



You make **possible**



ACI Cloud First

An ACI Fabric without an on-premises DC

Lionel Hercot, Technical Marketing Engineer, IBNG
@LHercot

BRKACI-2683

CISCO *Live!*

Barcelona | January 27-31, 2020



Cisco Webex Teams

Questions?

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

How

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

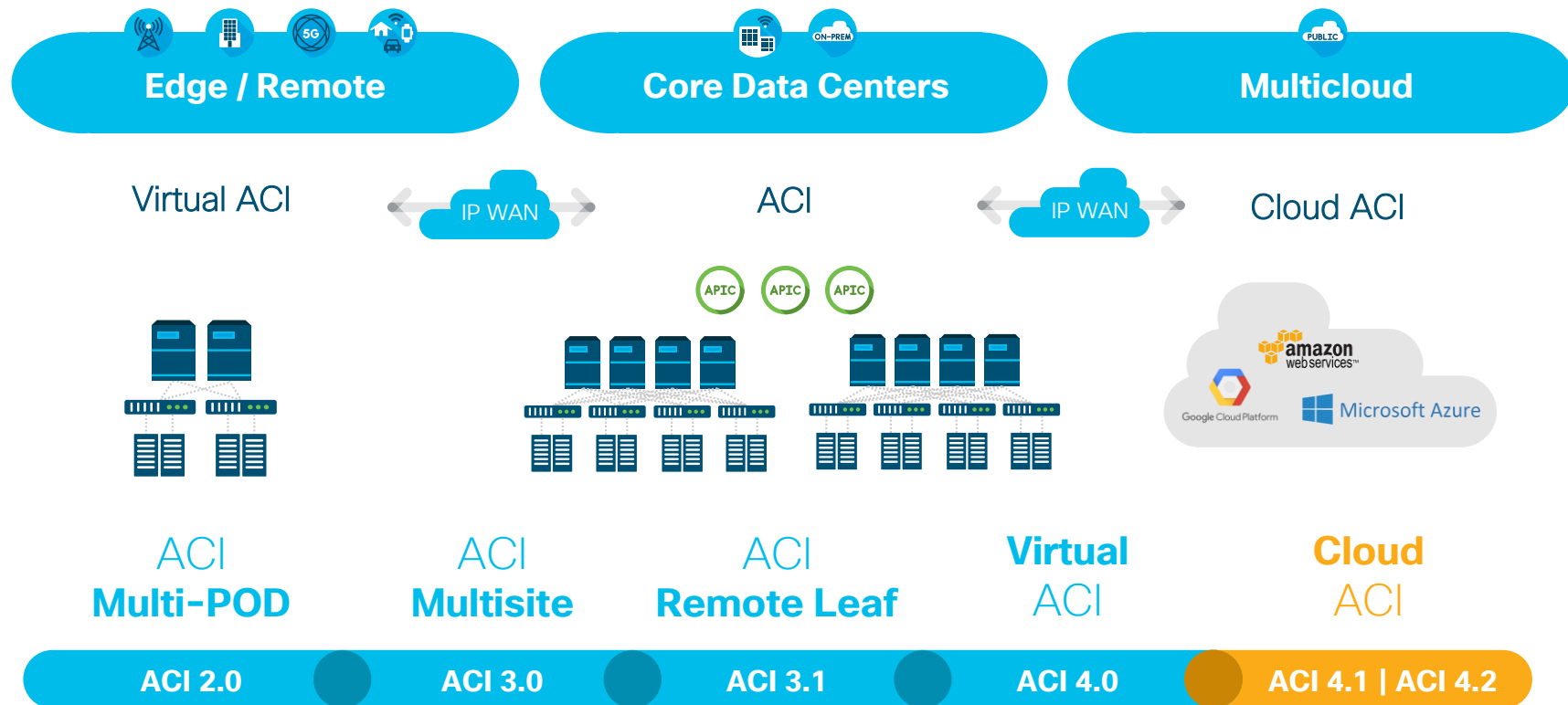


Agenda

- Introduction
 - AWS Cloud 101
 - Azure Cloud 101
- Cloud ACI Architecture
- Use Cases
- Demo
- Conclusion



ACI Anywhere



Challenges in building a Multi Cloud environment



- Building an automated and secure interconnect between On Premises and Cloud datacenters with ease of provisioning and monitoring at scale

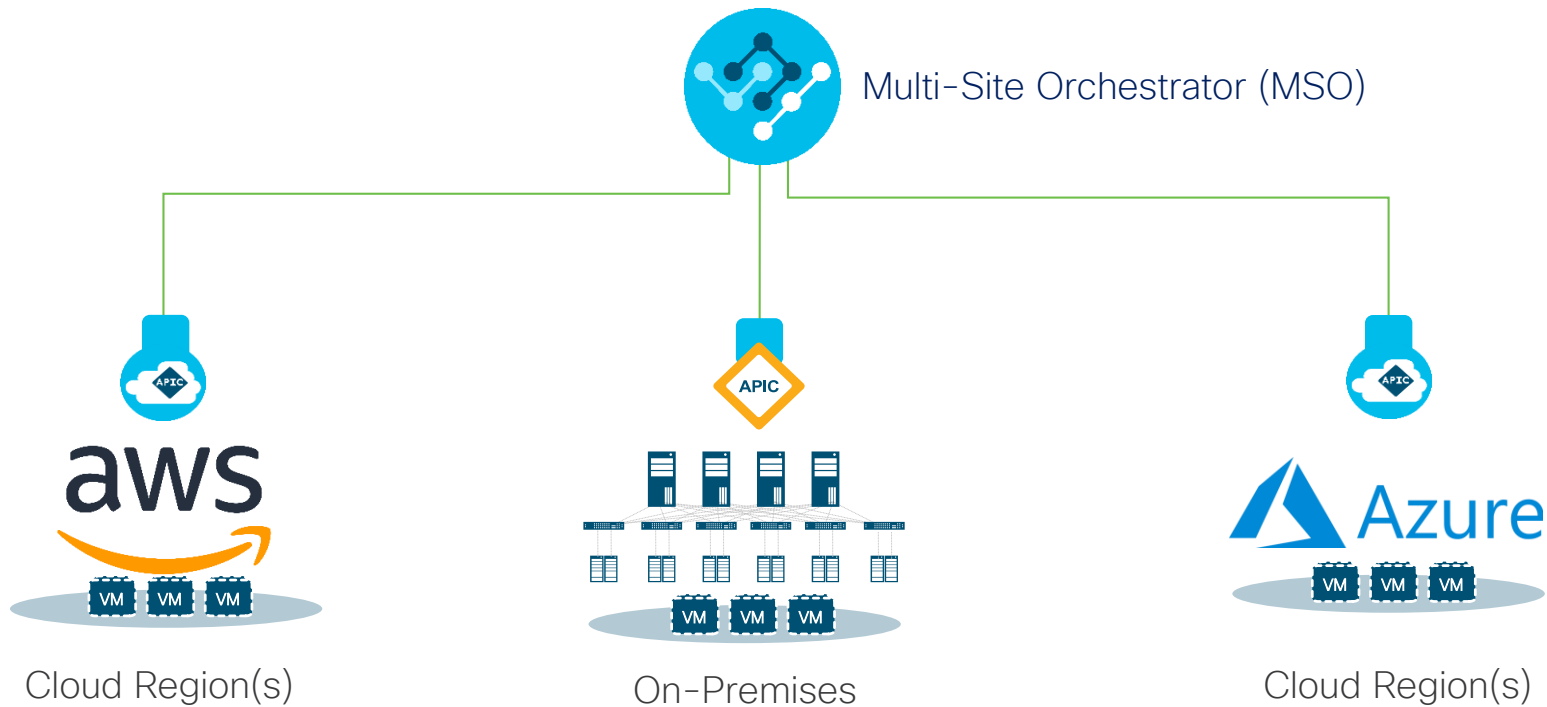


- Maintain consistent policy, security and analytics for workloads deployed across on-premises and cloud locations

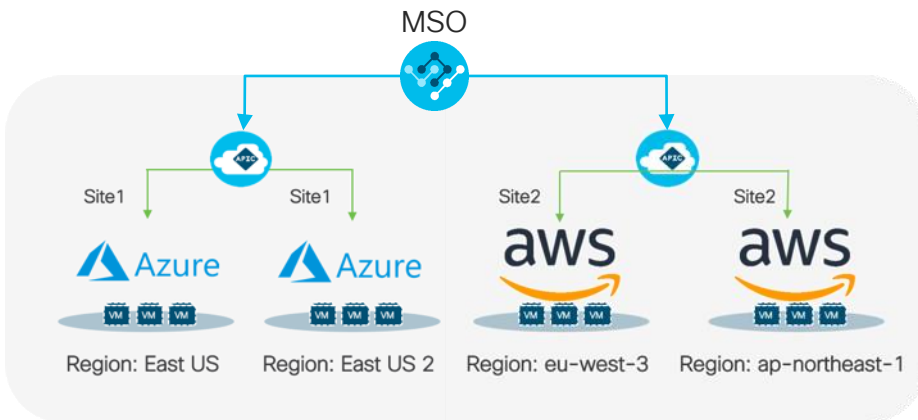
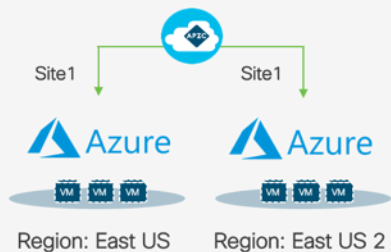


- Requires a single pane of glass to manage policies across on-premises and cloud locations

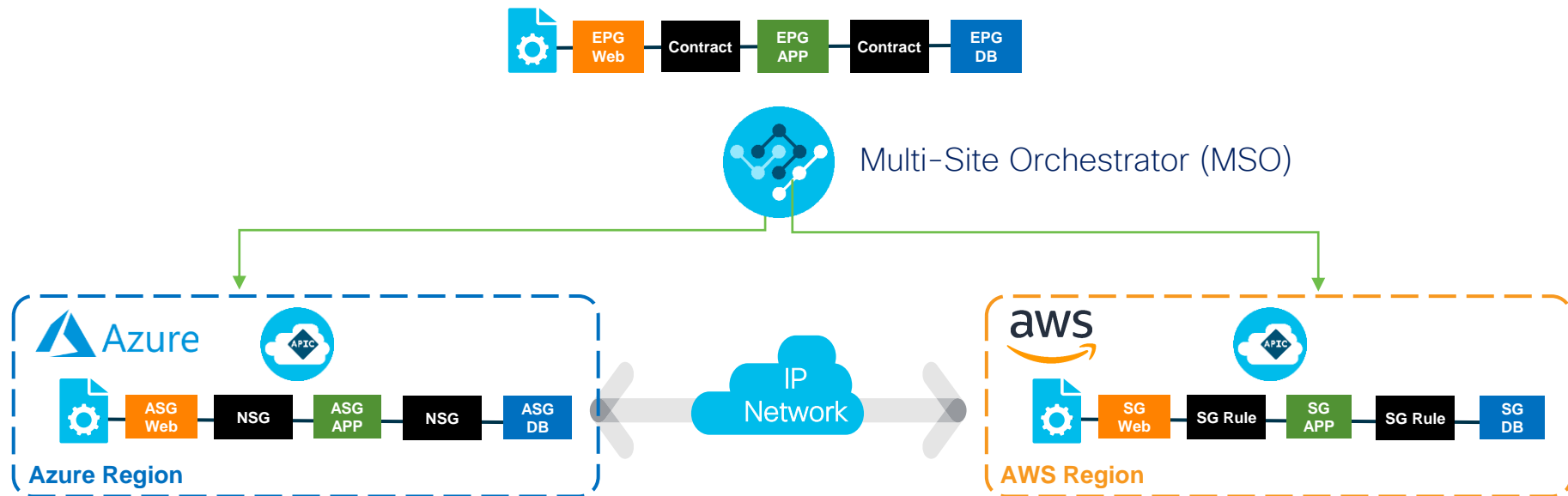
Cloud ACI



Cloud First



Cloud ACI

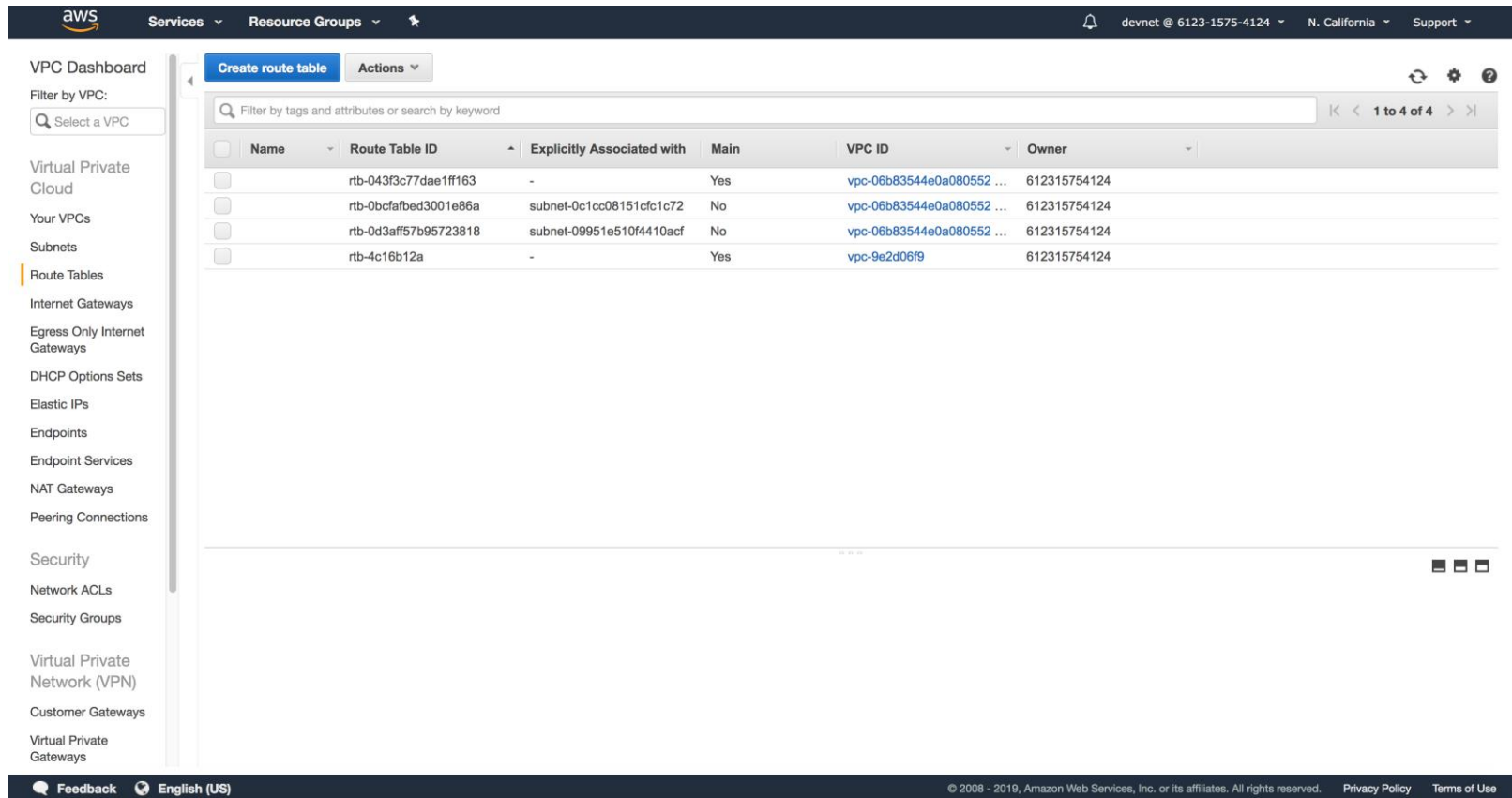


Consistent Policy Enforcement
on-Premises & Public Cloud

Automated Inter-connect
provisioning

Simplified Operations
with end-to-end visibility

Why does this matter?



The screenshot shows the AWS VPC Dashboard. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables (highlighted), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, Virtual Private Network (VPN), Customer Gateways, and Virtual Private Gateways. The main content area displays a table of route tables. The table has columns for Name, Route Table ID, Explicitly Associated with, Main, VPC ID, and Owner. There are four route tables listed. The first three are associated with subnets, and the fourth is the main route table for the VPC.

Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
	rtb-043f3c77dae1ff163	-	Yes	vpc-06b83544e0a080552 ...	612315754124
	rtb-0bcfafeb3001e86a	subnet-0c1cc08151cfc1c72	No	vpc-06b83544e0a080552 ...	612315754124
	rtb-0d3aff57b95723818	subnet-09951e510f4410acf	No	vpc-06b83544e0a080552 ...	612315754124
	rtb-4c16b12a	-	Yes	vpc-9e2d06f9	612315754124

Why does this matter?

WoS-VRF
Virtual network

Search (Cmd+/)

Refresh Move Delete

Resource group (change) : CAPIC_WoS_WoS-VRF_westus
Location : West US
Subscription (change) : ACI-Lionel Hercot-Demos
Subscription ID : 85ca999d-c9c7-484b-82b8-6854bc1e2af5

Address space : 10.101.200.0/24
DNS servers : Azure provided DNS service

Web_cloudapp-ANP
Application security group

Search (Cmd+/) Move Delete

Resource group (change) : CAPIC_WoS_WoS-VRF_westus
Location : West US
Subscription (change) : ACI-Lionel Hercot-Demos
Subscription ID : 85ca999d-c9c7-484b-82b8-6854bc1e2af5

Web_cloudapp-ANP
Network security group

Search (Cmd+/) Move Delete Refresh

Resource group (change) : CAPIC_WoS_WoS-VRF_westus
Location : West US
Subscription (change) : ACI-Lionel Hercot-Demos
Subscription ID : 85ca999d-c9c7-484b-82b8-6854bc1e2af5

Custom security rules : 8 inbound, 8 outbound
Associated with : 0 subnets, 1 network interfaces

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination
101	101	0-65535	Any	Web_cloudapp-ANP	Web_cloudapp-ANP
104	104	3306-3306	TCP	10.101.0.0/24	Web_cloudapp-ANP
106	106	0-65535	Any	10.101.0.0/24	Web_cloudapp-ANP

AWS Cloud 101

AWS Fundamentals

- Regions

Multiple data centers with more than one physical location. Pod or site equivalent in ACI

- Availability Zones (AZ)

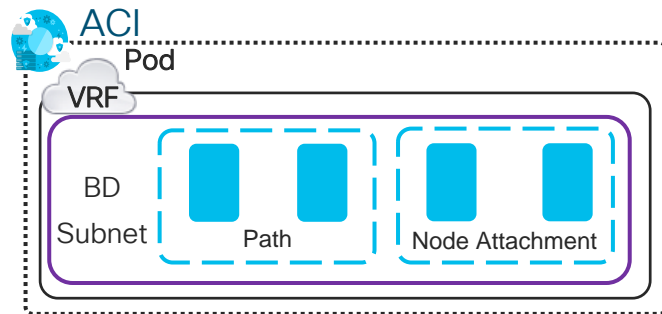
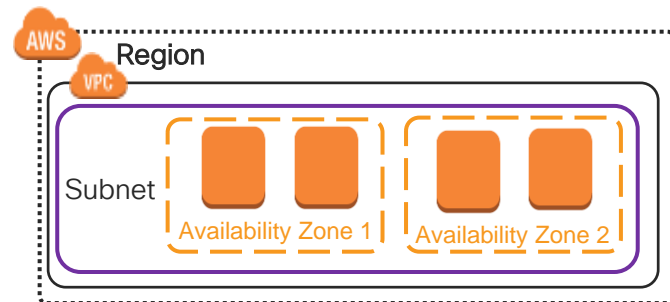
Set of buildings, Internet uplinks and power. Data center but may contains more than one physical location. Path or node attachment equivalent in ACI

- Virtual Private Cloud (VPC)

Set of subnets with one or more CIDR blocks running in a single region across multiple data centers (AZ). Similar to VRF

- Subnet

Range of IP addresses. Each subnet must reside within one AZ and can't span zones. Minimum subnet size is /28. BD Subnet



AWS Fundamentals (Cont.)

- Security Group

Act as a firewall for associated EC2 instance (VM), controlling both inbound and outbound traffic at network interface (EP) level. Equivalent to EPG with white-list

- Security Group Rule

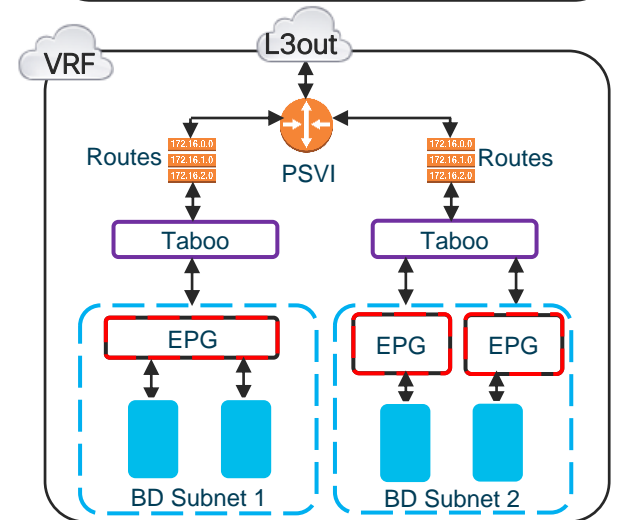
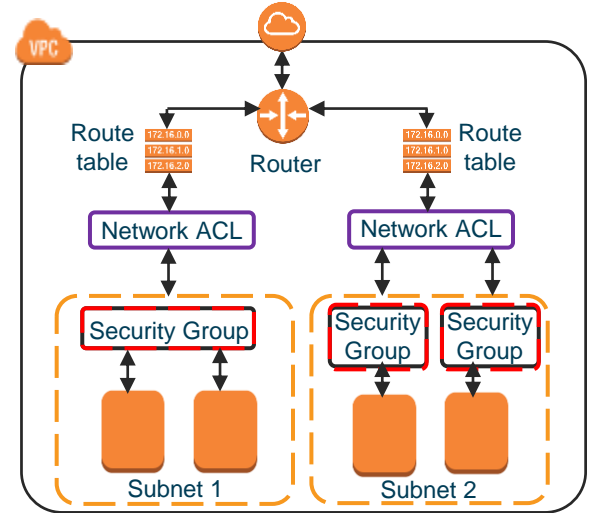
Rules applied to inbound traffic (ingress) or outbound traffic (egress).
Combination of contracts and filters in ACL

- Network ACL

Used to deny / permit select traffic at a subnet level. Network ACLs are stateless. In ACL, it is similar to taboo and grey-list contracts

- Route Table

Can be associated with multiple subnets. Acts like a source-based policy-based routing (PBR) rule.



Connectivity Terms

AWS Only – External Connectivity

- Internet Gateway (IGW)

Horizontally scaled, redundant and highly available VPC component that allows communication between instances in your VPC and the Internet

- NAT Gateway

Acts like an ECMP route to a set of NAT devices

- Virtual Private Gateway (VGW)

is the VPN concentrator. It terminates VPN and AWS Direct Connect. Also provides BGP control plane for route-exchange

- Virtual Private Network (VPN)

comes in two flavors: VPNs provided through VGW and instances running VPN software

- Direct Connect (DX)

Private dedicated link to an AWS region (not encrypted). Used for speed and throughput.

- In ACI, IGW / VGW / DX are equivalent to L3out.

Azure Cloud 101

Azure Fundamentals

The screenshot displays the Azure portal interface for managing subscriptions. The breadcrumb navigation at the top reads 'Home > Subscriptions > ACI-Chris-Demos'. The main header shows 'Subscriptions' with a filter icon and 'ACI-Chris-Demos' with a subscription icon. Below the header, there are three main sections:

- Left Panel:** Contains an 'Add' button, a message 'Showing subscriptions in Cisco-INSBU-ACI. Don't see a subscription? Switch directories', and filters for 'My role' (8 selected) and 'Status' (3 selected). An 'Apply' button is present. Below the filters is a checkbox for 'Show only subscriptions selected in the global subscriptions filter' and a search bar 'Search to filter items...'. At the bottom, there are columns for 'SUBSCRIPTION...' and 'SUBSCRIPTION ID'.
- Middle Panel:** A sidebar with a search bar and a list of navigation options: Overview (selected), Activity log, Access control (IAM), Diagnose and solve problems, Security, Events, and Cost Management.
- Right Panel:** Displays details for the 'ACI-Chris-Demos' subscription. At the top, there are action buttons: Manage, Transfer to a CSP, Cancel subscription, Rename, and Change directory. Below these, the details are organized into two columns:
 - Subscription ID:** c34ec242-1028-4112-8111-1bceef
 - Subscription name:** ACI-Chris-Demos
 - Directory:** Cisco-INSBU-ACI (ciscoinsbuaci.onmicrosoft.com)
 - Current billing period:** 10/1/2019-10/31/2019
 - My role:** Owner
 - Currency:** USD
 - Offer:** Enterprise Agreement
 - Status:** Active
 - Offer ID:** MS-AZR-0017PBelow the details, there is a purple banner with a rocket icon and the text 'For more cost management and optimization capabilities, try Azure Cost Management' with a right-pointing arrow. At the bottom, there is a 'Costs' section.

Subscription: Customer's agreement with Microsoft to obtain Azure services. ~ = Azure account. One user can have multiple subscriptions. Create one or more resource groups in the subscription.

Directory: This is Azure Active Directory used for access control management. For example lhercot@cisco.com belongs to directory cisco.com and directory Cisco-INSBU-ACI so lhercot@cisco.com can access resources in directories cisco.com and Cisco-INSBU-ACI.

Access control (IAM): Used for defining and assigning Roles. Azure has multiple built-in Roles with different permission levels. Cisco cAPIC must have at least Contributor Role for Read/write access to the account (subscription)

Azure Fundamentals (Cont. 1)

- Regions

Multiple data center with more than one physical location in large geographic location.

- Resource Group

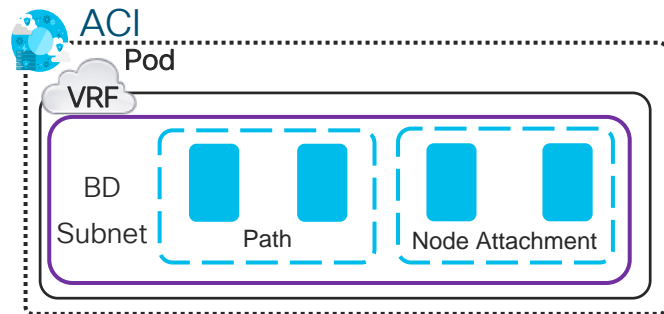
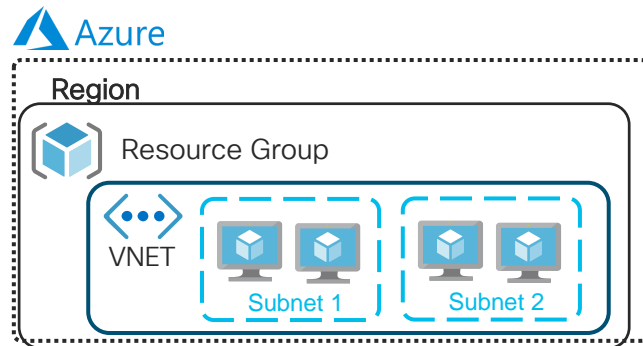
A container in Resource Manager that holds related resources for an application or a subset of one.

- Virtual Network (VNET)

Network construct with a set of subnets from an Address Space running in a single region across multiple data centers. Similar to VRF

- Subnet

Range of IP addresses. Each subnet can span a complete region. Minimum subnet size is /28. BD Subnet



Azure Fundamentals (Cont. 3)

- Application Security Group (ASG)

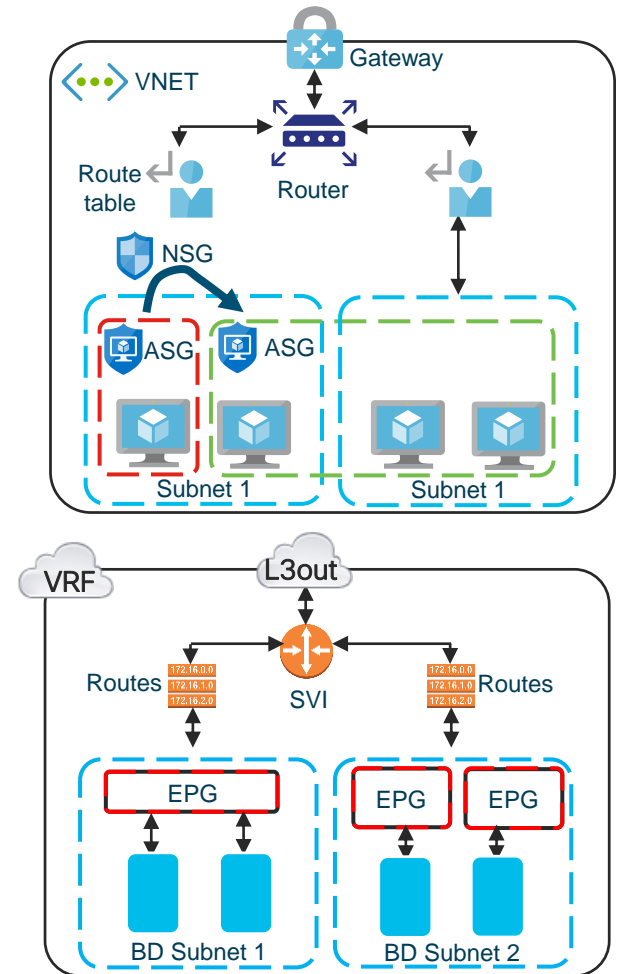
Group virtual machines together. Allow to apply Network Security Group (rules) at scale between Application Security Group. Equivalent to EPG.

- Network Security Group (NSG)

Contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. NSG can be applied between ASGs. Combination of contracts and filters in ACI.

- Route Table

Can be associated with multiple subnets. Allow to modify the routing behavior in a set of subnets.



Connectivity Terms

Azure Only – External Connectivity

- Outbound connections

Azure automatically do PAT for traffic generated by VMs with internal IP addresses. VMs can be assigned Instance-Level Public IP addresses to achieve NAT.

- VPN Gateway (VNG)

Virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. Each virtual network can have only one VPN gateway. Support BGP to exchange routes with peer router.

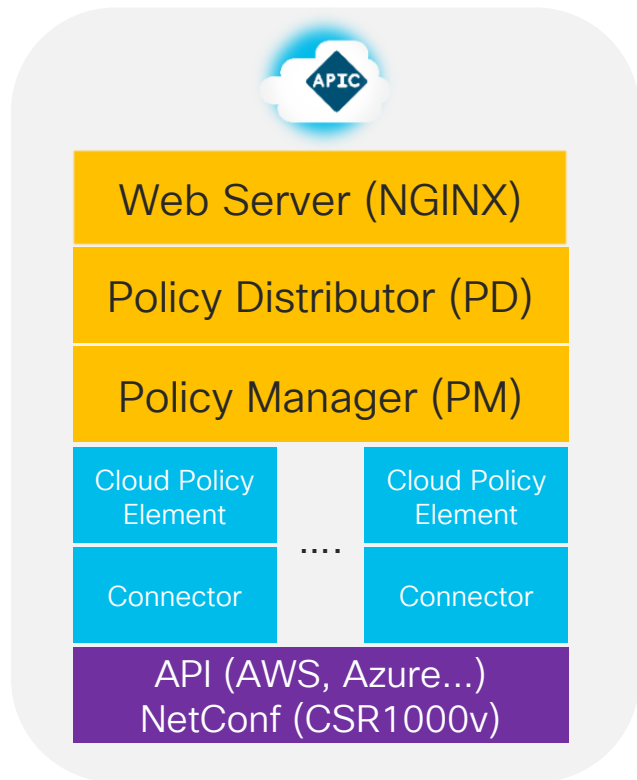
- ExpressRoute

Private dedicated link to an Azure region (not encrypted). Used for speed and throughput. Support BGP to exchange routes with peer router.

- In ACI, Outbound connections / VNG / ExpressRoute are equivalent to L3out

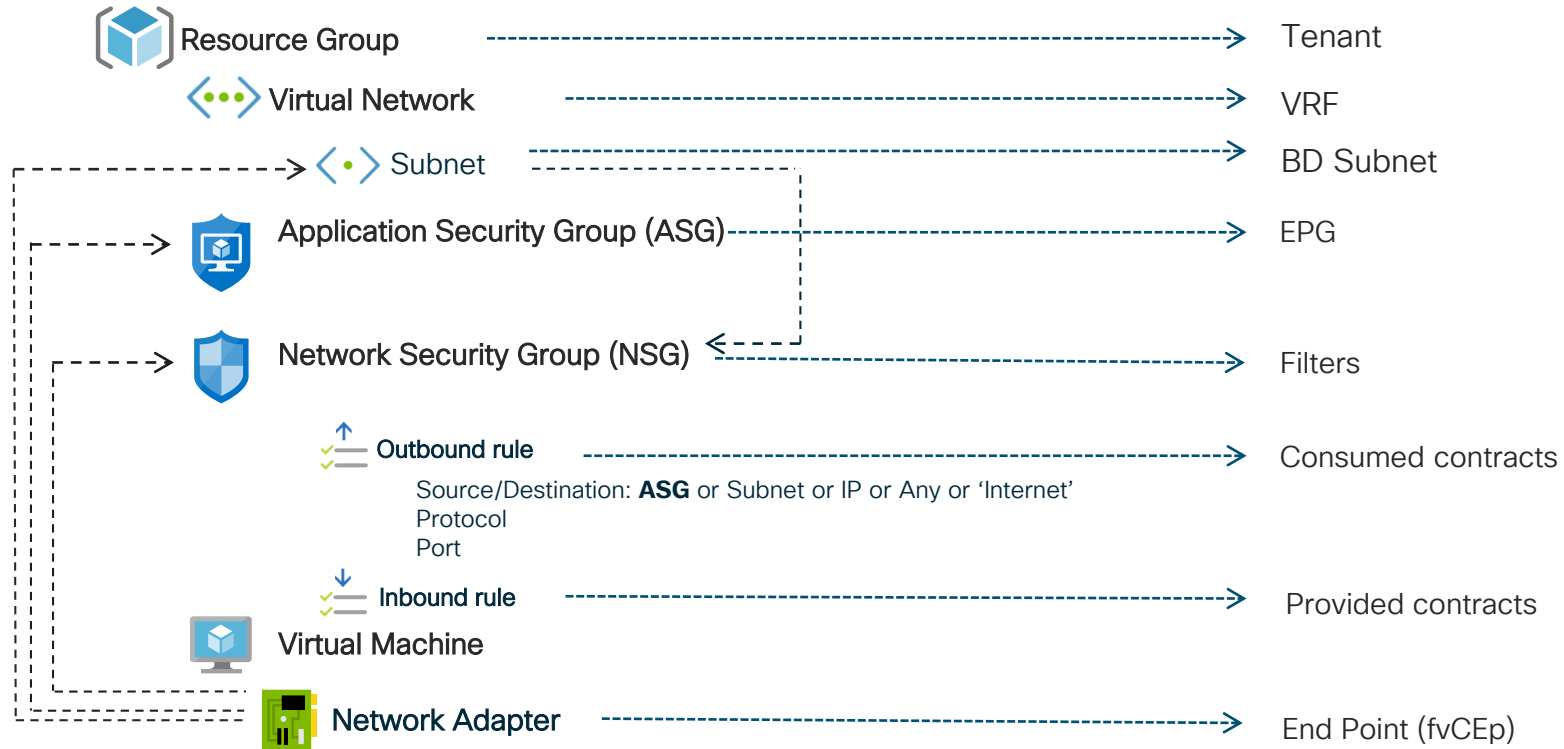
Architecture

Cloud APIC Architecture

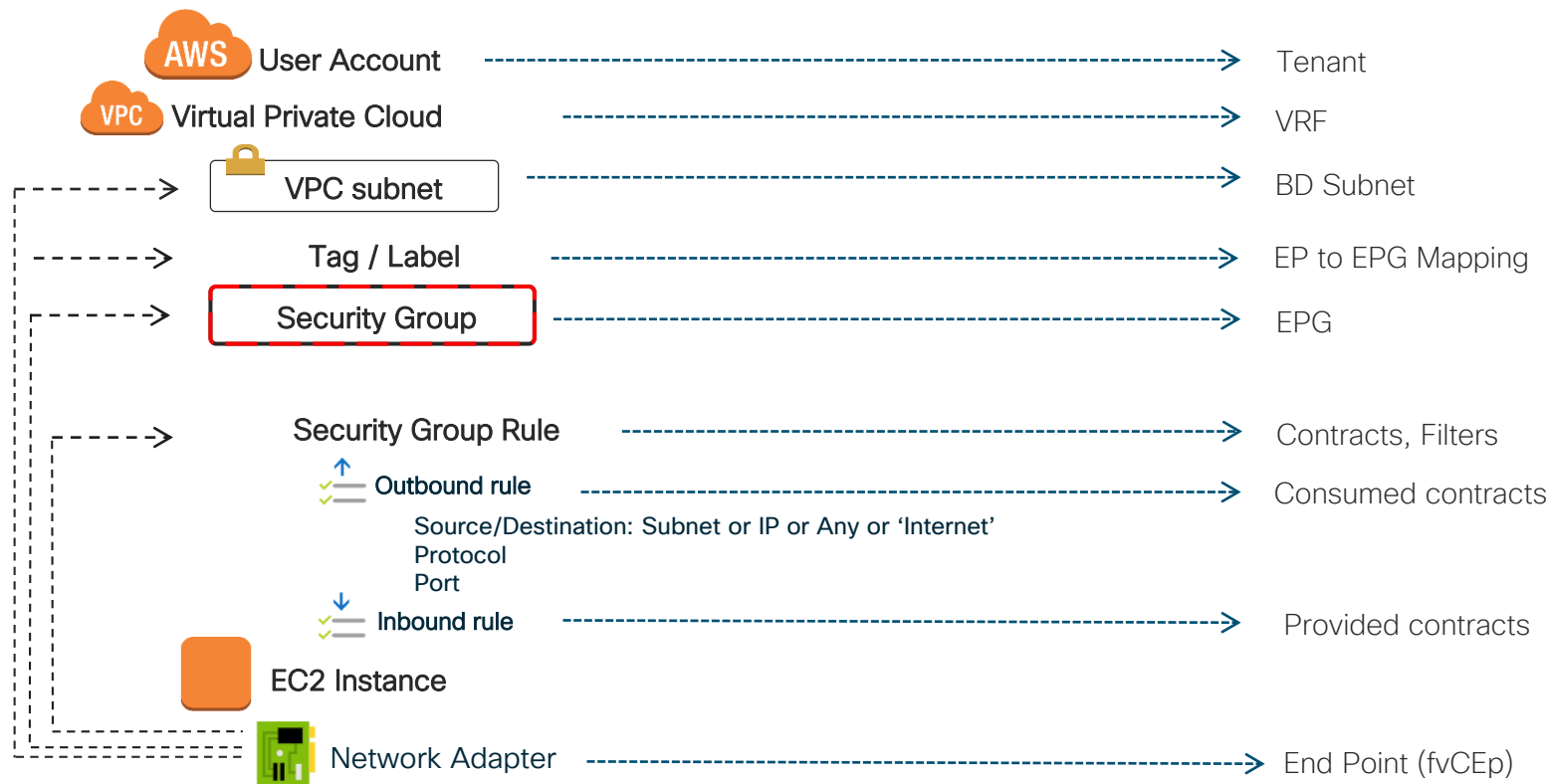


- Virtual Form Factor of APIC
- Automates / Manages Cloud Routers
- Translates ACI Policy to cloud native constructs
- Deploys cloud resources and infrastructure components
- Intuitive GUI and Similar ACI UI look and feel
- REST API North Bound Interface
- cAPIC manages 1 or more regions

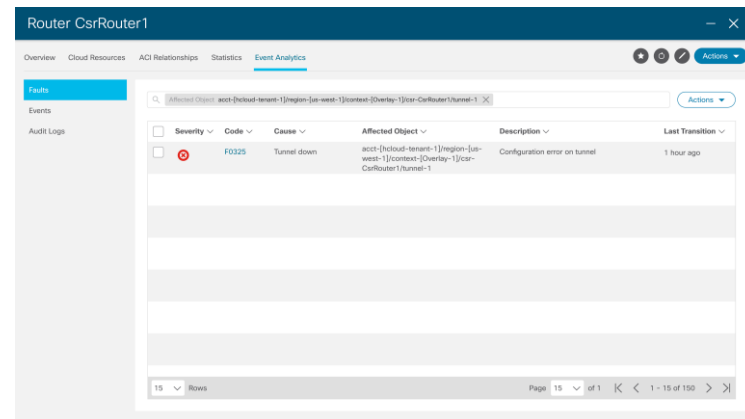
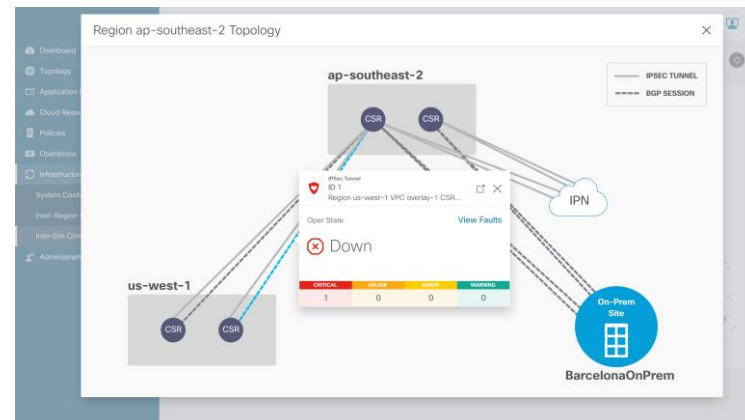
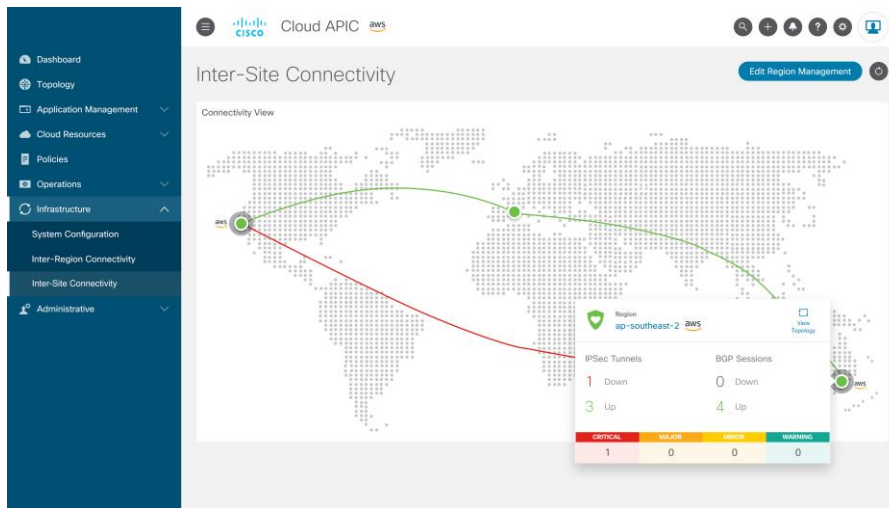
Policy Mapping - Azure



Policy Mapping - AWS



Topology Health



- Network connectivity and Health

Endpoints in an EPGs

EPG Web

OverviewTopologyCloud ResourcesApplication ManagementStatisticsEvent Analytics

Virtual NetworksEndpointsSecurity Groups

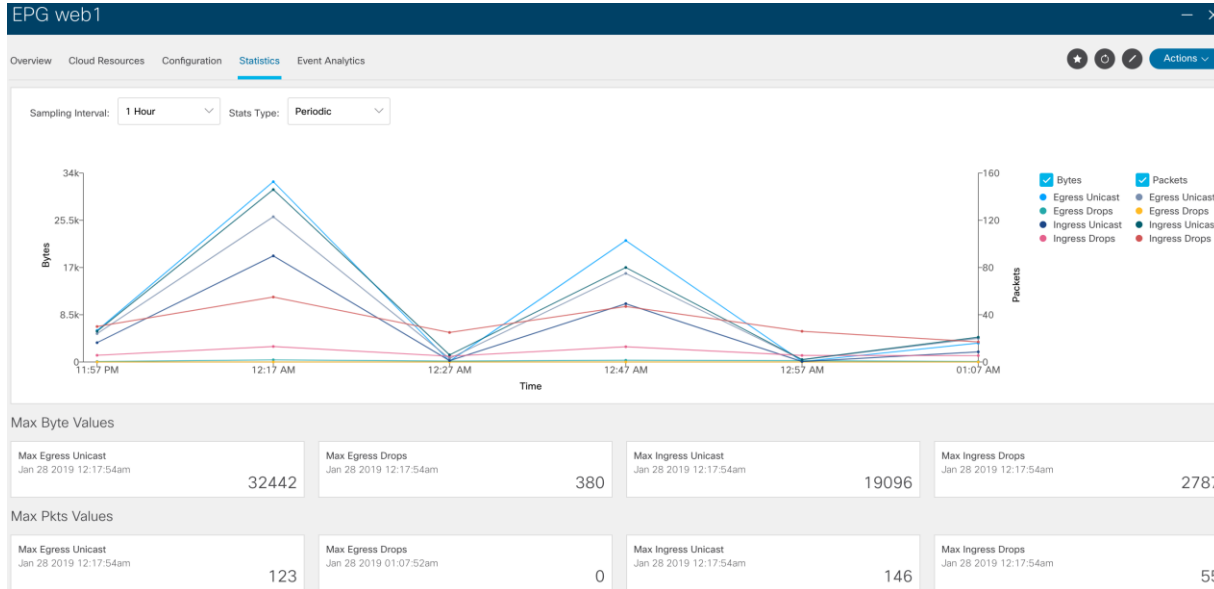
Filter by attributes

						Application Management	Cloud Resources	
Name	Oper State	Private IPv4 Addr.	Public IPv4 Addr.	EP Type	EPGs	Security Groups	Virtual Machines	
wos-wordpress946 WoS > westus > WoS-VRF 10.101.200.0/24 > 10.101.200.0/24 > 10.101.200.128/25	in-use	10.101.200.132	13.64.103.72	vm	1	1	1	

10Rows

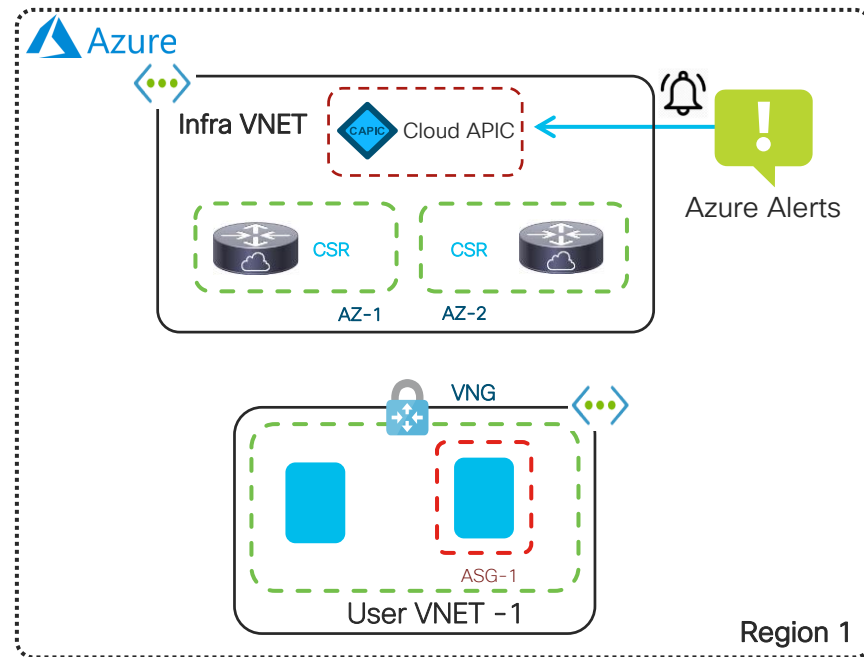
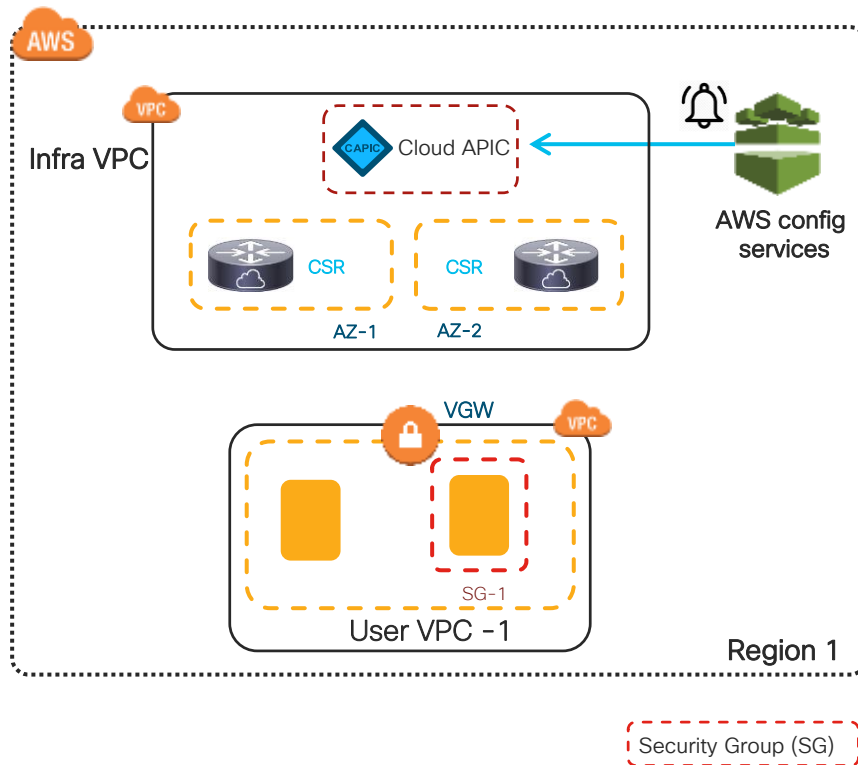
Page 1 of 11-1 of 1

Statistics



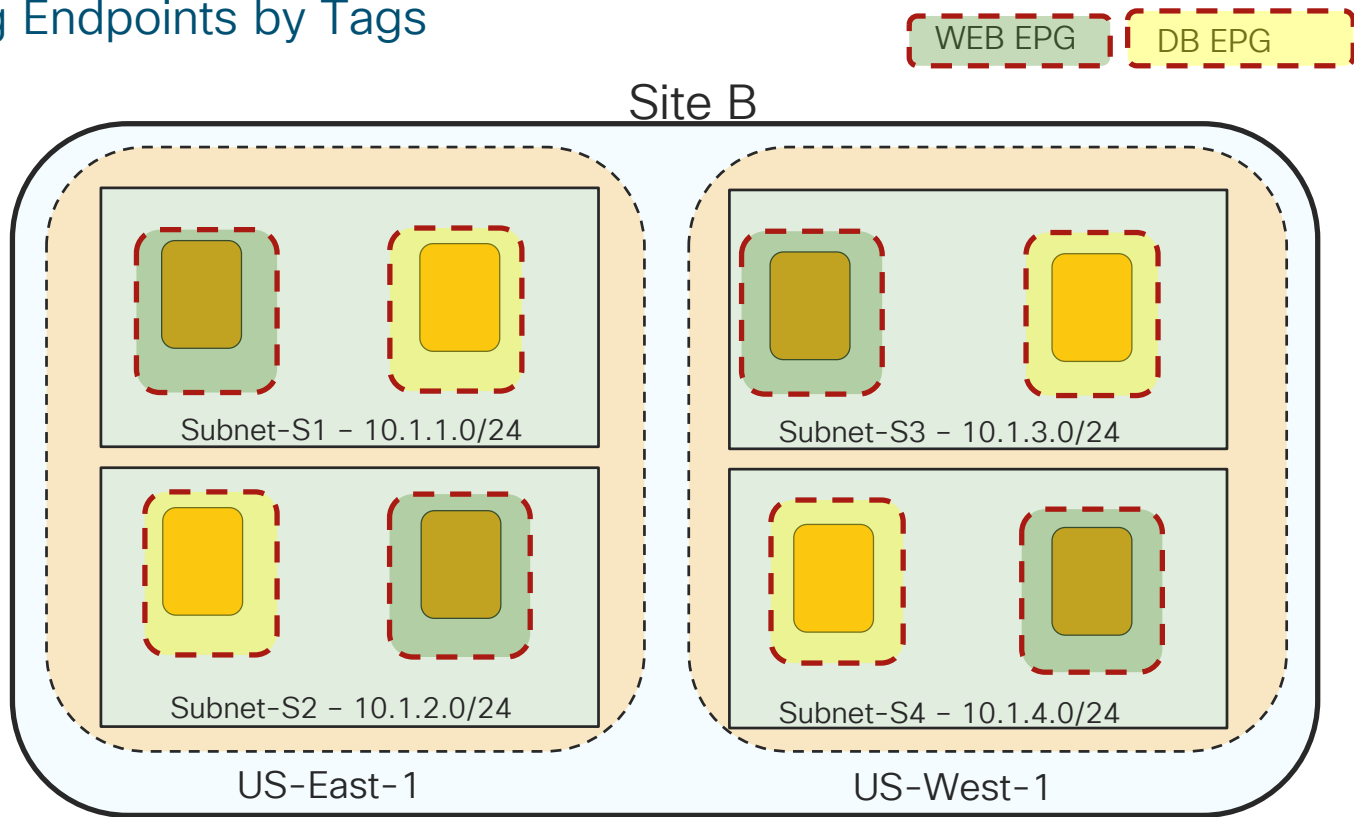
- We will show multiple statistics:
 - Inter-site
 - Inter-region
 - Inter-VPC
 - Cloud EPG
 - Cloud Routers

End Point Learning in Cloud

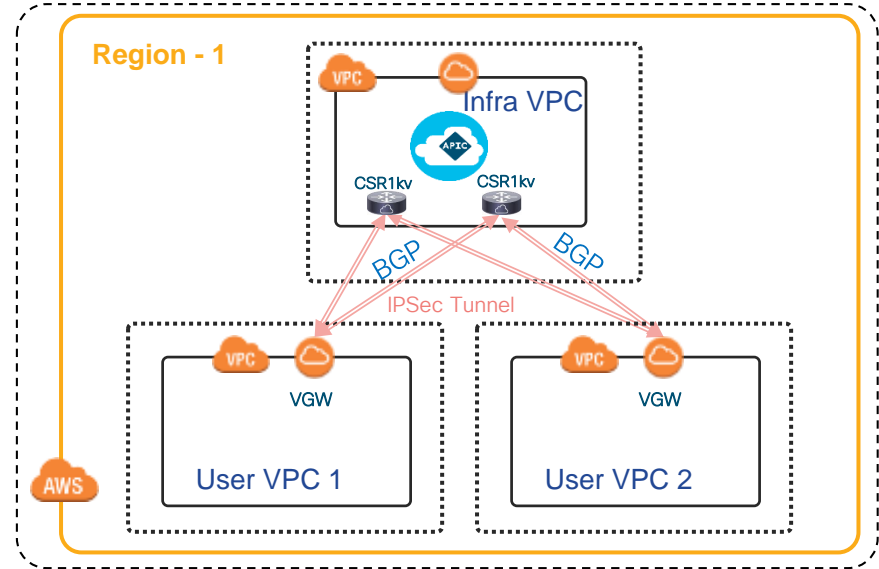
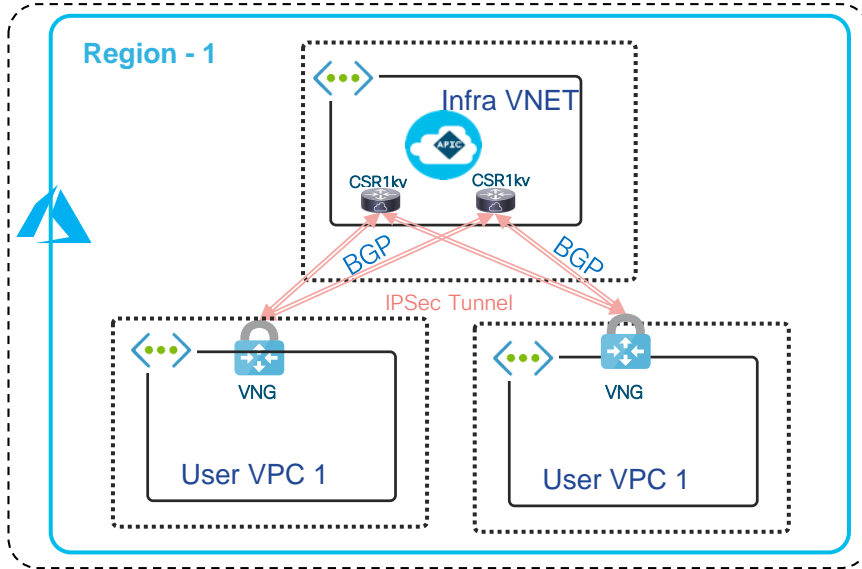


Cloud EPG

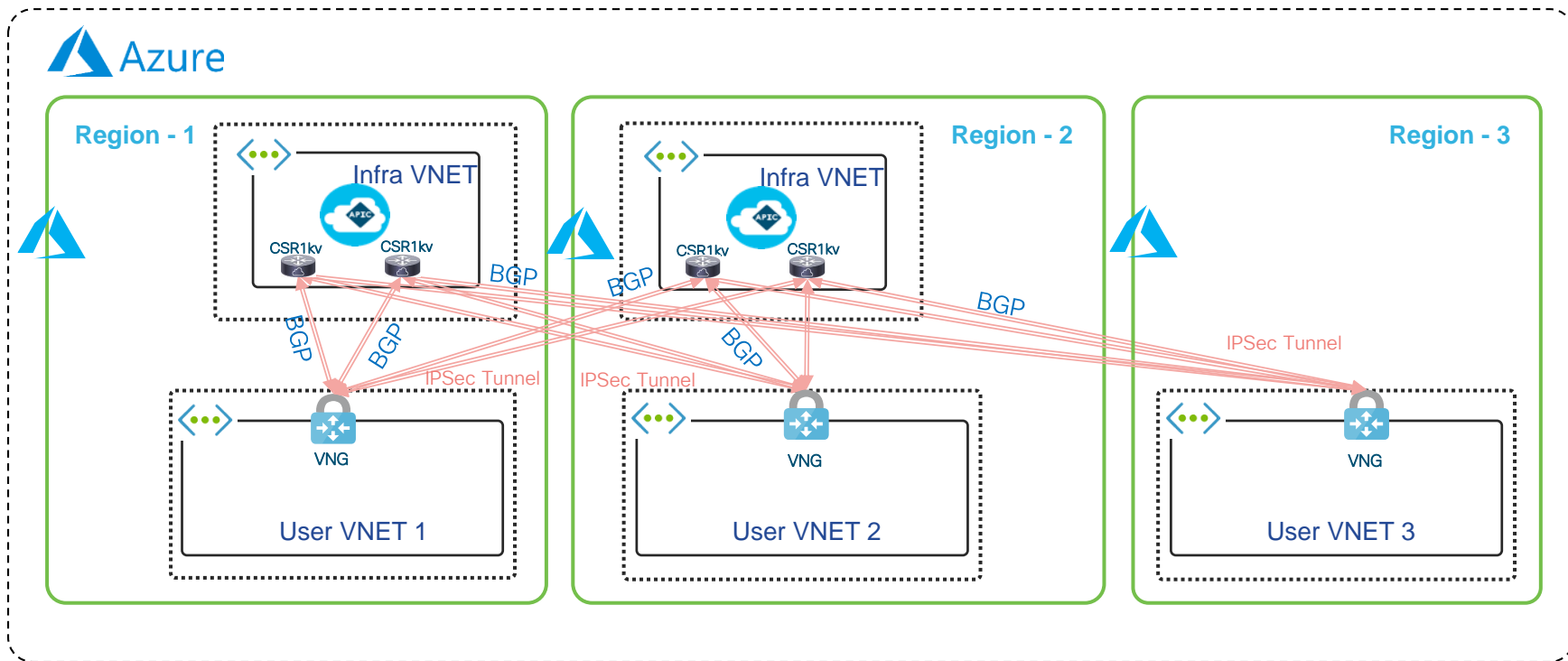
Mapping Endpoints by Tags



Cloud ACI Architecture



Architecture across regions



Let's Multi-Cloud

ACI Multi-Cloud First



MSO Form Factor



Hardware Appliance
(based on SE)

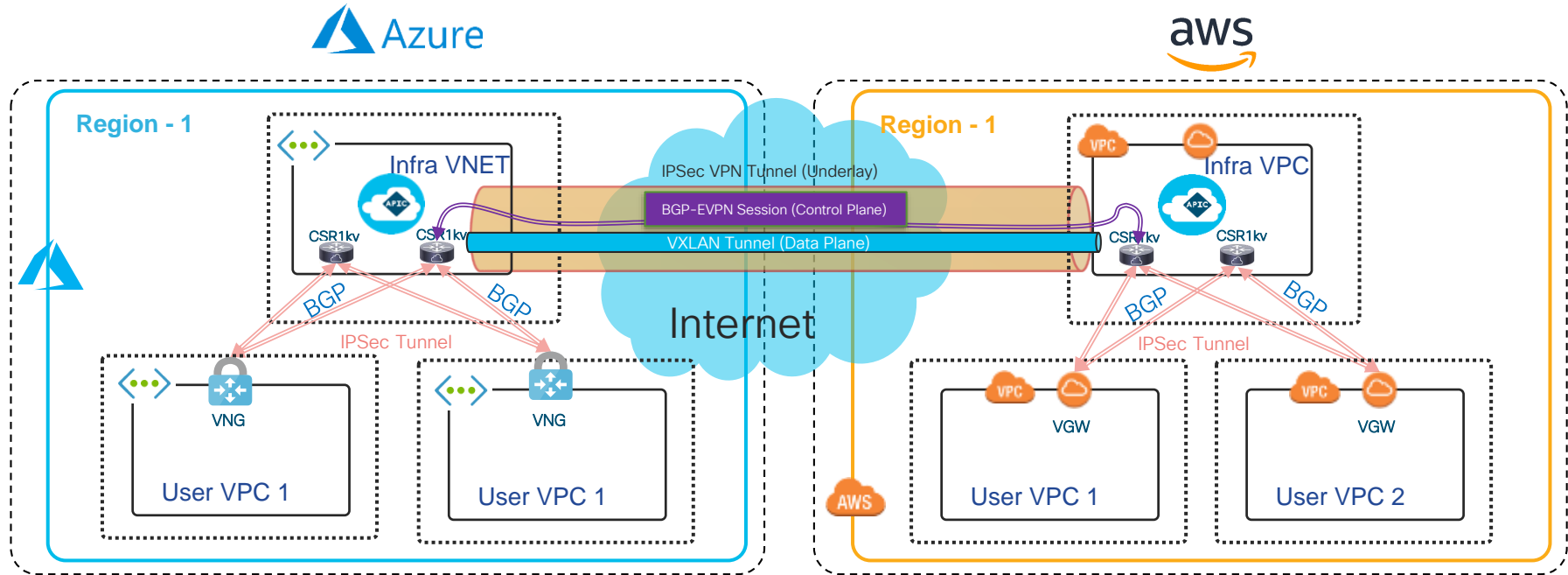


VMware OVA



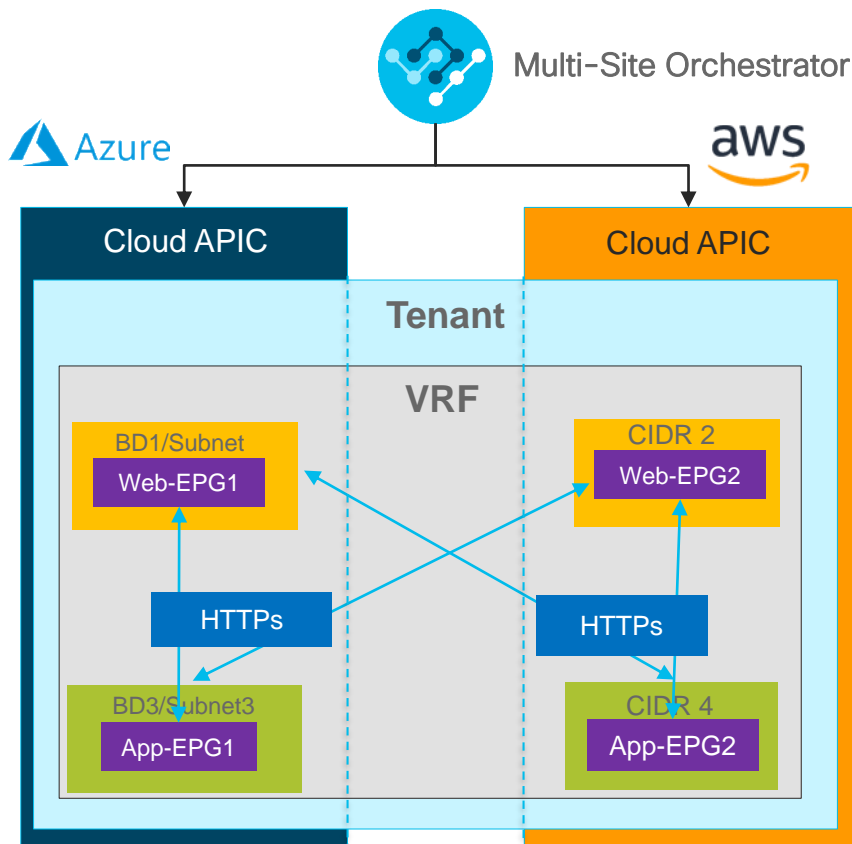
Cloud MSO for AWS

Multi-Cloud Architecture



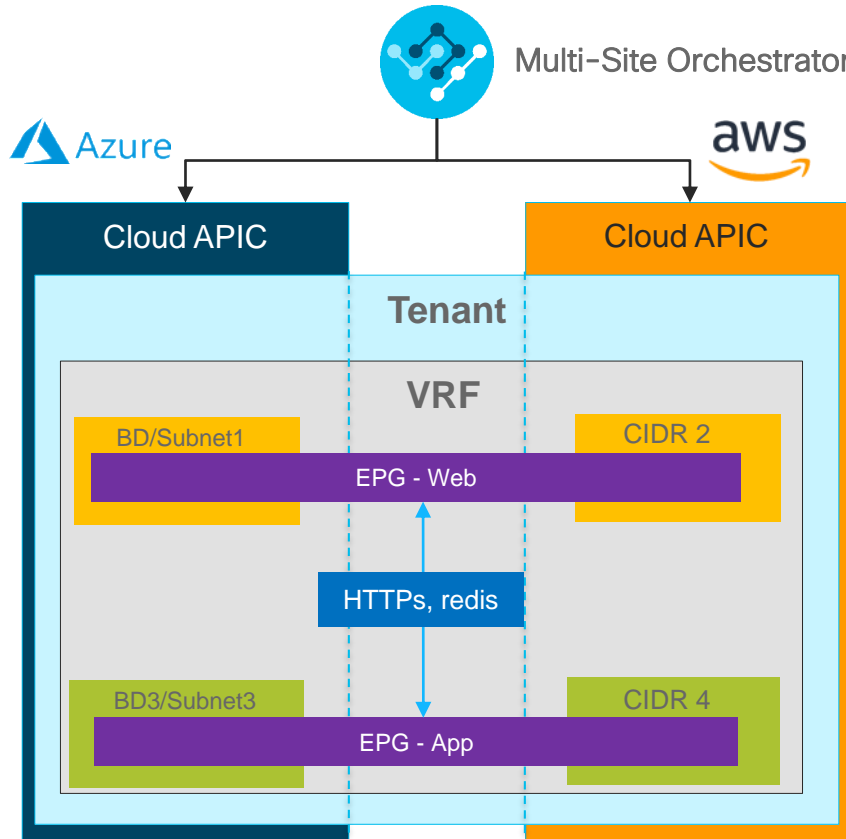
Use Cases

Application Stretch



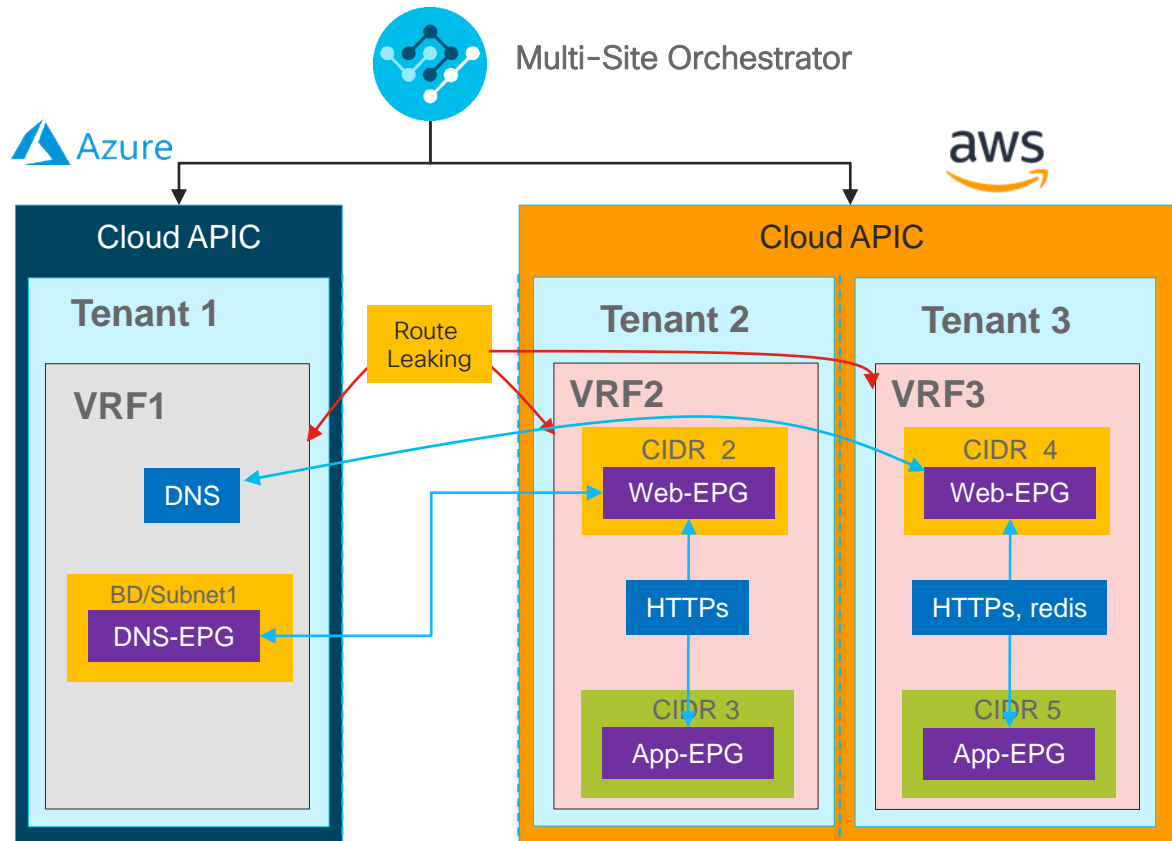
- Stretch tenant/VRF across cloud sites
- During peak times easily deploy application tiers and resources in the cloud site
- Consistent segmentation policy and enforcement within and across cloud sites
- Application stack failover between sites (active/disaster recovery)

Stretched EPG with Consistent Segmentation



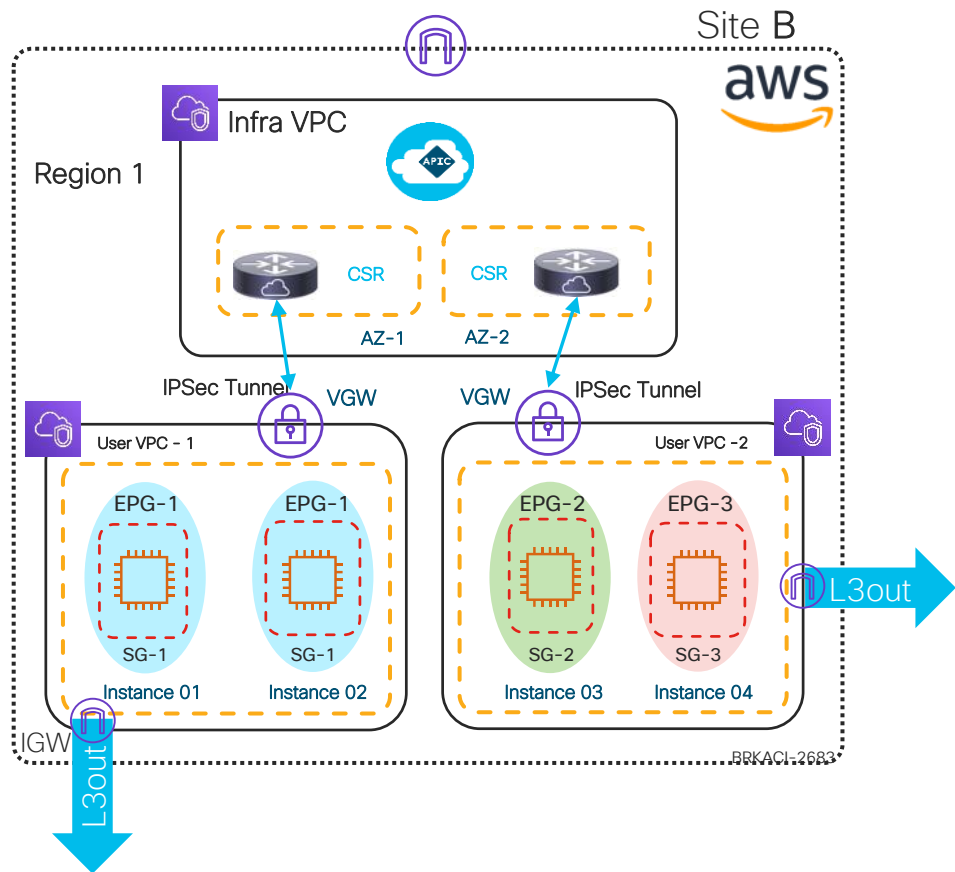
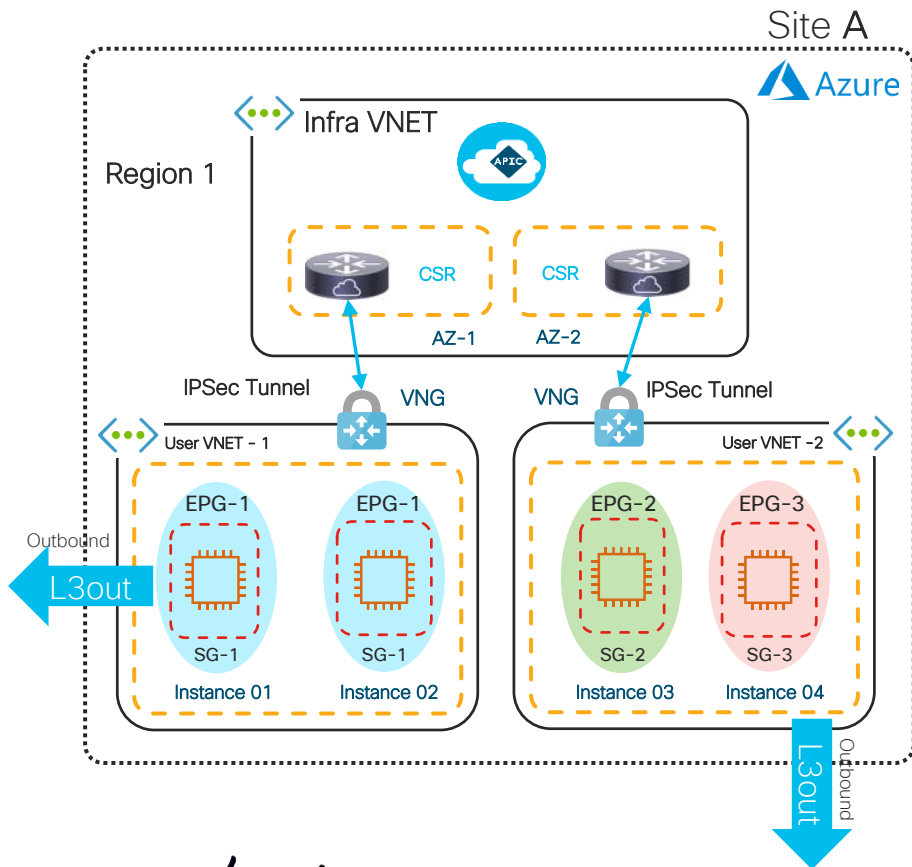
- Web Tier and App Tier are stretched and securely segmented across public cloud sites
- Consistent segmentation policy and enforcement for endpoints of Web/App Tier are independent of location

Shared Services for Multi-Cloud



- Provides a capability to deploy shared service across clouds
- Shared Service deployed in 1 Site can be consumed by endpoints across other sites
- Contract will leak subnet between VRFs for reachability

Cloud L3outs



Deploying Cloud APIC

Cloud APIC in Cloud Marketplaces

The screenshot shows the Cisco Cloud APIC listing on the Azure Marketplace. The header includes the Microsoft logo, 'Azure Marketplace', 'Apps', 'Consulting Services', a search bar, and user links for 'Sell', 'Blog', and 'Lionel'. The product title is 'Cisco Cloud APIC' by Cisco Systems, Inc., with a 'save for later' button. Below the title are tabs for 'Overview', 'Plans', and 'Reviews'. A 'GET IT NOW' button is highlighted in a red box. The 'Overview' section includes a diagram titled 'ACI Extensions to Azure' showing a multi-site architecture with On-Premise DC, Azure Cloud, and Site 2. The text describes how the solution extends the capabilities of Cisco Application Centric Infrastructure (ACI) into public cloud environments, supporting hybrid cloud and multi-cloud deployments. It mentions that the solution uses the Cisco Cloud Services Router (CSR) 1000V as the cloud router for connectivity between On-Premises and Azure Cloud environments. The 'Highlights' section lists: Manage multiple Azure regions from a single instance of Cisco Cloud APIC, Provide secure interconnect for multi-cloud environment and automate network connectivity across multiple On-Premises and Azure Public Cloud environments, and Enable Consistent Policy, Security and Operations between On-Premises and Azure Public Cloud environments. A 'Learn more' link is at the bottom.

<http://cs.co/capic-azure>

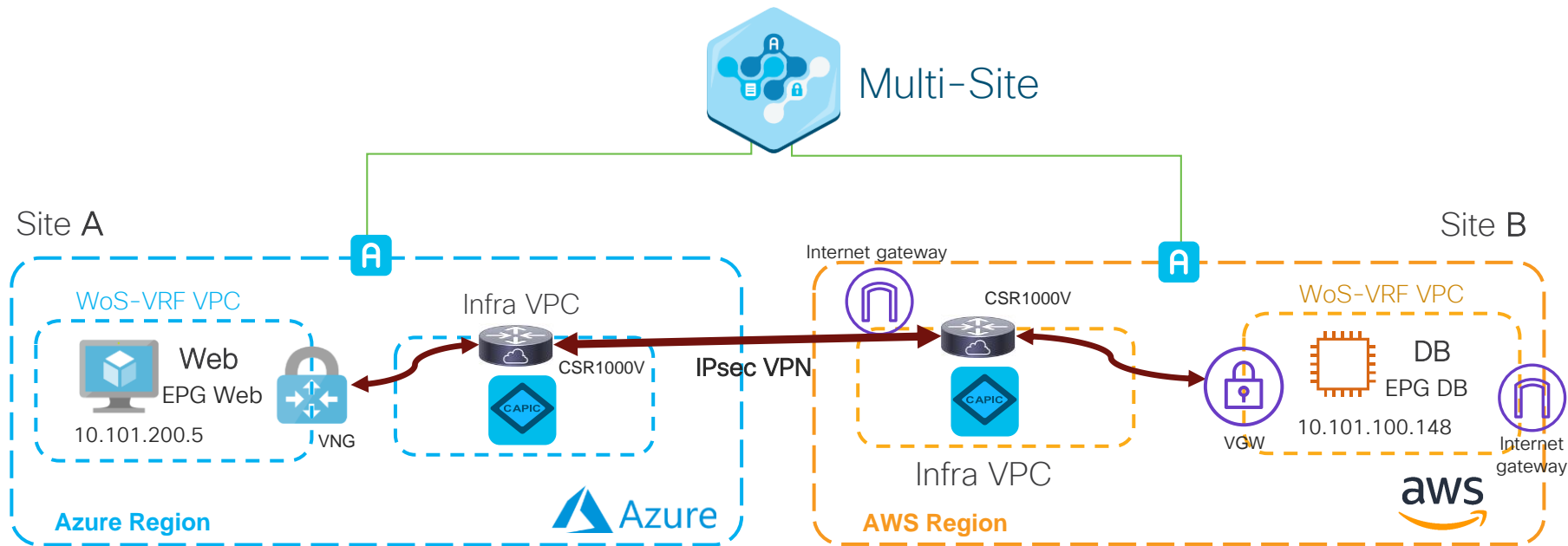
The screenshot shows the Cisco Cloud Application Policy Infrastructure Controller listing on the AWS Marketplace. The header includes the 'aws marketplace' logo, a search bar, and links for 'Sign in or Create a new account'. The product title is 'Cisco Cloud Application Policy Infrastructure Controller' by Cisco Systems, Inc., with a 'Latest Version: 4.1*' and a 'Continue to Subscribe' button. Below the title are tabs for 'Overview', 'Pricing', 'Usage', 'Support', and 'Reviews'. The 'Overview' section includes a diagram titled 'ACI Extensions to Azure' showing a multi-site architecture with On-Premise DC, Azure Cloud, and Site 2. The text describes how the solution extends the capabilities of Cisco Application Centric Infrastructure (ACI) into public cloud environments, supporting hybrid cloud and multi-cloud deployments between multiple ACI on-premises data center and AWS public cloud sites. It mentions that the solution introduces the Cisco Cloud Application Policy Infrastructure Controller, which runs natively in AWS public cloud to provide automated connectivity, policy translation, day two operations and enhanced visibility of workloads in the public cloud. The 'Highlights' section lists: Manage multiple AWS regions from a single instance of Cisco Cloud APIC, Provide secure interconnect for multi cloud environment and automate network connectivity across multiple On-Premises and AWS Public Cloud environments, and Enable Consistent Policy, Security and Operations between On-Premises and AWS Public Cloud environments. A 'Learn more' link is at the bottom.

<http://cs.co/capic-aws>

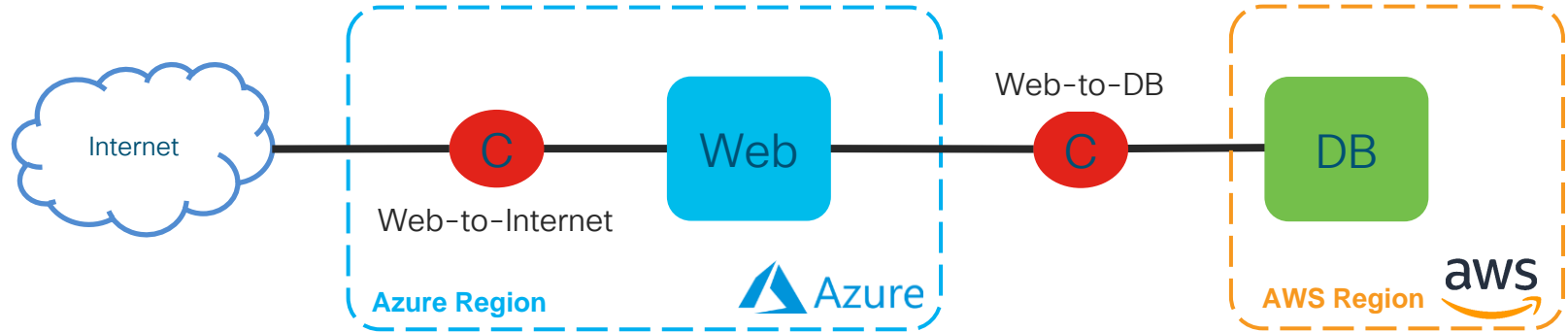


Demo

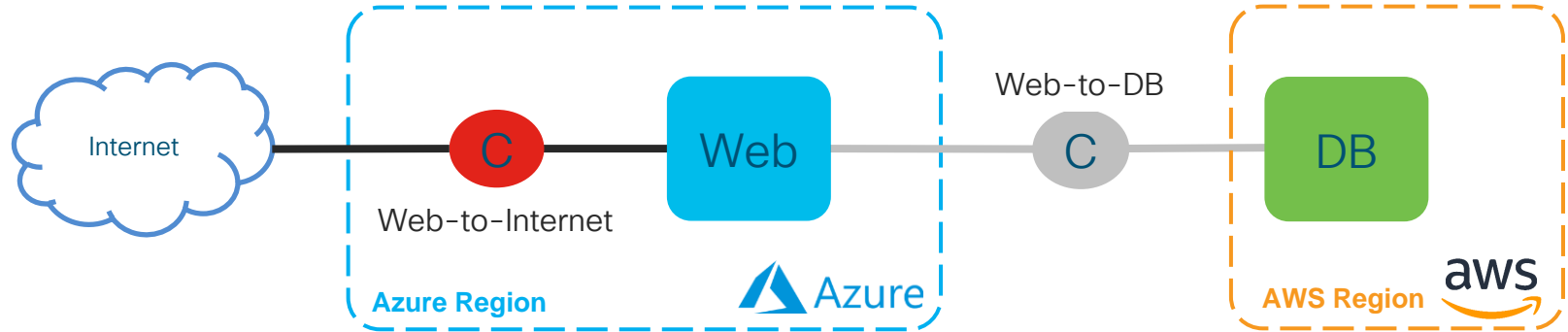
Demo #1 - Setup: Web in Azure / DB in AWS



Demo #1 - Logical View



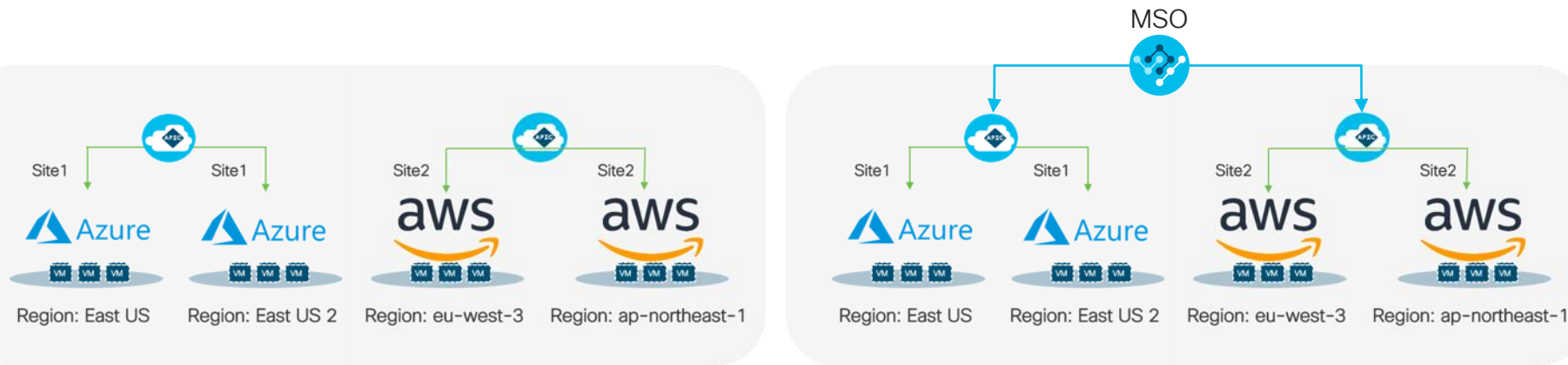
Demo #1 - Logical View



ACI Cloud First

Recap

You do not need an On-premises ACI Fabric to start with Cloud ACI



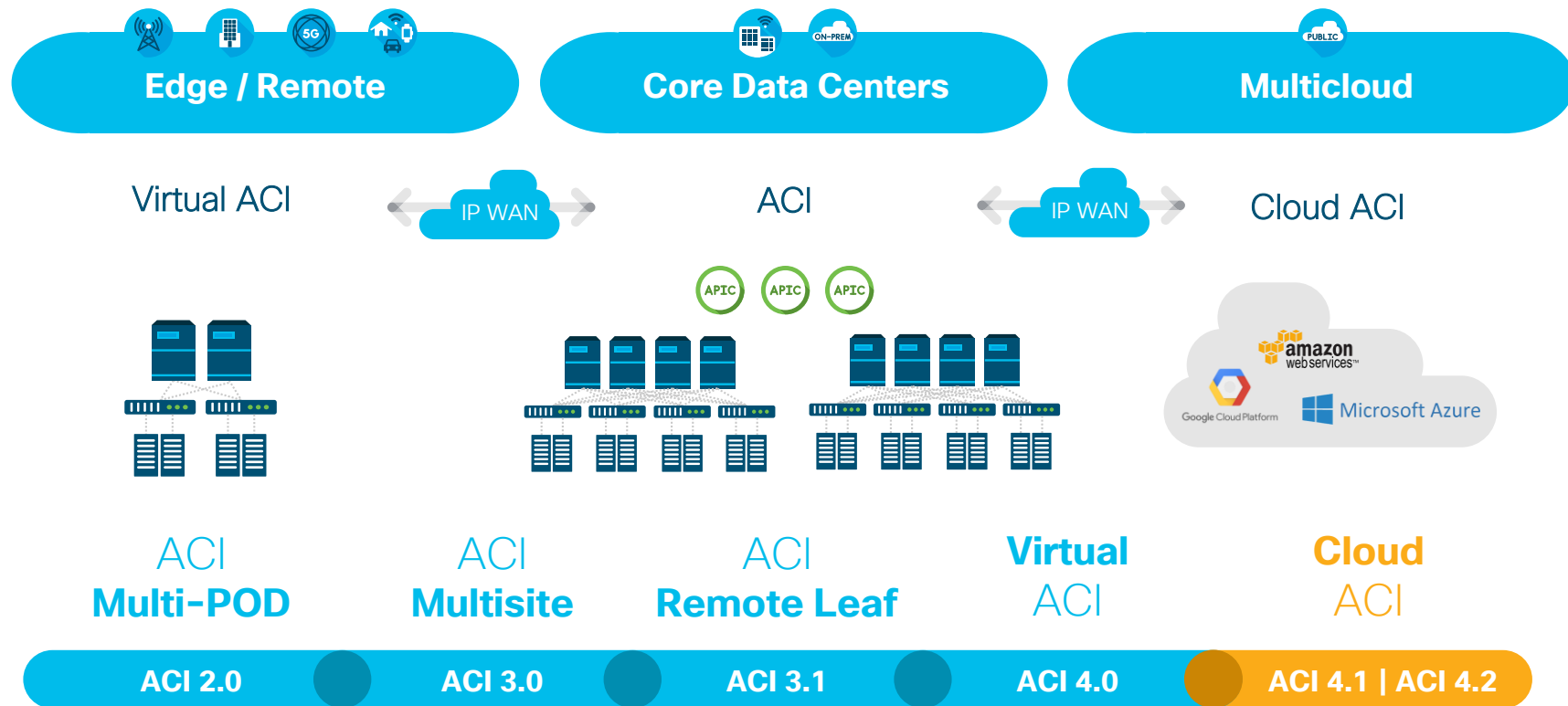
Consistent Policy Enforcement
on-Premises & Public Cloud

Automated Inter-connect
provisioning

Simplified Operations
with end-to-end visibility



ACI Anywhere



Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



Meet the Engineer
1:1 meetings



Related sessions



Thank you





You make **possible**