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 Live!

#CiscoLive

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXAR-2015

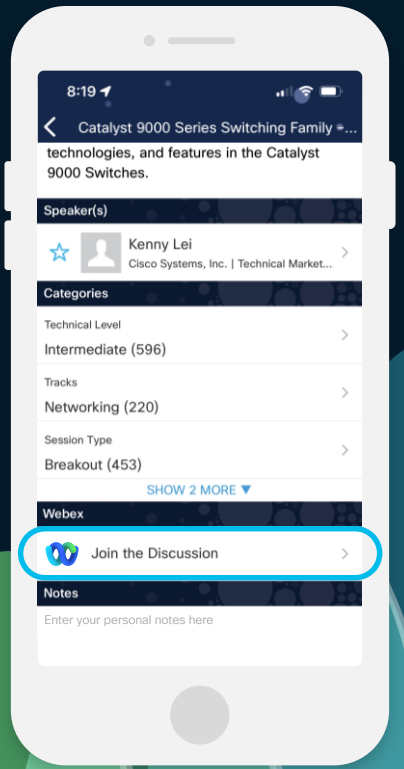
Questions?

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 7, 2024.



Agenda

- Introduction
- SD-WAN Evolution
- Cloud Networking Recap
- Cloud On-Ramp to AWS
- On-prem to Cloud Design Options
- Cloud as a Transport
- Security
- Demo

About Us

Praveen Poojary

Customer Delivery Architect

13 Years in Cisco

#3xCCIE

#CCDE

Lee Sudduth

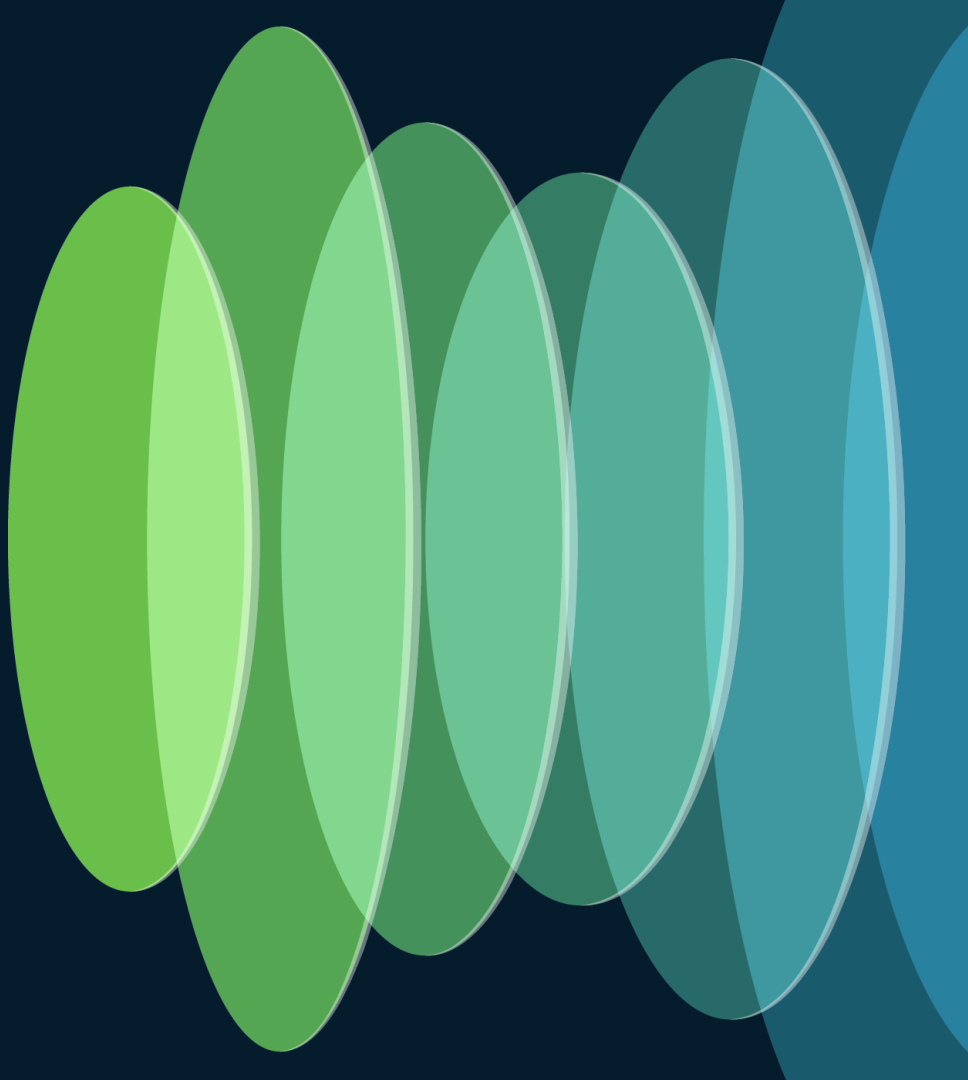
Customer Delivery Architect

24 Years in Cisco

#CCIE

#CCDE

SD-WAN Evolution

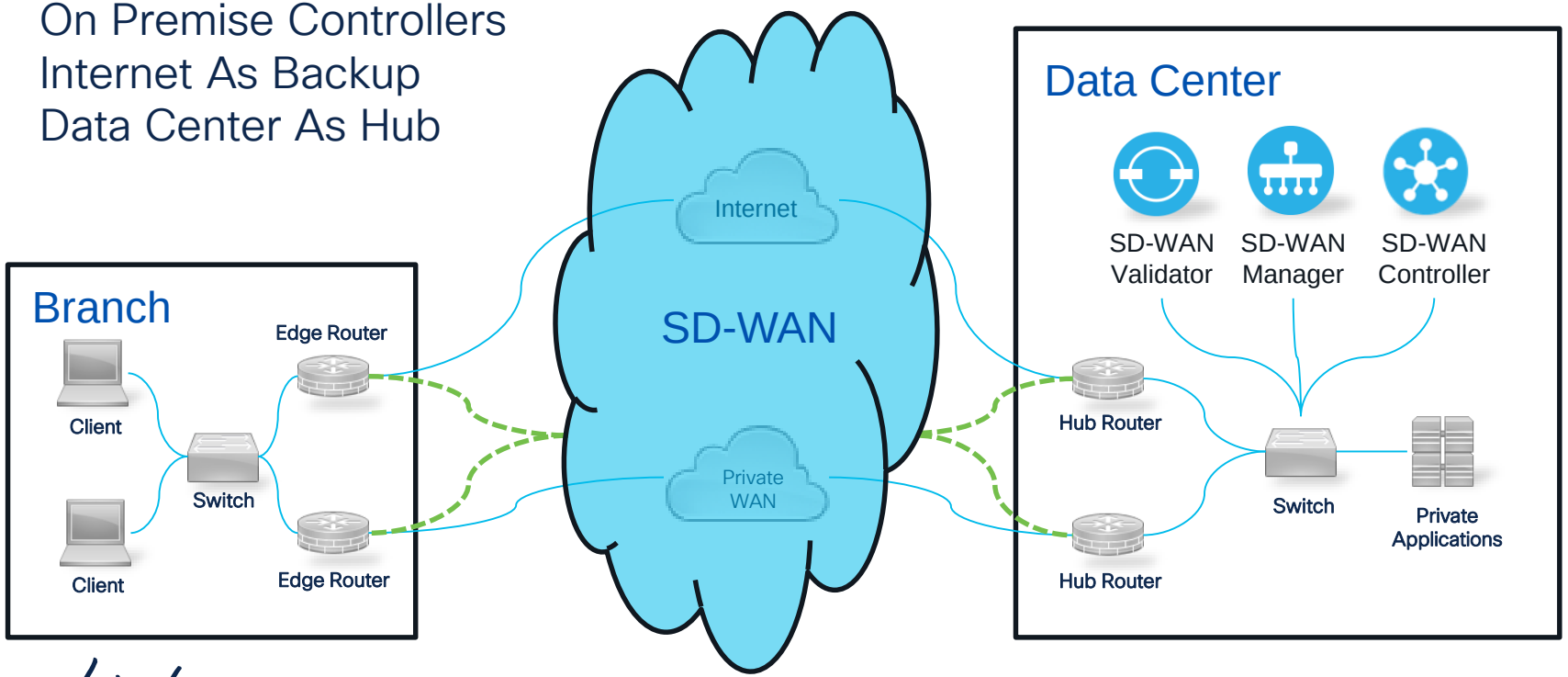


cisco Live!

From Data Center to Cloud

Traditional SD-WAN

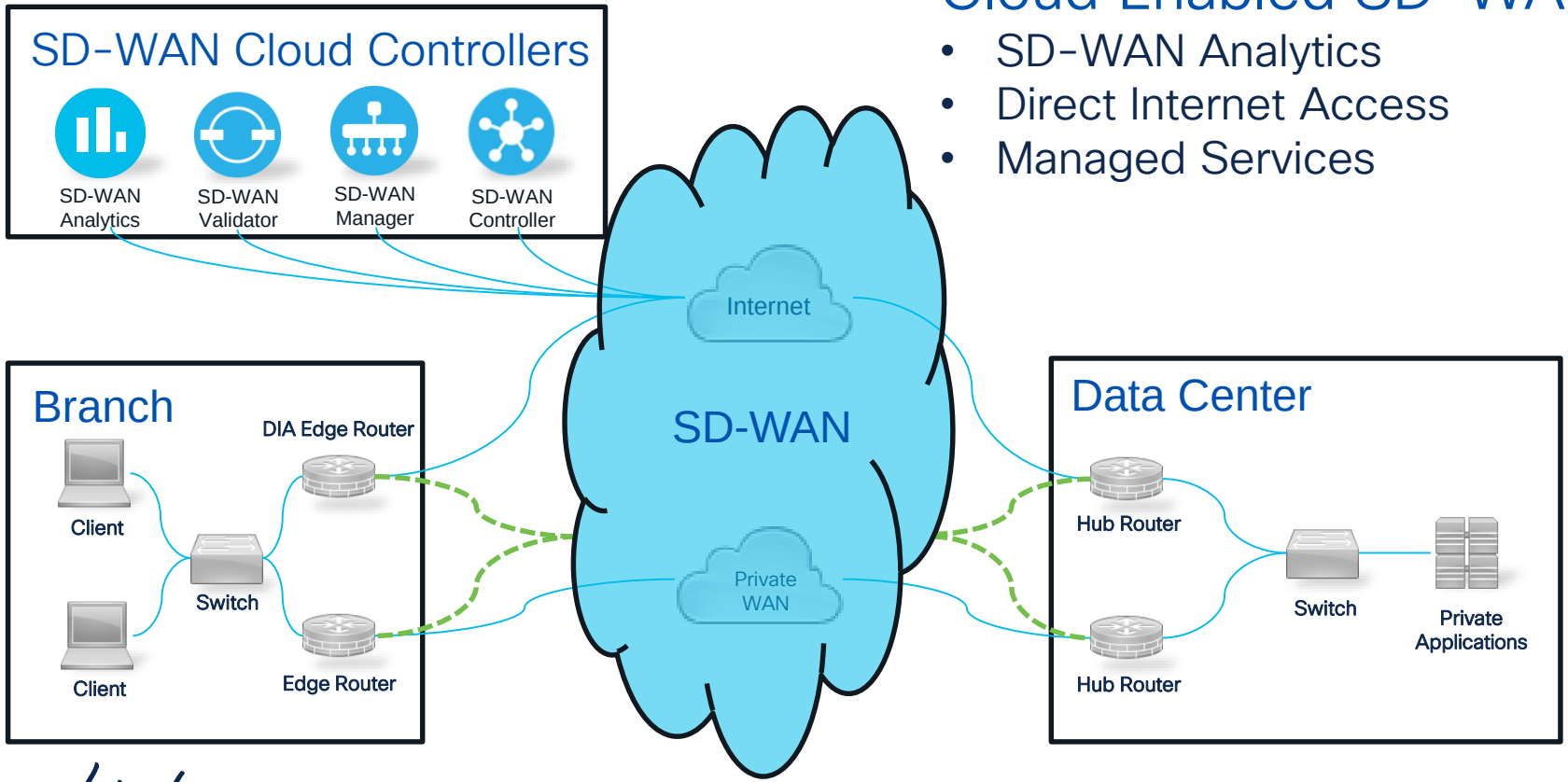
- On Premise Controllers
- Internet As Backup
- Data Center As Hub



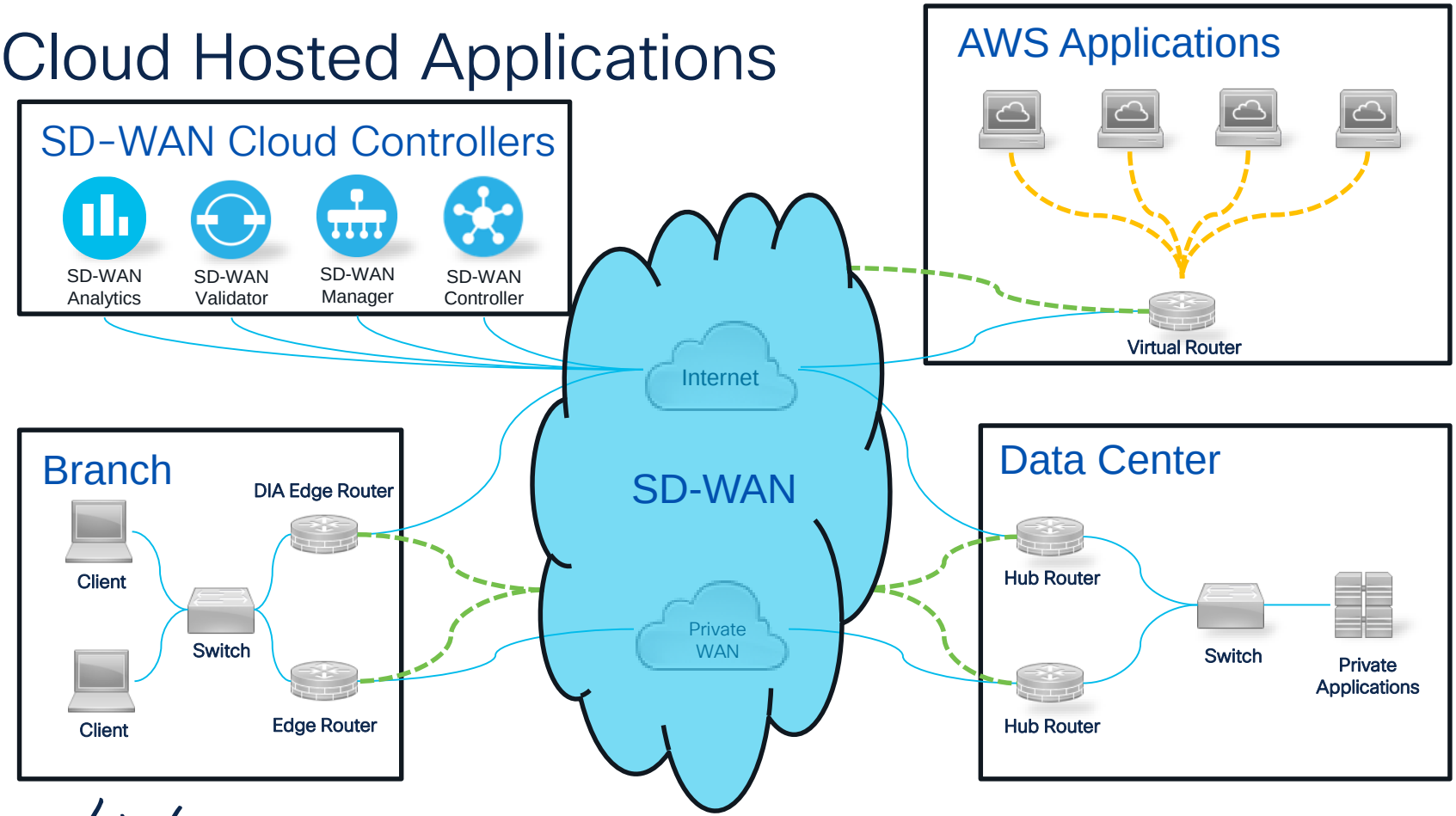
Cloud Hosted Controllers

Cloud Enabled SD-WAN

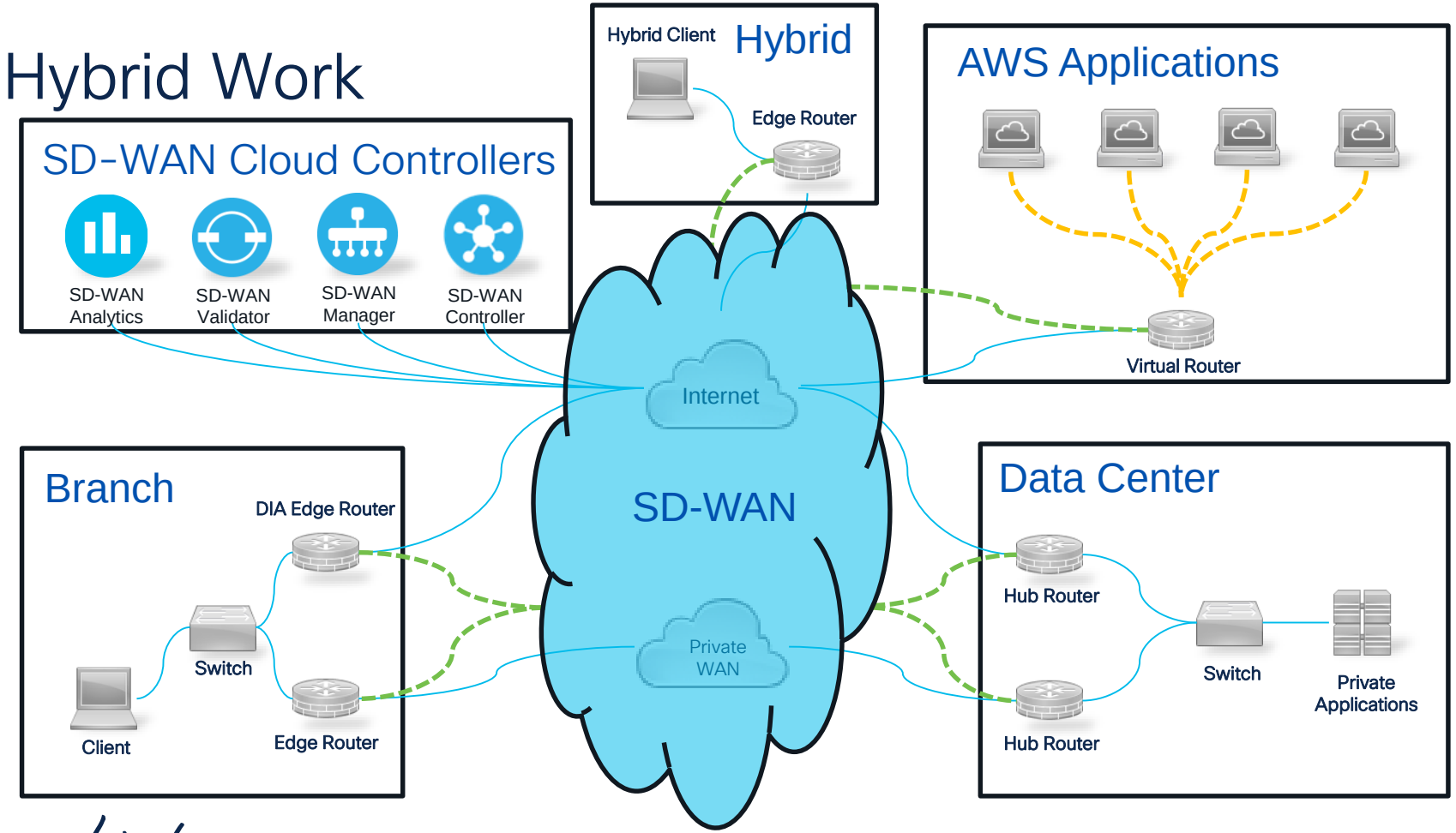
- SD-WAN Analytics
- Direct Internet Access
- Managed Services



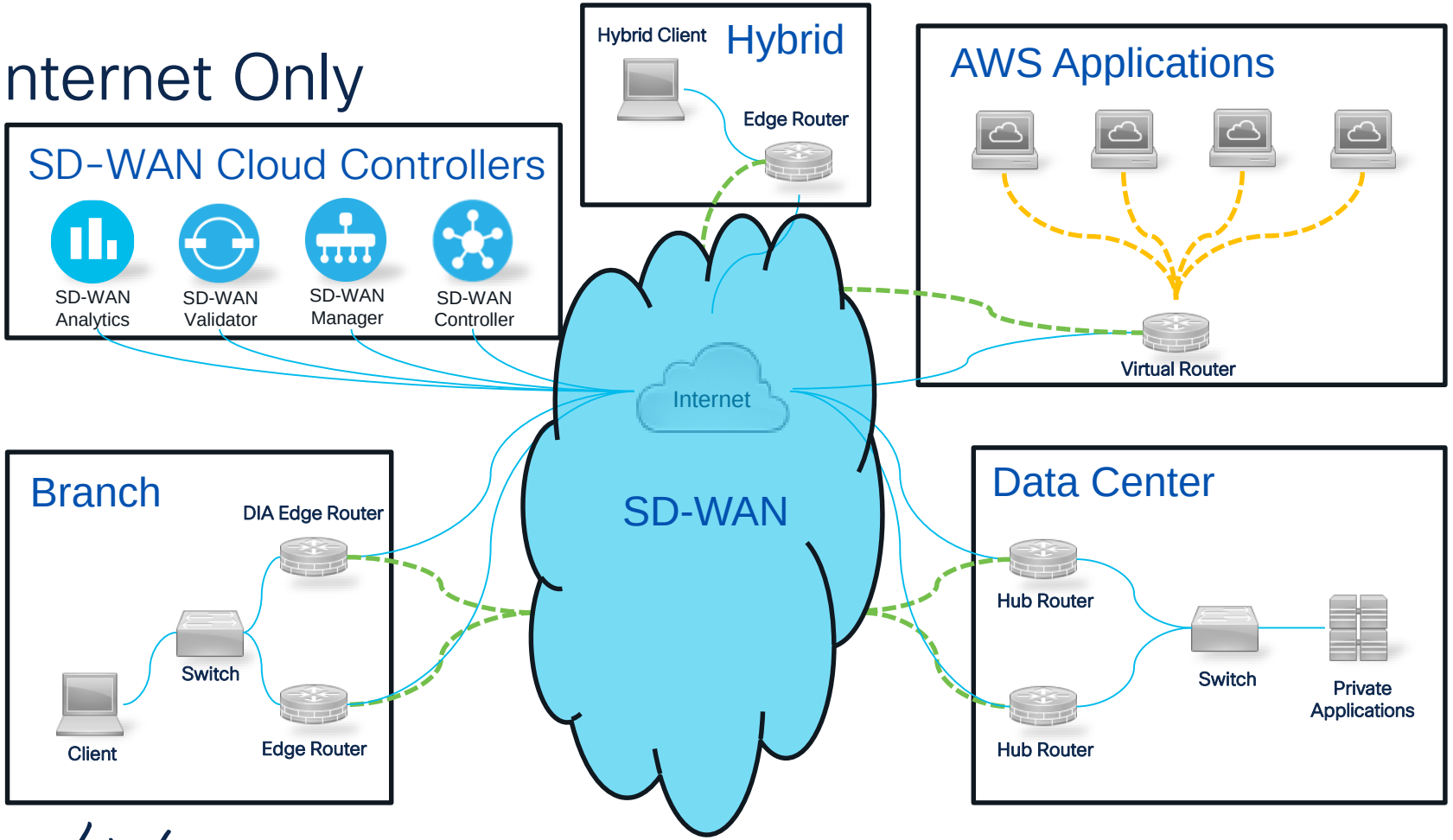
Cloud Hosted Applications



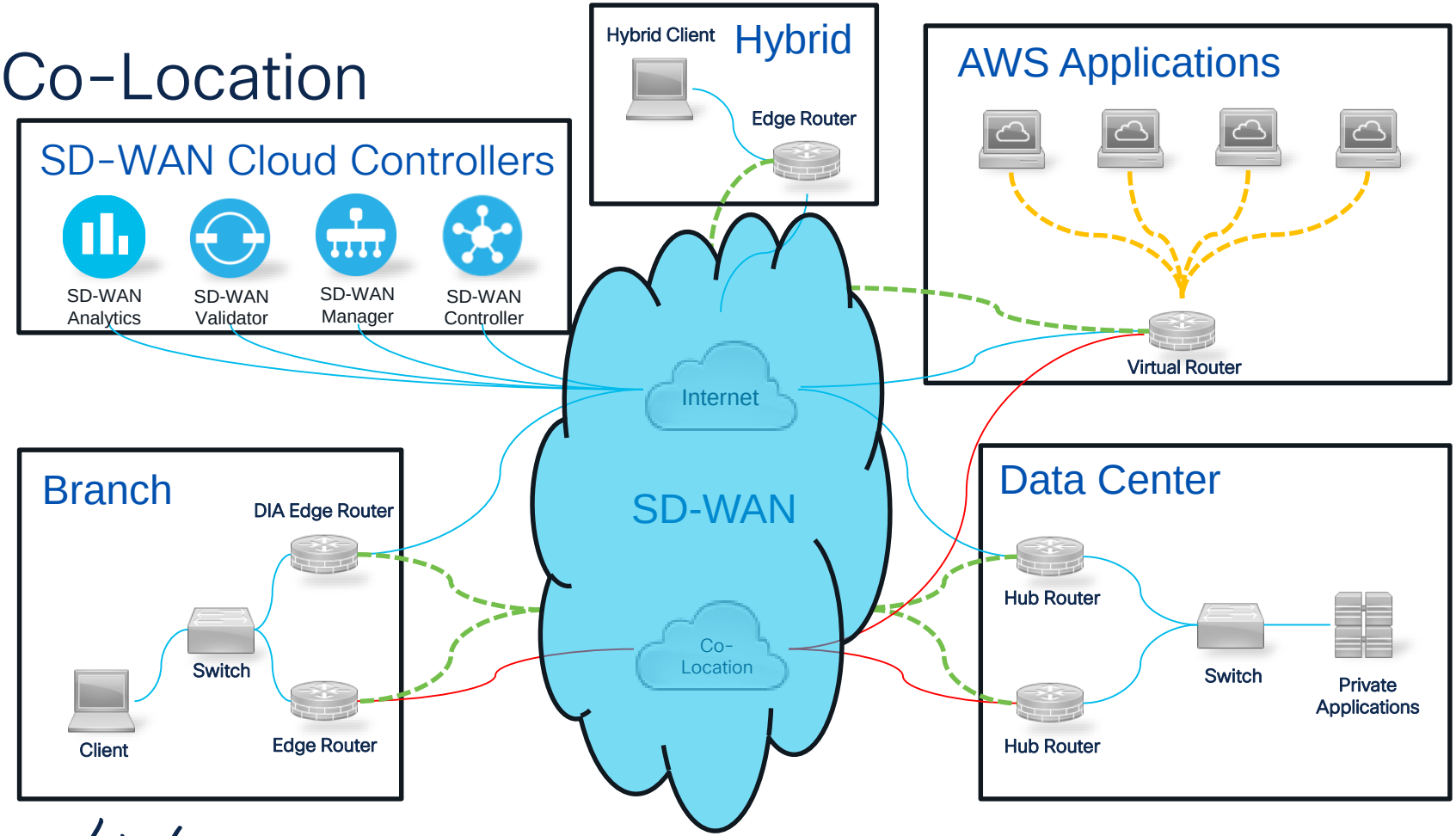
Hybrid Work



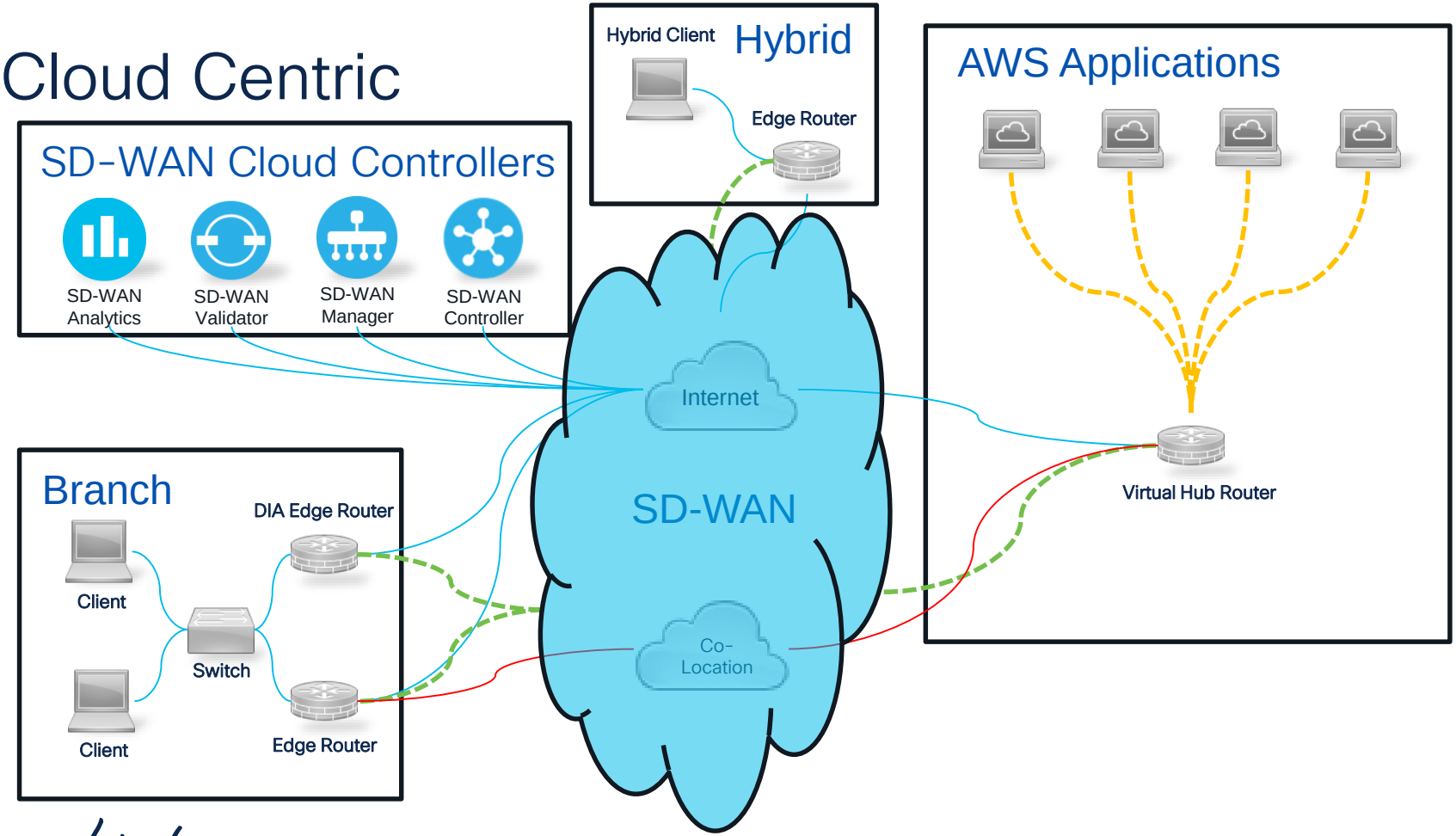
Internet Only



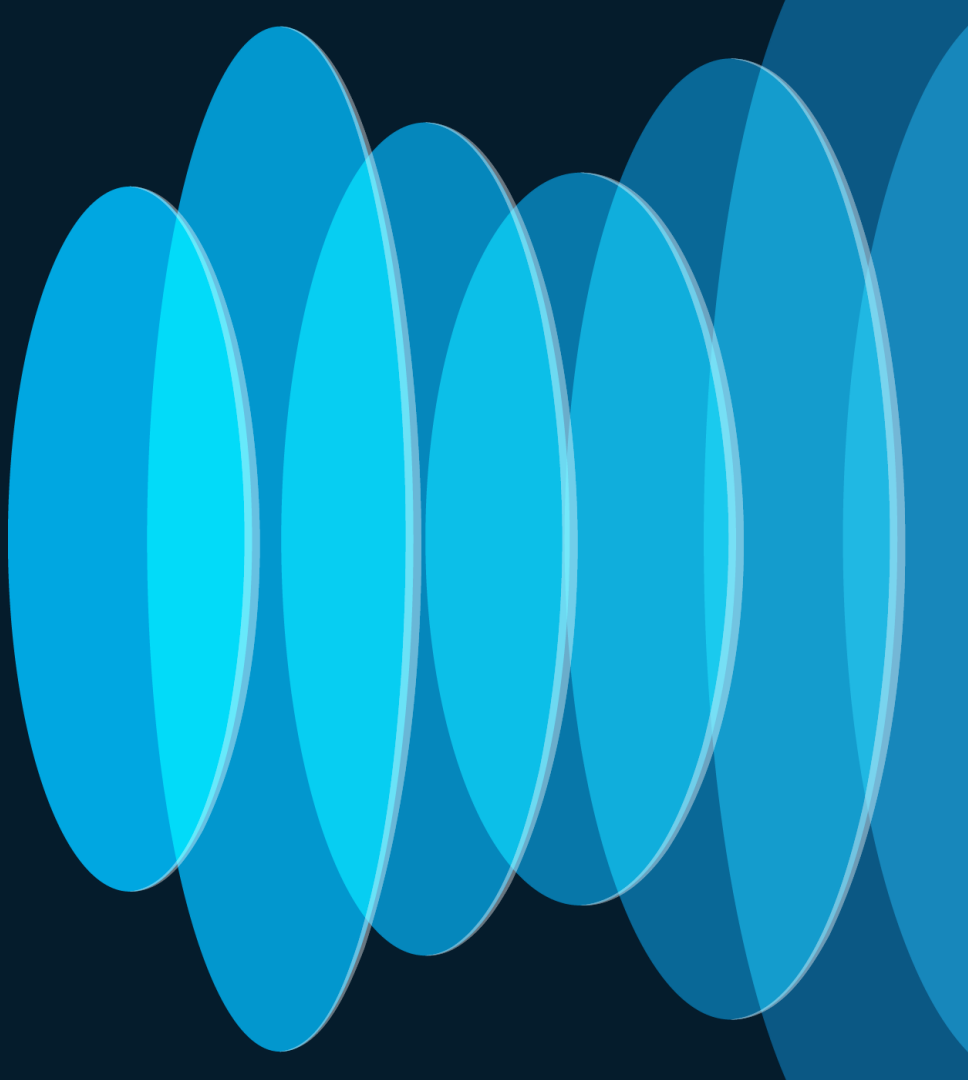
Co-Location



Cloud Centric

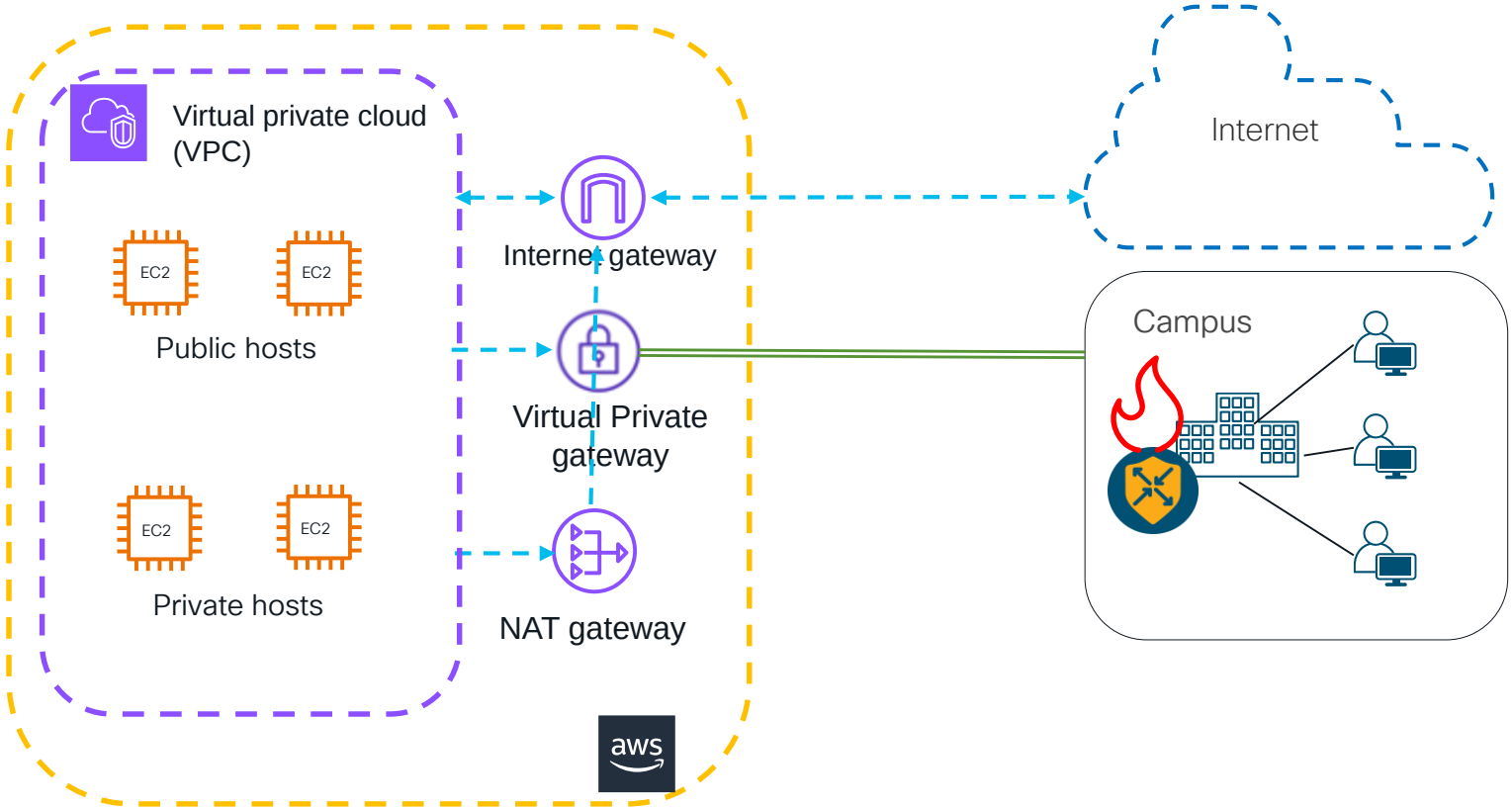


Cloud Networking Recap

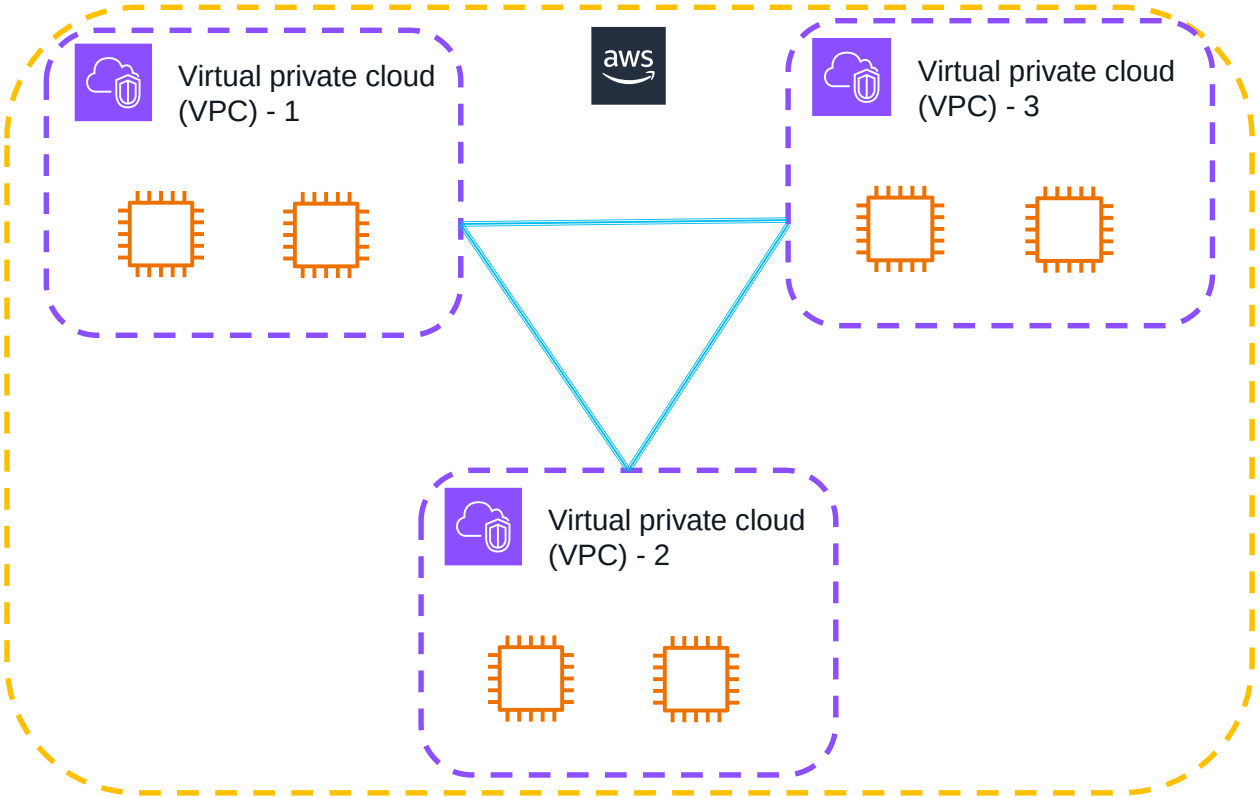


cisco Live!

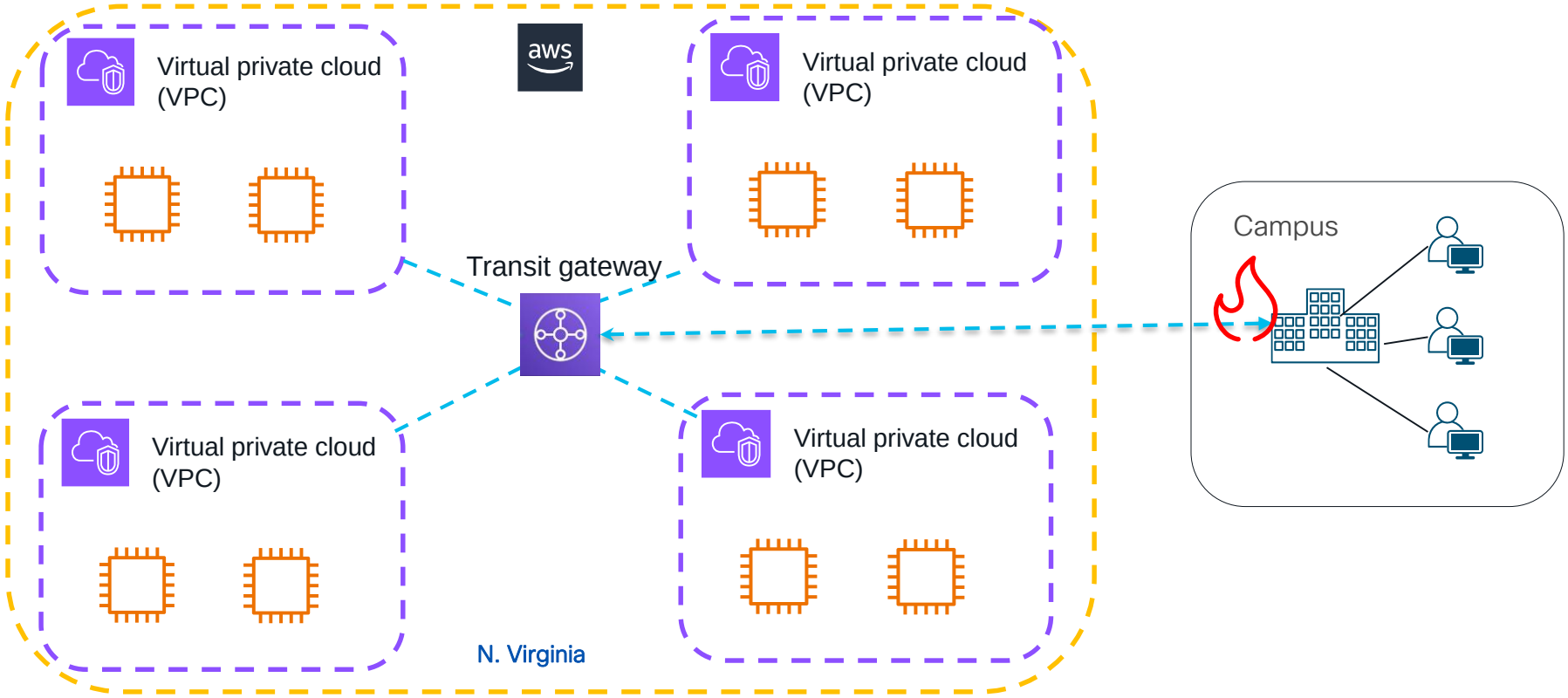
AWS Networking Recap



AWS Networking Recap



AWS Networking Recap

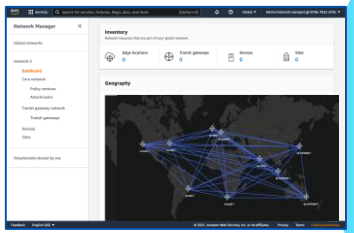


AWS Cloud WAN

Global Topology Dashboard

Simplified deployment

Policy and Configuration Control



AWS Network Manager

Monitoring using Network Manager + CloudWatch

Core Network Policy

VPC

VPC

Development

Test

Production

Shared Services

N. Virginia

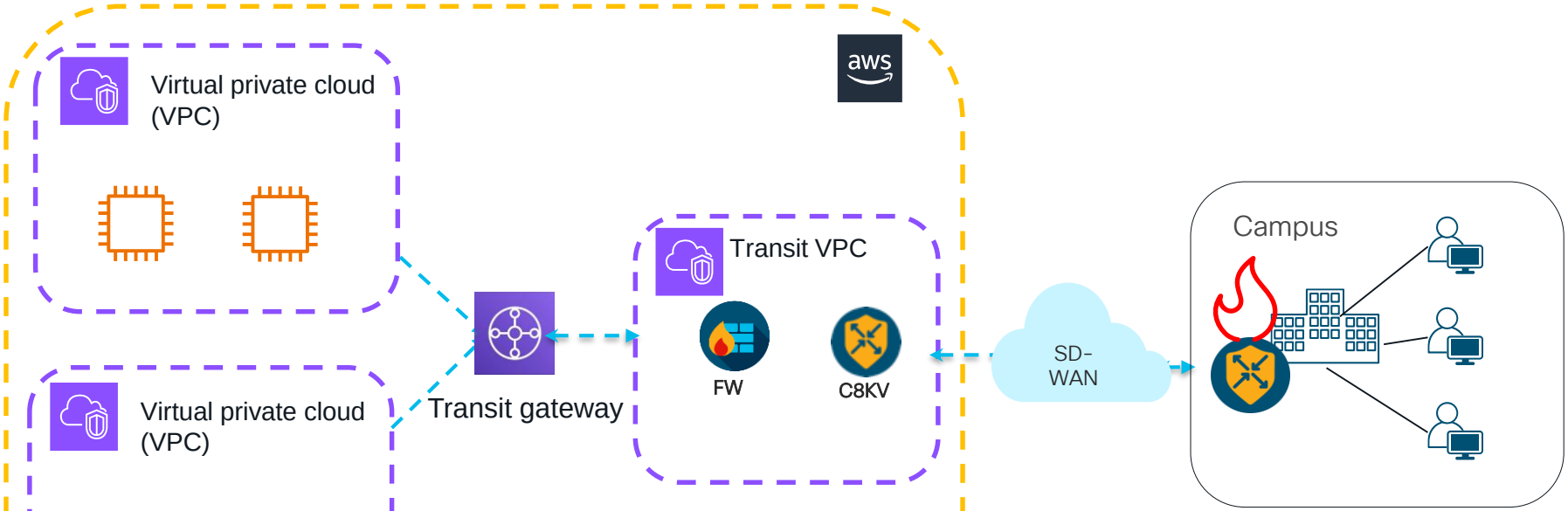
TGW

SD-WAN

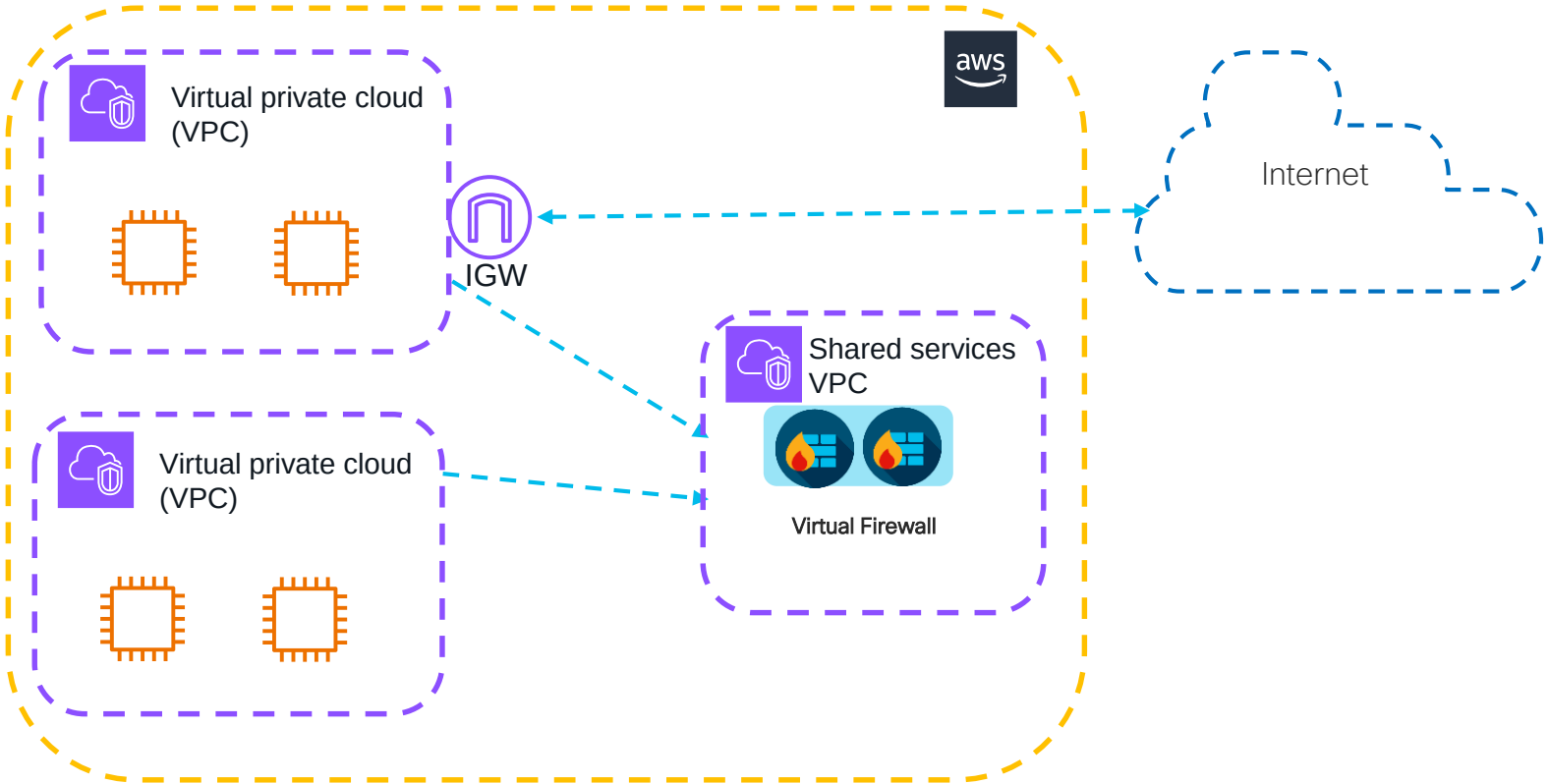
Firewall

Singapore

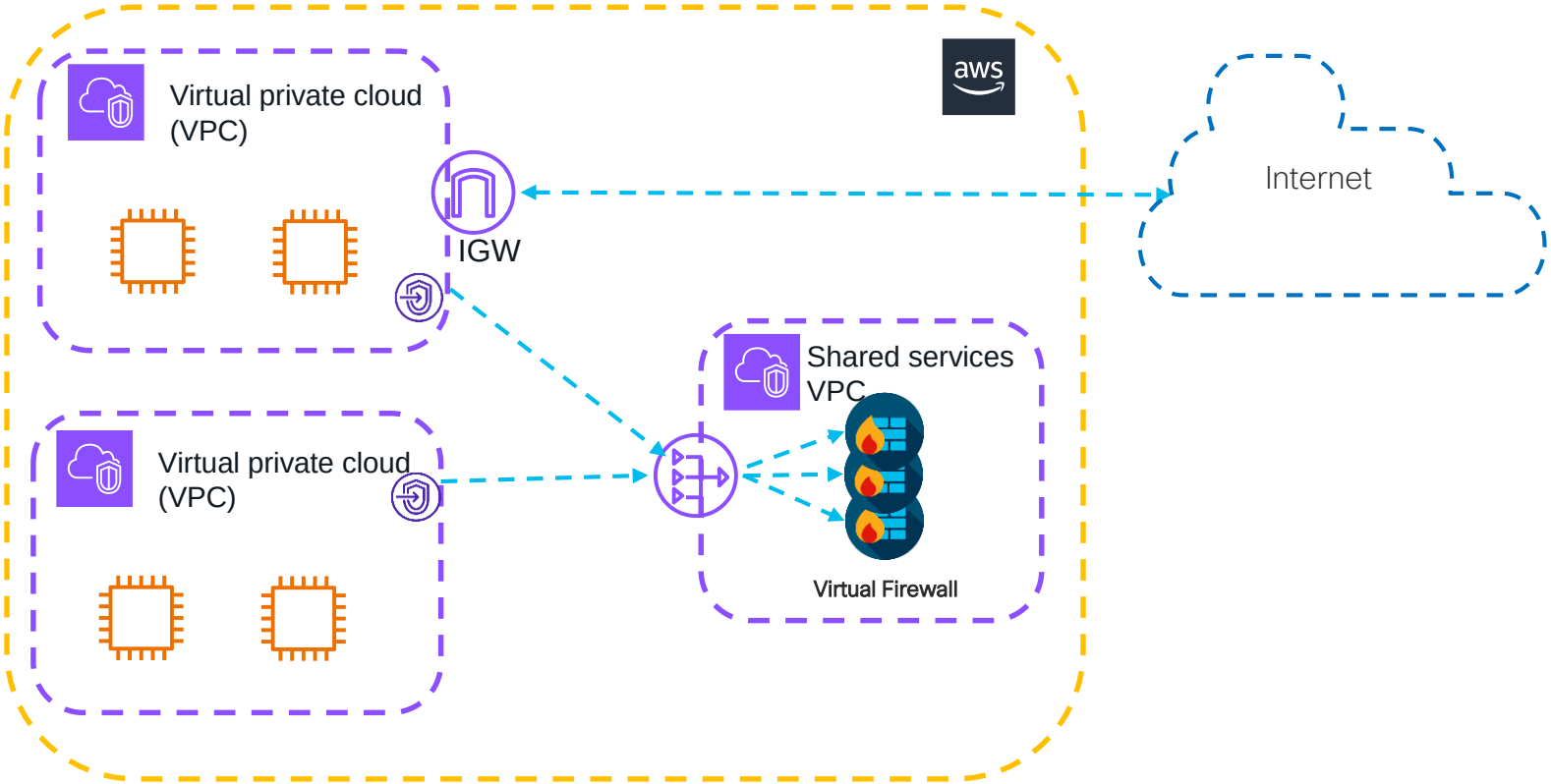
AWS Networking Recap



AWS Gateway Load-balancer



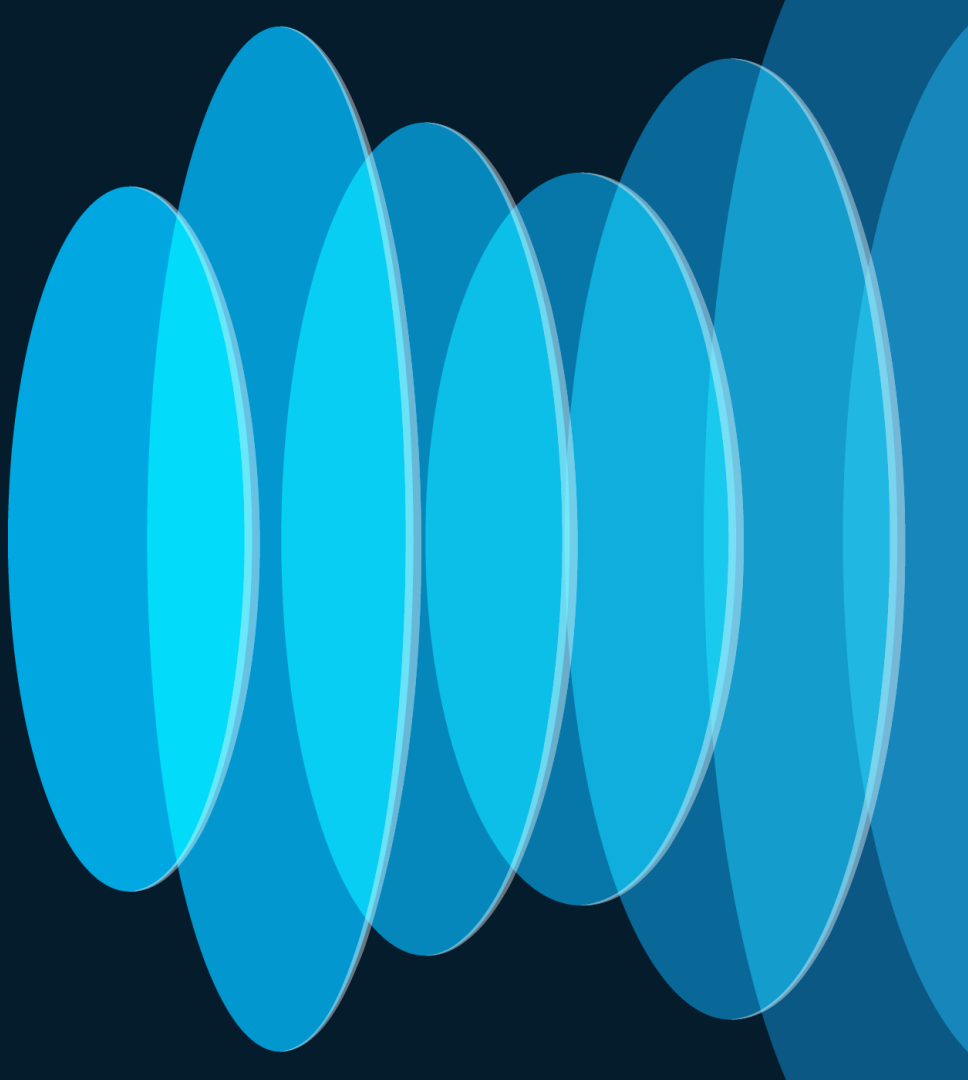
AWS Gateway Load-balancer



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

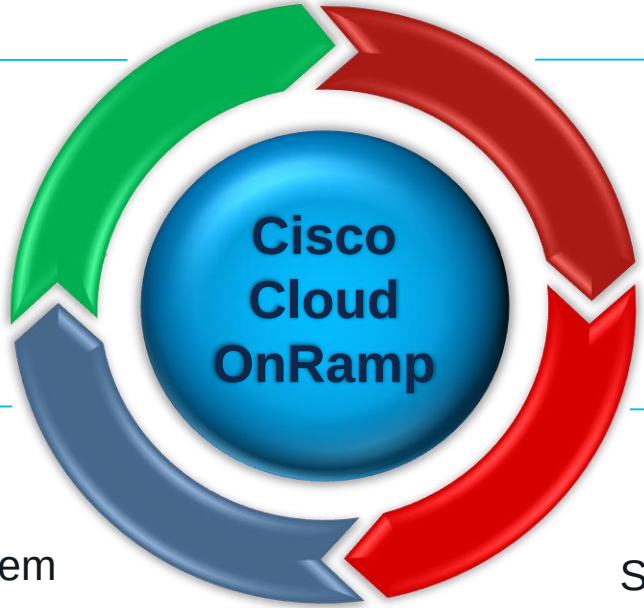
Cloud On-Ramp to AWS



Cisco Cloud OnRamp solves your cloud problems

Automation

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



Operations

Cloud Audit, Monitoring, Prediction and Recommendation

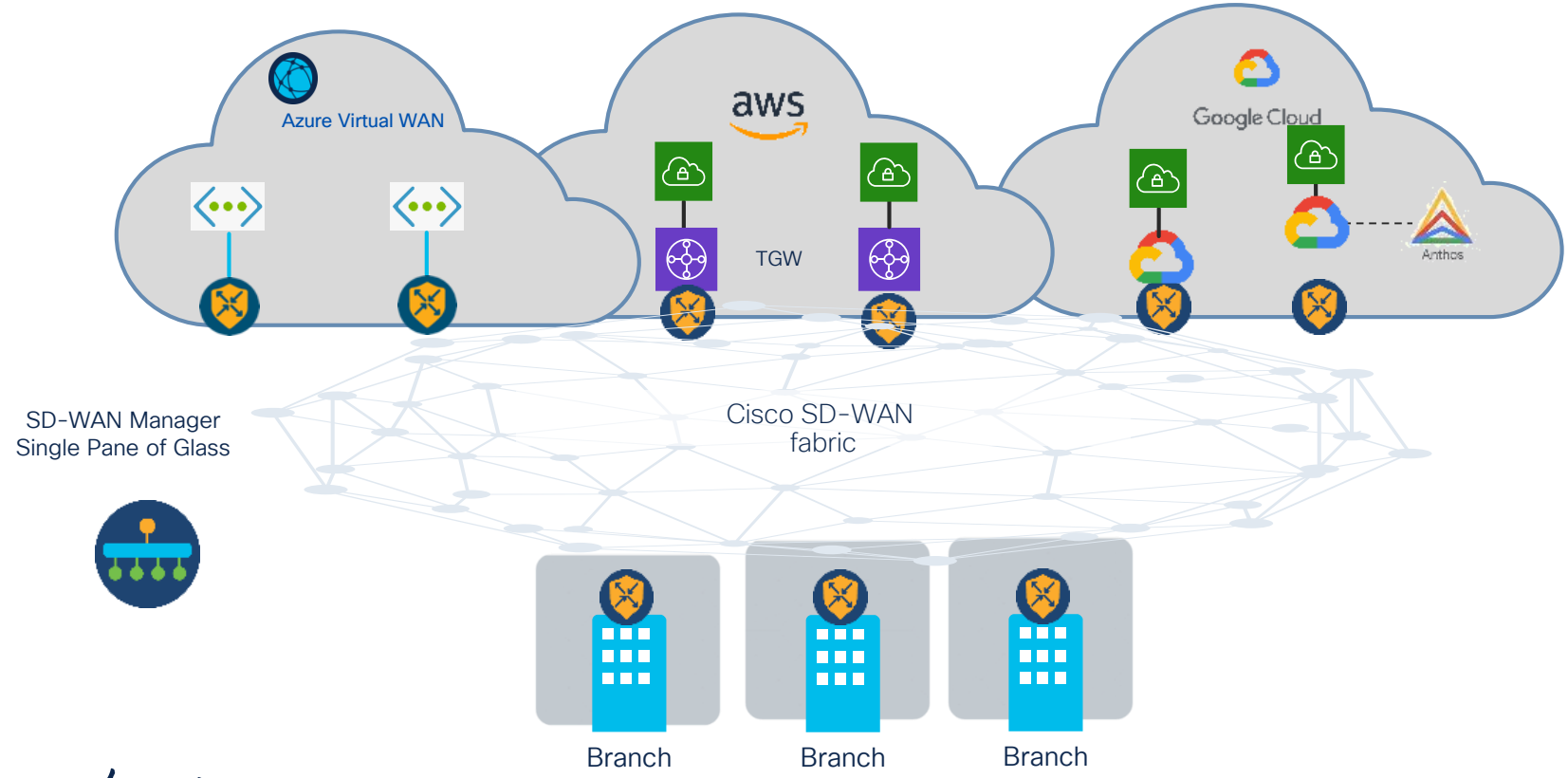
Security

Cloud Security, SIG, On-Prem

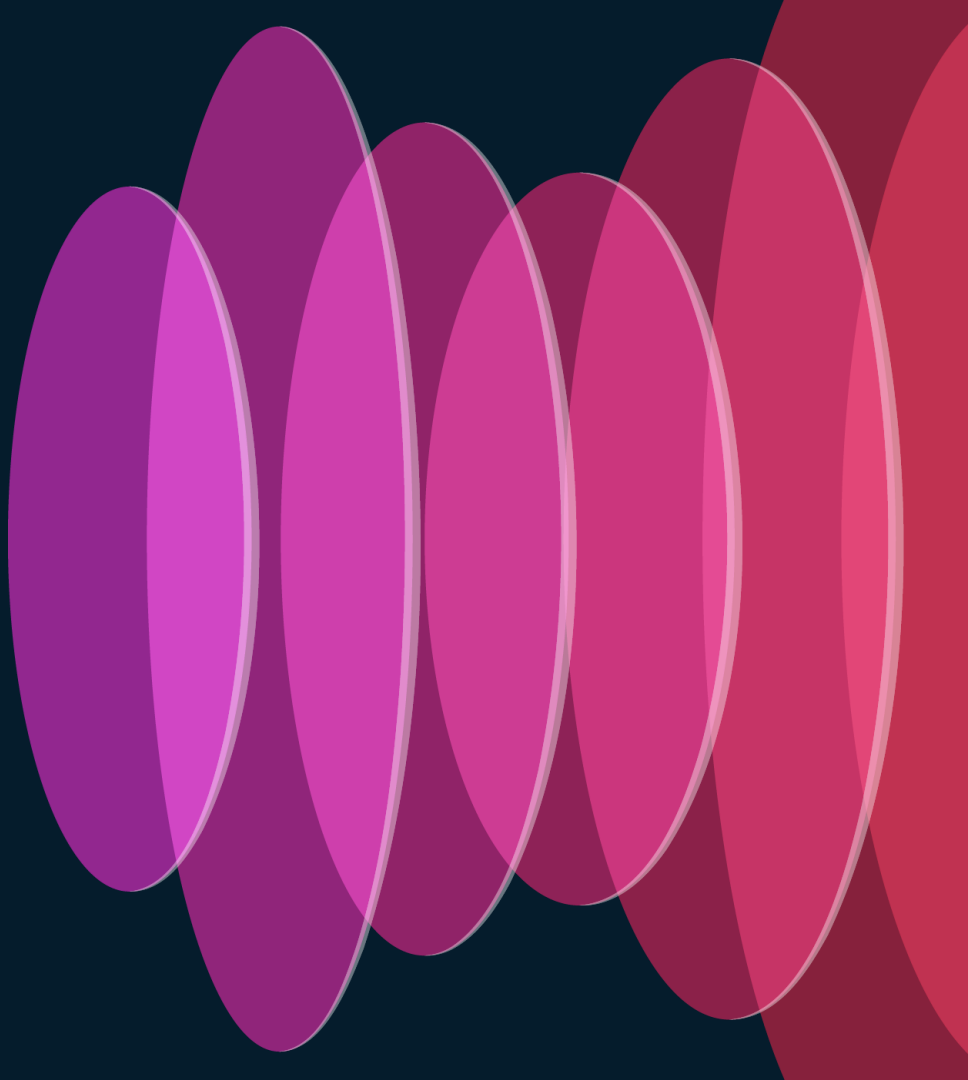
App Performance

Service Directory Integration, Mid-Mile Optimization

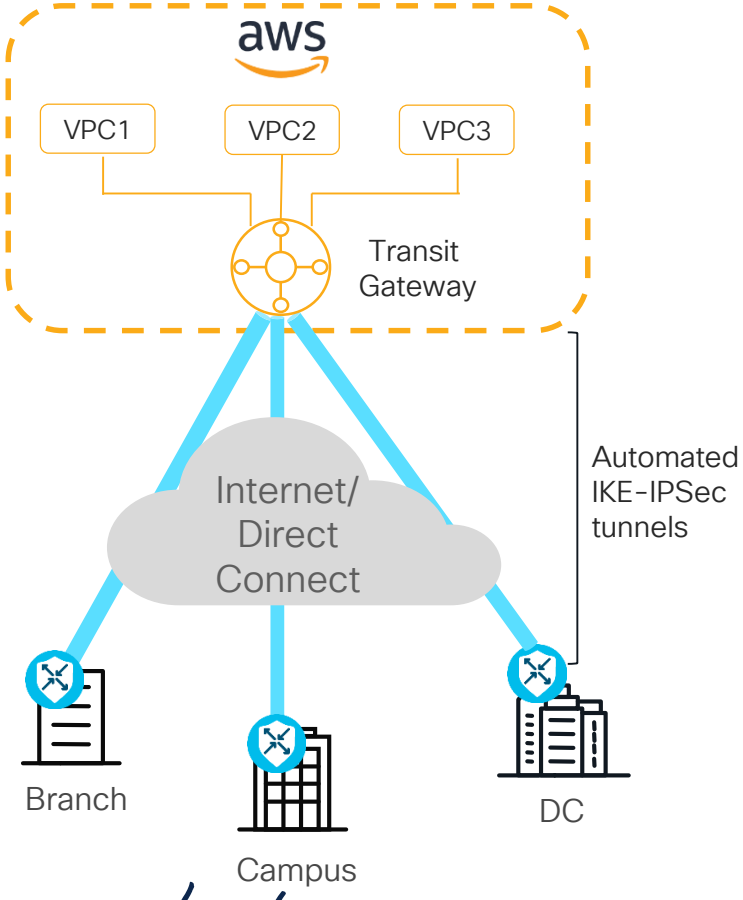
Cloud OnRamp for Multicloud



On-prem to Cloud Design Options

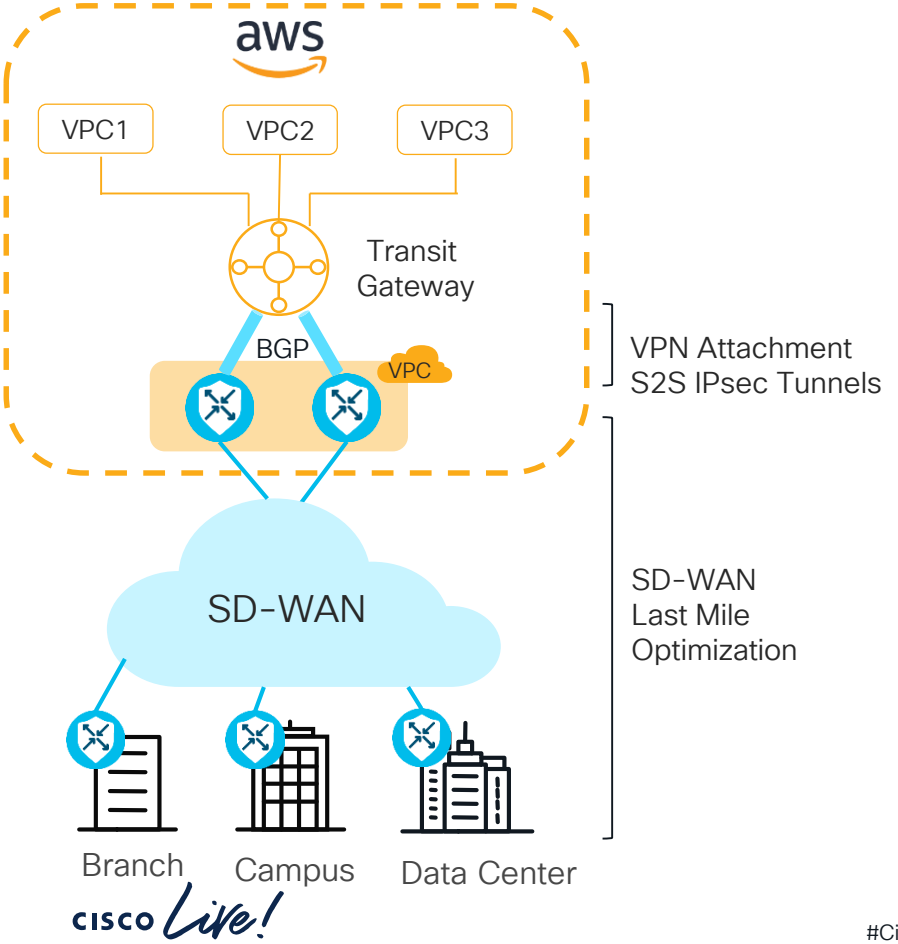


Design Option#1 – Branch Connect Model



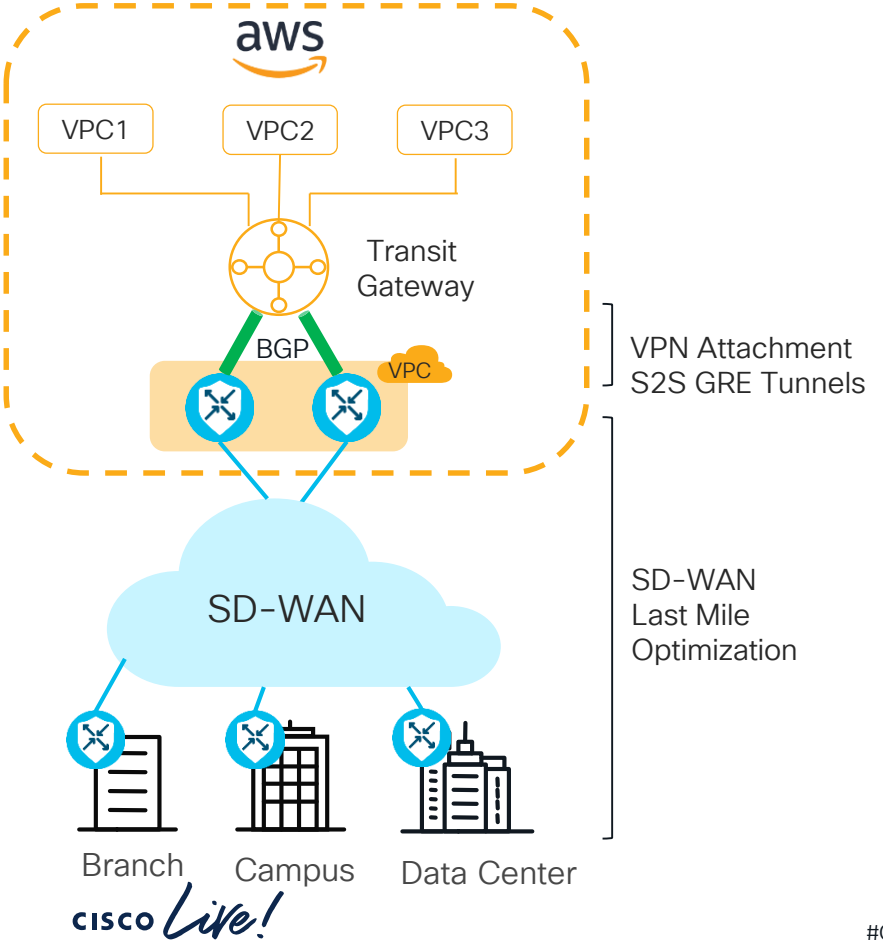
- Automated Provisioning
- Lower Costs
- More Bandwidth per Site
- HA Support
- Tunnel Monitoring Required

Design Option#2 – VPN (IPSec) based Model



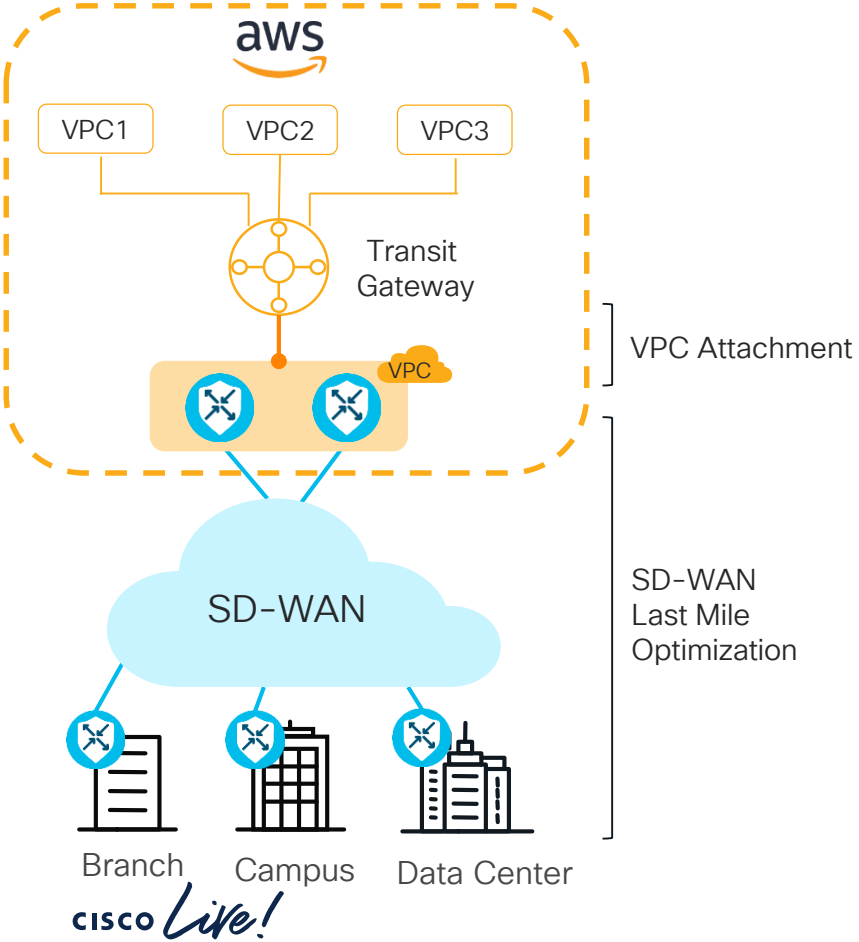
- Automation
- Centralized Policy
- Network Segmentation
- Lower OpEx
- SD-WAN for HA and Scaling

Design Option#3 – GRE Connect based Model



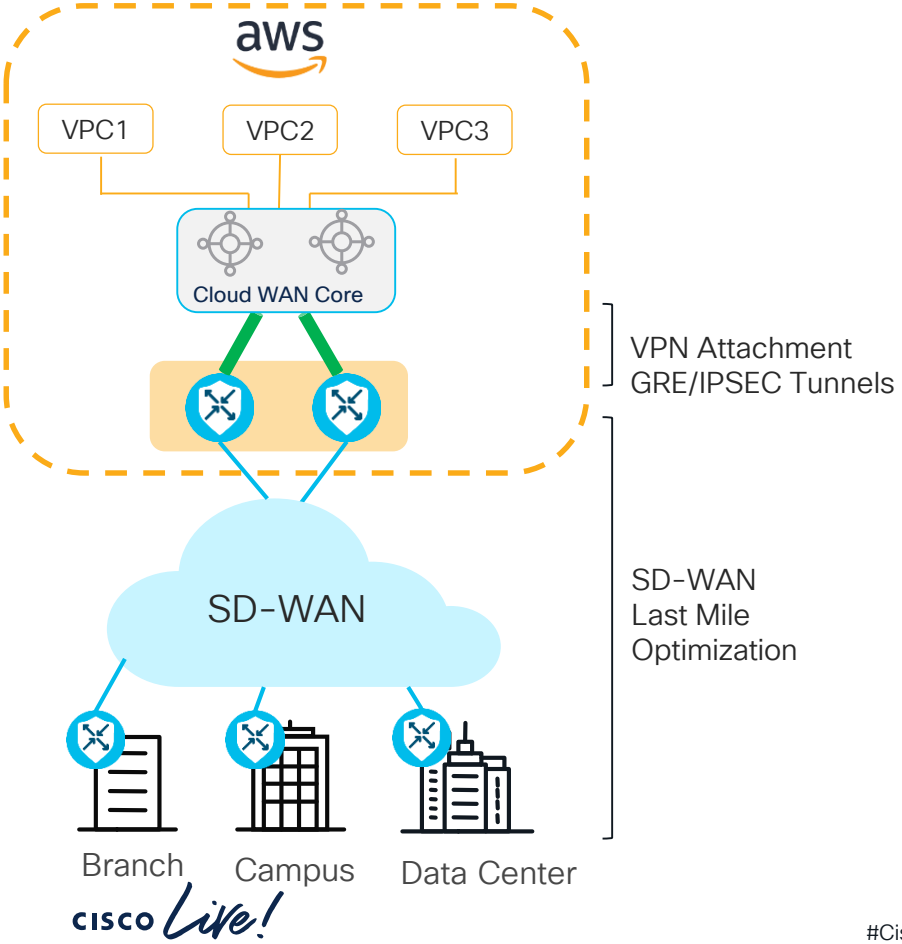
- Automation
- Centralized Policy
- Network Segmentation
- Lower OpEx
- SD-WAN for HA and Scaling
- Higher Scaling

Design Option#4 – VPC Attachment Model



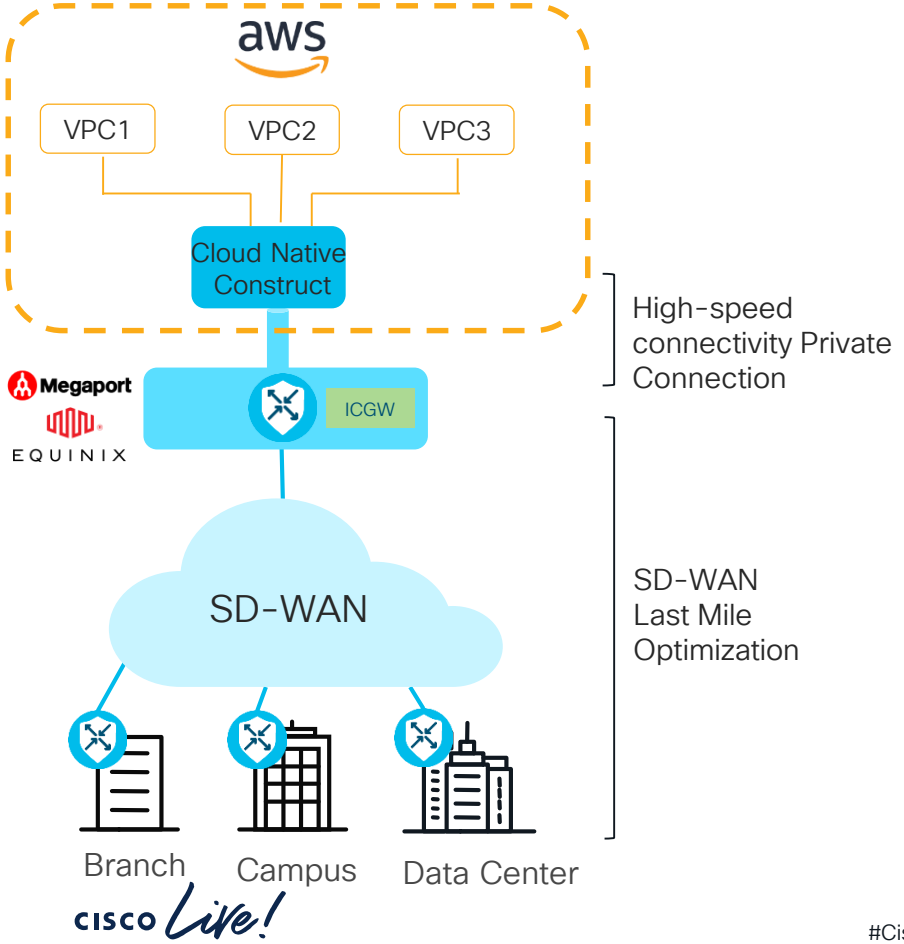
- Higher Bandwidth for Single Link
- Lower Cost
- Static Routing Only
- Manual Configuration

Design Option#5 – Cloud-WAN



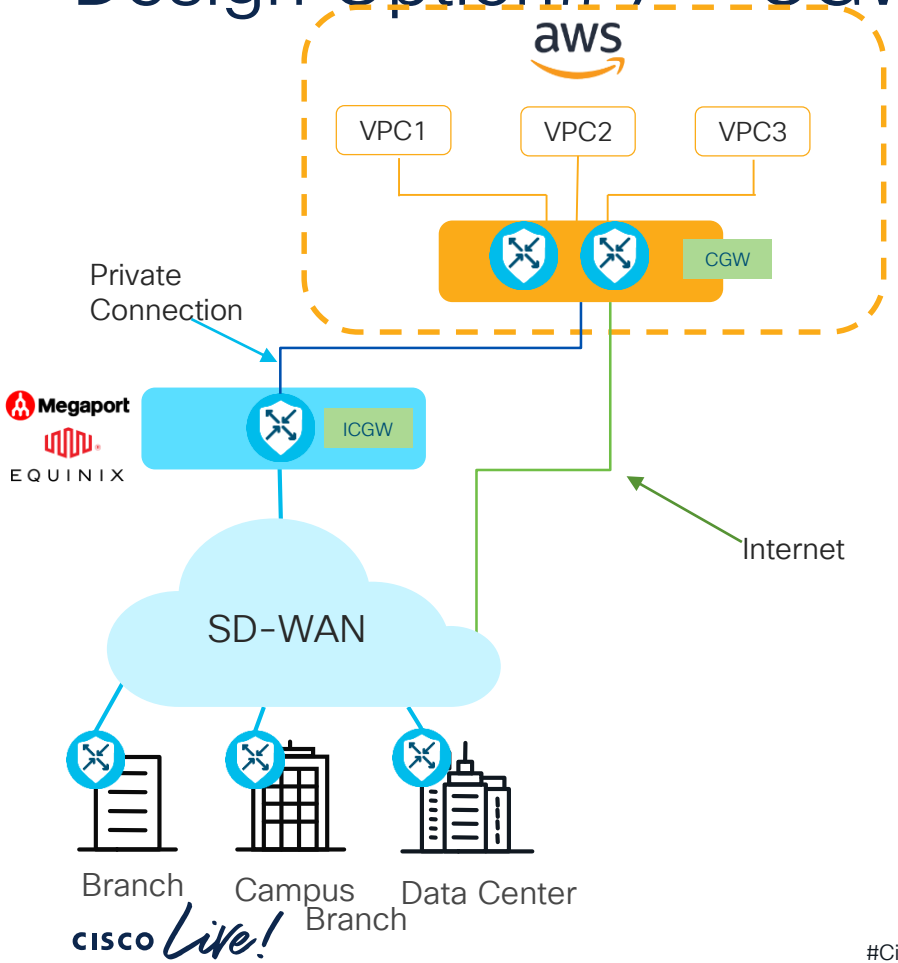
- Automation
- Centralized Policy
- Network Segmentation
- Lower OpEx
- SD-WAN for HA and Scaling
- Higher Scaling

Design Option# 6 – CoLo Interconnect Model



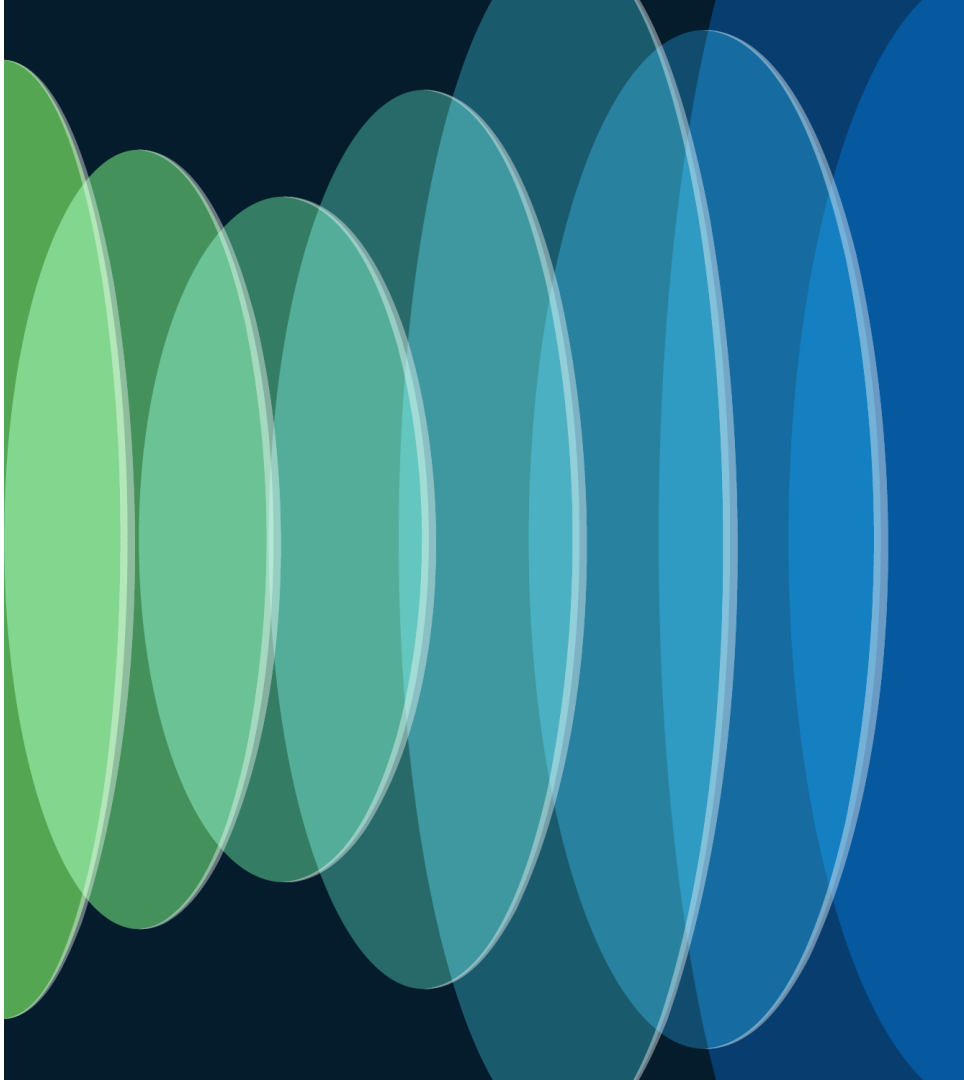
- High Speed Path to Cloud
- Scalability
- Service Chaining
- Optimized Routing
- SD-WAN for HA
- Encryption from Branch to Co-Lo

Design Option# 7 – CGW in SDCI Model

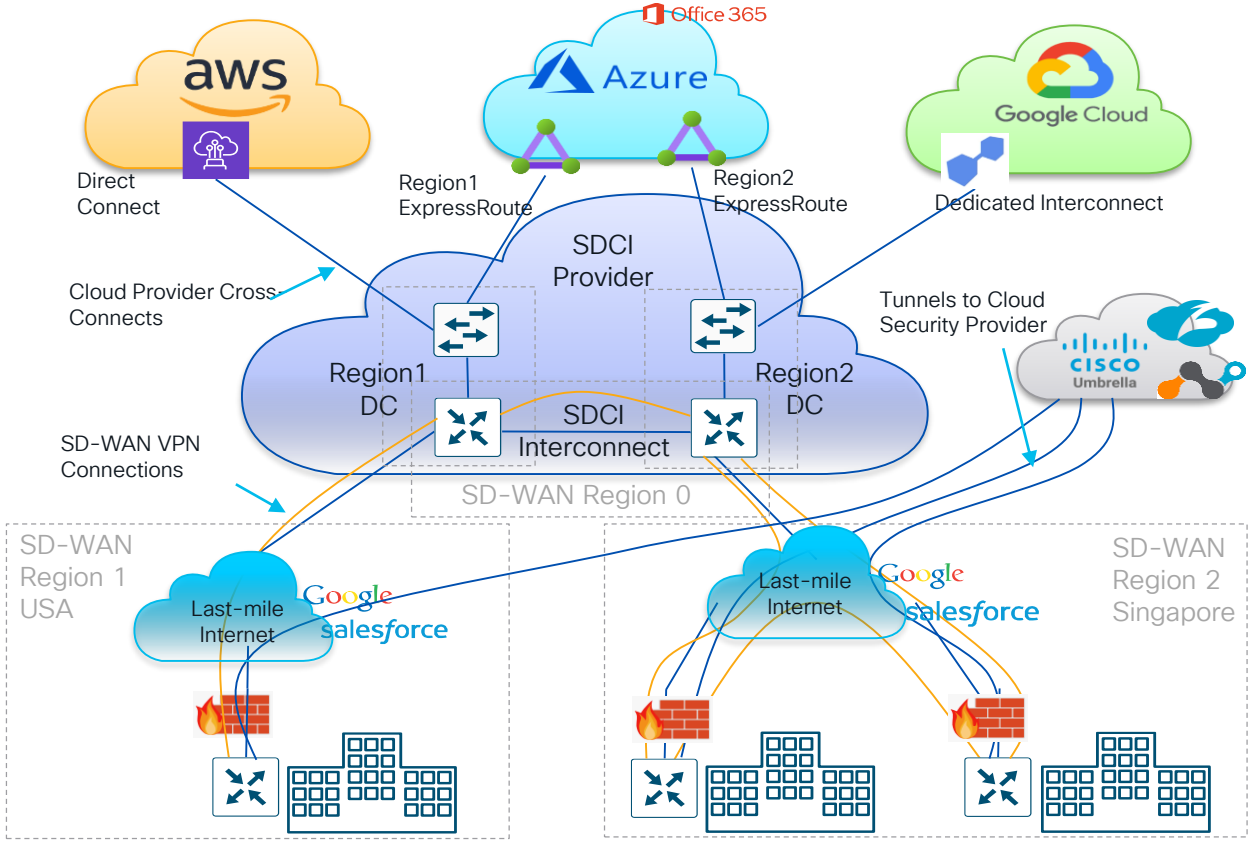


- End-to-end Encryption
- Multipath Support
- SD-WAN Everywhere

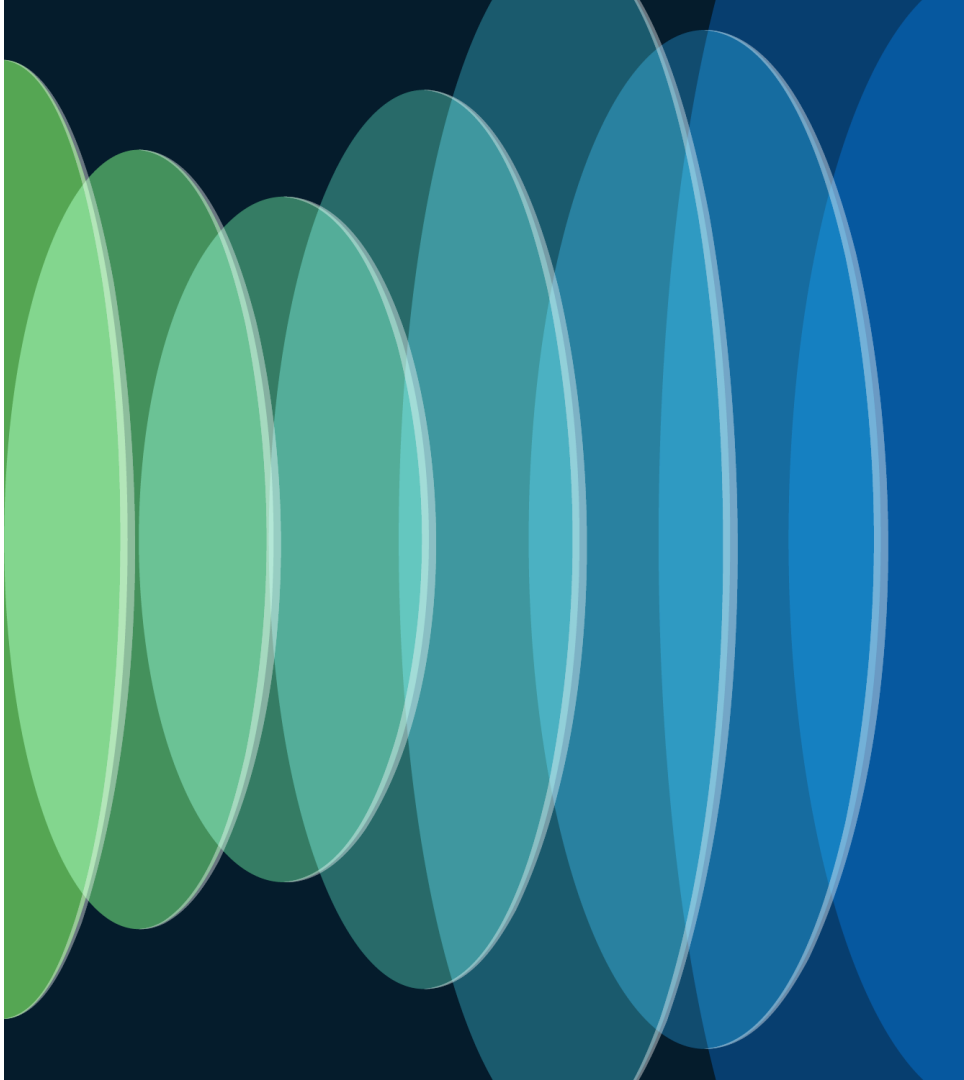
Cloud as a Transport



Cloud as a Transport

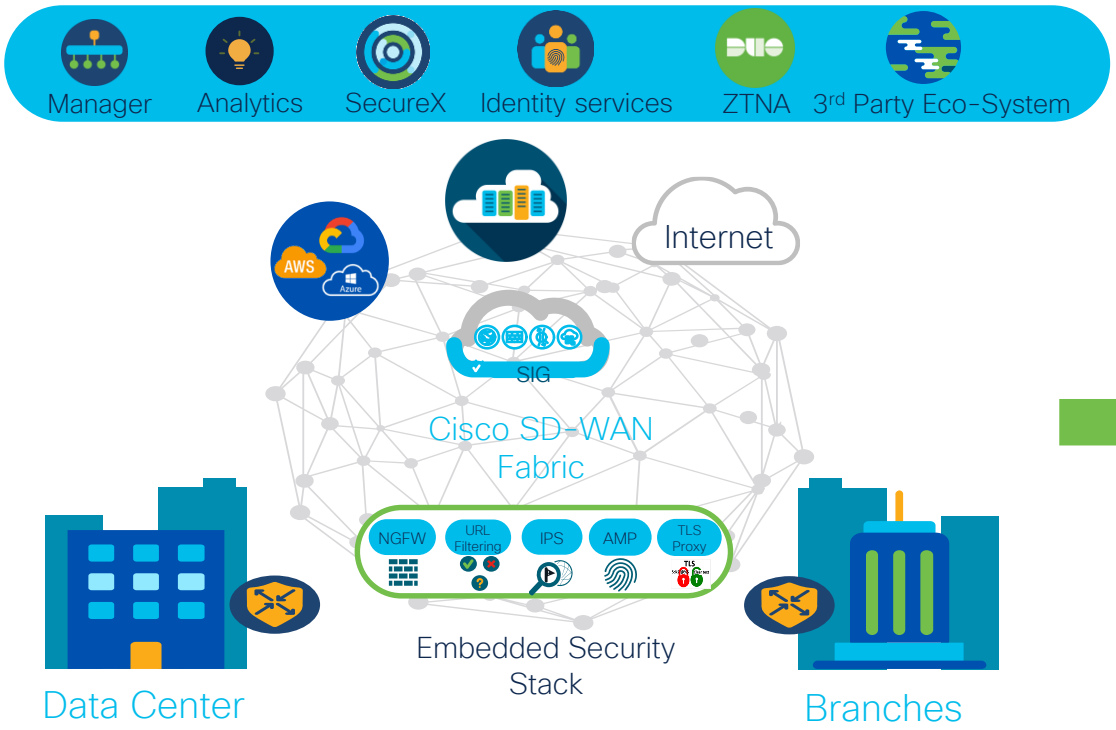


Security



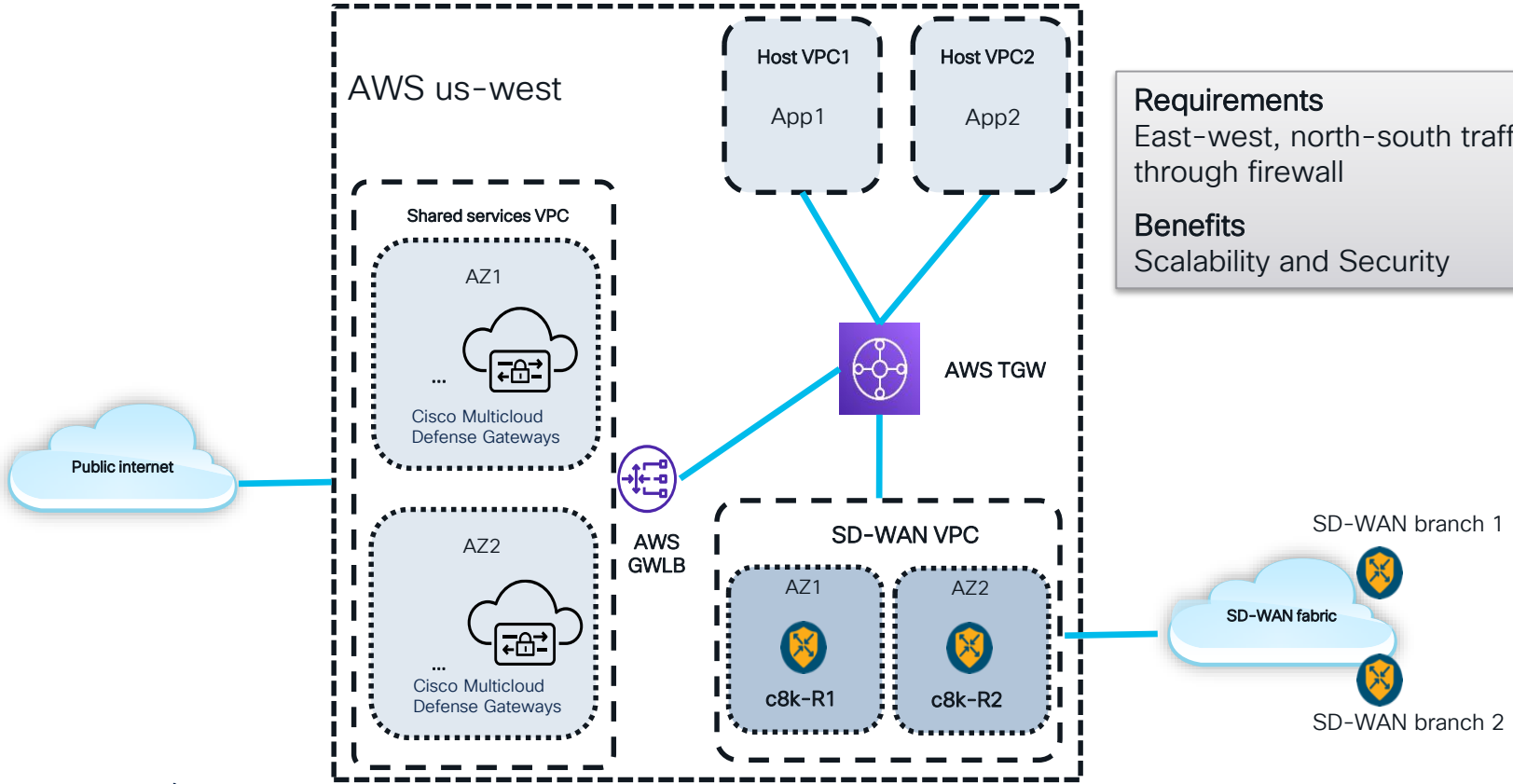
cisco Live!

SD-WAN Security – Overview



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

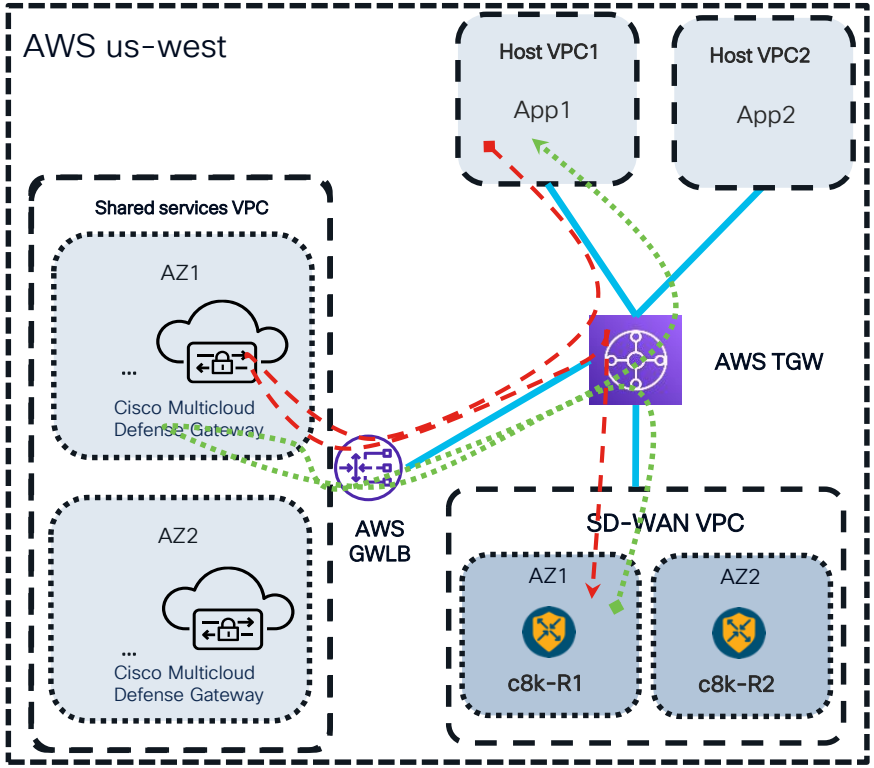
AWS: Centralized Firewall Design



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

Benefits
Scalability and Security

Packet flow: Simplified



From Host VPC to SD-WAN

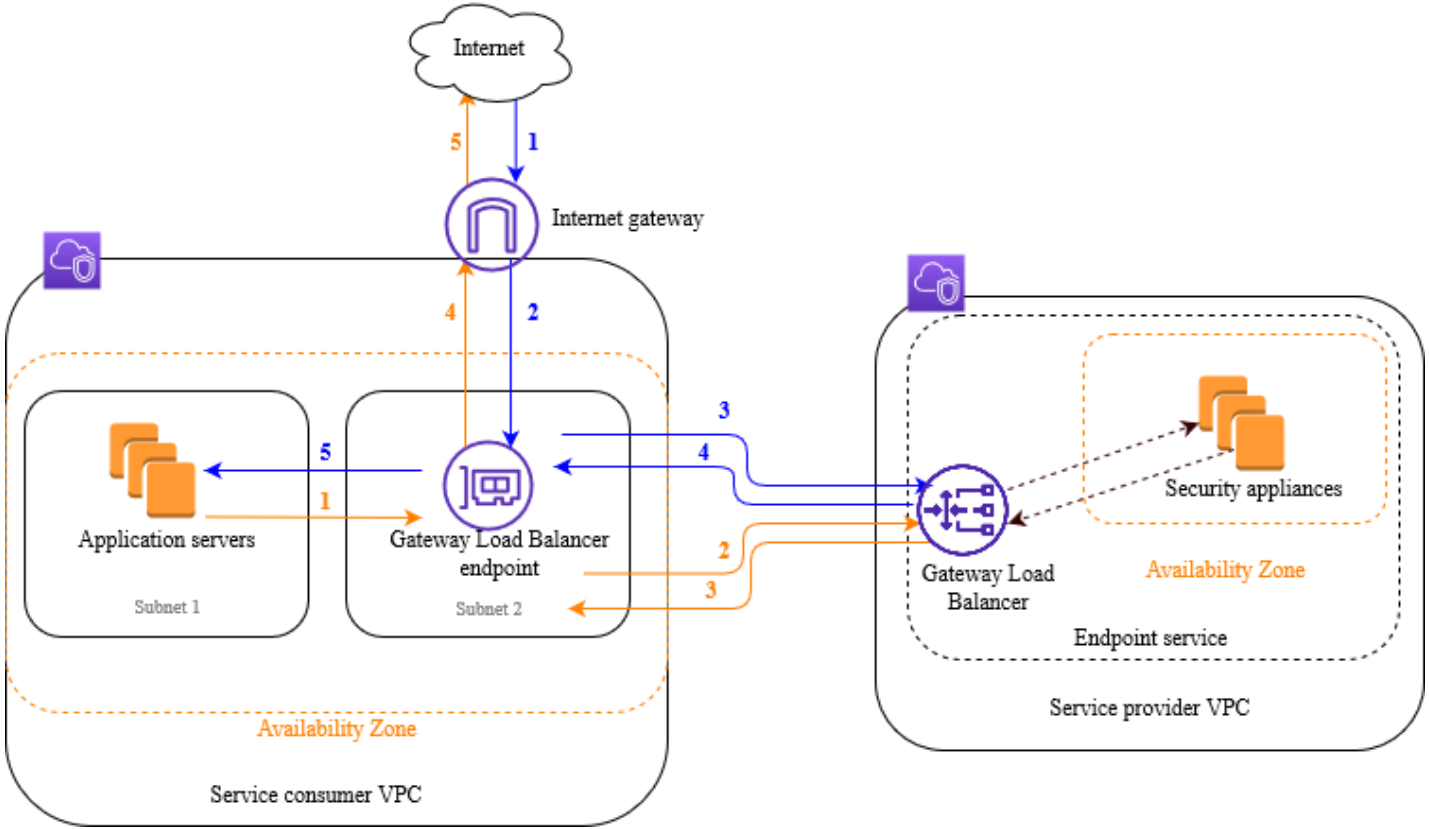
From SD-WAN to Host VPC

GENEVE protocol for load balancing between GWLB and Multicloud Defense Gateway

MDG = Cisco Multicloud Defense Gateway
GWLB = AWS Gateway Load Balancer

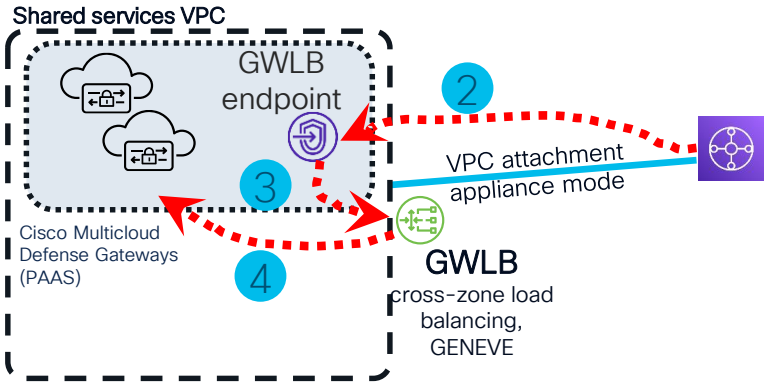
Geneve = Generic Network Virtualization Encapsulation
AZ = Availability Zone (AWS data center)

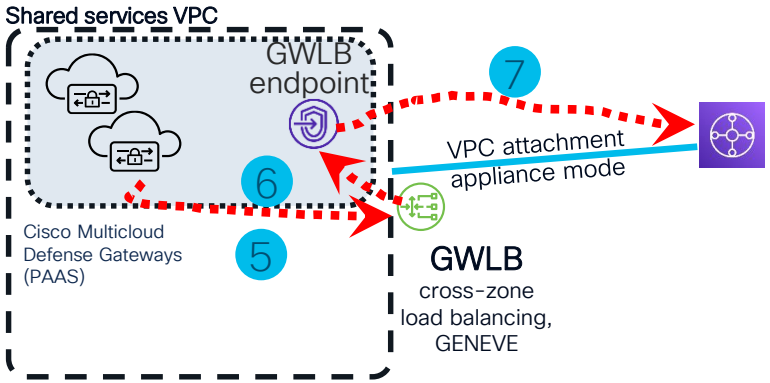
AWS Gateway Load Balancer Explained



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

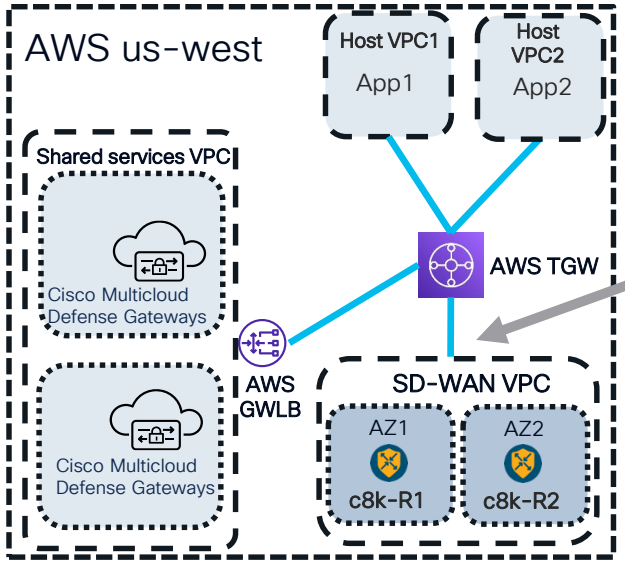
...

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

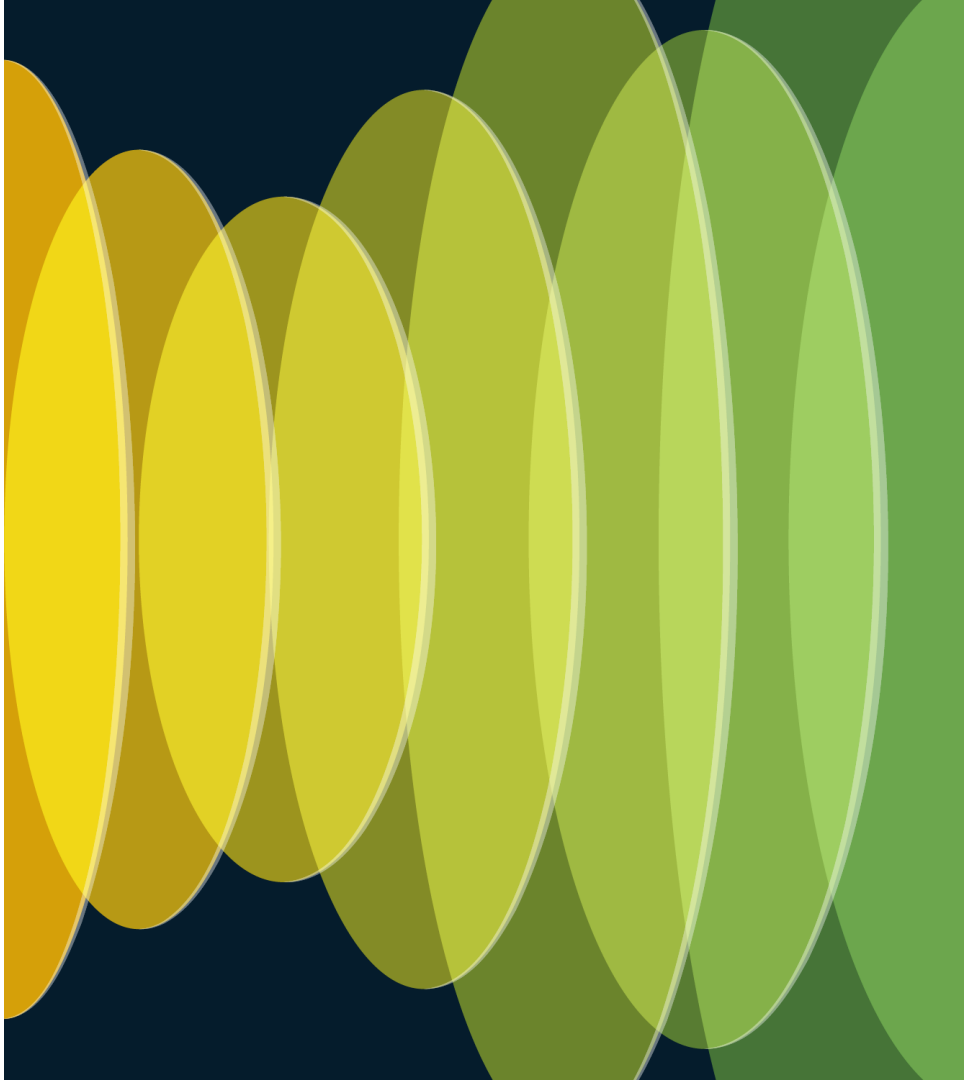
Step 7: GWLB endpoint sends packet to TGW

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

Demo



Multicloud Survey for Customers

Tiny URL: https://tinyurl.com/yc7evp89

As part of our continuous improvement cycle, we are requesting our customers to fill this short survey that will help guide our decisions for the future roadmap.

Of particular interest is the second-to-last box that allows for free-form suggestions - please use this if the previous questions do not cover your plans/vision adequately.

Scan the QR code to fill out this short survey or use the TinyURL

CLUS – Multicloud Sessions of Interest

- BRKENT-2283 : 7 Steps: Master the art of unifying Multicloud secure Connectivity and Design - Cisco SD-WAN + Multicloud Defense
- IBOENT-2005 : Exploring the Rise of NaaS: A Dynamic Shift from Self-Owned Infrastructure
- CISCOU-2031 : MultiCloud Connectivity using Catalyst SD-WAN (High-level)
- BRKXAR-2003 : Extending Enterprise Network into Public Cloud with Cisco Catalyst 8000V Edge Software
- BRKXAR-2015 : Extend the Enterprise to the Cloud: AWS Cloud Integration with Enterprise SD-WAN
- LTRENT-1423 : Cisco Catalyst and Meraki SD-WAN – The Power of One
- LTRCRT-2011 : CCNP Enterprise Cloud Connectivity Hands-On Lab

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

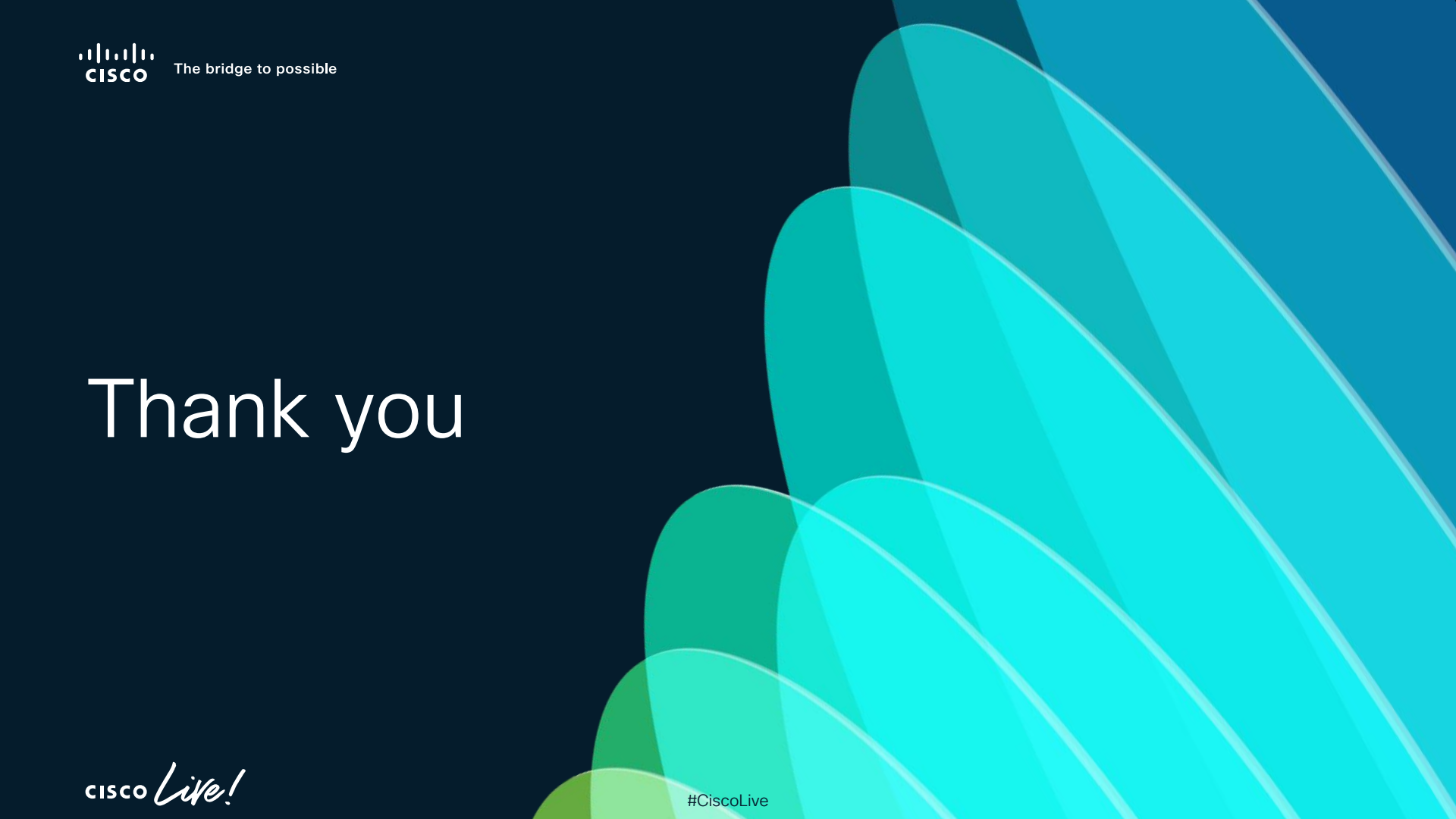
Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

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

Contact me at: lsudduth@cisco.com
pravpooj@cisco.com


The bridge to possible
Thank you
cisco Live!
#CiscoLive