Multicloud Conectivity with ACI

Justin Cooke, Technical Solutions Architect

BRKACI-2690-V

Agenda

- Introduction
- ACI Cloud Concepts
- Extending Networking to the Cloud
- Extending Policy to the Cloud
- Conclusion

Introduction

You make networking **possible**

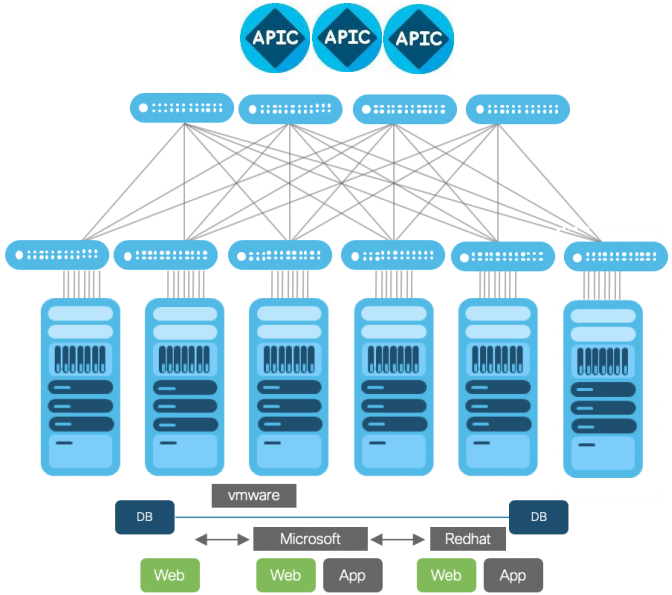
Challenges in building a Multi Cloud environment

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

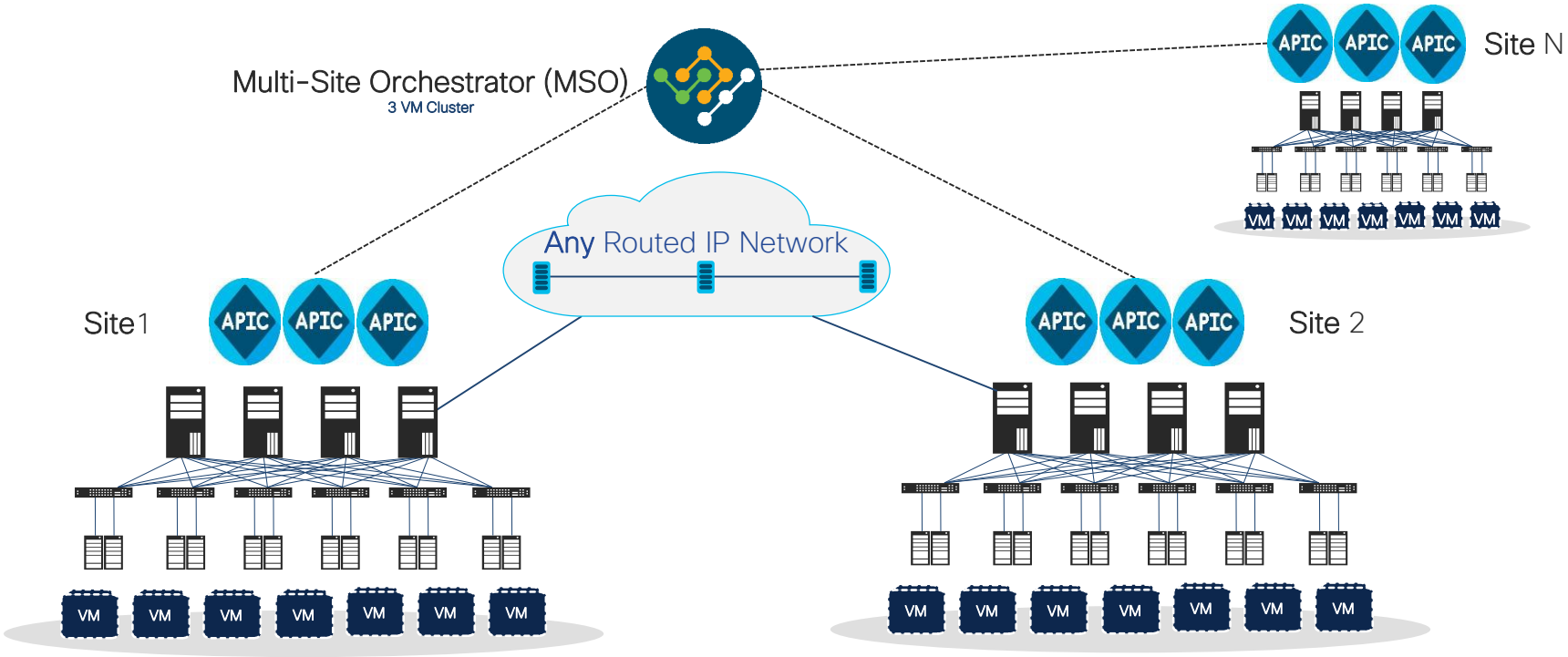
Requires a single pane of glass to manage policies across on-premise and cloud locations

ACI Single Fabric



- Tenants
- End Points
- Grouping Endpoints (EPG)
- Contracts
- Service Insertion

ACI Multi-Site

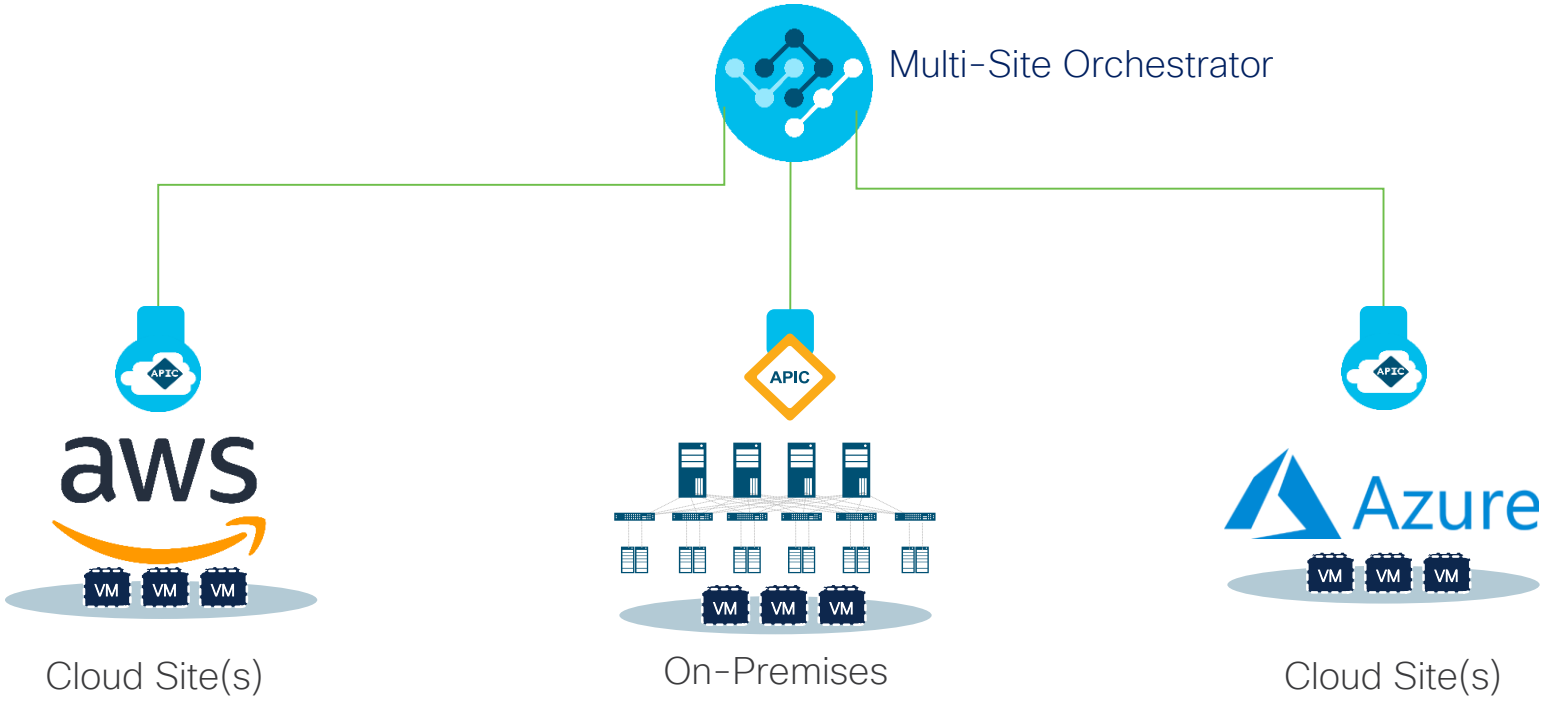


No Multicast
Phased Changes (Zones)

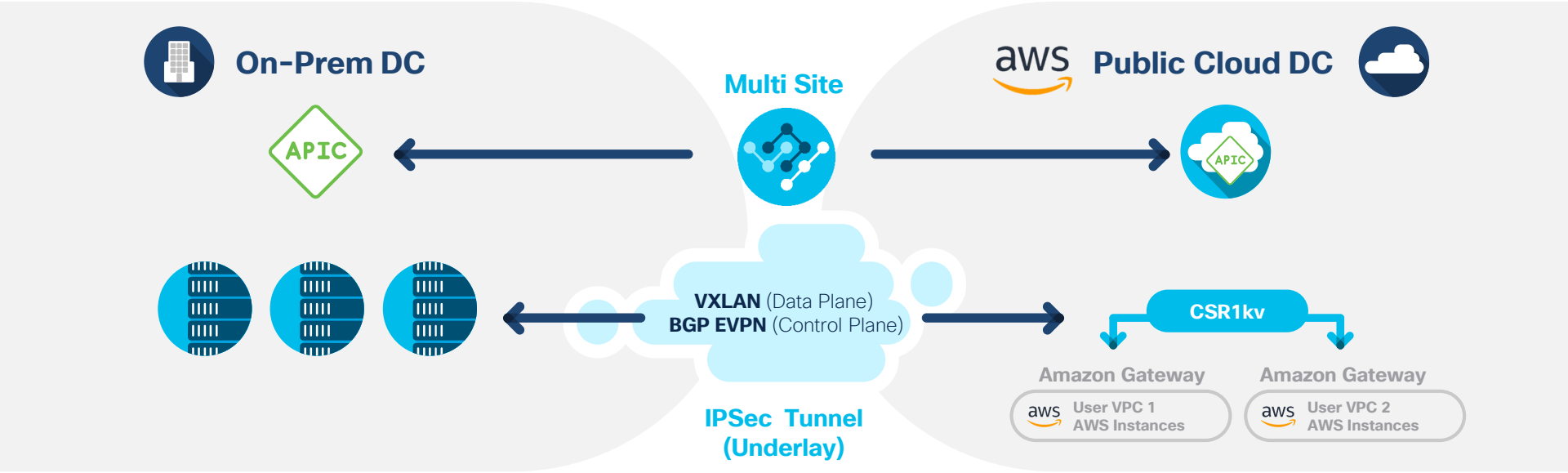
<= 1s RTT Required (MSO → APIC)
Up to 12 Sites, distributed gateway

Single central management (MSO)
Automated L2 DCI VXLAN extension

ACI Extensions to Multi-Cloud



Simplifying Cloud Connectivity



Automated network extension to AWS

Encrypted tunnel option

AWS Multi-region Support

End-to-end control plane for route and policy exchange

Uniform Connectivity Policy

Automated policy translation to native AWS constructs

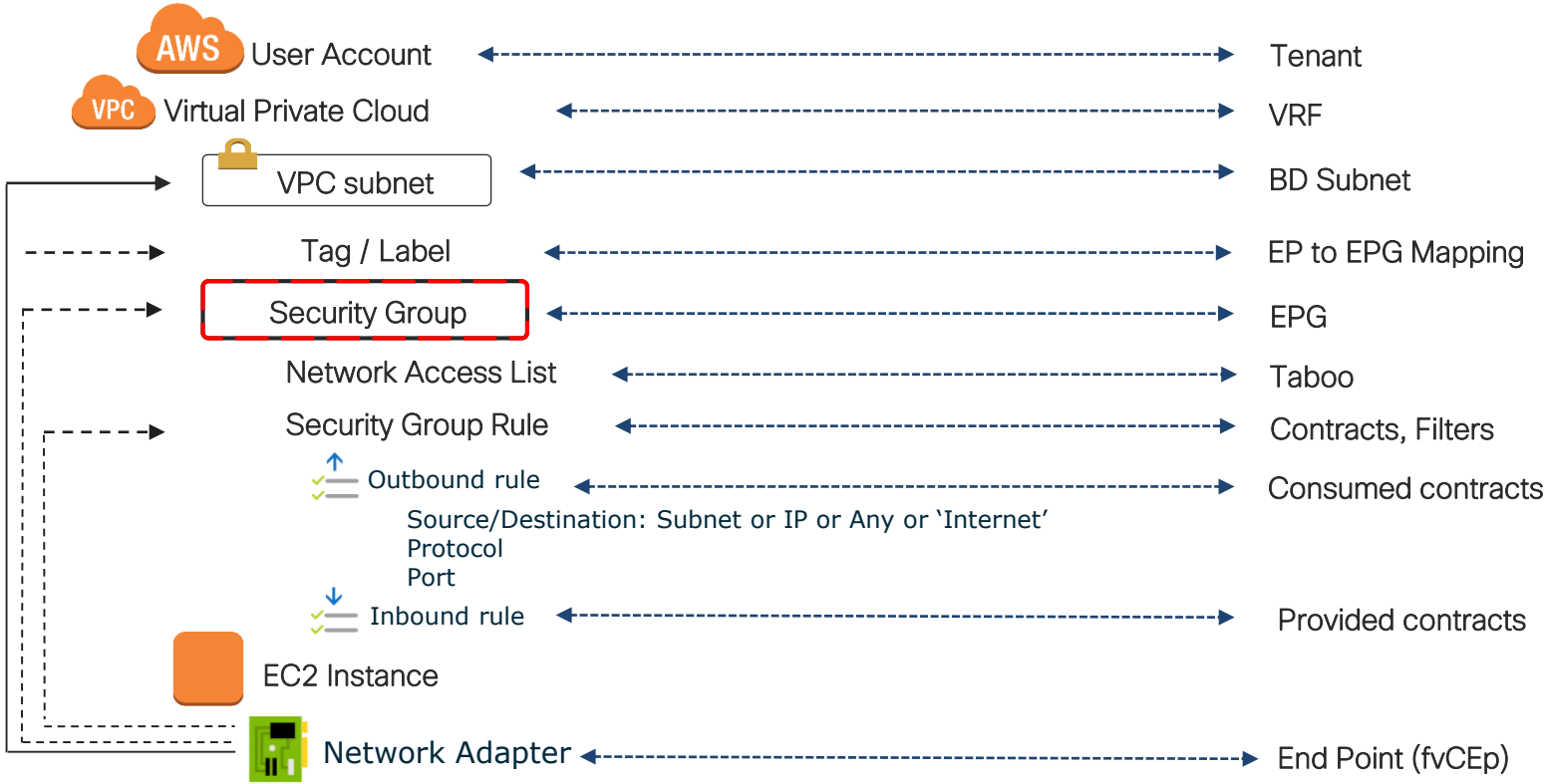
ACI MSO as single point of policy management and orchestration

Lifecycle management of CSR1000v and AWS VGW

Consistent Policy Extensions across sites

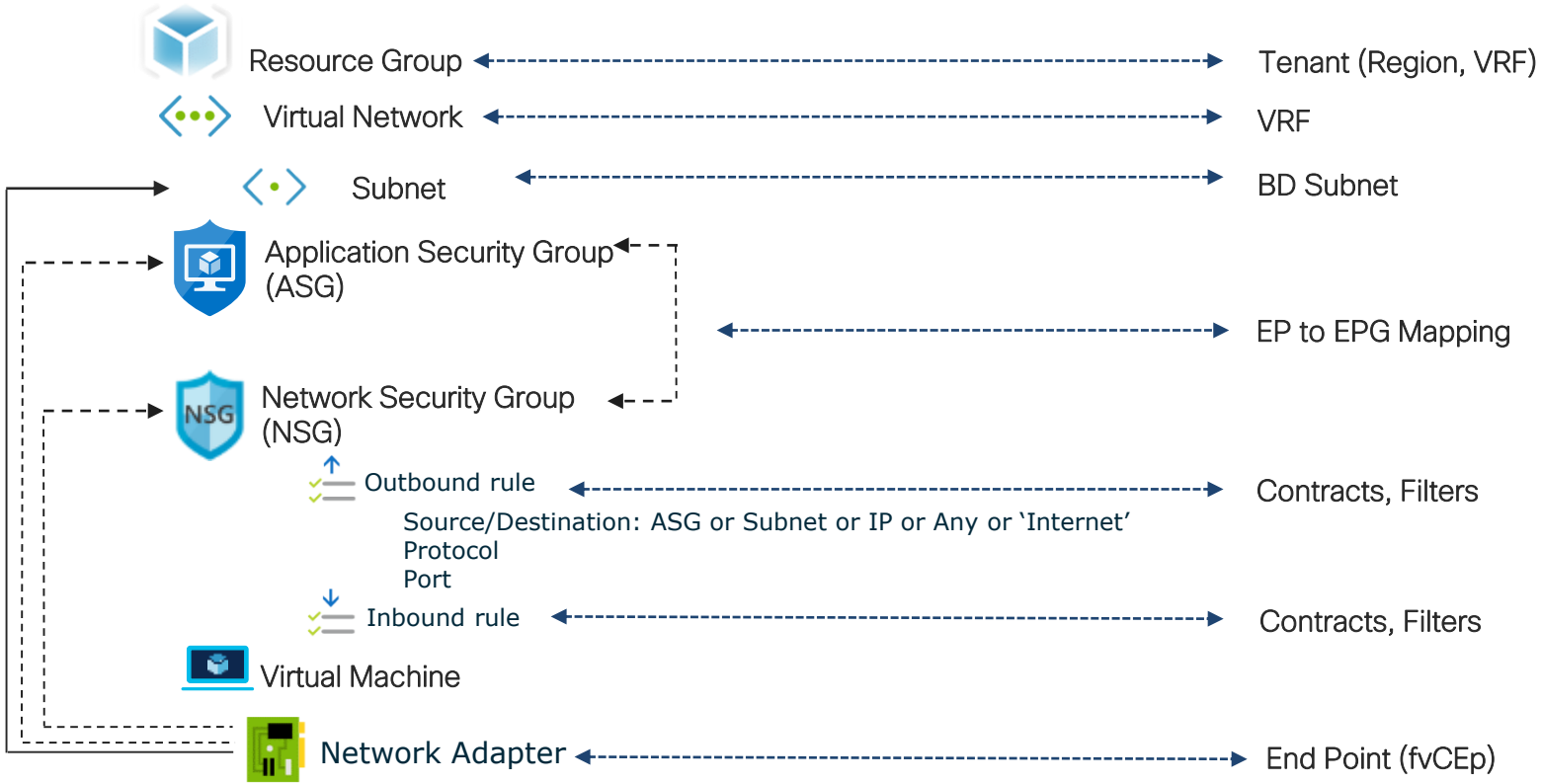
Policy Mapping – AWS

For your info & reference



Policy Mapping – Azure

For your info & reference



ACI Cloud Concepts

You make multi-cloud **possible**

Cloud EPG and Cloud ExtEPG

- *Cloud EPG*:

  A collection of network interfaces on the cloud provider, which will share the same security policy. Can have endpoints in one or more subnets as well as can span across regions. Tied to a VRF

- *Cloud Ext EPG*:

  A set of subnets that represent the outside world compared to the cloud provider. Outside world can either be another site or Internet.

  Example: IPv4 internet as outside, cloudExtEPg will be identified with the subnet 0.0.0.0/0

Cloud EP Classification
Operators

- Below are few examples. You can use any combination

Key	Operator	Value
IP Address / Subnet	=, !=	10.10.10.1, 10.10.10.0/24
Region	In, Not in	us-west-1, us-east-1
Zone	In, Not in	us-west-1a, us-west-1b
Custom Application	Has key Doesn't have key	web, db

Example : Cloud EP Classification
Micro Segmentation

- Example 1: Cloud EPG ”Dev”

Condition	Key(s) + Operator(s) + Value(s)
Match expression	Custom:department == Engineering, Region In (us-west-1, us-east-1), custom:Role NotIn (Management, ITStaff)

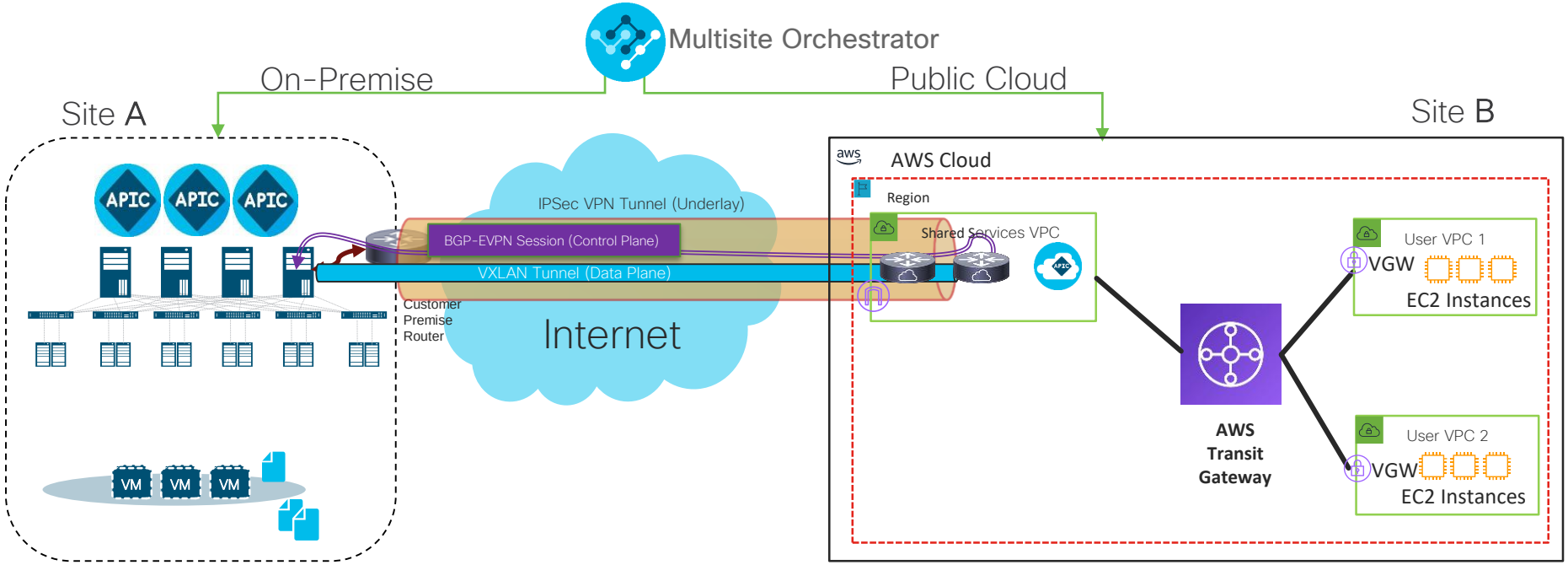
- Example 2: Cloud EPG ”Finance”

Condition	Key(s) + Operator(s) + Value(s)
Match expression	Custom:department == Finance, Region In (us-west-1, us-east-1), IP == 172.16.0.0/24

Extending Networking

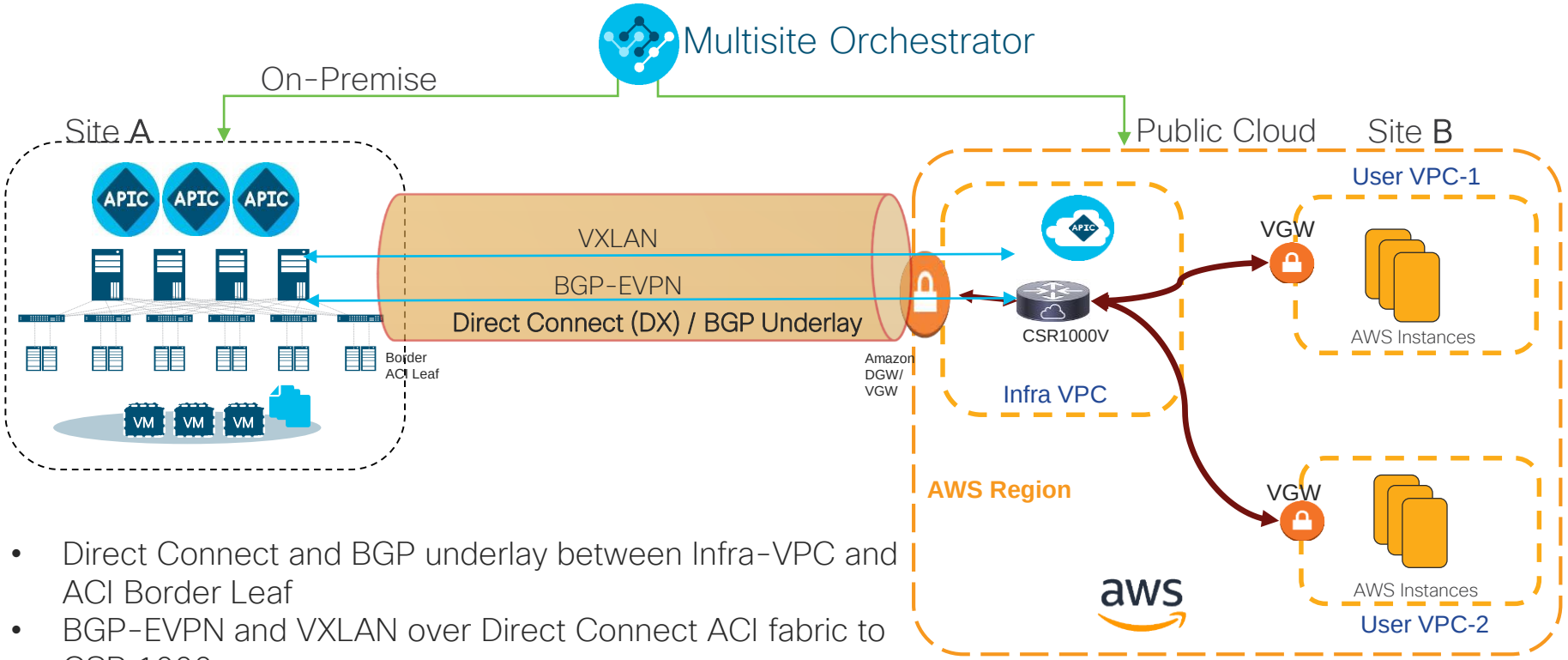
You make networking **possible**

Virtual Private Network (VPN)



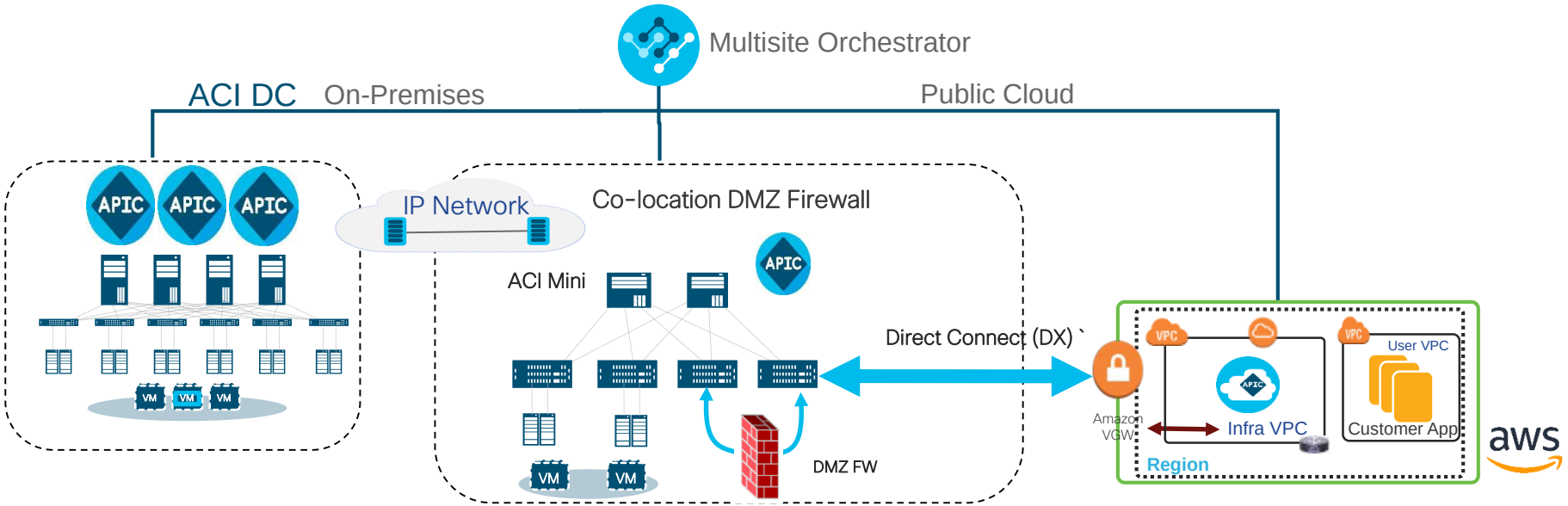
- VXLAN data-plane connects ACI fabric and Cloud site
- BGP-EVPN routing reachability between ACI fabric and Cloud Site
- IPSec VPN connection between customer Premise Router before ACI fabric and CSR1kv

Direct Connect (DX)



- Direct Connect and BGP underlay between Infra-VPC and ACI Border Leaf
- BGP-EVPN and VXLAN over Direct Connect ACI fabric to CSR 1000v

DMZ with Firewall

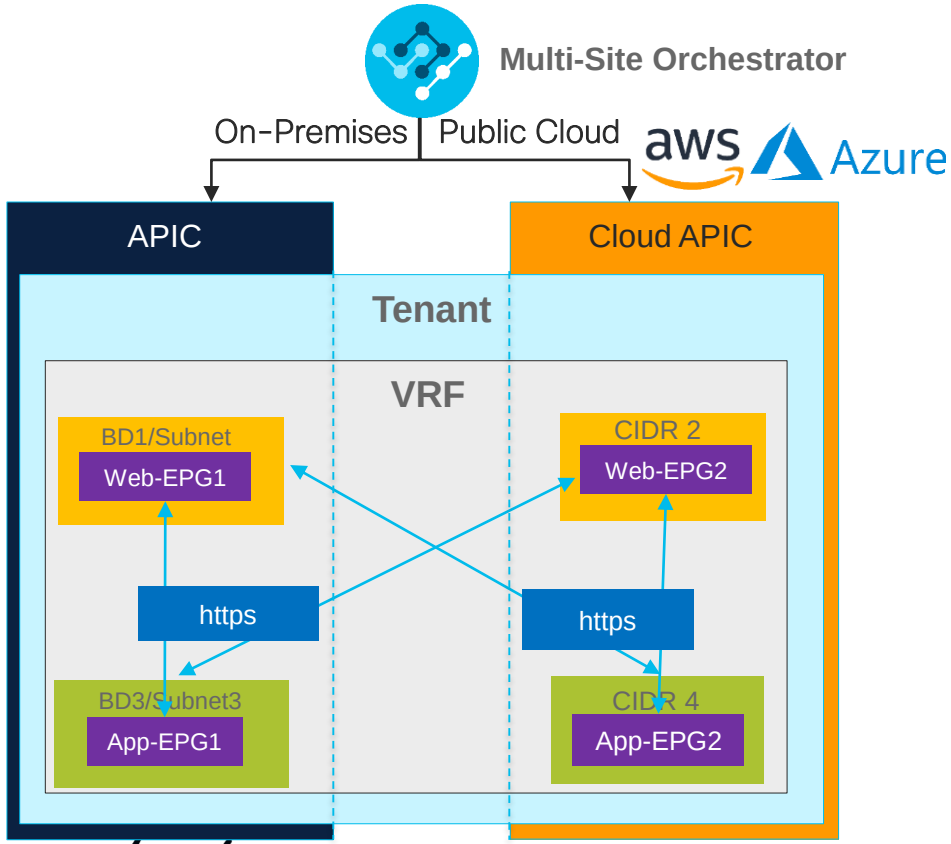


- ACI Mini Fabric in Co-location DMZ terminates AWS Direct Connect
- DMZ firewall provides perimeter security
- L1/L2/L3 PBR can be used to steer traffic into Firewall

Connectivity Policy

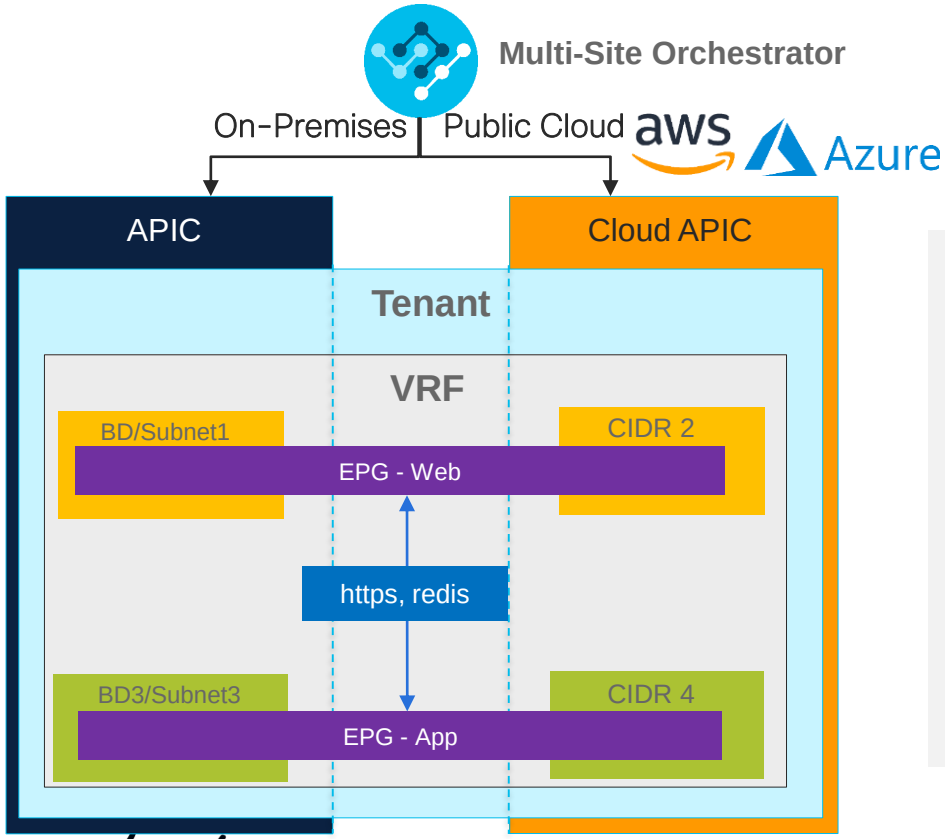
You make security **possible**

Application Stretch



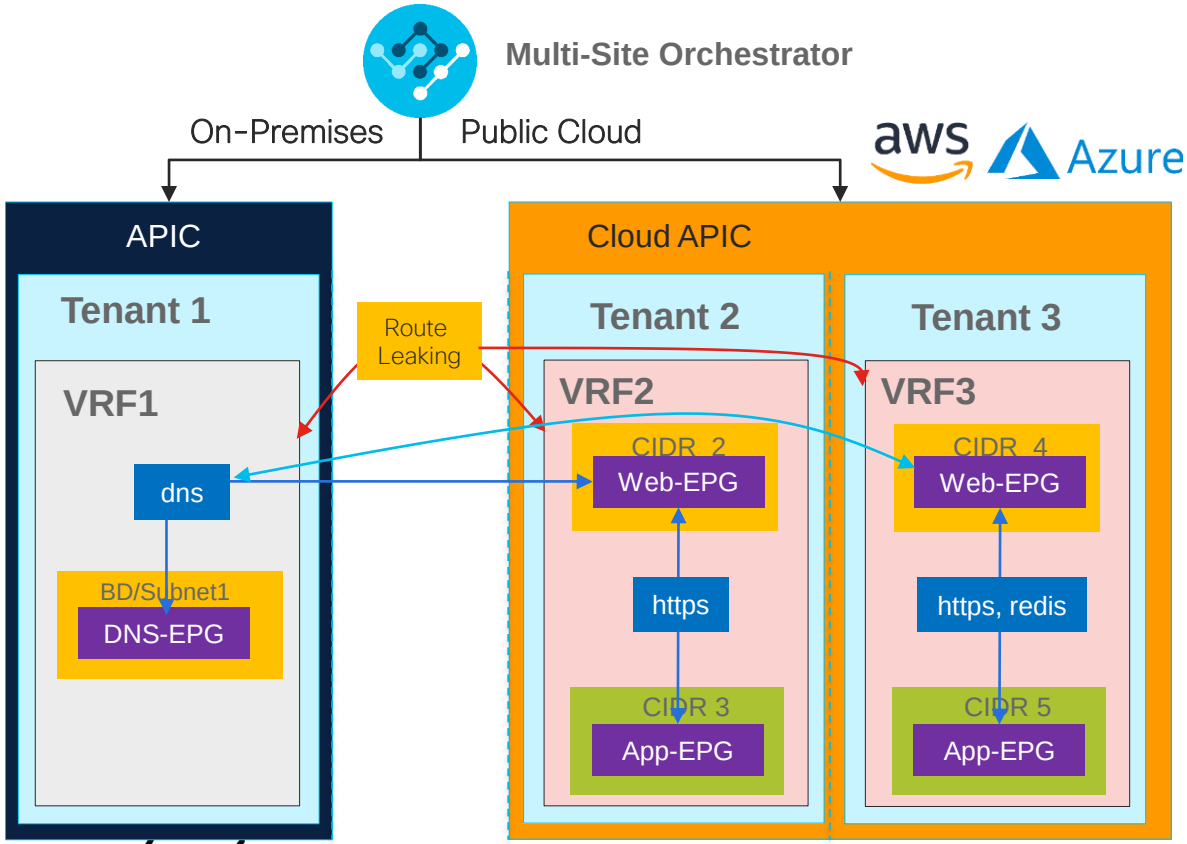
- Stretch tenant/vrf across on-premises and cloud sites
- During peak times easily deploy application tiers and resources in the cloud site
- Consistent segmentation policy and enforcement within and across on-premises and cloud sites
- Application stack failover between sites (active/disaster recovery)

Stretched EPG with Consistent Segmentation



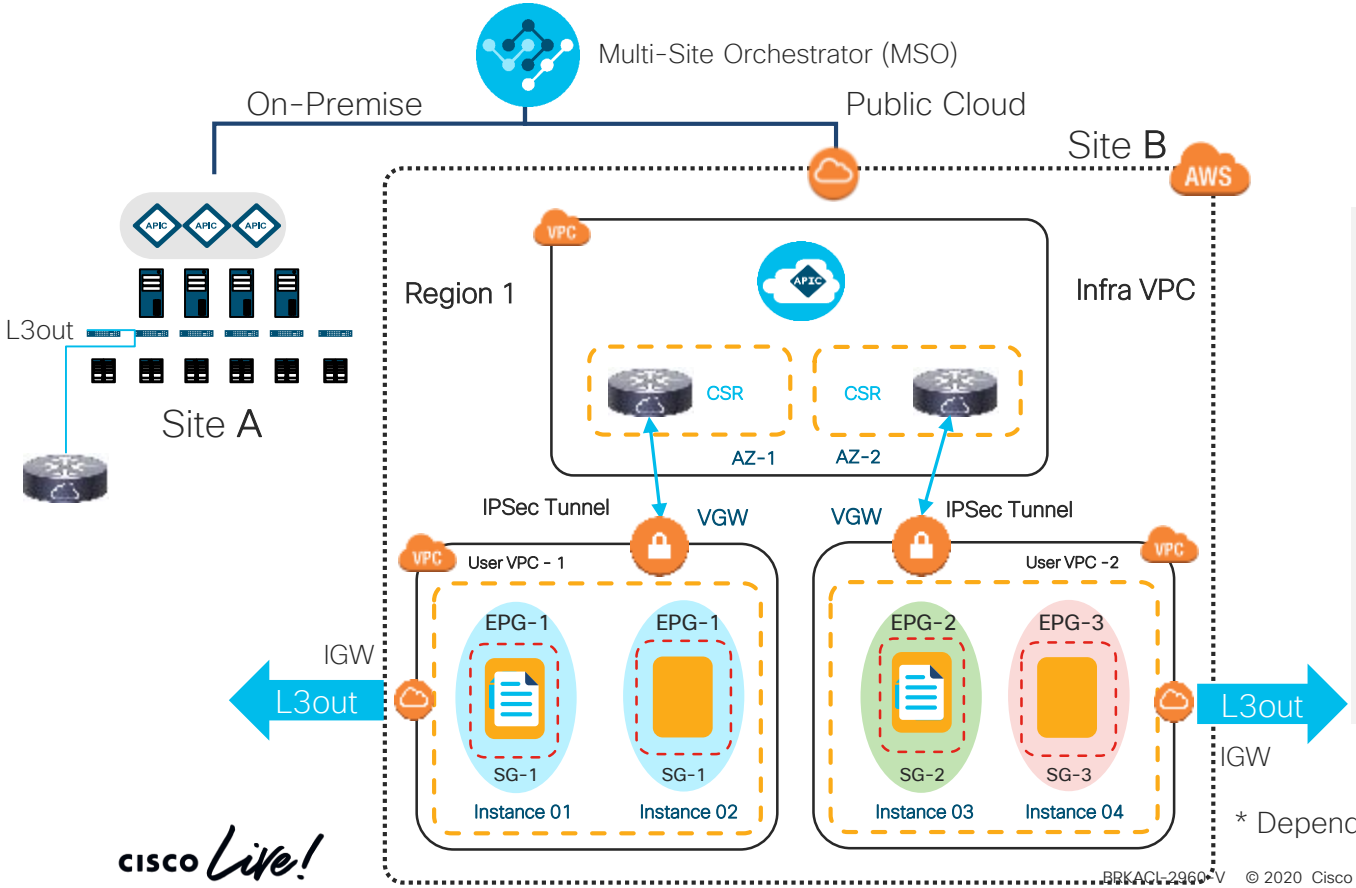
- Web Tier and App Tier are stretched and securely segmented across on-premise and public cloud sites
- Consistent segmentation policy and enforcement for endpoints of Web/App Tier are independent of location

Shared Services for Hybrid-Cloud



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

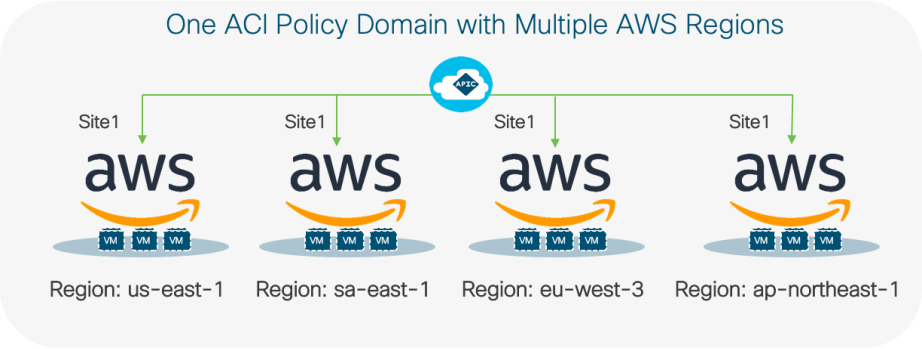
Cloud and On-Prem L3outs

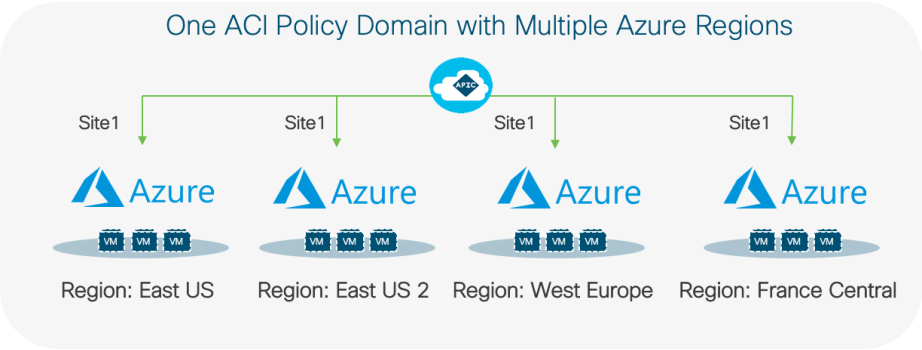


- Cloud local L3out via IGW
- On-Prem local L3out
- On-Prem site endpoints cannot use Cloud L3out
- Shared On-Prem L3out for Cloud VPCs *

* Depends on QA Validation Completion by FCS

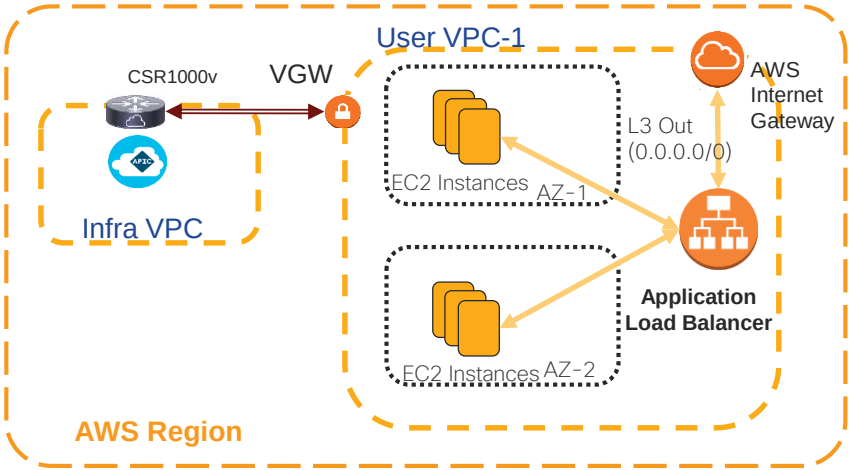
Cloud First





- Cloud APIC only without on-premises ACI or MSO
- Abstract AWS / Azure networking constructs from user that is familiar with ACI, delivering ACI-consistent policy and operational model
- Deploy EPG and contracts on top of AWS public cloud

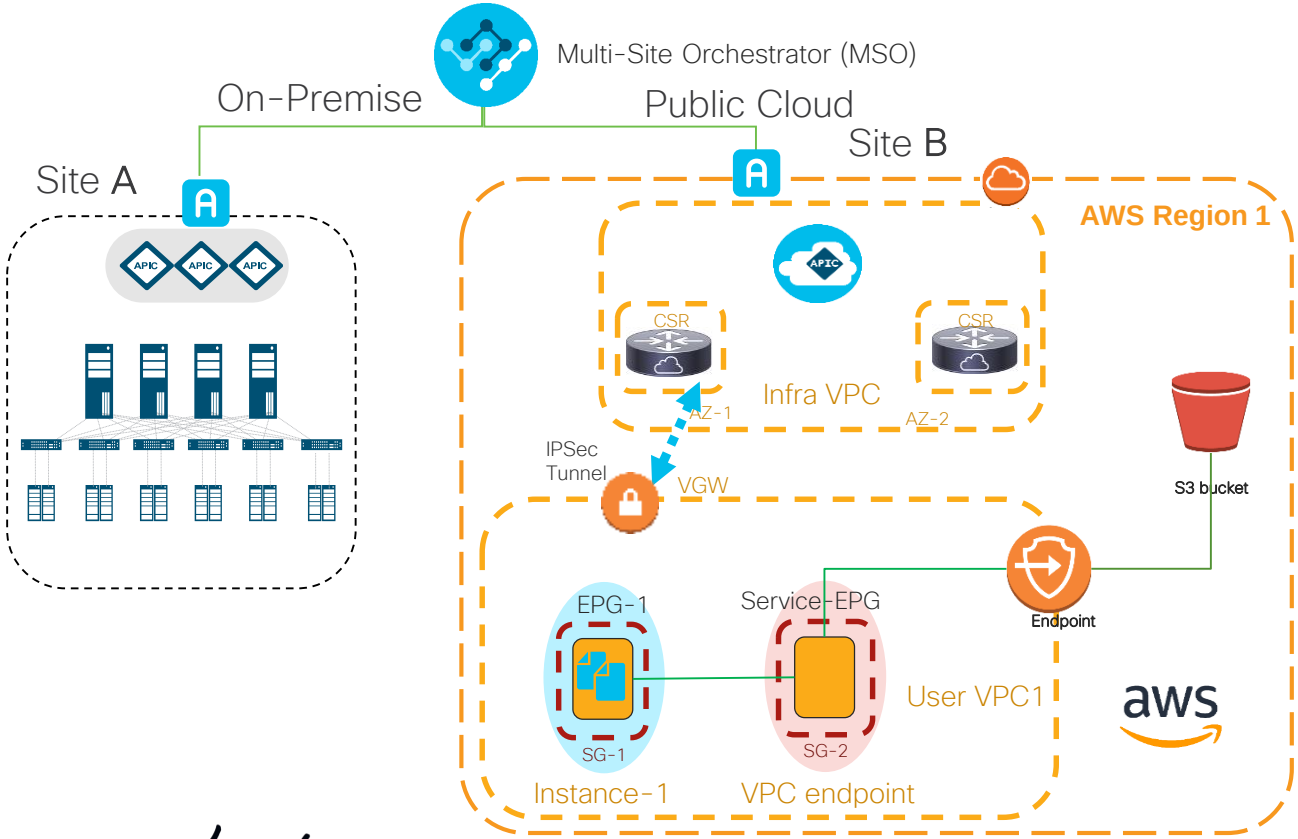
Application Load Balancer



2 Packet Flows

1. Packet arrives from IGW L3out is sent to ALB
2. Packet from user VPC is sent to ALB

AWS Cloud Native Services



- EC2 instances access Cloud Native Service (eg. S3 bucket) via VPC endpoint

References

You make the power of data **possible**

References

- Cisco Live on Demand Session : BRKACI-2690 How to extend your ACI fabric to Public Clouds (AWS and Azure), Barcelona 2020
- Cisco ACI

https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html#~stickynav=1

- Cloud ACI

https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/cloud-aci.html

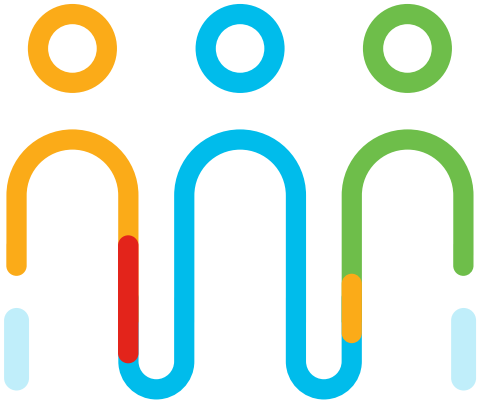
- Cisco Cloud ACI on AWS Whitepaper

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-741998.html

- Cisco Cloud ACI on Microsoft Azure Whitepaper

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-742844.html

Conclusion



You make customer experience **possible**

Cloud ACI

1. Universal Policy and Operational Model for MultiCloud
2. Network Automation across On-Premises and MultiCloud
3. Uniform Segmentation Policy for On-Premises and Cloud
4. Automated life cycle management of CSR1KV & Cloud Resources
5. Extensible, Elastic Software Architecture
6. End-to-End visibility, Monitoring, Troubleshooting and Common governance
7. Foundation for Multi Domain Policy Connectivity

Thank you