
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Extend the Enterprise to the Cloud

AWS Cloud integration with Enterprise SD-WAN

Lee Sudduth, Customer Delivery Architect
Praveen Poojary, Customer Delivery Architect

BRKXAR-2015

Cisco Webex App

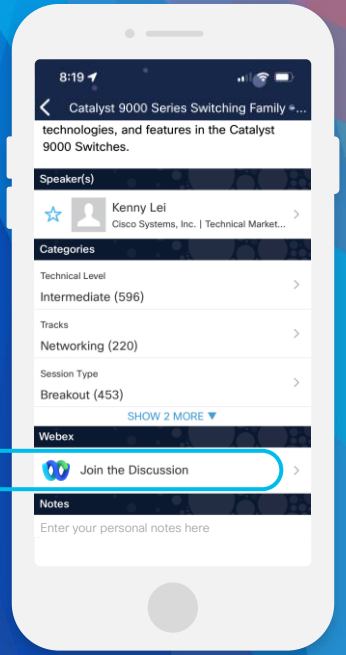
Questions?

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/#BRKXAR-2015

About Us

Praveen Poojary

Customer Delivery Architect

12 Years in Cisco

#3xCCIE

#CCDE

Lee Sudduth

Customer Delivery Architect

23 Years in Cisco

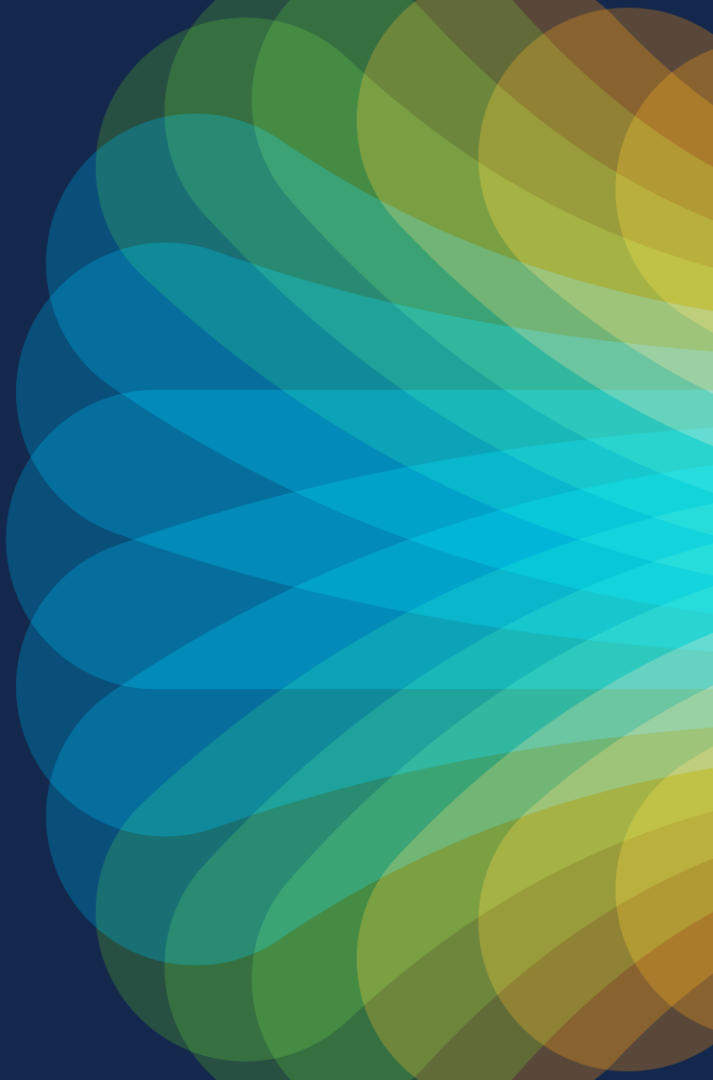
#CCIE

#CCDE

Agenda

- Introduction
- SDWAN Evolution
- Cloud On Ramp to AWS
- Site-to-Cloud Connectivity
- Security
- Demo

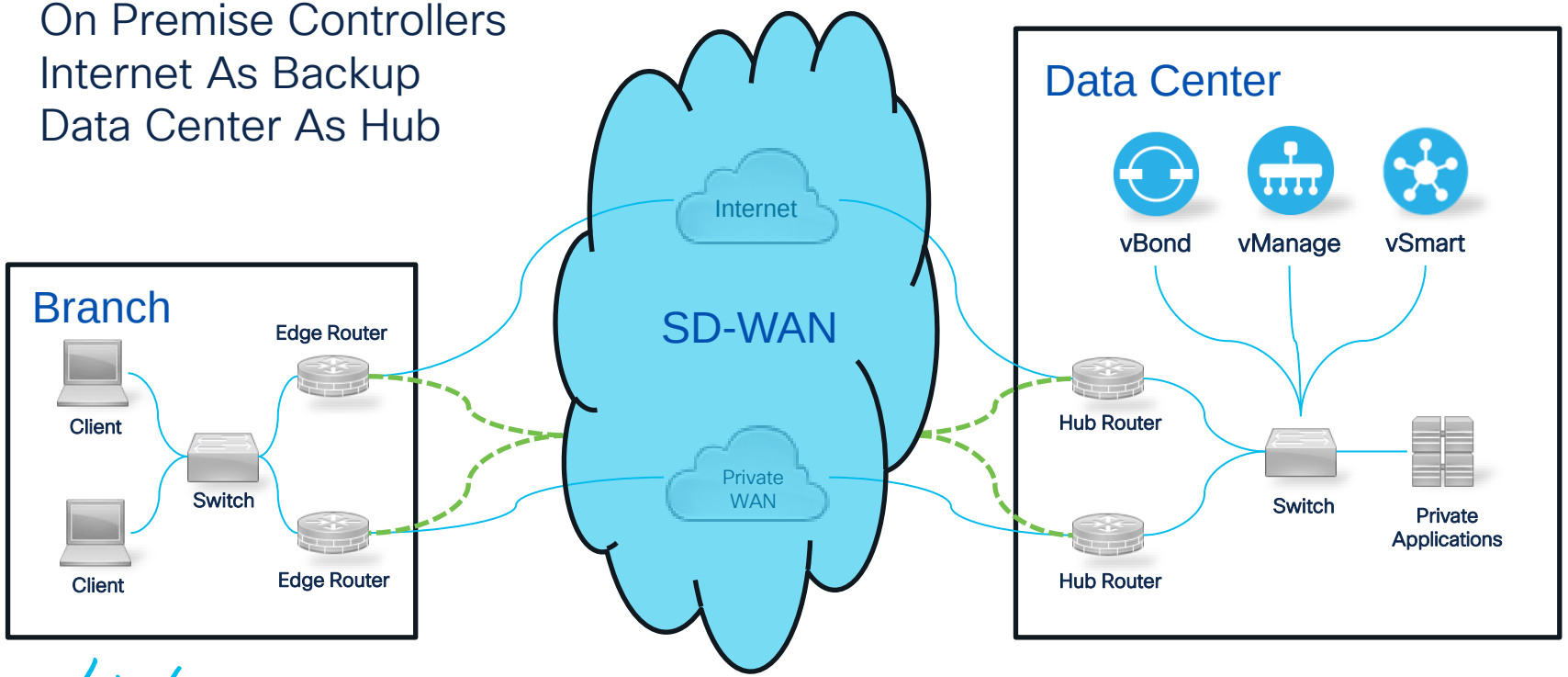
SD-WAN Evolution



From Data Center to Cloud

Traditional SD-WAN

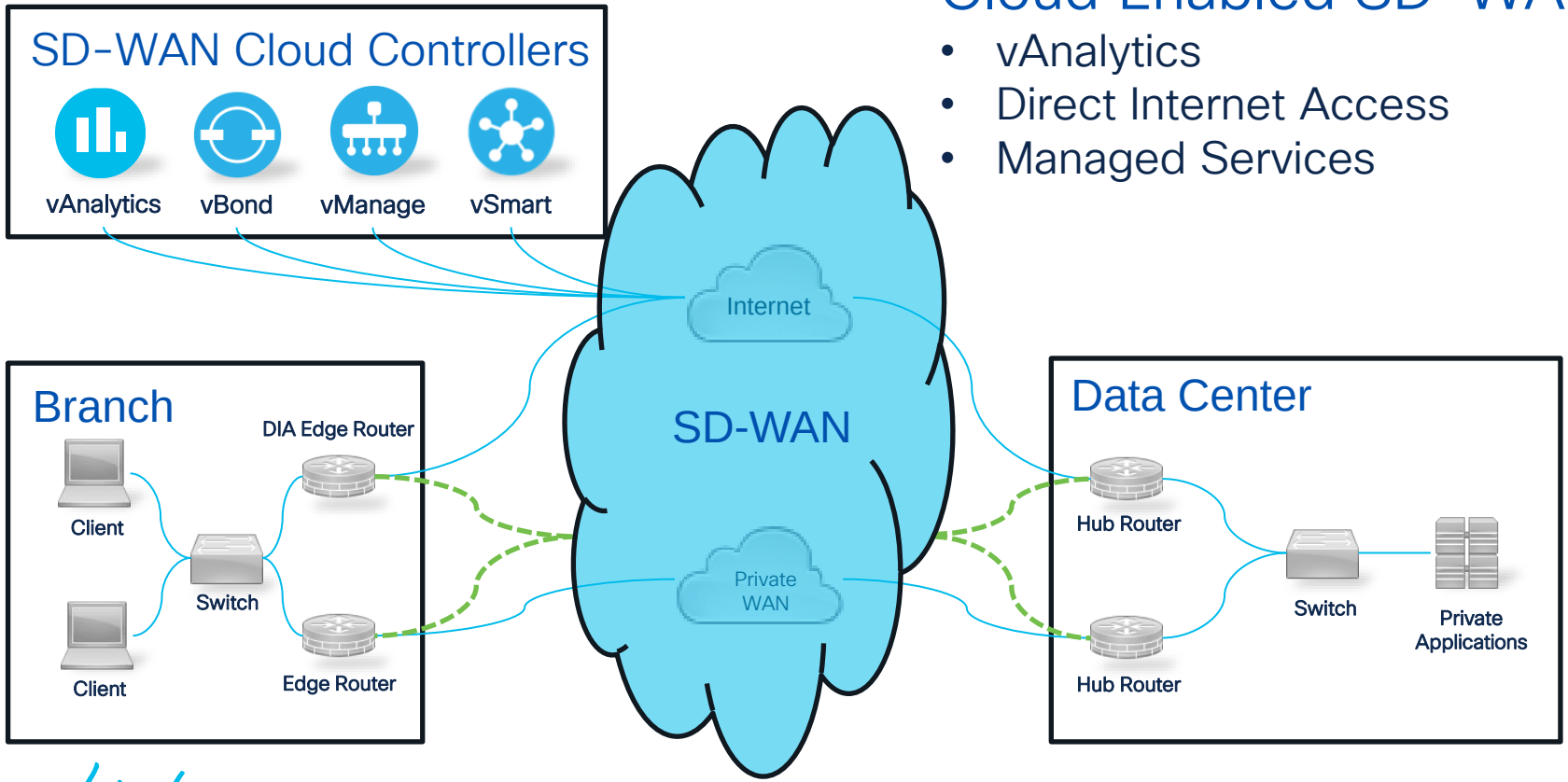
- On Premise Controllers
- Internet As Backup
- Data Center As Hub



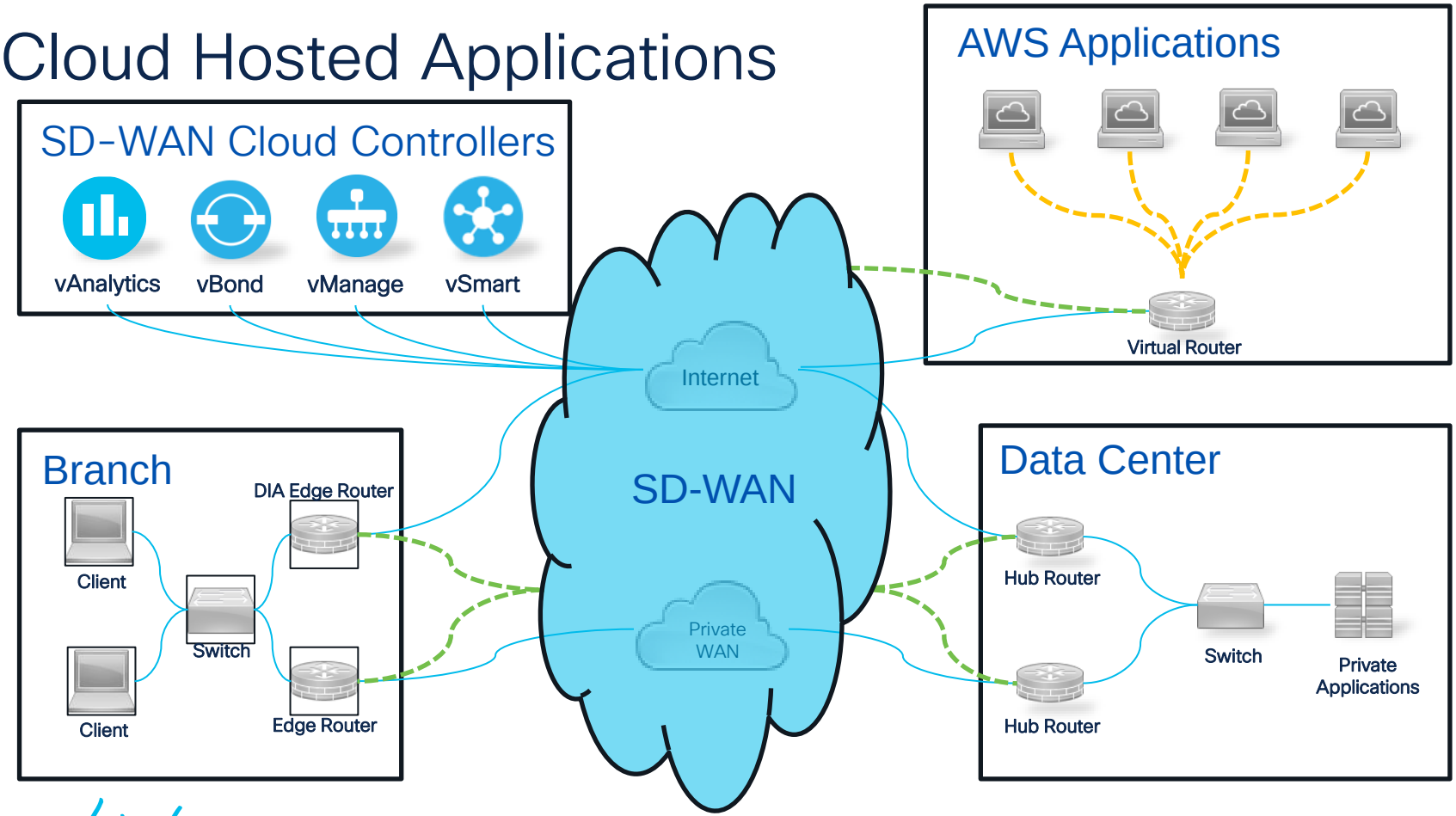
Cloud Hosted Controllers

Cloud Enabled SD-WAN

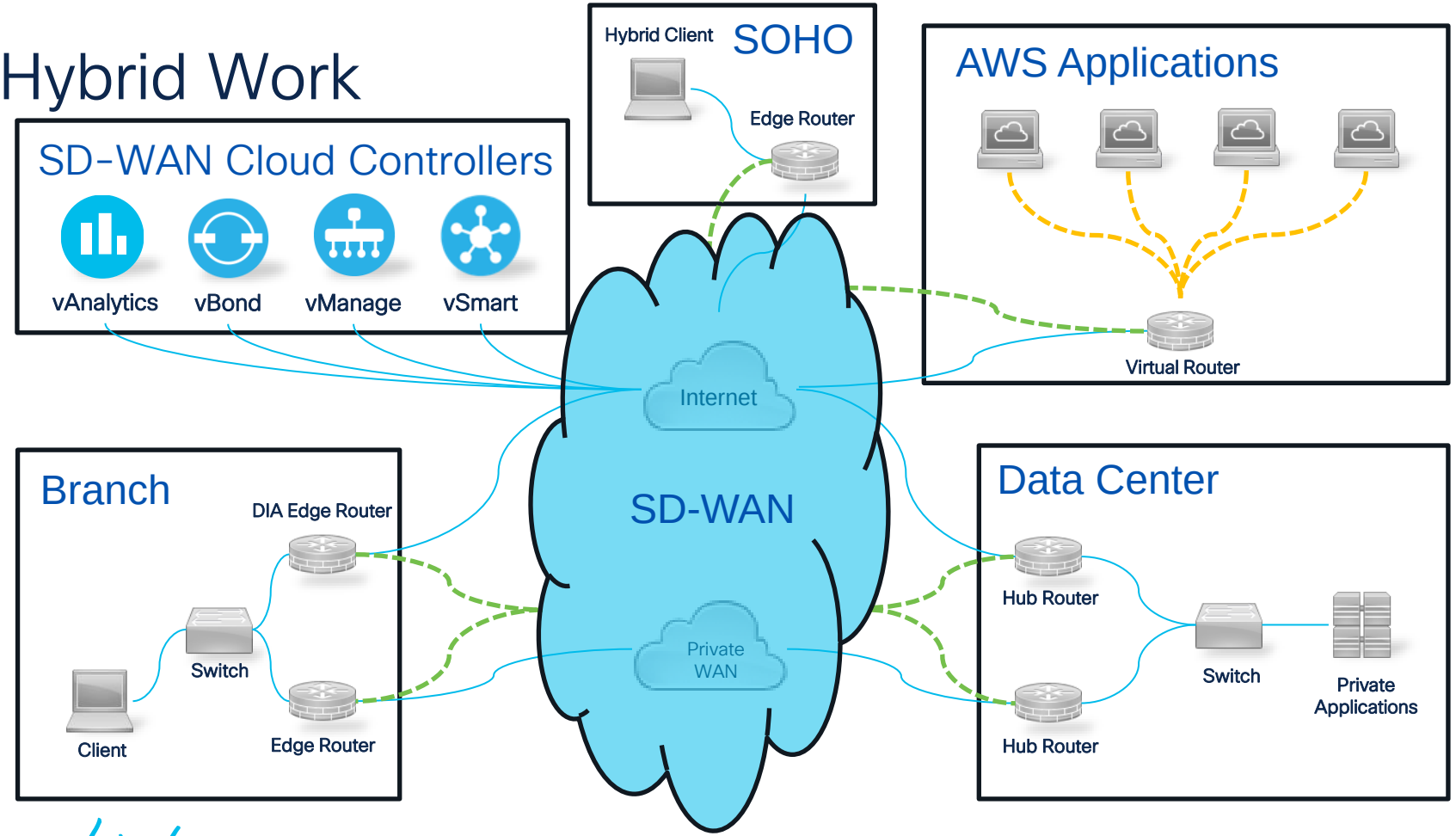
- vAnalytics
- Direct Internet Access
- Managed Services



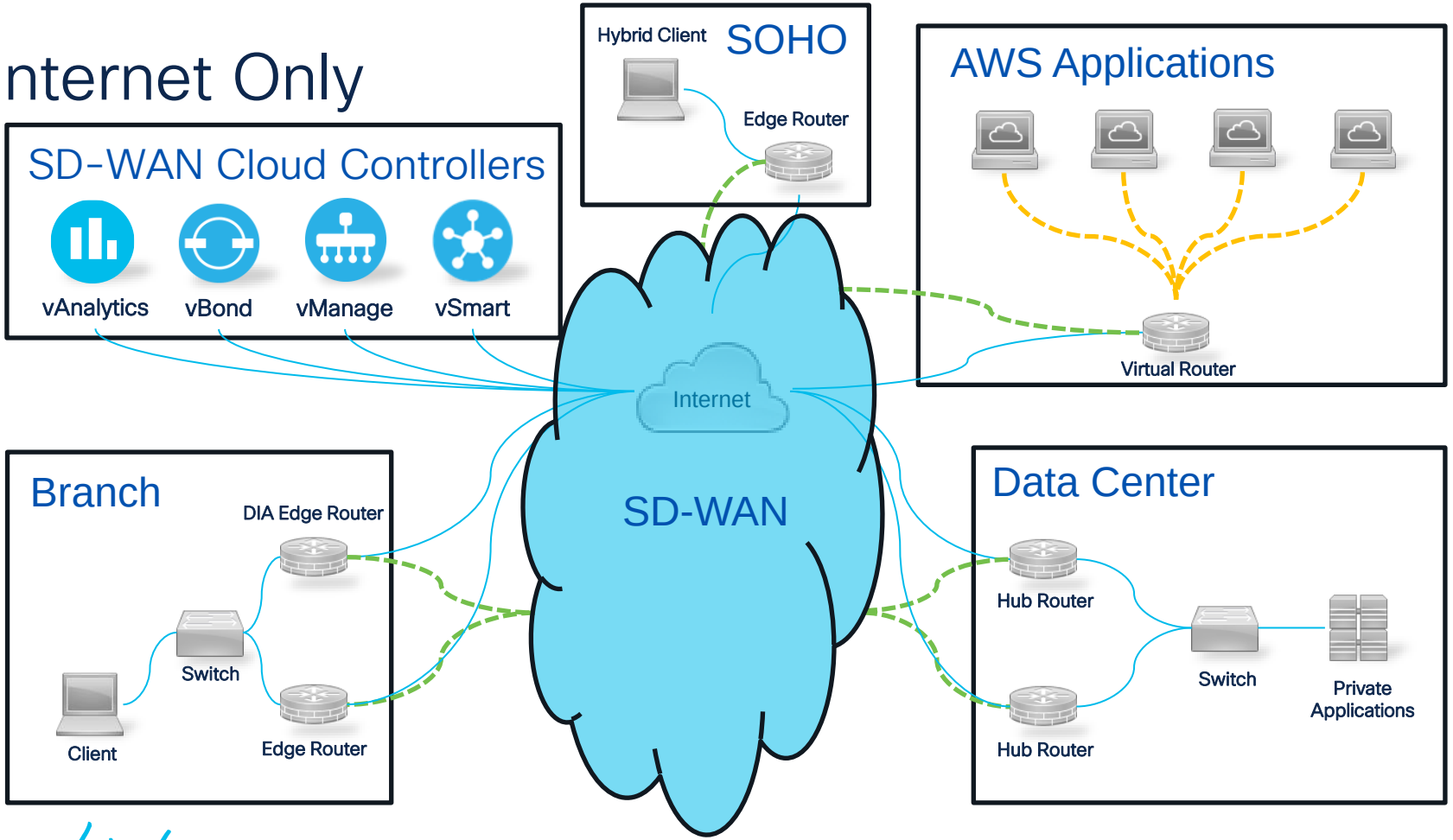
Cloud Hosted Applications



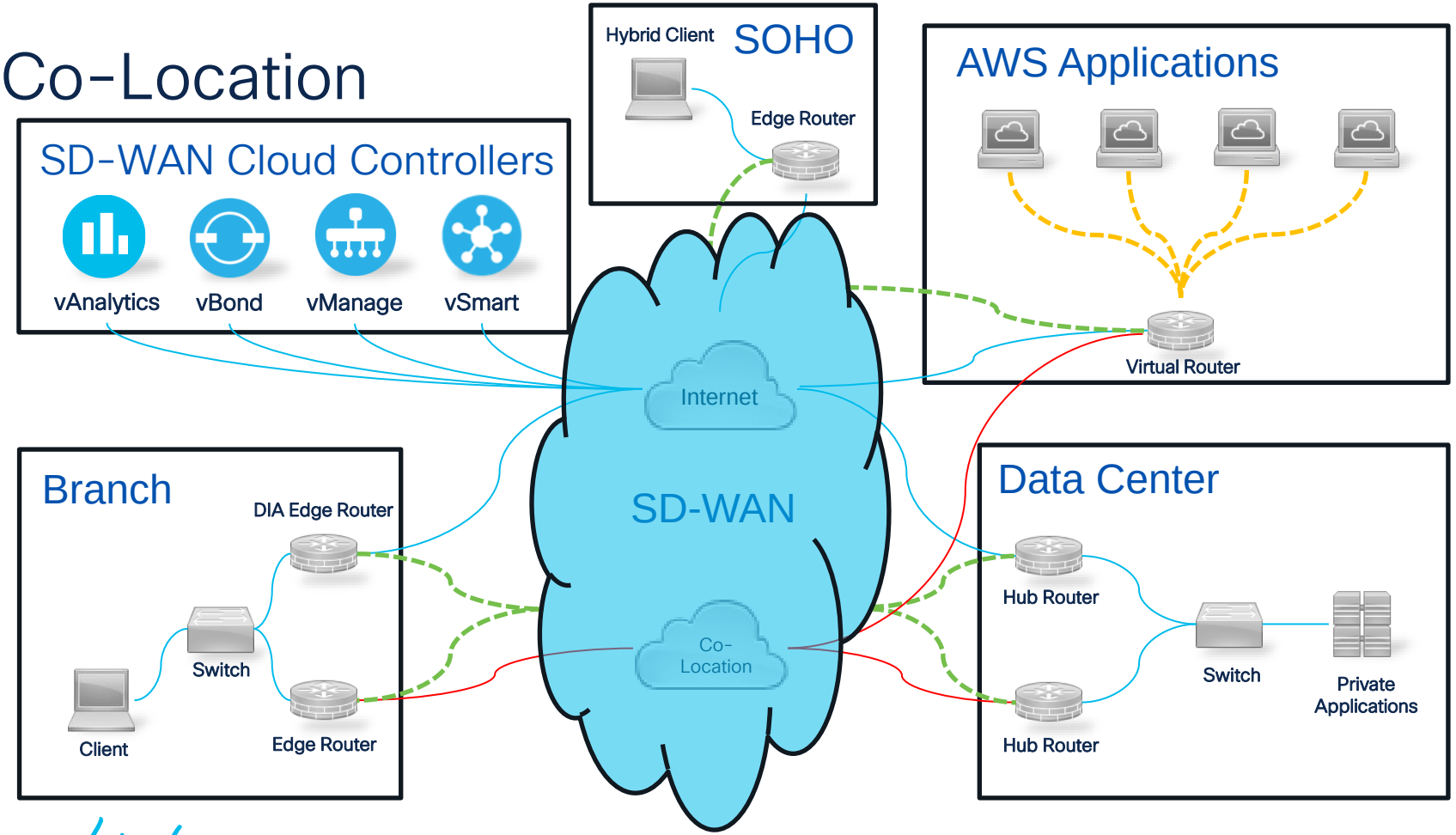
Hybrid Work



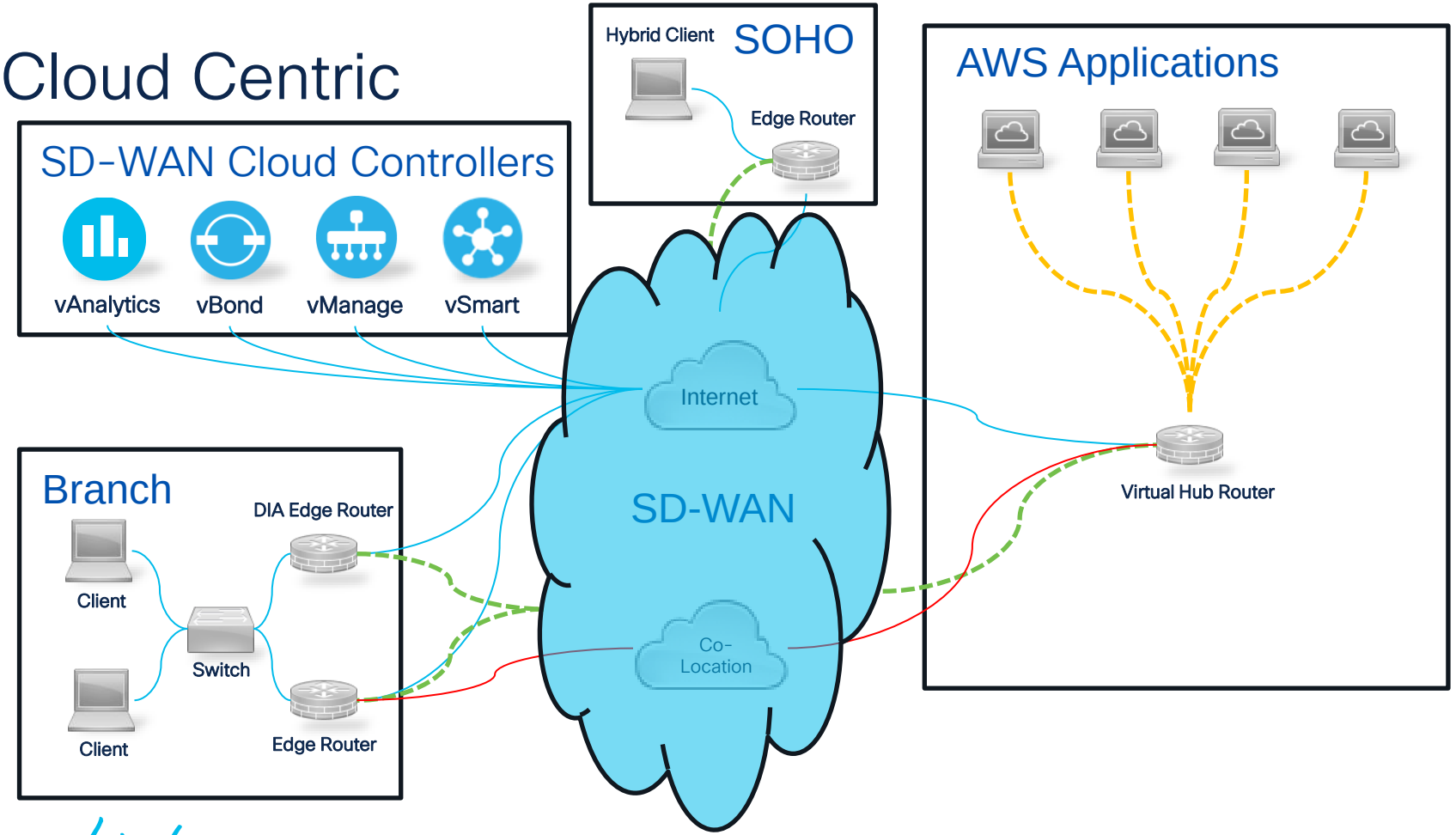
Internet Only



Co-Location

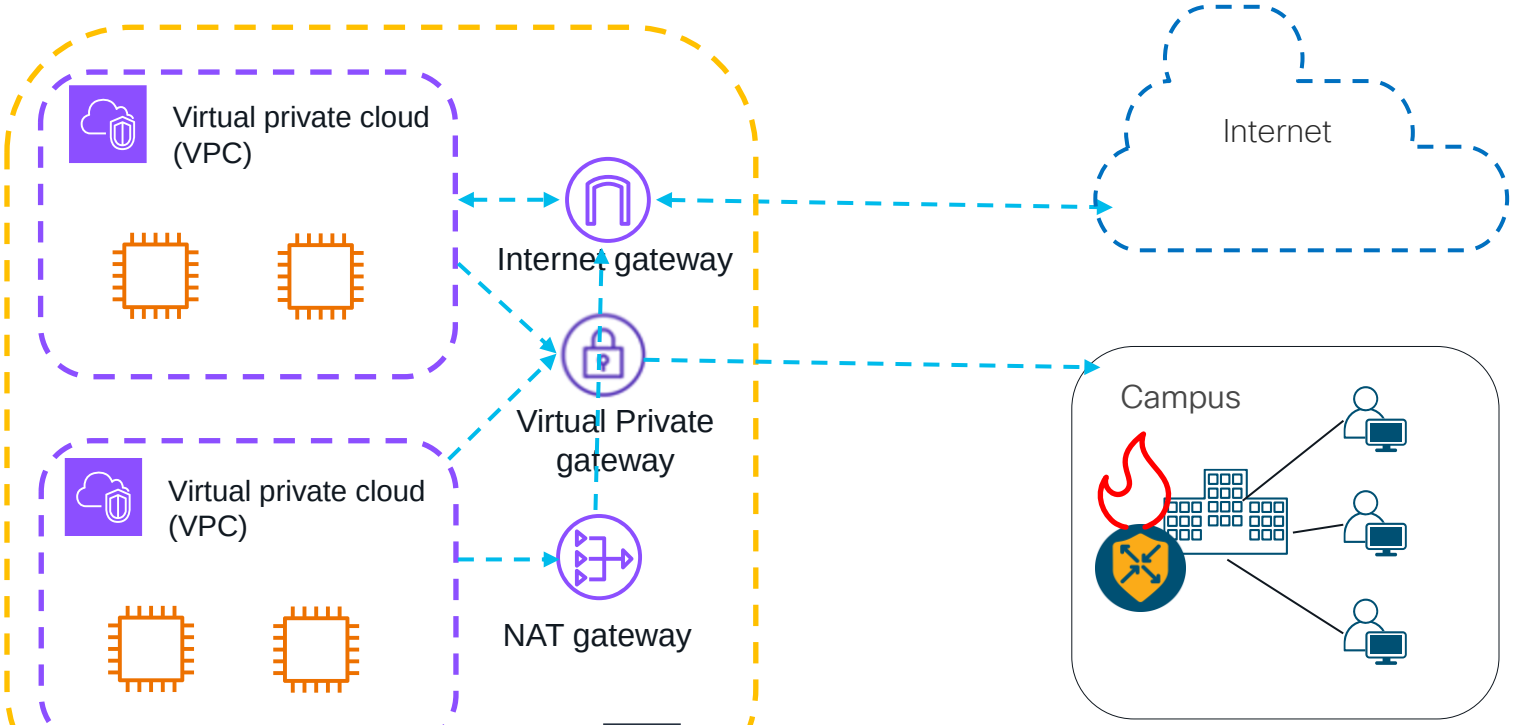


Cloud Centric

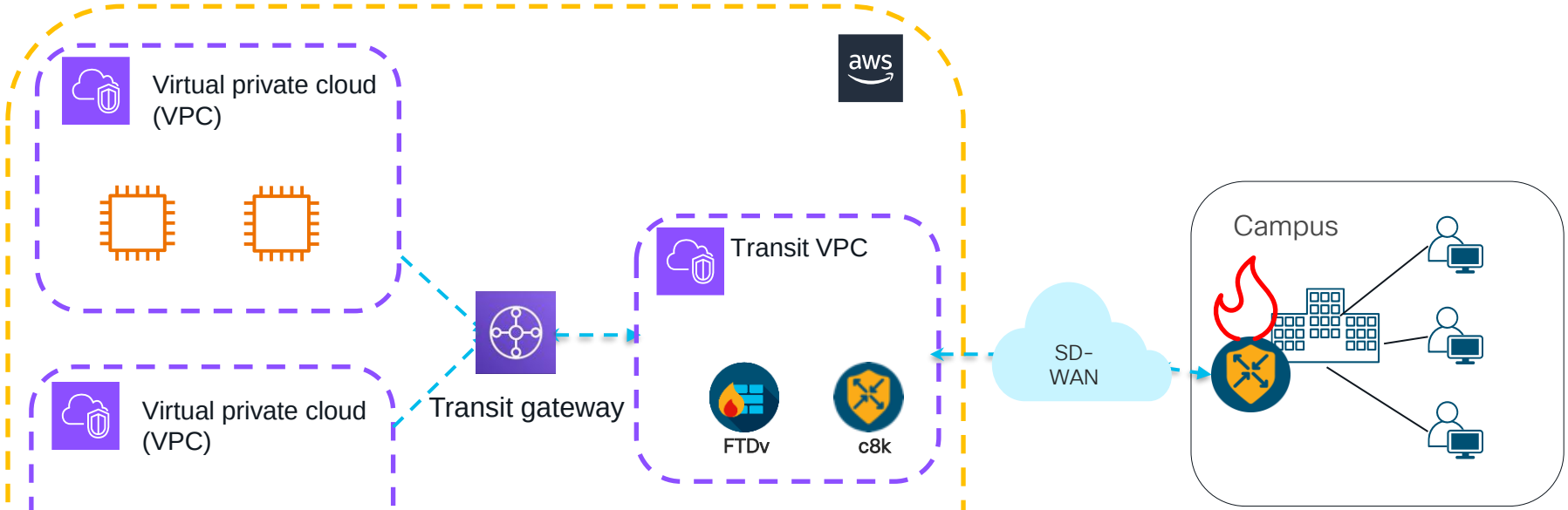


Cloud Networking Recap

AWS Networking Recap



AWS Networking Recap



Comparison of services

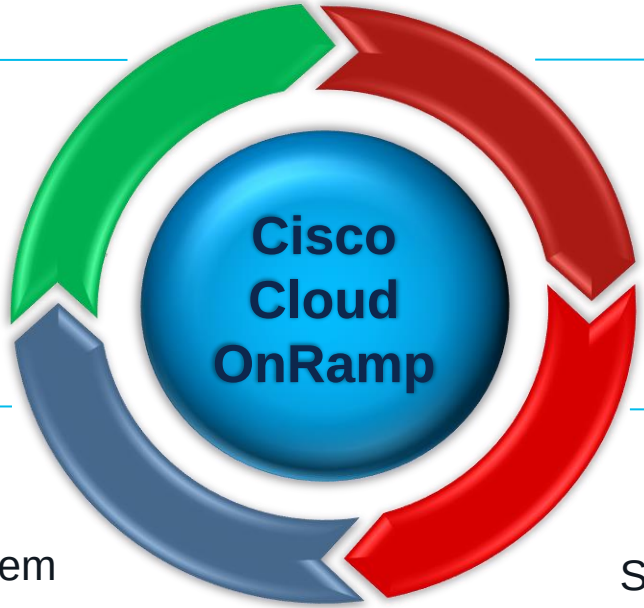
Criteria	VPC peering	Transit VPC	Transit Gateway
Architecture	Full mesh	VPN-based hub-and-spoke	Attachments-based hub-and-spoke. Can be peered with other TGWs.
Complexity	Increases with VPC count	Customer needs to maintain EC2 instance/HA	AWS-managed service; increases with Transit Gateway count
Scale	125 active Peers/VPC	Depends on virtual router/EC2	5000 attachments per Region
Segmentation	Security groups	Customer managed	Transit Gateway route tables
Latency	Lowest	VPN encryption overhead	Additional Transit Gateway hop
Bandwidth limit	No limit	Subject to EC2 instance bandwidth limits based on size/family	Up to 50 Gbps (burst)/attachment
Cost	Data transfer	EC2 hourly cost, VPN tunnels cost and data transfer	Hourly per attachment, data processing, and data transfer

Cloud On Ramp to AWS

Cisco Cloud OnRamp solves your cloud problems

Automation

Site-to-Site, Site-to-Cloud, Cloud-to-Cloud



Operations

Cloud Audit, Monitoring, Prediction and Recommendation

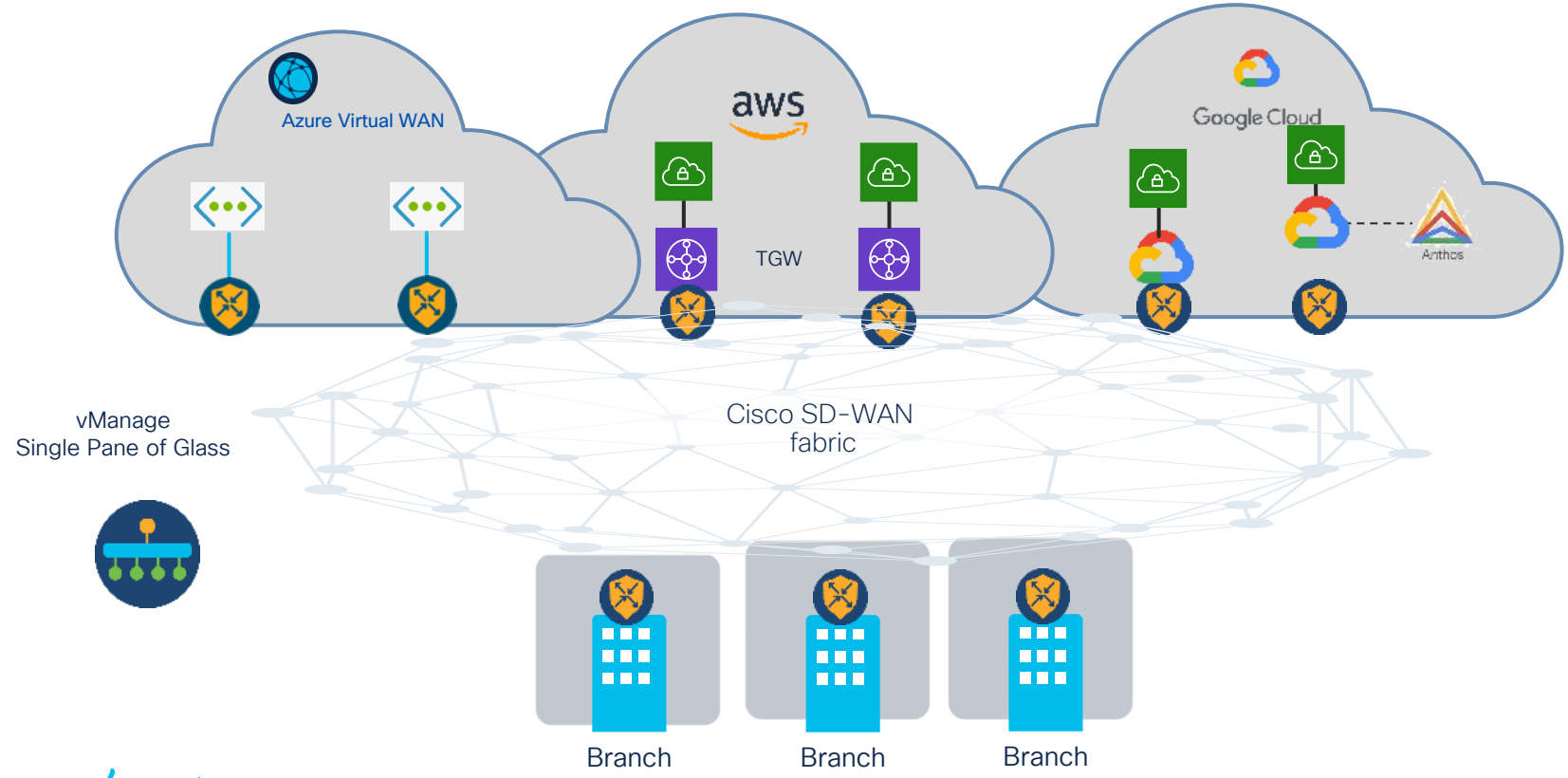
Security

Cloud Security, SIG, On-Prem

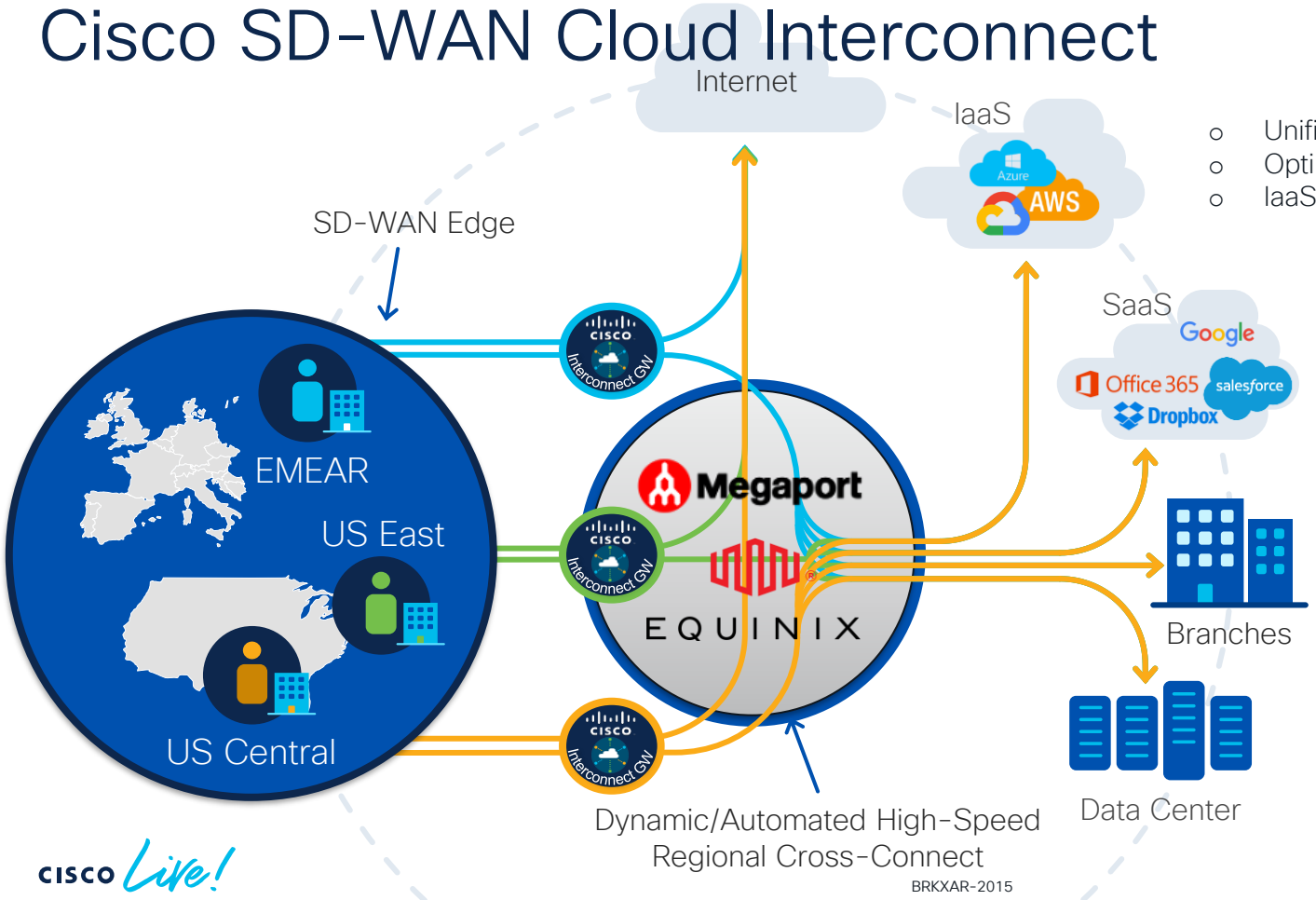
App Performance

Service Directory Integration, Mid-Mile Optimization

Cloud OnRamp for Multicloud



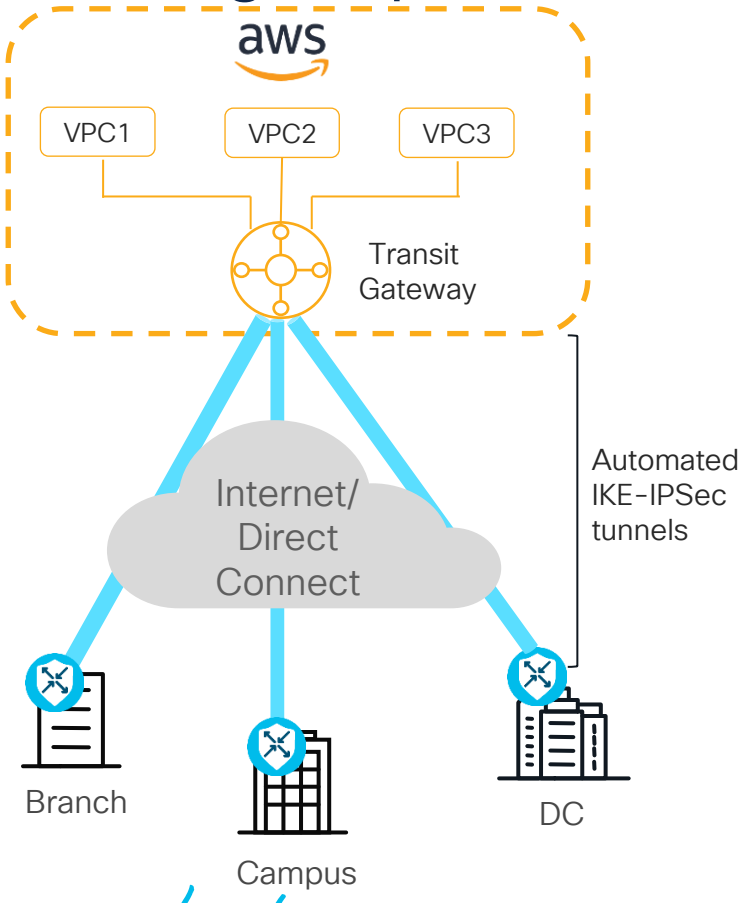
Cisco SD-WAN Cloud Interconnect



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

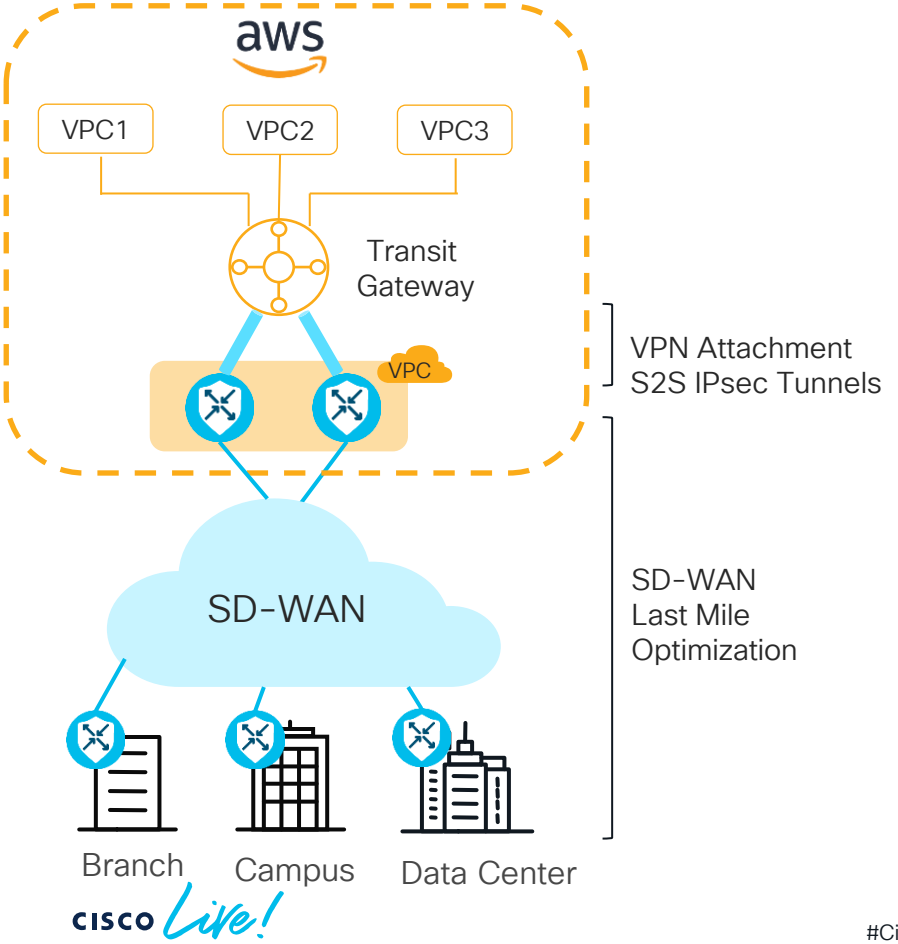
AWS -Site to Cloud – Connectivity Deep dive

Design Option#1 – Branch Connect Model



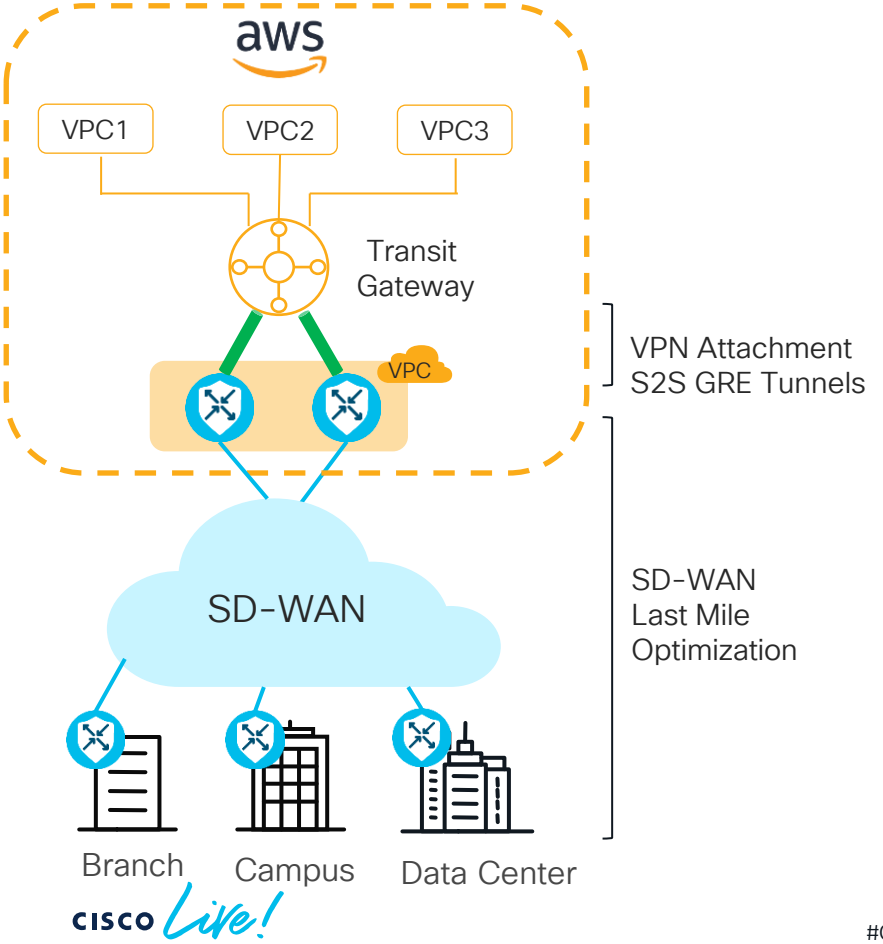
- Automated Provisioning
- Lower Costs
- More Bandwidth per Site
- HA Support
- Tunnel Monitoring Required

Design Option#2 – VPN (IPSec) based Model



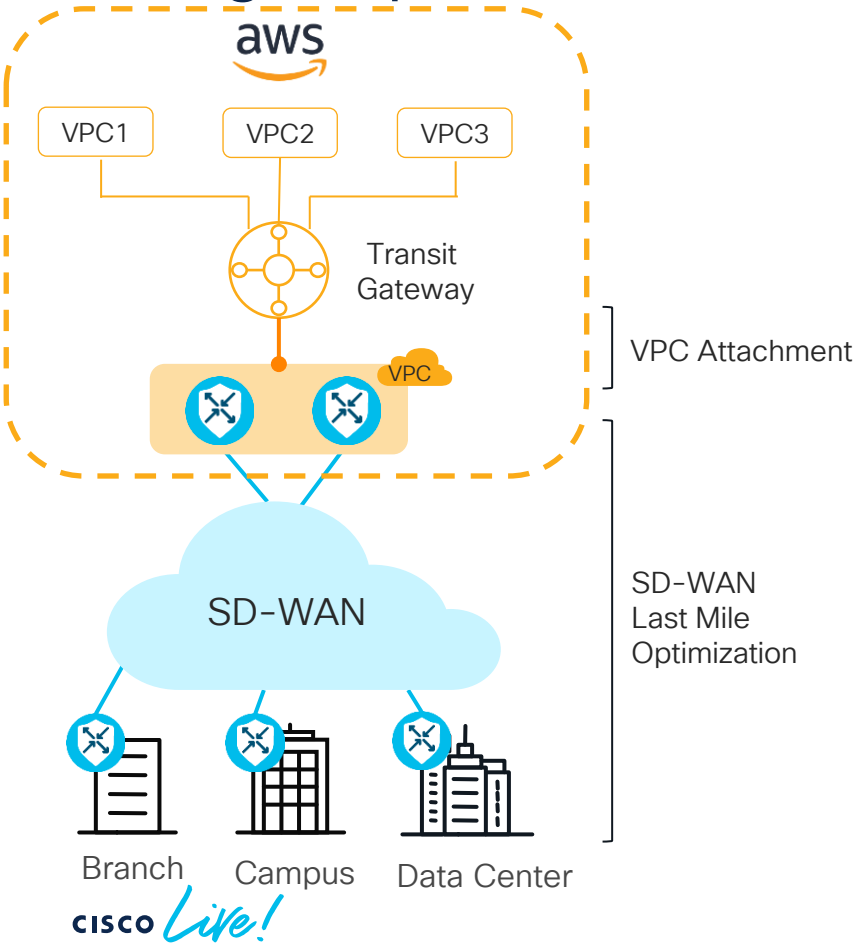
- vManage Automation
- Centralized Policy
- Network Segmentation
- Lower OpEx
- SD-WAN for HA and Scaling

Design Option#3 – GRE Connect based Model



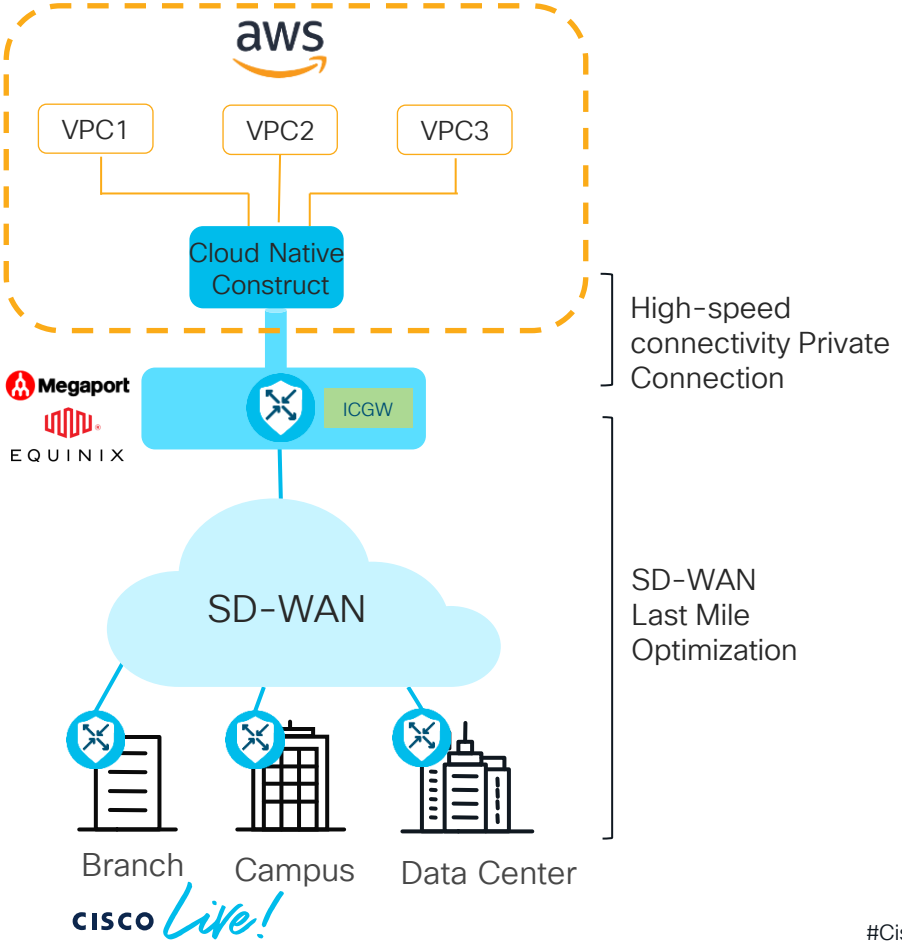
- vManage Automation
- Centralized Policy
- Network Segmentation
- Lower OpEx
- SD-WAN for HA and Scaling
- Higher Scaling

Design Option#4 – VPC Attachment Model



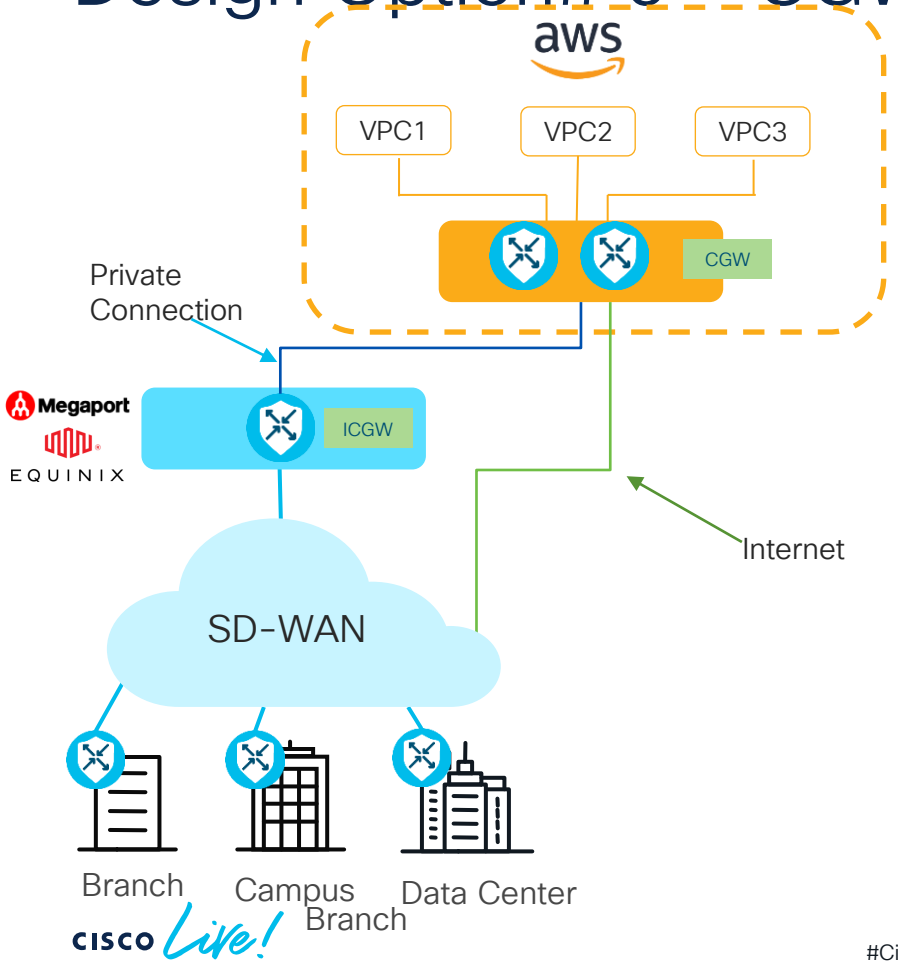
- Higher Bandwidth for Single Link
- Lower Cost
- Static Routing Only
- Manual Configuration

Design Option# 5 – CoLo Interconnect Model



- High Speed Path to Cloud
- Scalability
- Service Chaining
- Optimized Routing
- SD-WAN for HA
- Encryption from Branch to Co-Lo

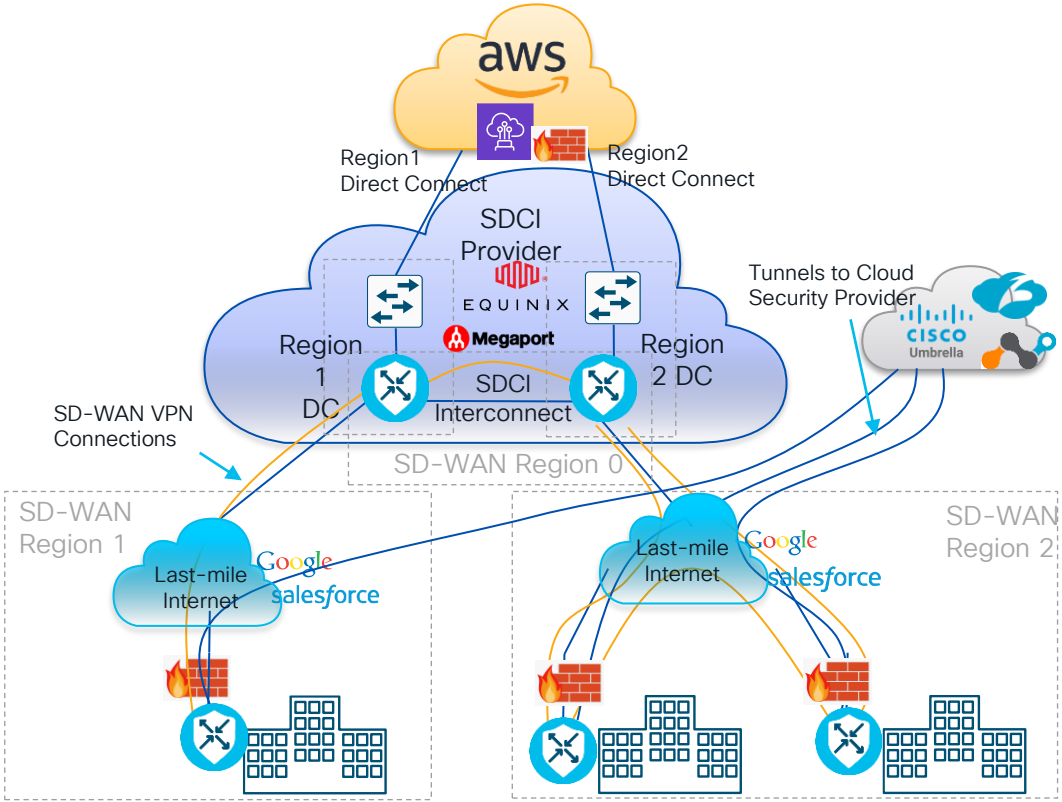
Design Option# 6 – CGW in SDCI Model



- End-to-end Encryption
- Multipath Support
- SD-WAN Everywhere

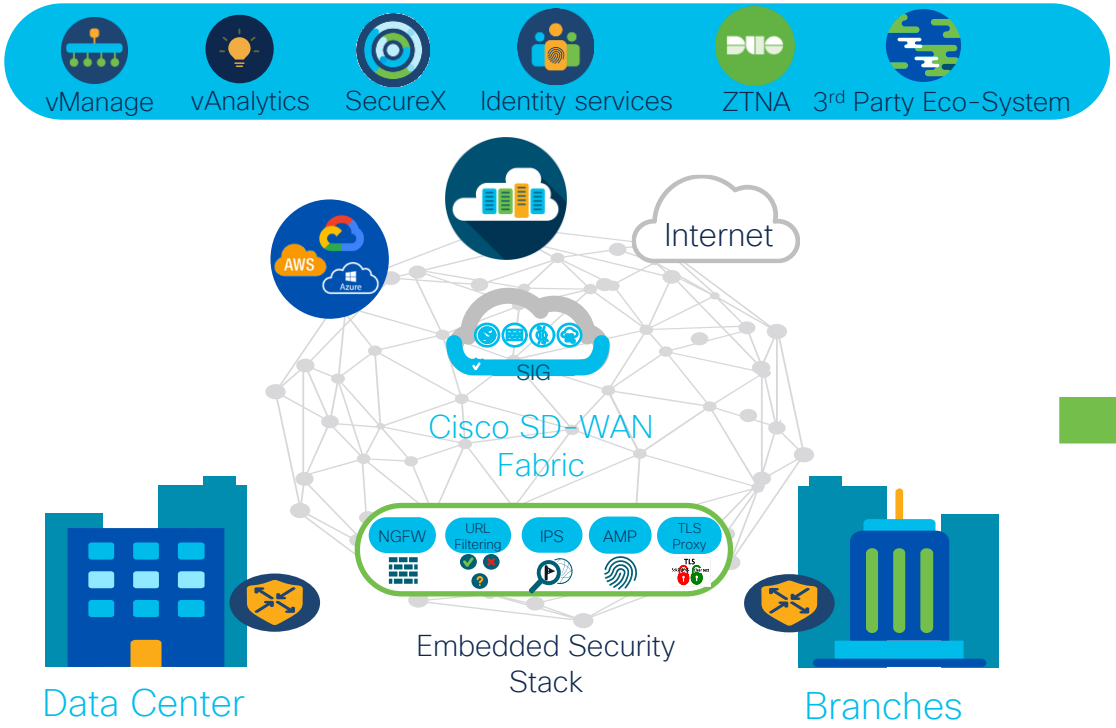
Cloud as a Transport

Cloud as a Transport



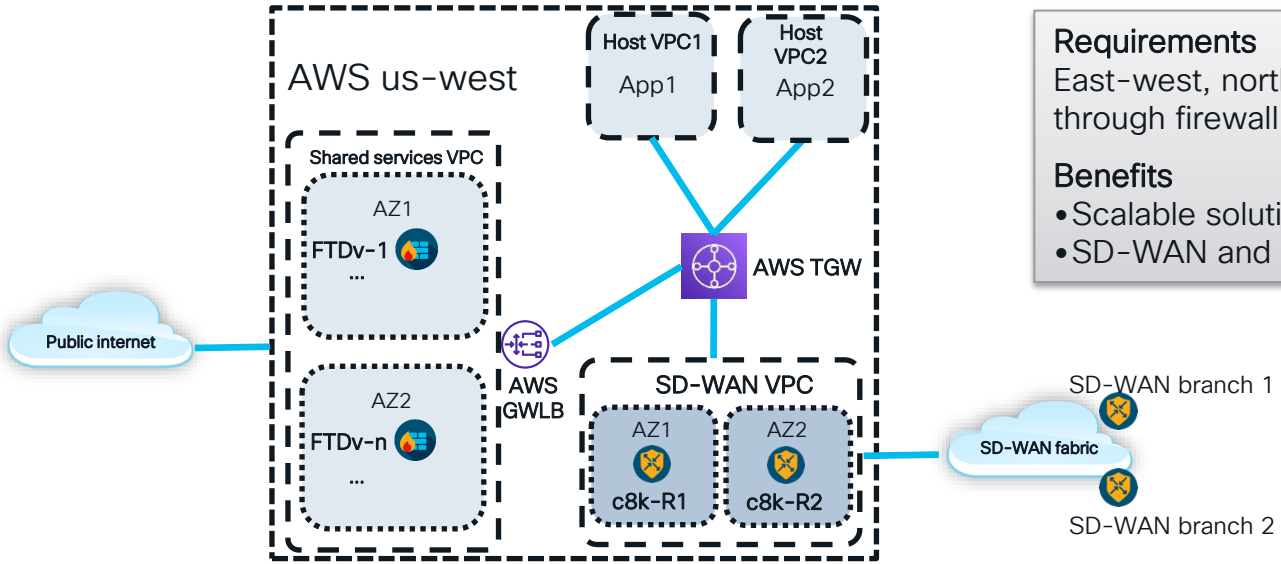
Security

SD-WAN Security – Overview



- SASE
- Identity Zero Trust
- Unified Policy Management
- Distributed Security Enforcement
- Secure Internet Gateway
- Visibility & Reporting

AWS: Centralized Firewall Design



Requirements

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

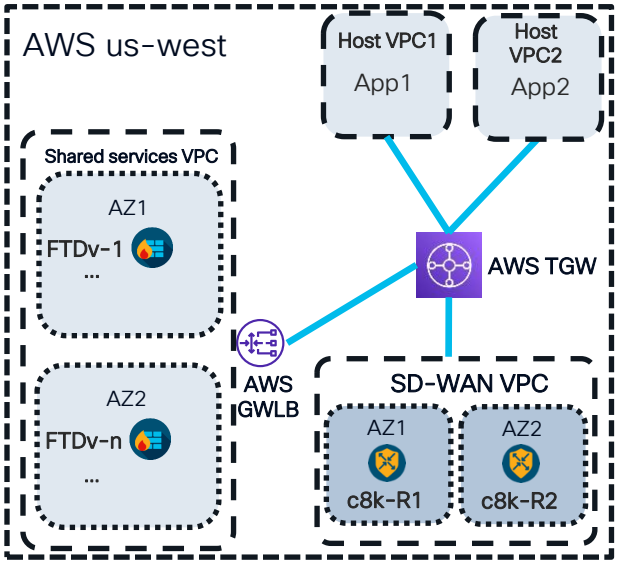
Benefits

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

Full Details: https://youtu.be/LHdW_0C3Y6E?t=351

GitHub Repo: https://github.com/CiscoDevNet/sdwan-cor-labinfra

Packet flow: Simplified



From Host VPC to SD-WAN
Host VPC ➔ AWS TGW ➔ GWLB ➔ FTDv ➔ TGW ➔ SD-WAN

Returning traffic
SD-WAN ➔ AWS TGW ➔ GWLB ➔ FTDv ➔ TGW ➔ Host VPC

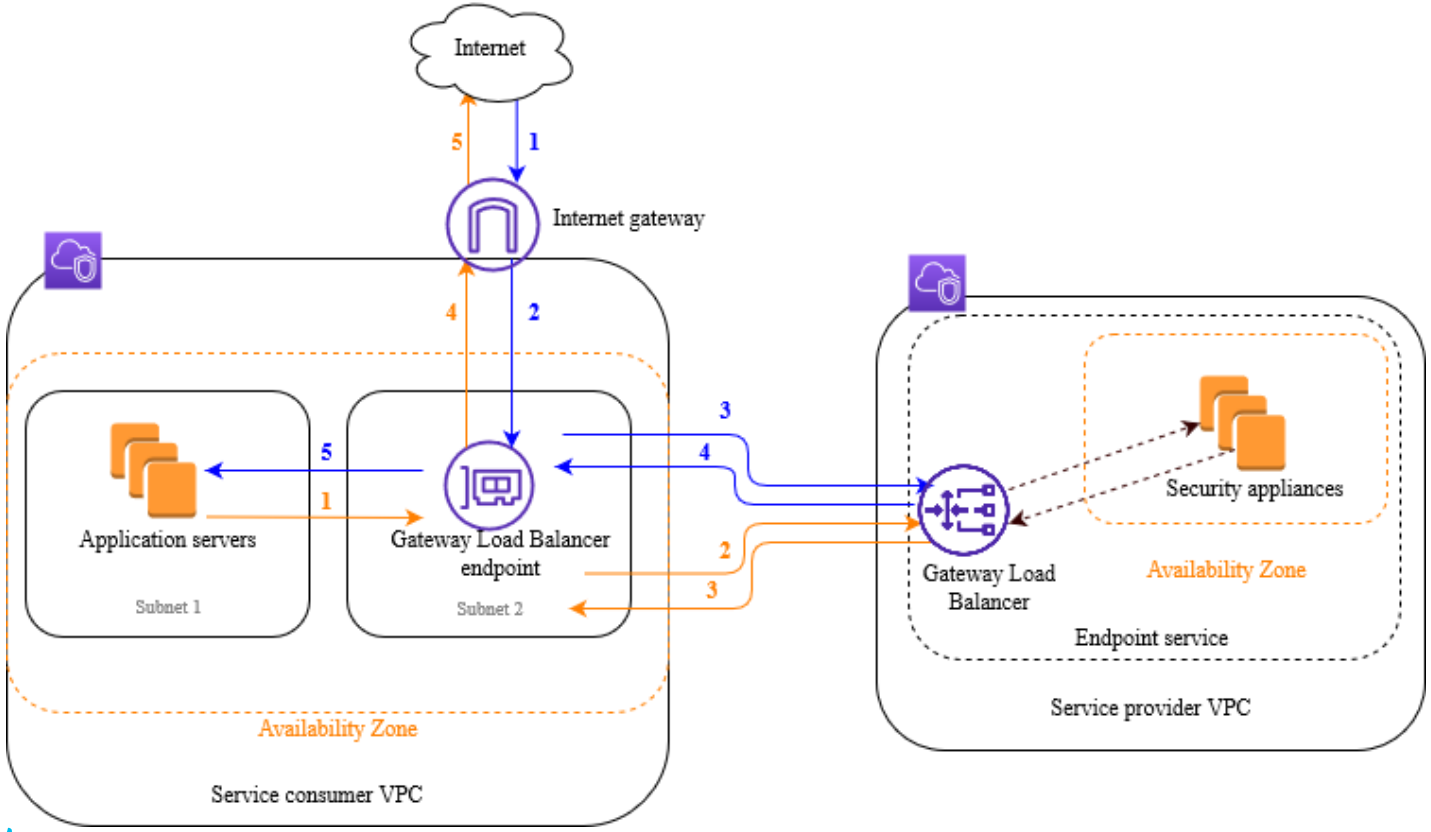
GENEVE protocol for load balancing between GWLB and FTDv

Appliance mode is required for symmetric routing

FTDv = Secure Firewall Threat Defense Virtual (aka FTDv / NGFWv)
GWLB = AWS Gateway Load Balancer

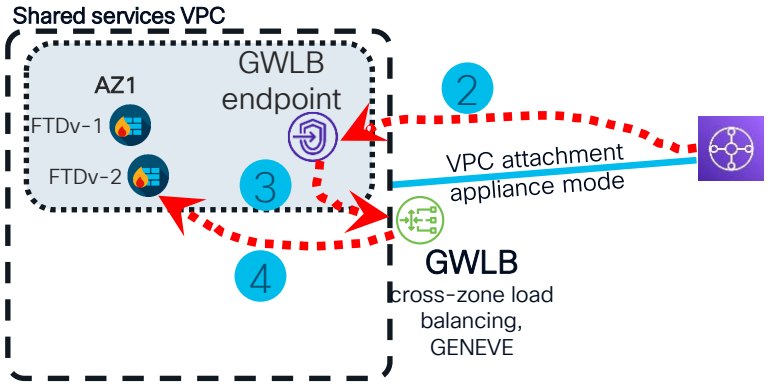
Geneve = Generic Network Virtualization Encapsulation
AZ = Availability Zone (AWS data center)

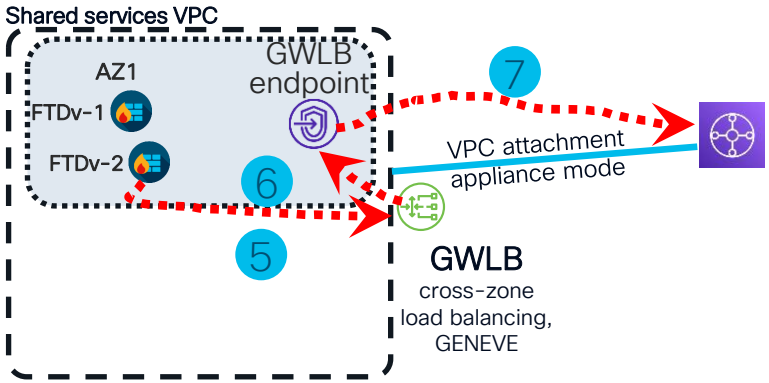
AWS Gateway Load Balancer Explained



Packet flow: Details for shared services VPC

For Your Reference





Step 2: TGW routes to GWLB endpoint – shared services route table

10.102.0.0/16	local		
0.0.0.0/0	vpce-XYZ	FW-Endpoint-Service-AZ1	10.102.3.91

Step 3: GWLB endpoint routes traffic to GWLB using AWS PrivateLink

Step 4: GWLB routes traffic to a firewall using GENEVE

Target Group: FW-Target-Group-Geneve with 4 firewalls:

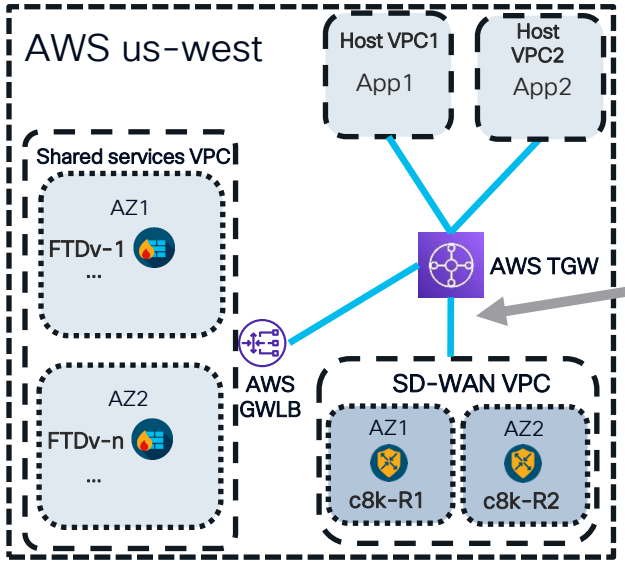
10.102.3.174	MC-FTD-IFT-1	6081	us-west-AZ1
10.102.13.67	MC-FTD-IFT-2	6081	us-west-AZ1
...			

Step 5: Firewall decapsulates GENEVE, inspects the packet, re-encaps and sends it back to GWLB

Step 6: GWLB removes GENEVE header and forwards packet to the appropriate GWLB endpoint

Step 7: GWLB endpoint sends packet to TGW

Connecting SD-WAN



- VPN or connect attachment for SD-WAN VPC
- BGP between AWS TGW and SD-WAN routers
- Cisco Catalyst 8000V as SD-WAN router
- Multi-Region via TGW Peering, AWS Cloud WAN support in near future
- Automation: GitHub repo SD-WAN CoR LabInfra

Demo

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 Game** for every survey completed.

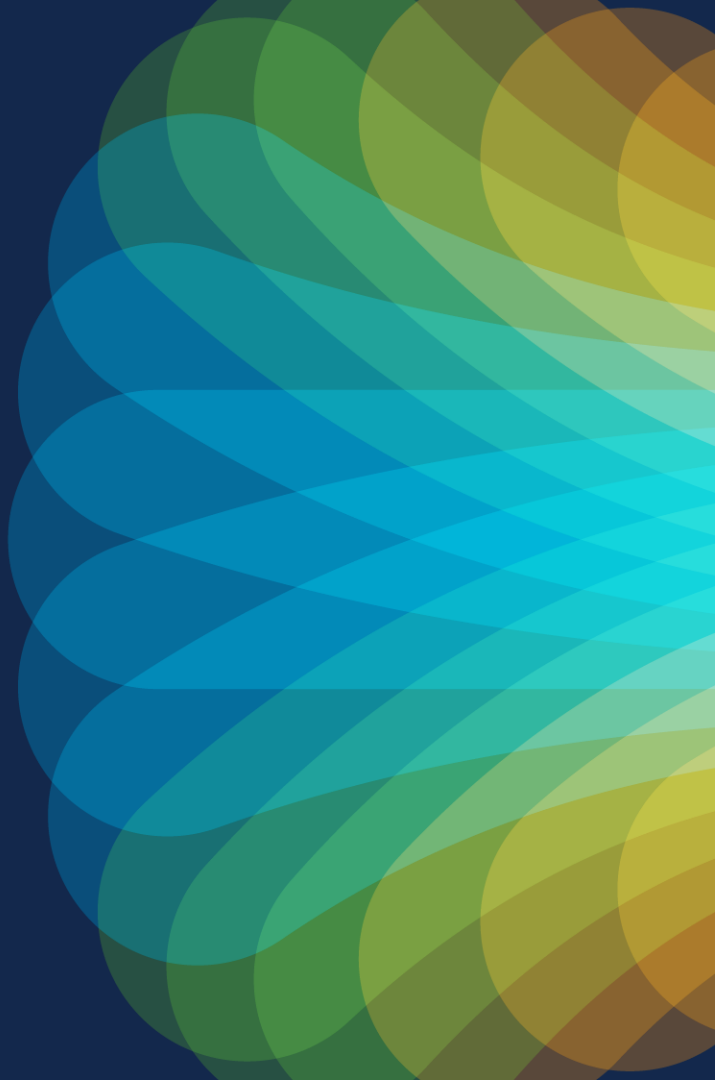
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

The bridge to possible

Thank you



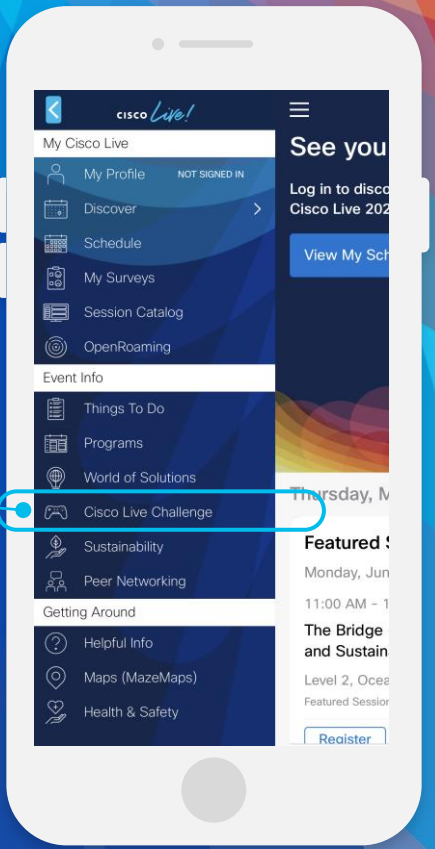
Cisco Live
Challenge

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:




cisco Live!
Let's go
#CiscoLive