The bridge to possible

Multi-Cloud SD-WAN Design

Chandra Balaji Rajaram, Technical Marketing Leader, Cisco SD-WAN

Cisco Webex App

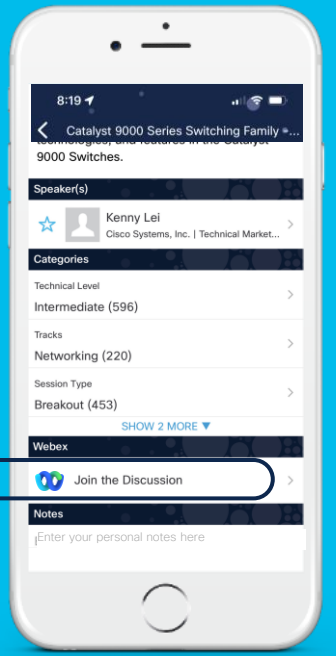
Questions?

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 until February 24, 2023.

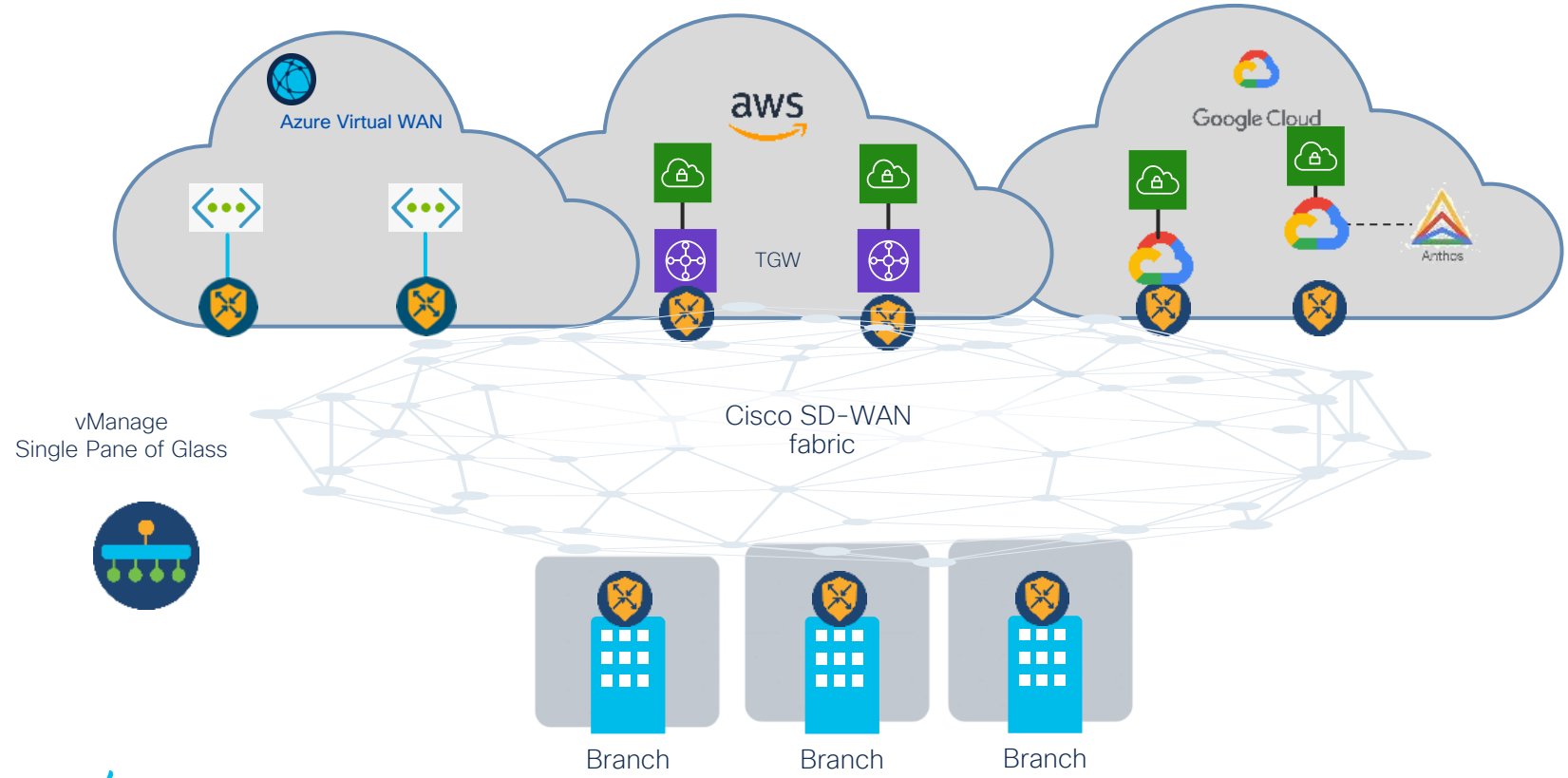


Agenda

- Introduction
- Site-to-Cloud Designs
- Site-to-Site Designs
- Multi-Region fabric using Cloud as core
- Key Design Asks
- Conclusion

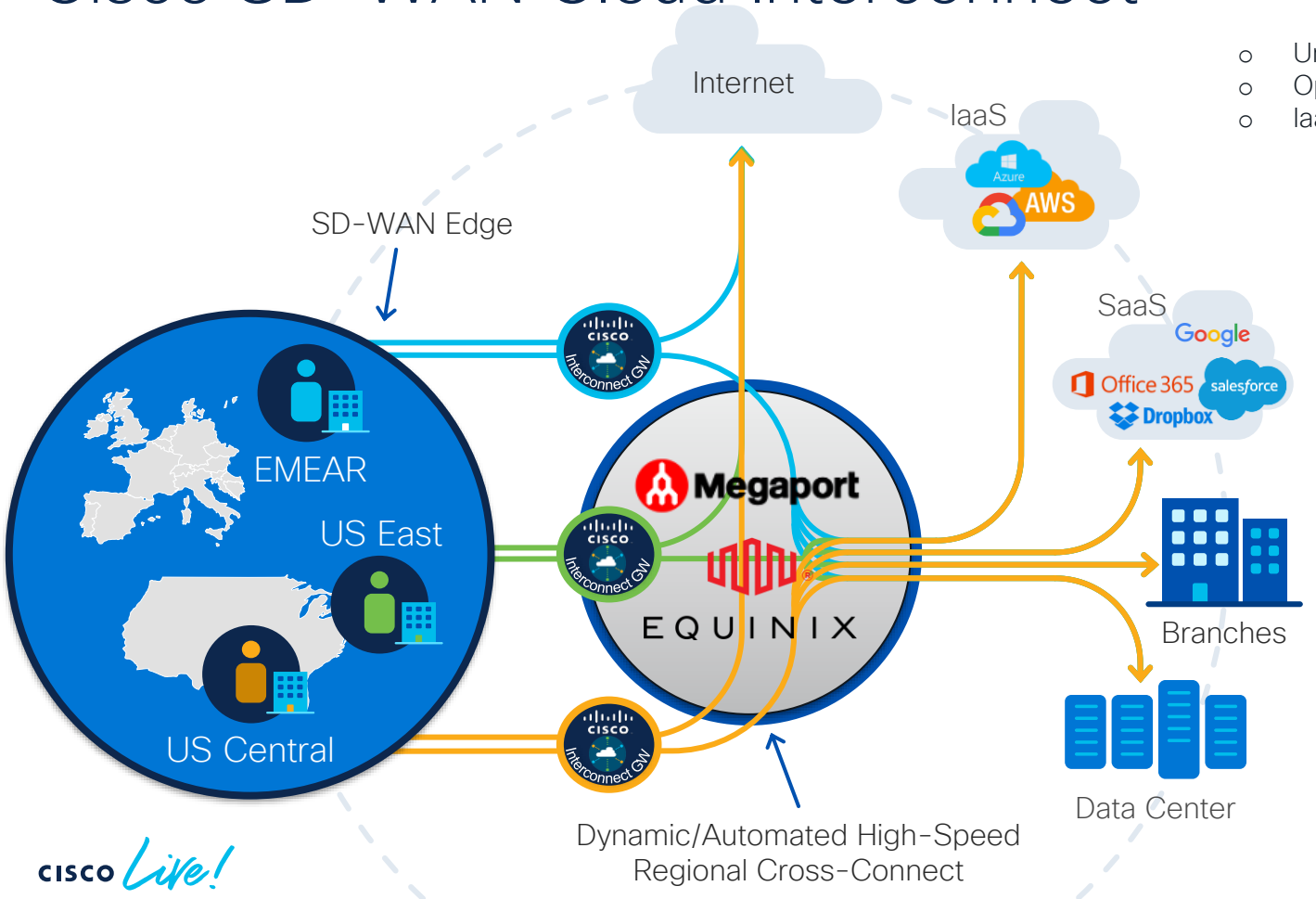
Introduction

Cloud OnRamp for Multicloud



Cisco SD-WAN Cloud Interconnect

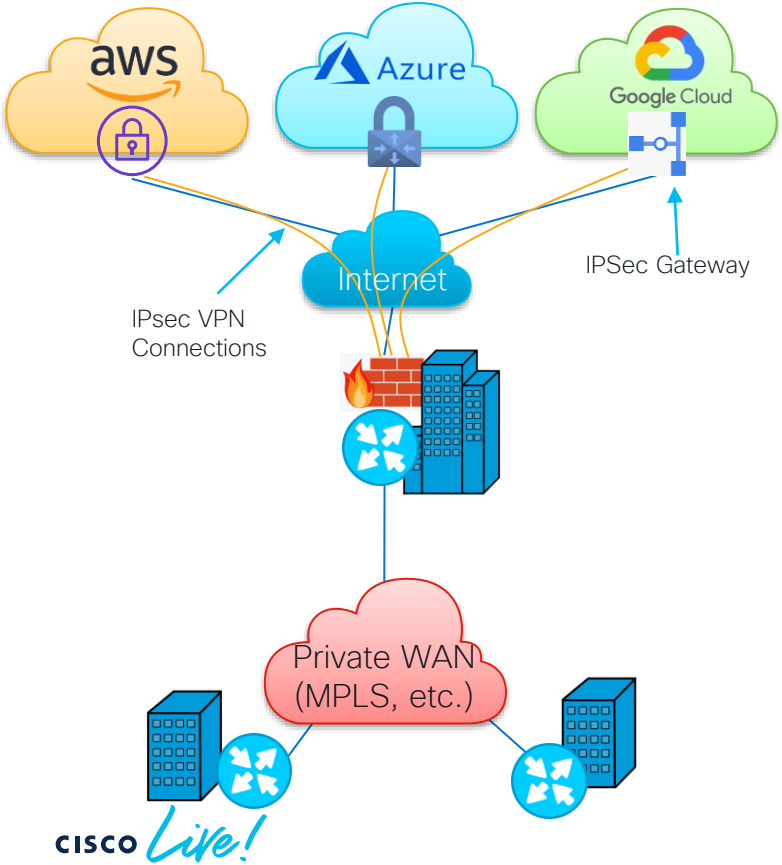
- Unifies Fractured Access Peering
- Optimize Network Peering Points
- IaaS Delivered Network Service



Site-to-Cloud Design

Traditional Cloud Connectivity

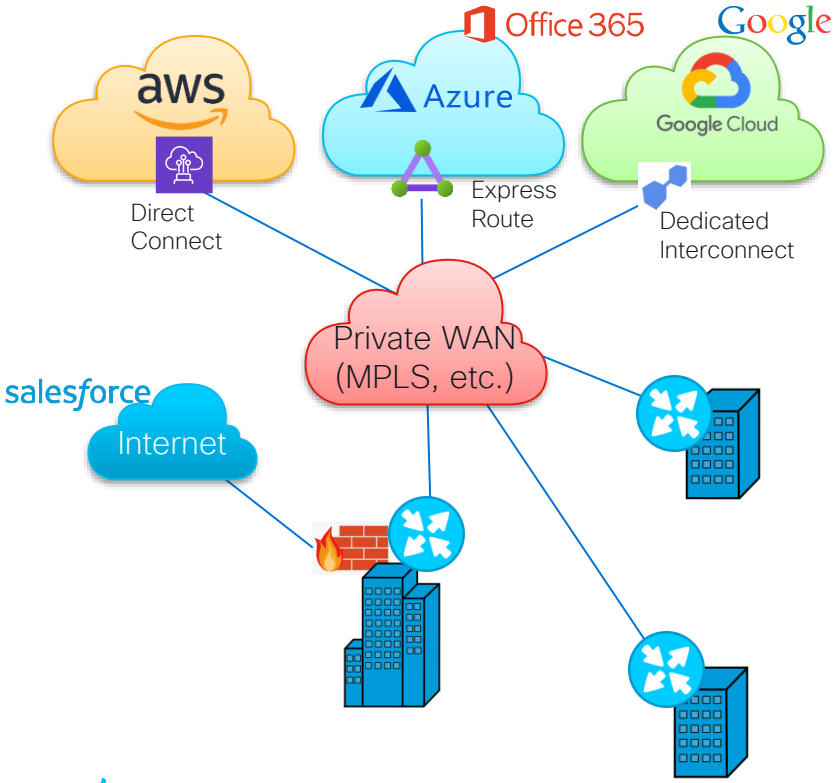
Private WAN with Internet-Based Cloud Connectivity



- Internal Site-to-Site Traffic – uses Private WAN
- Internet-bound traffic is backhauled across the private WAN to one or more HQ / data center sites
- Cloud hosted workloads are accessible from HQ/DC using IPSec connections over Internet.
  - Multiple models – IPSec GW within individual VPCs or vNETs, IPSec GW within Transit VPC or vWAN/vHub, etc.
- Guaranteed service levels (BW, latency, loss) between corporate sites, but no guarantees of SLAs to cloud providers

Traditional Cloud Connectivity

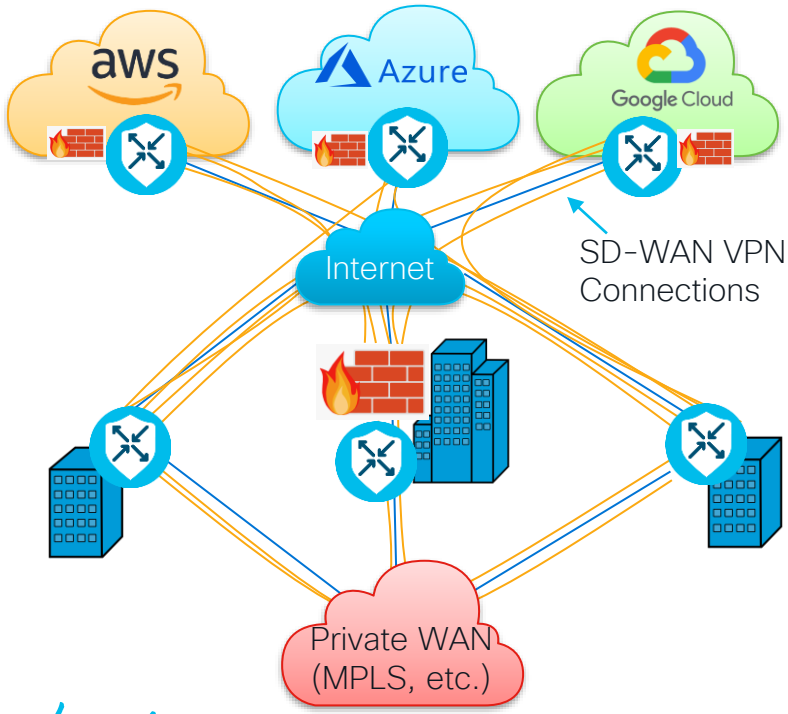
Private WAN with Dedicated Cloud Connectivity



- Internal Site-to-Site Traffic – uses Private WAN
- Internet-bound (non-cloud) traffic backhauled via the private wan to one or more HQ / data center sites
- Traffic to Cloud hosted workloads and some SaaS traffic are sent leveraging MPLS provider integration with public cloud providers
- Guaranteed service levels (BW, latency, loss) between corporate sites, and out to public cloud IaaS (and some SaaS Apps) providers
- Connectivity between cloud provider VPCs/vNets via the public cloud provider network, MPLS provider network, and/or corporate sites

SD-WAN & Cloud Connectivity

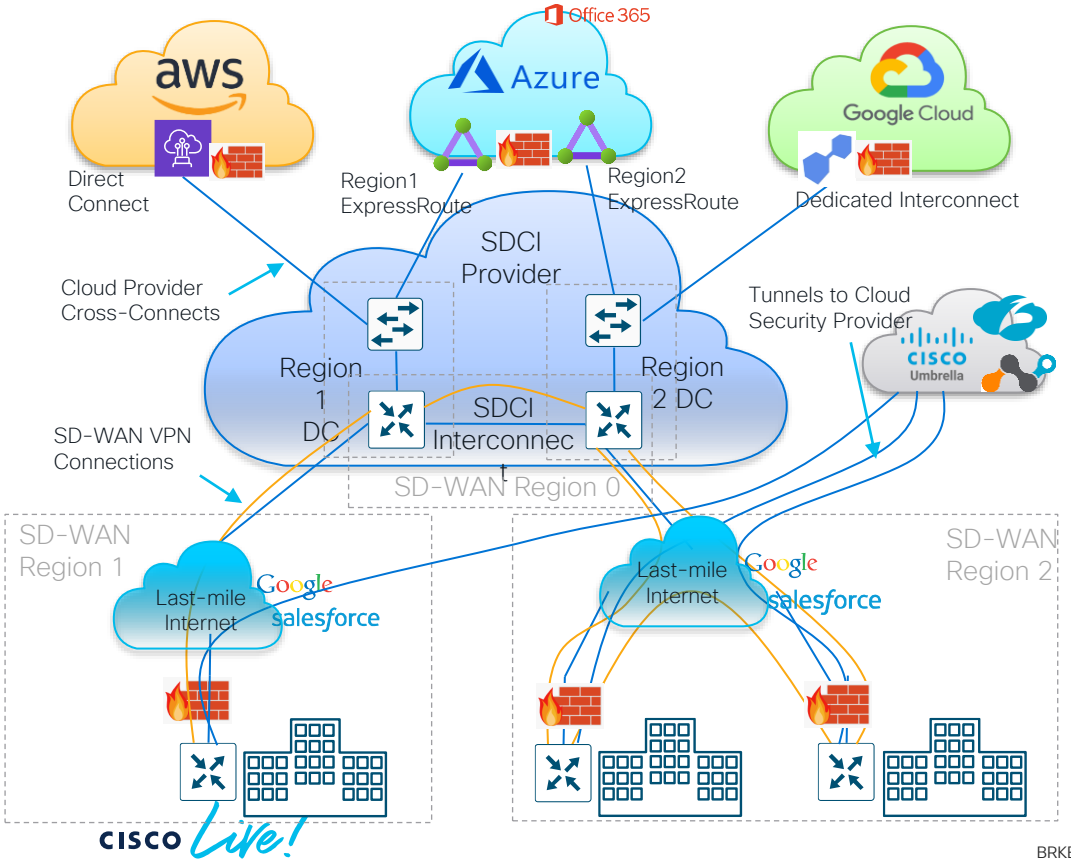
Private WAN with Internet-Based Cloud Connectivity



- Internal Site-to-Site Traffic – uses both Private WAN & INTERNET WAN
- Internet-bound traffic is backhauled across the private WAN to one or more HQ / data center sites
- Cloud hosted workloads are accessible from HQ/DC using IPSec connections over Internet.
  - Multiple models – VGW within individual VPCs or vNETs, VGW within Transit VPC or vWAN/vHub, etc.
- Guaranteed service levels (BW, latency, loss) between corporate sites, but no guarantees of SLAs to cloud providers

SD-WAN & Cloud Connectivity

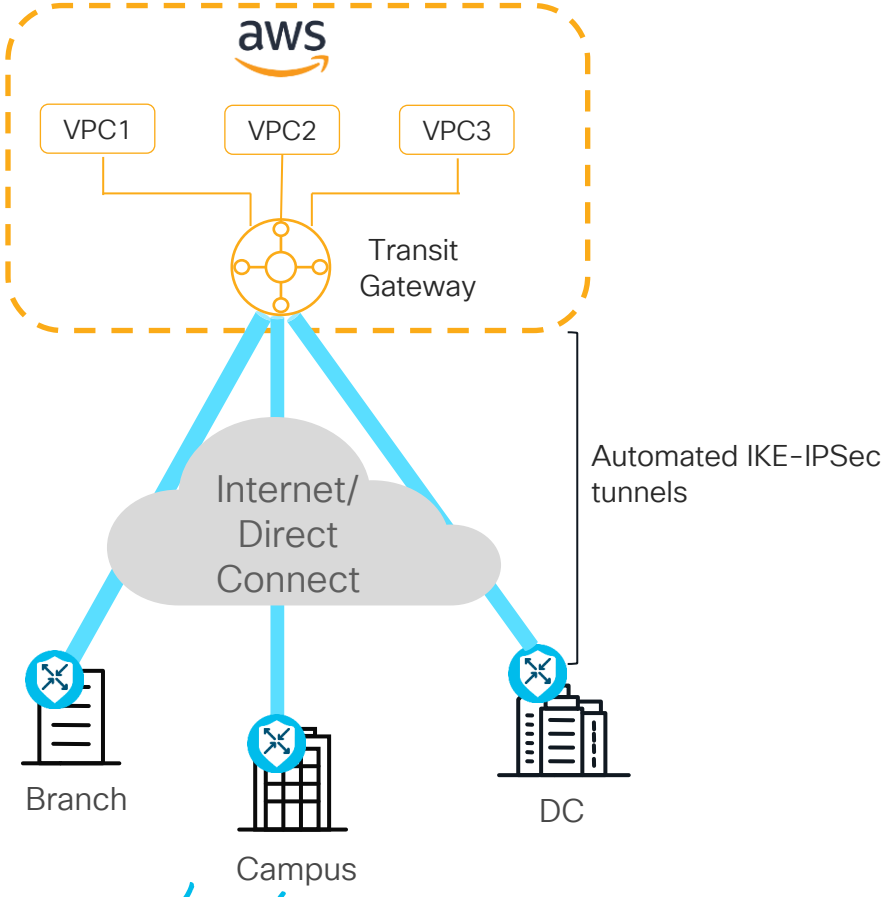
Private WAN with SDCI-Based Cloud Connectivity



- SDCI provider for internal site-to-site traffic and cloud connectivity, with multi-region fabric (hierarchical) SD-WAN model.
- Site-to-site & Site-to-Cloud traffic traverses last-mile Internet connectivity via SD-WAN tunnels to logical cloud gateway instances within the SDCI provider.
  - Logical SDCI Interconnect provides connectivity between SDCI data centers in different geographic regions.
  - Cloud provider cross-connects within the SDCI provider data centers provide direct access to public cloud providers (AWS, GCP, Azure, etc.) for IaaS and some SaaS applications
- Access to Internet and some SaaS traffic is enabled through Internet Edge (firewall, etc.) or through SIG (Umbrella, Zscaler, etc.).
- Guaranteed service levels (BW, latency, loss) within the SDCI provider and to cloud provider network.

Site to Cloud – Connectivity options…AWS as an example

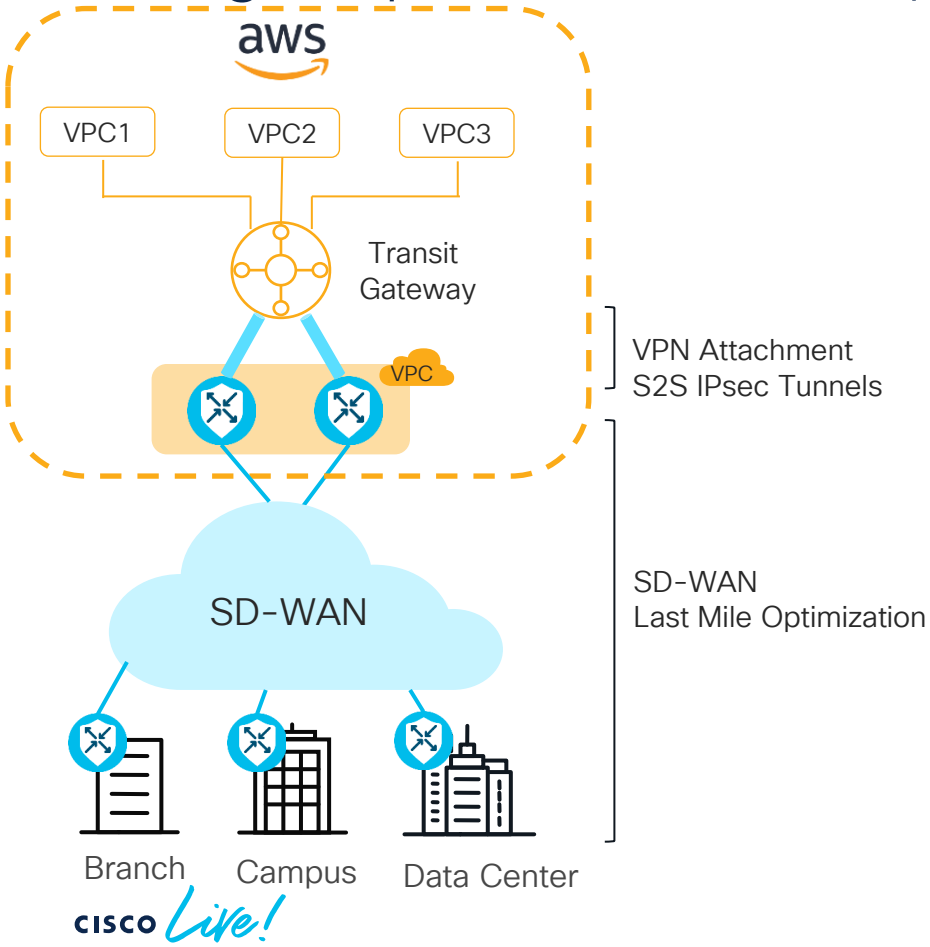
Design Option#1 – Branch Connect Model



Design Considerations:

- Automated provisioning through vManage (CoR-MC-Branch Connect)
- Lower costs while comparing to Transit VPC design
- More BW available per site (~1.25 Gbps per tunnel – which is a Cloud limitation)
- HA Support for IKE-IPSec tunnels
- Needs monitoring of individual tunnels from all the branches to TGW

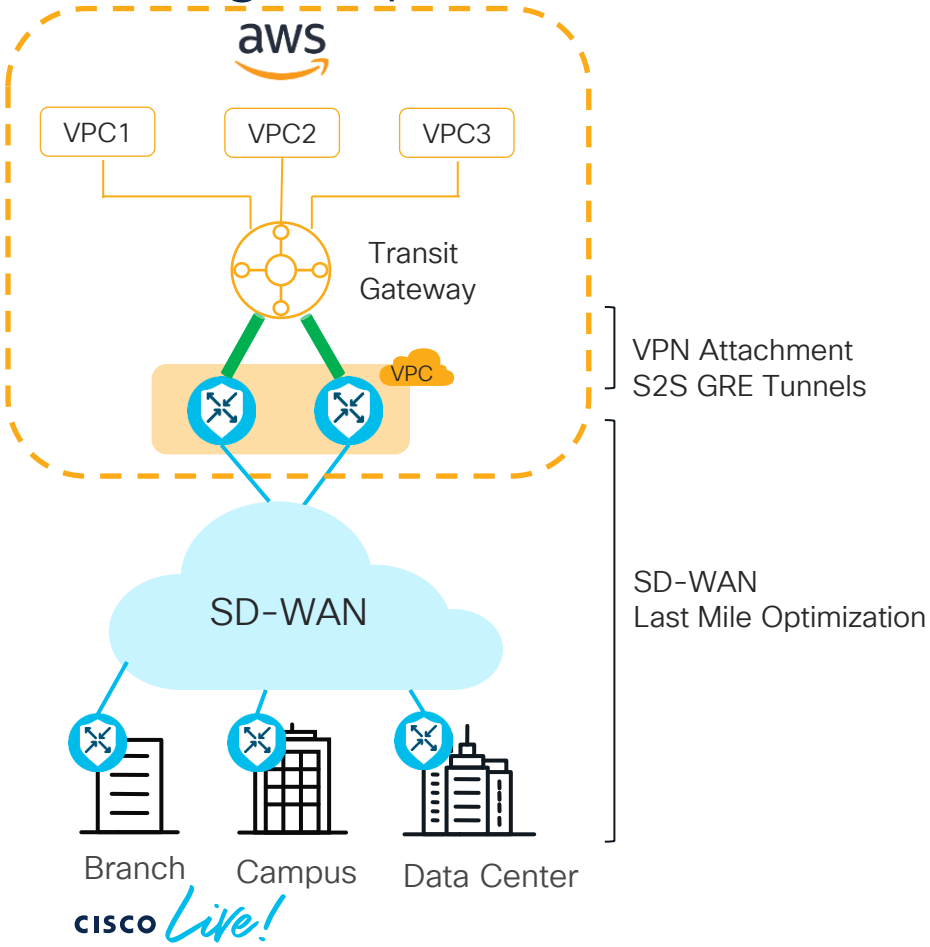
Design Option#2 – VPN (IPSec) based Model



Design Considerations:

- Extend SD-WAN up to TGW
  - vManage automation
  - Apply uniform business intent via SD-WAN policies all the way into cloud
  - Extend existing network segmentation into the cloud
- Optimized routing and path selection
- Lower operational overhead
- DPI and flow visibility, up to the cloud
- Leverage SD-WAN for HA architecture
- S2S VPN tunnel (one per service VPN) max limits to ~1.25 Gbps. It can be Mitigated by suing multiple VPN tunnels and leverage ECMP

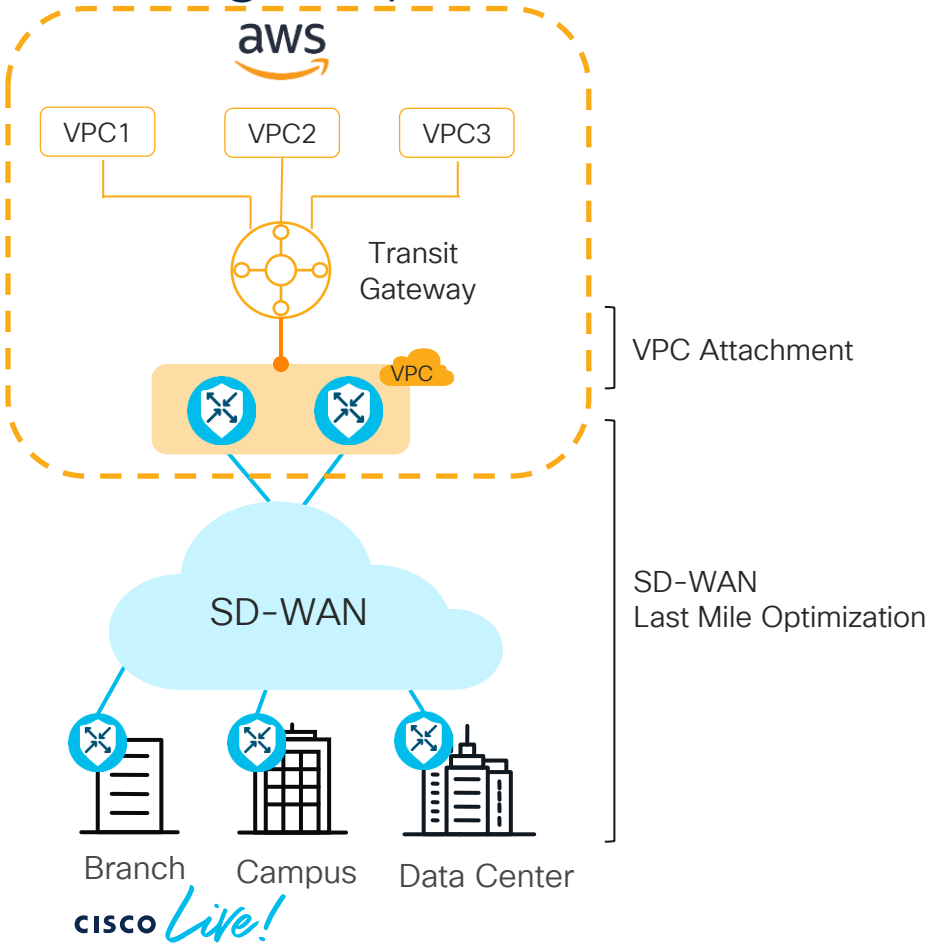
Design Option#3 – GRE Connect based Model



Design Considerations:

- Extend SD-WAN up to TGW
  - vManage automation
  - Apply uniform business intent via SD-WAN policies all the way into cloud
  - Extend existing network segmentation into the cloud
- Optimized routing and path selection
- Lower operational overhead
- DPI and flow visibility, up to the cloud
- Leverage SD-WAN for HA architecture
- Max throughput of 5 Gbps for each AWS GRE tunnel
- C8Kv instance size determines the throughput (up to 20 Gig IMIX throughput)

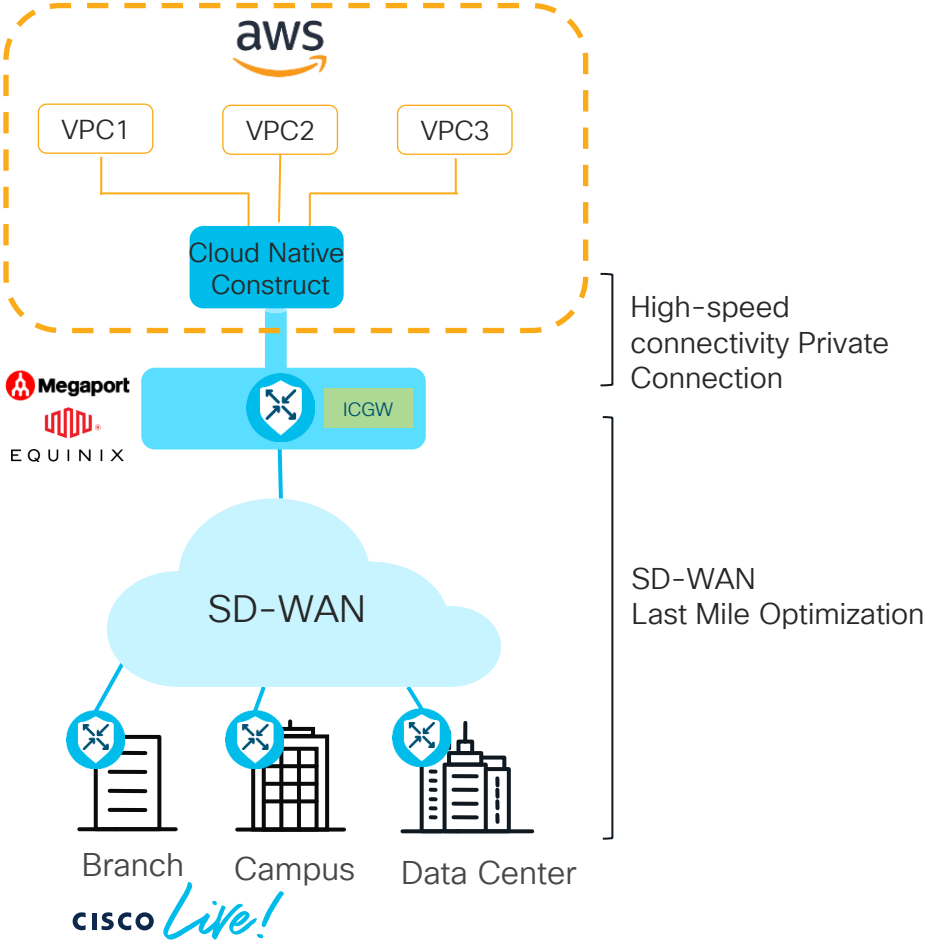
Design Option#4 – VPC Attachment Model



Design Considerations:

- Higher single connection bandwidth
  - Terminating SD-WAN VPC to AWS Transit Gateway as a VPC attachment eliminates 1.25 Gbps limitation
- Saves the cost associated with AWS S2S VPN connections
- Connection between the SD-WAN VPC and AWS Transit Gateway is unencrypted
- Needs Static routing to be configured manually
- No vManage Built-in automation, can be done through custom automation tools like Terraform

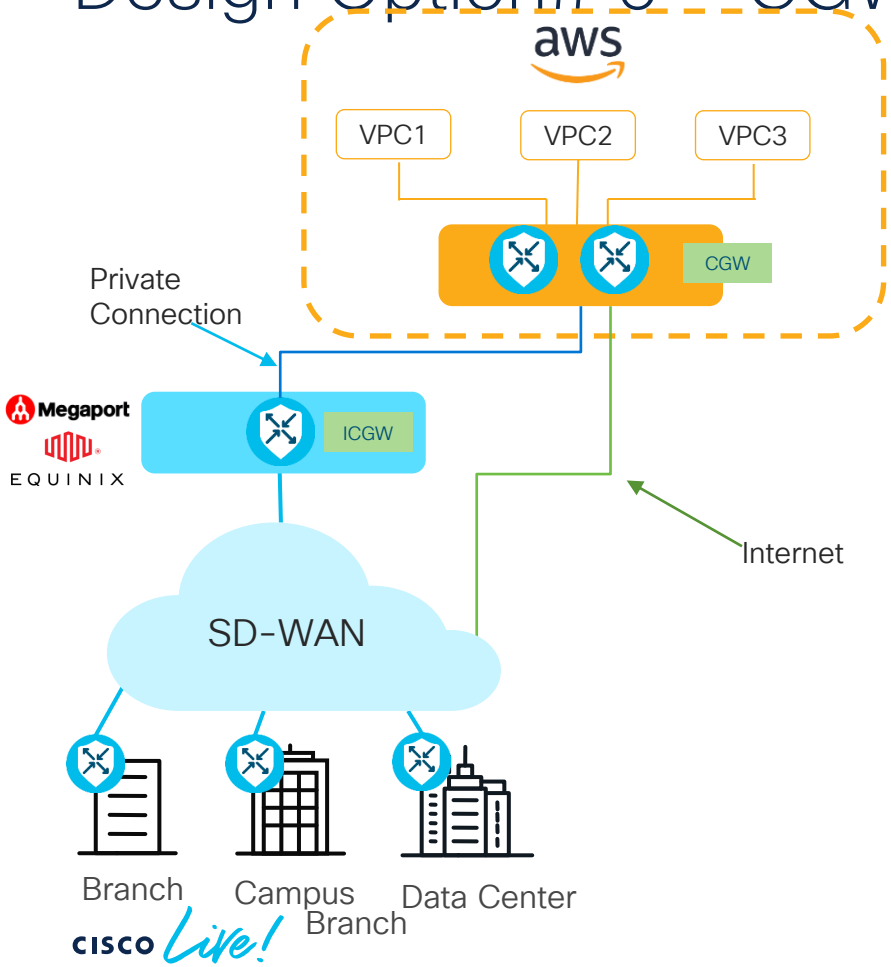
Design Option# 5 – CoLo Interconnect Model



Design Considerations:

- Regionalized CoLo design benefits
  - Service Chain
  - Scale as you grow
  - High speed path to cloud
- Optimized routing and path selection to the CoLo
- Leverage SD-WAN for HA architecture
- CSP Prefix limitation applies
- Encryption is done upto ICGW

Design Option# 6 – CGW in SDCI Model



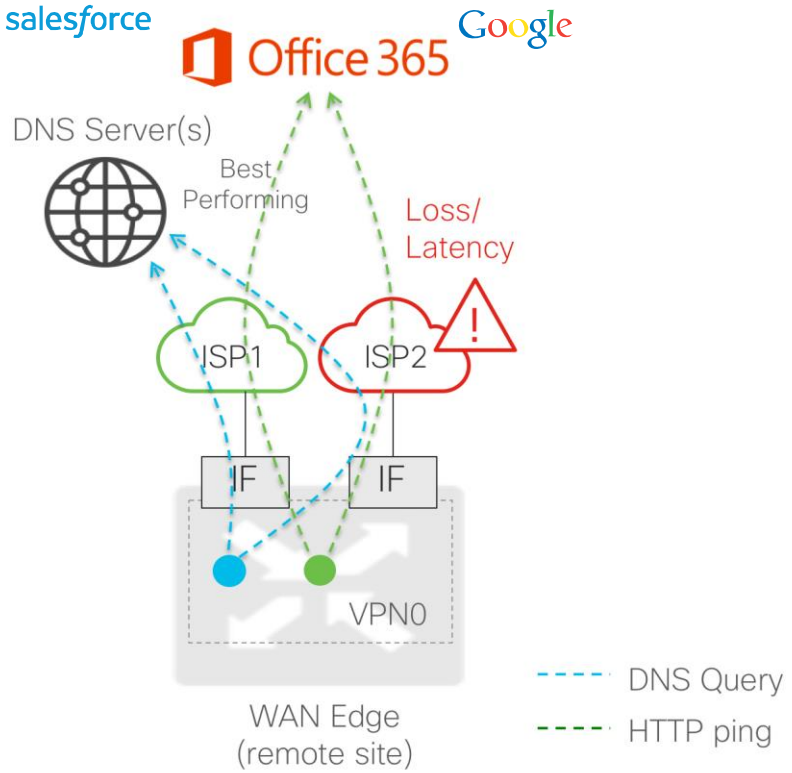
Design Considerations:

- End-to-End Encryption from branch to SDCI to Cloud
- Multi Segment
- Multi-Path support (Internet & private)
- Avoids prefix-advertisement limitation applied by CSPs.

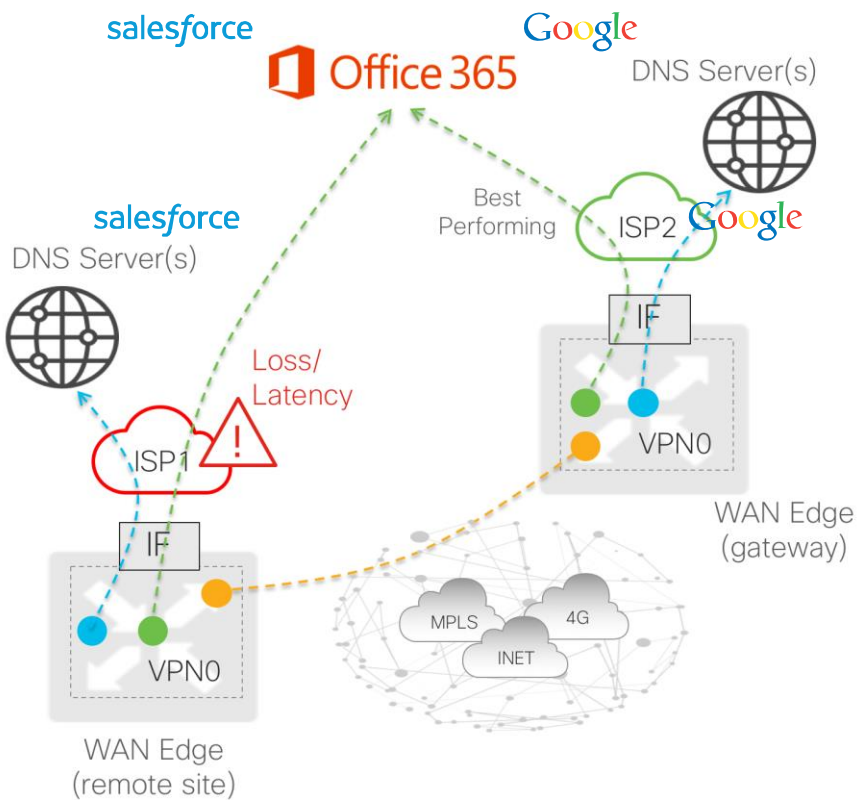
Site-to-SaaS Connectivity Models

Internet based connectivity to SaaS Cloud Providers

Dual DIA

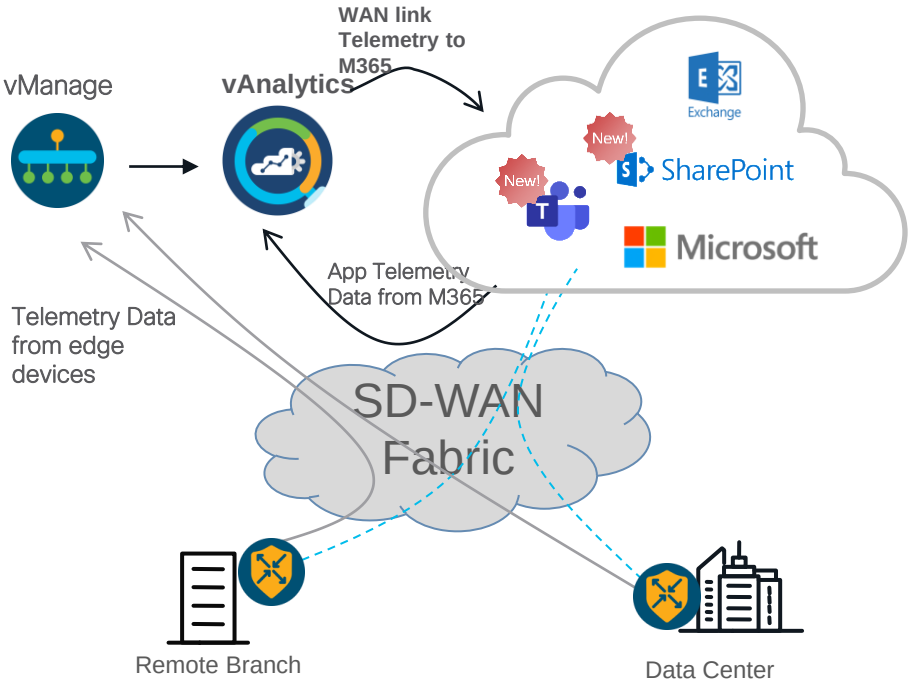


Single DIA



- Supports Custom App

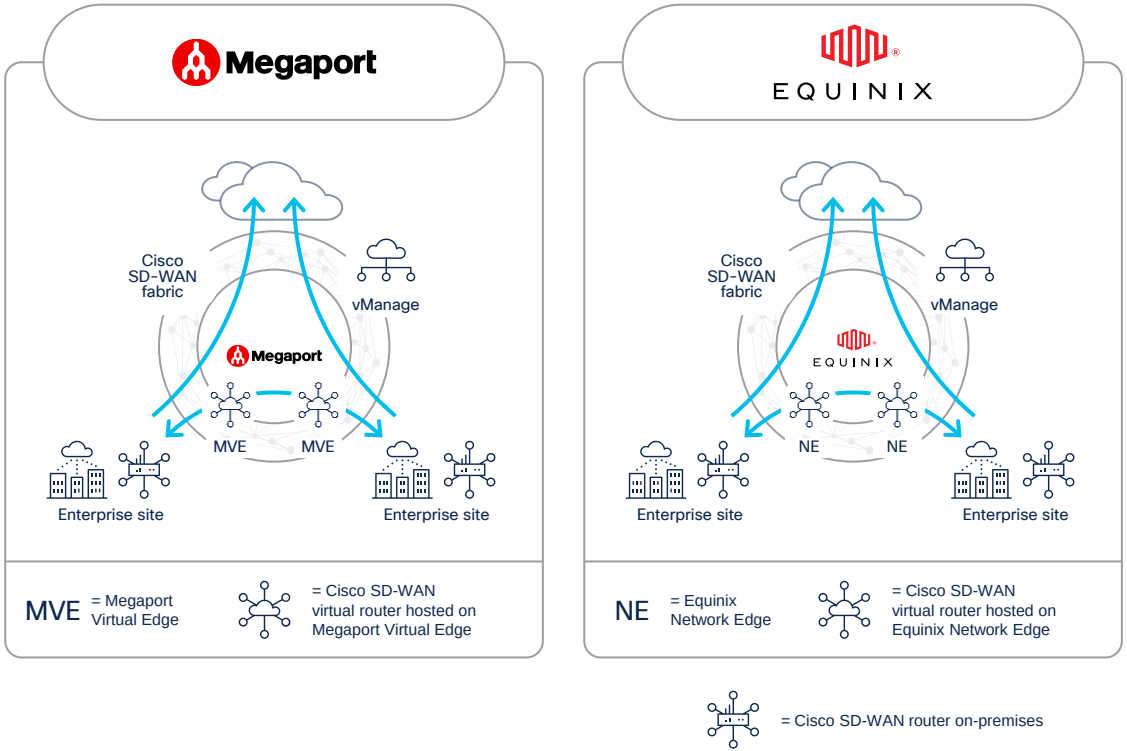
Cloud OnRamp for M365
Microsoft Teams and SharePoint support



- First Packet Match for M365 Traffic
- vAnalytics receives Teams and SharePoint telemetry data from Microsoft
- Application and Network Telemetry provides application performance insights
- vAnalytics uses Network and App telemetry data to compute best path
- SD-WAN router selects best path based on results received from vAnalytics

Site-to-Site Design

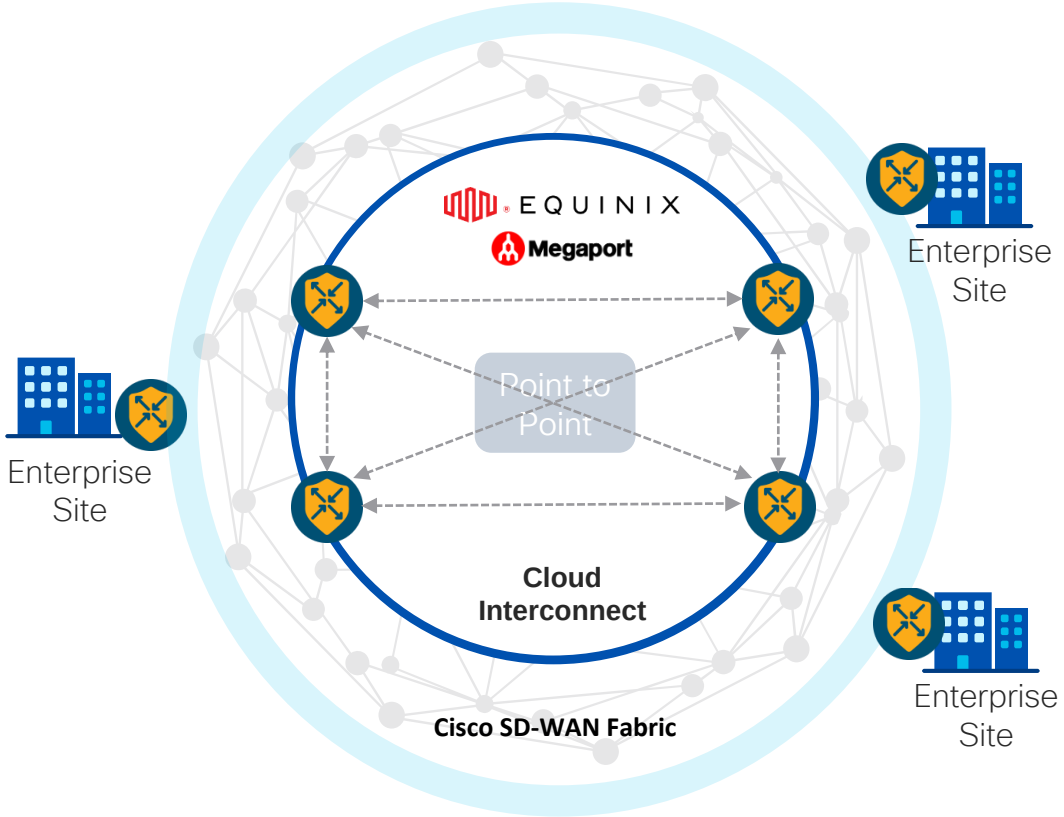
SDCI / Cloud Interconnect



Benefits:

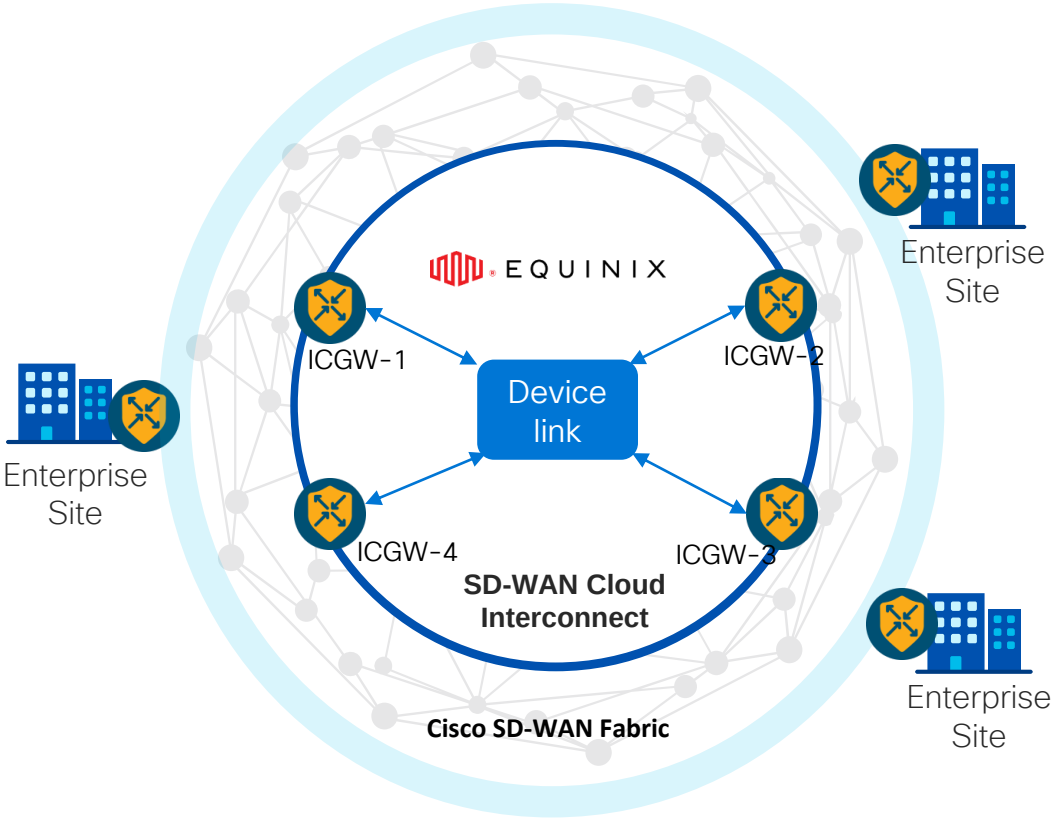
- Return on investment
- Single pane of glass automation
- Secure Multicloud networking

SDCI – Point-to-point connectivity



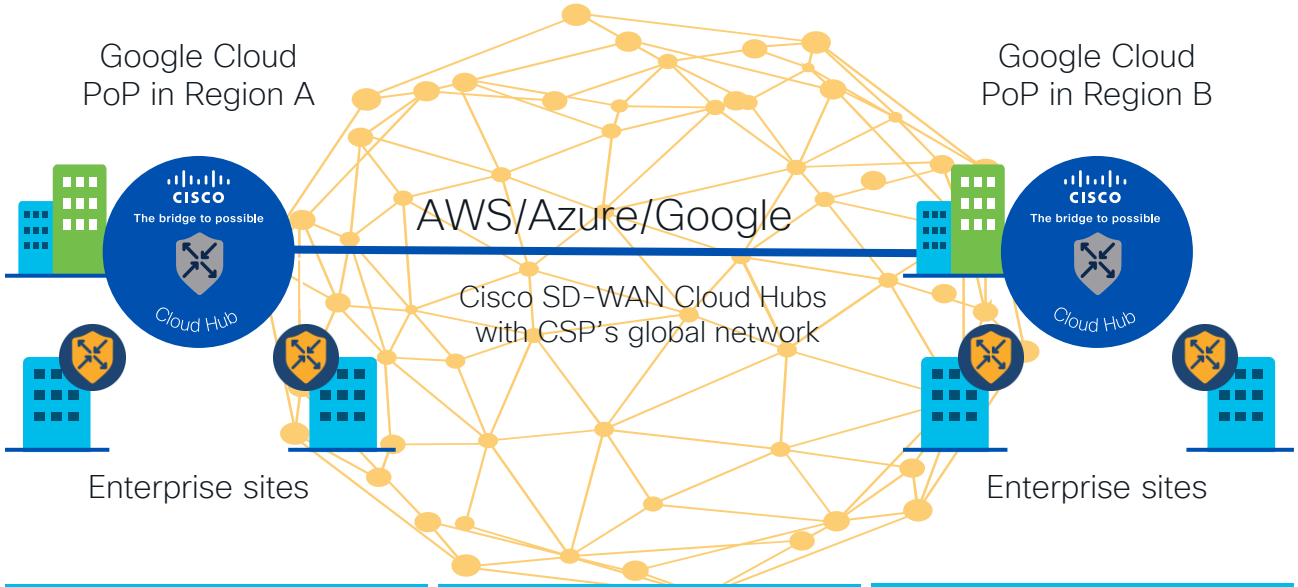
- A cloud-delivered regional aggregation service with rich set of programmable cloud direct-connects
- Point-to-point full mesh connectivity between ICGWs in SDCI
- Guaranteed SLAs on SDCI Backbone

SDCI – Device link connectivity



- Device Link connectivity is specific to EQUINIX (Point-to-multipoint connectivity -> simplifies the policy, ease of use).
- Creates one Broadcast Domain.
- Only ICGWs can be Device link Group Member.
- Extension for site-to-site connection.
- All Device link Group members are connected using virtual links to form full-mesh.

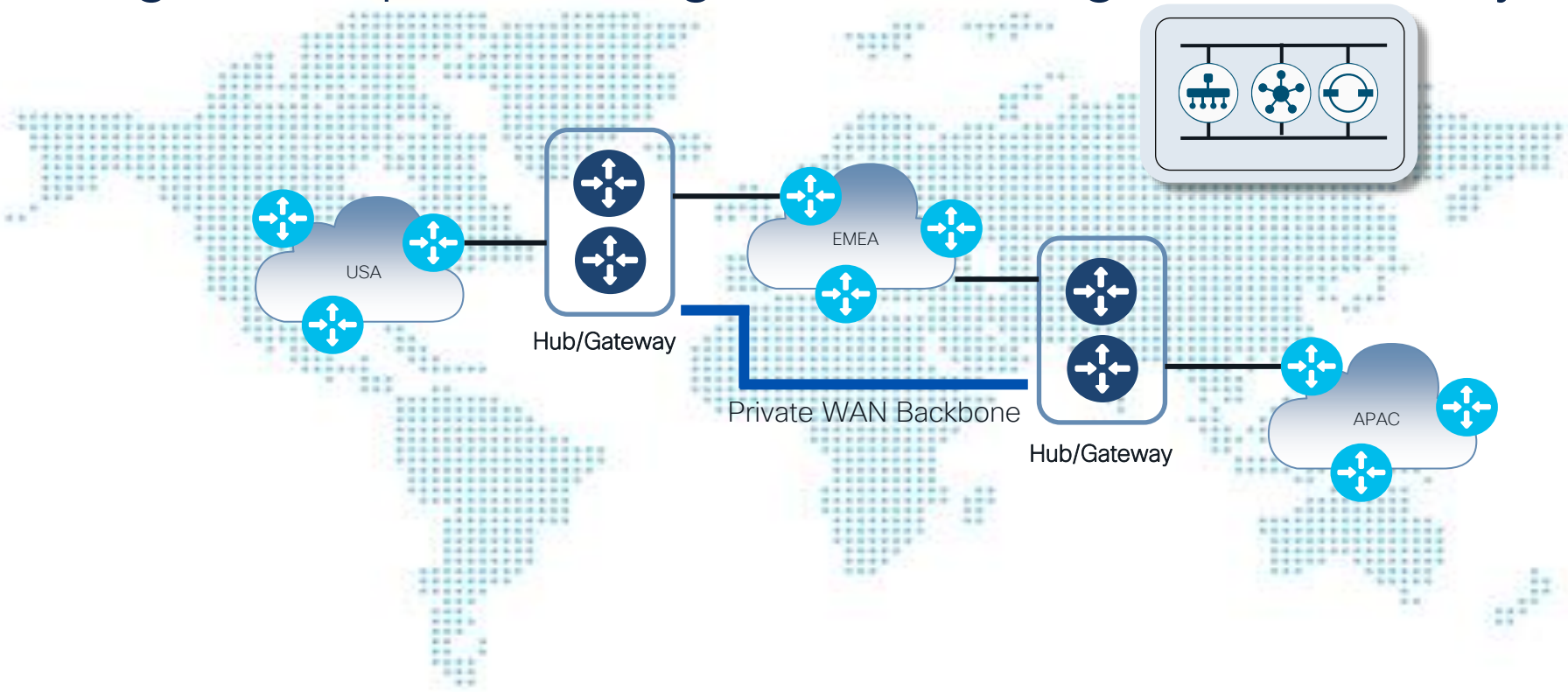
Cloud Service Provider (CSP) SD-WAN Architecture for Site-to-Site Connectivity



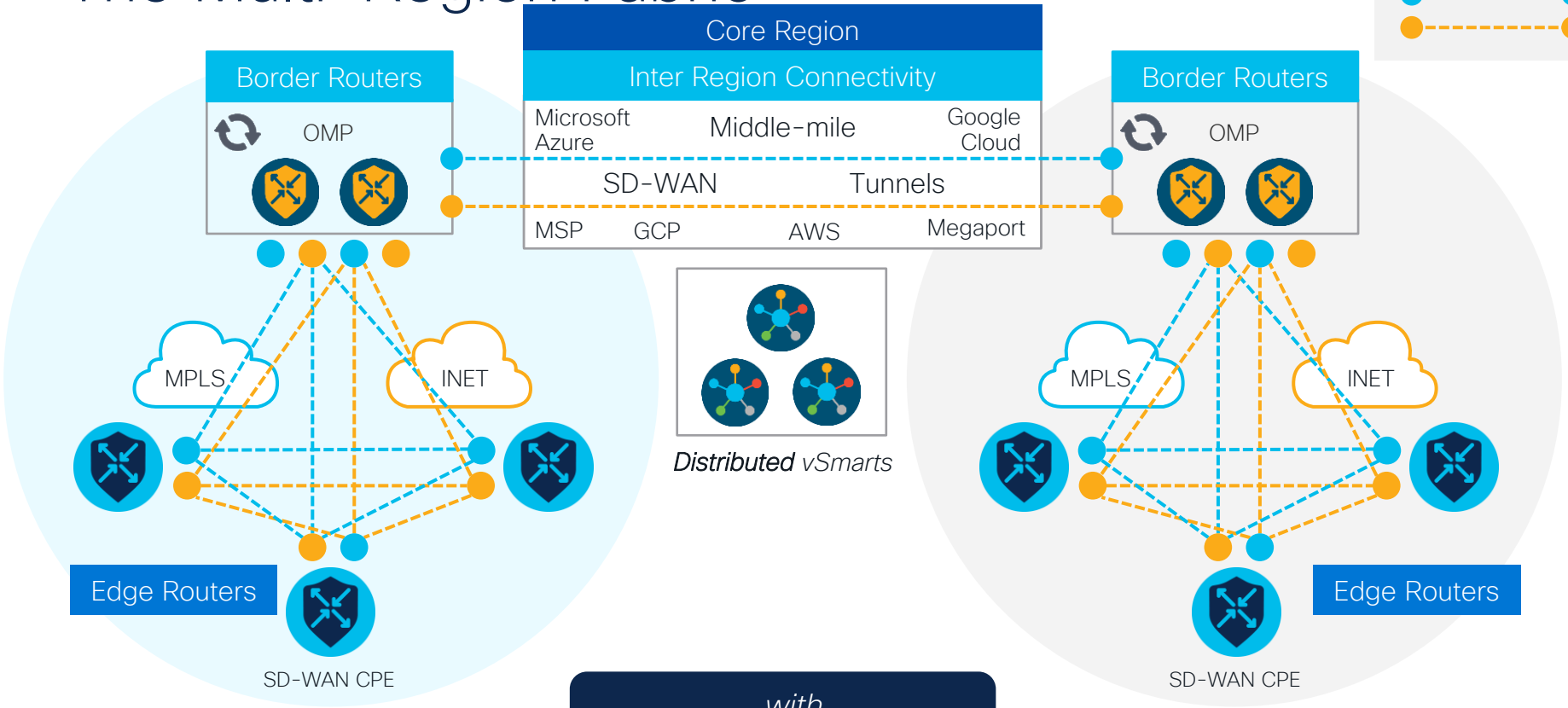
Multi-Region Fabric

Using Cloud as Core

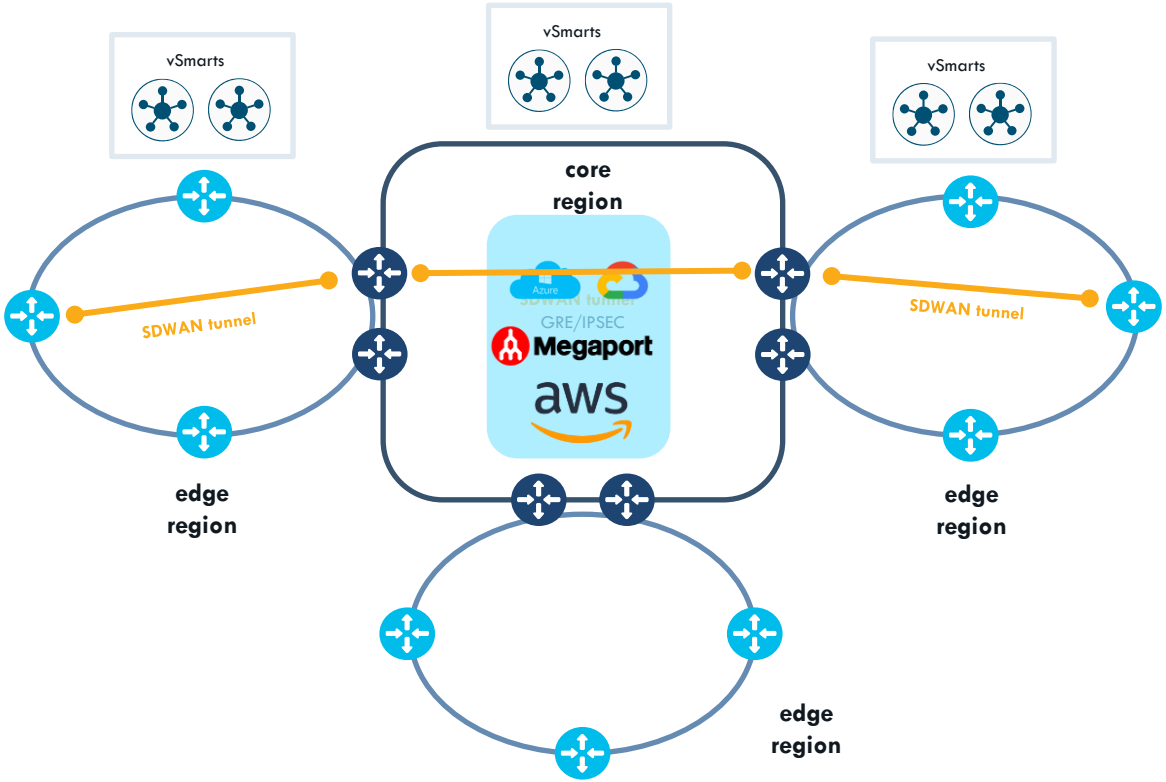
Large Enterprise – Regional Meshing and Gateways



The Multi-Region Fabric



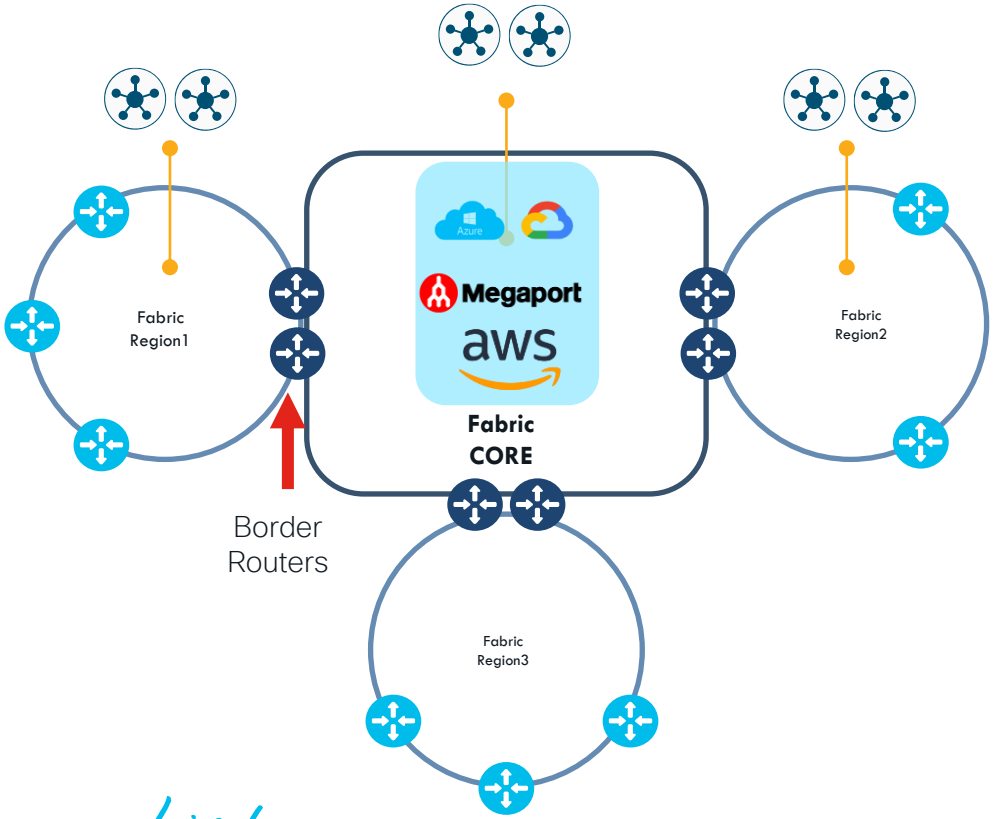
Topology – IP Forwarding



Topology

- 2-Layer Architecture
- SDWAN tunnels limited to regions
- Hop by Hop tunnels
- Decrypt/Encrypt on all nodes along the path
- IP Lookup and Forwarding per node
- Requires Service VPN on intermediate nodes (Border Routers)
- Mix of encapsulation is possible GRE in core/access
  Example: IPsec on access region and GRE on core

Border router & Distributed vSmarts



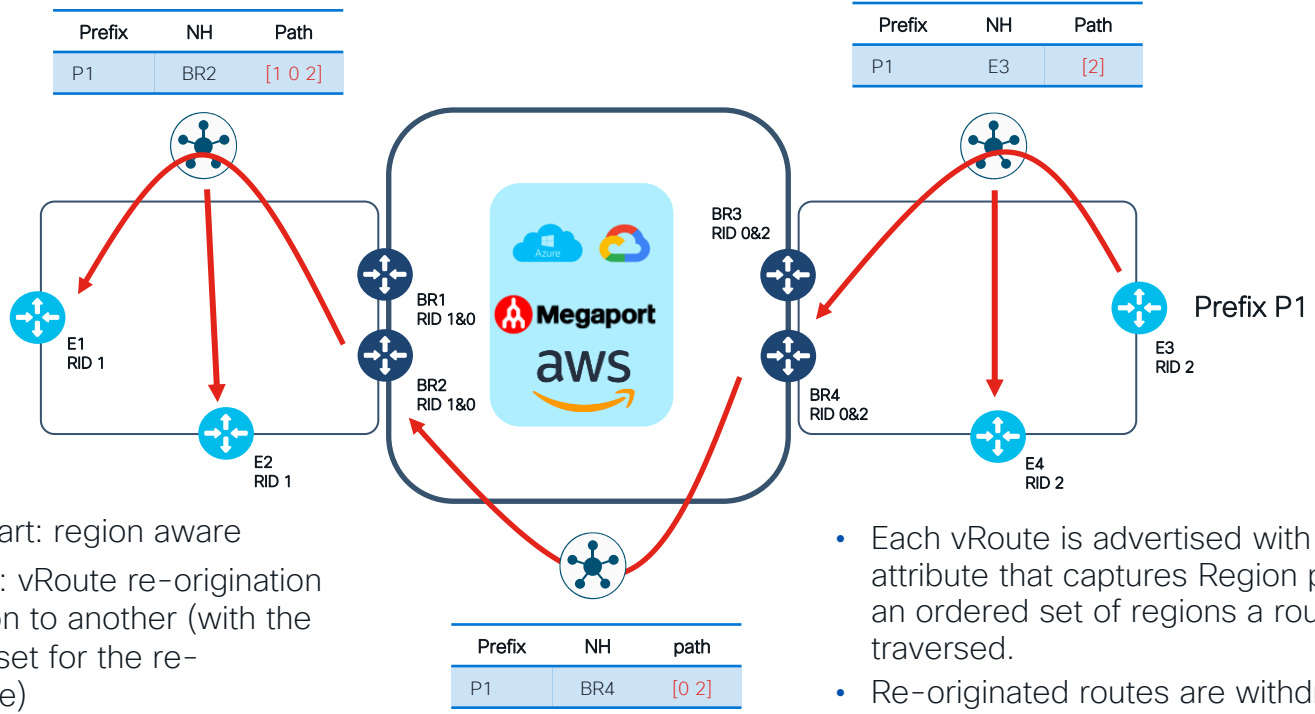
Border Router

- Provides inter-region connectivity by connecting regional overlay to a common core or back bone overlay
- Hosted in MSP POP, Cisco POP, CSP, SDCI
- Horizontally scalable
- Only serves 1 access and 1 core region

Regional vSmart

- In MRF, vSmart controllers become regional
- Mitigates the path scale challenges

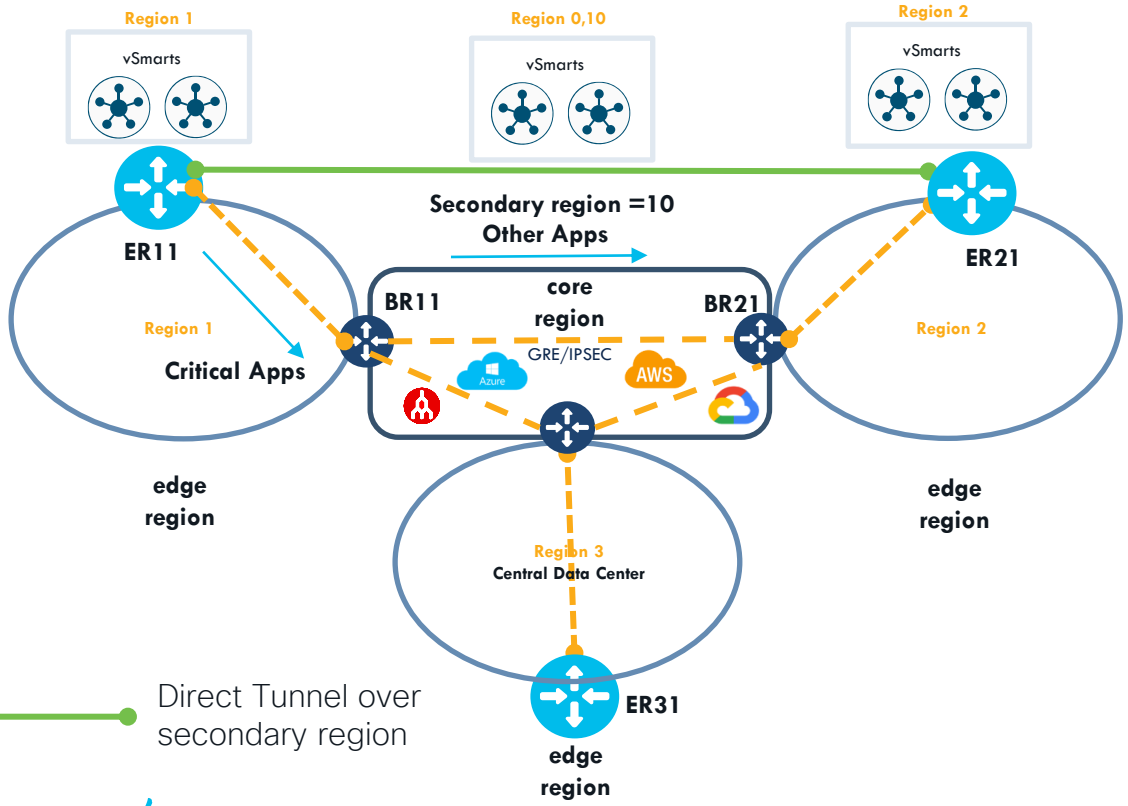
Routing in Hierarchical SD-WAN aka MRF



- OMP and vSmart: region aware
- Border routers: vRoute re-origination from one region to another (with the correct TLOC set for the re-originated route)

- Each vRoute is advertised with a new attribute that captures Region path- which is an ordered set of regions a route has traversed.
- Re-originated routes are withdrawn if the connectivity goes down. This helps prevent blackholing scenarios.

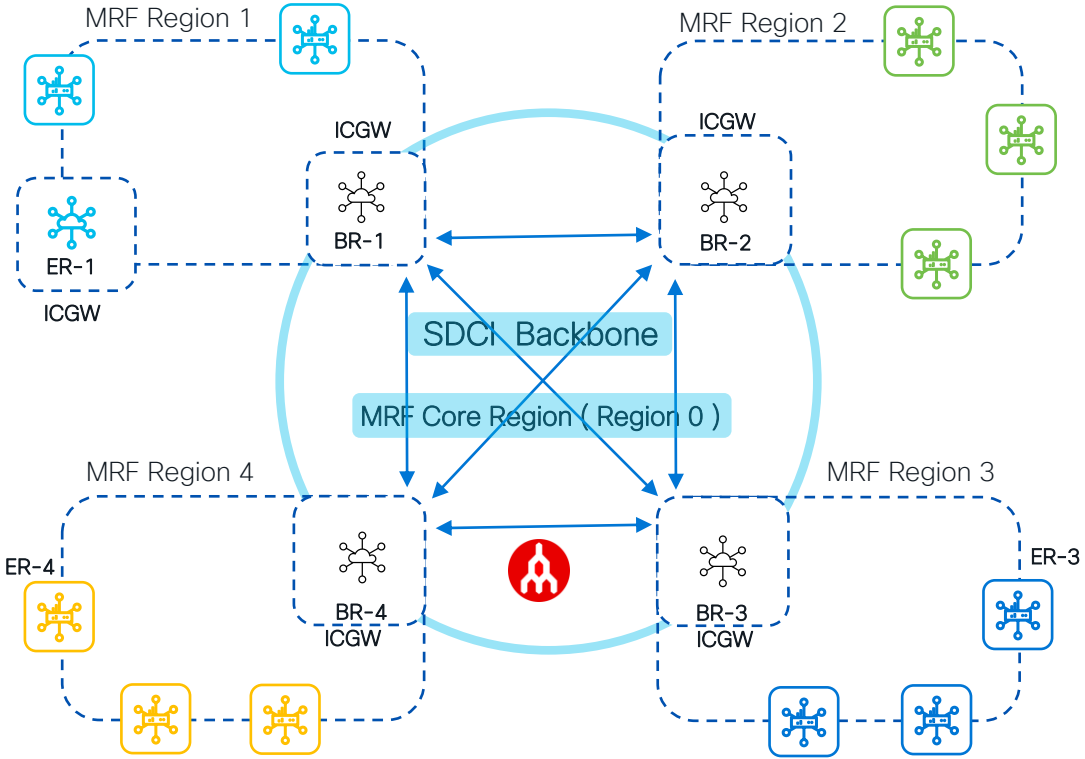
Secondary Region – Direct vs Indirect Tunnels



Use-cases

Send non-critical traffic using cheap links rather than using optimal Middle-mile bandwidth or PAYG links

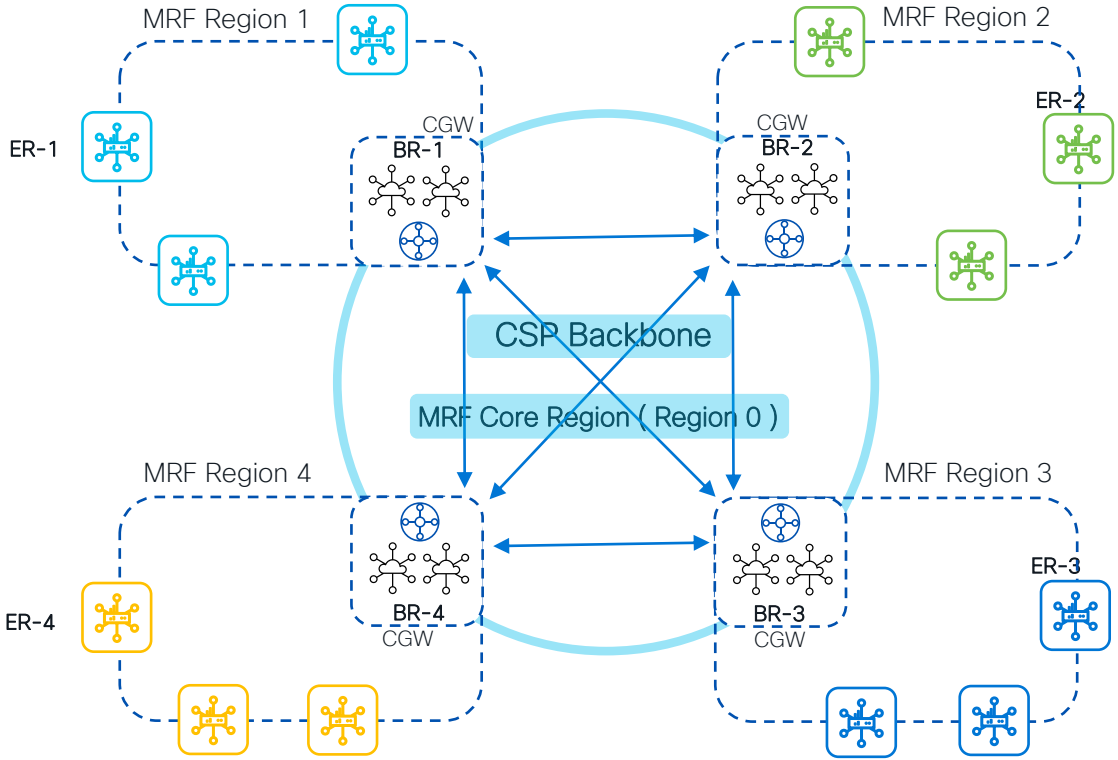
MRF with SDCI: (Megaport)



- Create one or more ICGW as BR for a Region.
- Full-Mesh connectivity between the Border-Router ICGWs is recommended. (but not required)
- Appropriate ICGW instance license and VXC licenses, supplemental licenses should be available.
- ICGW can be BR or ER role in a topology.
- The ICGW c8kv version should be 17.8 and higher for MRF support
- Equinix not supported.

cisco Live!

MRF with Multicloud:



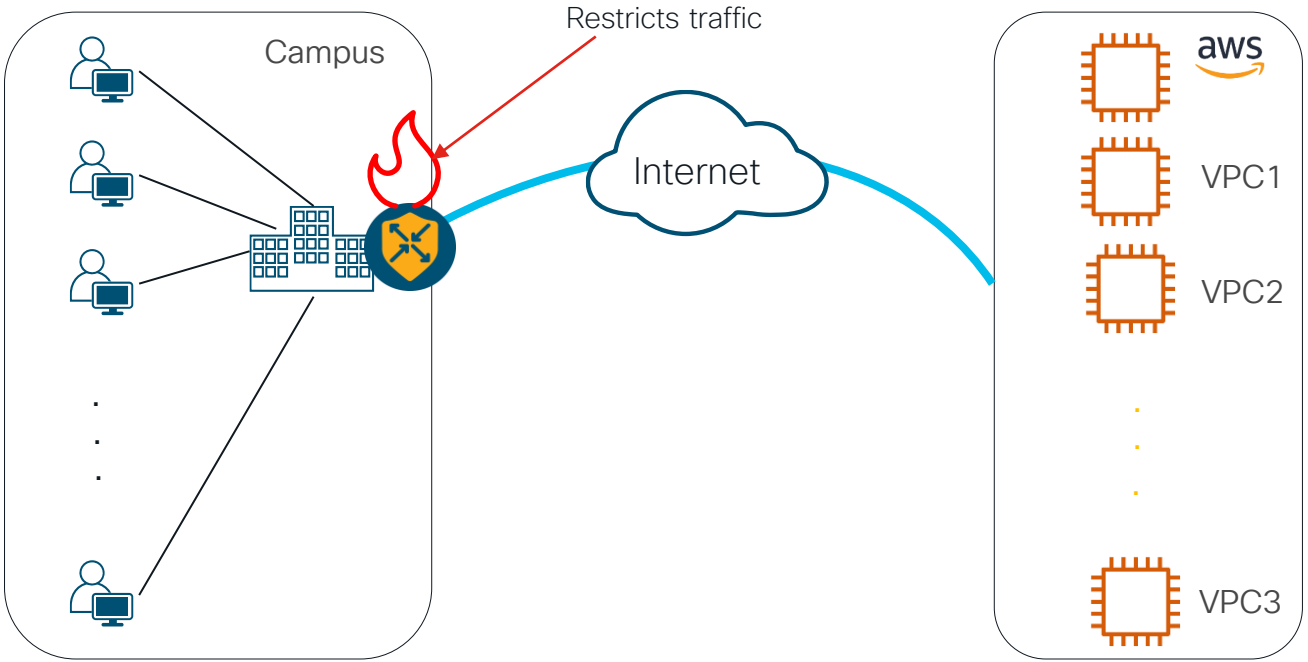
- Enable CSP-Specific requirement for full-mesh S2S (Core) connectivity.
- Both the SD-WAN router instance in the CGW should cater to the same region.
- Supports AWS, Azure, GCP, AWS GovCloud, Azure GovCloud.
- The CGW c8kv version should be 17.8 and higher for MRF support

cisco Live!

Some Key Design Asks

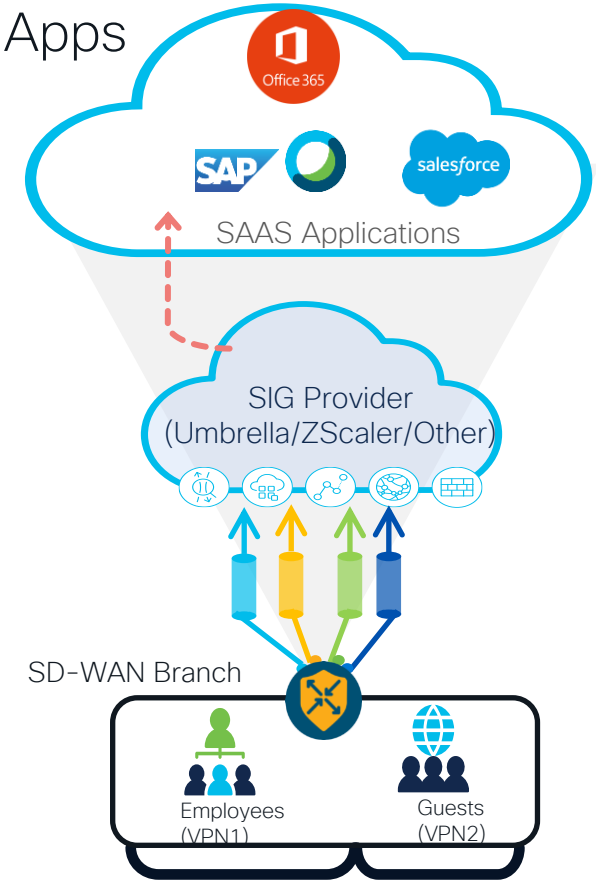
Ask# 1

Enterprise customer wants to extend multiple LAN segments into AWS cloud platform to access cloud hosted workloads



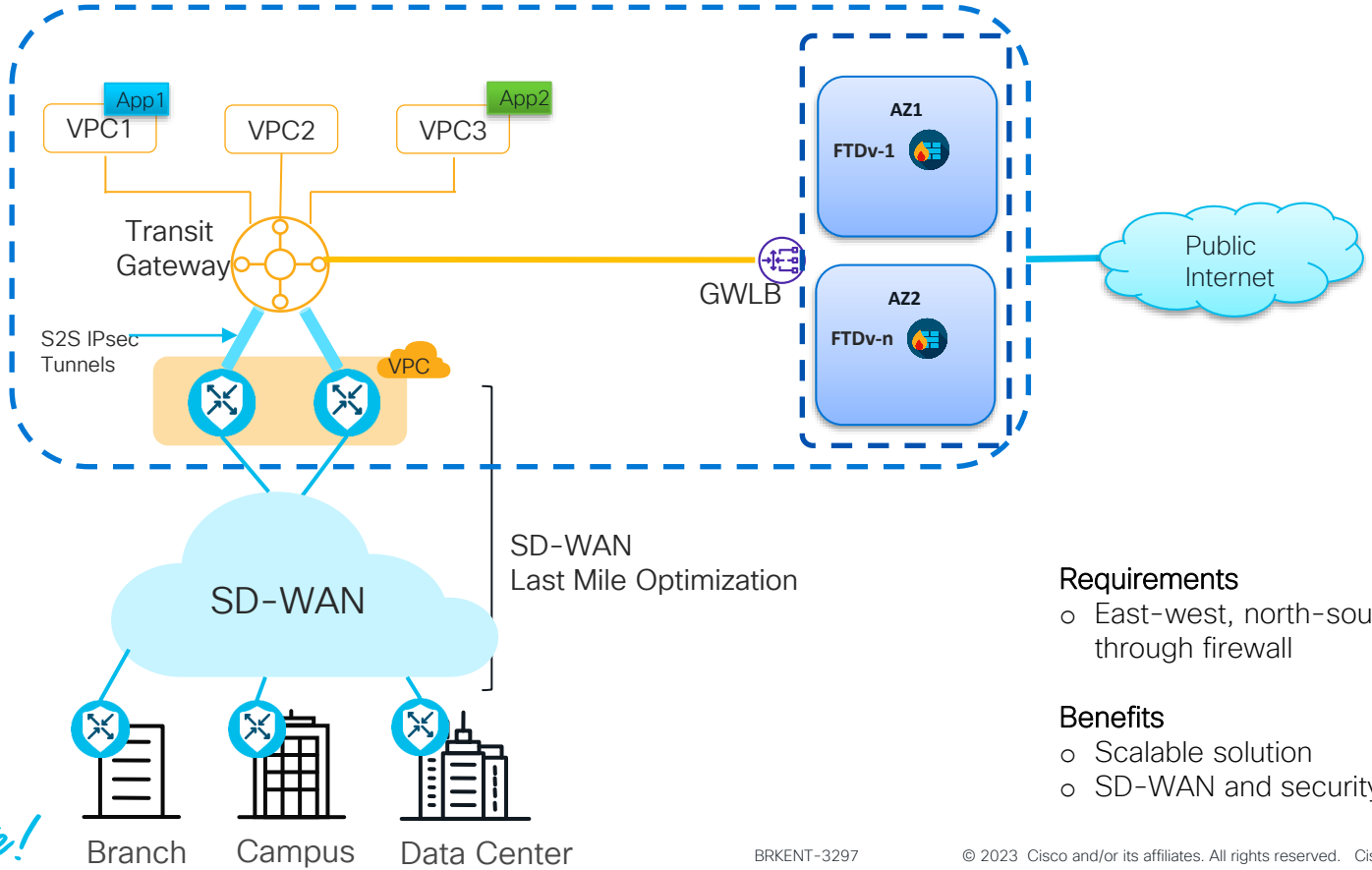
Ask# 2

A Healthcare customer wants to leverage Cloud based Security (SIG) to access SAAS Apps



Ask# 3

A Finance customer wants to leverage 3rd party firewall (Example: FTDv) for East-West traffic



Requirements

- East-west, north-south traffic must go through firewall

Benefits

- Scalable solution
- SD-WAN and security from one hand

Ask# 3

A Finance customer wants to leverage 3rd party firewall (Example: FTDv) for East-West traffic

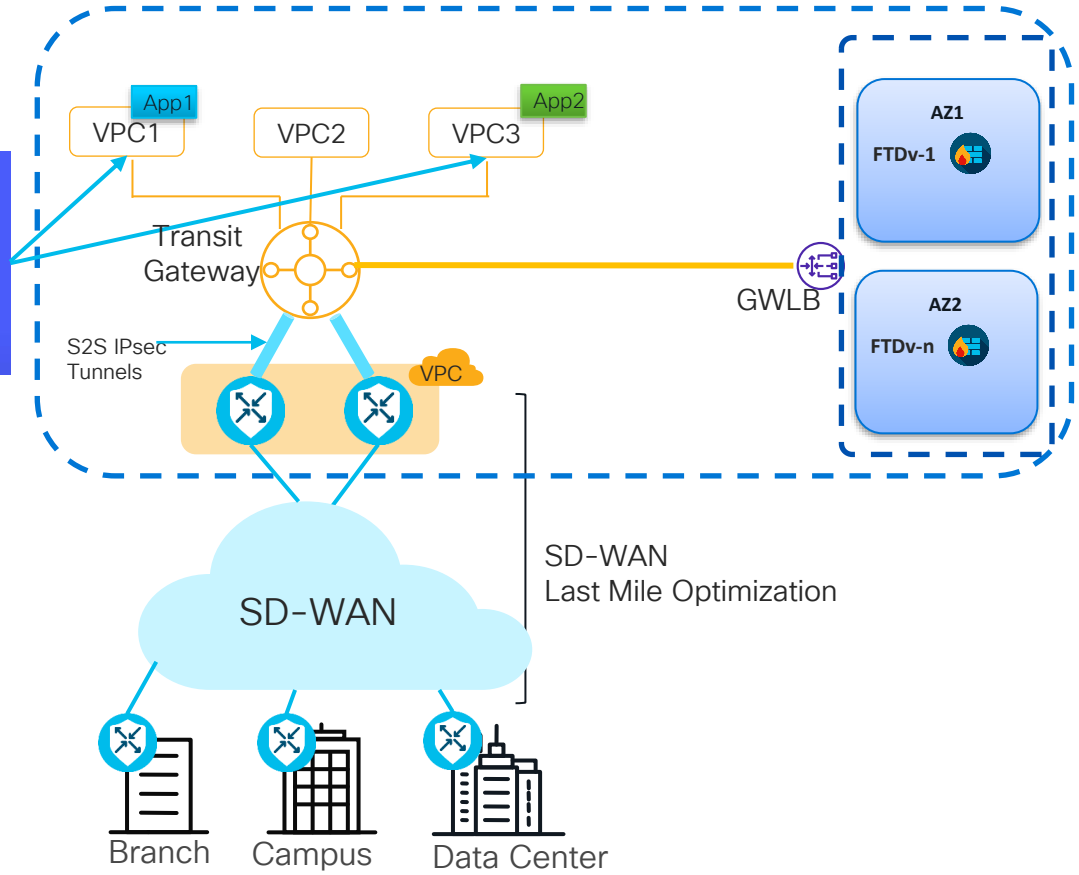
Design options

Design option 1: Host VPC route points to GLWB endpoint

10.111.0.0/16	local	
0.0.0.0/0	vpce-XYZ	FW-Endpoint-Service

Design option 2: Host VPC route points to AWS TGW

10.111.0.0/16	local	
0.0.0.0/0	tgw-XYZ	AWS Transit Gateway



Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from 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 Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN