
cisco Live!
Let's go

The bridge to possible

# Introduction to ACI

Chris Merkel, DC TSA – CCIE 17841

# ACI Learning Roadmap

**START**

Monday, February 5 | 8:30 a.m.
**TECDCN-2438**
Next Generation ACI Data Center Architecture and Deployment Best Practices

Tuesday, February 6 | 8:00 a.m.
**BRKDCN-1601**
Introduction to ACI

Tuesday, February 6 | 2:45 p.m.
**BRKDCN-2949**
Cisco ACI Multi-Pod Design and Deployment

Tuesday, February 6 | 5:00 p.m.
**BRKDCN-2980**
ACI Multi-Site Architecture and Deployment

Wednesday, February 7 | 8:45 a.m.
**BRKDCN-2910**
Why You Shouldn't Fear Upgrading Your ACI Fabric - The Handbook!

Wednesday, February 7 | 1:45 p.m.
**BRKDCN-2906**
Infrastructure as Code for ACI using Ansible

Thursday, February 8 | 8:30 a.m.
**BRKDCN-3900**
A Network Engineer's Blueprint for ACI Forwarding

Thursday, February 8 | 10:30 a.m.
**BRKDCN-3678**
ACI Troubleshooting: Advanced L3out Features

Thursday, February 8 | 1:30 p.m.
**BRKDCN-2626**
ACI Troubleshooting: expand your toolset with Nexus Dashboard Insights

Thursday, February 8 | 3:00 p.m.
**BRKDCN-3982**
ACI L4-L7 Policy-Based Redirect (PBR) Deep Dive and Tips

Thursday, February 8 | 5:00 p.m.
**BRKDCN-3615**
ACI Troubleshooting: A deep dive into PBR

**FINISH**

Friday, February 9 | 9:00 a.m.
**BRKDCN-2984**
ACI: the foundation of an internal private cloud

# Agenda

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

# Fabric Basics

# ACI: One Network, any location

# What is Cisco ACI?

An application centric model- networking framework

**Software-defined network that takes a systems approach to deliver best-in-class automation through integration of hardware, software, physical and virtual elements**


**Policy-model (application basic components)**

**Application Policy Infrastructure Controller (APIC)**

**Fabric (Cisco Nexus 9000)**

The unified point of automation and management for the Cisco ACI fabric, policy enforcement and health monitoring for physical, virtual and cloud infrastructures

ACI Anywhere

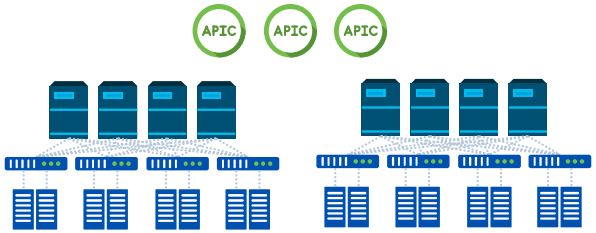
Edge / Remote

Core Data Centers

Hybrid Cloud & Multicloud

IP WAN

IP WAN





ACI
**Remote Leaf**

ACI
**Single-POD**

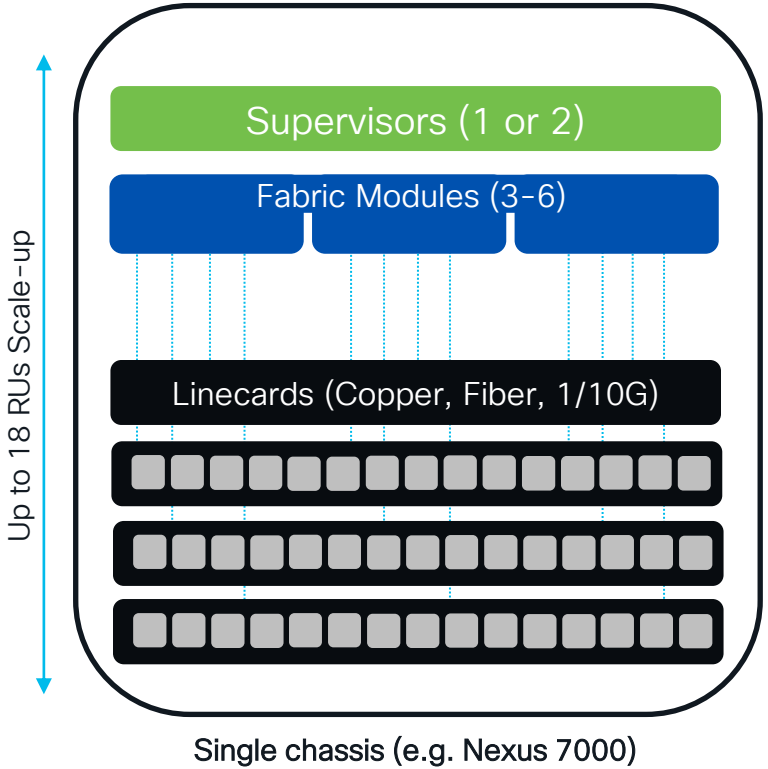
ACI
**Multi-POD**

ACI
**Multisite**

**Cloud**
ACI

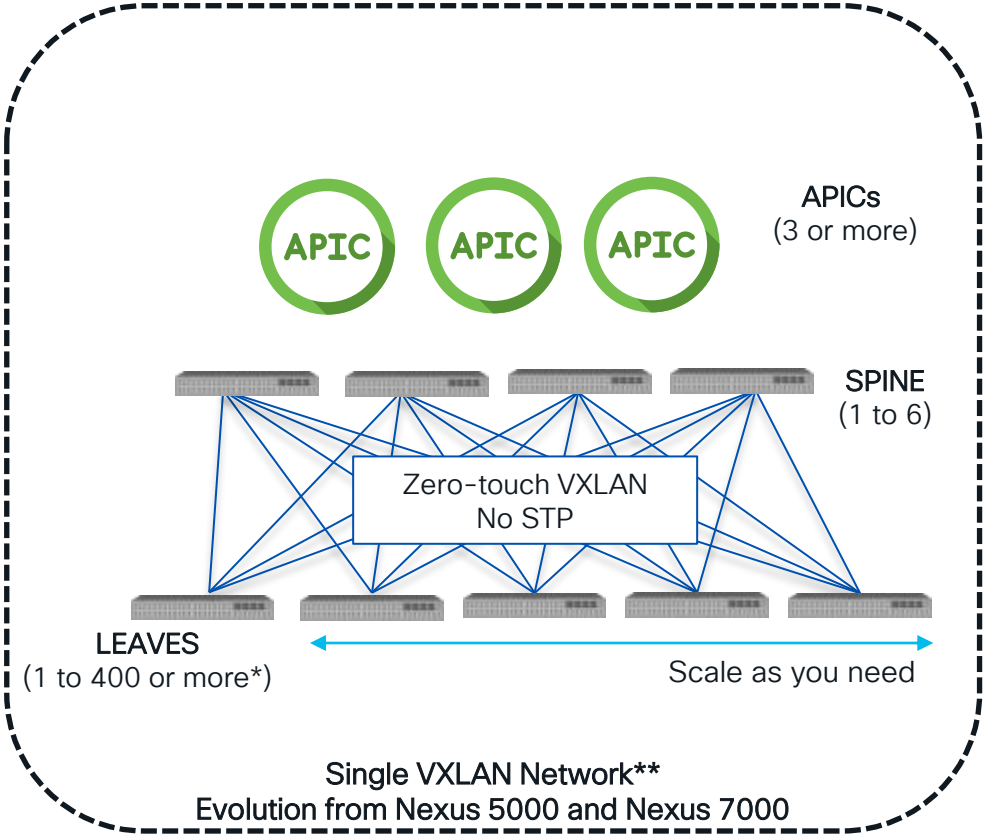
**The easiest Data Center and Cloud Interconnect Solution in the Market** **Try it today!**

# The DC network before
## Classic modular switching




Single chassis (e.g. Nexus 7000)

# The DC network NOW
## ACI



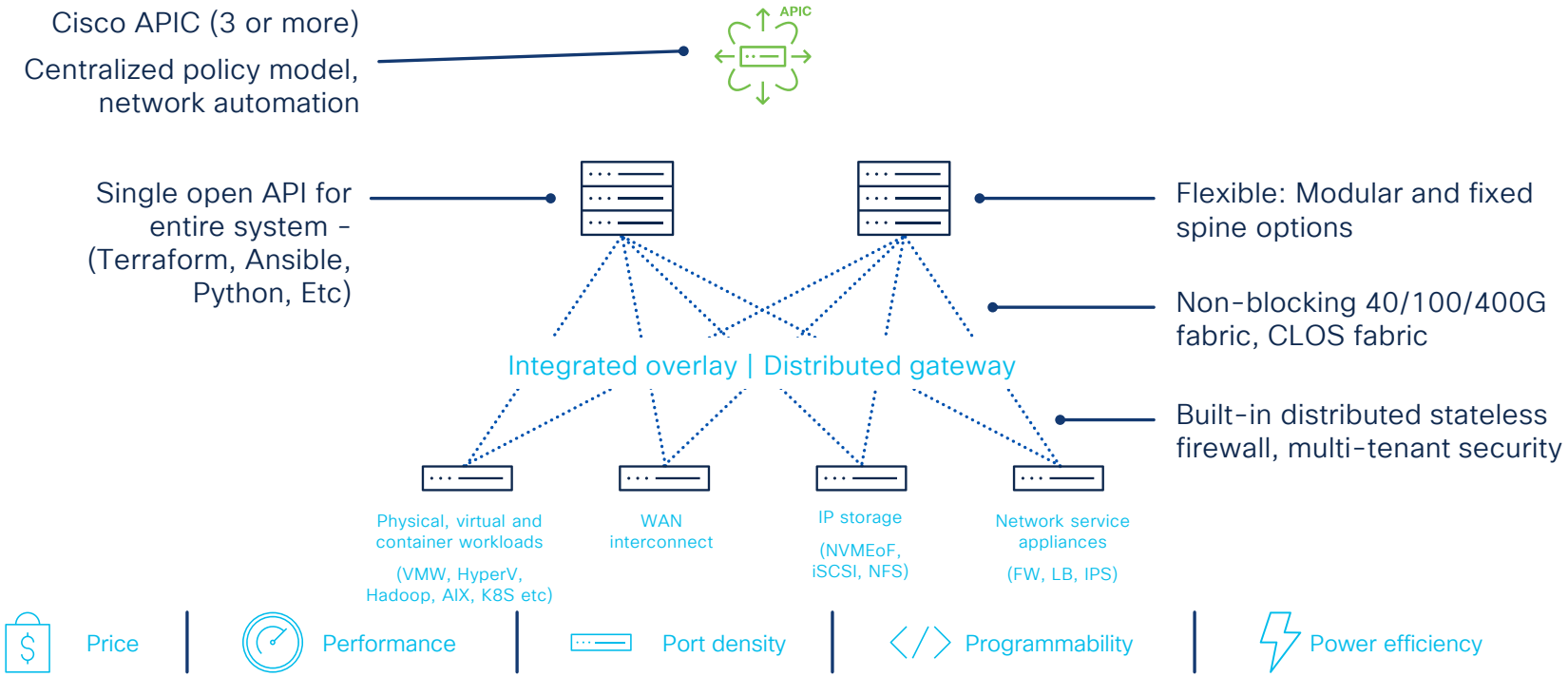

Single VXLAN Network**
Evolution from Nexus 5000 and Nexus 7000

cisco Live!

* 500+ Leaves with MultiPod/Multi-Site
** Other topologies available (e.g. 3-tier, etc)

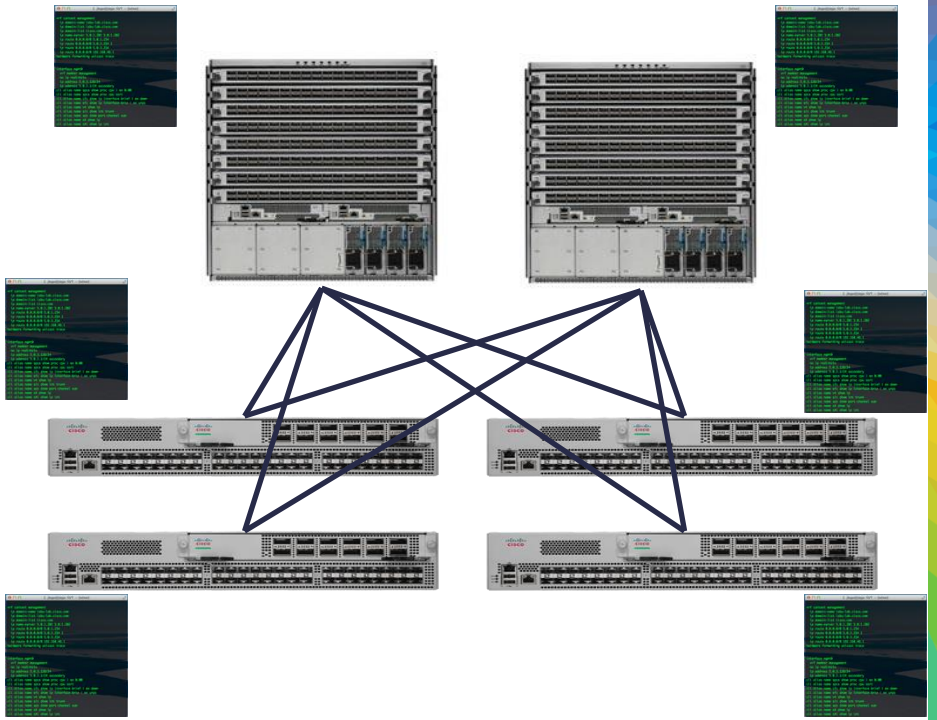
# Application Centric Infrastructure building blocks

Built on Cisco 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 second
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

- 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 second
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)

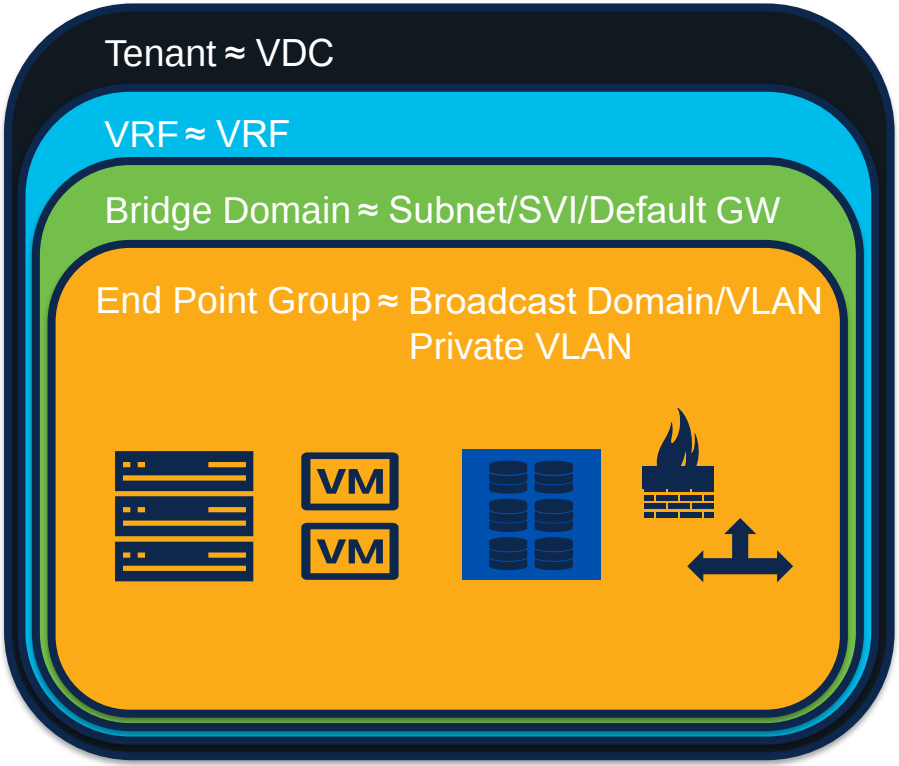
### NOW

- 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

**ACI Automated tasks From HOURS to seconds!**

# ACI Policy Model Simplified

# The ACI Policy Model



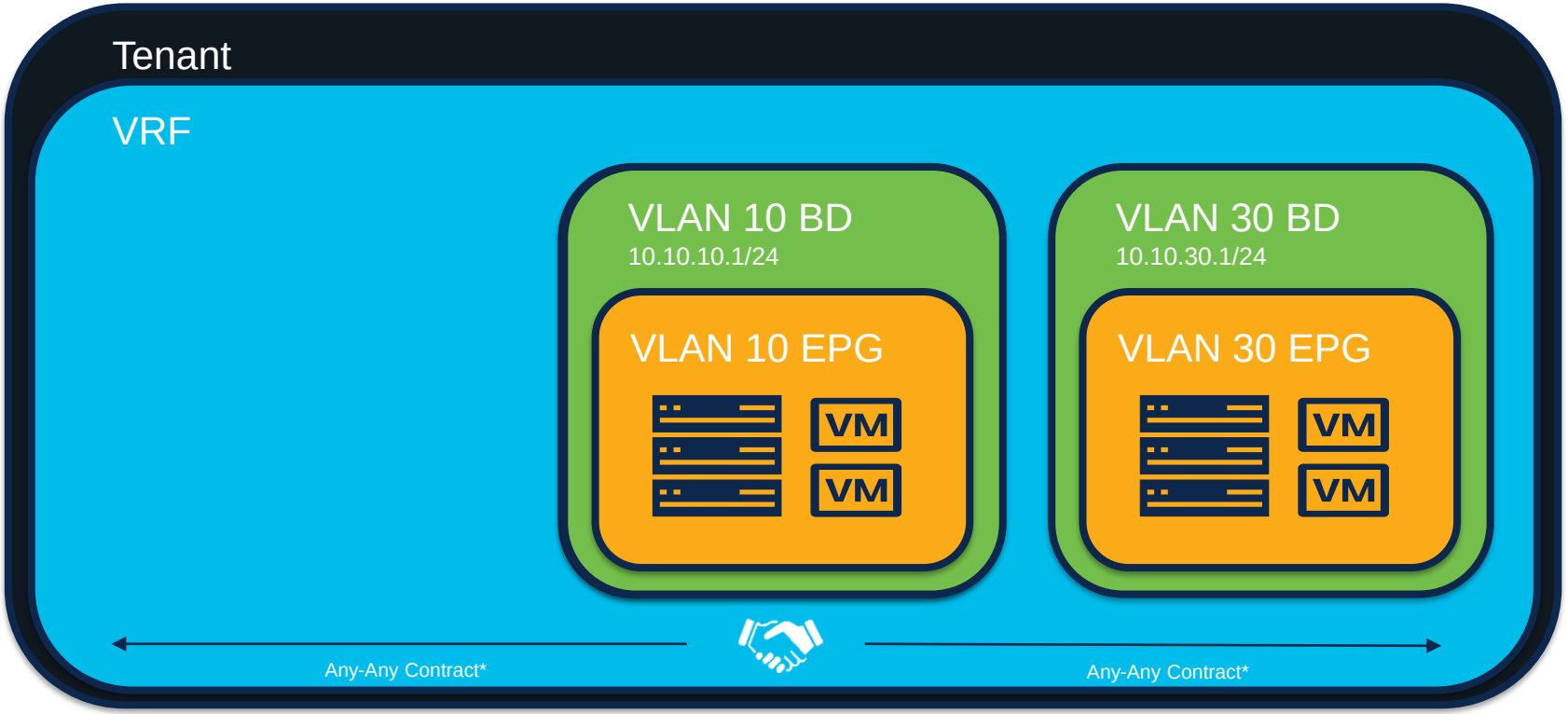

Contracts ≈ More Intelligent Access Lists


L2 External EPG≈ 802.1q Trunk

L3 External EPG≈ L3 Routed Link

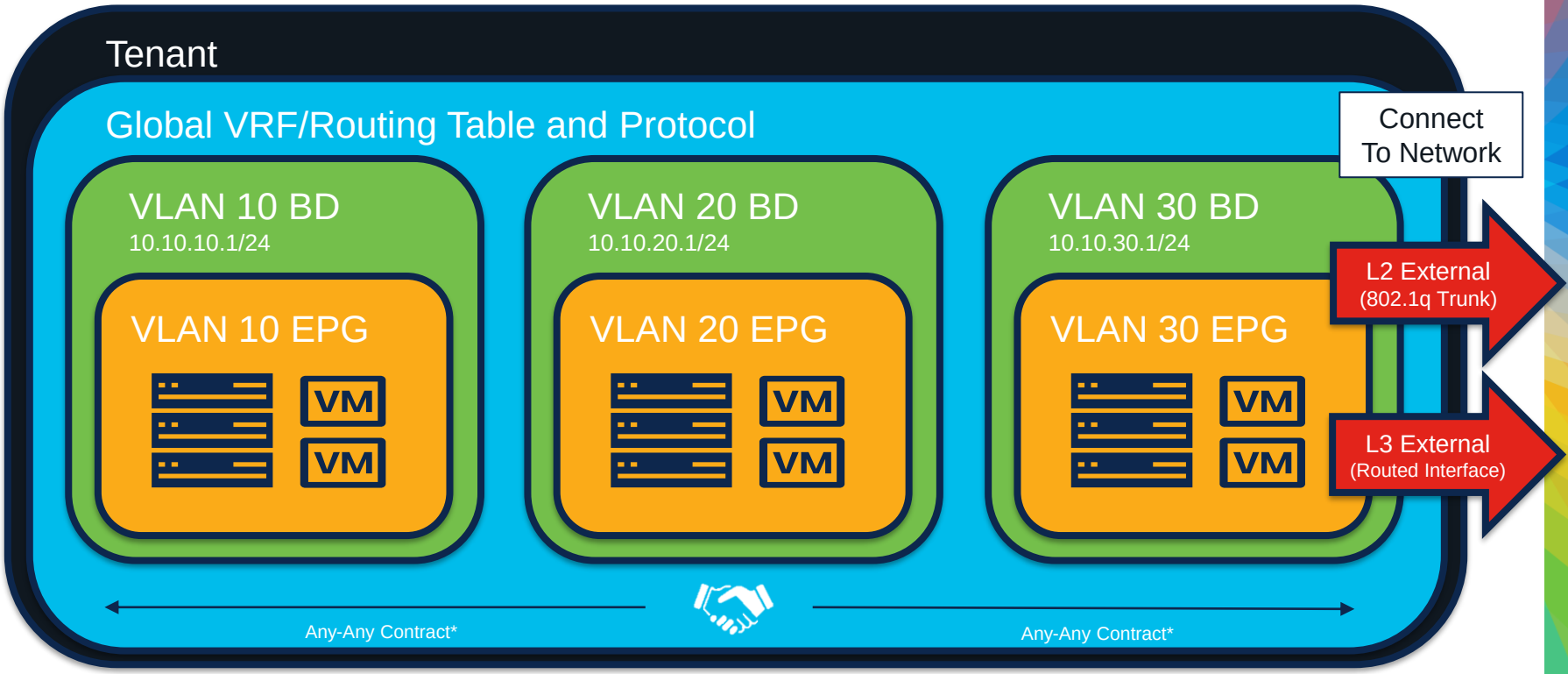
* Preferred group or vzAny Contract achieves the same outcome

# The ACI Policy Model – Starting off with ACI



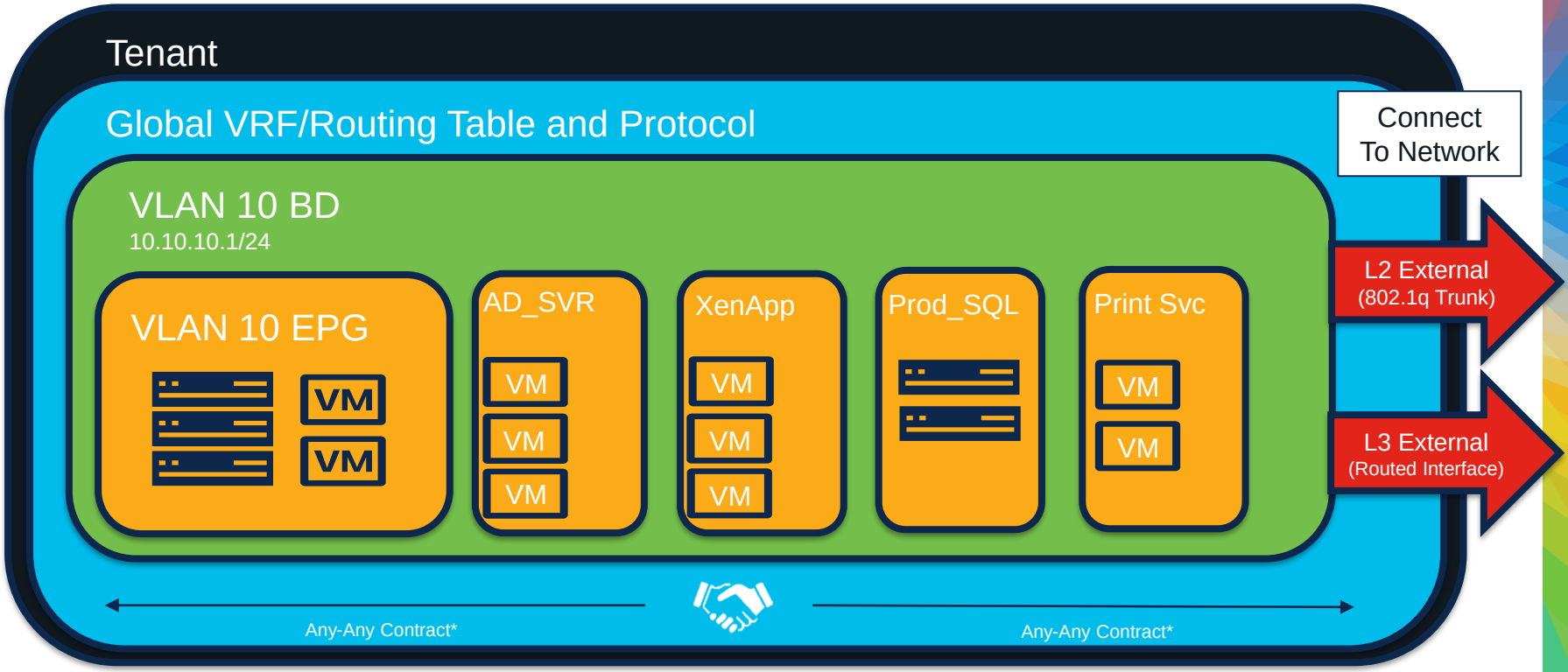

* Preferred group or vzAny Contract achieves the same outcome

# The ACI Policy Model – Starting off with ACI




* Preferred group or vzAny Contract achieves the same outcome

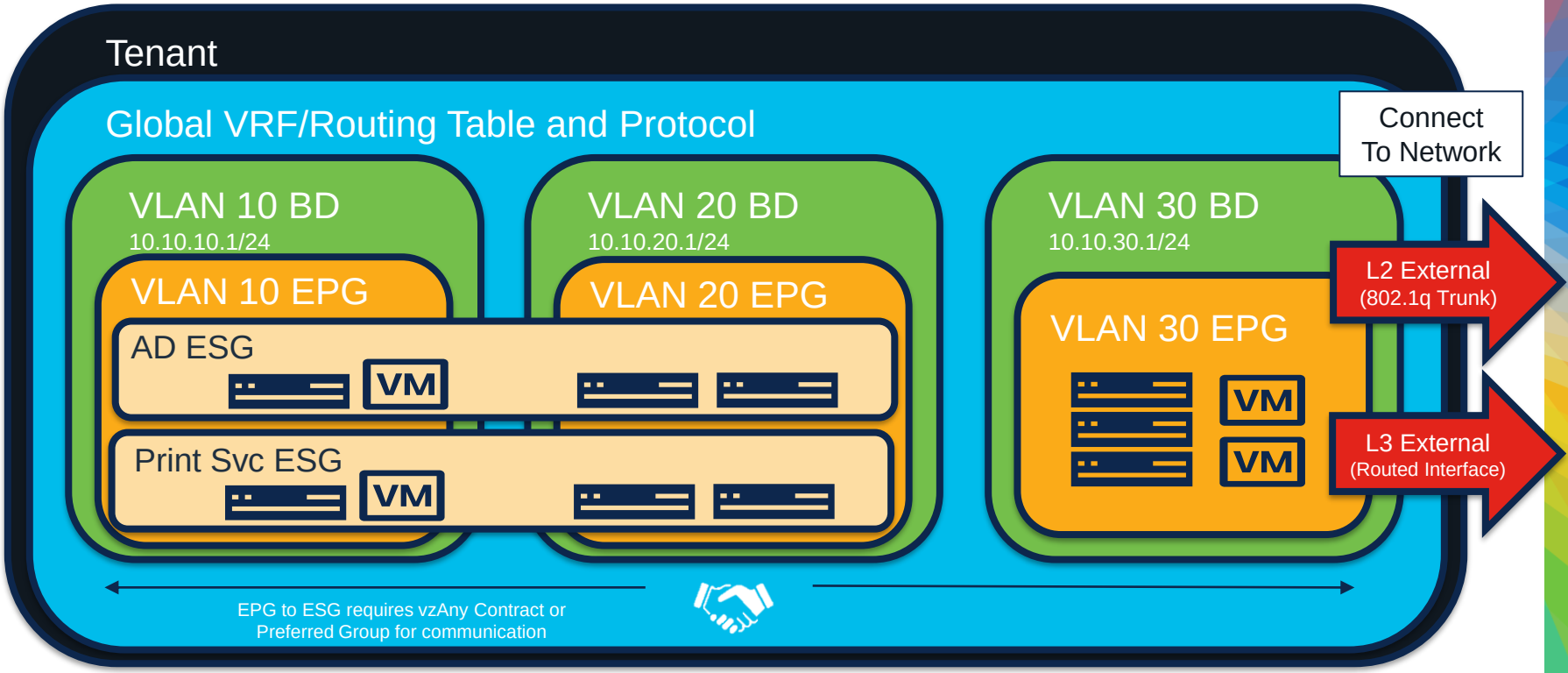
# The ACI Policy Model – Extending the configuration
## Endpoint Groups



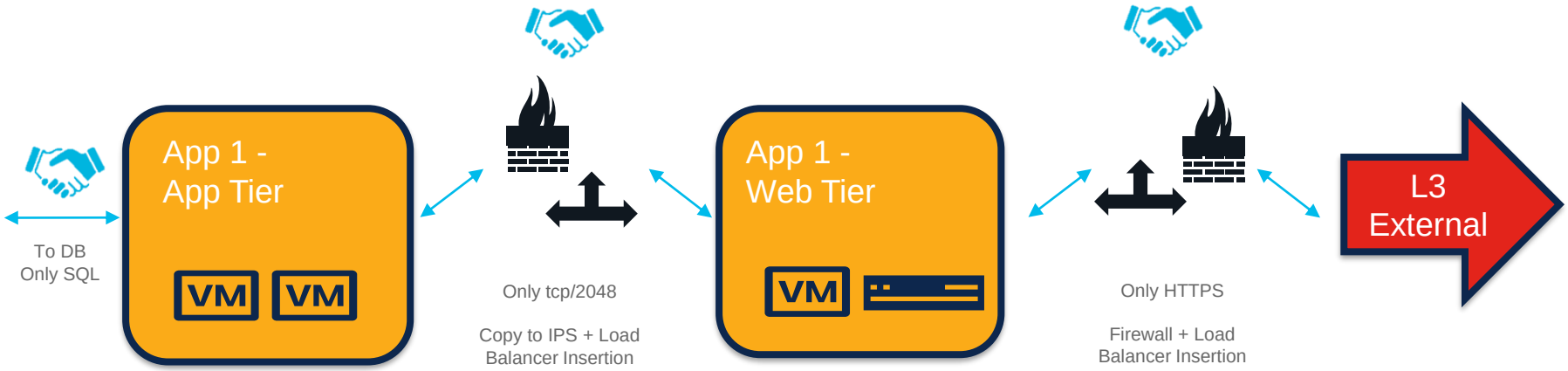

* Preferred group or vzAny Contract achieves the same outcome

# The ACI Policy Model – Extending the configuration

## Endpoint Security Groups (ESG) - ACI 5.0 and greater



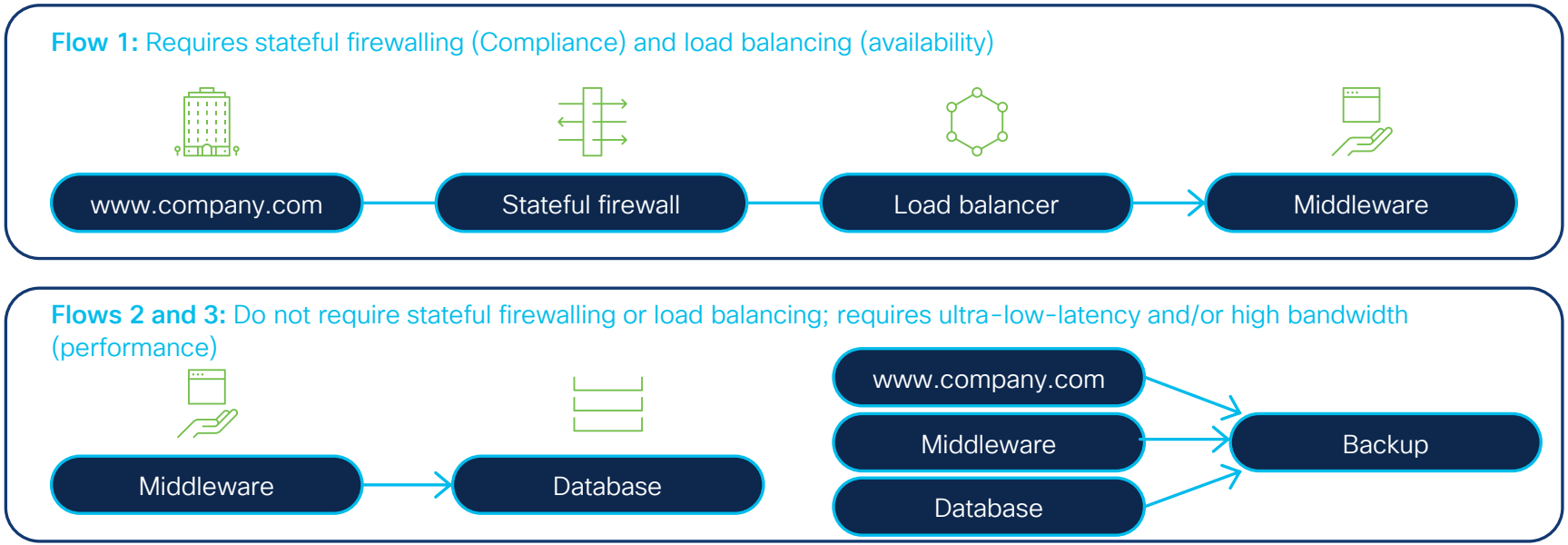
# Advancing the ACI Configuration




Policy Based Redirect with Service Graphs

# Cisco ACI application aware service chaining

Different forwarding treatment for different flows in a multi-tiered web application




**Benefits**

- Redirect specific flows based on business requirements
- Offload traffic from expensive firewalls and load balancers
- Decouple appliance placement from routing table
- Forward traffic based on compliance and performance

# ACI Deployment Options

ACI Anywhere

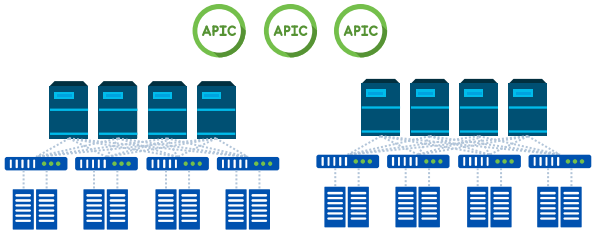
Edge / Remote

Core Data Centers

Hybrid Cloud & Multicloud

IP WAN

IP WAN





ACI
**Remote Leaf**

ACI
**Single-POD**

ACI
**Multi-POD**

ACI
**Multisite**

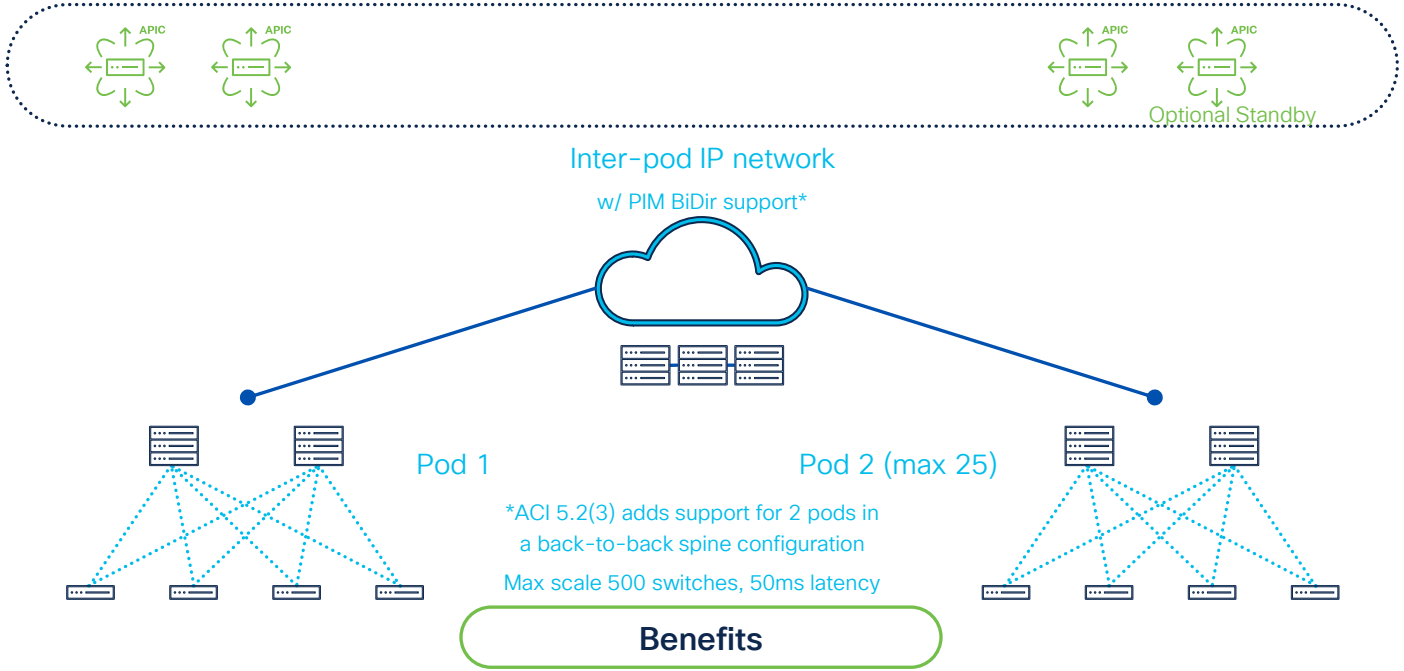
**Cloud**
ACI

**The easiest Data Center and Cloud Interconnect Solution in the Market**

**Try it today!**

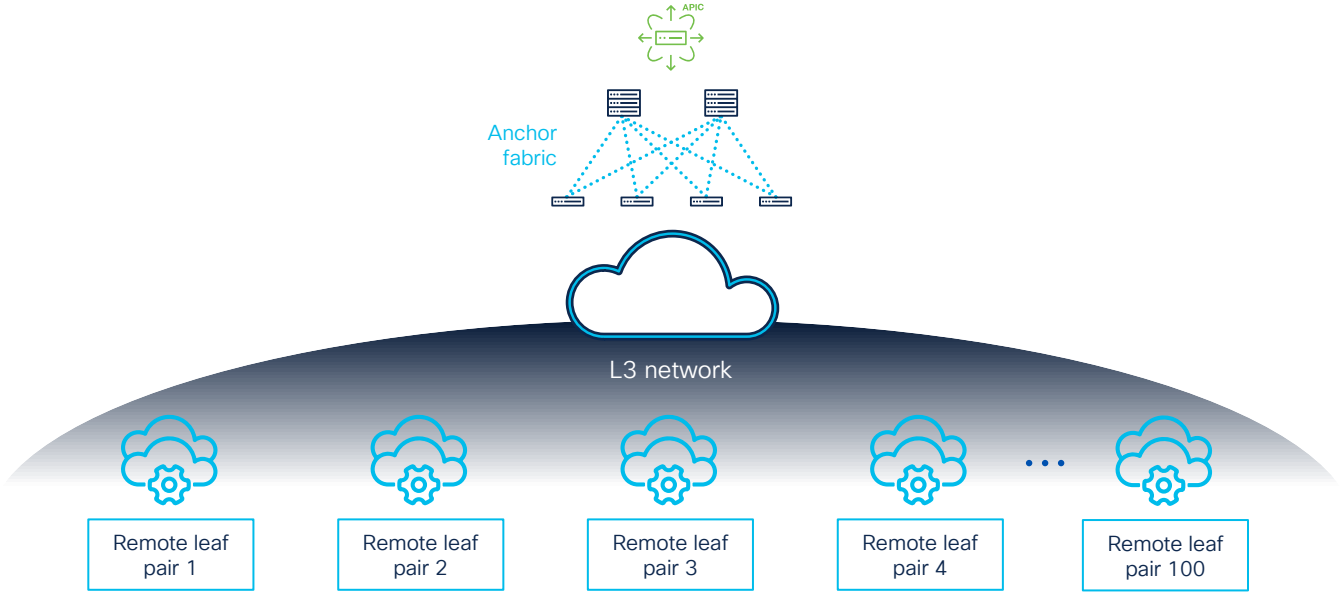
# Cisco ACI multi-pod

Create on-prem availability zones with multiple fabrics, evolution of stretched fabric



# Cisco ACI: Remote leaf

Enable low-touch remote application deployments with the power of Cisco ACI

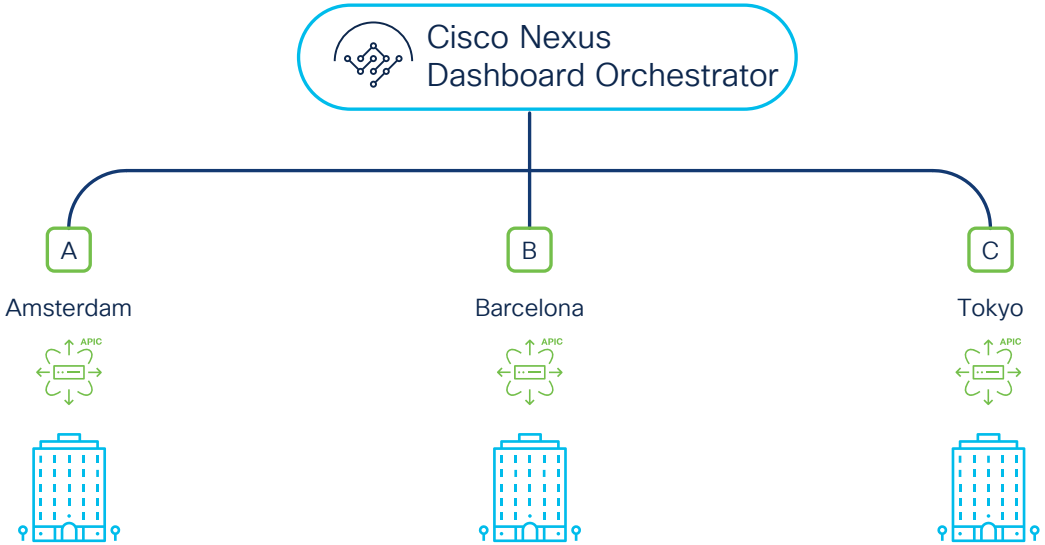



**Benefits**

- Single management plane for core fabric and remote leaf (RL)
- Up to 200 RLs per site
- DC Migration / OTV replacement
- End-to-end security using Cisco ACI's segmentation model

# Cisco ACI multi-site

Create fault tolerant regions in geographically distributed on-prem data centers




**Benefits**

Deploy applications based on geo-performance

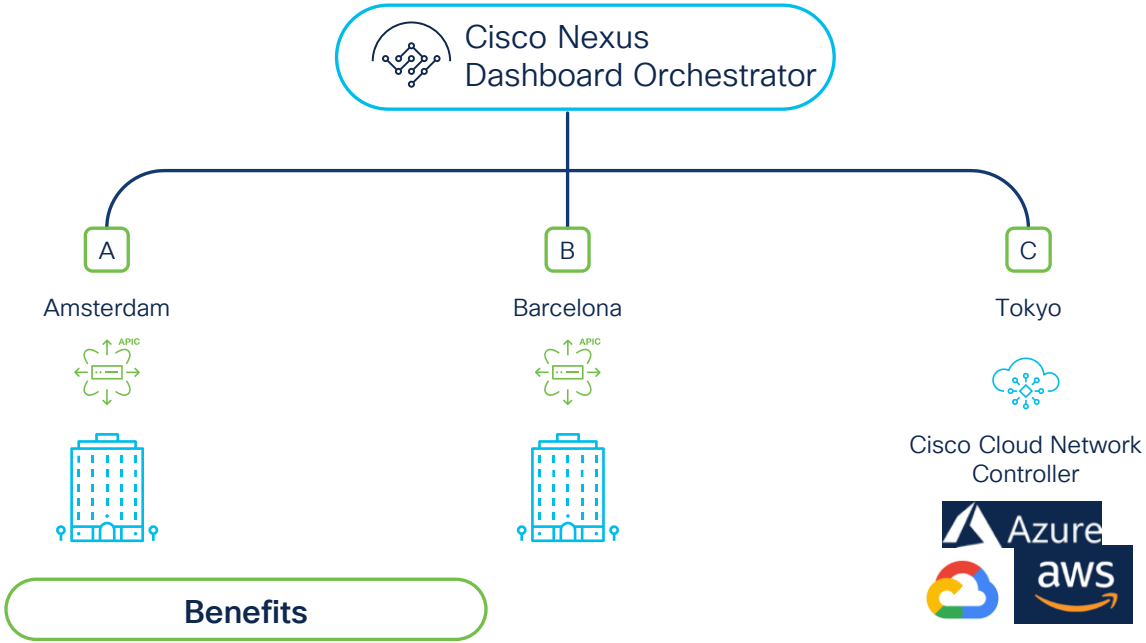
Geo-compliance and data privacy

Limit blast radius to a single application geography

Unify Cisco ACI policy geographically

# Cisco ACI multi-site

Create fault tolerant regions in geographically distributed on-prem data centers and cloud




**Benefits**

Deploy applications based on geo-performance

Geo-compliance and data privacy

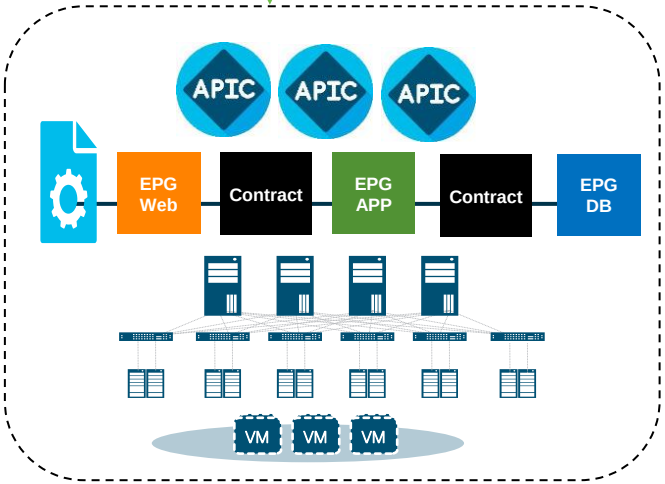
Limit blast radius to a single application geography

Unify Cisco ACI policy geographically

# ACI Policy in the Cloud

Nexus Dashboard Orchestrator

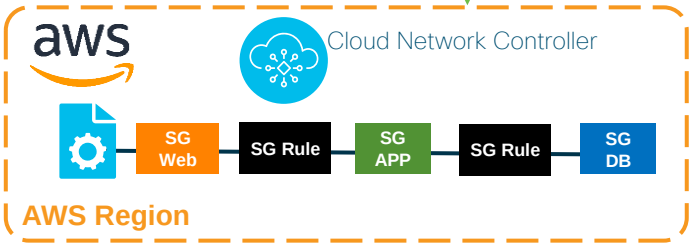
On-Premises DC

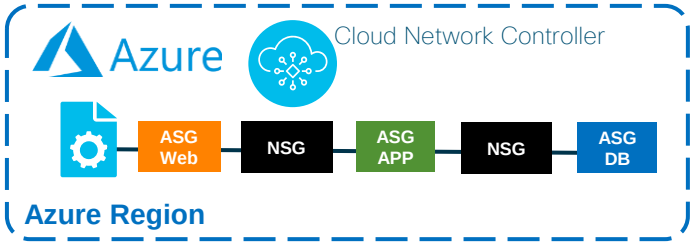



IP Network

IP Network

Public Clouds




Consistent Policy Enforcement on-Premises & Public Cloud

Automated Inter-connect provisioning

Simplified Operations with end-to-end visibility

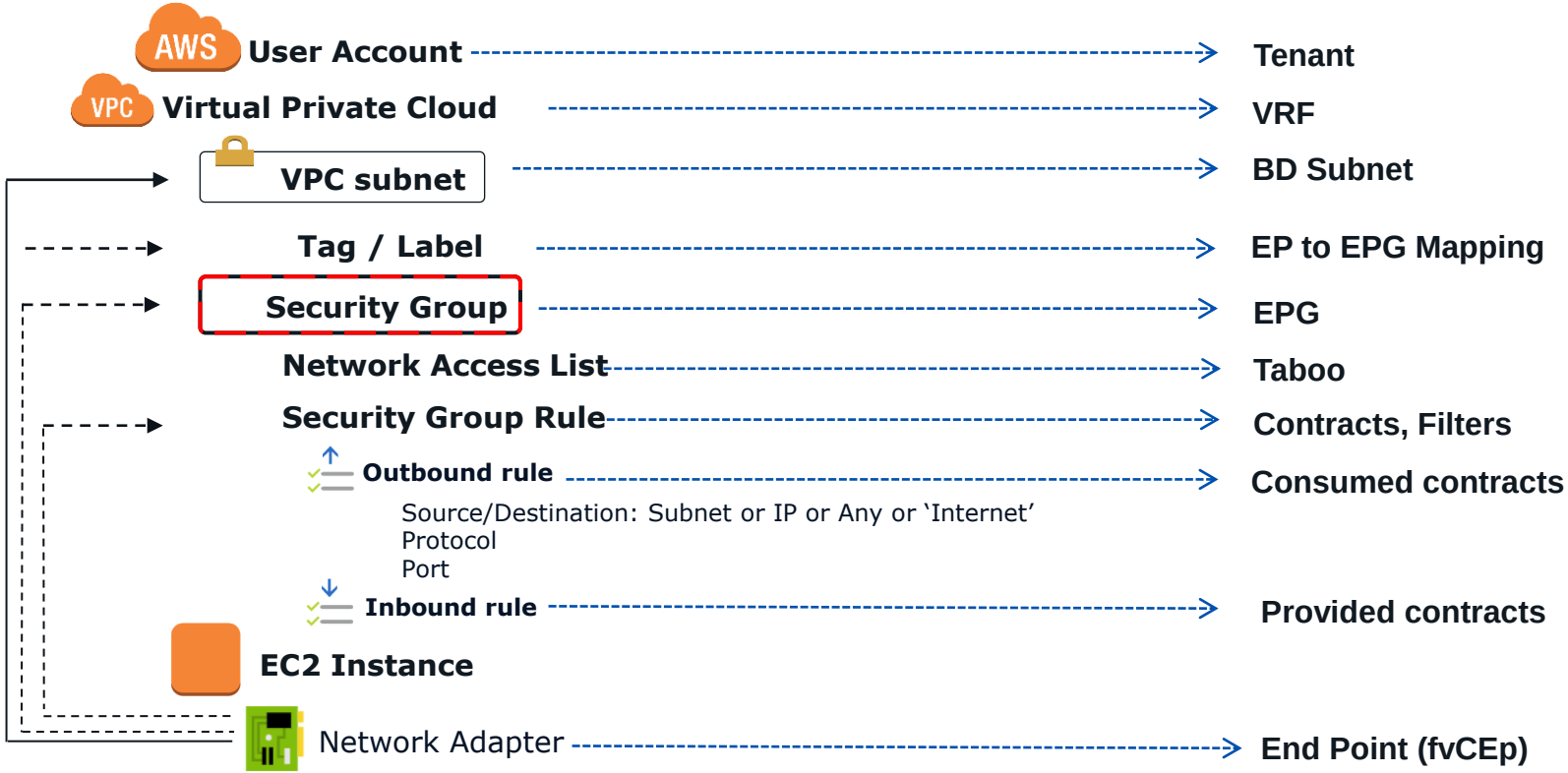
# The network-admin challenge

## Provisioning and monitoring complexity = Risk

| NX-OS | ACI | aws | | |
|---|---|---|---|---|
| Separate Infrastructure + VXLAN | Tenant | Account | Subscription/ Resource Group | Account/Project |
| Data Center | Site/Pod | Region | Region | Region |
| VRF | VRF | VPC | VNet | VPC |
| VLAN | Bridge Domain/ Subnet | CIDR/Subnet | Subnet | Subnet |
| VLAN Tag | Endpoint Groups / Endpoint Security Groups | Security Groups | Application/Network Security Groups | Firewall |
| Access-list (ACL) | Contracts & Filters | Security Group Rules | Security Rules | Firewall Rules |

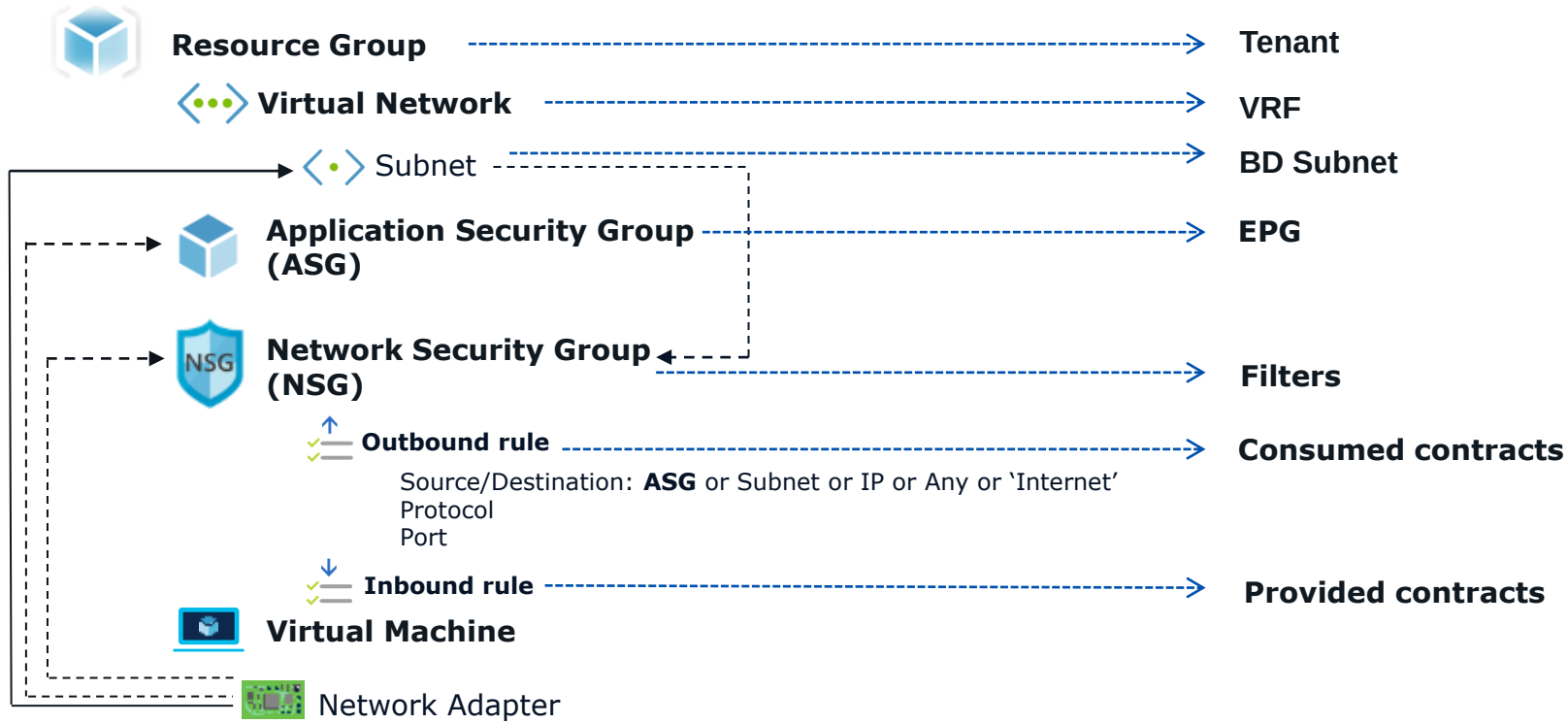
For your info & reference

# Policy Mapping – AWS



For your info & reference

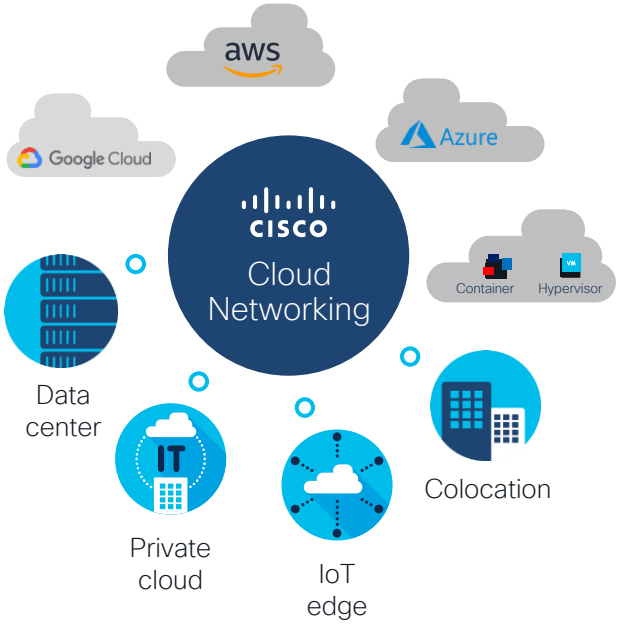
# Policy Mapping – Azure



# ACI Day 2 and Beyond – Making ACI Hum

cisco Live!

# 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.

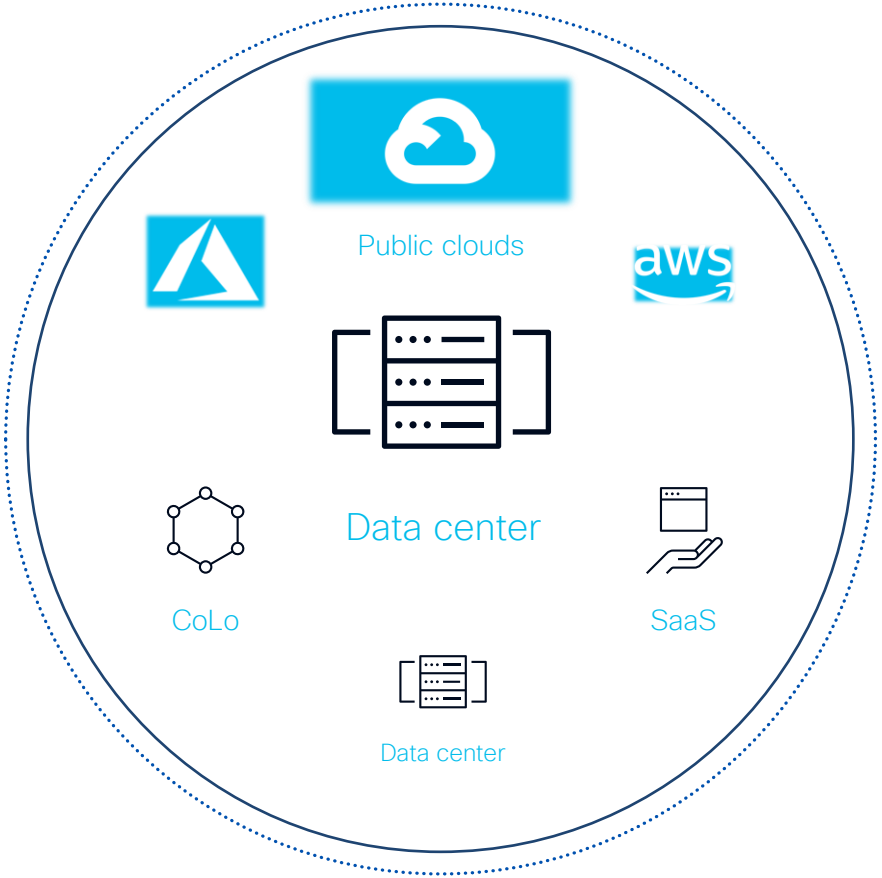
Need for homogenous experience across heterogenous cloud environments

# Solving the customer complexity

## Customer Needs

Cloud-delivered or On-premise
Agility | Simplicity | Turn-key

High performance infrastructure
Speed | Scale | Sustainability



# Cisco Nexus Dashboard

## Simple to automate, simple to consume

Cisco Nexus Dashboard

Powering automation
Unified agile platform


* Roadmap

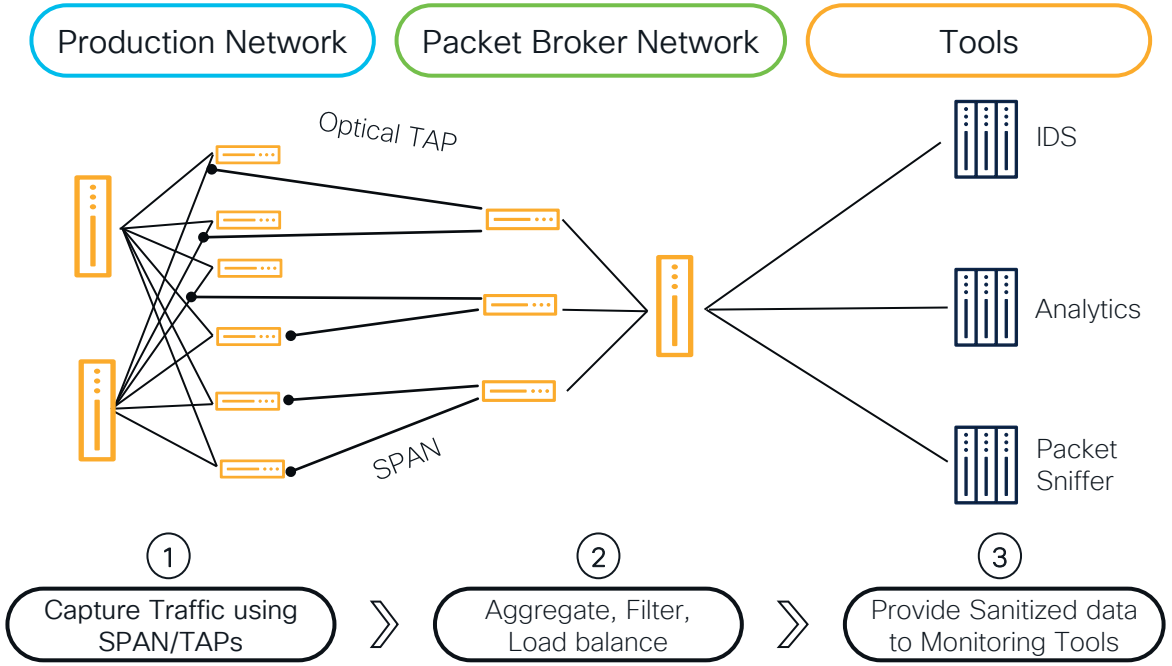
# SPAN and Tap Aggregation

Production Network Types

Cisco NX-OS fabrics

Cisco ACI fabrics

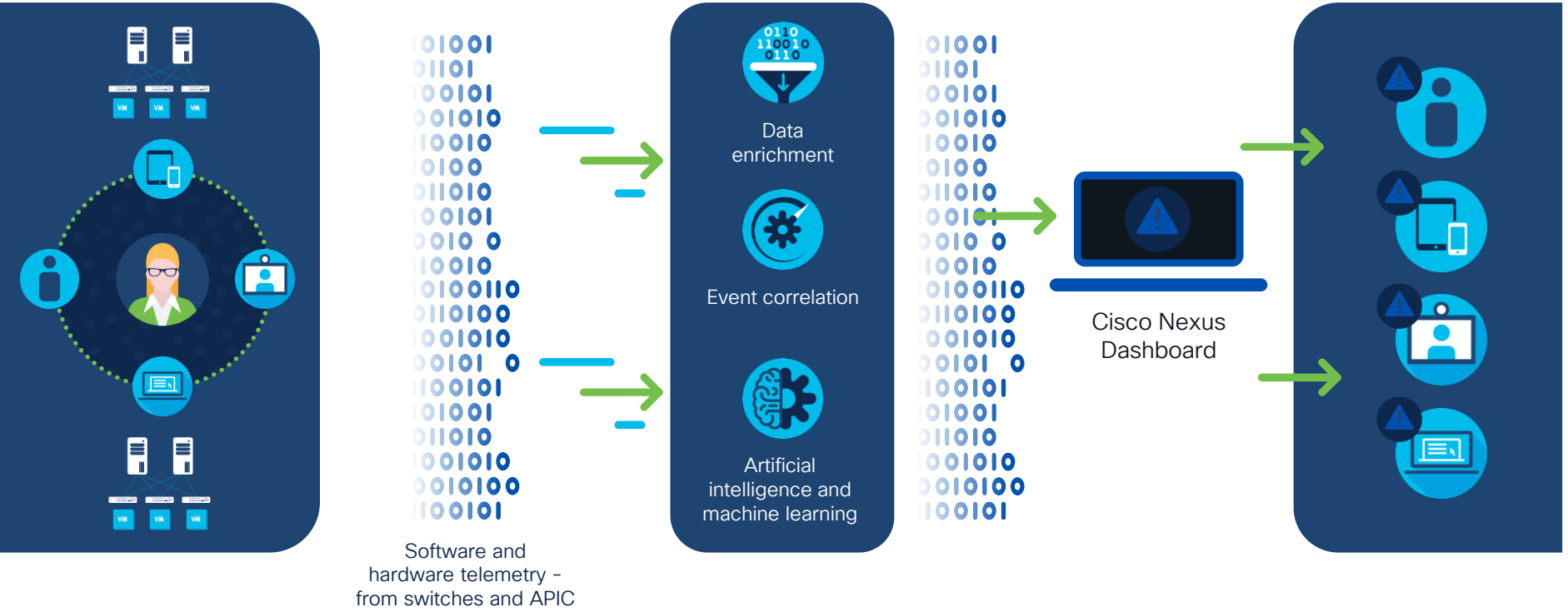
Cisco Enterprise networks




Benefits

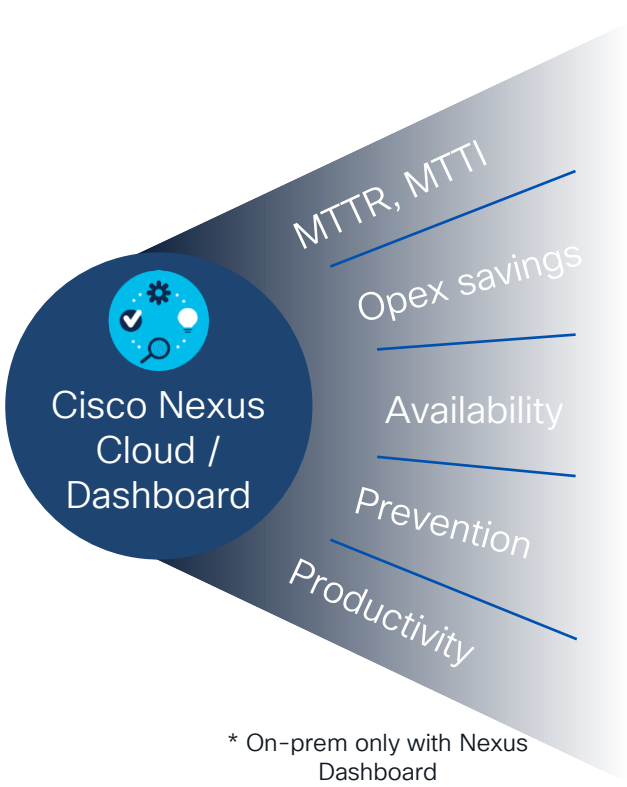
| | | | |
|---|---|---|---|
| Nexus switch functions as packet broker | Cost effective | Turnkey automation with NDDB Controller | Supports Tap Aggregation and inline redirection |

# Intelligent operations powered by telemetry



# Cisco Nexus Dashboard

## Use cases and benefits




* On-prem only with Nexus Dashboard

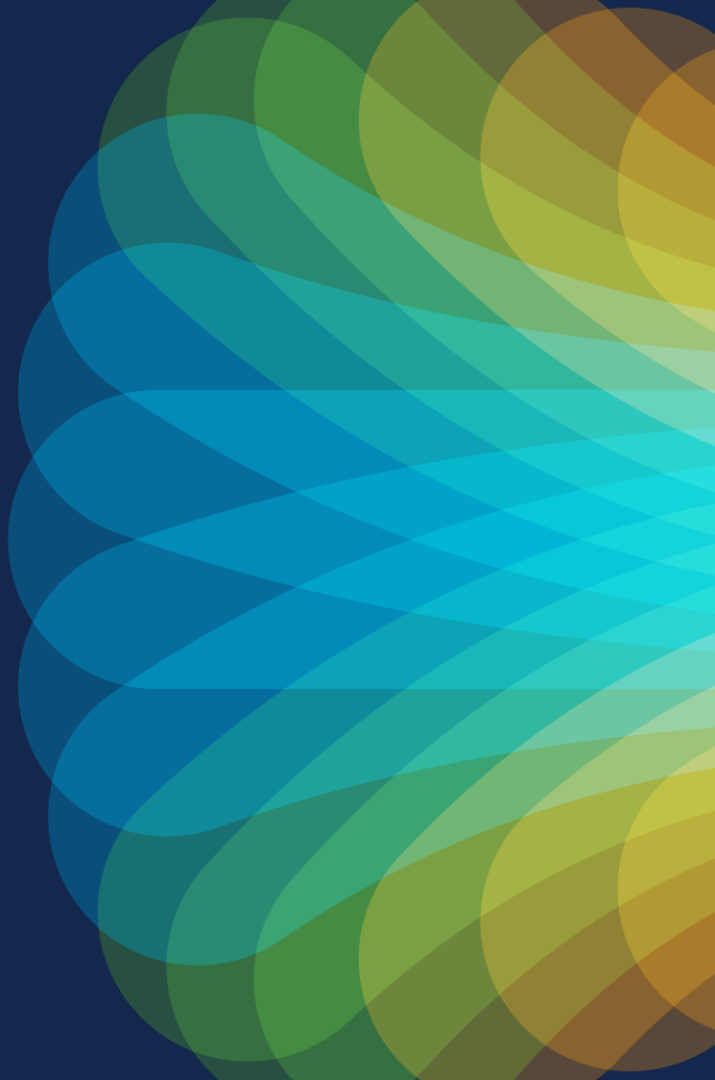
- Identify, locate, root cause, remediate
- Upgrade impact advisories
- Error detection, latency, packet drops*
- Control plane issue
- Mitigate
- Prevent outages
- Automated alerts
- Explorer
- Hardening checks
- Software hardware recommendations
- Pre-change analysis*
- Compliance alerts
- PSIRT notices
- EoS/EoL notices
- End-to-end workflows
- Guided remediation
- TAC assist
- Topology checker

# 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 enables proactive day 2 operations for ACI to give a better understanding of how the applications interact with network

The bridge to possible

# Thank you




cisco Live!
Let's go
#CiscoLive