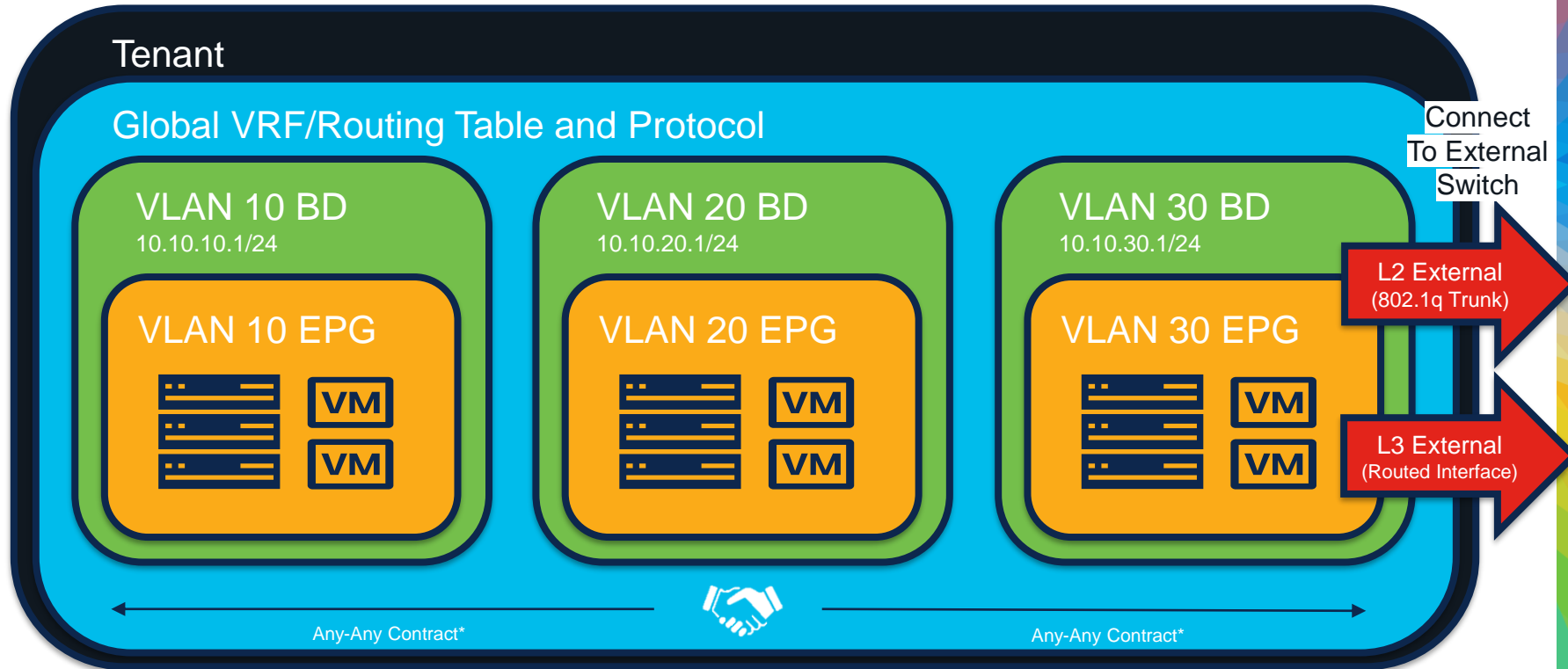
L3 External EPG ≈ L3 Routed Link

# The ACI Policy Model – Migrating into ACI



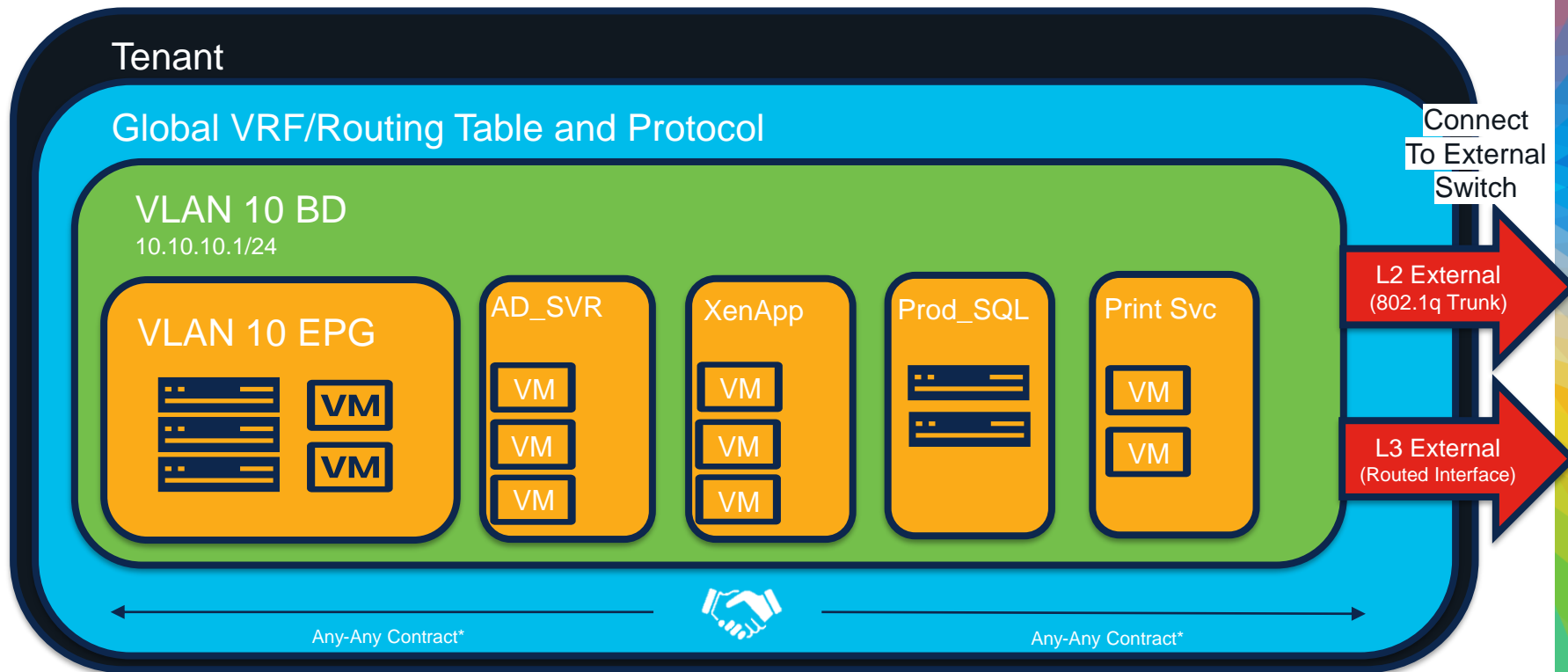


# The ACI Policy Model – Migrating into ACI



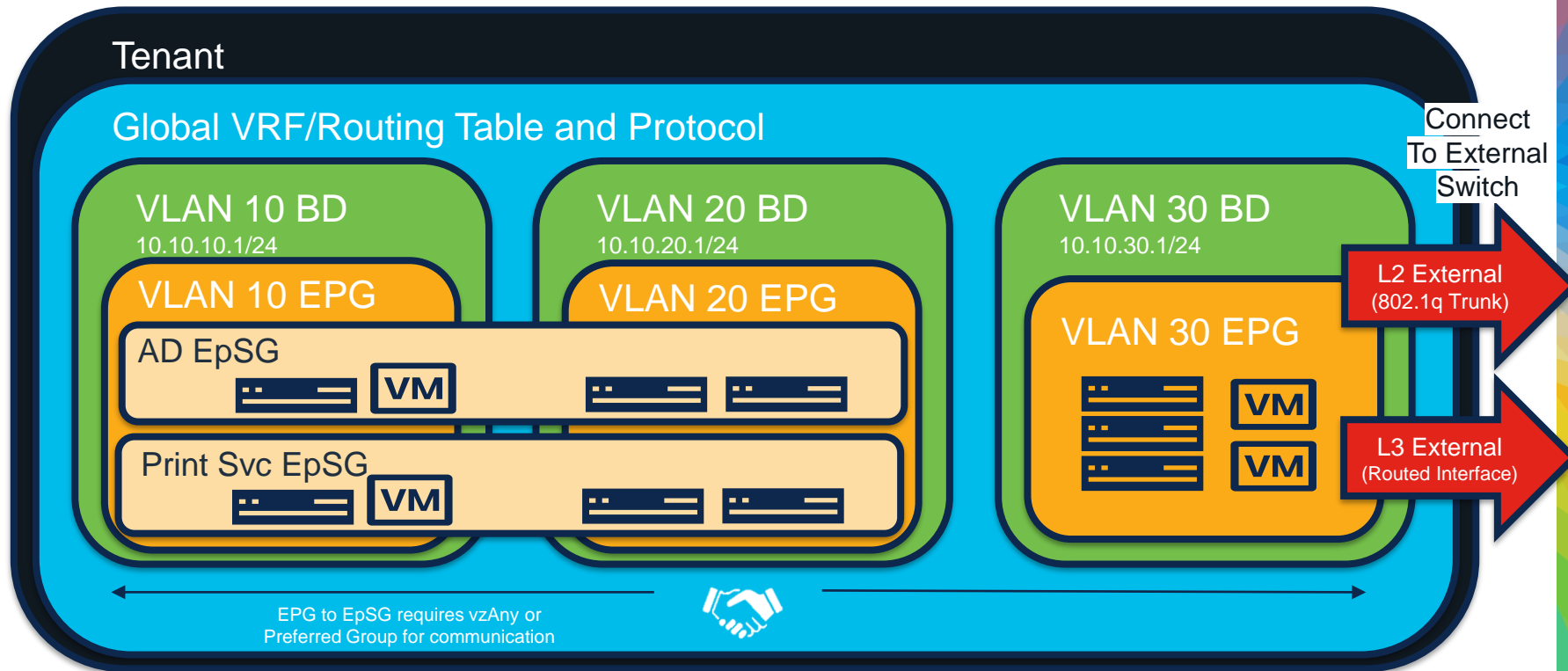
# The ACI Policy Model – Extending the configuration

## Endpoint Groups

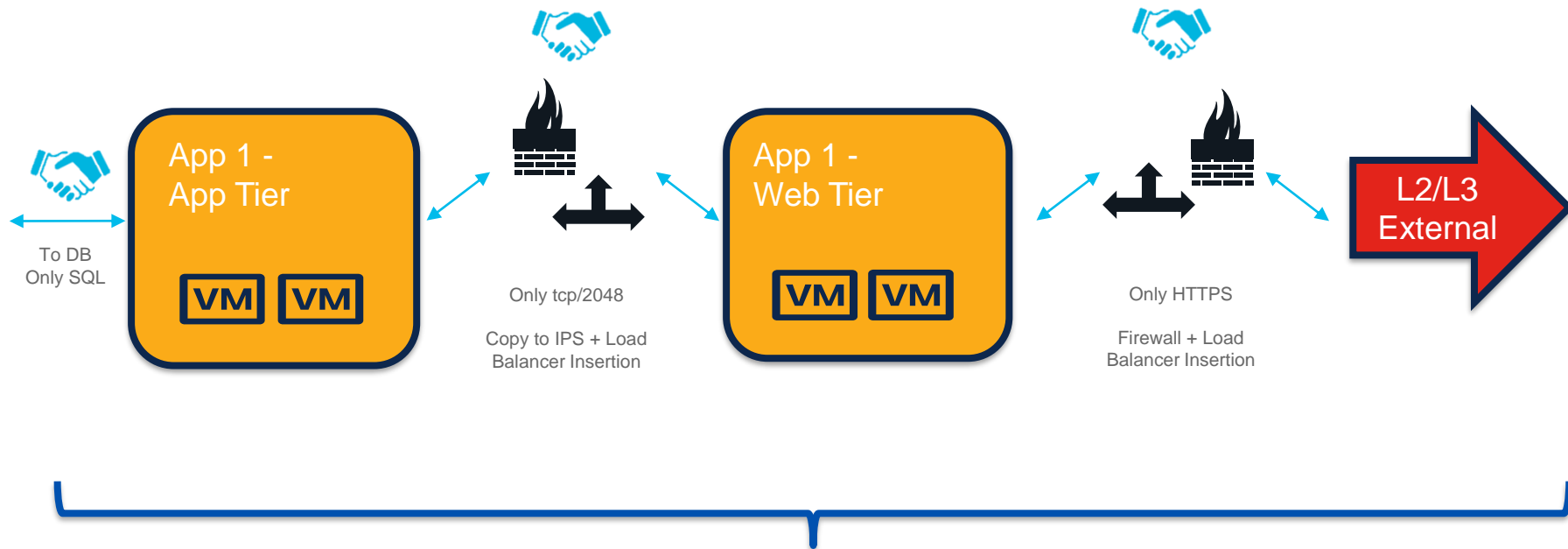


# The ACI Policy Model – Extending the configuration

## Endpoint Security Groups – ACI 5.0 and greater



# Advancing the ACI Configuration

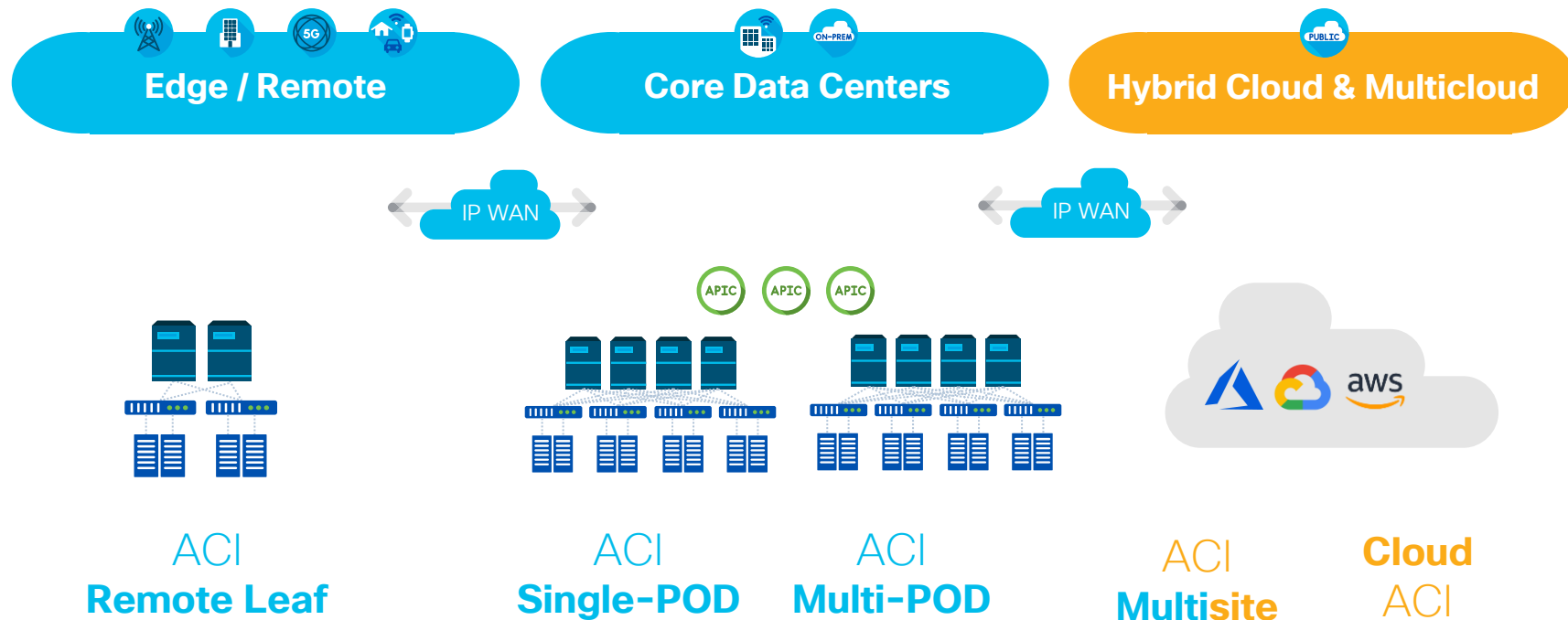


## Policy Based Redirect with Service Graphs

# ACI Deployment Options



## ACI Anywhere

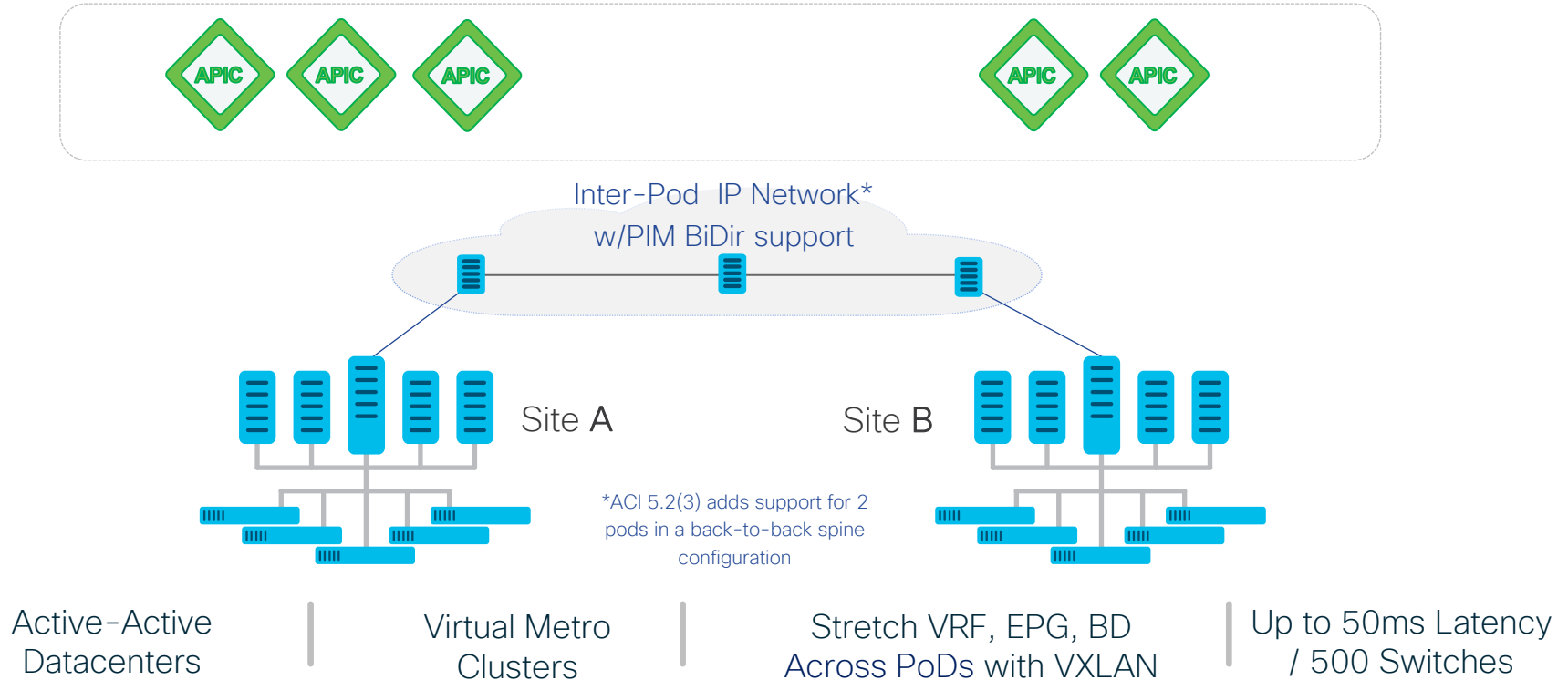


The easiest Data Center and Cloud Interconnect Solution in the Market

Try it today!

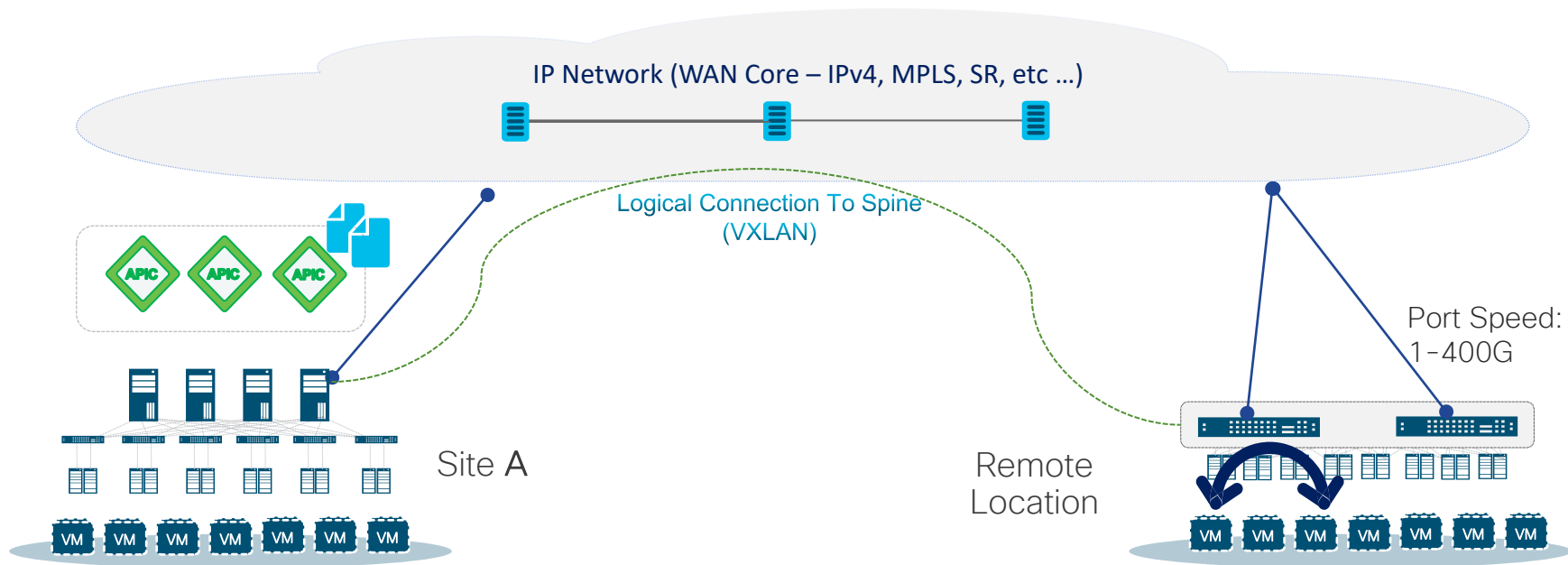
# ACI MultiPod

## The evolution of a stretched fabric



# ACI: Physical Remote Leaf

## Extend ACI to Satellite Data Centers



Zero Touch Auto  
Discovery of Remote Leaf

Two switches per site  
Up To 200 Remote Leaf  
Switches (ACI 6.0) – 300ms

Stretch EPG, BD, VRF,  
Tenant, Contract

DC Migration /  
OTV replacement

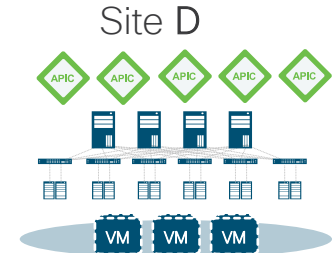
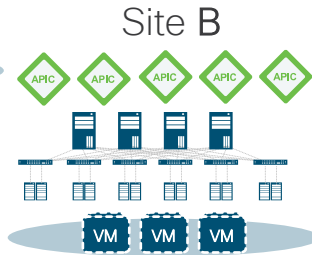
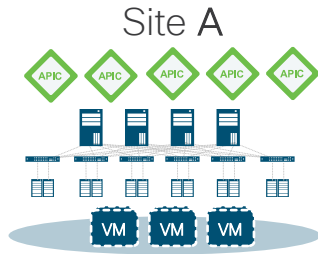


# ACI Multi-Site

## Nexus Dashboard Orchestrator



- ✓ Consistent Policy across sites
- ✓ Single Point of Orchestration
- ✓ Fault Isolation
- ✓ Scale



Policy  
Consistency

Single Point Of  
Orchestration

Availability  
Fault Isolation

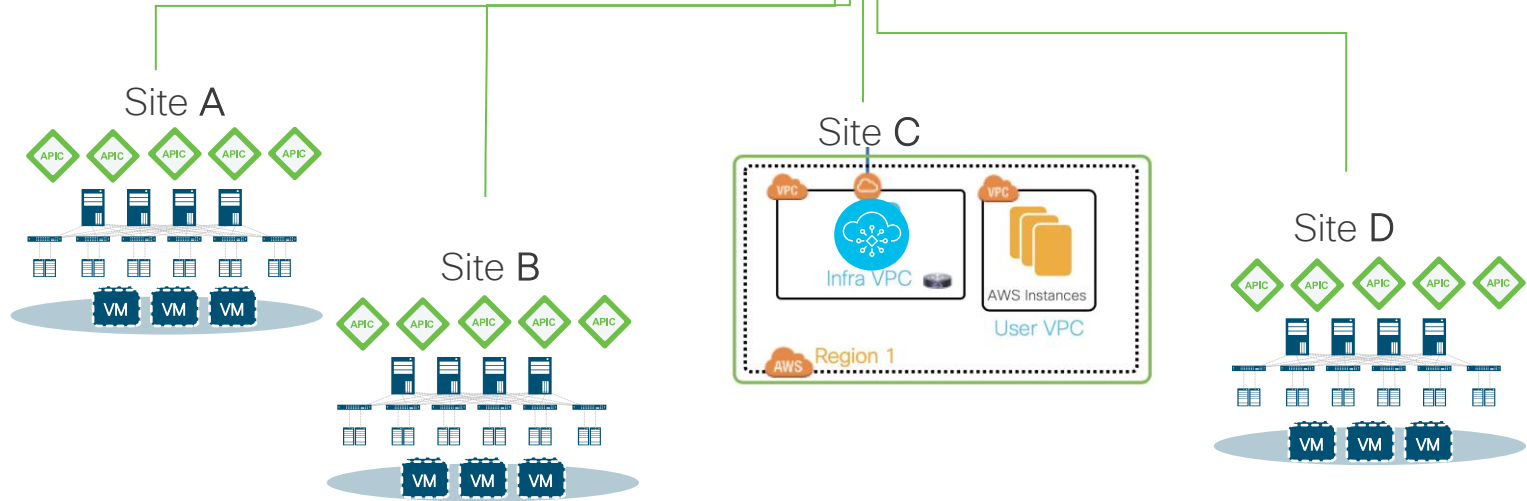
Scale

# ACI Multi-Site Cloud Integration

Nexus Dashboard  
Orchestrator



- ✓ Consistent Policy across sites
- ✓ Single Point of Orchestration
- ✓ Fault Isolation
- ✓ Scale



Policy  
Consistency

Single Point Of  
Orchestration

Availability  
Fault Isolation

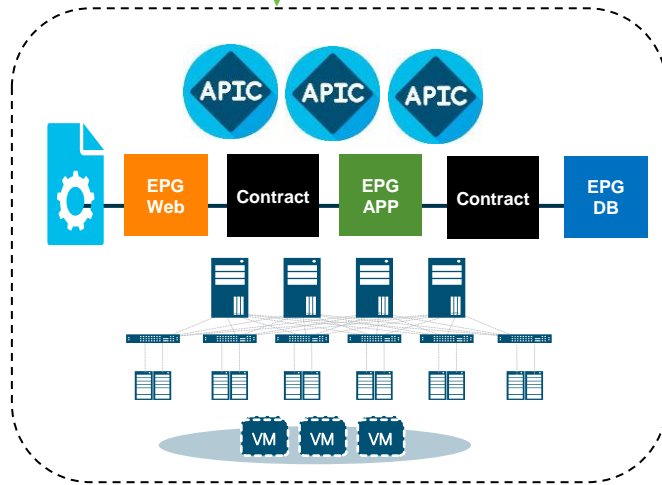
Scale

# ACI Policy in the Cloud



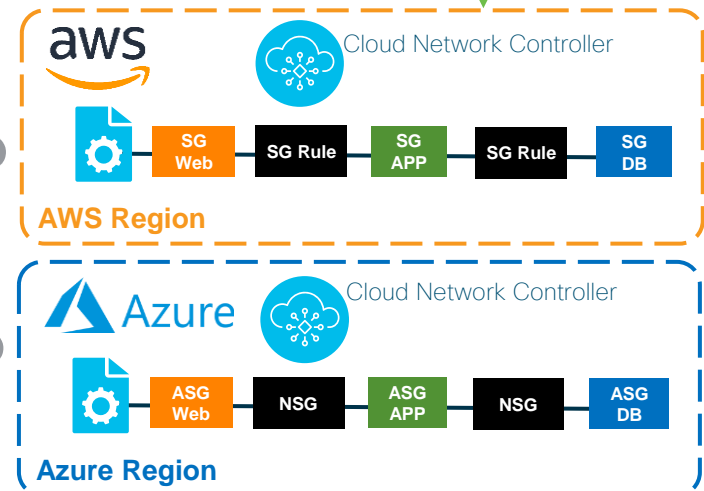
Nexus  
Dashboard  
Orchestrator

On-Premises DC



Consistent Policy Enforcement  
on-Premises & Public Cloud

Public Clouds

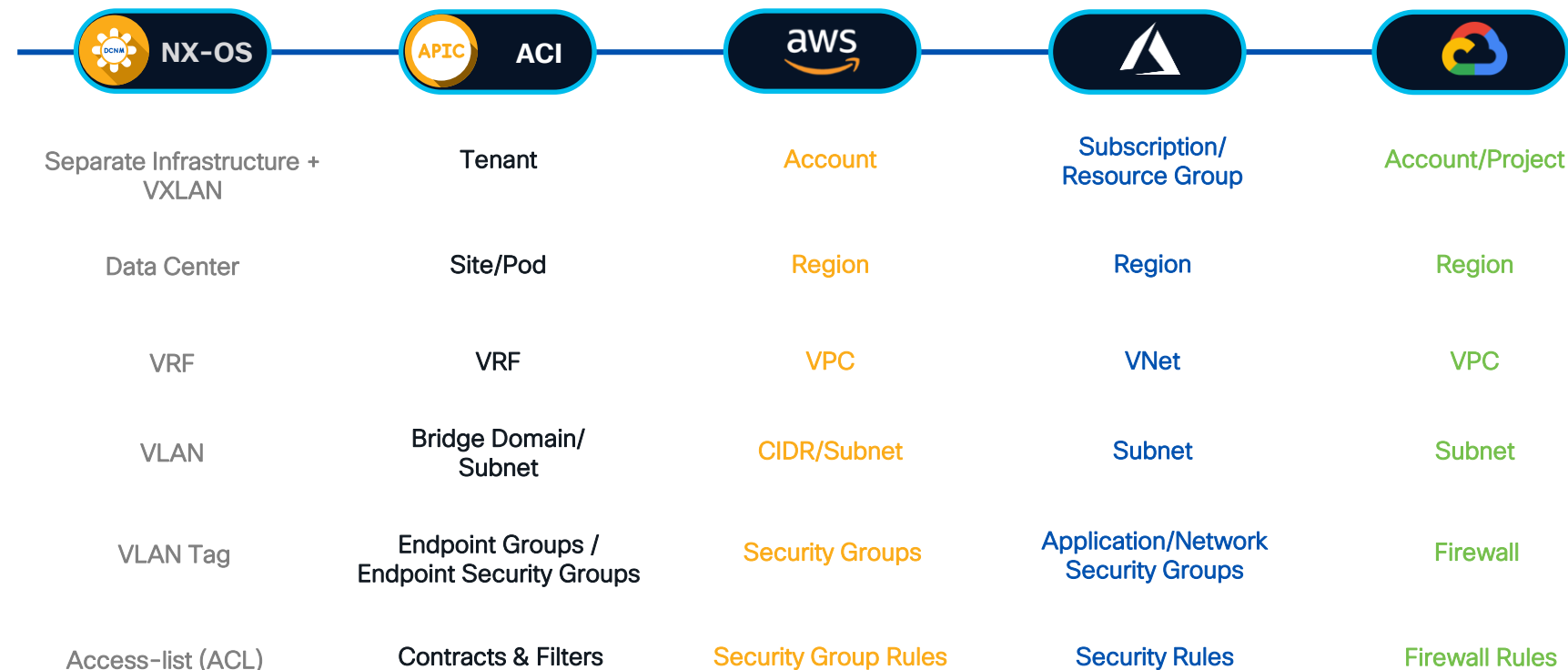


Automated Inter-connect  
provisioning

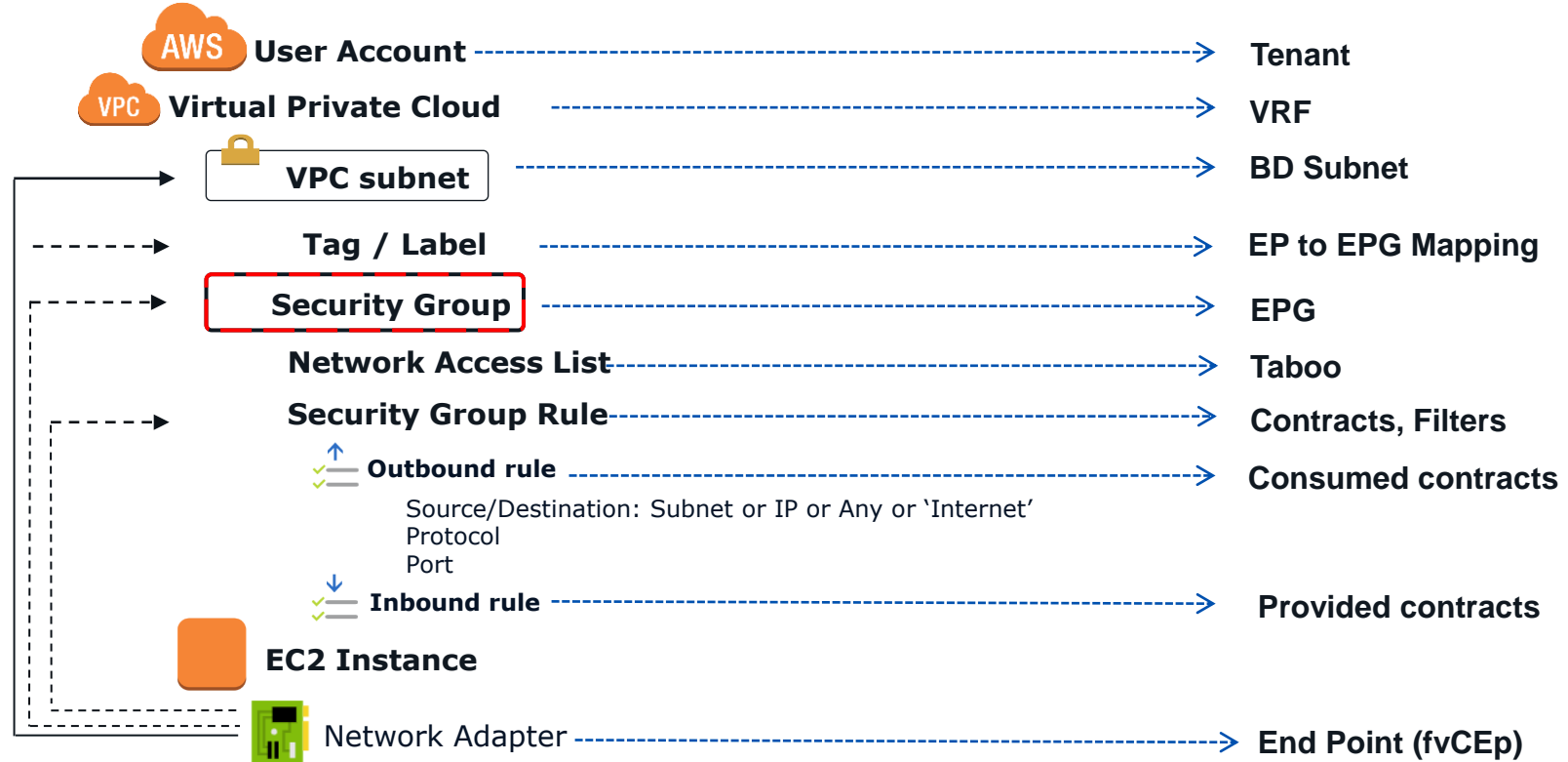
Simplified Operations  
with end-to-end visibility

# The network-admin challenge

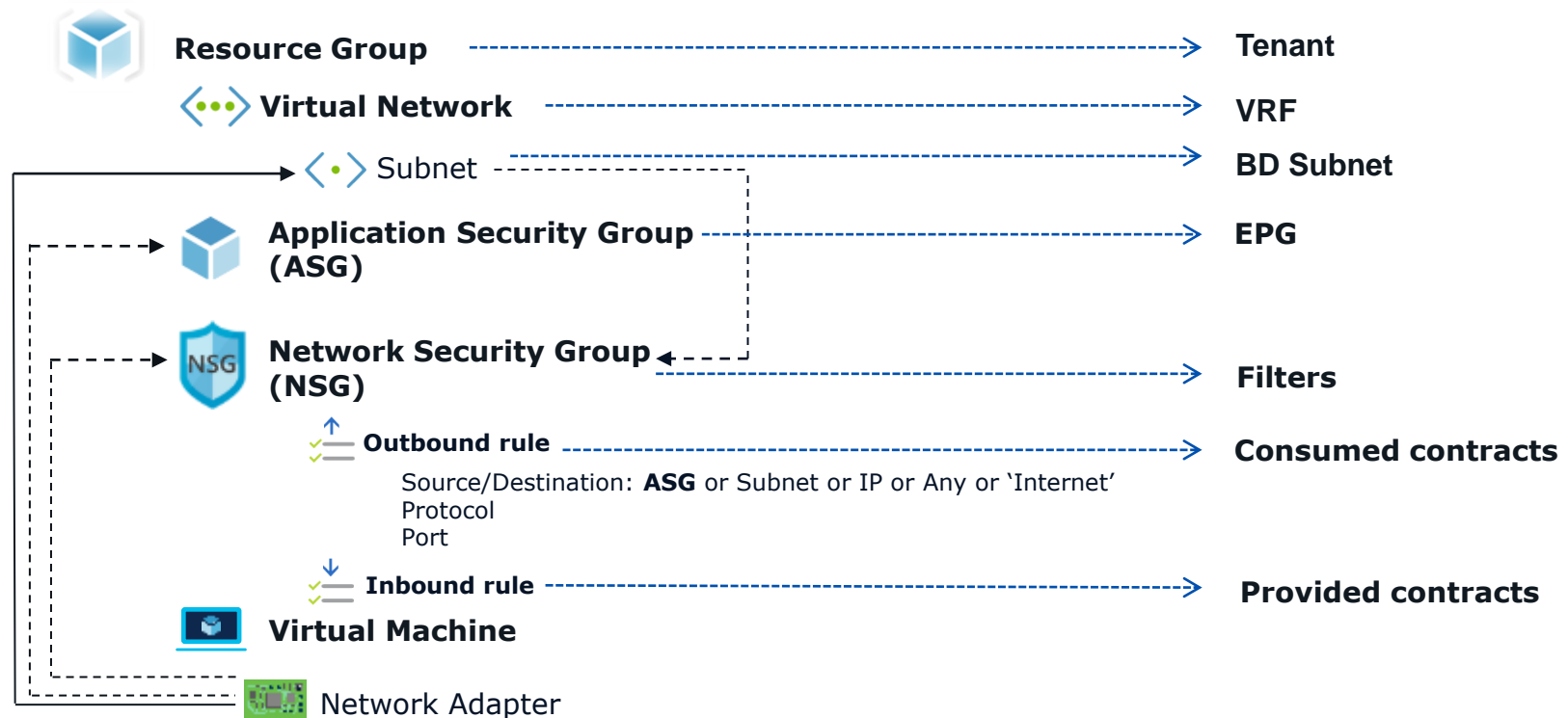
Provisioning and monitoring complexity = Risk



# Policy Mapping - AWS

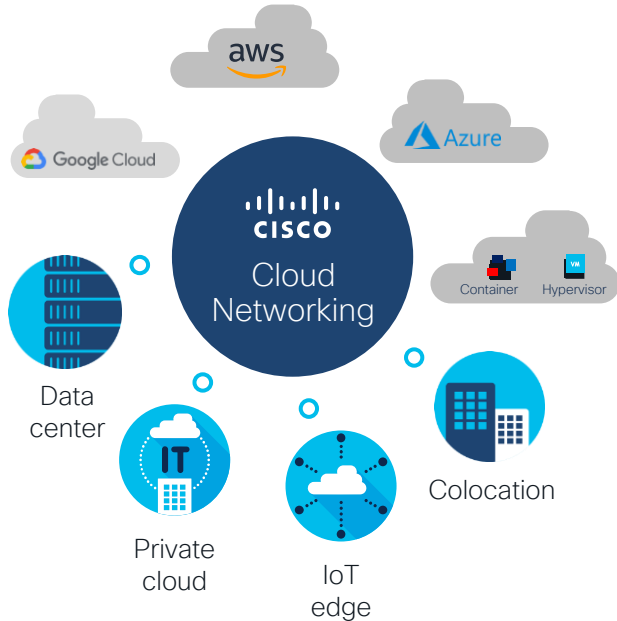


# Policy Mapping - Azure



# ACI Day 2 and Beyond – Making ACI Hum

# Cloud Networking: Challenges



## Connectivity and management



Workloads are increasingly distributed and diverse. **Complex to connect** workloads across multiple public cloud providers, data centers and edge locations.

## Visibility and automation



**Troubleshooting challenges** due to more decentralized architectures with different environments.

## Zero trust and security



Workload migration and mobility of users imposes **significant challenges to enforce right security policies** across different environments.

Need for **homogenous experience** across heterogenous cloud environments

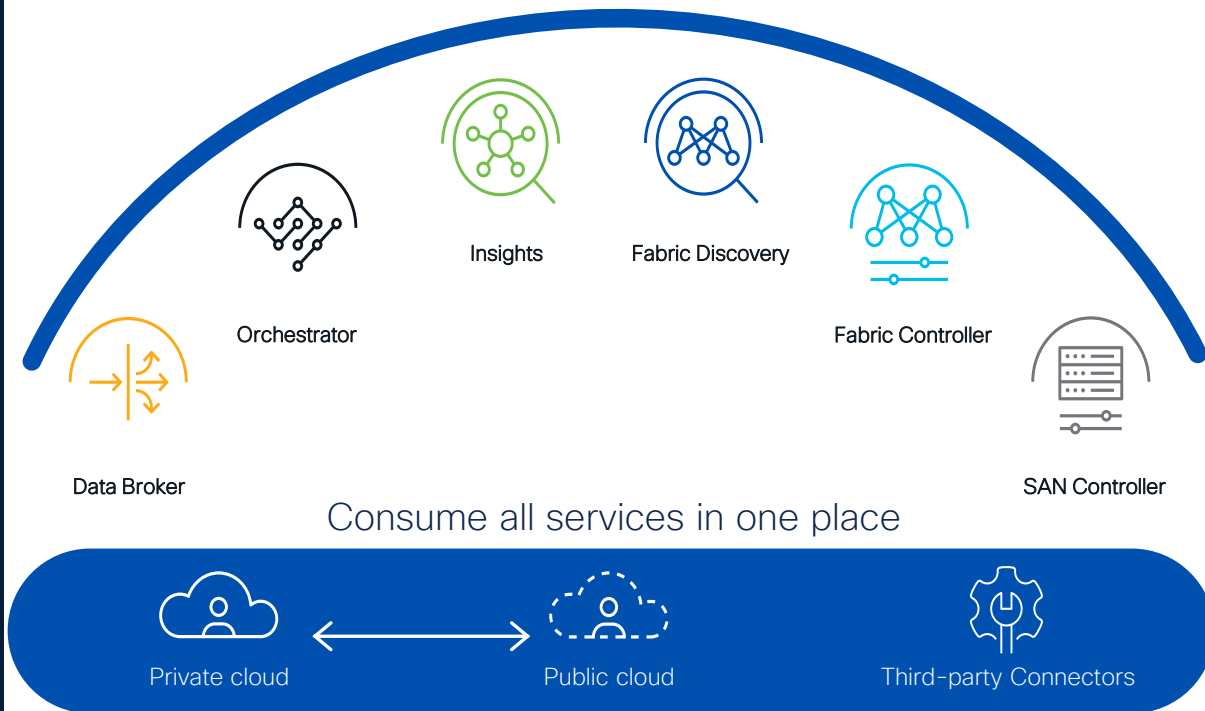


# Cisco Nexus Dashboard

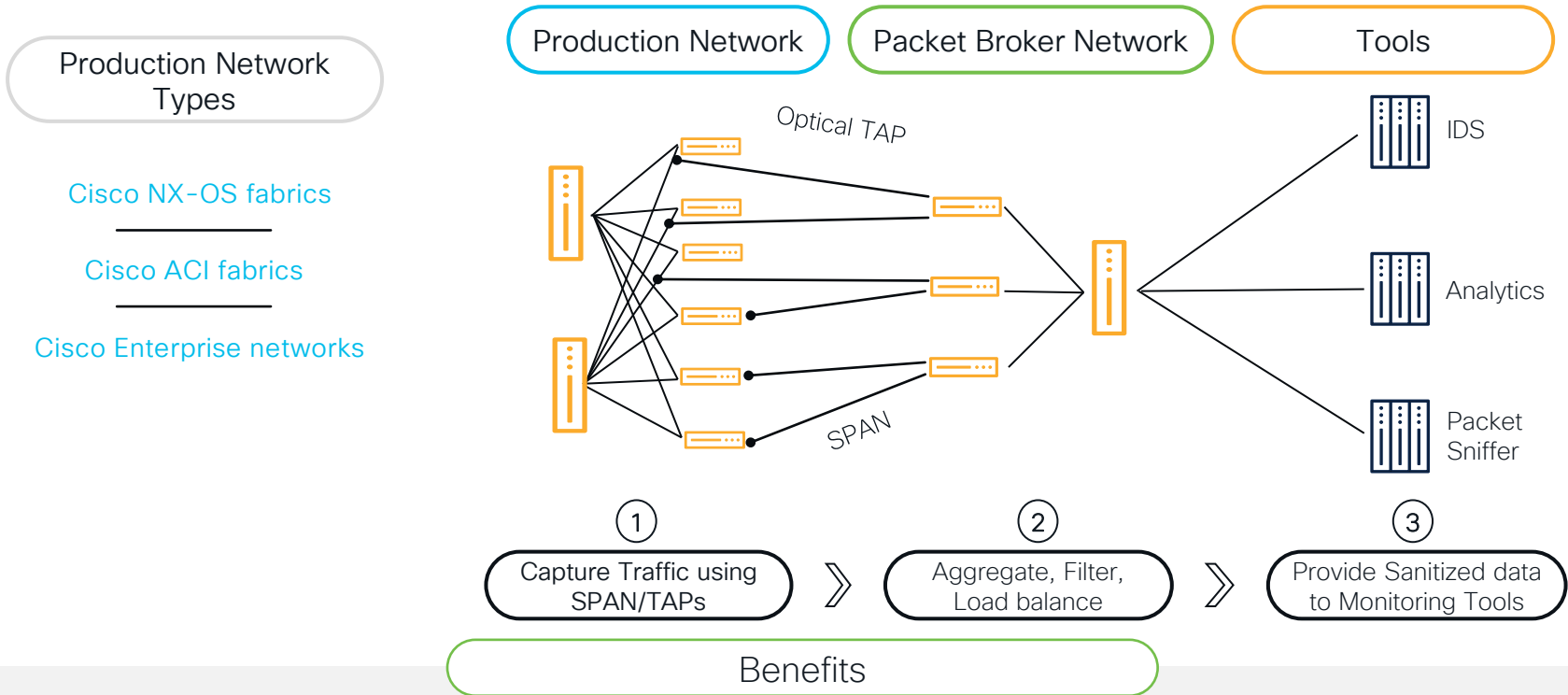
Simple to automate,  
simple to consume



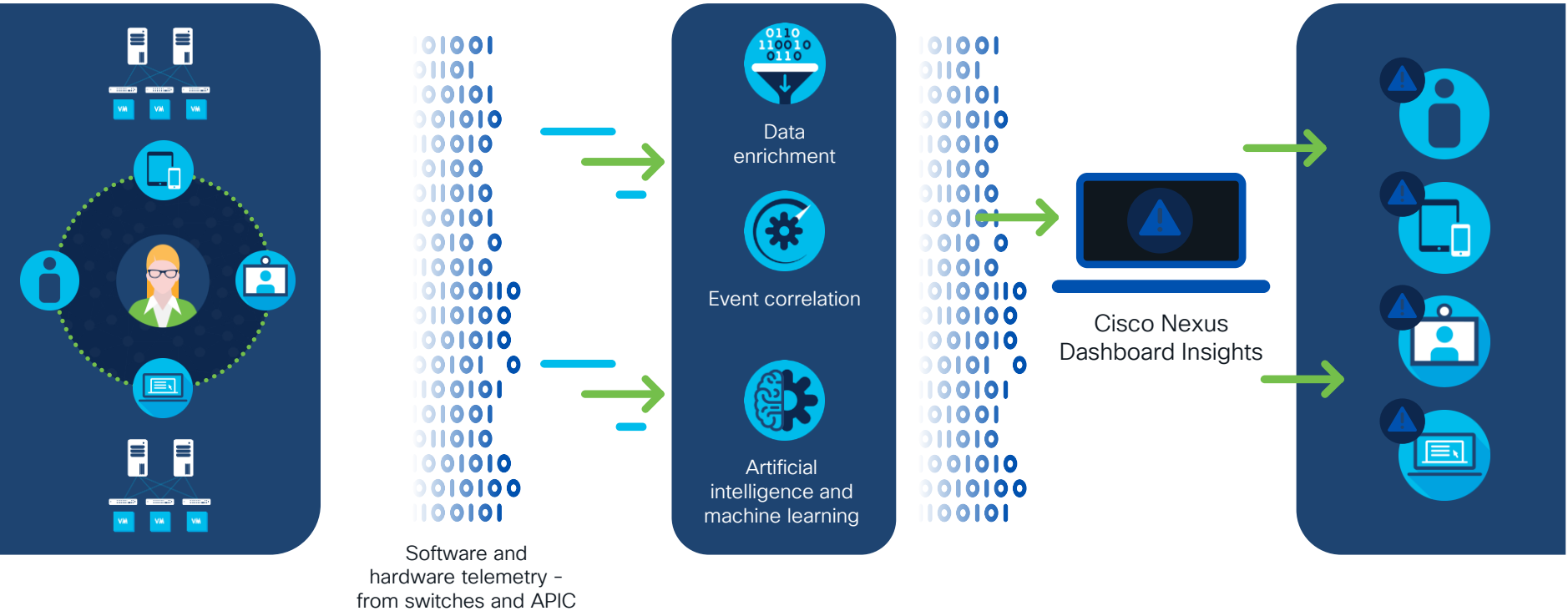
Powering **automation**  
Unified **agile** platform



# SPAN and Tap Aggregation with Data Broker



# Intelligent operations powered by telemetry



# Cisco Nexus Dashboard Insights

## Use cases and benefits



# Key Takeaways

- Consistent SDN enabled network policy across all the switches within a fabric
- The Multi-site architecture allows the same network policy to be applied across multiple sites, even cloud
- Nexus Dashboard Insights enables proactive day 2 operations for ACI to give a better understanding of how the applications interact with network

# 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](https://www.CiscoLive.com/on-demand)

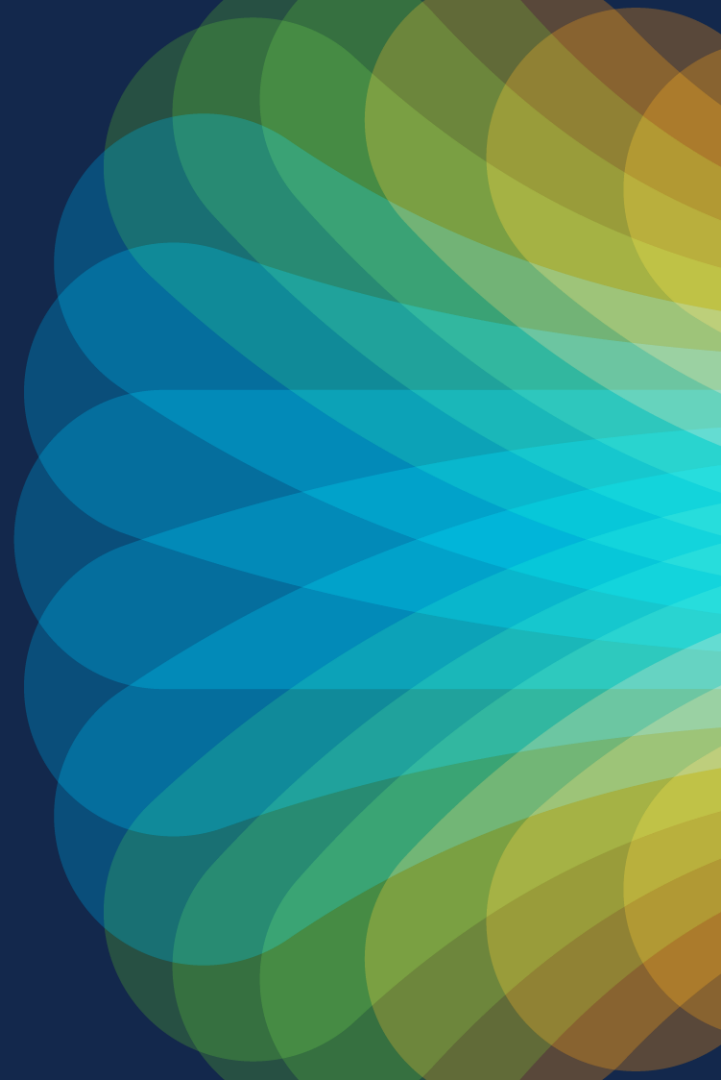


The bridge to possible

# Thank you



#CiscoLive



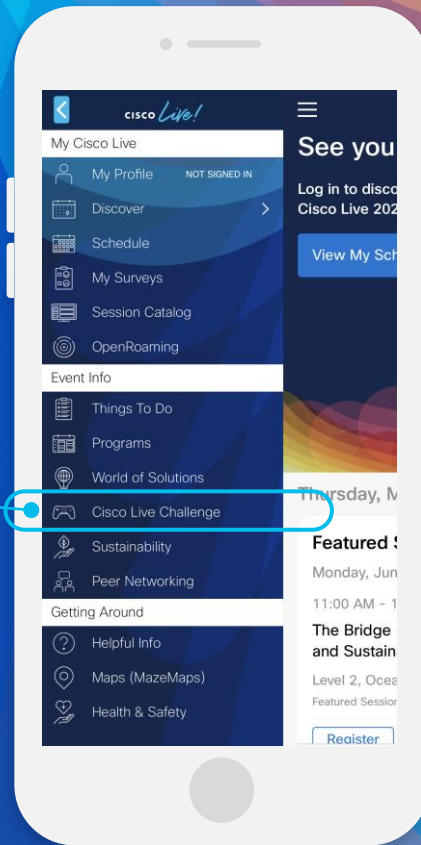
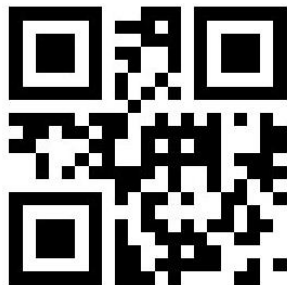


# Cisco Live Challenge

Gamify your Cisco Live experience!  
Get points for attending this session!

## How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive