cisco The bridge to possible

Approach to Cloud Networking

Traditional Solutions to SDN

Iñigo Alonso
Principal Architect – Cisco Customer Experience

Cisco Webex App

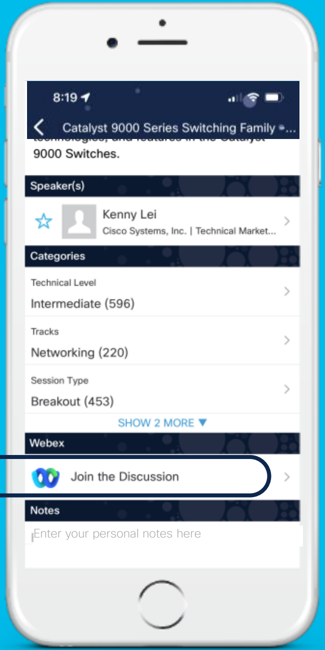
Questions?

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.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

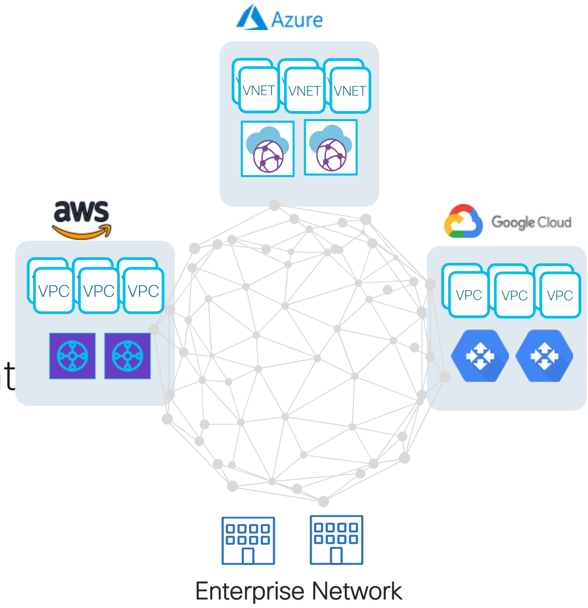
Enter your personal notes here

Agenda

- Introduction
- Generic Cloud Networking
- Connecting to the Public Cloud
- Multi-Cloud Network Topologies

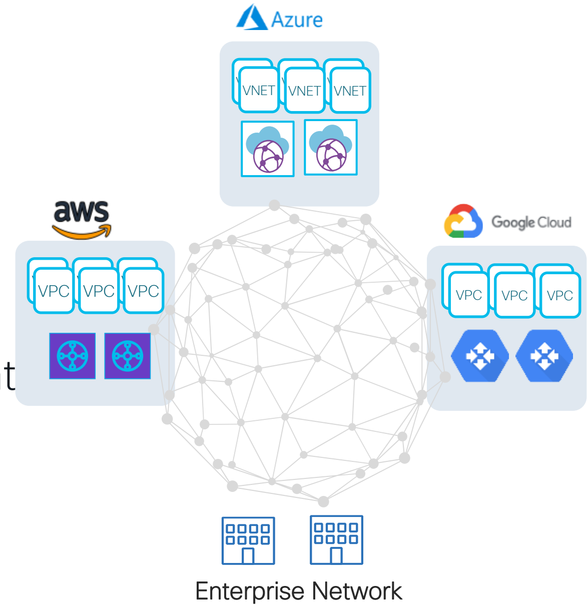
Multi-Cloud Networking

- **Traditional**: native cloud networking constructs
- **Software-Defined Network**: controller-based multi-cloud overlay
- Context:
  - Multi-Cloud = consumption of two or more clouds, including hybrid cloud (private + public)
  - Public cloud as an extension of the private IT environment
  - Cloud benefits without compromising security and compliance
  - Multi-cloud private app-to-app communication



Multi-Cloud Networking

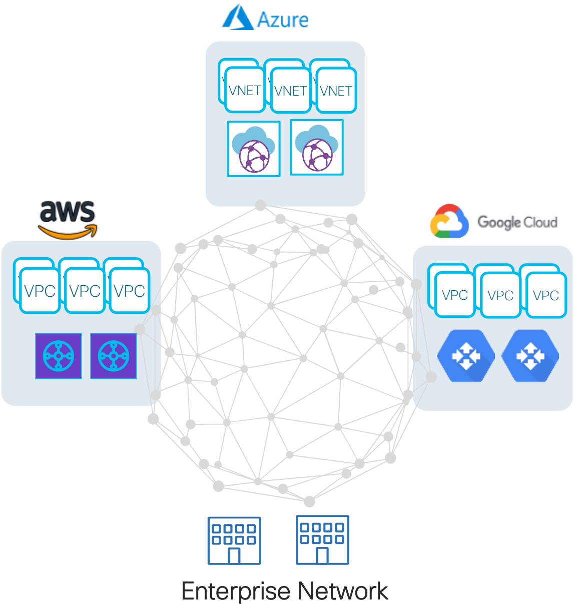
- **Traditional**: native cloud networking constructs
- **Software-Defined Network**: controller-based multi-cloud overlay
- Context:
  - Multi-Cloud = consumption of two or more clouds, including hybrid cloud (private + public)
  - Public cloud as an extension of the private IT environment
  - Cloud benefits without compromising security and compliance
  - Multi-cloud private app-to-app communication



Is there a case for SDN in Multi-Cloud?

Multi-Cloud Networking

- Common requirements and design criteria
  - Performance, Scalability, Cost effective
  - High Availability, Resilience
  - Security, Compliance, Segmentation
  - Management, Operations, Visibility, Assurance
  - Consistency, Automation, Agility
  - Modularity, Flexibility, Simplicity
  - Cloud native support: programmability, integrations, devops user experience
  - Broader context



Hybrid/Multi Cloud Networking

Core Challenges

Connectivity

How do I connect distributed components across multiple cloud and edge providers?

Zero Trust and Security

How do I maintain a consistent security posture that is agnostic to where my app and clients are located?

Visibility

How do I observe and analyze traces, logs, and metrics across distributed threads of execution and time?

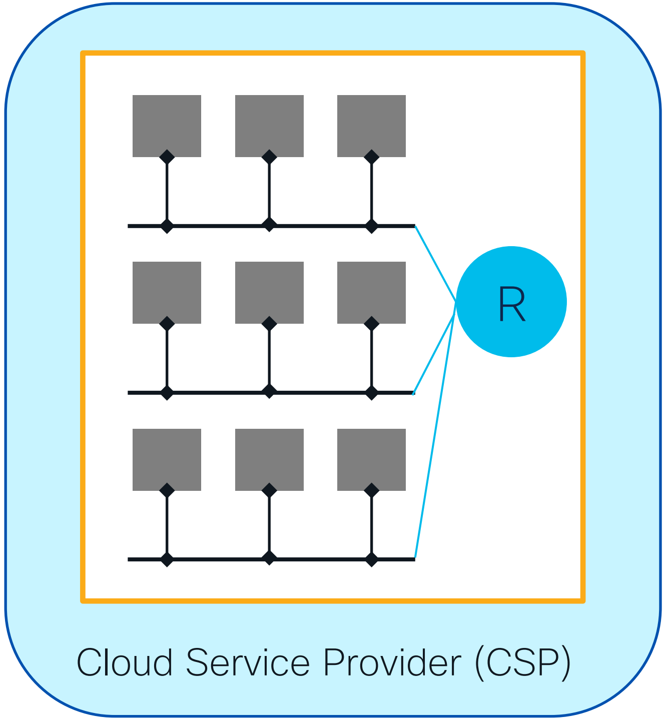
Application Networking

Developers need a declarative way to signal application connectivity requirements.

Need For Homogenous Experience Across Heterogenous Cloud Environments

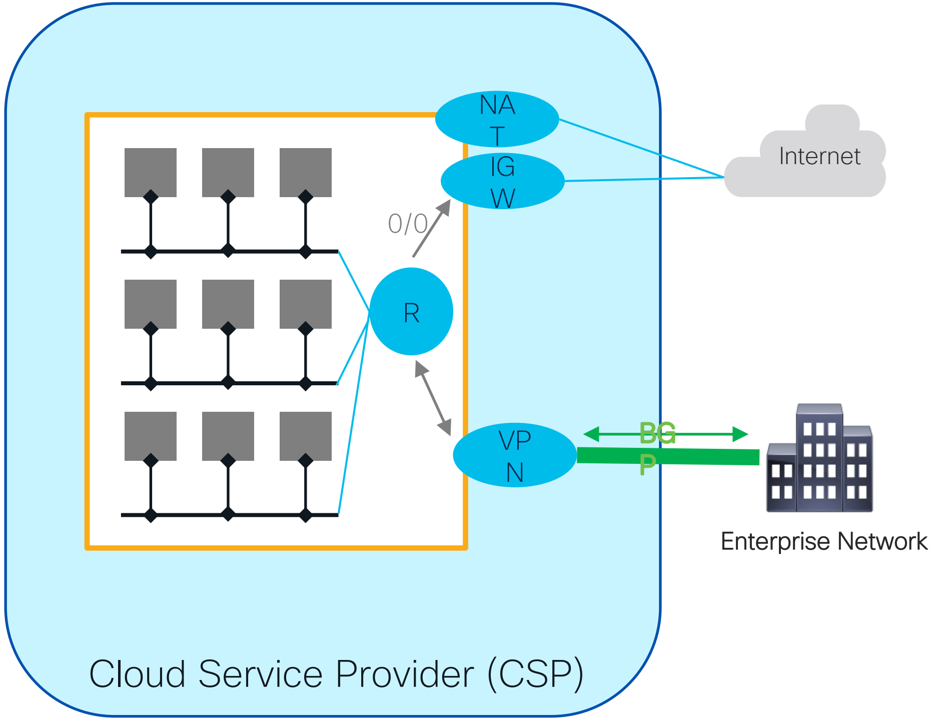
Generic Cloud Networking

- Virtual Data Center
  - AWS VPC, Azure VNET, GCP VPC
  - Regional or Global (GCP)
  - Connectivity for instances and endpoints
  - Subnets: zonal or regional
  - Private & public IP addressing
  - Static routing
  - L4 traffic filtering rules: Security groups, ACLs



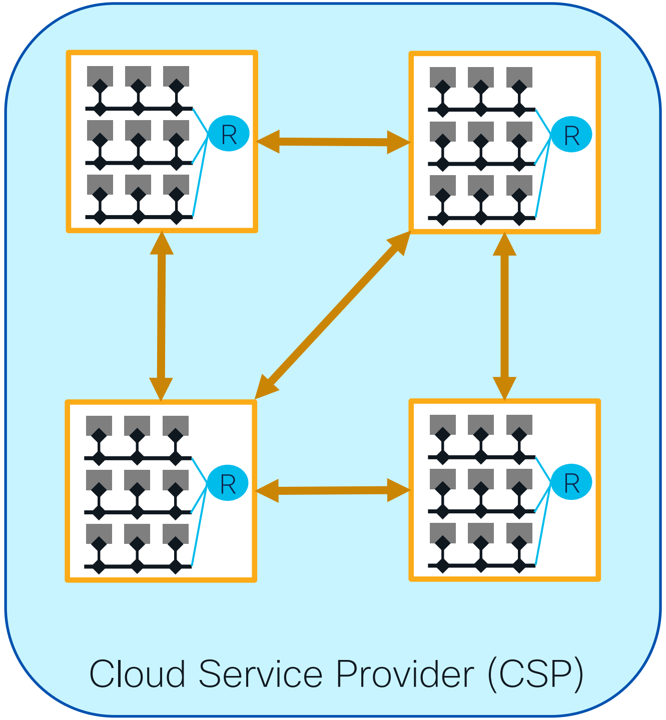
Generic Cloud Networking

- Virtual Data Center
  - Internet access
  - NAT: 1:1 (instance with public IP address), or address pool
  - VPN to remote public or private endpoints
    - Static or BGP routing
    - Propagate learned routes into routing table
    - Advertise VPC/VNET CIDR or subnets



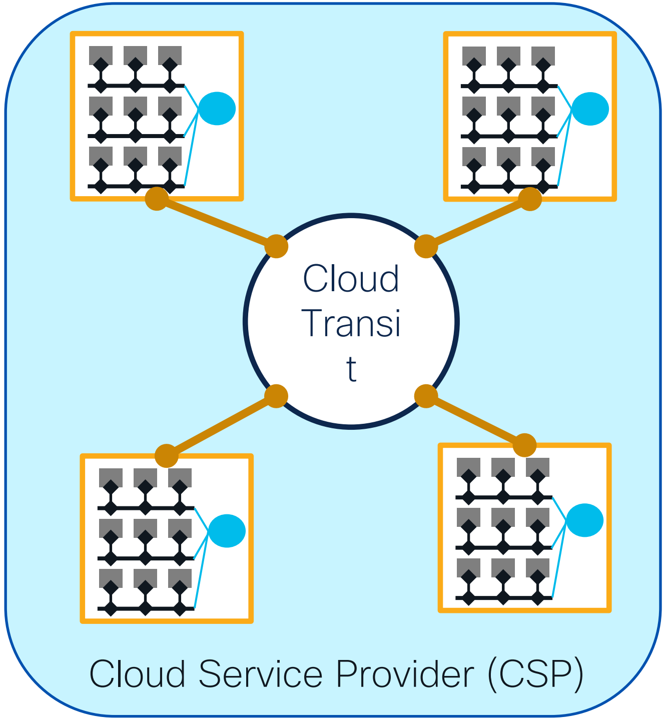
Generic Cloud Networking

- Virtual Data Center Peering
  - Intra-region or inter-region
  - Non-transitive
  - Full mesh required for any-to-any communication
  - Scale challenges



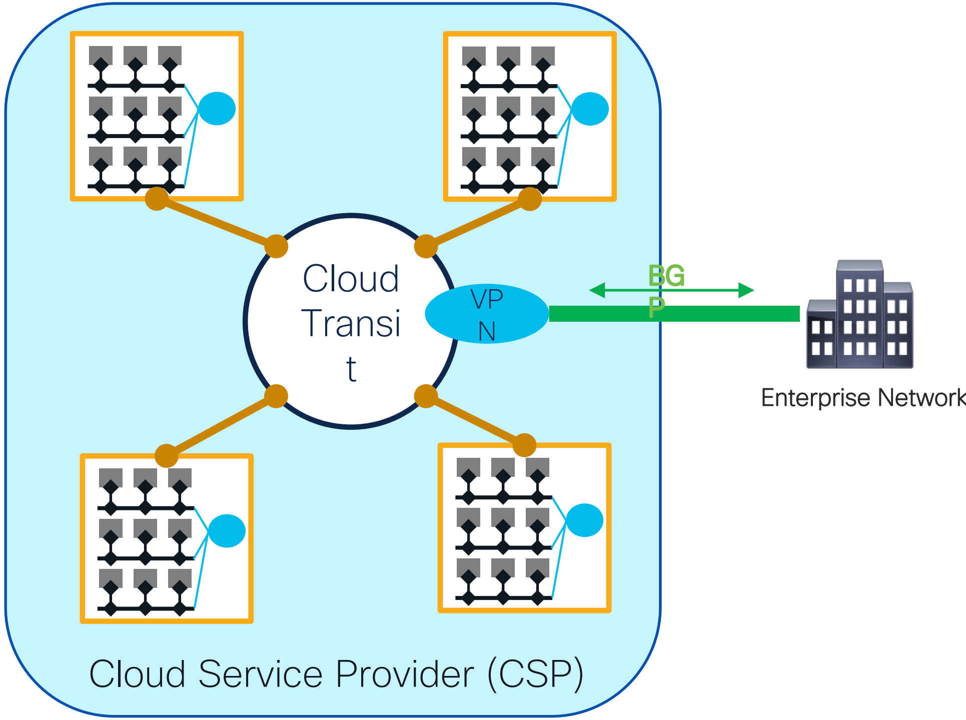
Generic Cloud Networking

- Cloud Transit
  - AWS Transit Gateway, Azure vWAN Hub, GCP Transit VPC
  - Interconnect VPCs/VNETs
  - Hub & Spoke connectivity model
  - Regional scope; 1 or more per region
  - Static routing; multiple routing tables



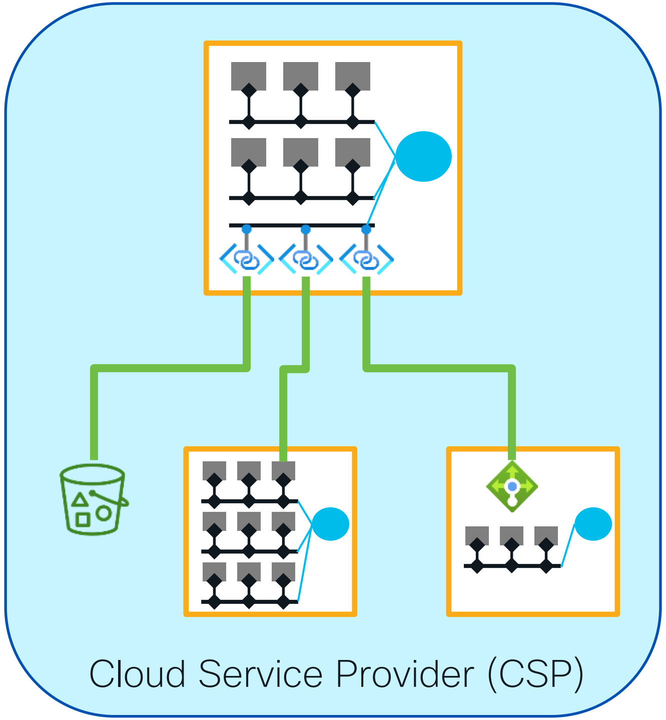
Generic Cloud Networking

- Cloud Transit
  - AWS Transit Gateway, Azure vWAN Hub, GCP Transit VPC
  - Interconnect VPCs/VNETs
  - Hub & Spoke connectivity model
  - Regional scope; 1 or more per region
  - Static routing; multiple routing tables
  - VPN to remote public or private endpoints; static and dynamic routing (BGP)



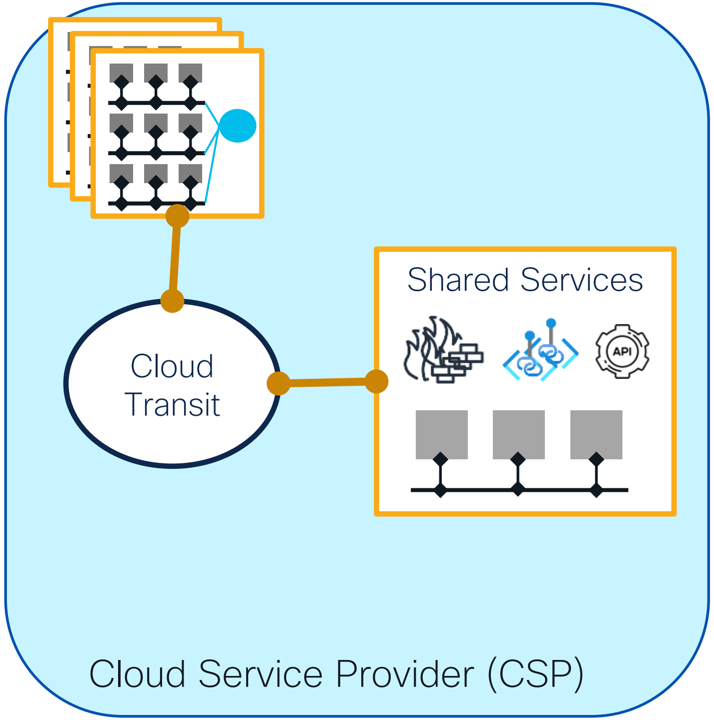
Generic Cloud Networking

- Private Access to Services
  - Access to CSP's PaaS services (Storage, DB, etc) via private endpoints
  - Access to services in other virtual environments via private endpoints – within and across organizations
  - Access to Load Balancers via private endpoints
  - Ex: AWS interface endpoints and gateway endpoints; Azure Private Link; GCP Private Service Connect



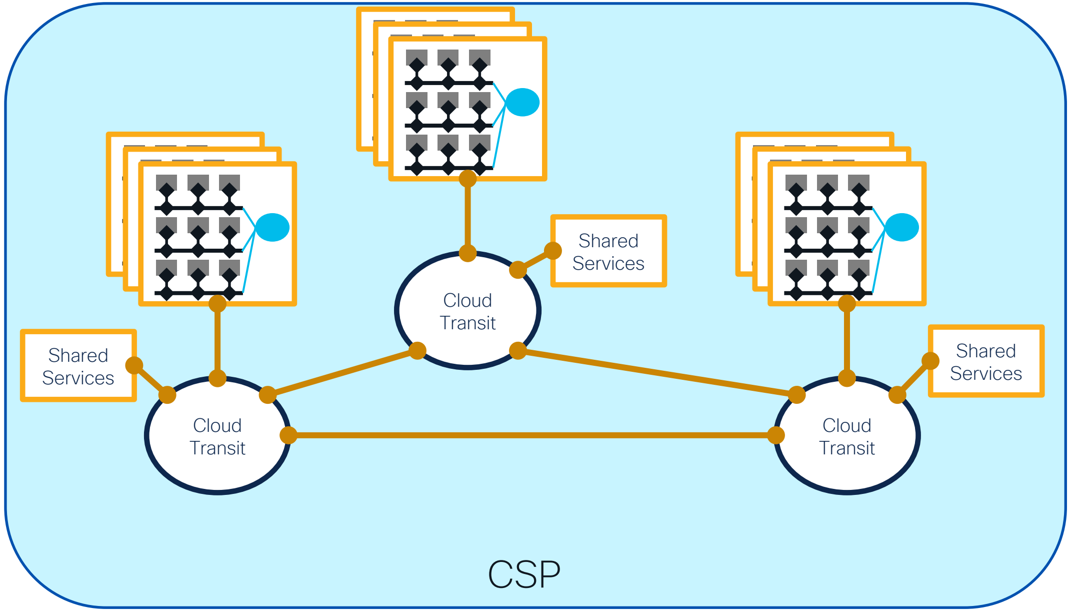
Generic Cloud Networking

- Shared Services
  - Common infrastructure services shared by multiple groups
  - Network services: DNS, proxy
  - Security: firewall, inspection
  - App middleware: API gateway, data broker
  - Private access to services
  - Monitoring, logging



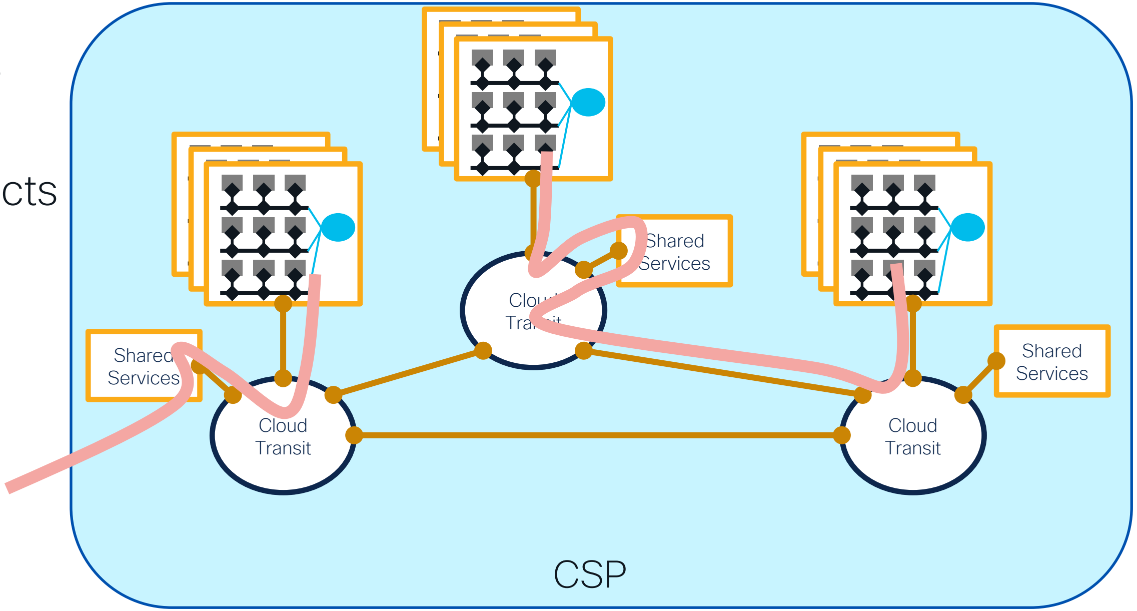
Generic Cloud Networking

- Multi-Region Cloud Transit
  - Modular design, repeatable
  - Native CSP network constructs



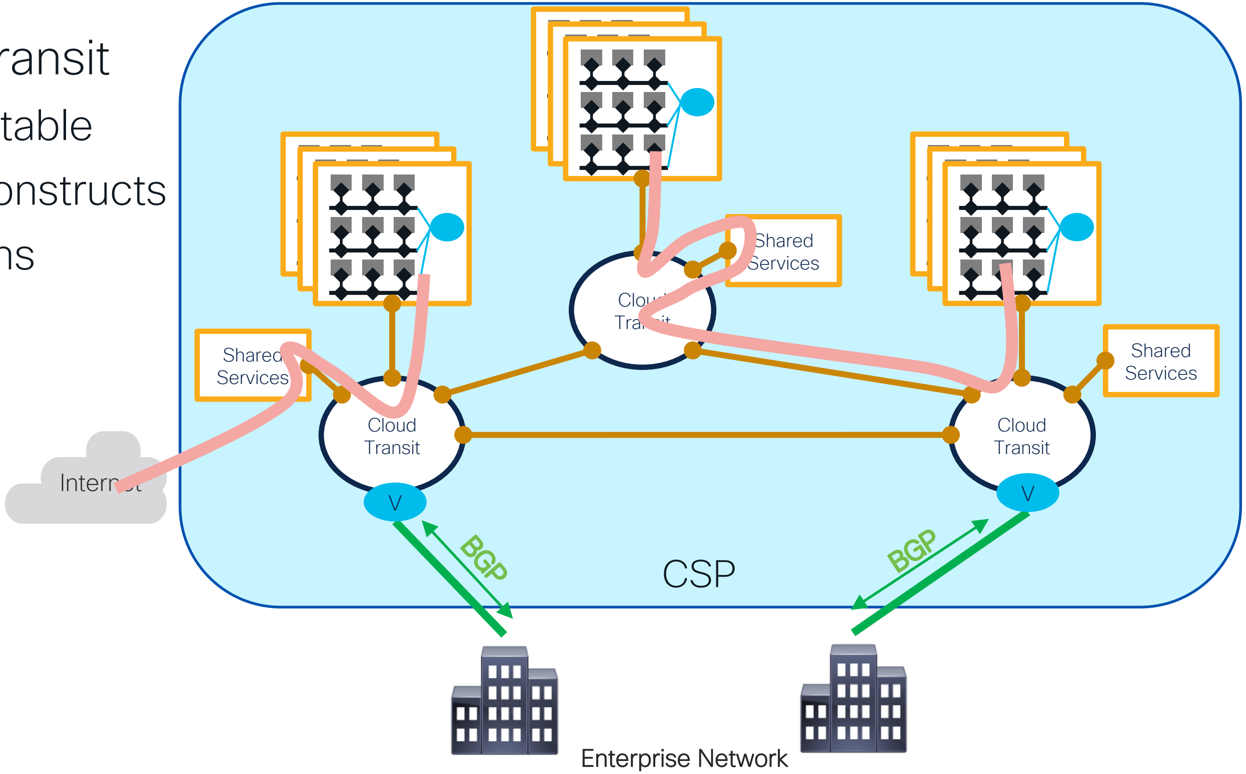
Generic Cloud Networking

- Multi-Region Cloud Transit
  - Modular design, repeatable
  - Native CSP network constructs
  - Common traffic patterns



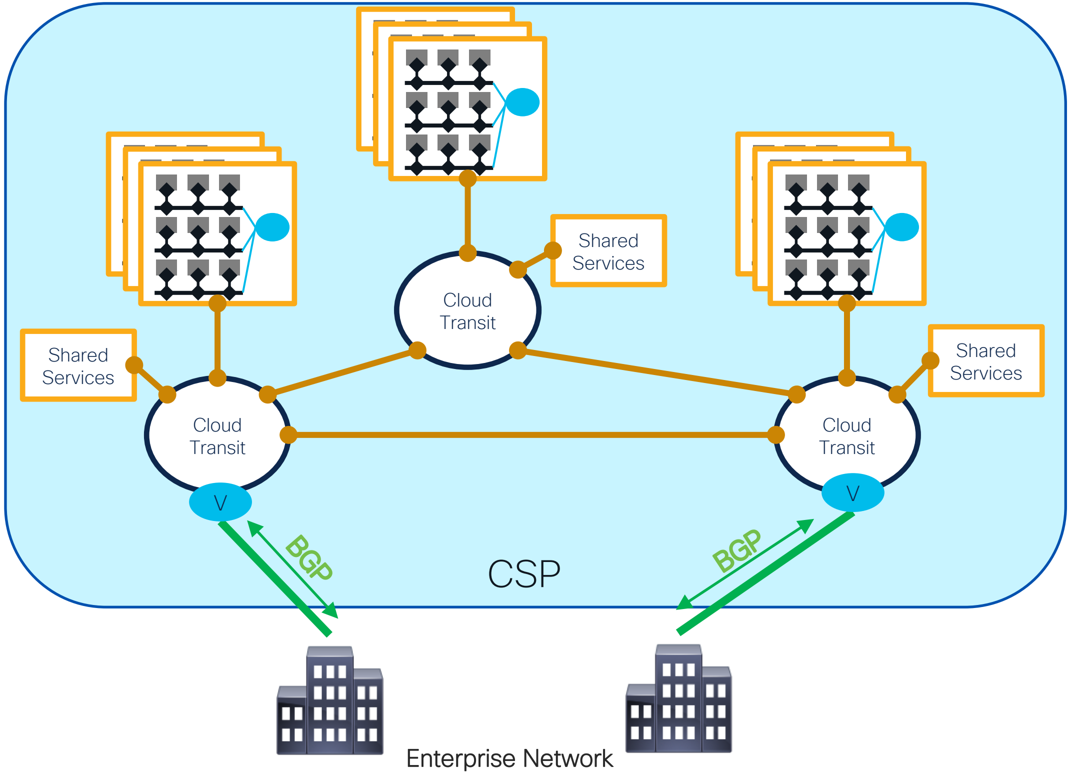
Generic Cloud Networking

- Multi-Region Cloud Transit
  - Modular design, repeatable
  - Native CSP network constructs
  - Common traffic patterns
  - External connections



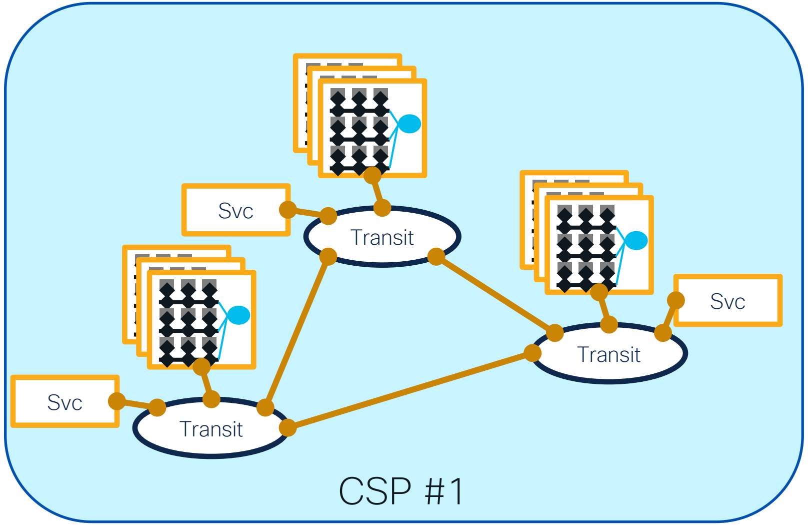
Generic Cloud Networking

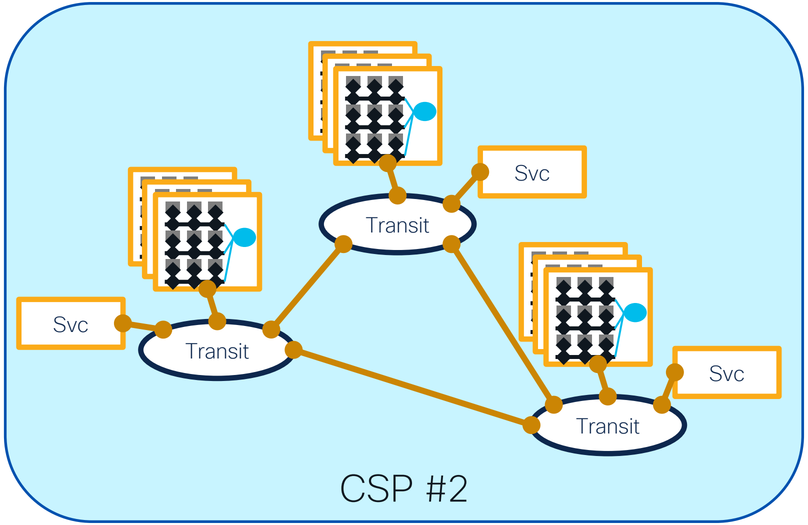
- Multi-Region Cloud Transit
  - Modular design, repeatable
  - Native CSP network constructs
  - Common traffic patterns
  - External connections
  - Limitations*
    - Limited control & visibility
    - Networking features and scaling
    - Different implementation in CSPs
    - Multiple cost factors
    - Not designed for multi-cloud



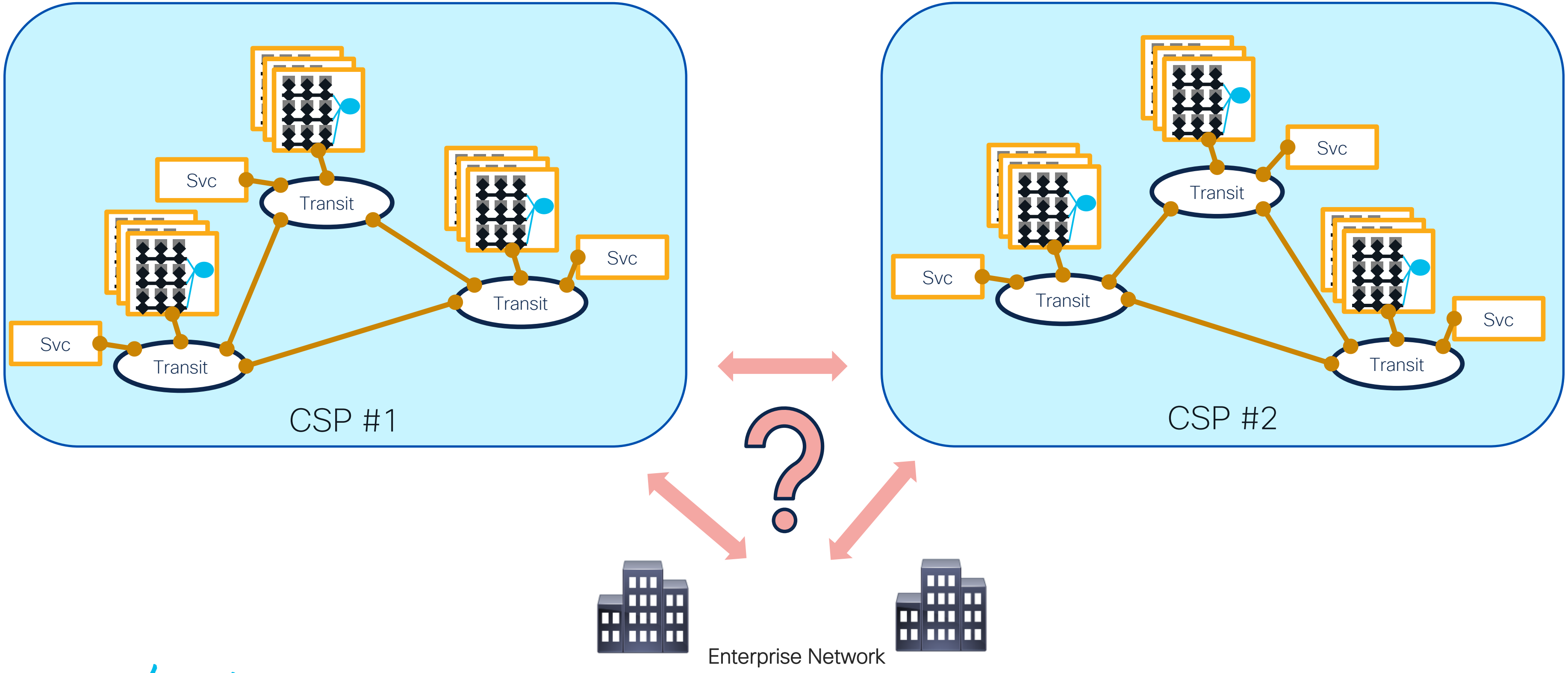
(*) CSP Networking Features are continuously evolving

Generic Cloud Networking

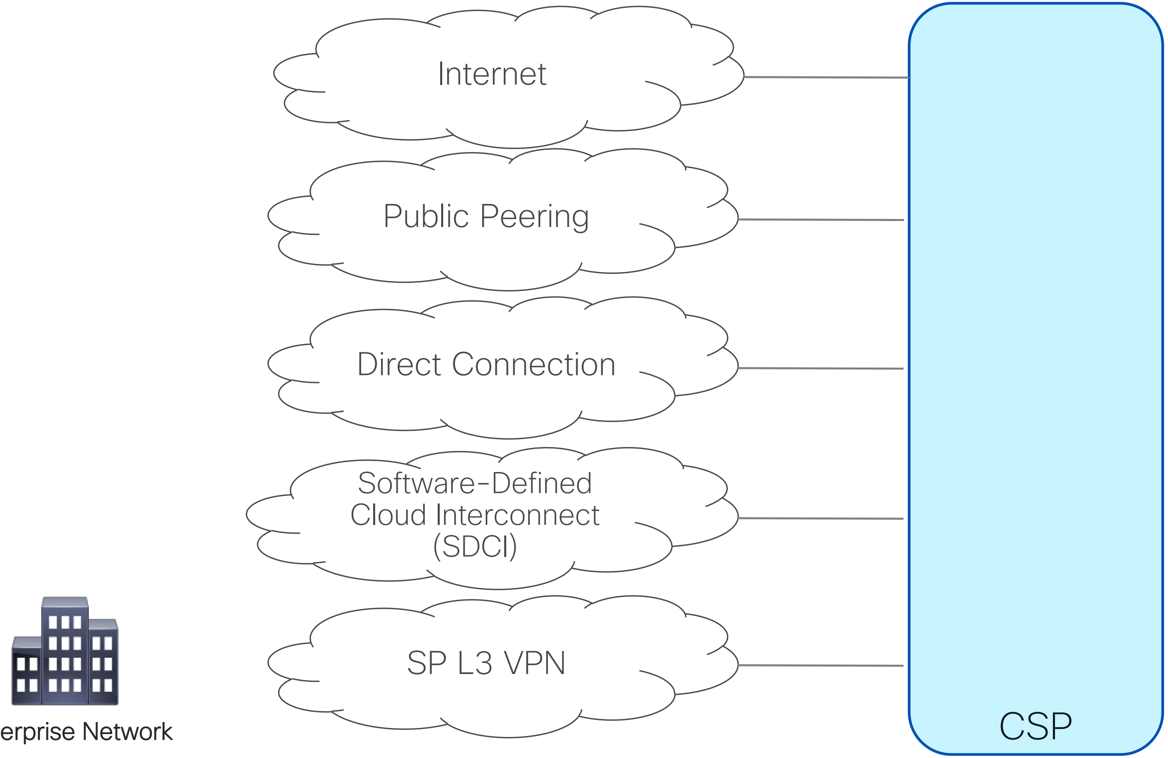




Generic Cloud Networking



Connecting to the Public Cloud


Internet

Public Peering

Direct Connection

Software-Defined Cloud Interconnect (SDCI)

SP L3 VPN

Enterprise Network

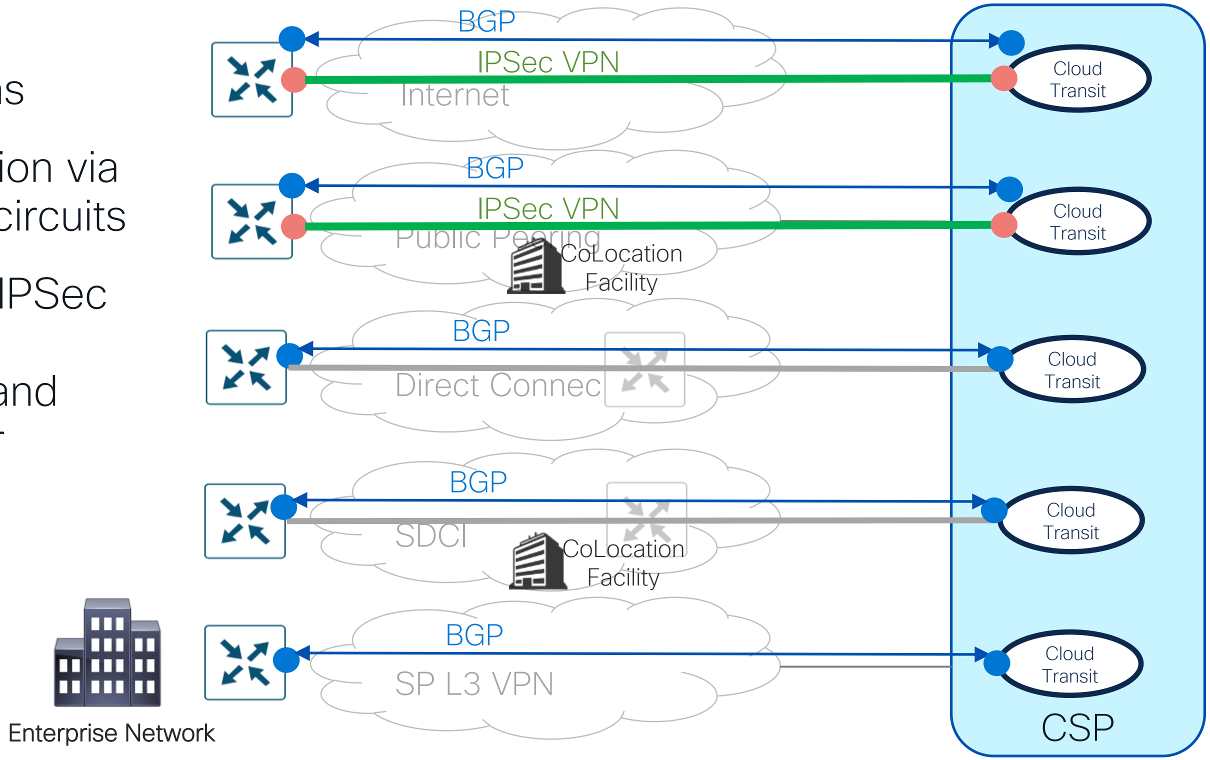
CSP

Connecting to the Public Cloud

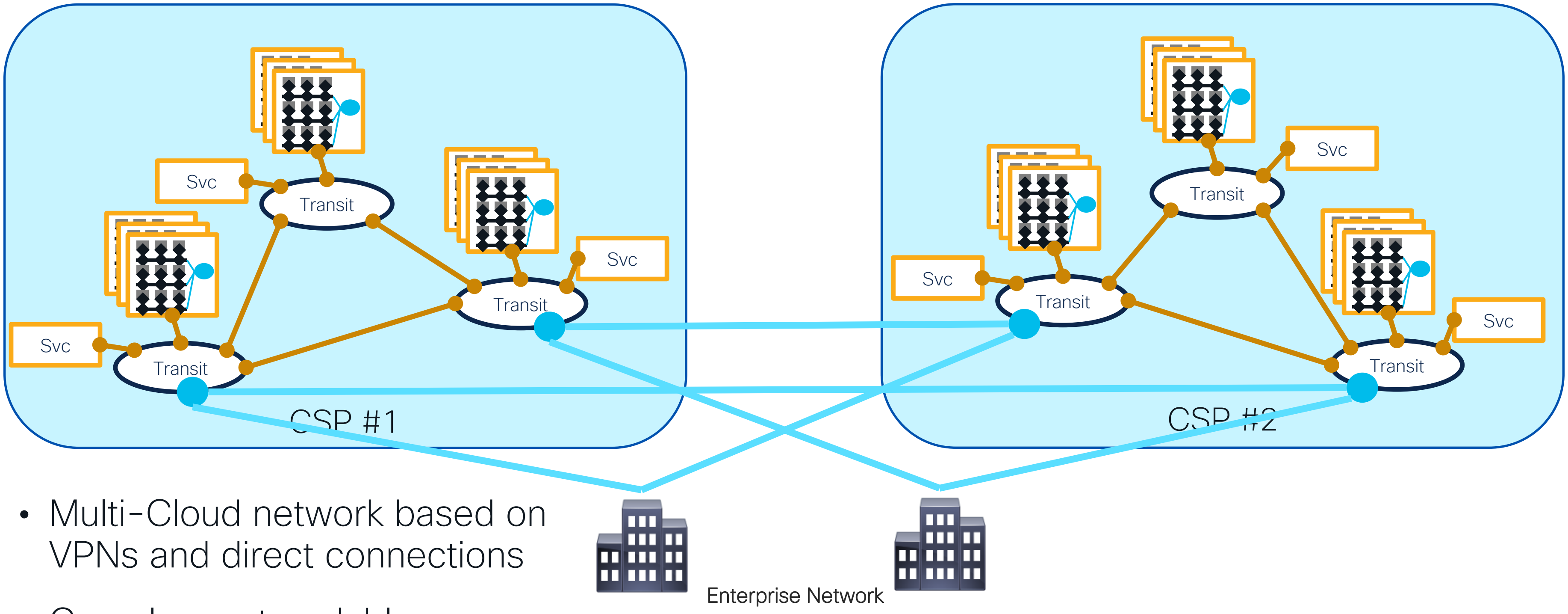
- Public & Private connection options
- Macro segmentation via multiple VPNs or circuits
- All CSPs support IPSec VPN and BGP – implementations and options may differ

● Private IP endpoint

● Public IP endpoint

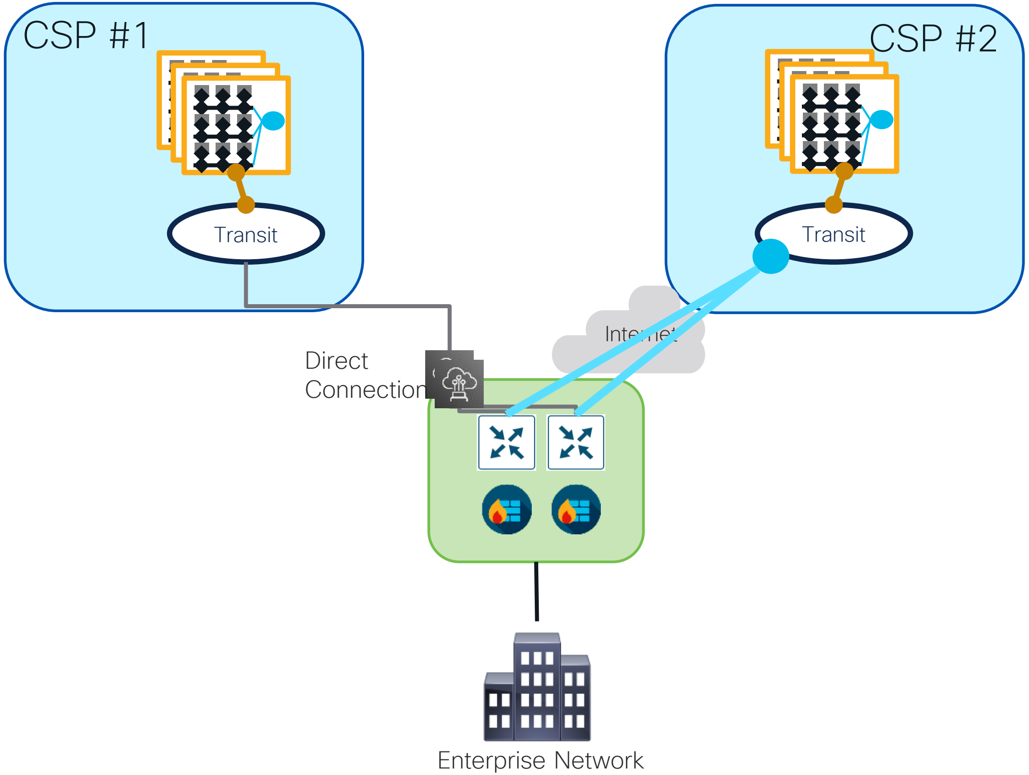


Multi-Cloud Network Topologies

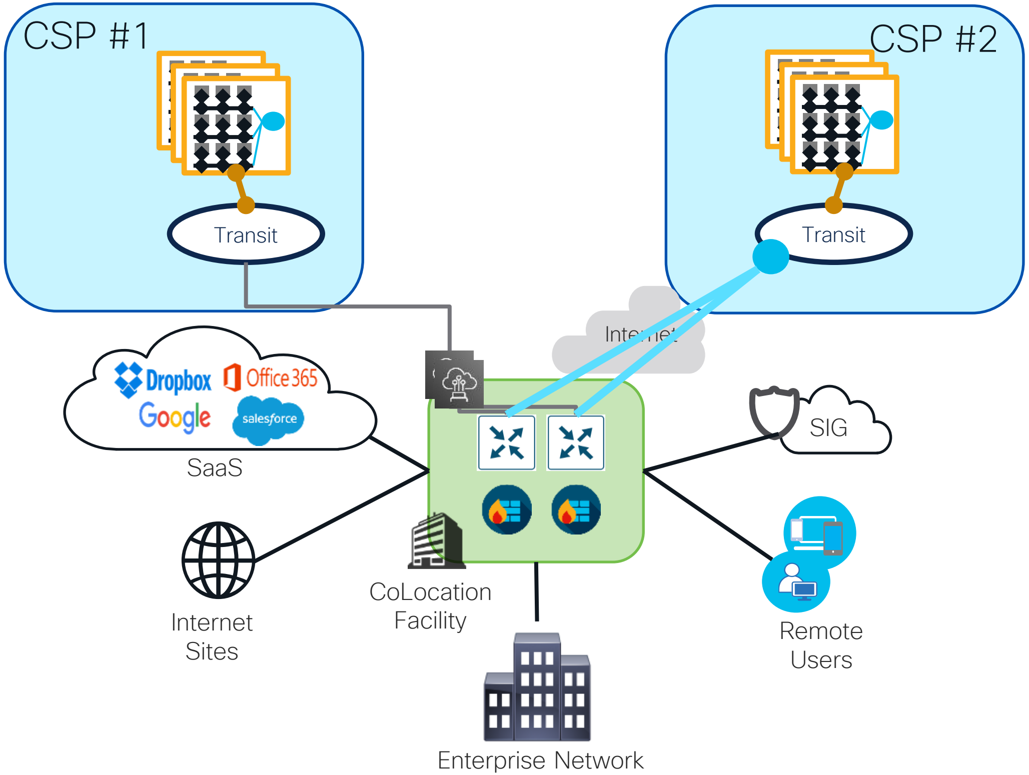


- Multi-Cloud network based on VPNs and direct connections
- Complex, not scalable

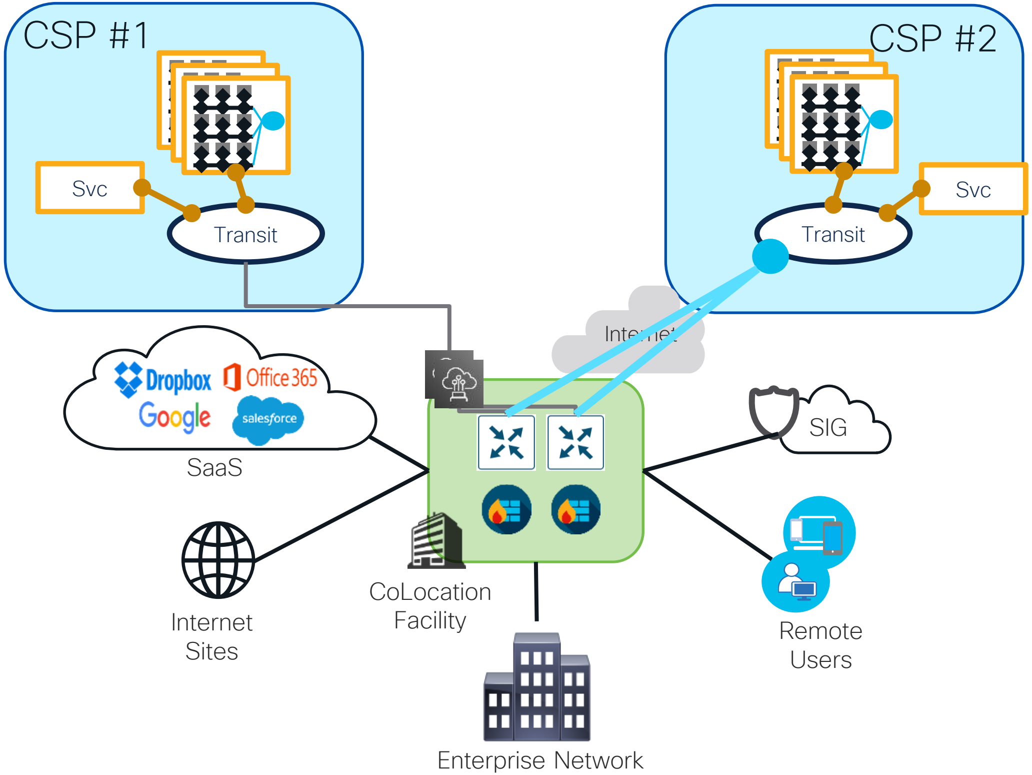
Multi-Cloud Network Topologies



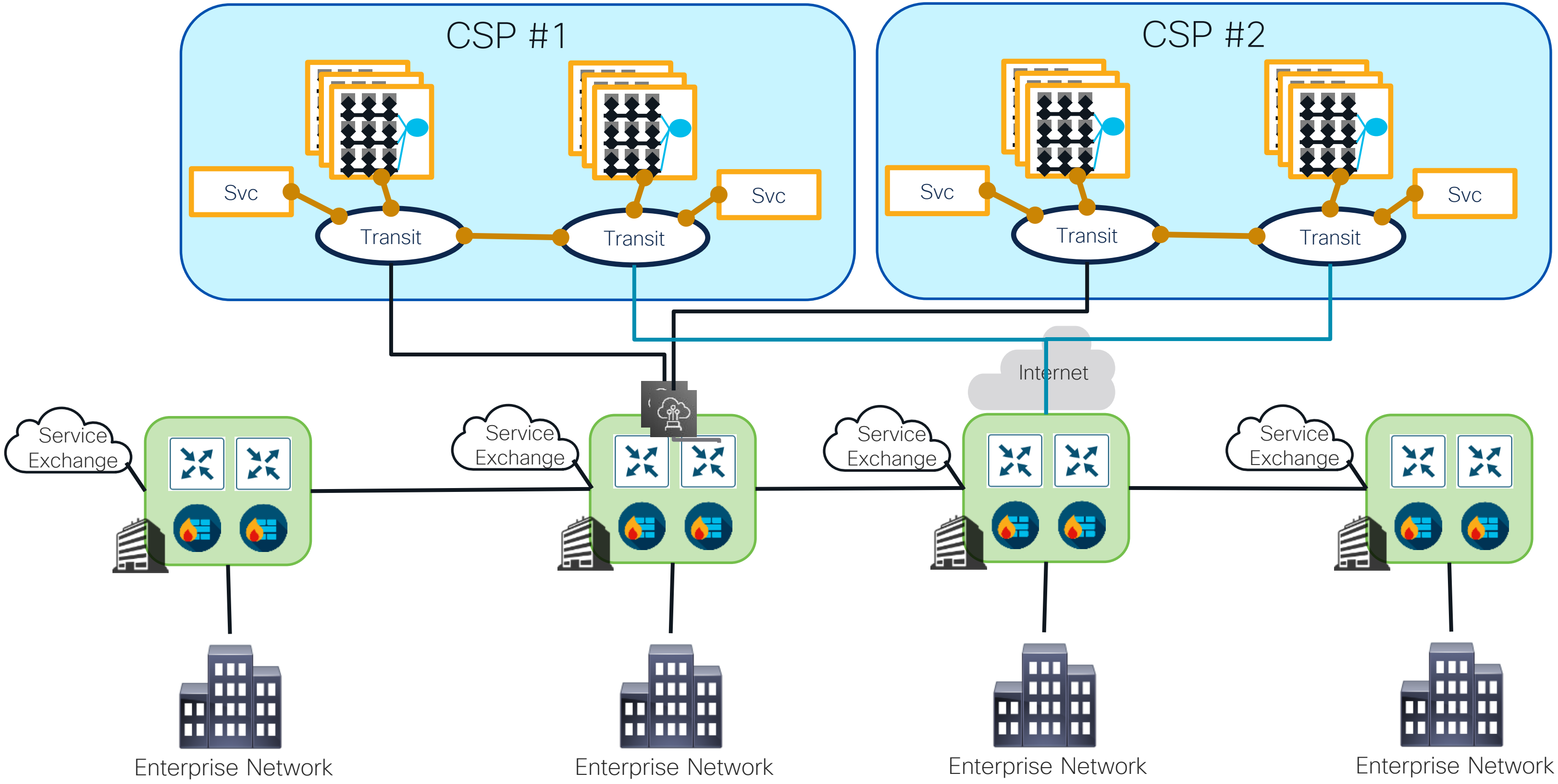
Multi-Cloud Network Topologies



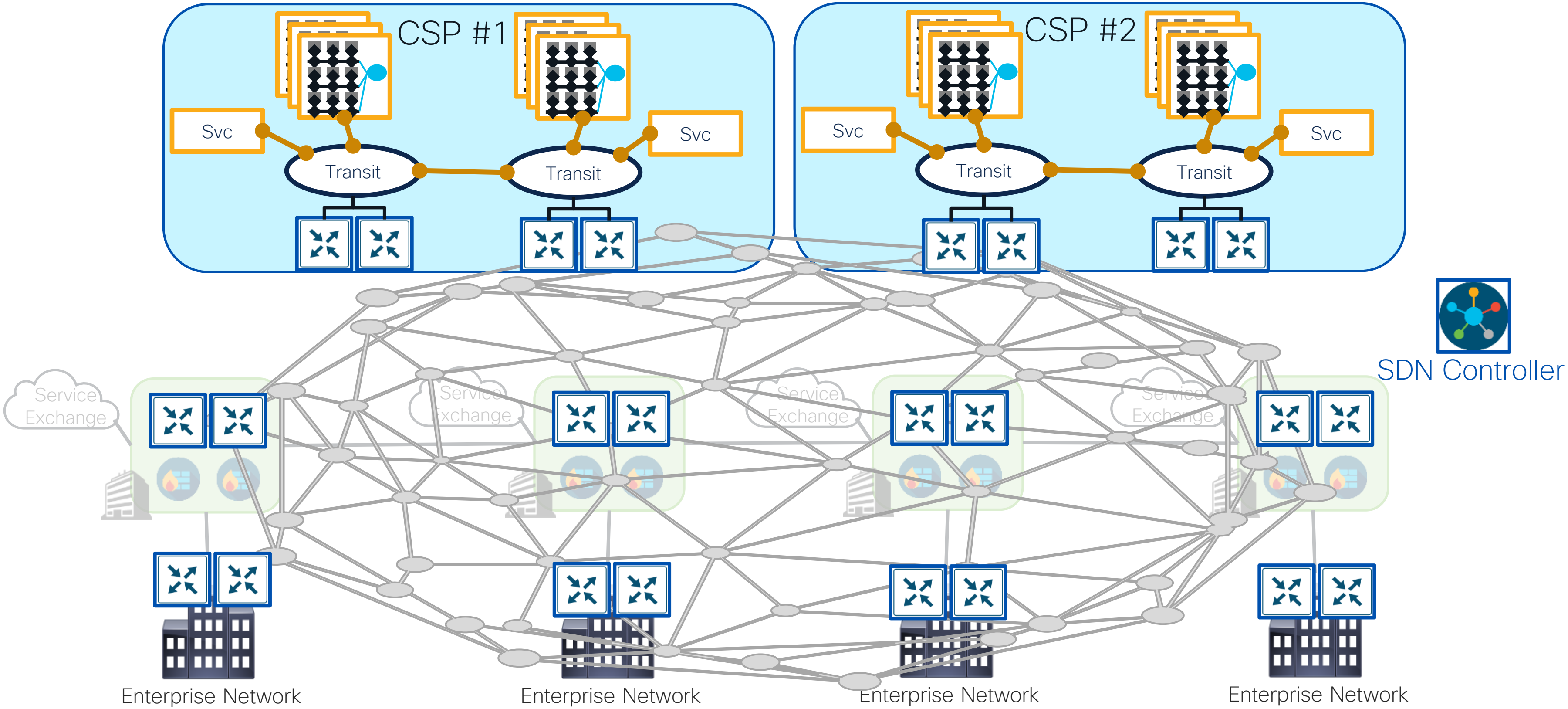
Multi-Cloud Network Topologies



Multi-Cloud Network Topologies

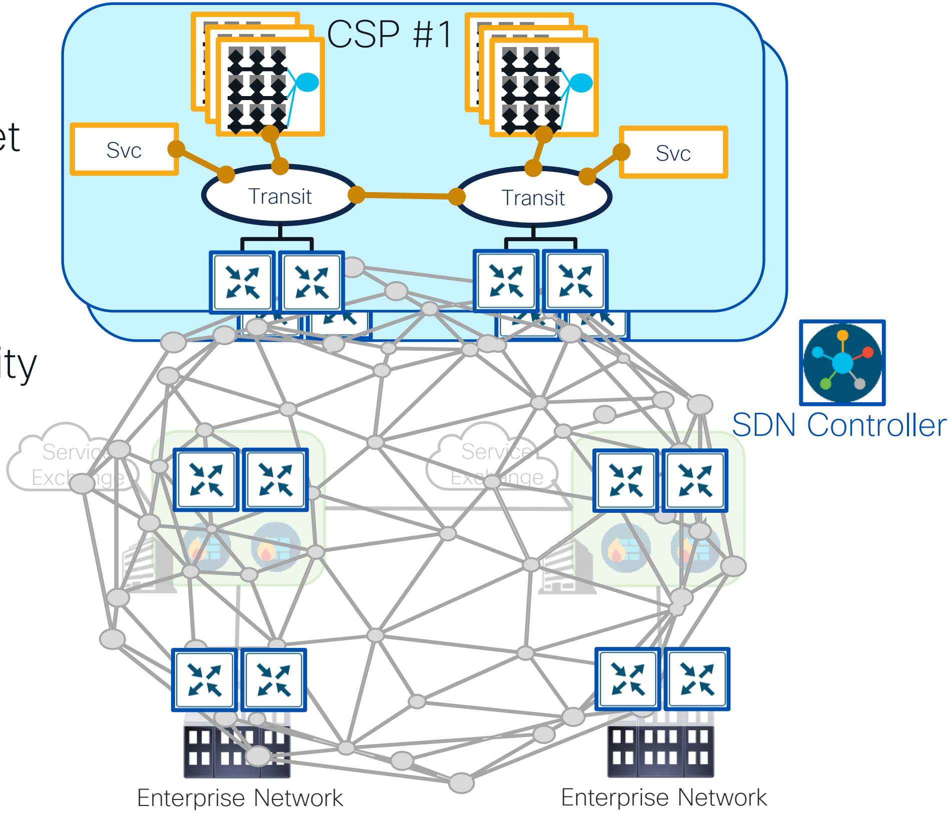


Multi-Cloud Network Topologies – SDN



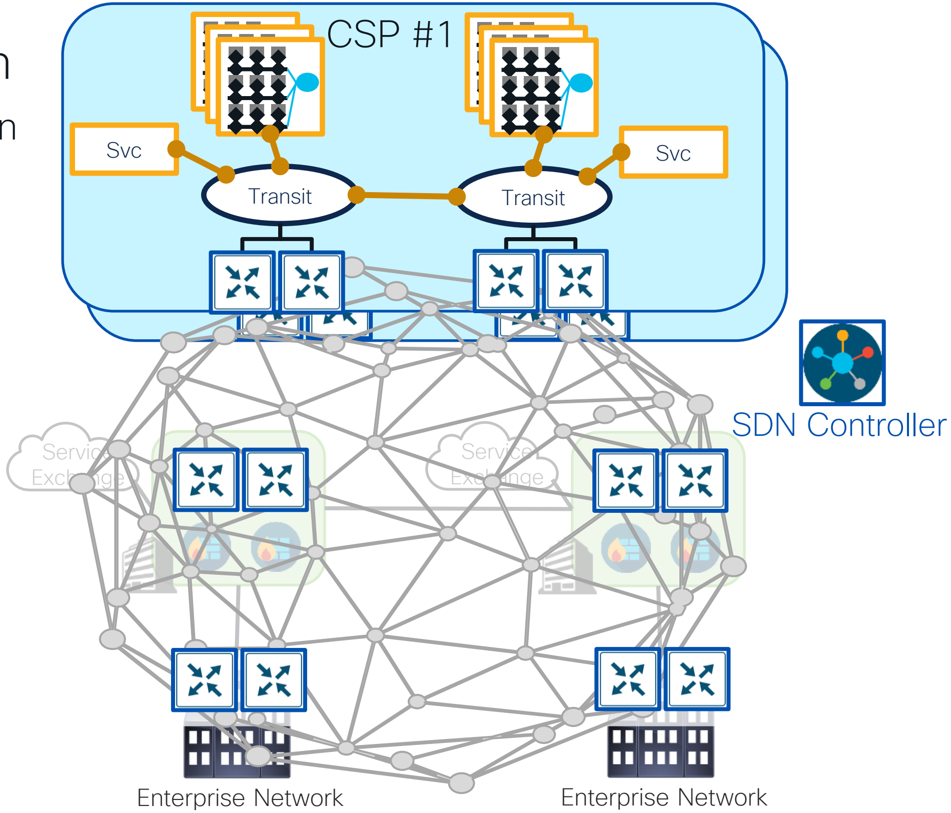
Multi-Cloud Network Topologies – SDN

- SDN Approach
  - + Match the capabilities and feature set of non-SDN solutions
  - + Support any transport, private or public
  - + Normalize the multi-cloud connectivity
  - — An additional solution
  - — Overhead and performance
  - — Programmability and integrations



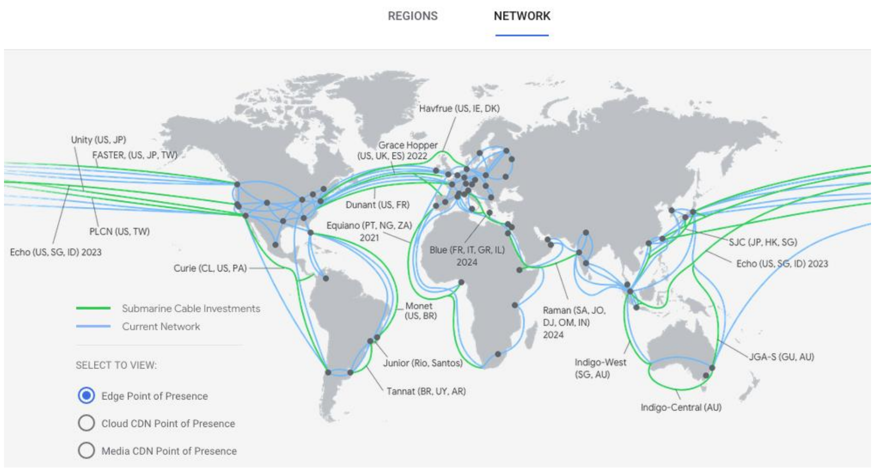
Multi-Cloud Network Topologies – SDN

- Path Monitoring and Path Selection
  - Advanced application-based path selection policies
  - Any transport: private, public, or CSP backbone
  - Underlay and overlay path measurements; detect path degradation
  - Can include app telemetry and synthetic probing data (ex: Cisco ThousandEyes)
  - Can be combined with data analytics



Multi-Cloud Network Topologies – SDN

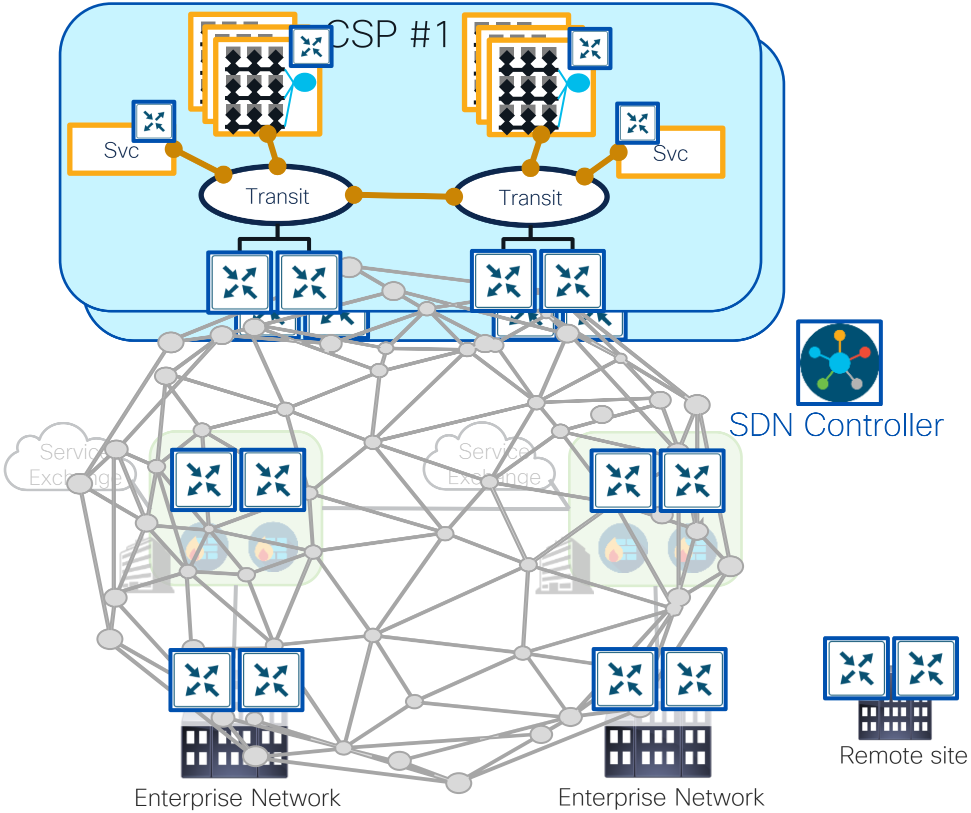
- Path Monitoring and Path Selection
  - Advanced application-based path selection policies
  - Any transport: private, public, or CSP backbone
  - Underlay and overlay path measurements; detect path degradation
  - Can include app telemetry and synthetic probing data (ex: Cisco ThousandEyes)
  - Can be combined with data analytics



GCP Global Network

Multi-Cloud Network Topologies – SDN

- SDN Extensions
  - Extend to the CSP virtual data centers
  - Tighter end-to-end control and visibility
  - Possibility to extend/integrate at the micro-services layer
- SDN Flexibility
  - Policy-based hierarchical topology
  - Adapt to special situations, ex: large or critical remote sites
- End-to-end segmentation
  - Macro & micro segmentation



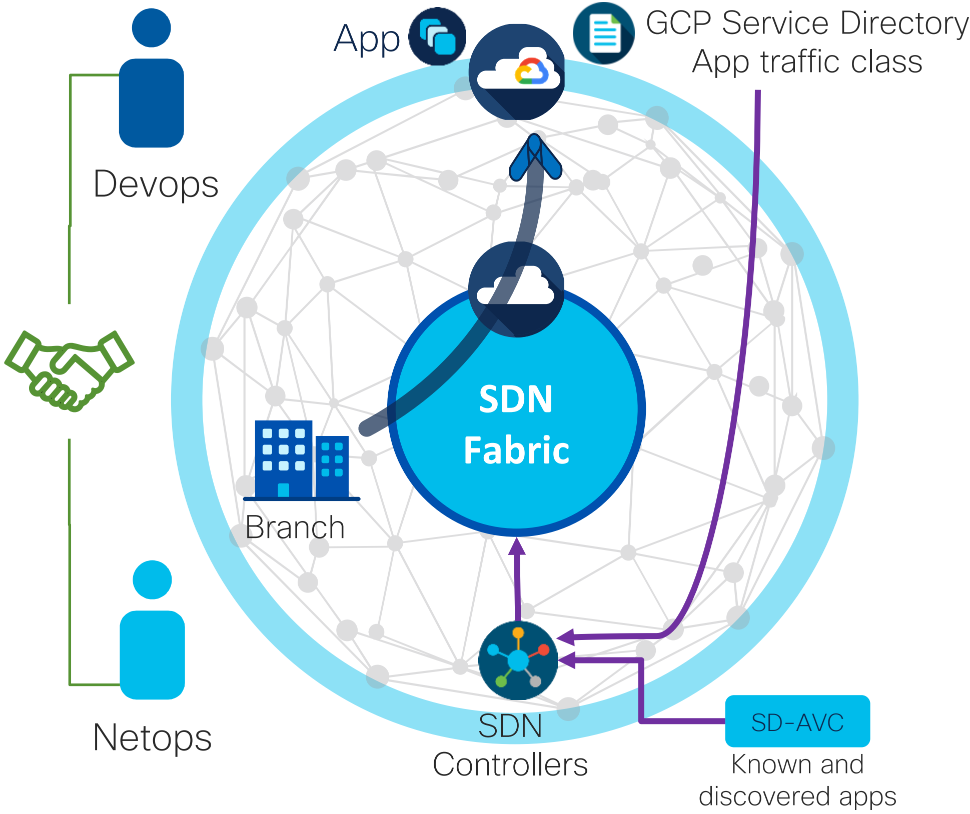
SDN Automatic Application Discovery

Use Case Summary

Devops: register cloud apps in GCP Service Directory.
App metadata includes traffic type or class.

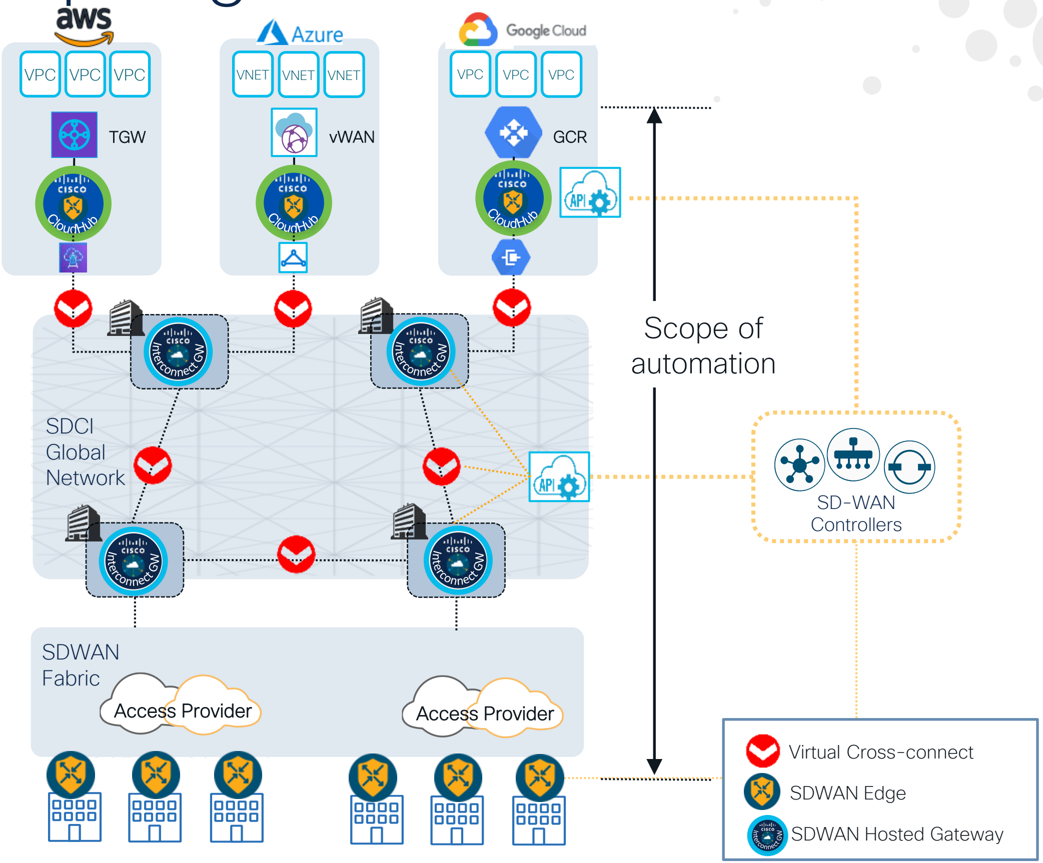
Netops: create and maintain SDN policies for the different traffic types/classes.

SDN controllers: read apps from Service Directory; distribute policies and app info to the network.



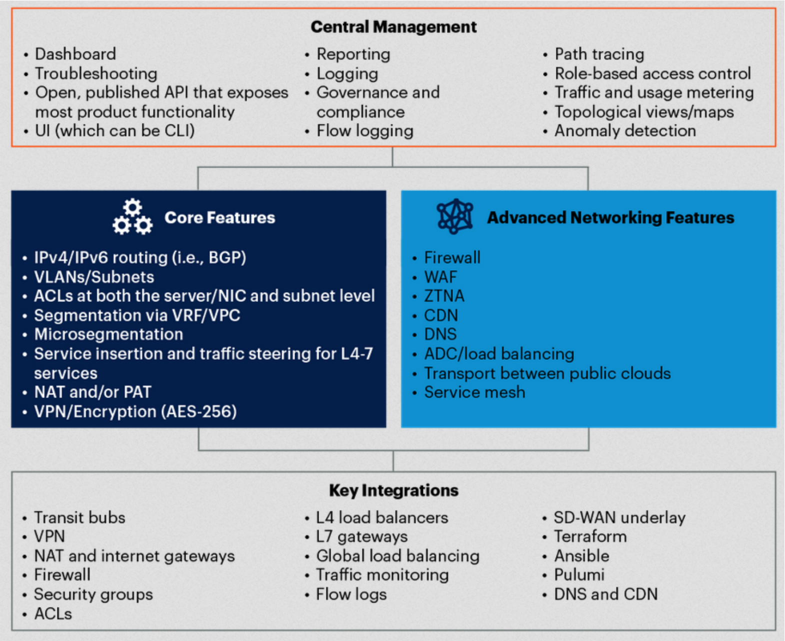
Multi-Cloud Network Topologies – SDN

- Programmability
  - Programmable, Automated, On-demand WAN Core network-as-a-service
  - Automation of SDCI service and CSP connectivity
  - Controller-based orchestration and overlay topology
  - Full segmentation, traffic engineering policy control



Multi-Cloud Network Topologies – SDN

- Feature Set for Multi-Cloud



Central Management

- Dashboard
- Troubleshooting
- Open, published API that exposes most product functionality
- UI (which can be CLI)
- Reporting
- Logging
- Governance and compliance
- Flow logging
- Path tracing
- Role-based access control
- Traffic and usage metering
- Topological views/maps
- Anomaly detection

Core Features

- IPv4/IPv6 routing (i.e., BGP)
- VLANs/Subnets
- ACLs at both the server/NIC and subnet level
- Segmentation via VRF/VPC
- Microsegmentation
- Service insertion and traffic steering for L4-7 services
- NAT and/or PAT
- VPN/Encryption (AES-256)

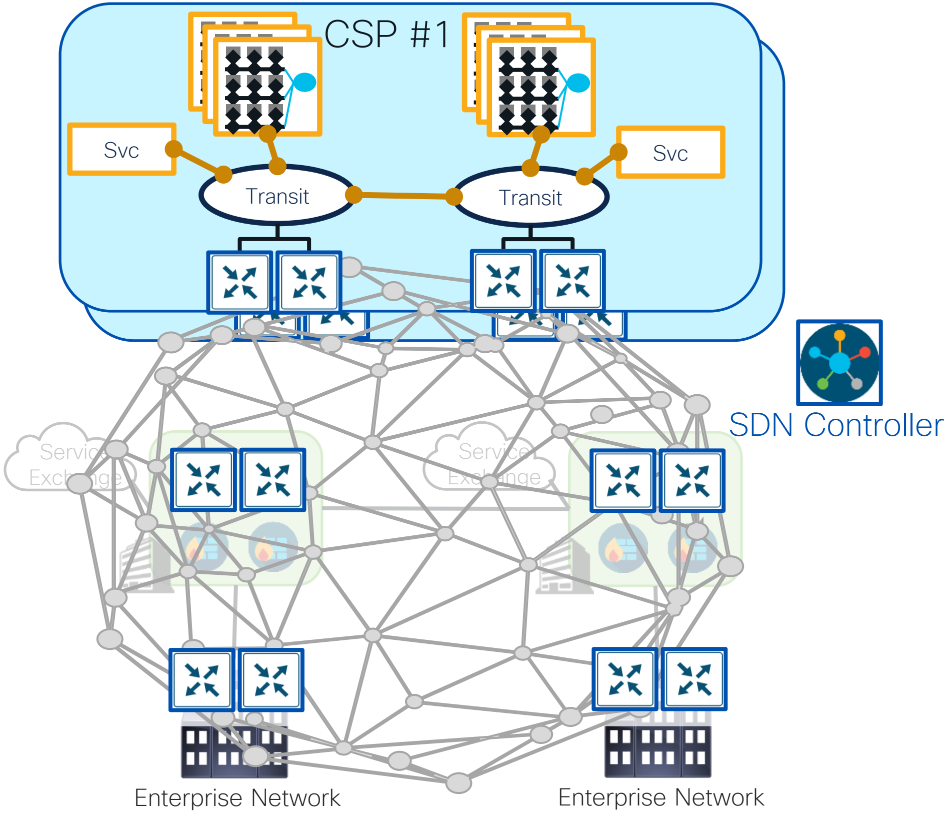
Advanced Networking Features

- Firewall
- WAF
- ZTNA
- CDN
- DNS
- ADC/load balancing
- Transport between public clouds
- Service mesh

Key Integrations

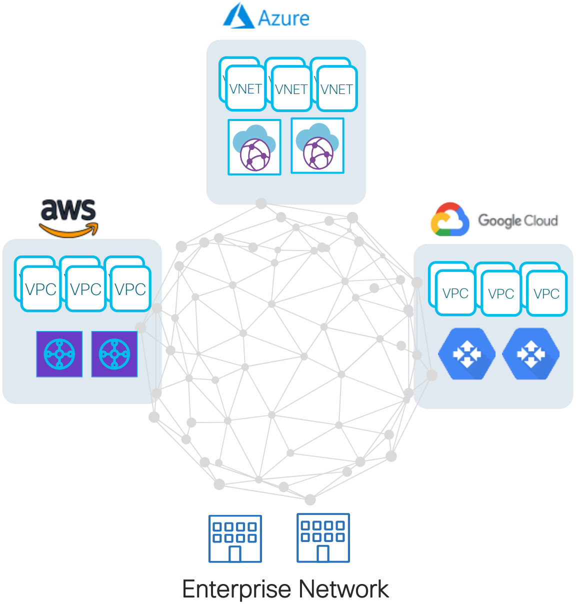
- Transit bubs
- VPN
- NAT and internet gateways
- Firewall
- Security groups
- ACLs
- L4 load balancers
- L7 gateways
- Global load balancing
- Traffic monitoring
- Flow logs
- SD-WAN underlay
- Terraform
- Ansible
- Pulumi
- DNS and CDN

Source: Gartner



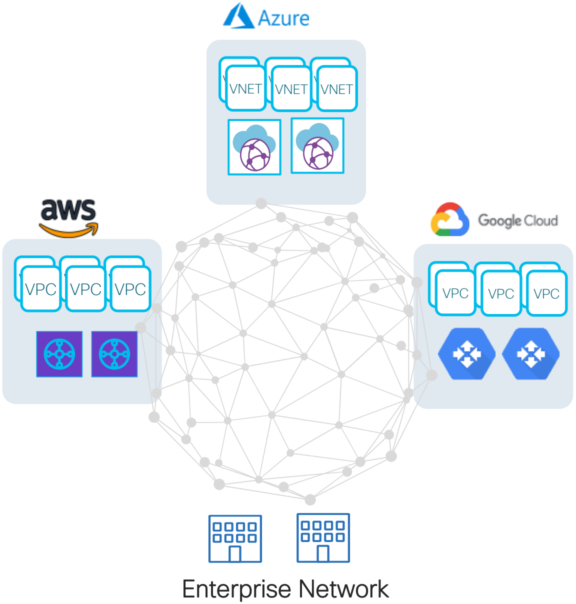
Multi-Cloud Networking

- Is there a case for SDN in Multi-Cloud?
  - + Global network, any location any service any transport
  - + Advanced features & policy engine
  - + Programmable, easy to consume
  - – Suitable non-SDN solution for the requirements
  - – Evolution of native Cloud services and networking
  - – Additional complexity, scalability



Multi-Cloud Networking

- What does the Artificial Intelligence say?

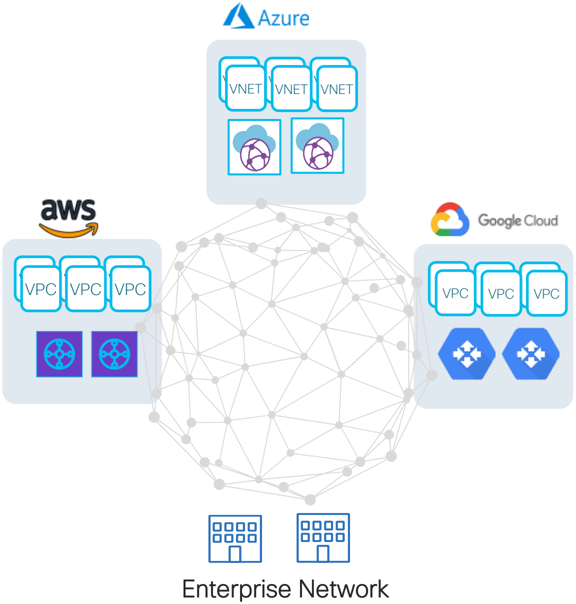


Multi-Cloud Networking

- What does the Artificial Intelligence say?

ChatGPT AI (Feb'2023):

Q) *Best approach for multi-cloud networking?*



Multi-Cloud Networking

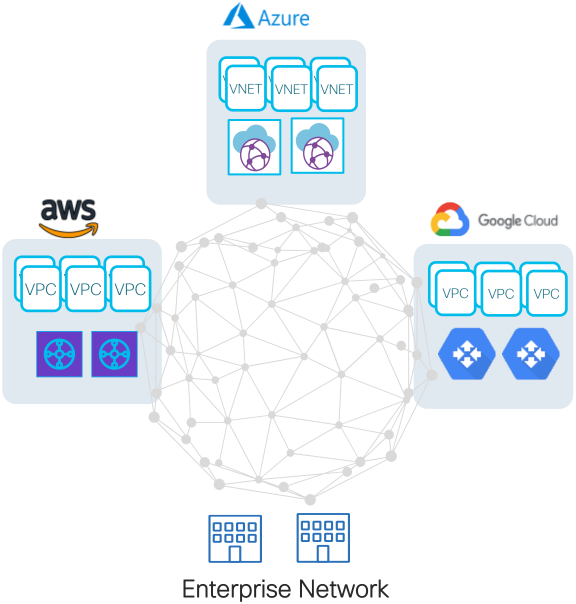
- What does the Artificial Intelligence say?

ChatGPT AI (Feb'2023):

Q) *Best approach for multi-cloud networking?*

"A commonly recommended approach for multi-cloud networking is to implement a software-defined network (SDN) solution, such as an overlay network, that abstracts and centralizes network management and allows for consistent policy enforcement across different clouds. (…)".

"Software-defined networking (SDN) solutions for multi-cloud networking have some potential drawbacks that need to be considered: complexity, interoperability, latency, scalability, security, cost."



Reference CiscoLive Sessions

- CL2023
  - BRKENT-2060: Cisco SD-WAN Cloud onramp for Multicloud
  - BRKENT-3297: Multi-Cloud SD-WAN Design
  - BRKDCN-2653: Cisco Cloud Network Controller – Hybrid Multi-Cloud Infrastructure and Policy Automation enabler
  - BRKENT-2809: Enterprise Direct Cloud Connectivity with Catalyst 8500 Series
- CL2022
  - BRKENT-2157: Securing Private Links to Public Cloud Providers
  - BRKAPP-1002: Cloud Bound, Key differences in Public Cloud Connectivity Architectures
  - BRKENT-2001: Secure SD-WAN and Cloud Edge Transformation
  - BRKDCN-2221: Architecting Hybrid / Multi-Cloud Infrastructures

Complete your 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 (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.

The bridge to possible

Thank you

cisco Live!
ALL IN