7 Steps: Master the art of unifying Multicloud secure Connectivity and Design

Cisco SD-WAN + Multicloud Defense

Prashant Tripathi
Global Principal Architect SD-WAN & Multi-Cloud

Praveen Patnala
Sr. Director of Engineering Cisco Security

BRKENT-2283

Webex App

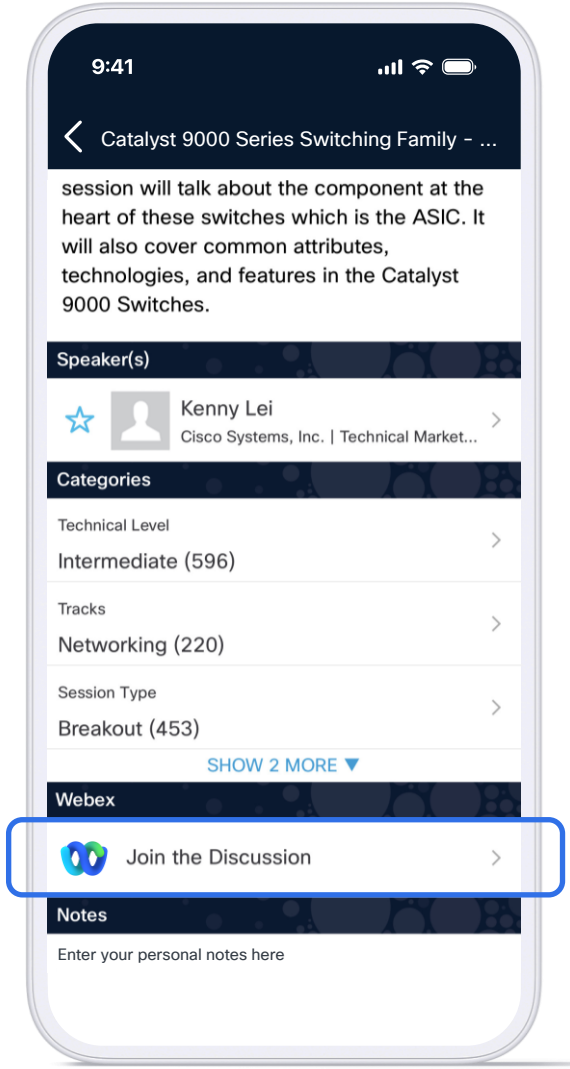
Questions?

Use Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 27, 2026.



Agenda

01 Cloud Networking & Security use case and Challenges

02 Cisco Recommended and Automated Cloud Networking Architecture

03 Security insertion in the Multi-Cloud

Cloud Networking Use case and Challenges

Hybrid Cloud Connectivity

Extend on-premises to public clouds for workload migration & disaster recovery

Multi-Region Global Networking

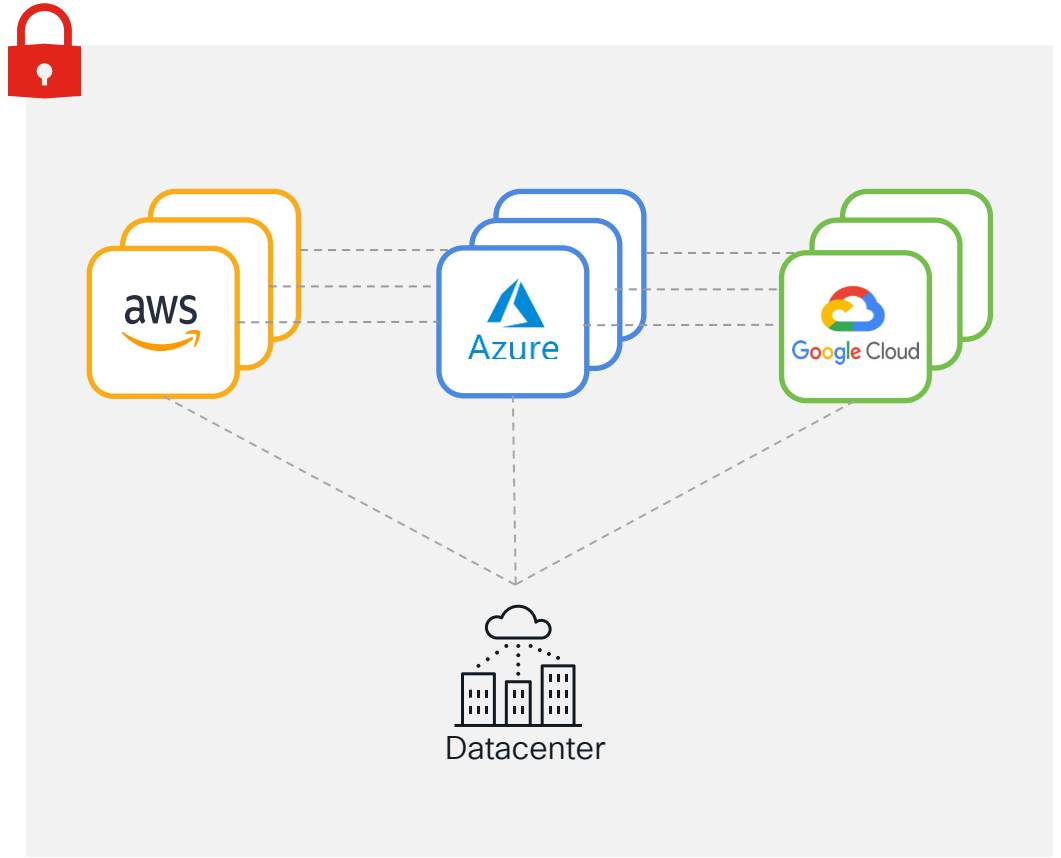
Deploy applications across regions to reduce latency and meet data sovereignty requirements

Multi-Cloud Interconnect

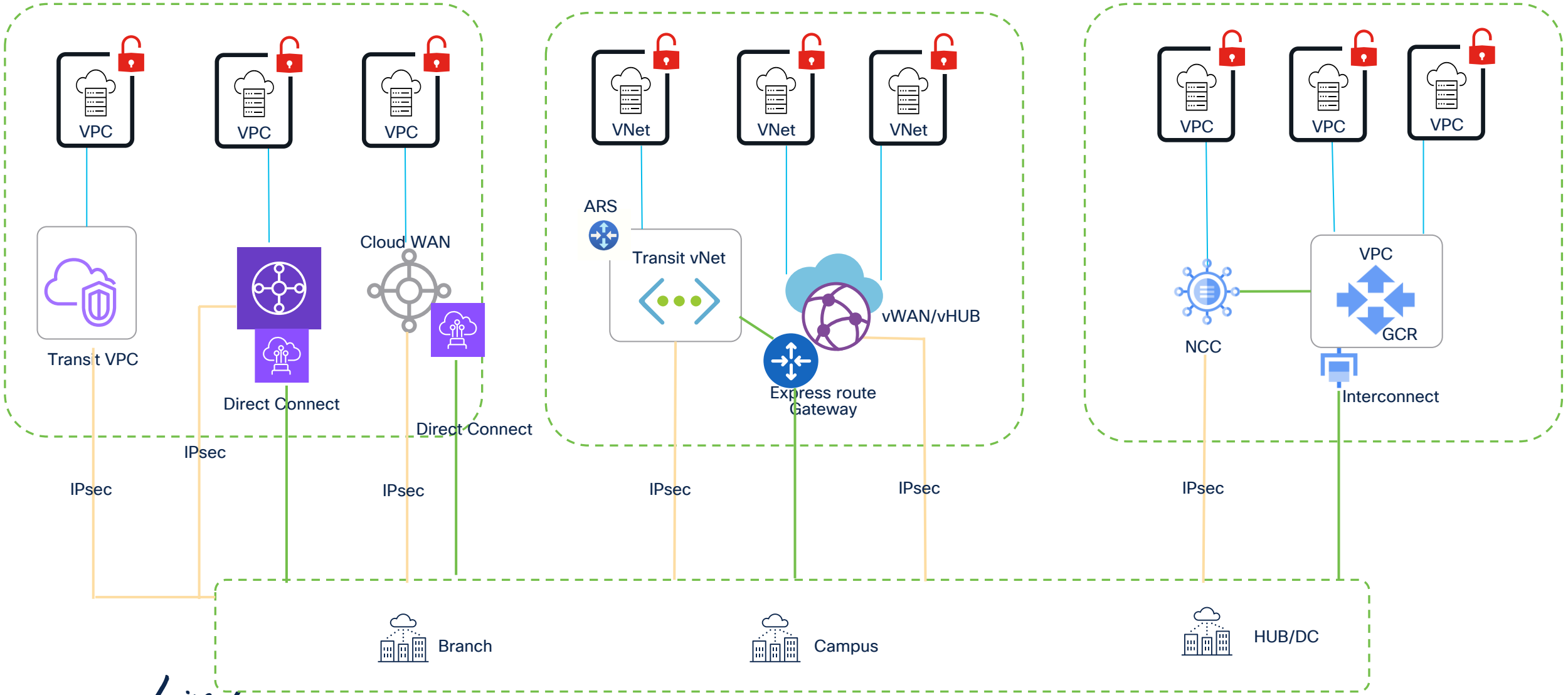
Leverage best-of-breed services and interconnect

Security

Enforce consistent security policies, micro-segmentation across hybrid/multi-cloud environments



Cloud Networking Use case and Challenges



Cisco Multi-Cloud Networking use cases

Cloud Networking & Security Use cases

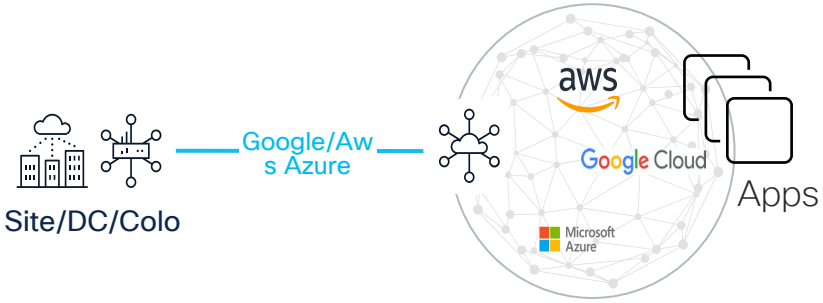
Cisco SD-WAN & Multicloud Defense

= Cisco SD-WAN virtual router hosted at Cloud Service Provider POP

= Cisco SD-WAN router on-premises

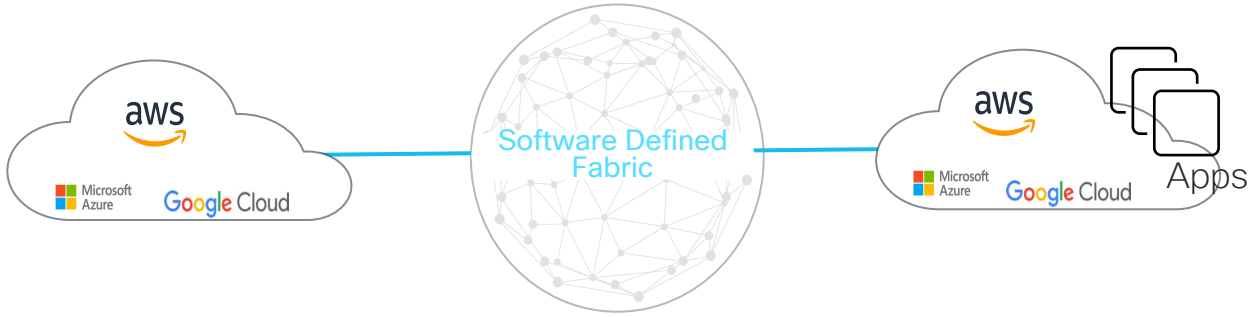
= Multicloud Defense

Hybrid Cloud Connectivity

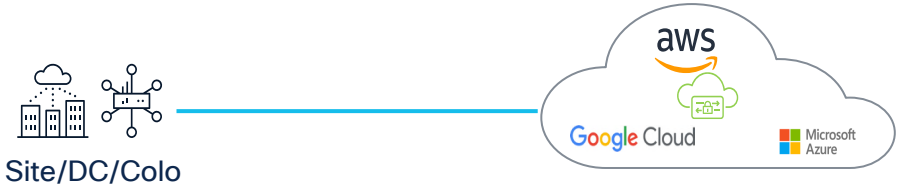


Multi-Region Global Networking

Multi-Cloud Interconnect

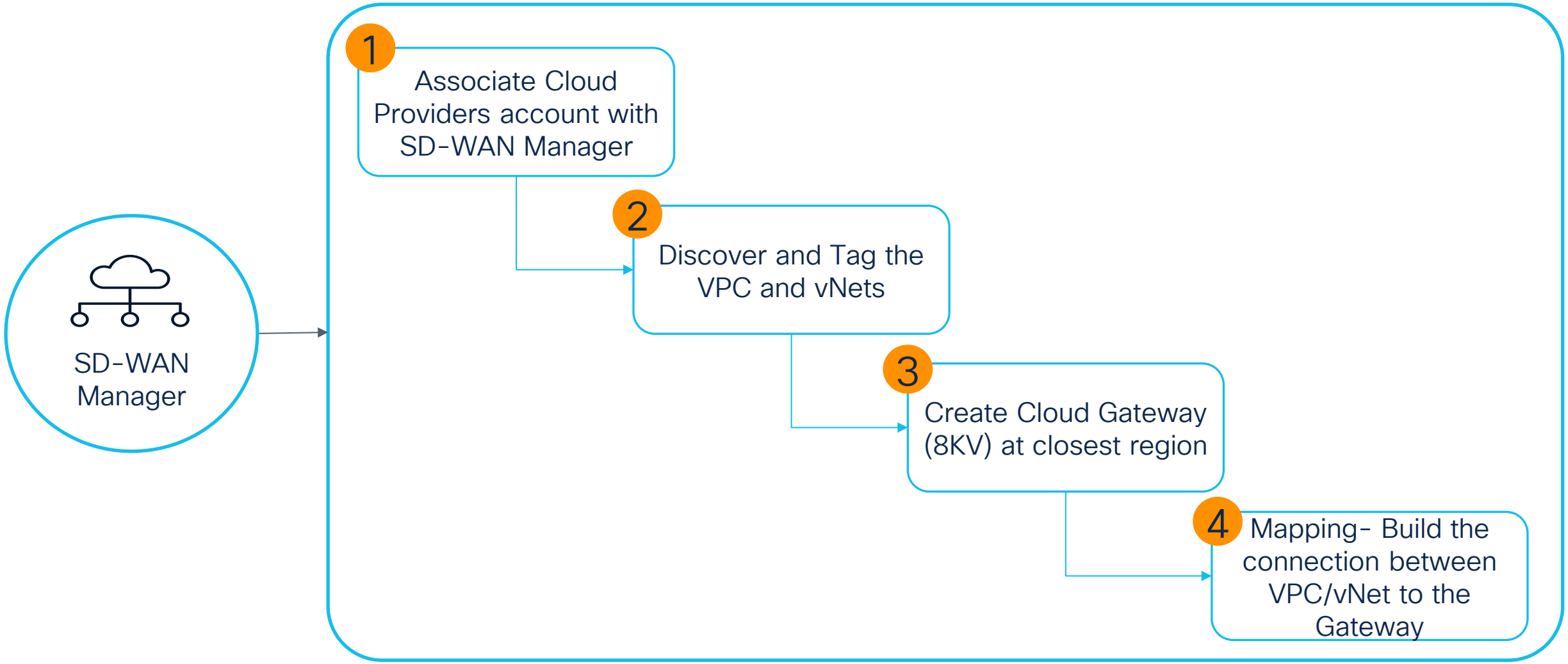


Security

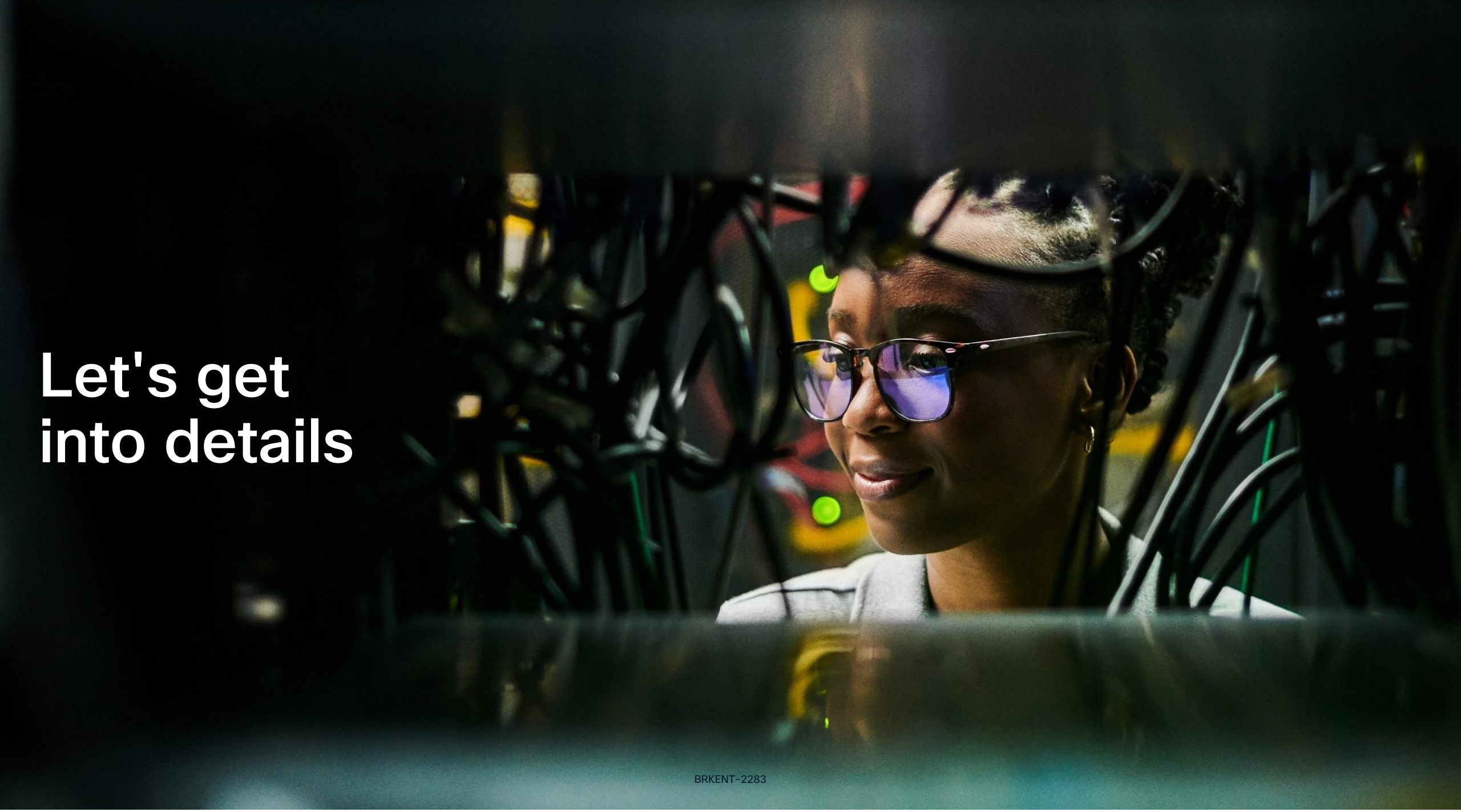


Multicloud Networking Workflow

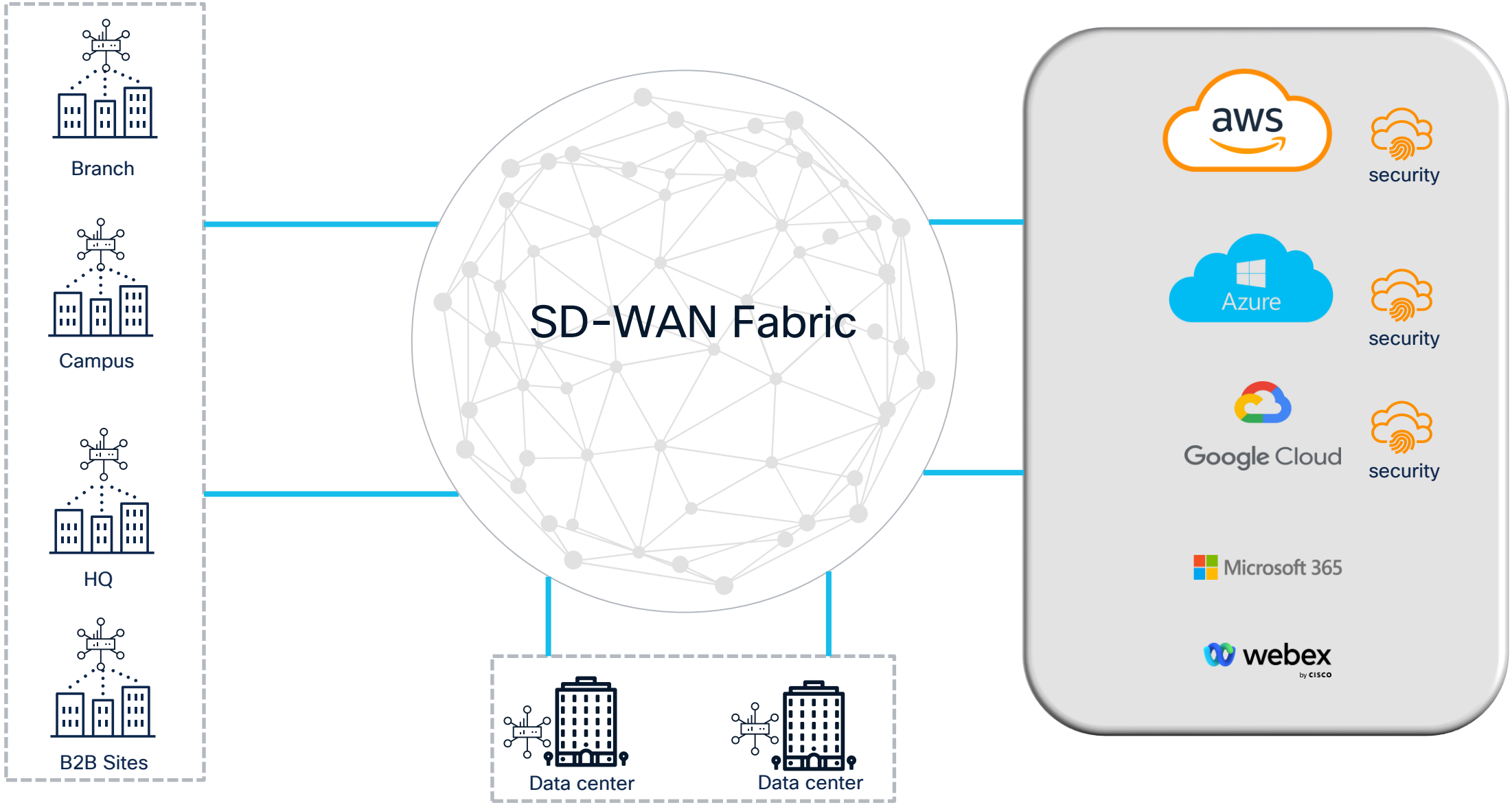
Secure Connectivity achieved in minutes....



Let's get into details



Architecture Option – Direct access to the Cloud



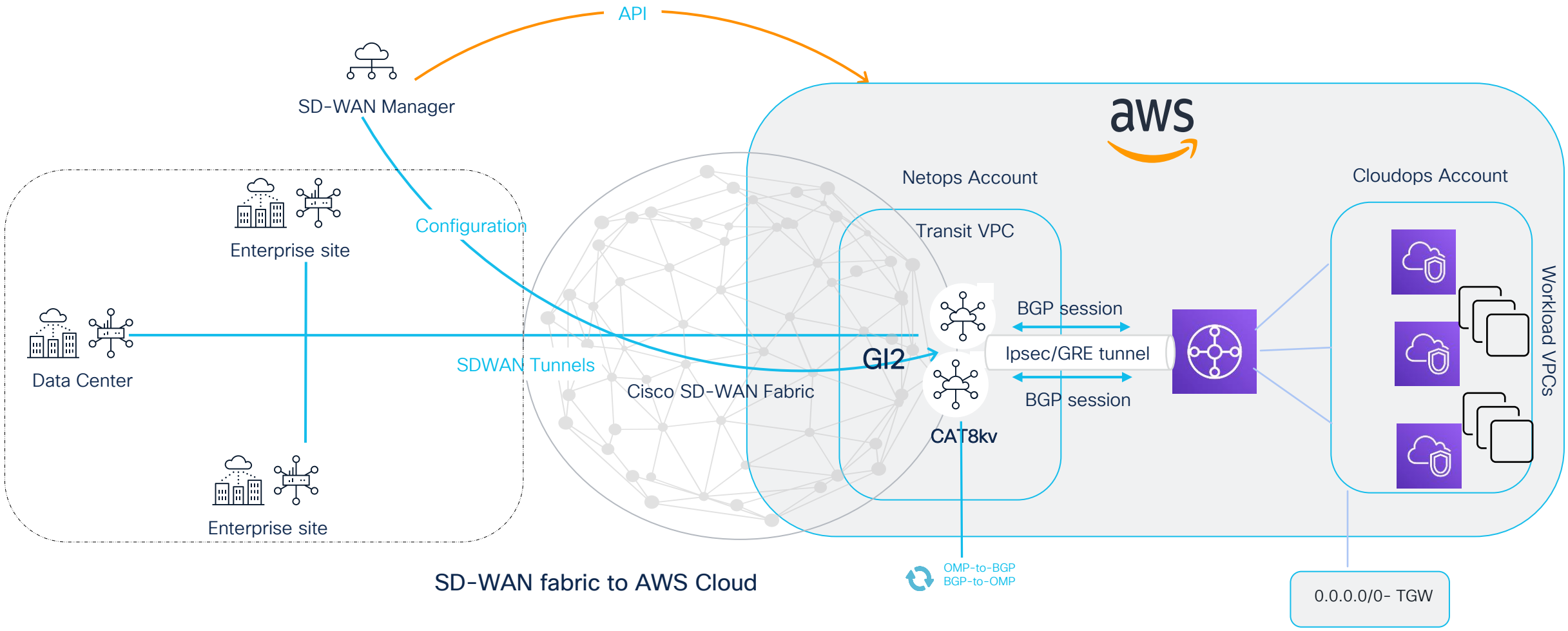
cisco

Direct Cloud Access - AWS

Hybrid Cloud Connectivity

Hybrid Cloud Connectivity – TGW

SD-WAN Native Integration using **IKE Ipsec/ GRE** between Transit VPC cat8kv/vMX and Transit Gateway

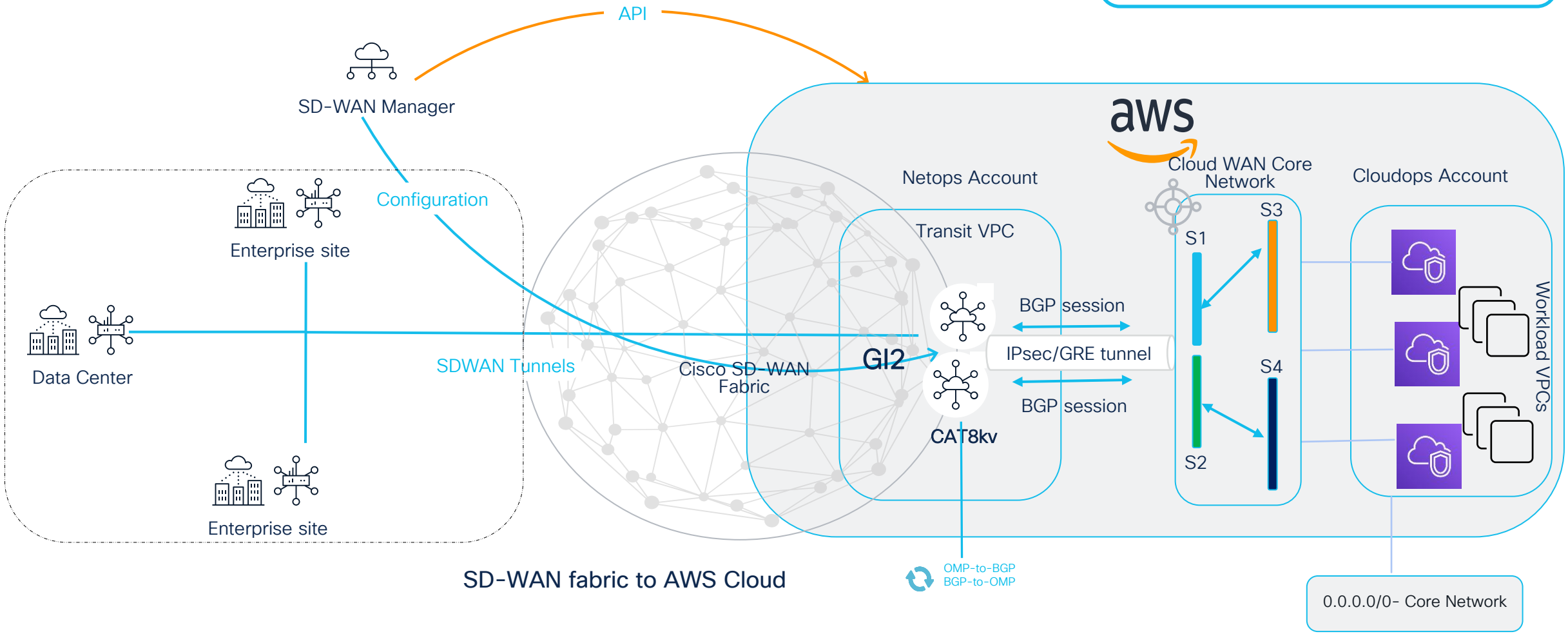


SD-WAN fabric to AWS Cloud

Simple | Automated | Secure

Hybrid Cloud Connectivity – Cloud WAN

SD-WAN Native Integration using IKE Ipsec or CONNECT (GRE) between Transit VPC C8Kvs/vMx and Cloud WAN.

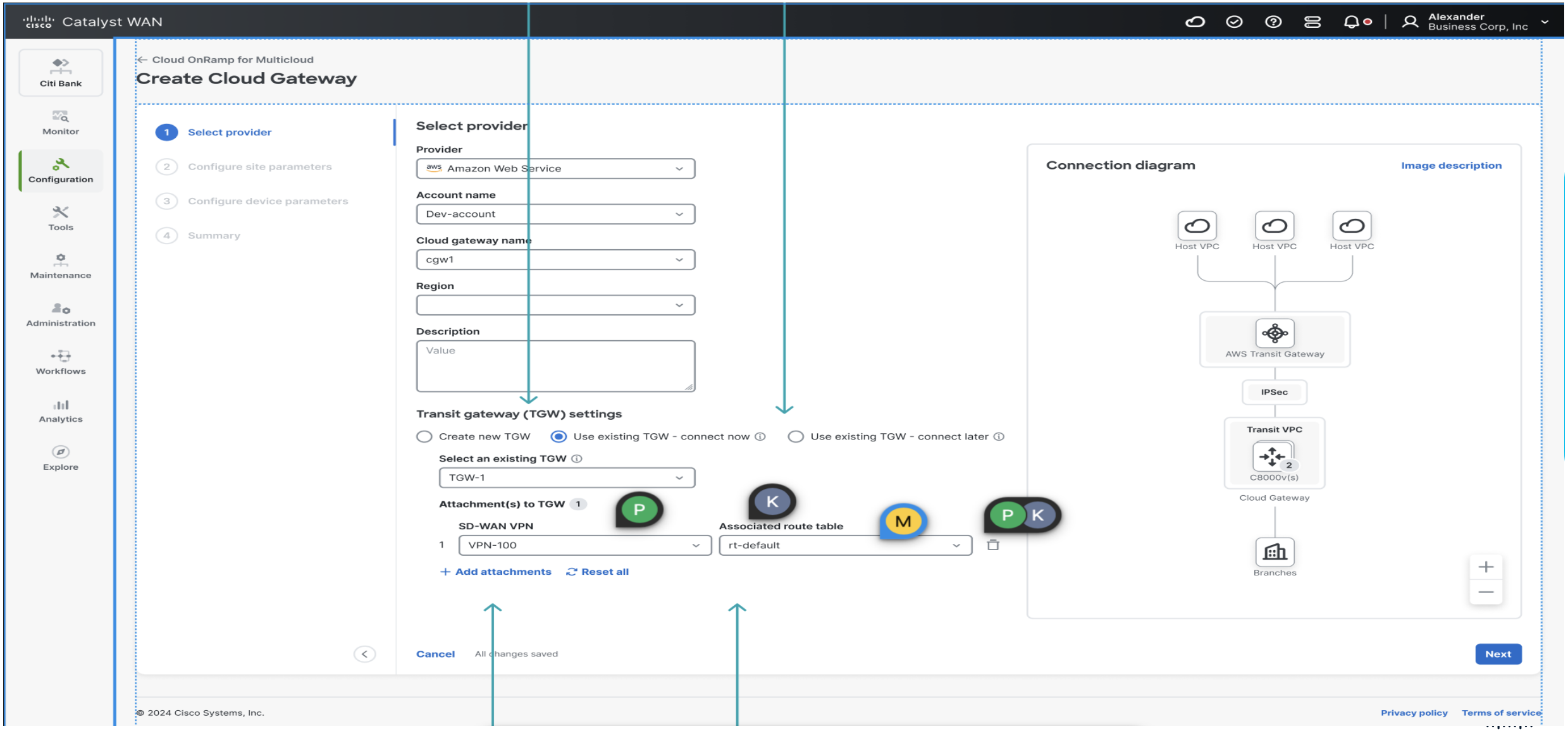


SD-WAN fabric to AWS Cloud

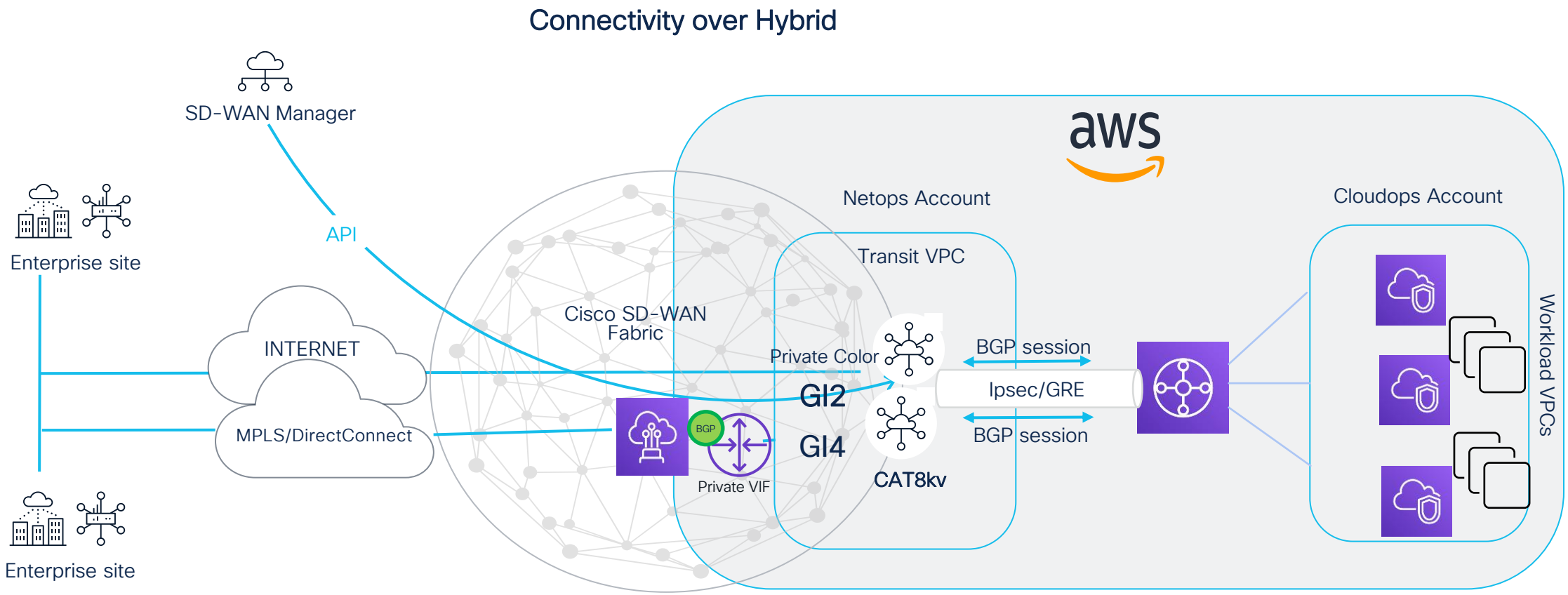
Simple | Automated | Secure

Hybrid Cloud Connectivity - TGW

SD-WAN Native Integration using **IKE Ipsec/ GRE** between Transit VPC cat8kv/vMX and Transit Gateway



Hybrid Cloud Connectivity - Resilient connectivity



Simple

Automated

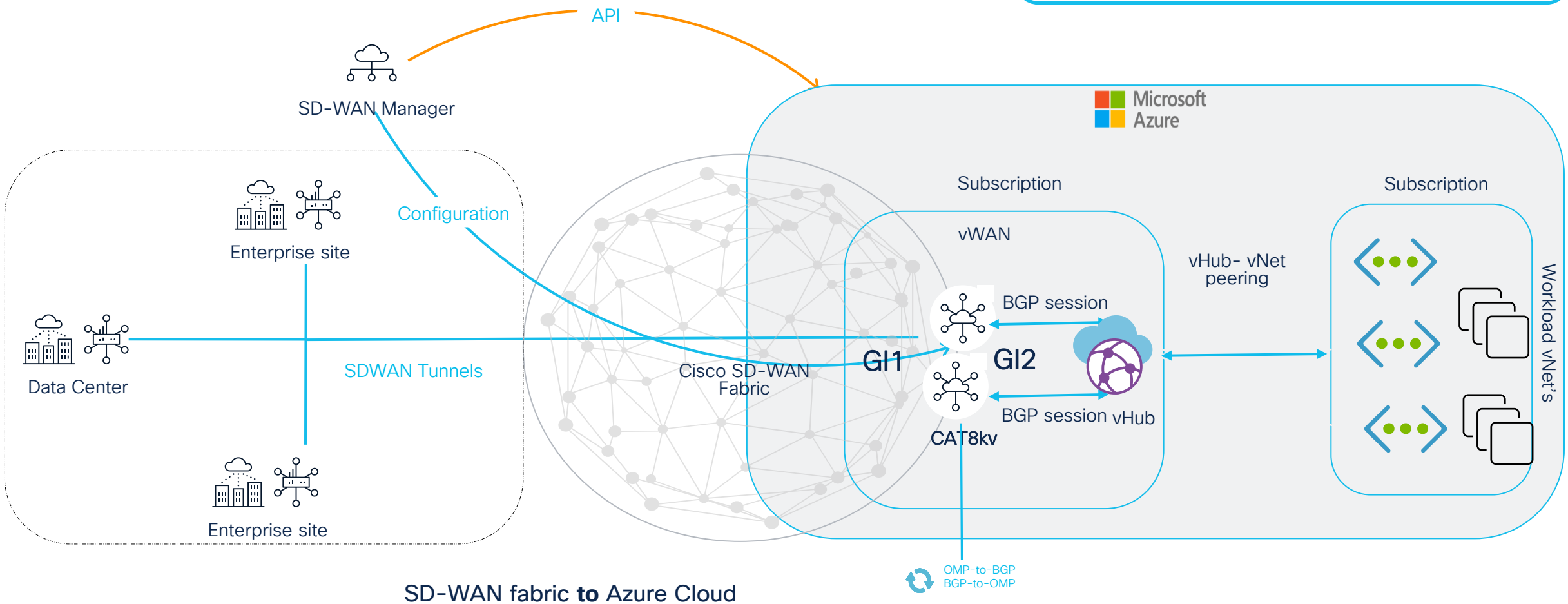
Secure

Direct Cloud Access - Azure

Hybrid Cloud Connectivity

Hybrid Cloud Connectivity – vWAN/vHUB

CAT8k Network virtual appliances are hosted in vHub, running BGP to vHub control plane to learn vNet mappings

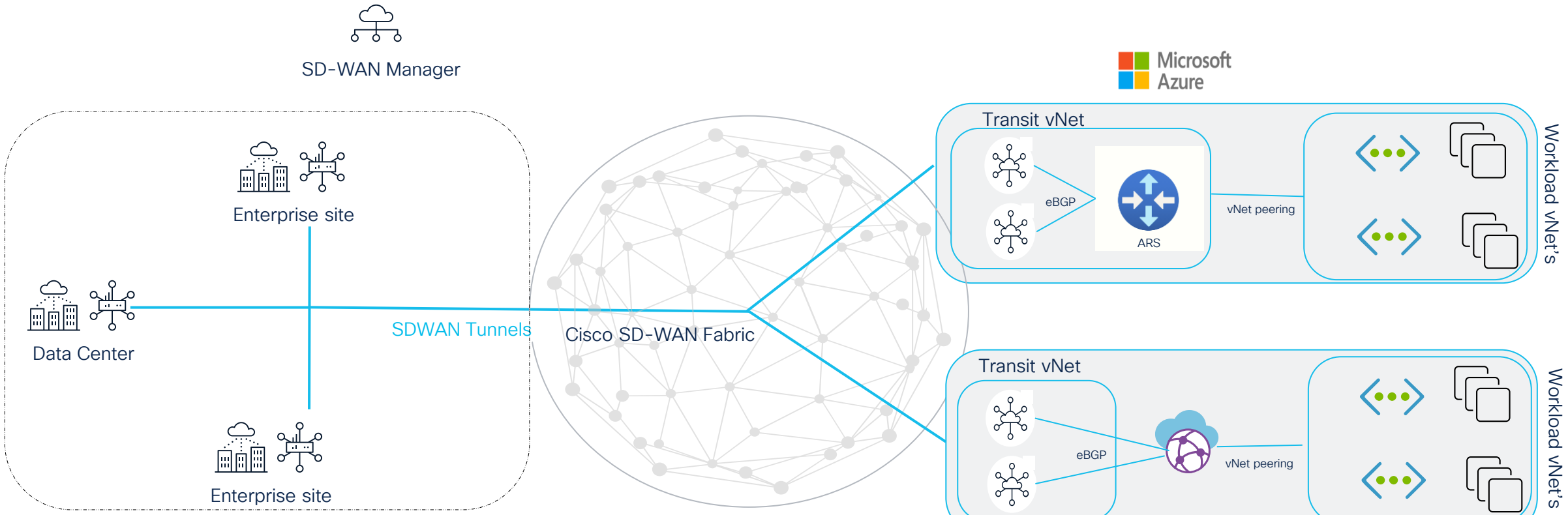


SD-WAN fabric **to** Azure Cloud

Simple | Automated | Secure

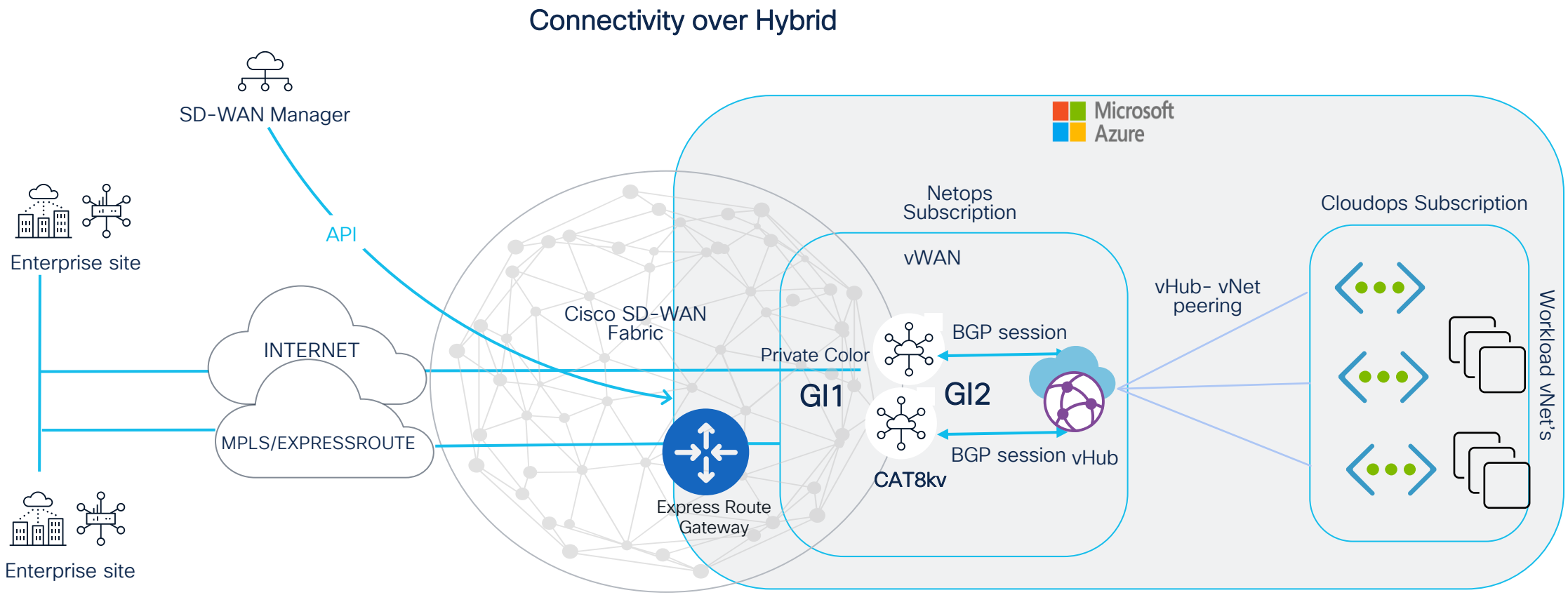
Hybrid Cloud Connectivity- ARS/ vHUB

vMX Network virtual appliances are hosted in transit vNet



SD-WAN fabric to Azure Cloud

Hybrid Cloud Connectivity - Resilient connectivity



Simple

Automated

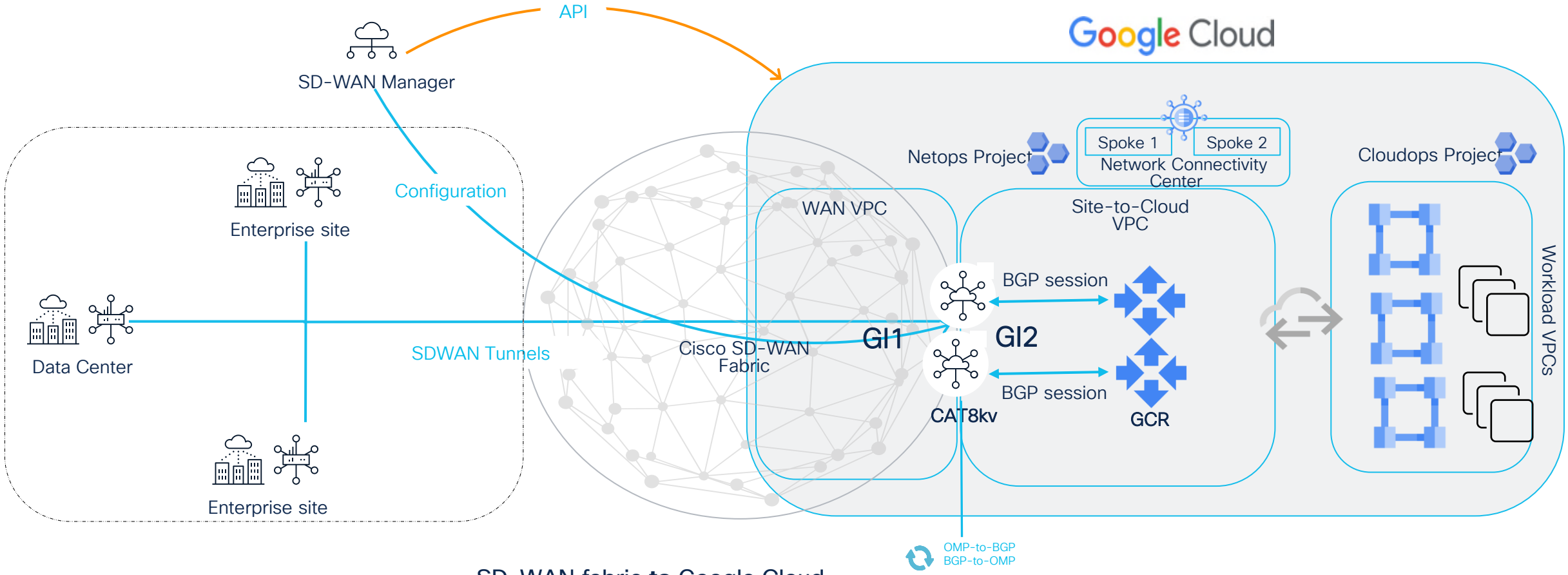
Secure

Direct Cloud Access – Google Cloud

Hybrid Cloud Connectivity

Hybrid Cloud Connectivity – GCR/NCC

Cisco SD-WAN Cloud Hub will be hosted on Google cloud , it runs BGP from service VPN to Google cloud routers to learn and advertise routes from VPC



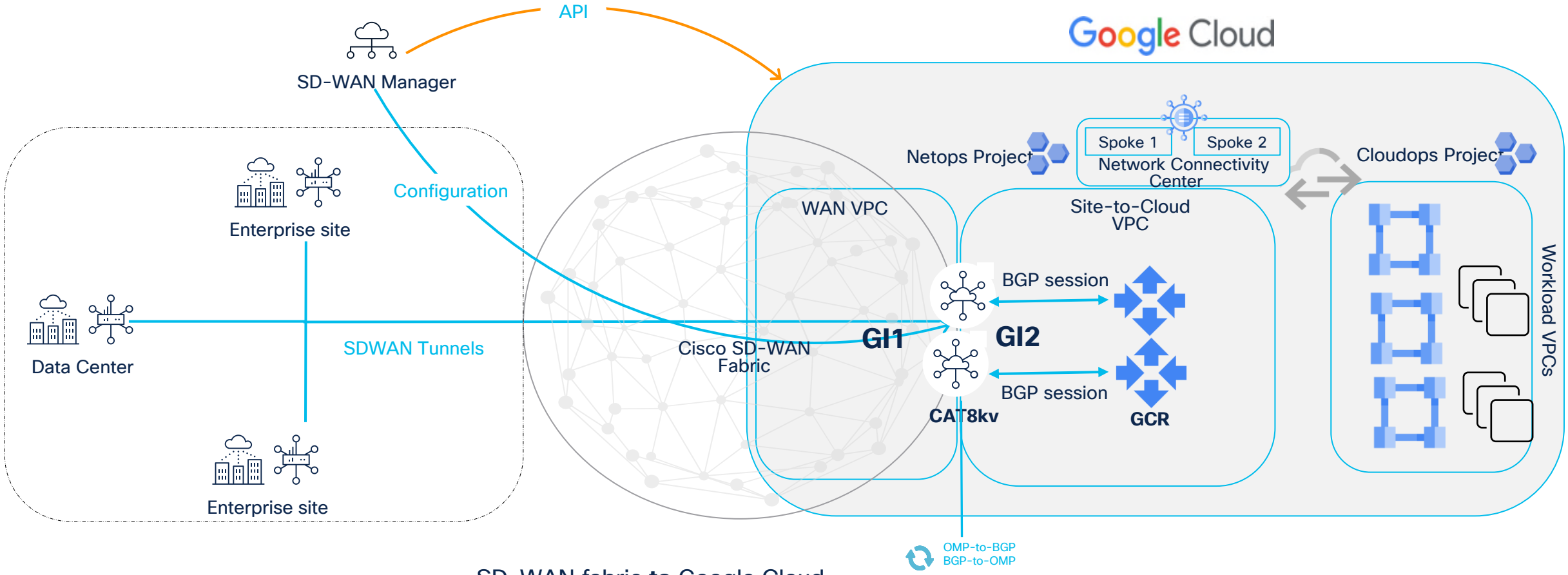
SD-WAN fabric **to** Google Cloud

Simple | Automated | Secure

Google Cloud Router

Hybrid Cloud Connectivity- NCC/GCR

Cisco SD-WAN Cloud Hub will be hosted on Google cloud , it will from BGP from service VPN to Google cloud routers to learn the VPC routes



SD-WAN fabric **to** Google Cloud

Simple

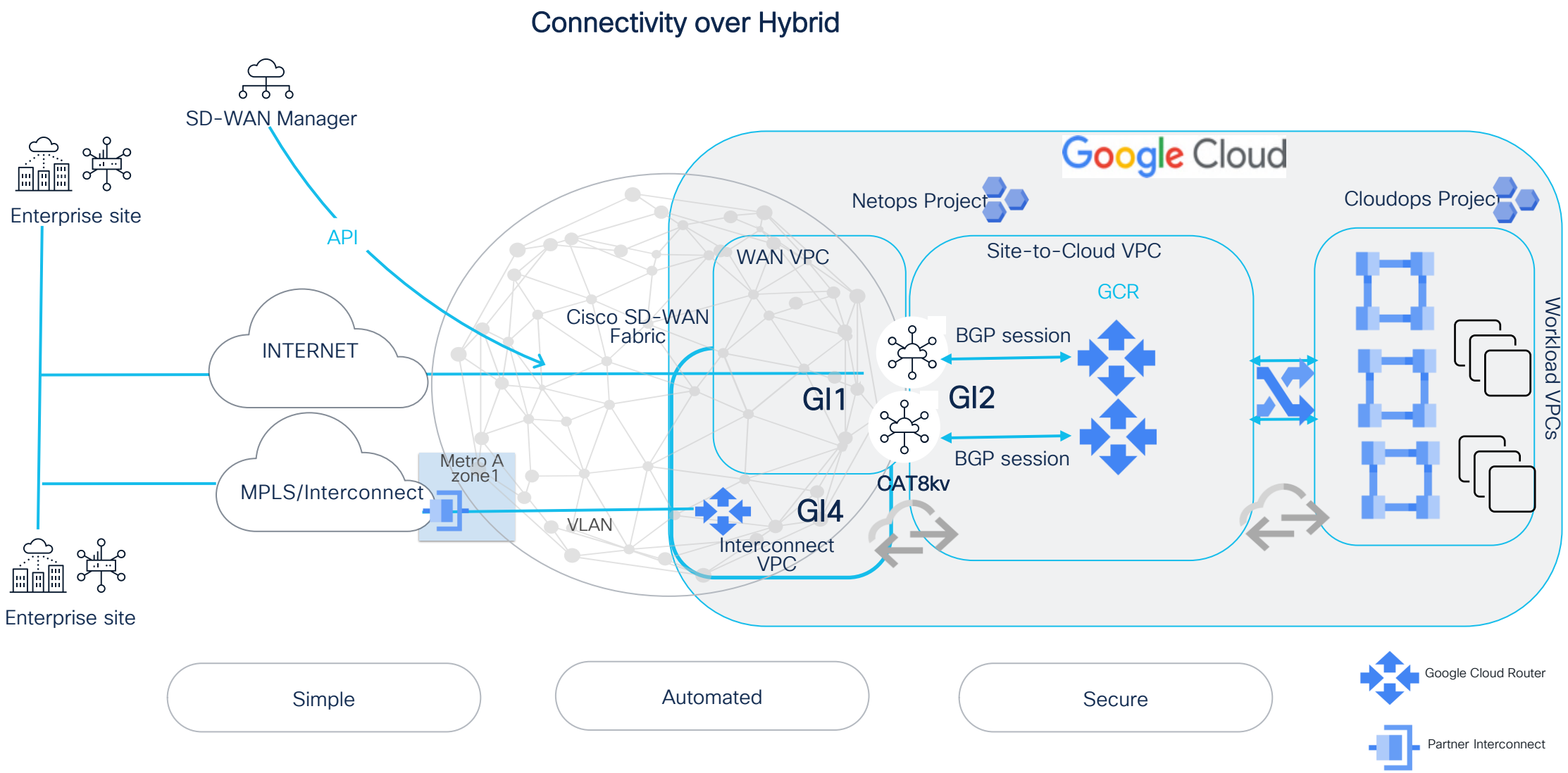
Semi Automated

Secure

Google Cloud Router

cisco

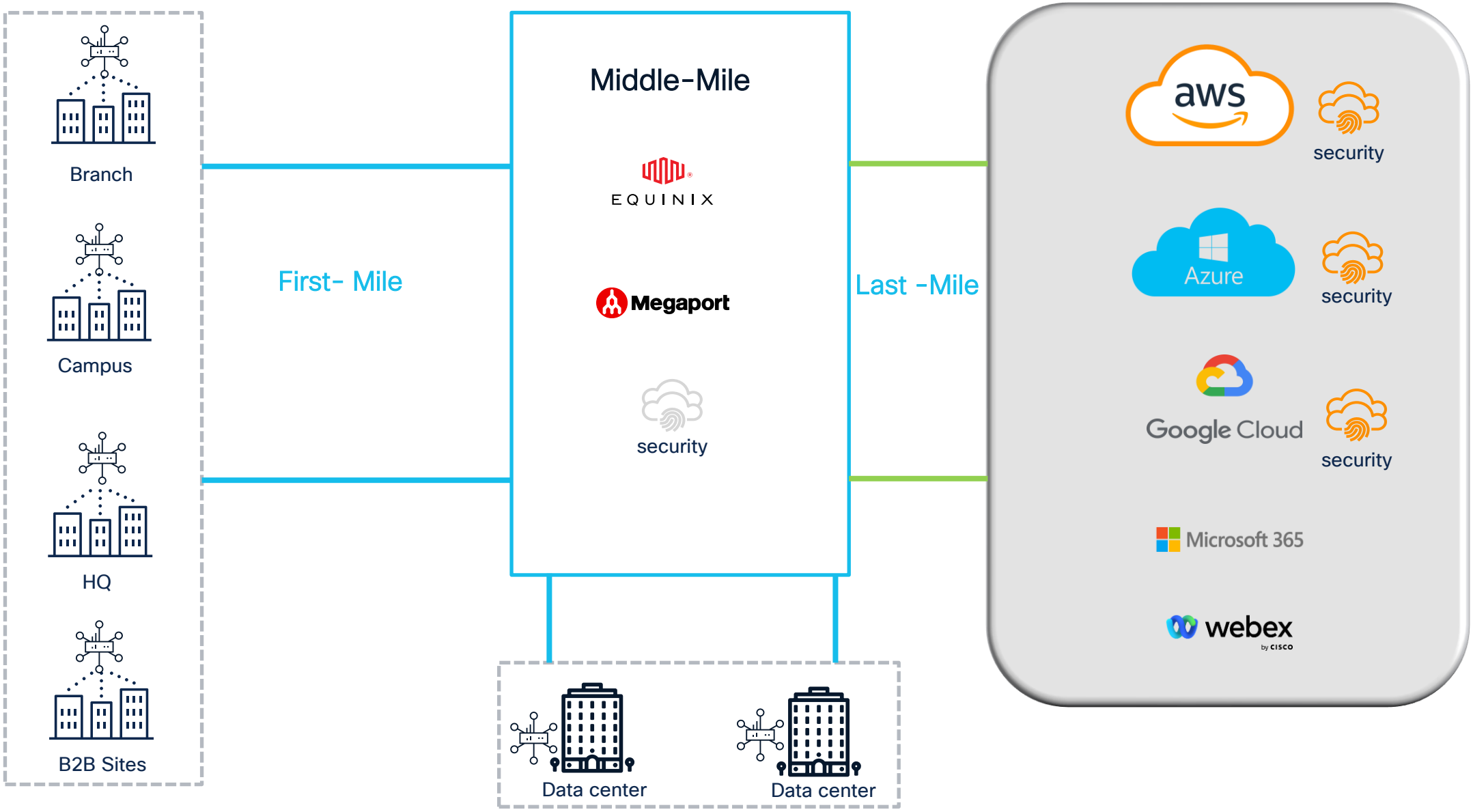
Hybrid Cloud Connectivity - Resilient connectivity



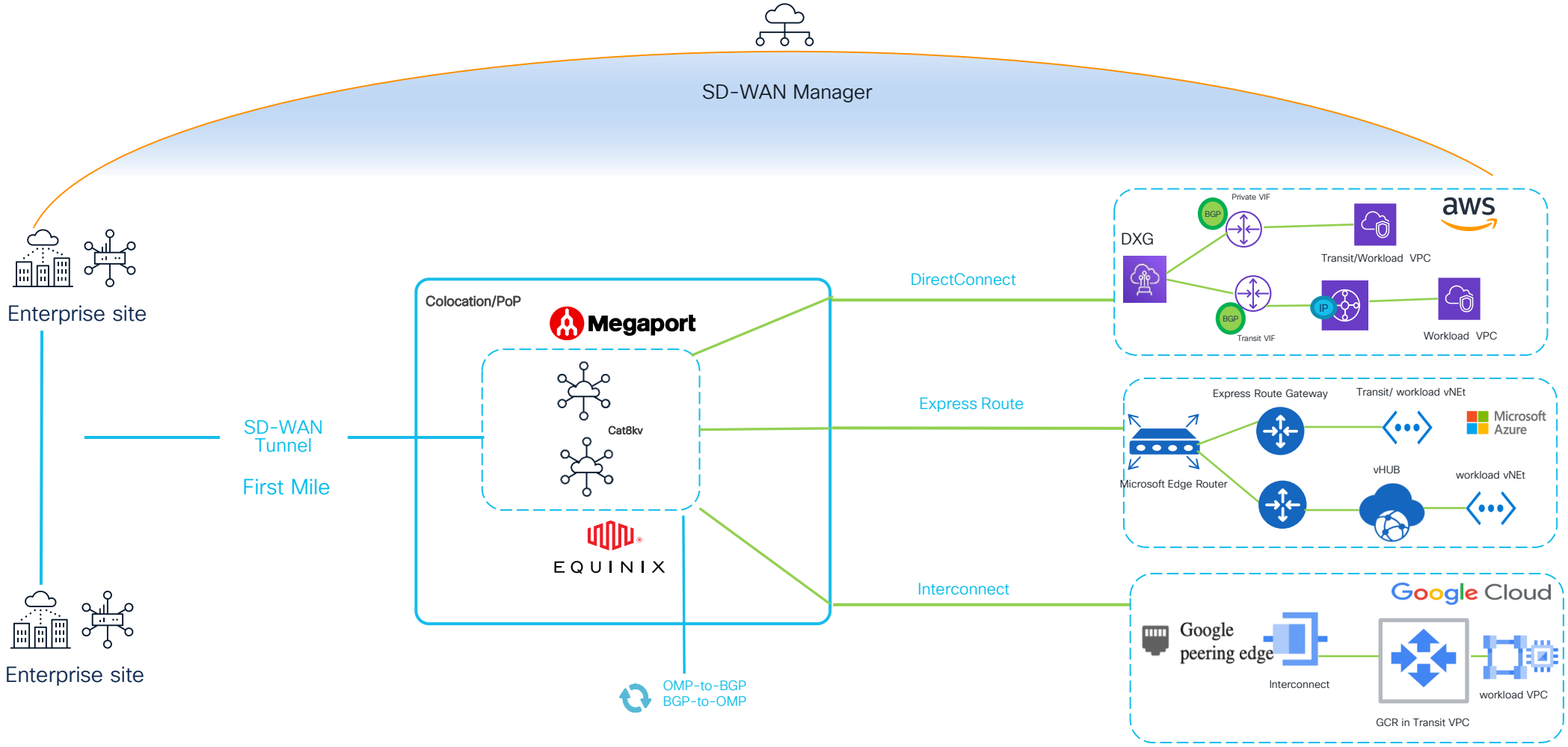
Hybrid Cloud Connectivity via Interconnect/Carrier Neutral Facilities

With Equinix & Megaport

Architecture Option 2- via Cloud interconnect

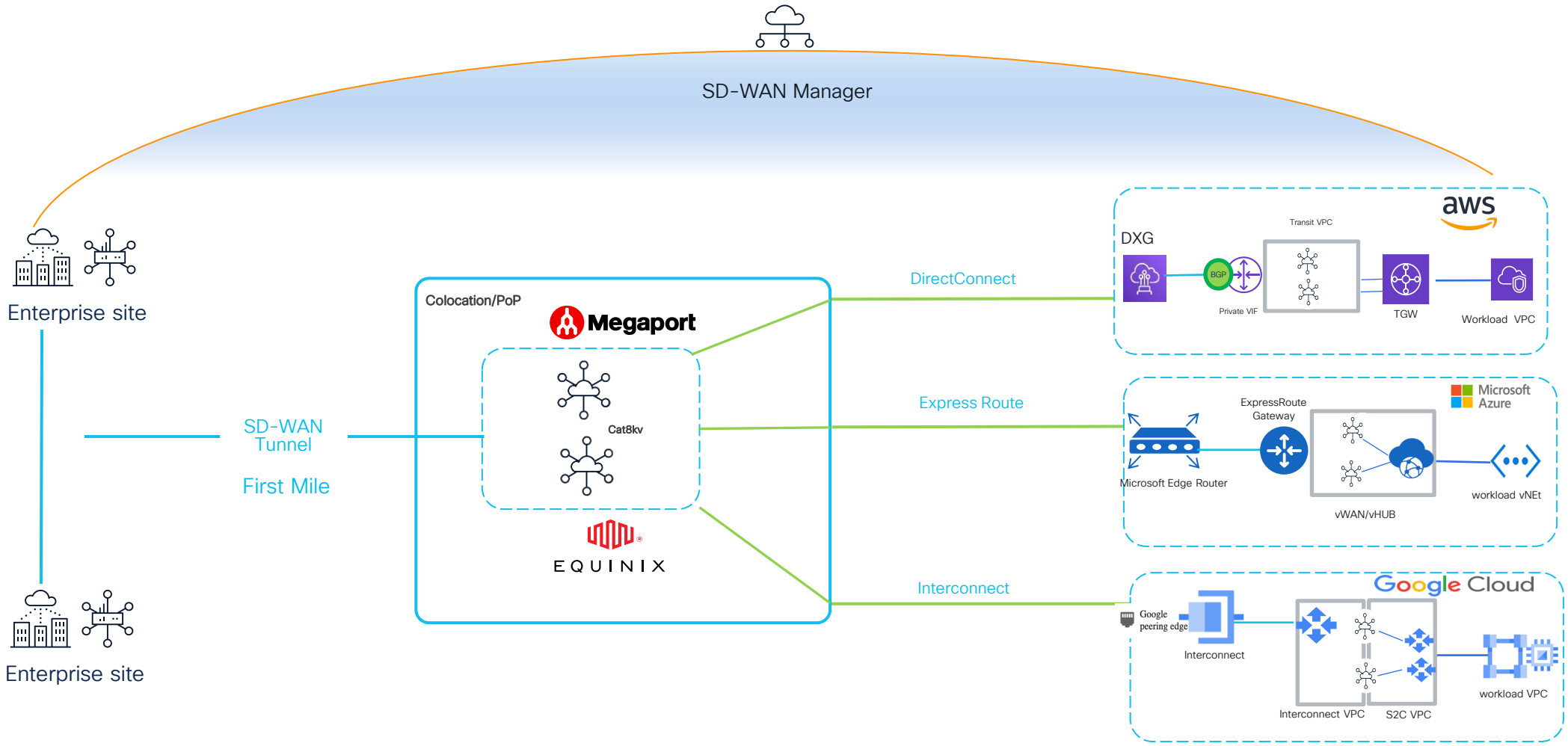


Hybrid Cloud Connectivity – Megaport or Equinix



Hybrid Cloud Connectivity – Megaport or Equinix

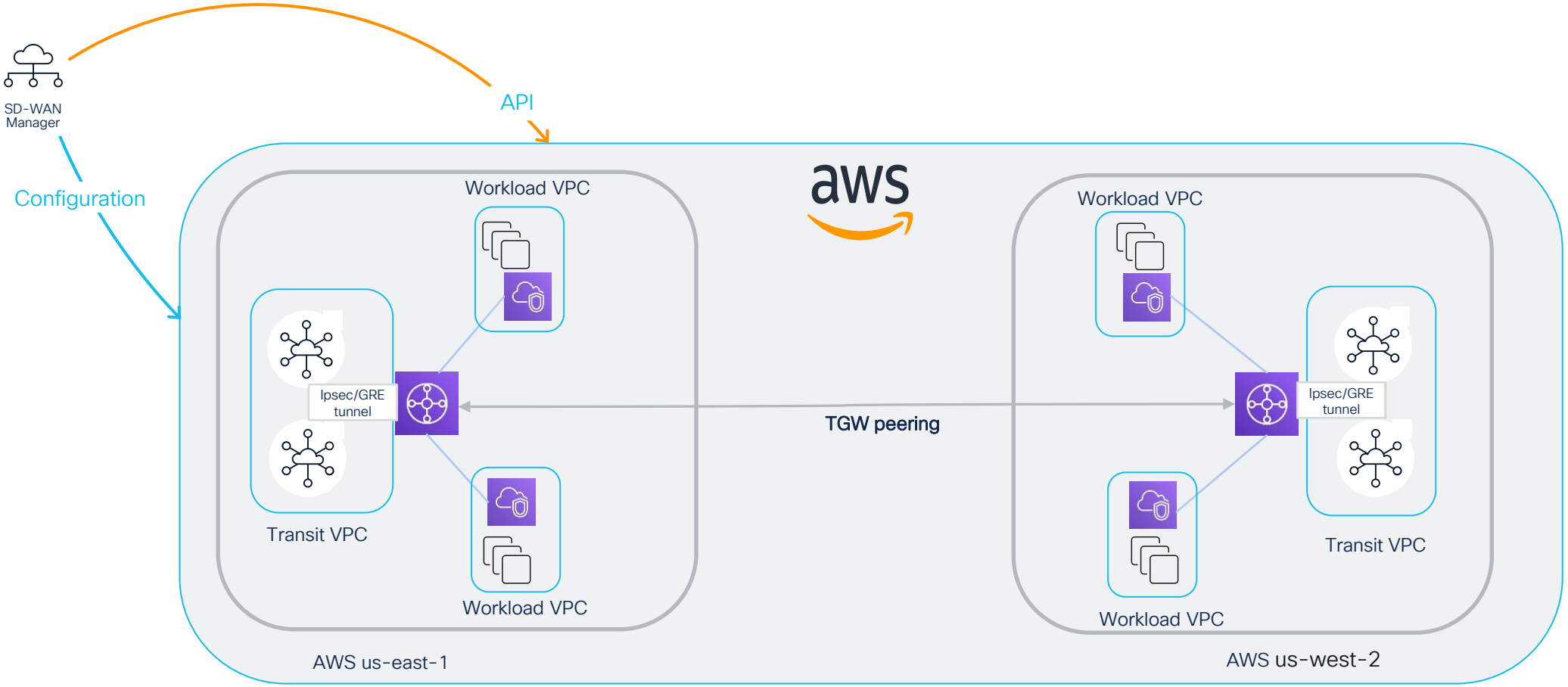
Fully Encrypted



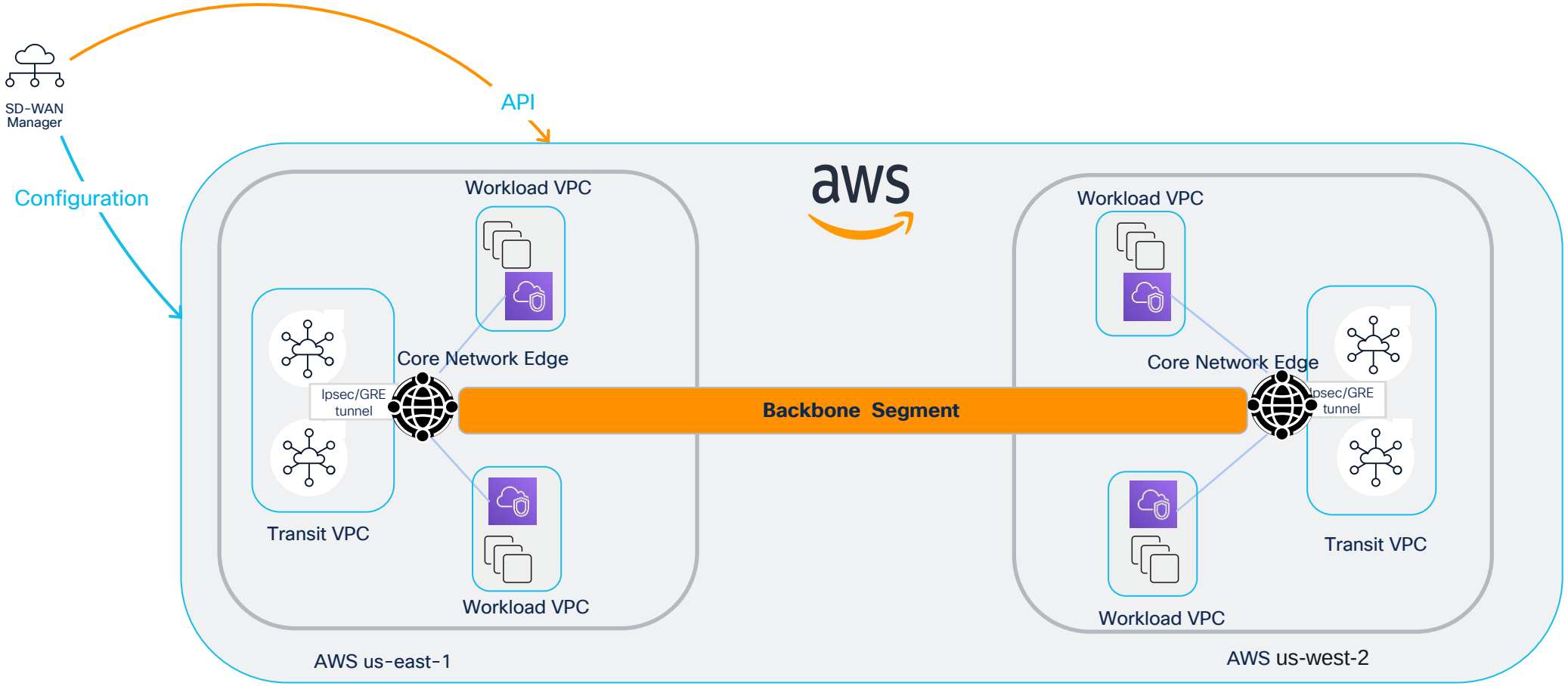
For distributed applications

Multi-Region Global Networking

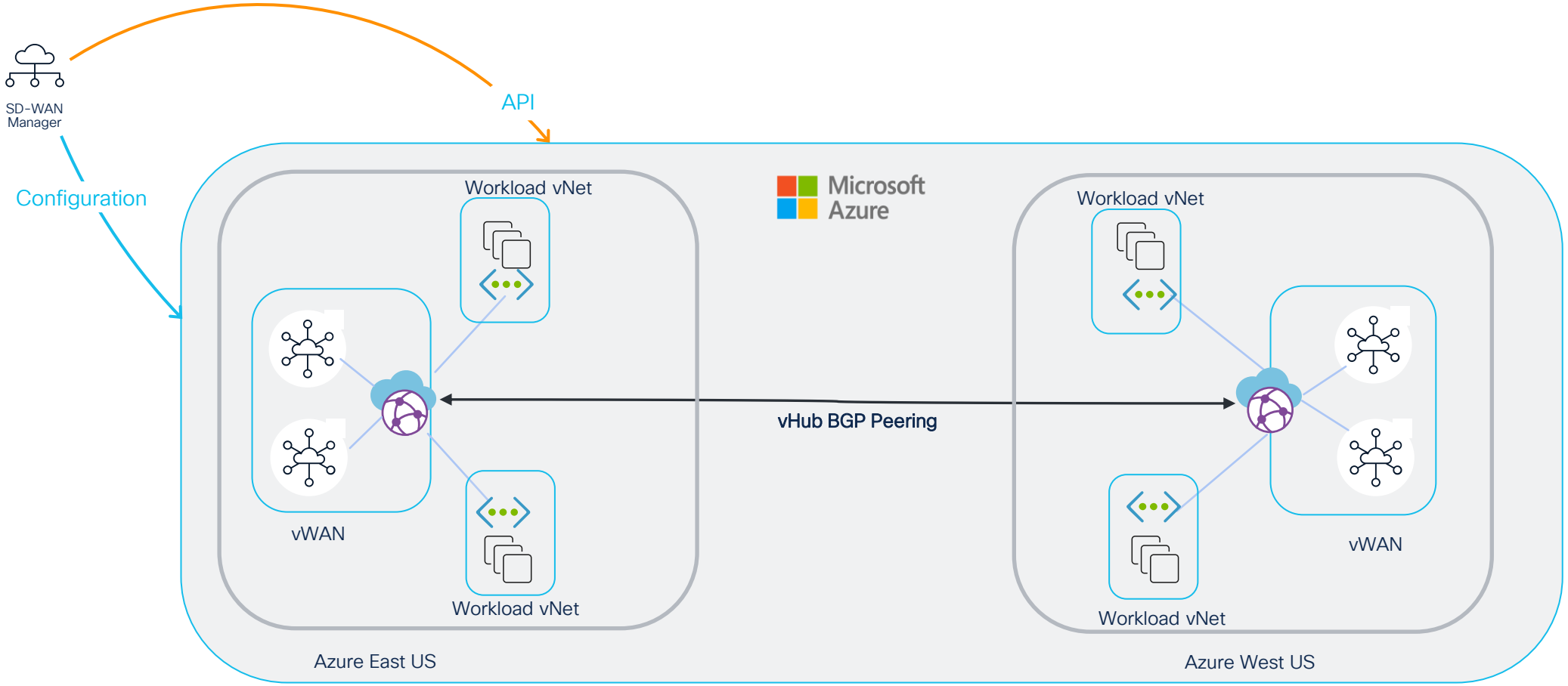
Multi-Region Global Networking - TGW



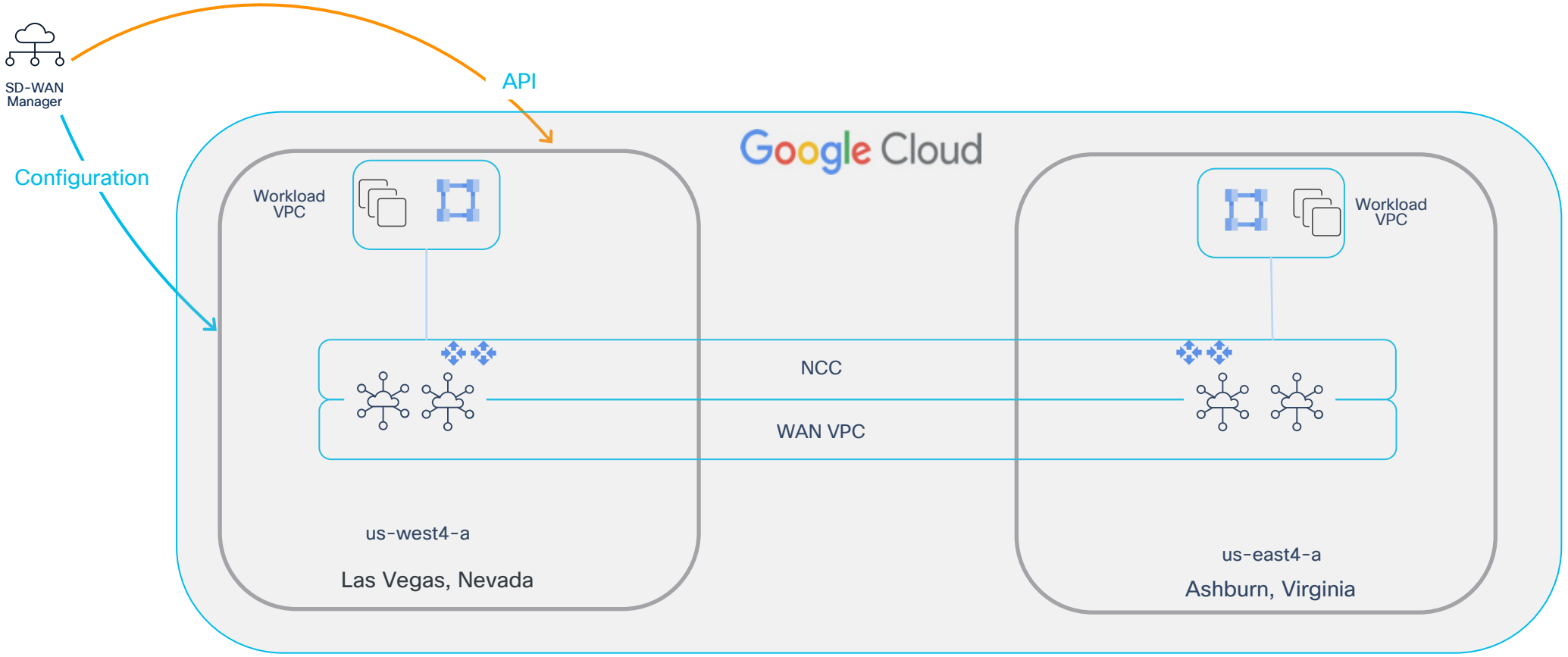
Multi-Region Global Networking -Cloud WAN



Multi-Region Global Networking- vWAN/vHUB



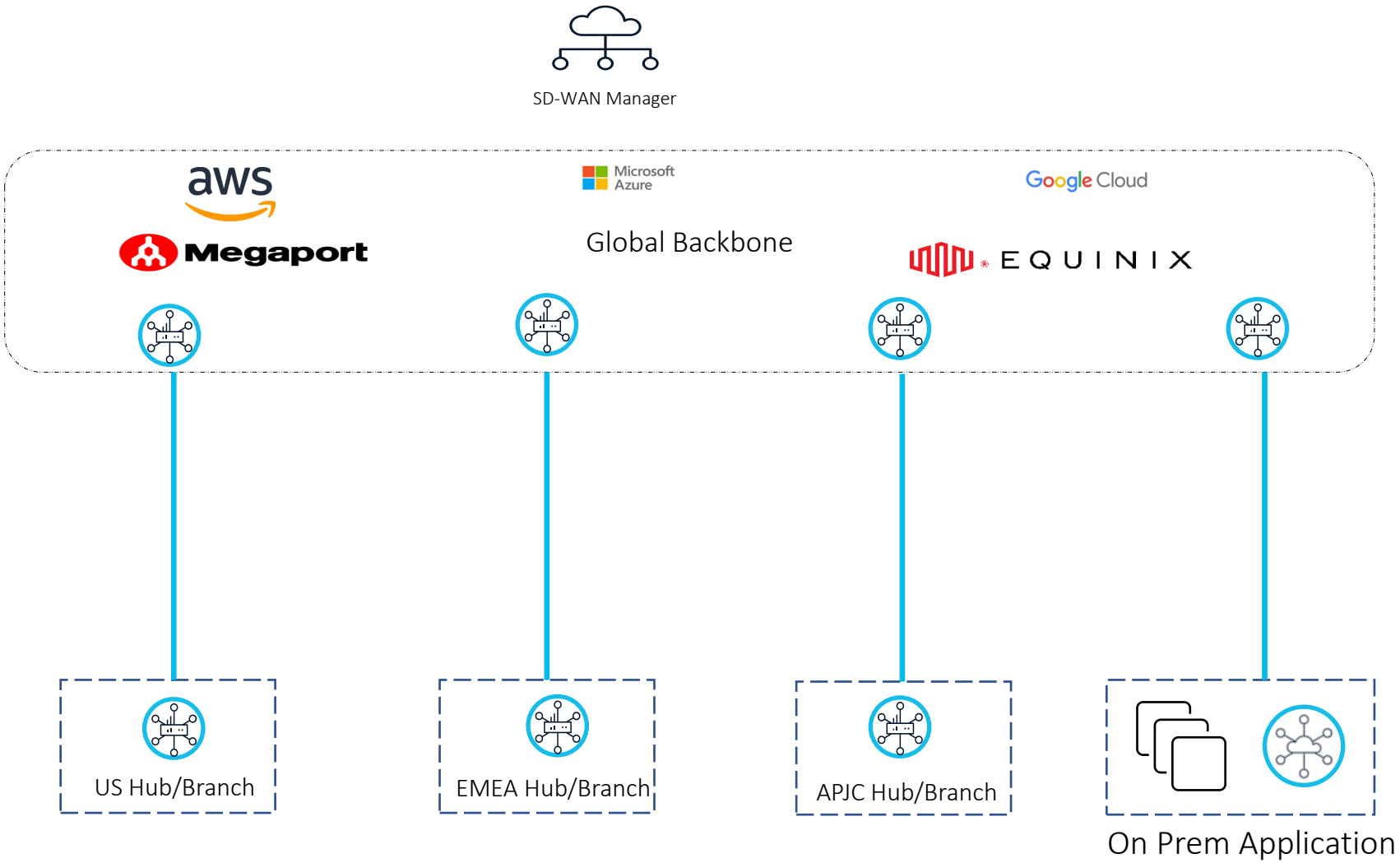
Multi-Region Global Networking : NCC/Cloud WAN



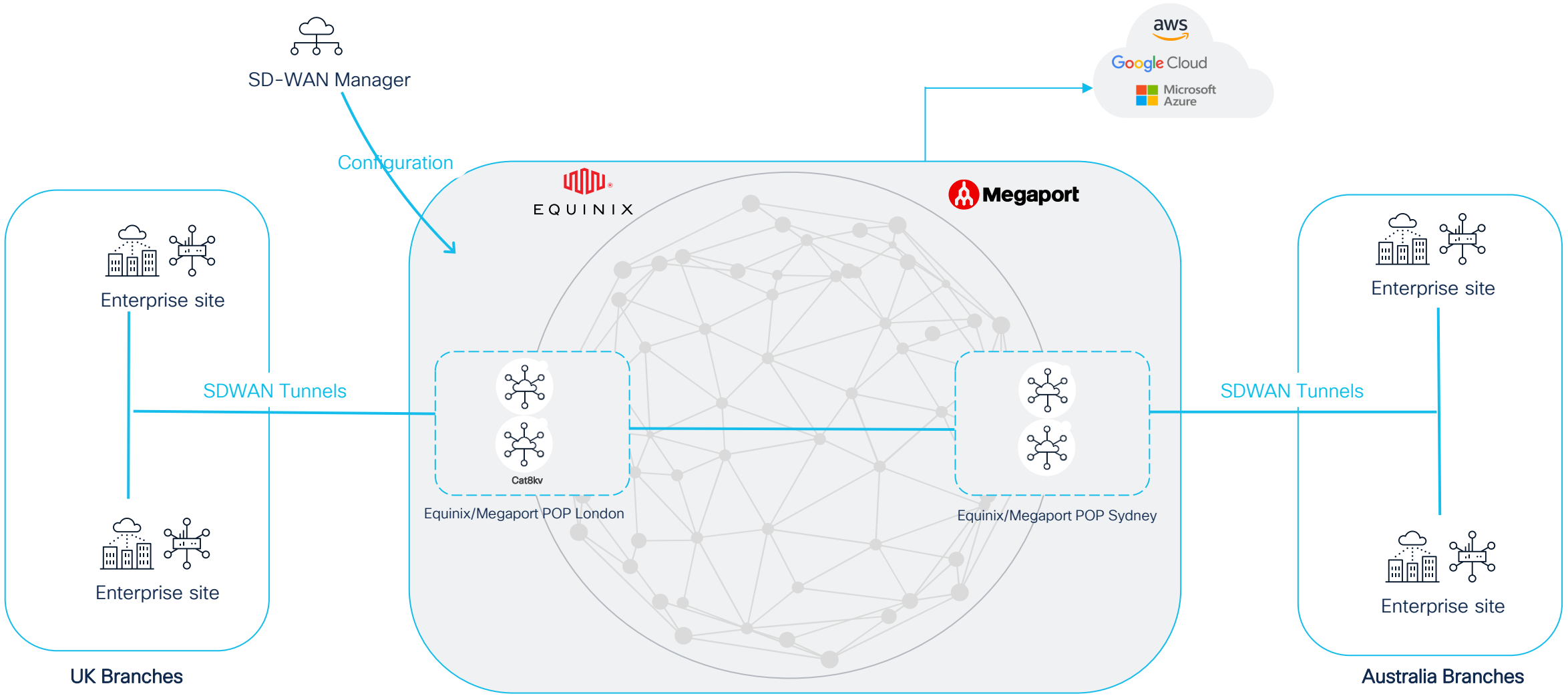
Multi-Region Global Networking

For International sites / Building a Global backbone

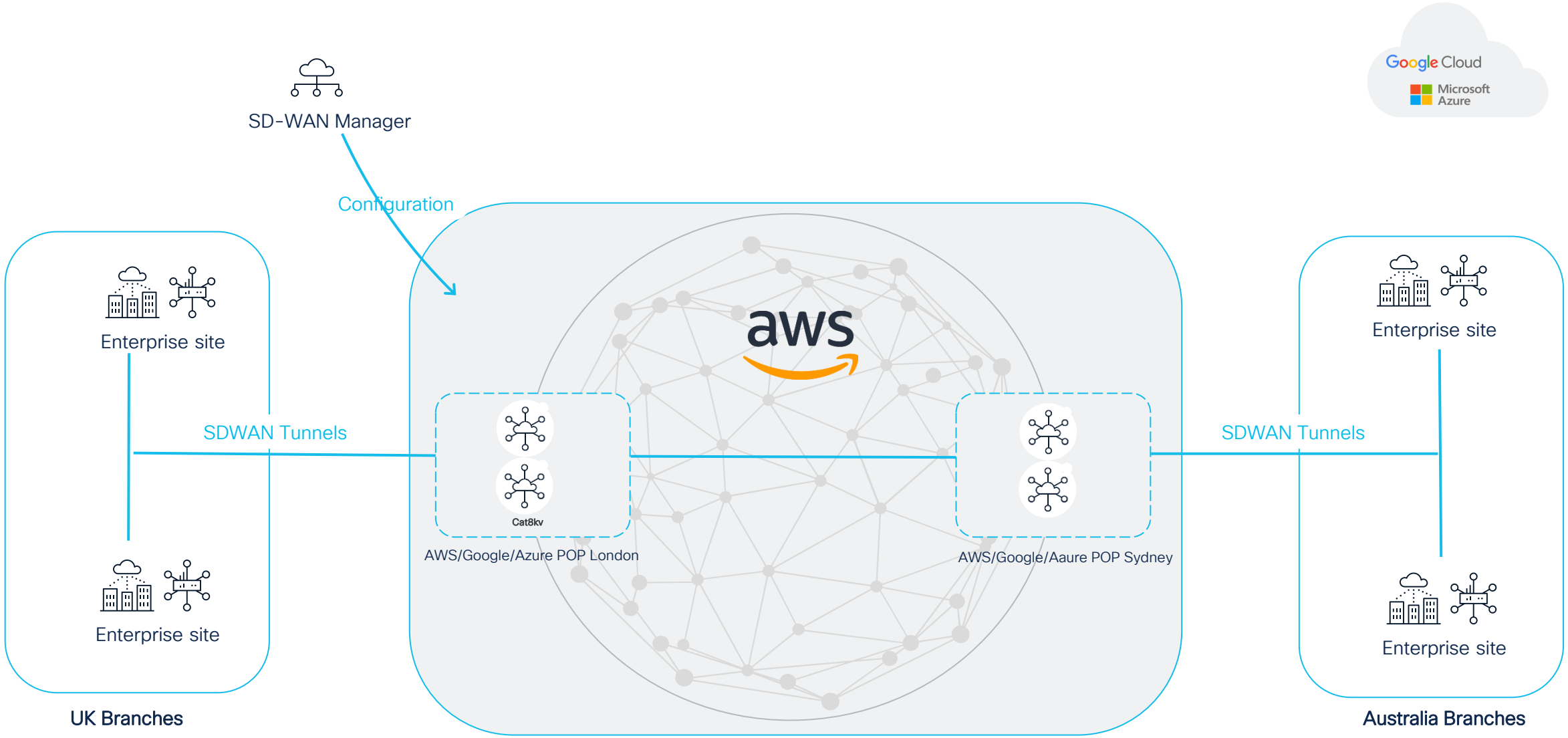
Flexible backbone and connectivity to Cloud



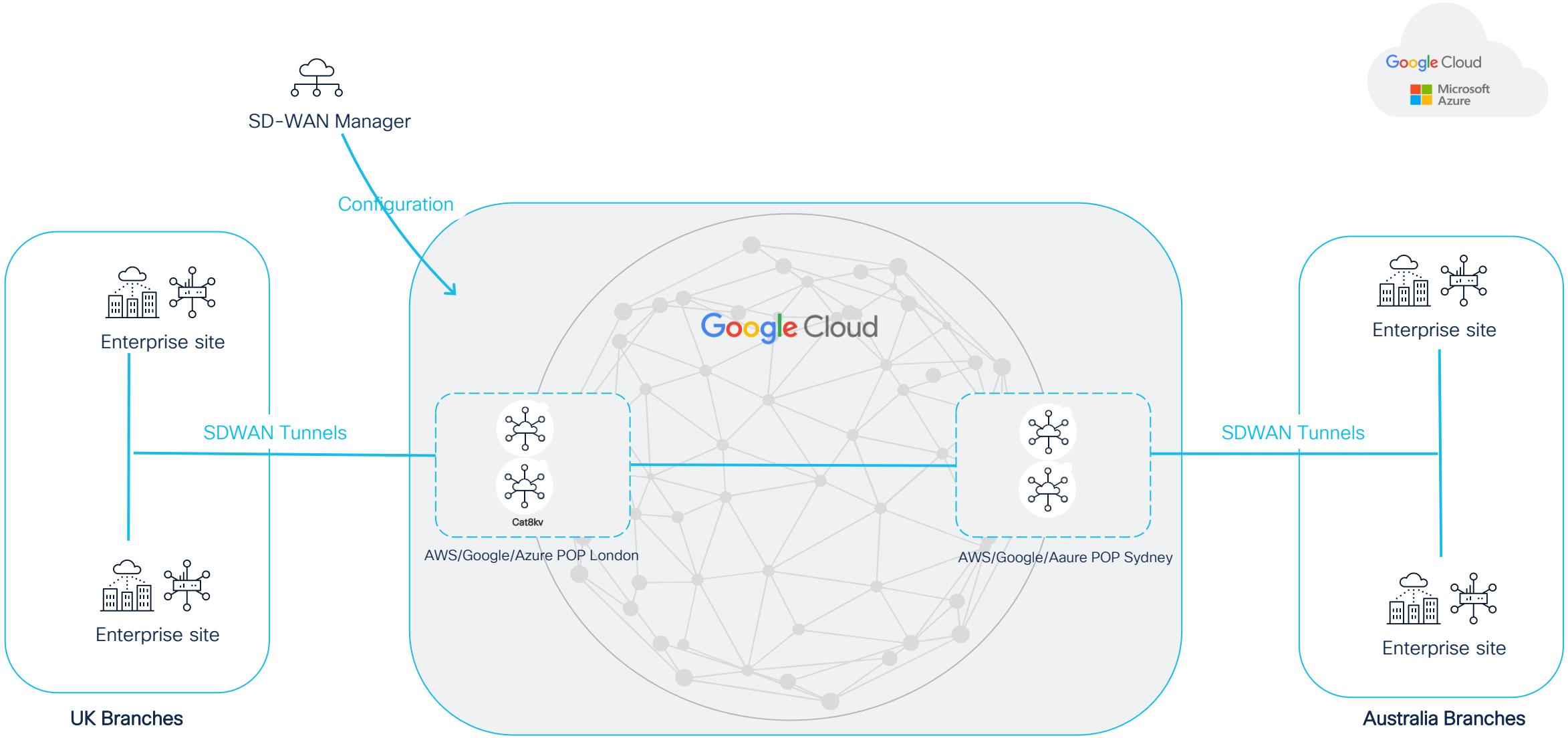
For International sites – Cloud Agnostic



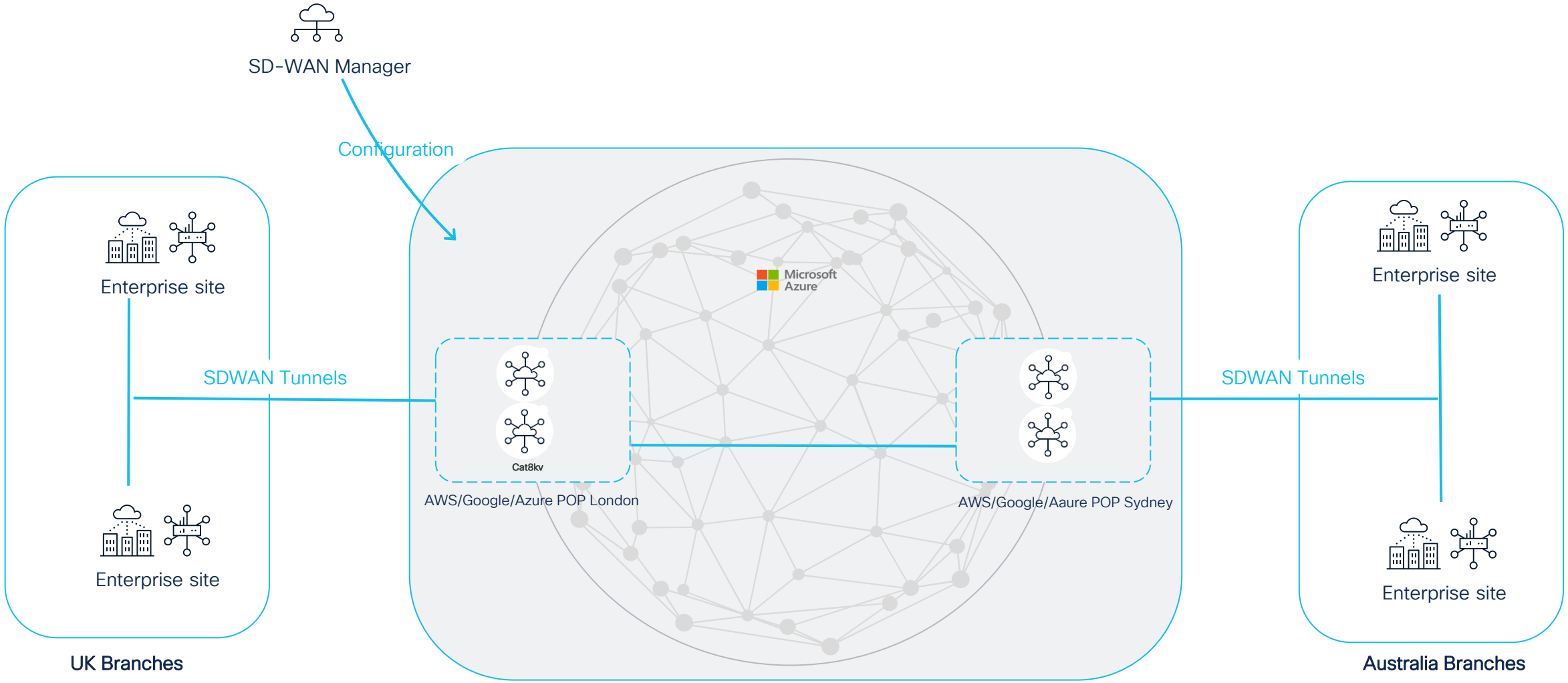
For International sites – AWS



For International sites – Google Cloud

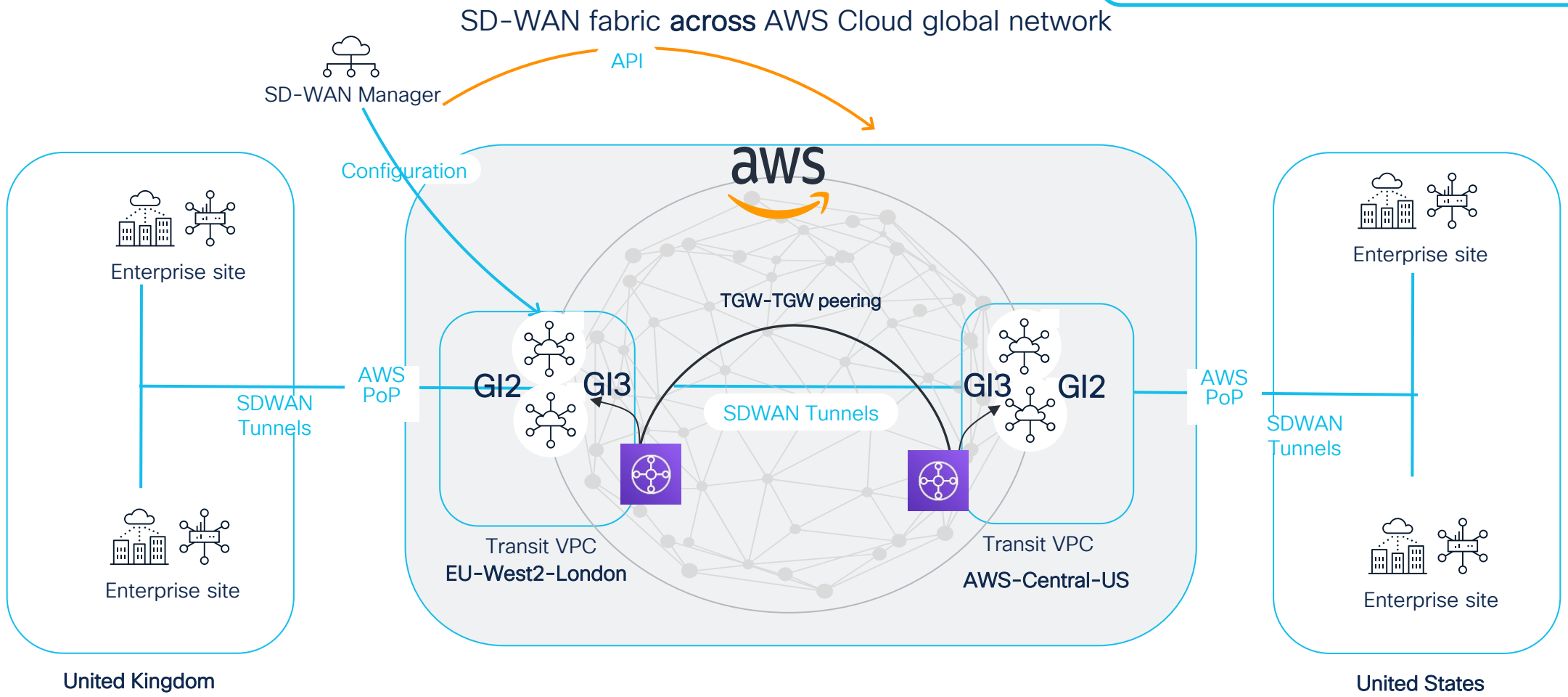


For International sites - Azure



For International sites AWS TGW

TGW-TGW peering to build Backbone. Control policy or Multi region Fabric required for traffic redirection



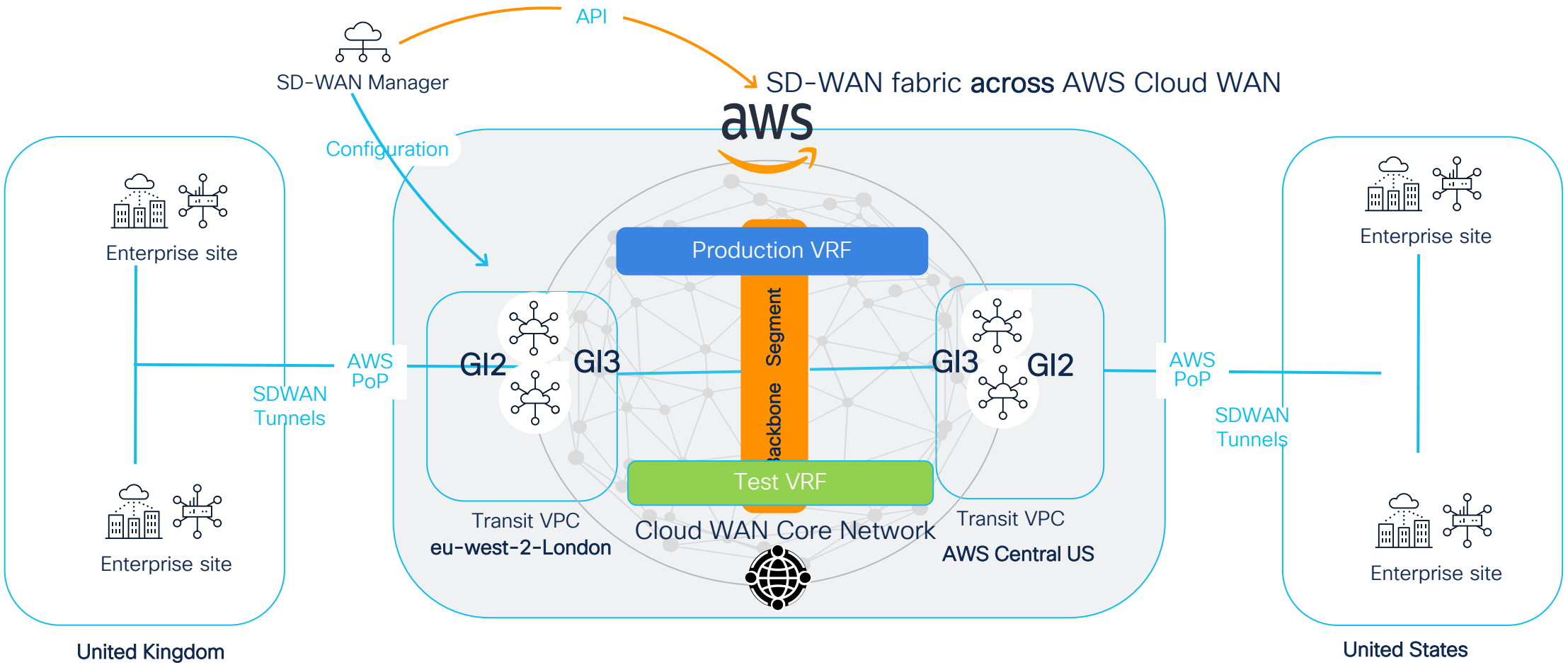
On-demand

High performance

Global connectivity

For International sites AWS Cloud WAN

High performance dynamic architecture that is uniquely co-innovated by Cisco and AWS



On-demand

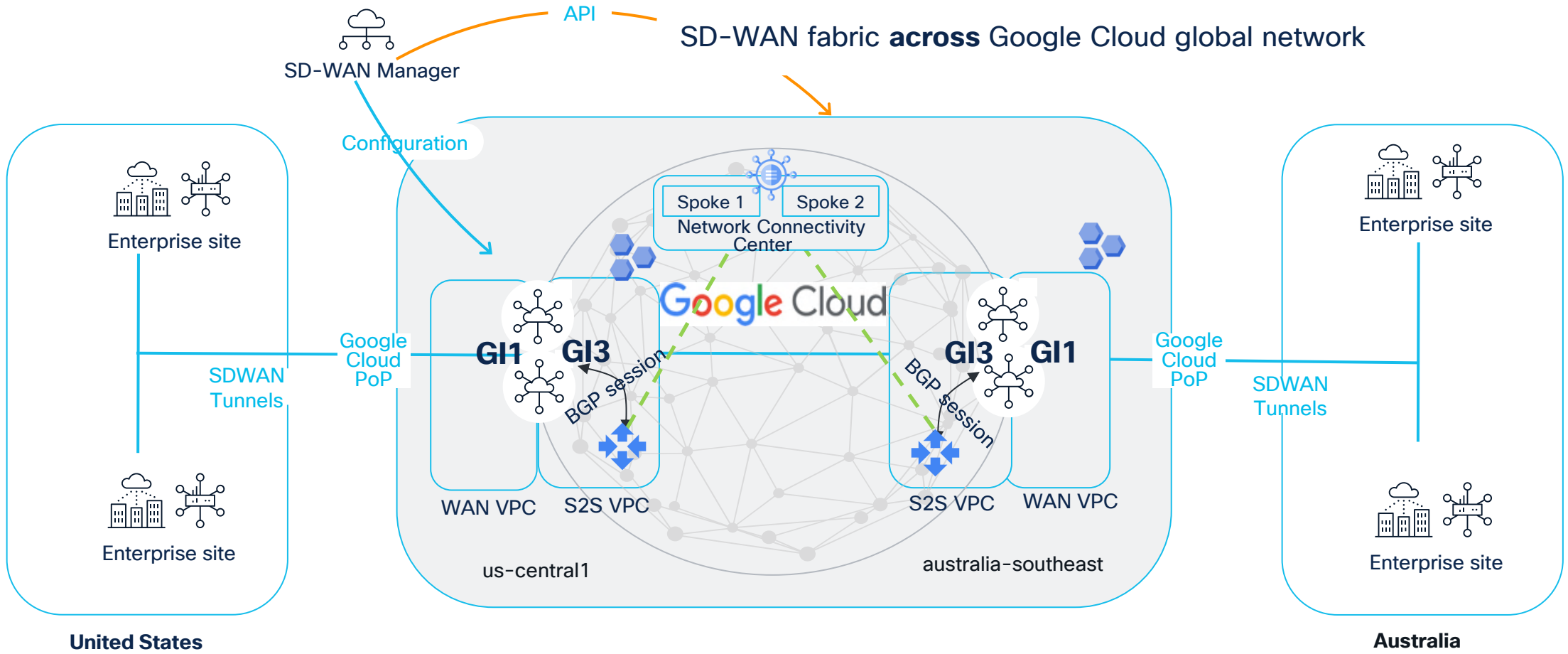
High performance

Global connectivity

cisco

For International sites Google NCC/Cloud WAN

SD-WAN will leverage cloud service provider's backbone (Google NCC) to extend SD-WAN fabric from any site to Site, Control policy or Multi region Fabric required for traffic redirection



On-demand

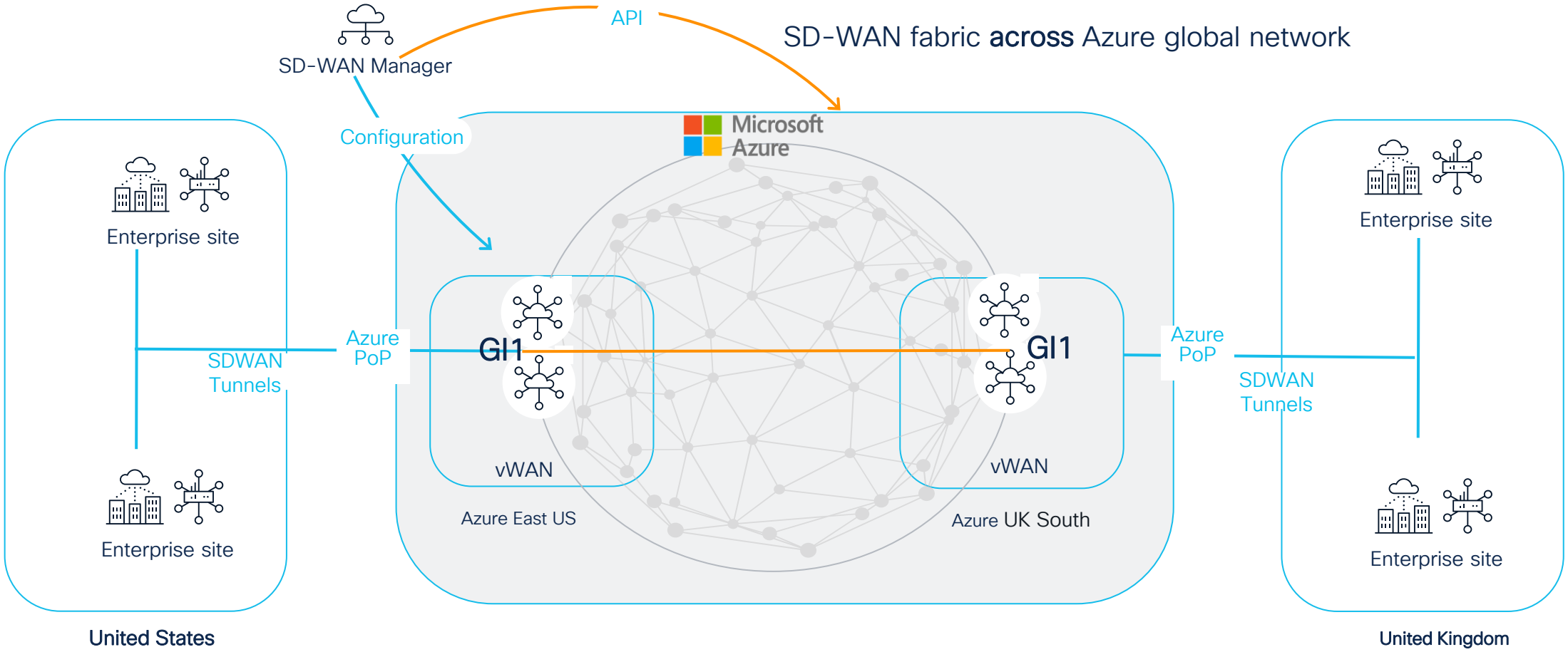
High performance

Global connectivity

Google Cloud Router

For International sites Azure

SDWAN tunnels with Azure Public IPs on NVAs go through Azure Backbone. Control policy or Multi region Fabric required for traffic redirection



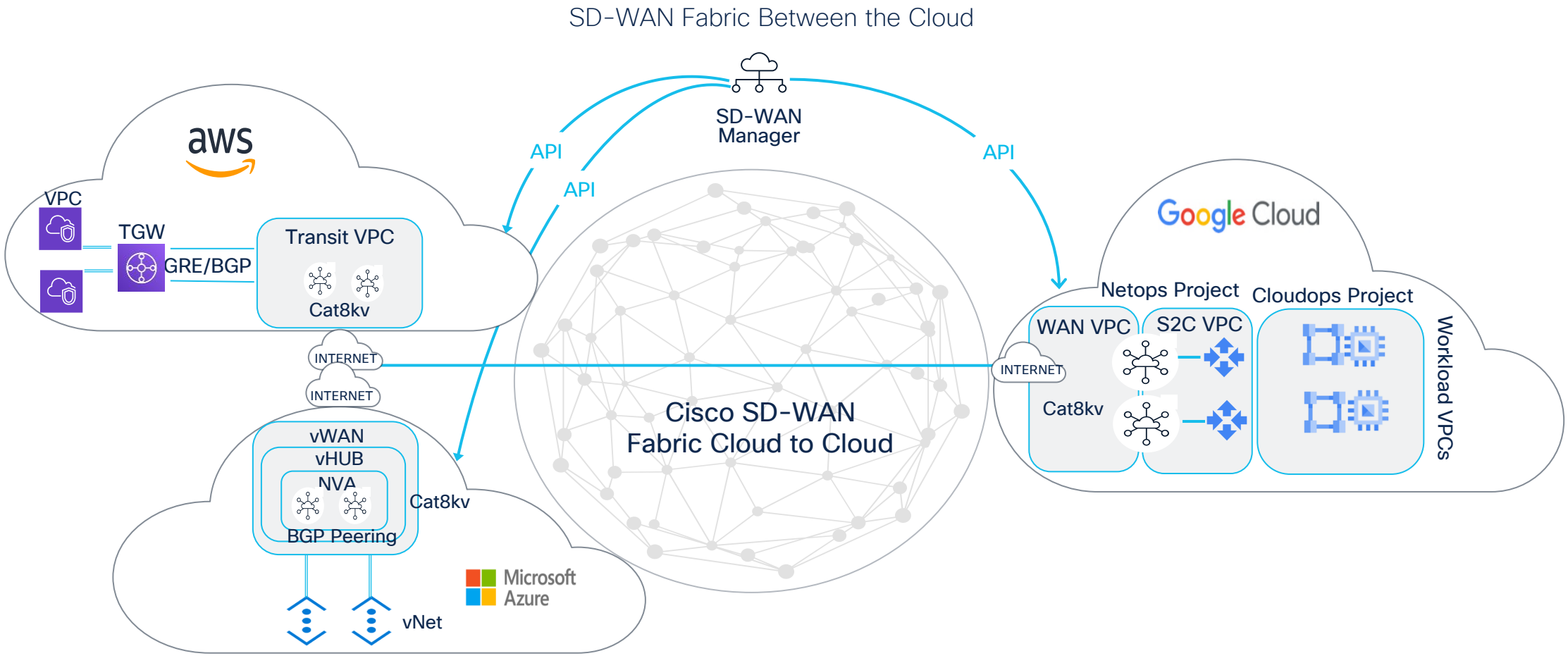
On-demand

High performance

Global connectivity

Multi-Cloud Integration

Multi-Cloud Integration – Over Internet or MSP Underlay

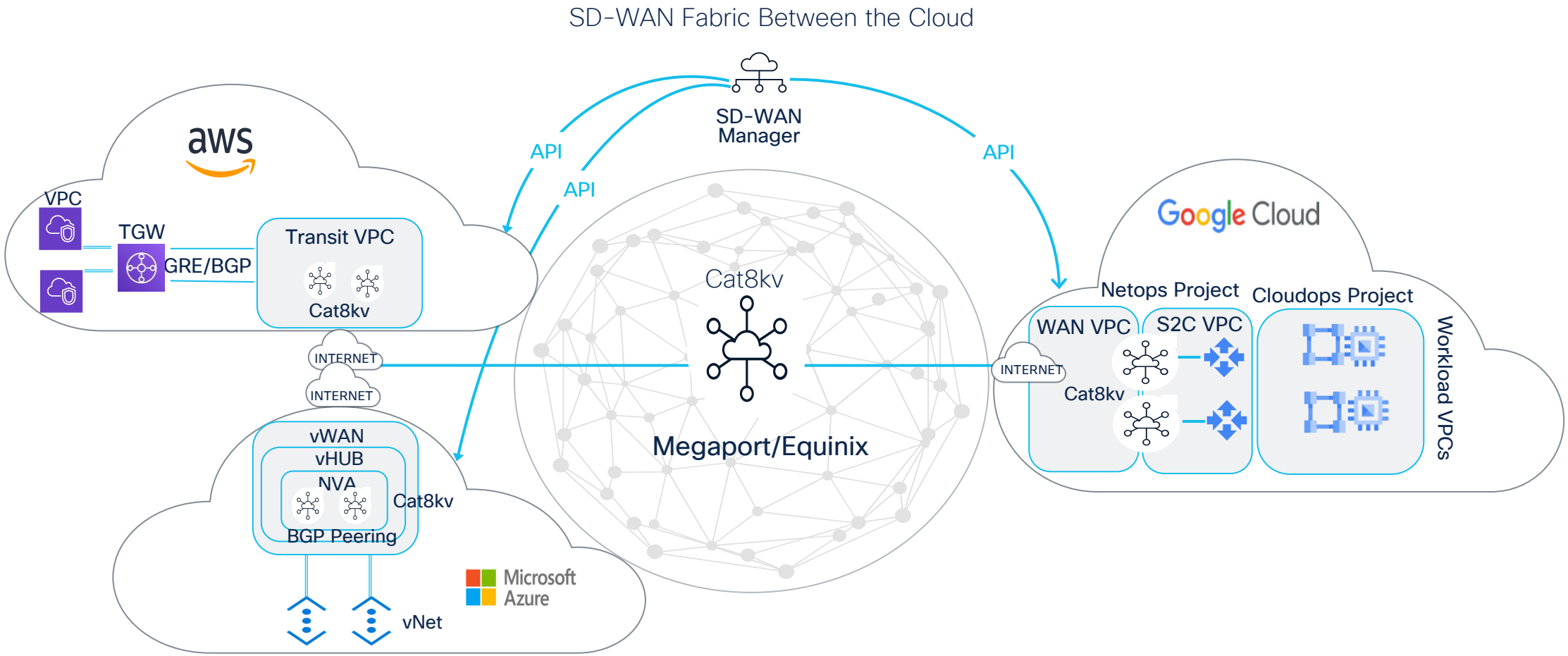


On-demand

High performance

Global connectivity

Multi-Cloud Integration – via Megaport/Equinix

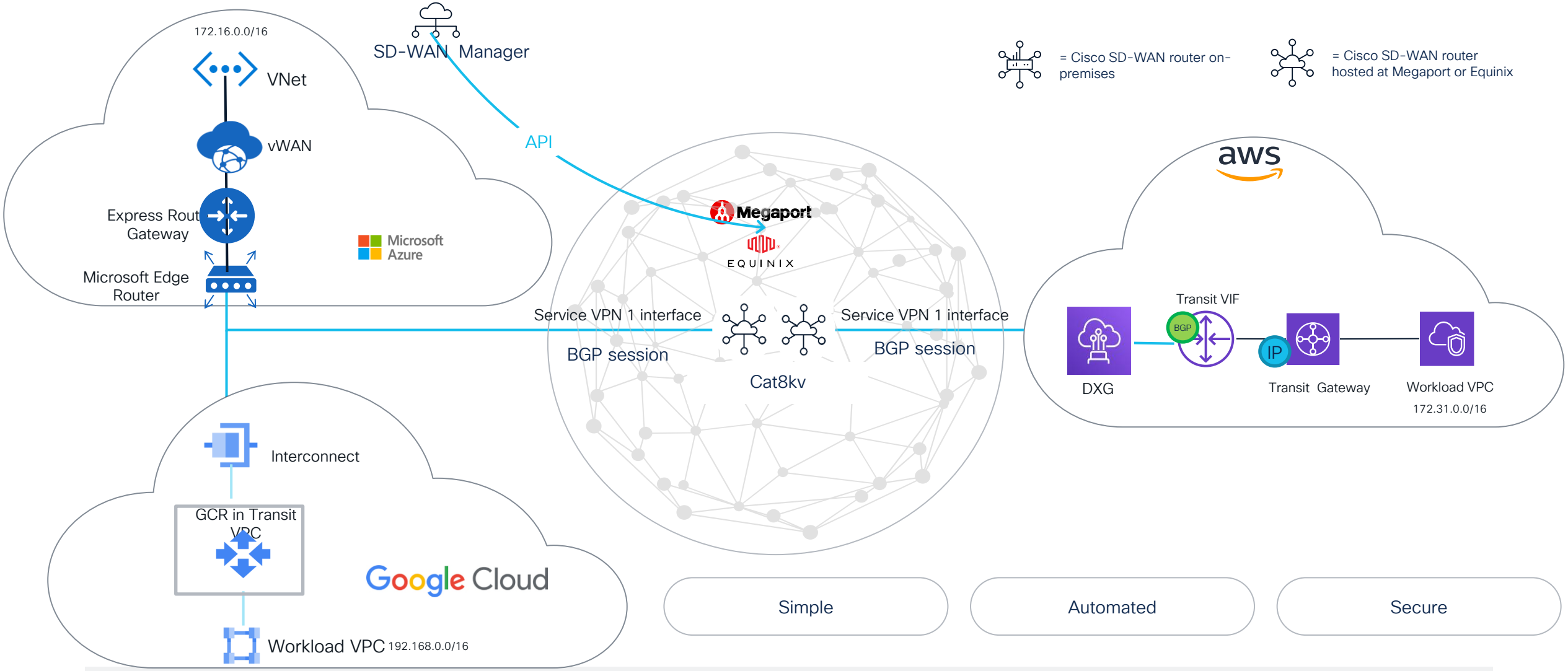


On-demand

High performance

Global connectivity

Multi-Cloud Integration – via Megaport/Equinix BGP



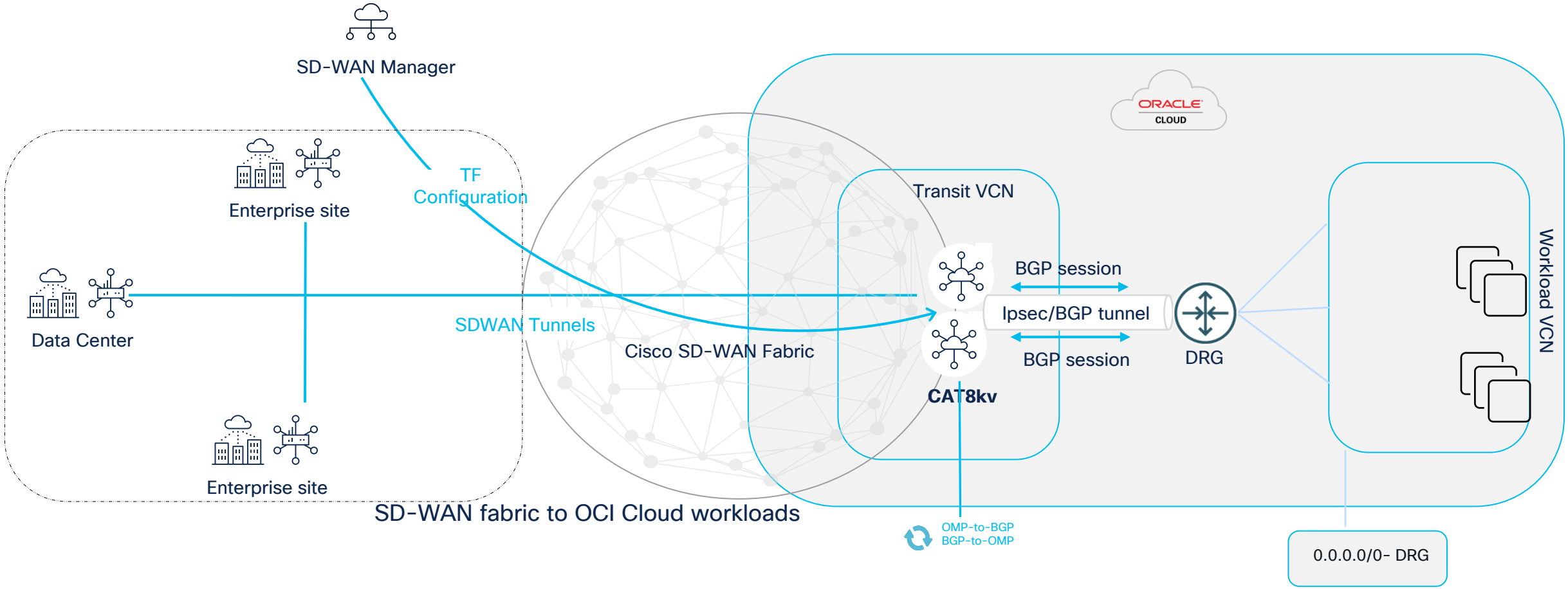
Simple | Automated | Secure

Automated with Cisco SD-WAN Manager

OCI support

OCI- Site-to-Cloud

SD-WAN Native Integration using **IKE**
IpsecTransit VCN cat8kv and DRG



Simple

Automated

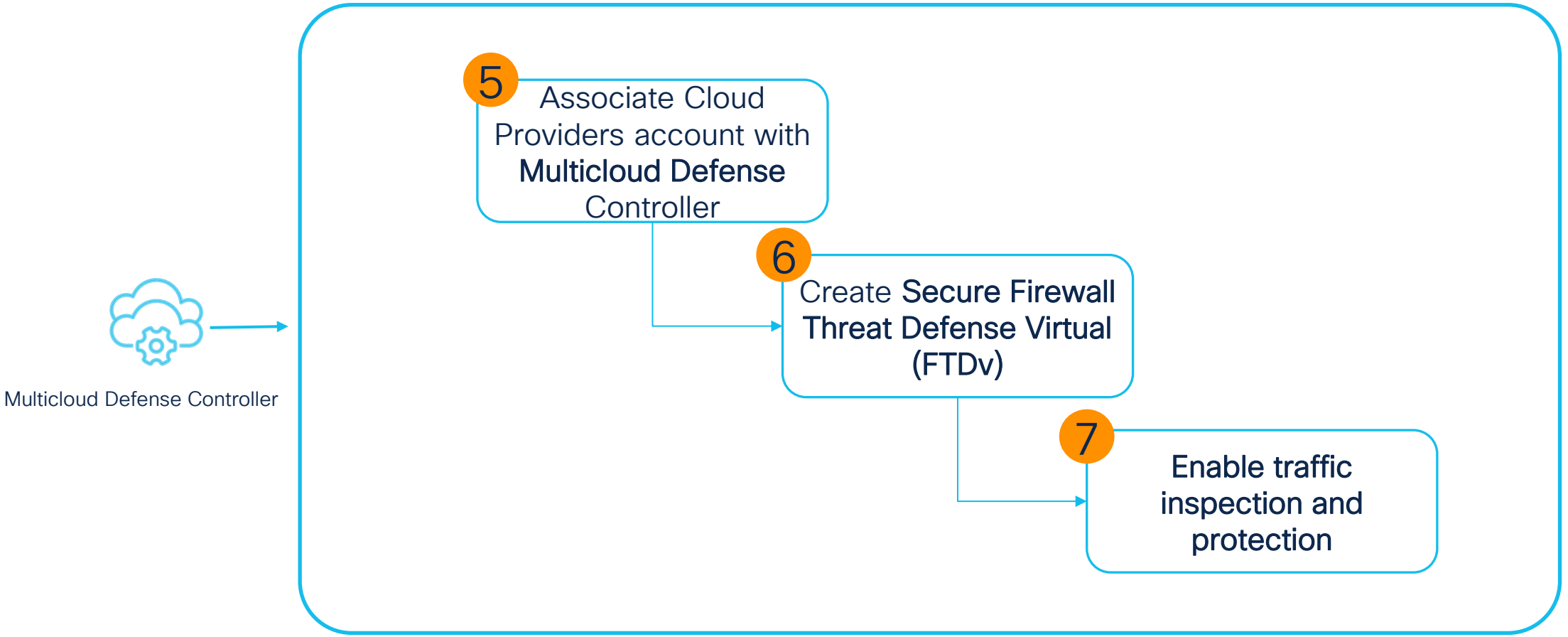
Secure

Security and Compliance with Cloud Networking

With Cisco Multicloud Defense

Multicloud Defense Workflow

Secure Connectivity achieved in minutes....



Cisco Multicloud Defense is the Multicloud Network Security Platform

Consolidated security for cloud networks to consistently connect and protect workloads and data

Inbound

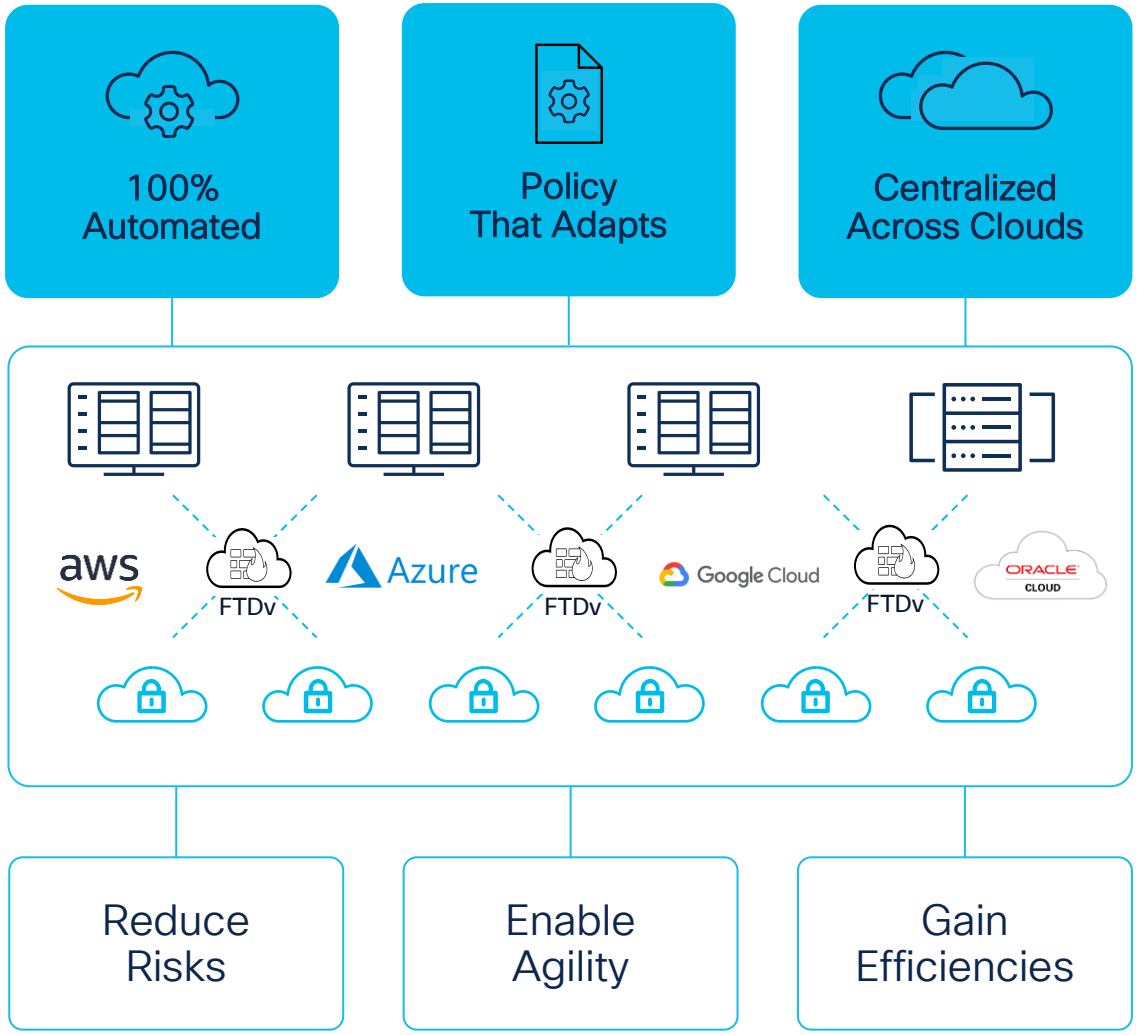
Stop Inbound Threats for Web & Non-Web Apps

Outbound

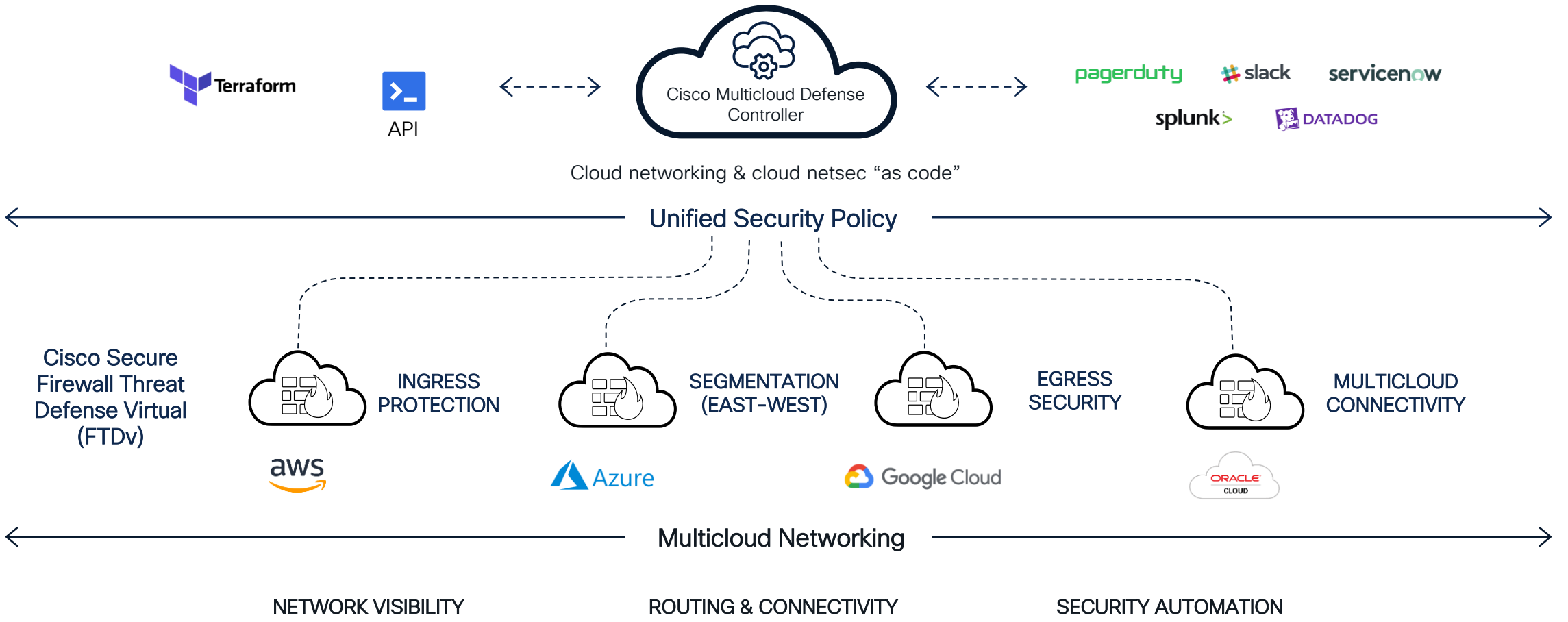
Block Command & Control, Botnets, Data Exfiltration

Lateral

Mitigate Attacker Movement



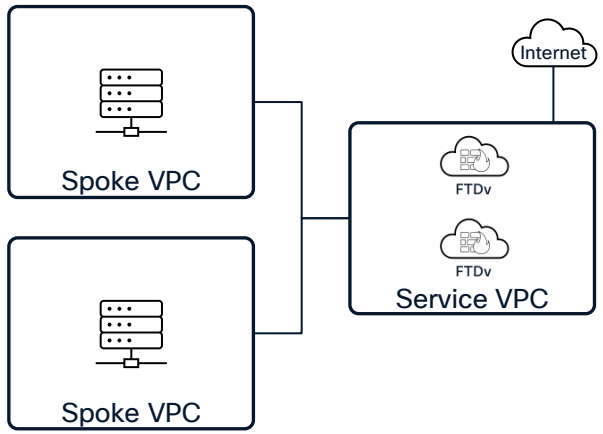
Cisco Multicloud Defense



cisco

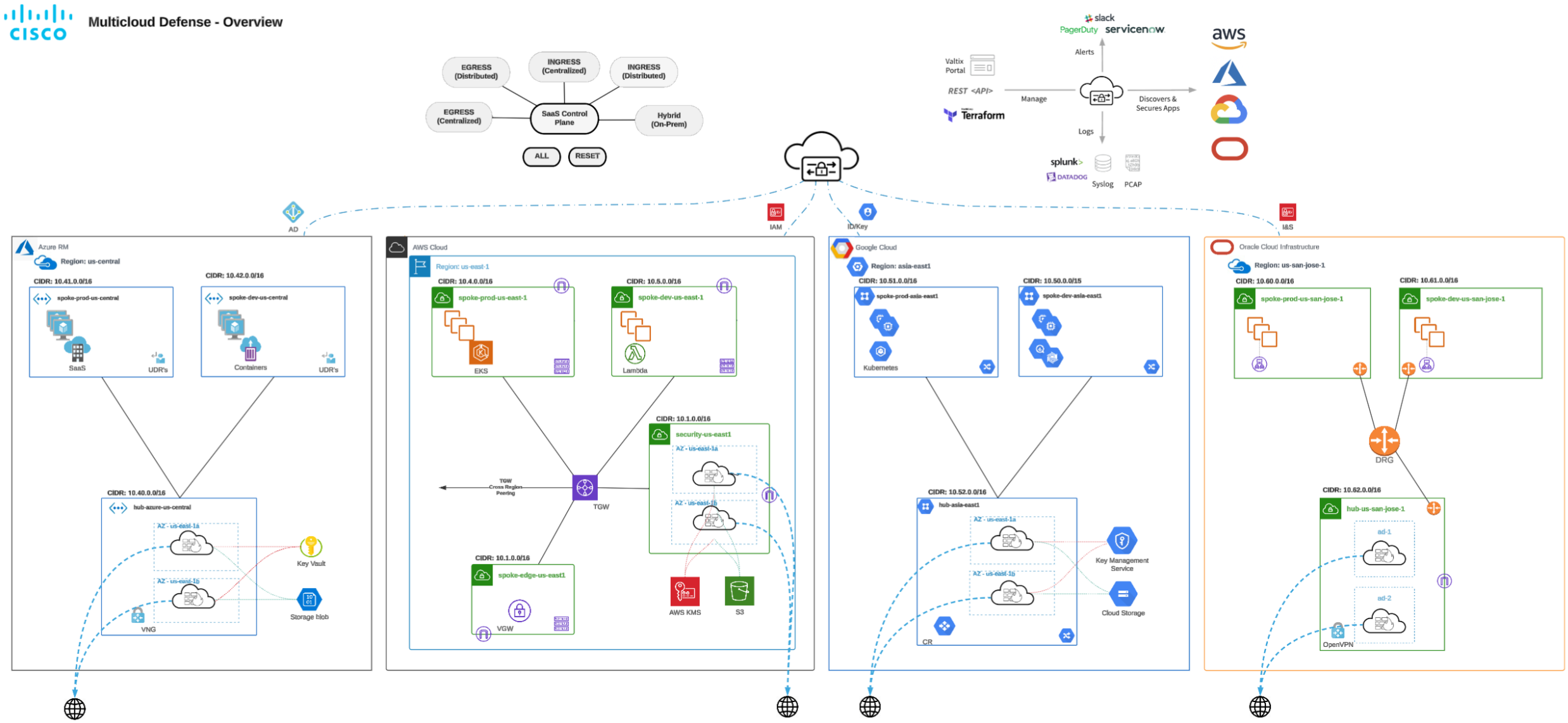
Security Model

- Firewalls are deployed in Service VPC
- Traffic from Spoke VPC is routed to Service VPC for inspection
- Traffic Inspection: Ingress, Egress, and E/W
- Fully orchestrated Load balancer sandwich model



Centralized Security Model

Multicloud Defense Architecture – Overview

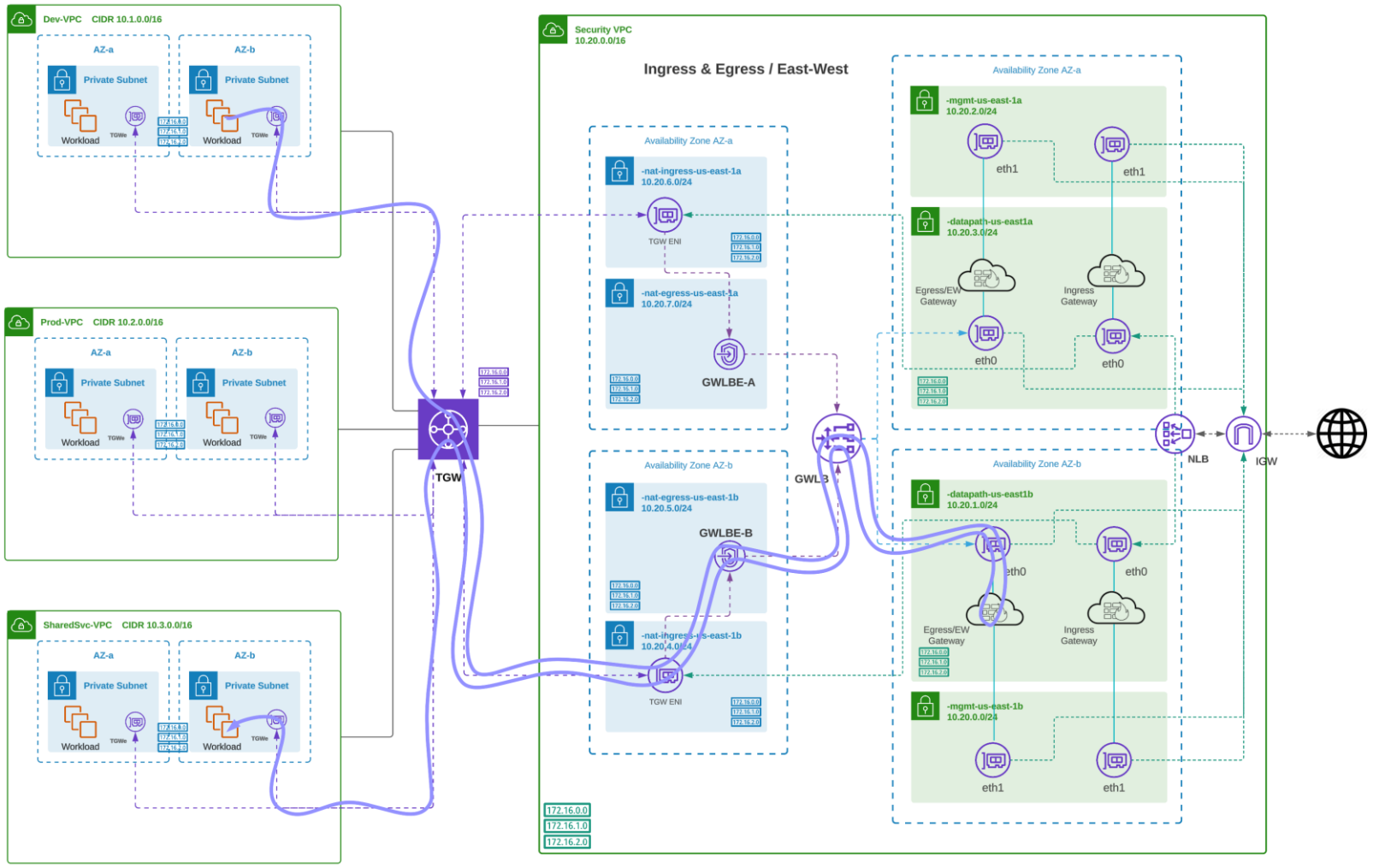


AWS Cloud Centralized

- East-West

Controller simplifies orchestration

- Security VPC
- Secure Firewall Threat Defense Virtual
  - Deployment
  - Insertion
  - Autoscaling
- AWS Transit Gateway
  - New or existing TGW
  - TGW attachment
- Traffic engineering (routing)
  - VPC subnet routing to TGW
- AWS GWLB for scalability



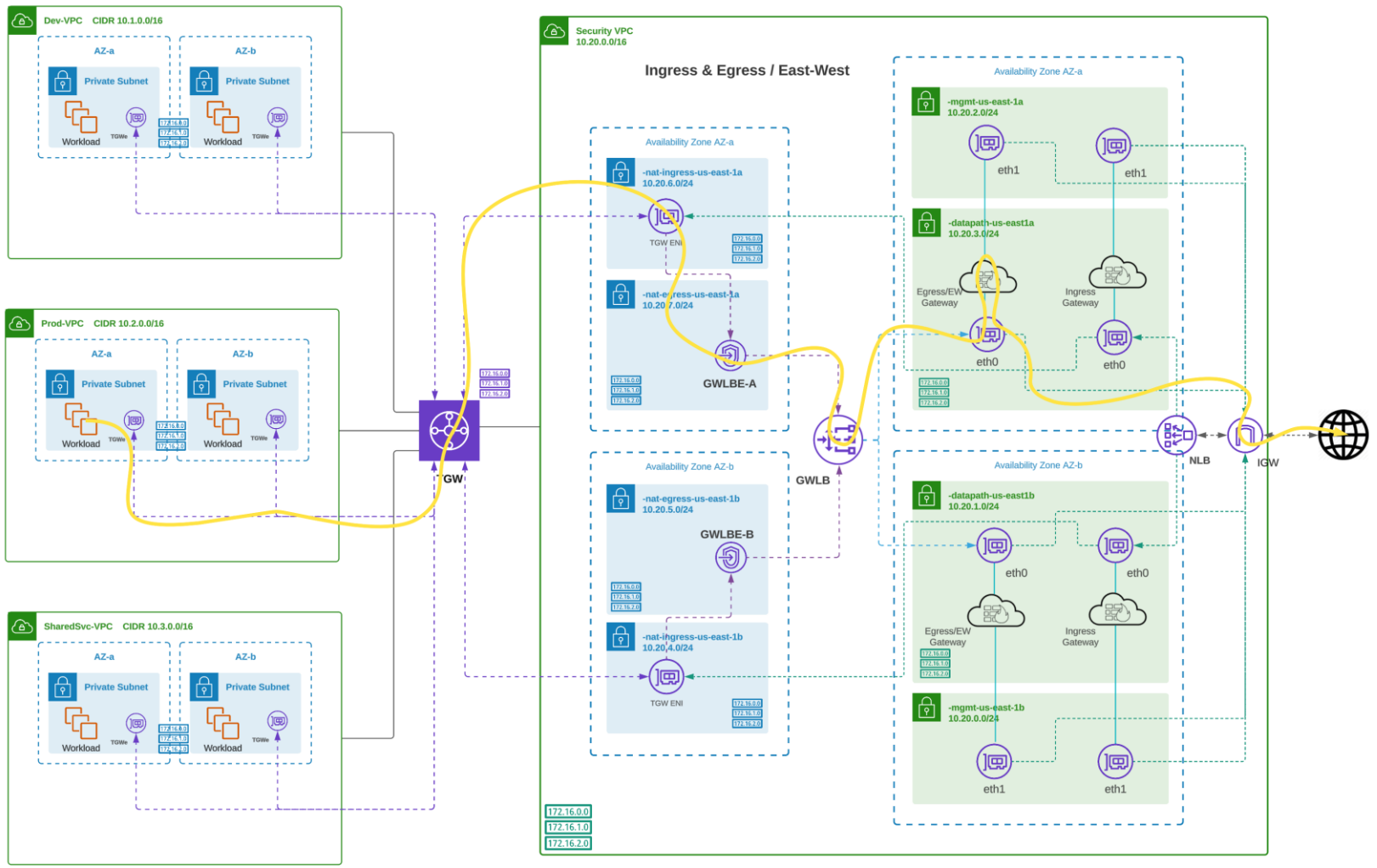
AWS Cloud Centralized – East-West Traffic Inspection

AWS Cloud Centralized

- Egress

Controller simplifies orchestration

- Security VPC
- Secure Firewall Threat Defense Virtual
  - Deployment
  - Insertion
  - Autoscaling
- AWS Transit Gateway
  - New or existing TGW
  - TGW attachment
- Traffic engineering (routing)
  - VPC subnet routing to TGW
- AWS GWLB for scalability



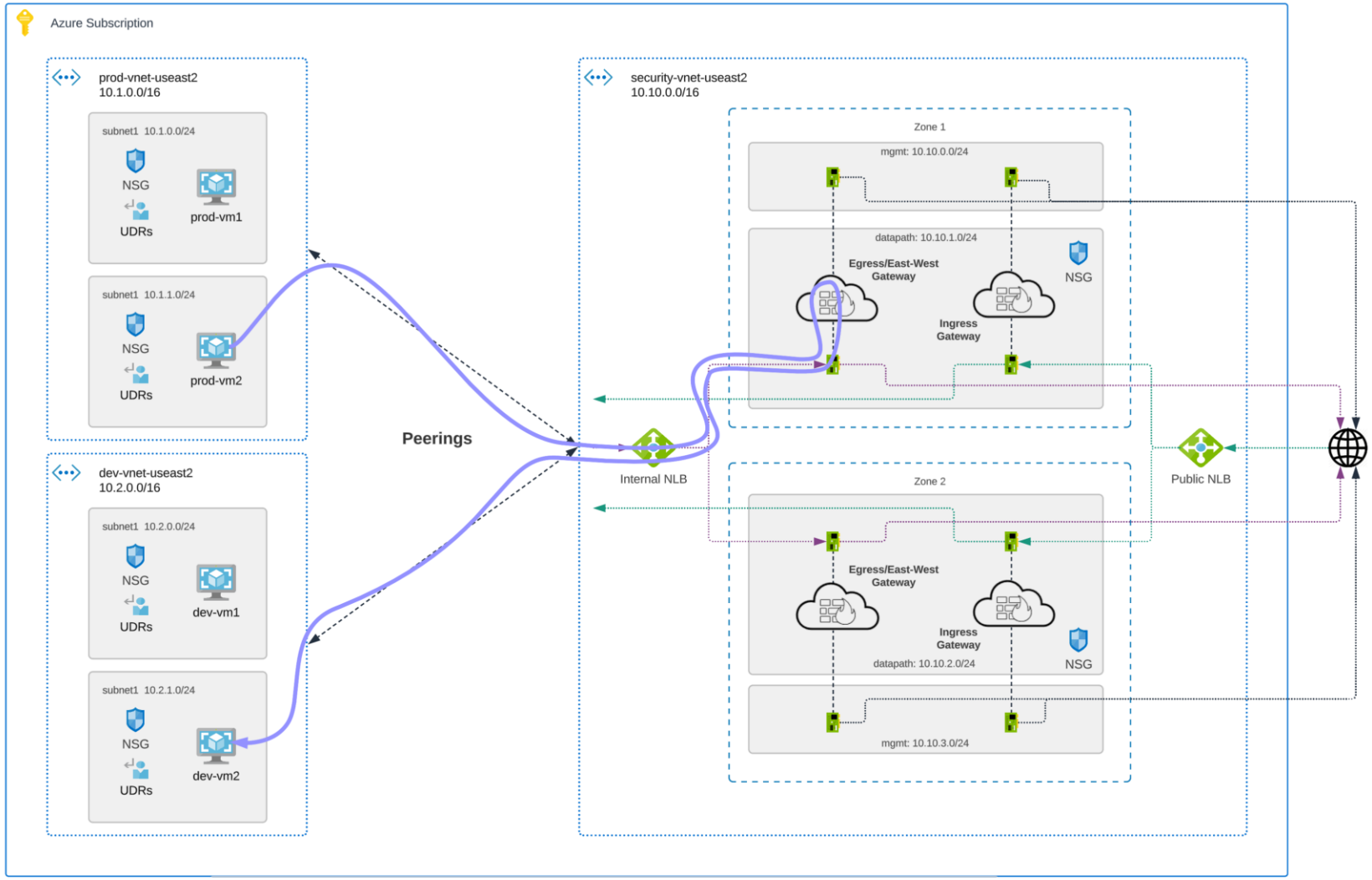
AWS Cloud Centralized – Egress Traffic Inspection

Azure Cloud Centralized

- East-West

Controller simplifies orchestration

- Security VNet
- Network Load Balancers
- Secure Firewall Threat Defense Virtual
  - Egress and East-West
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling



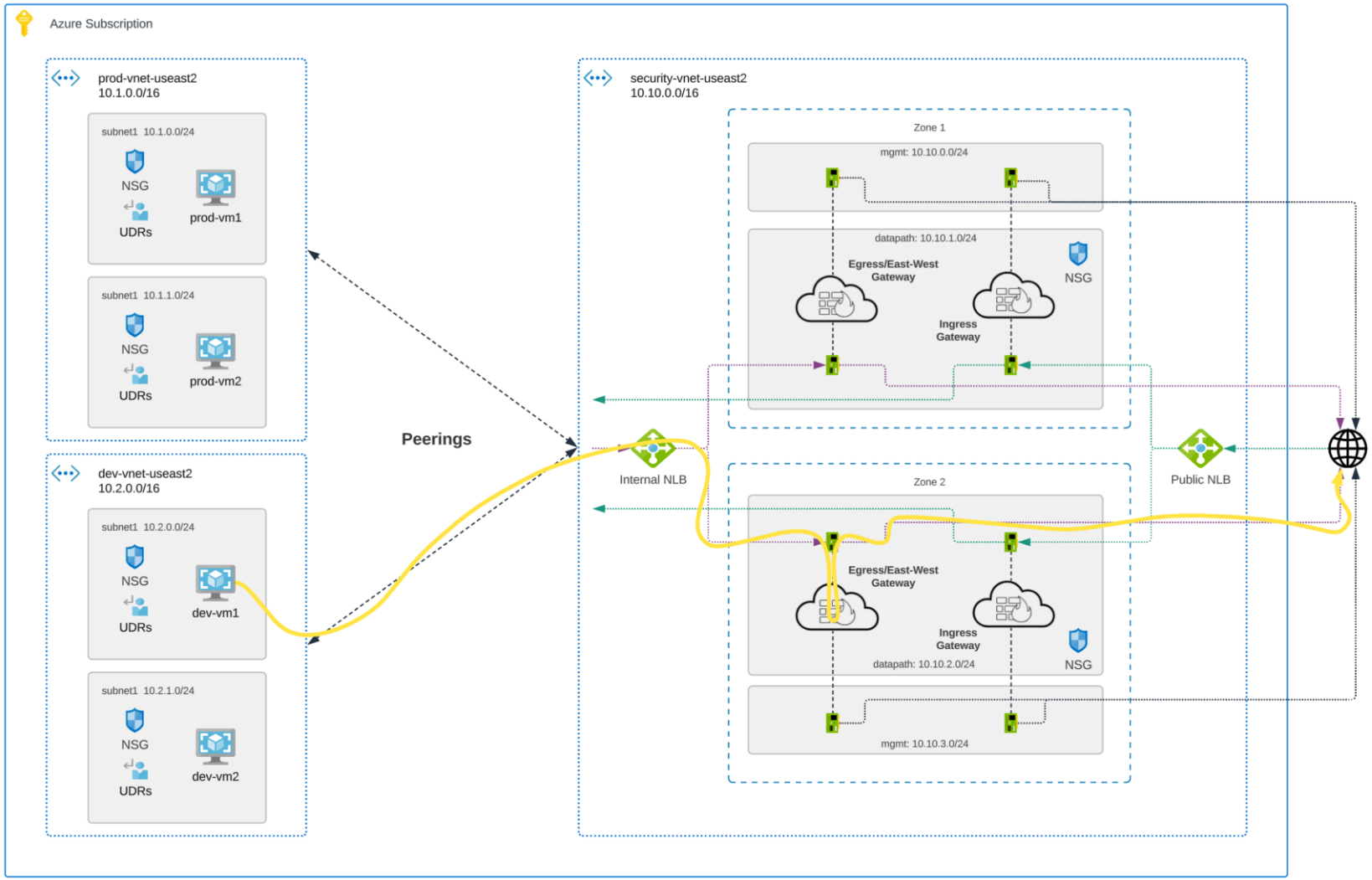
Azure Cloud Centralized – East-West Traffic Inspection

Azure Cloud Centralized

- Egress

Controller simplifies orchestration

- Security VNet
- Network Load Balancers
- Secure Firewall Threat Defense Virtual
  - Egress and East-West
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling



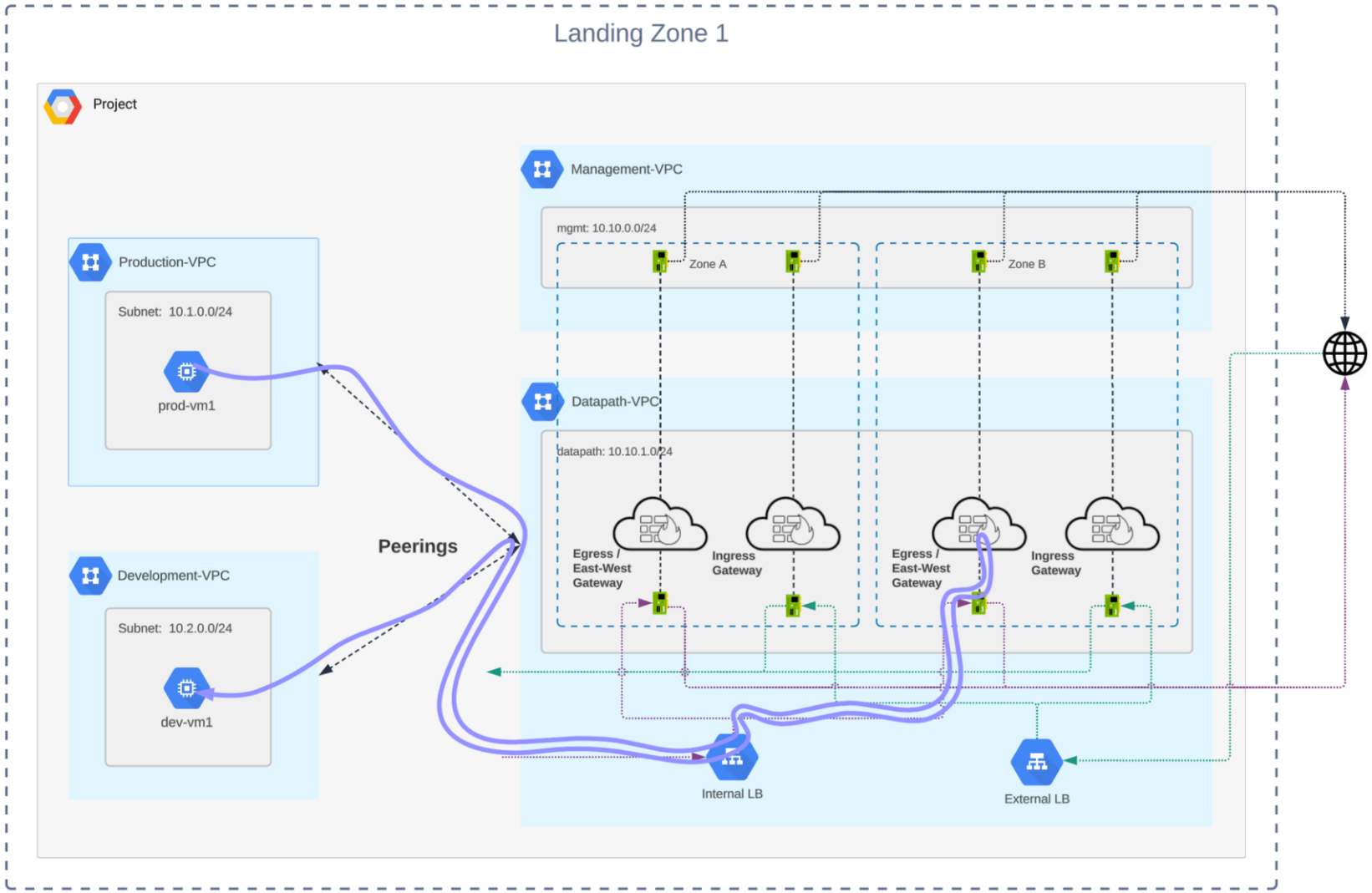
Azure Cloud Centralized – Egress Traffic Inspection

Google Cloud Centralized

- East-West

Controller simplifies orchestration

- Security VPC
- Network Load Balancers
  - Internal
- Secure Firewall Threat Defense Virtual
  - Ingress Traffic inspection
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling



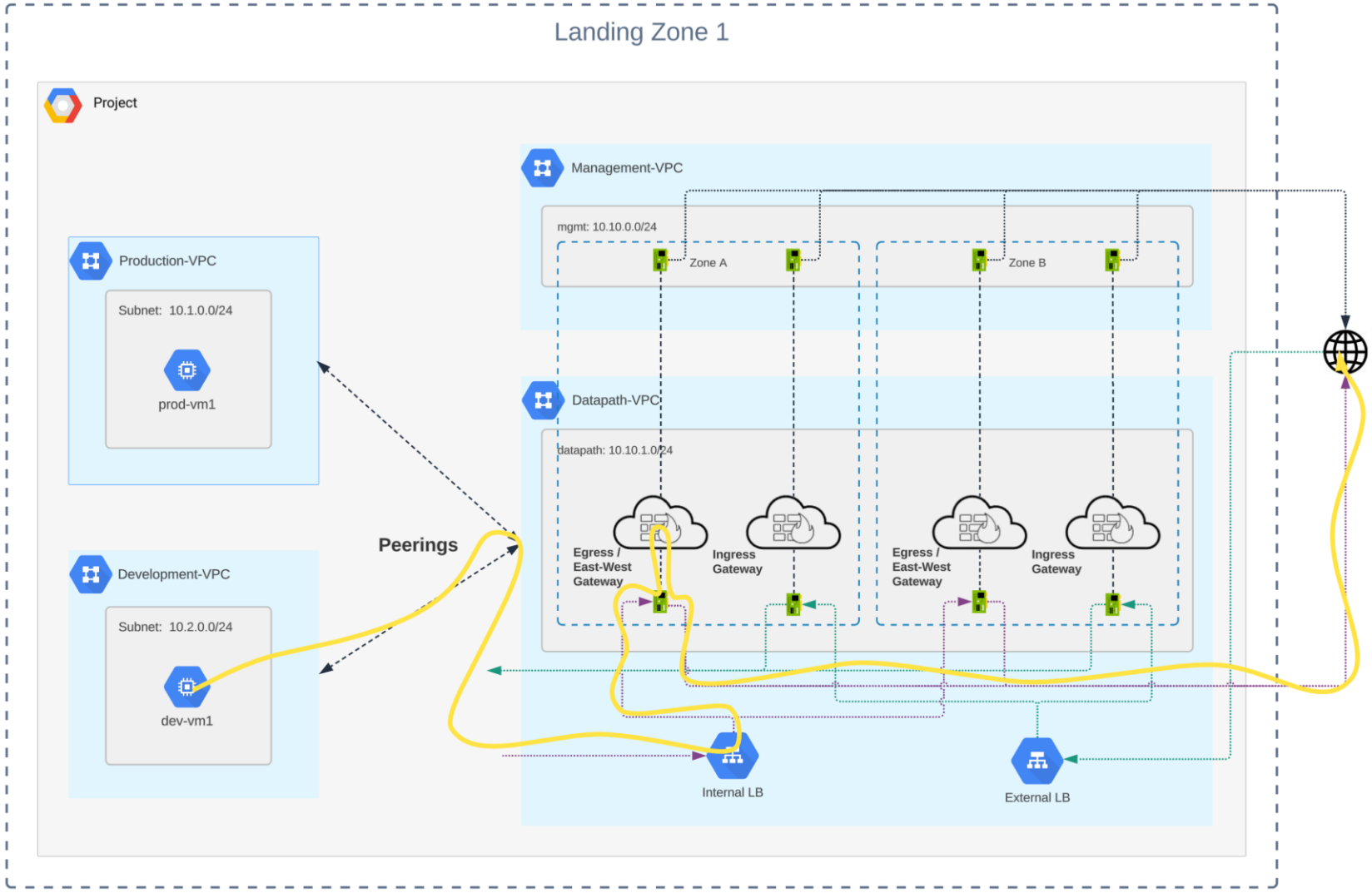
Google Cloud Centralized – East-West Traffic Inspection

Google Cloud Centralized

- Egress

Controller simplifies orchestration

- Security VPC
- Network Load Balancers
  - Internal
- Secure Firewall Threat Defense Virtual
  - Ingress Traffic inspection
- Automation
  - Peering
  - Routing
  - Load balancer configuration
  - Autoscaling

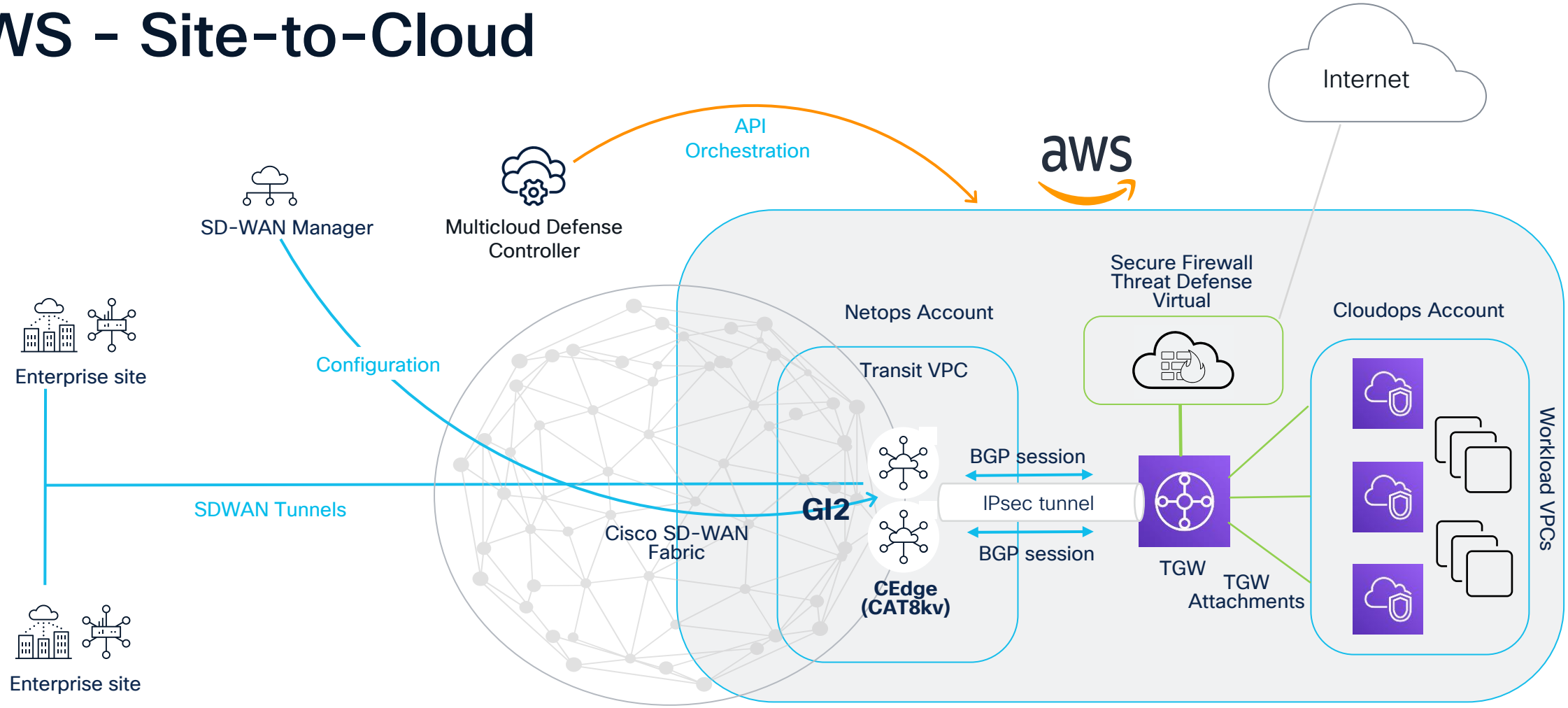


Google Cloud Centralized – Egress Traffic Inspection

Multicloud Defense + SDWAN

Secure connections

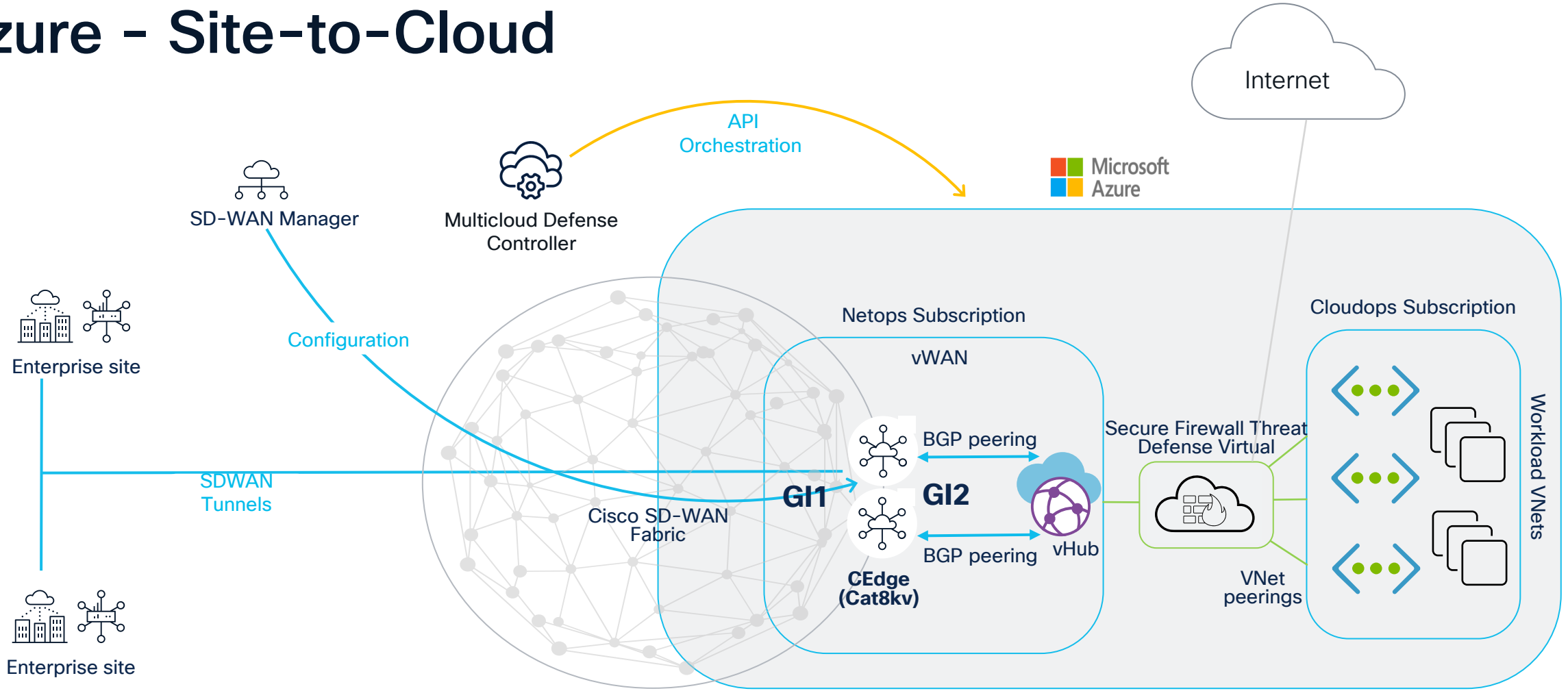
AWS - Site-to-Cloud



SD-WAN fabric **to** AWS Cloud workloads

Simple | Automated | Secure

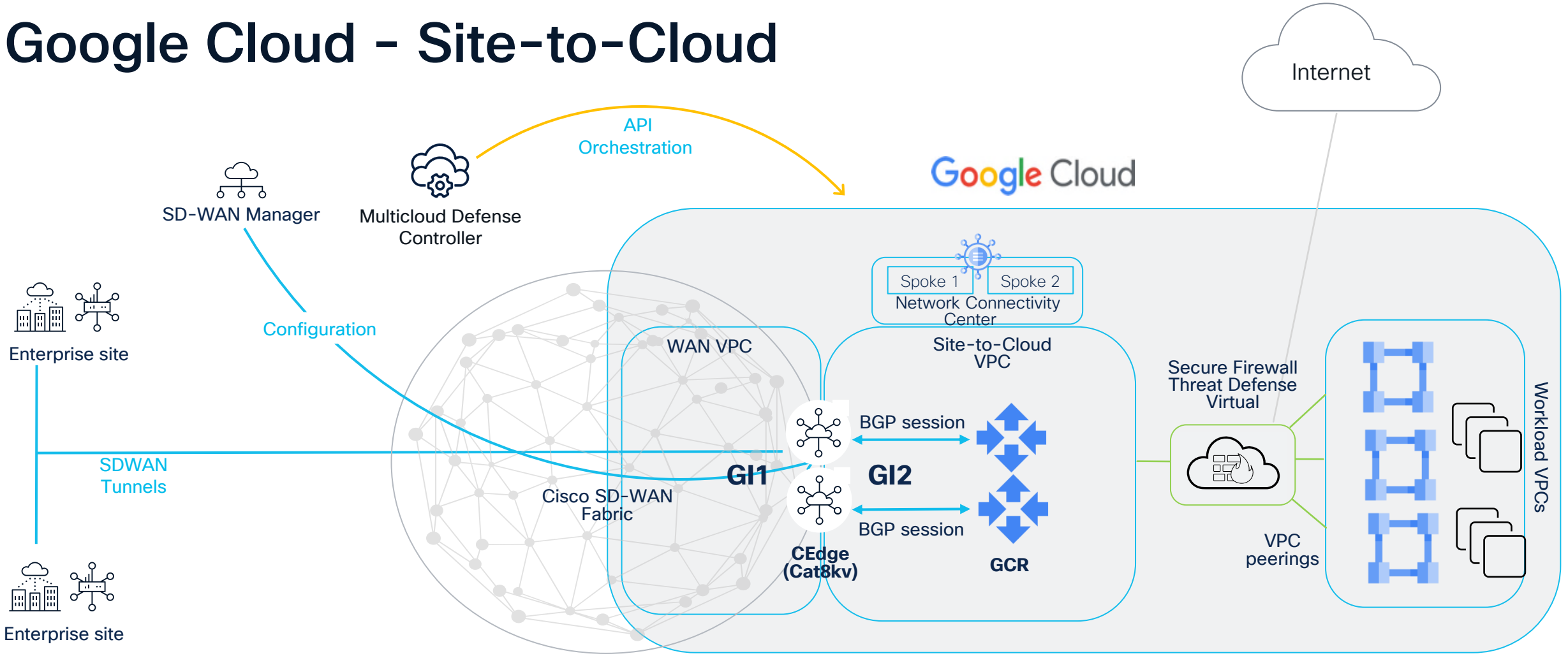
Azure - Site-to-Cloud



SD-WAN fabric **to** Azure Cloud workloads

Simple | Automated | Secure

Google Cloud - Site-to-Cloud



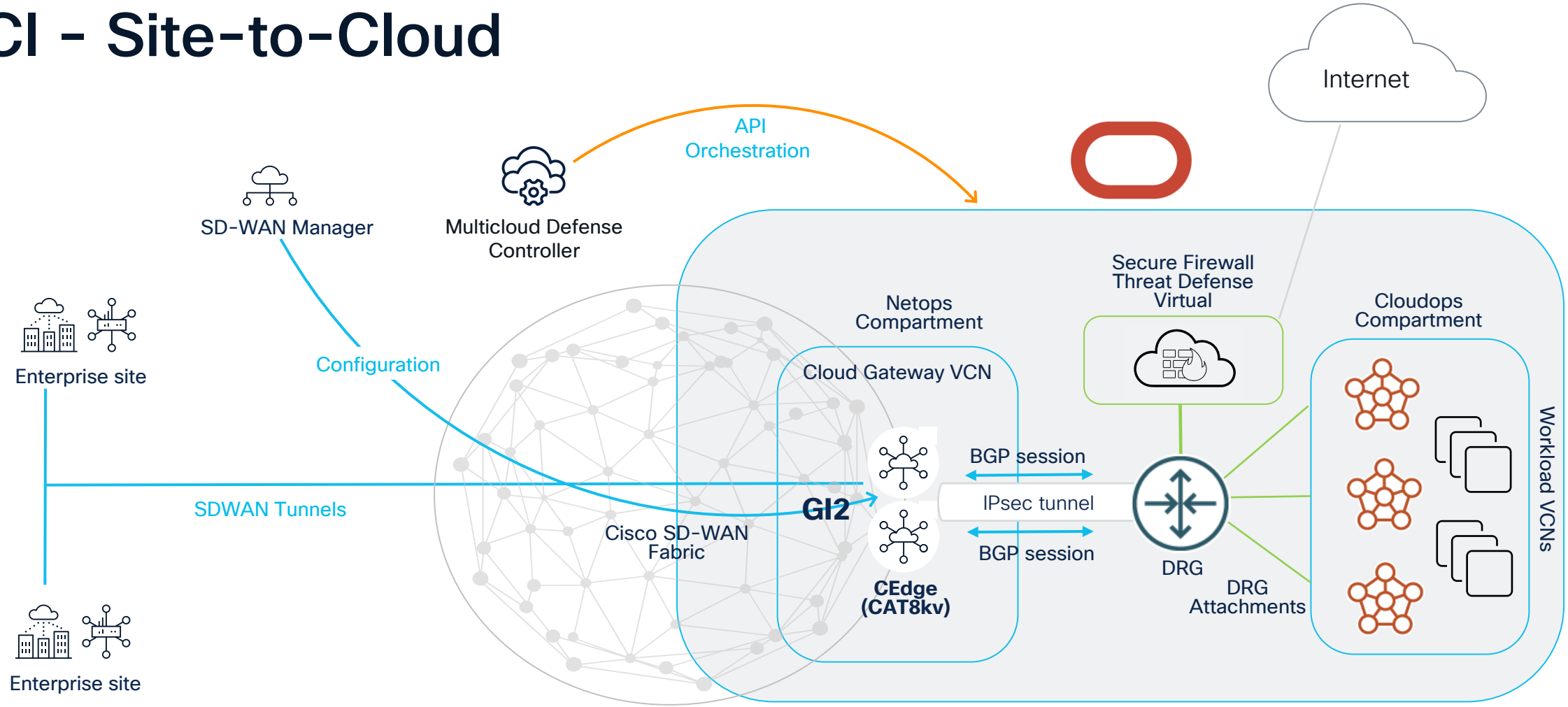
SD-WAN fabric **to** Google Cloud workloads

Simple

Automated

Secure

OCI - Site-to-Cloud

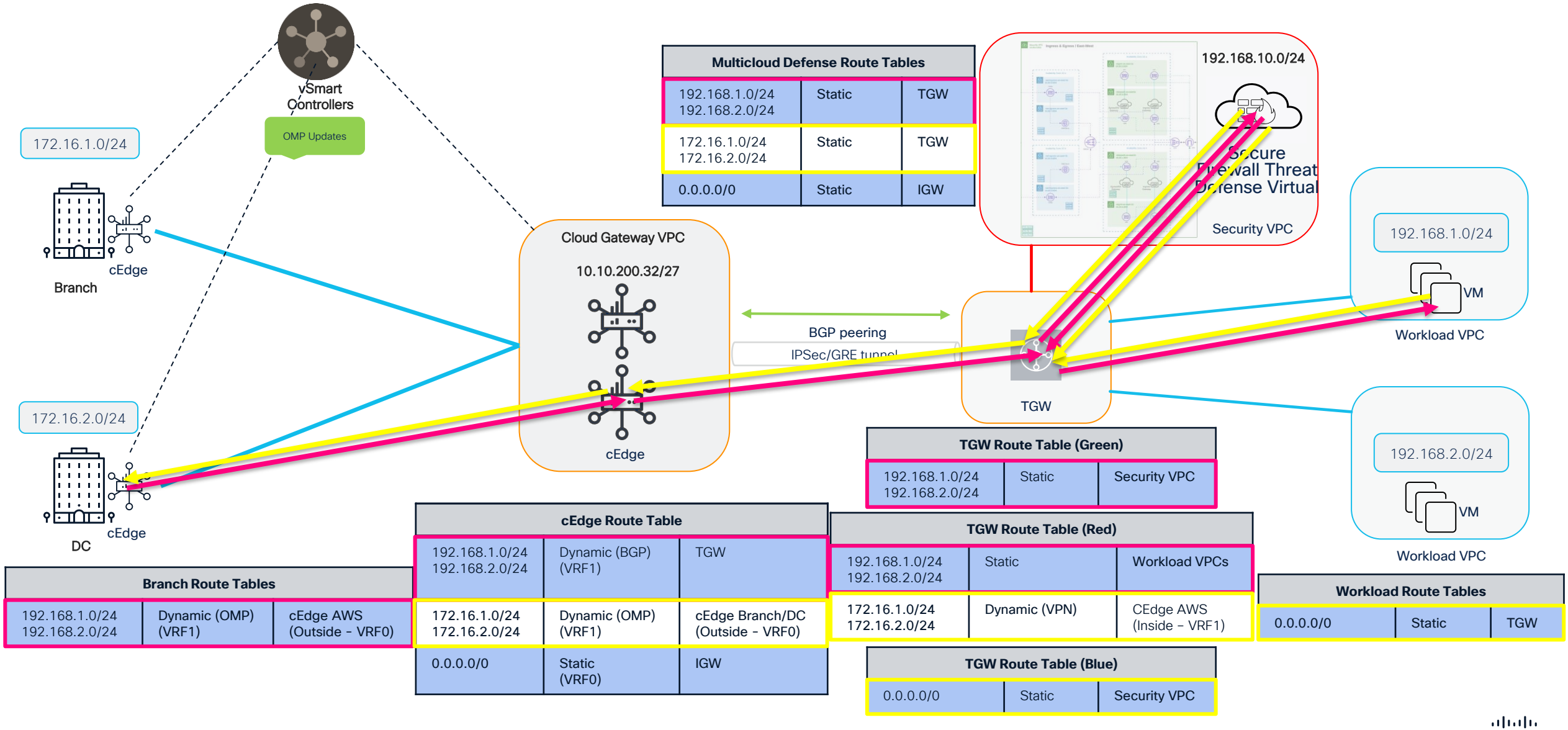


SD-WAN fabric **to** OCI Cloud workloads

Simple | Automated | Secure

Detailed Architecture

Branch to AWS Workload VPC Connectivity



Multicloud Defense Route Tables		
192.168.1.0/24 192.168.2.0/24	Static	TGW
172.16.1.0/24 172.16.2.0/24	Static	TGW
0.0.0.0/0	Static	IGW

TGW Route Table (Green)		
192.168.1.0/24 192.168.2.0/24	Static	Security VPC

cEdge Route Table		
192.168.1.0/24 192.168.2.0/24	Dynamic (BGP) (VRF1)	TGW
172.16.1.0/24 172.16.2.0/24	Dynamic (OMP) (VRF1)	cEdge Branch/DC (Outside - VRF0)
0.0.0.0/0	Static (VRF0)	IGW

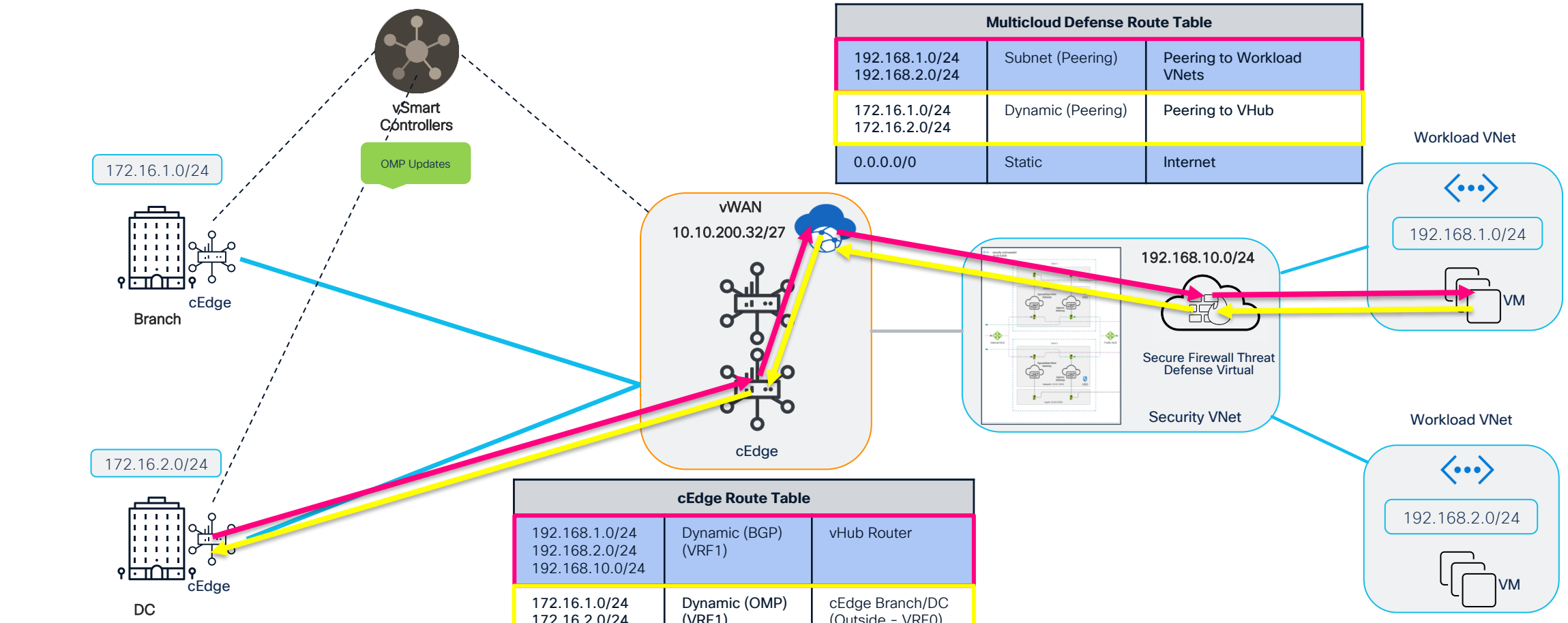
TGW Route Table (Red)		
192.168.1.0/24 192.168.2.0/24	Static	Workload VPCs
172.16.1.0/24 172.16.2.0/24	Dynamic (VPN)	CEdge AWS (Inside - VRF1)

Branch Route Tables		
192.168.1.0/24 192.168.2.0/24	Dynamic (OMP) (VRF1)	cEdge AWS (Outside - VRF0)

Workload Route Tables		
0.0.0.0/0	Static	TGW

TGW Route Table (Blue)		
0.0.0.0/0	Static	Security VPC

Branch to Azure Workload VNet Connectivity



Multicloud Defense Route Table		
192.168.1.0/24 192.168.2.0/24	Subnet (Peering)	Peering to Workload VNets
172.16.1.0/24 172.16.2.0/24	Dynamic (Peering)	Peering to VHub
0.0.0.0/0	Static	Internet

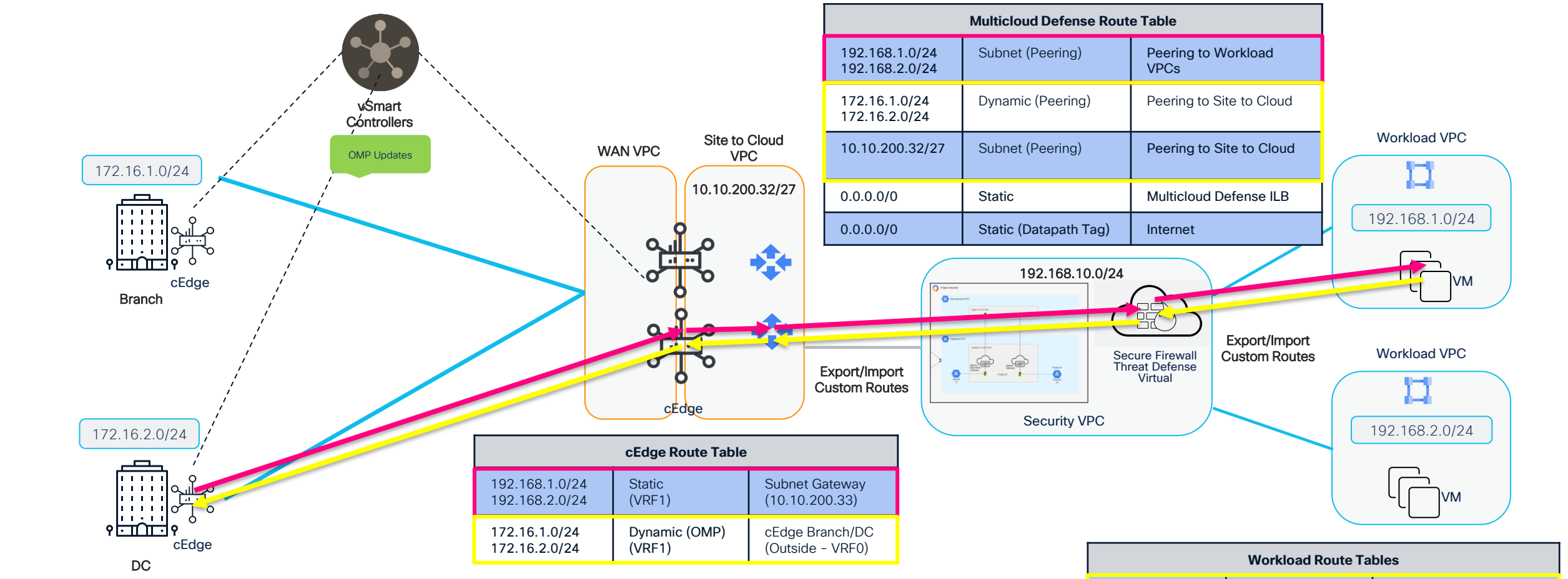
cEdge Route Table		
192.168.1.0/24 192.168.2.0/24 192.168.10.0/24	Dynamic (BGP) (VRF1)	vHub Router
172.16.1.0/24 172.16.2.0/24	Dynamic (OMP) (VRF1)	cEdge Branch/DC (Outside - VRF0)

Branch Route Tables		
192.168.1.0/24 192.168.2.0/24	Dynamic (OMP) (VRF1)	cEdge Azure (Outside - VRF0)

vHub Route Table		
192.168.1.0/24 192.168.2.0/24	Static	Multicloud Defense ILB
172.16.1.0/24 172.16.2.0/24	Dynamic (BGP)	cEdge Azure (Inside - VRF1)

Workload Route Tables		
192.168.10/24	Subnet (Peering)	Peering to Security VNet
0.0.0.0/0	Static	Multicloud Defense ILB

Branch to GCP Workload VPC Connectivity



Multicloud Defense Route Table		
192.168.1.0/24 192.168.2.0/24	Subnet (Peering)	Peering to Workload VPCs
172.16.1.0/24 172.16.2.0/24	Dynamic (Peering)	Peering to Site to Cloud
10.10.200.32/27	Subnet (Peering)	Peering to Site to Cloud
0.0.0.0/0	Static	Multicloud Defense ILB
0.0.0.0/0	Static (Datapath Tag)	Internet

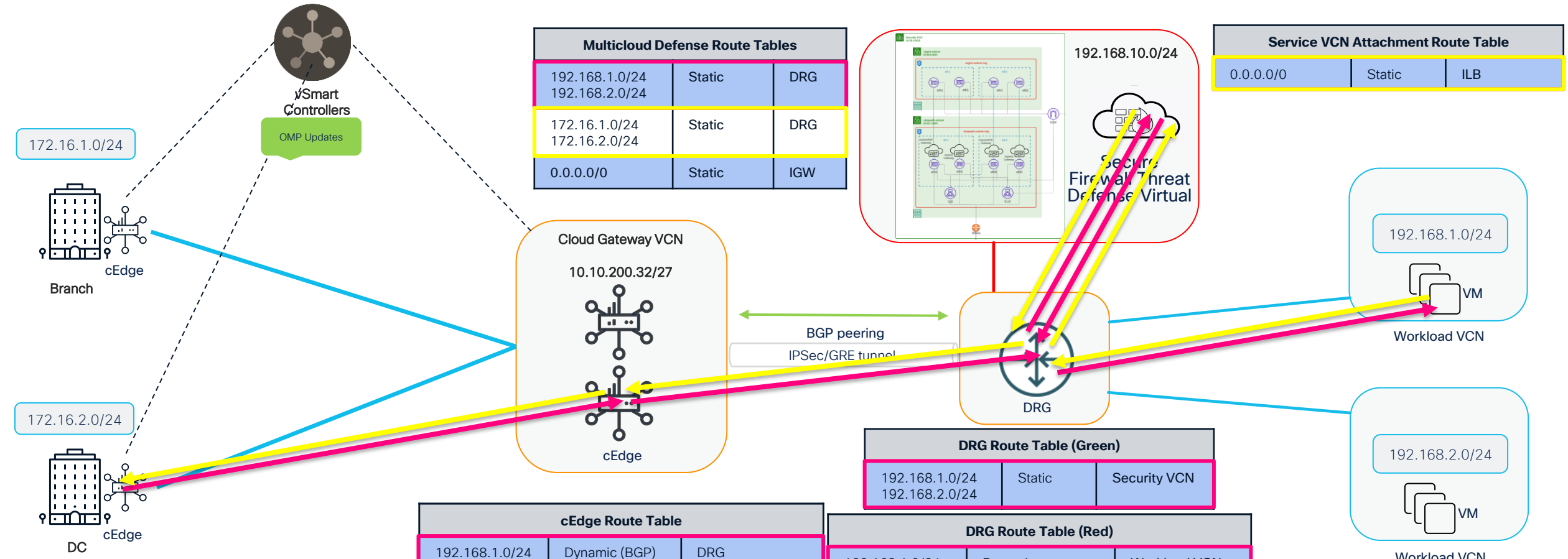
cEdge Route Table		
192.168.1.0/24 192.168.2.0/24	Static (VRF1)	Subnet Gateway (10.10.200.33)
172.16.1.0/24 172.16.2.0/24	Dynamic (OMP) (VRF1)	cEdge Branch/DC (Outside - VRF0)

Branch Route Tables		
192.168.1.0/24 192.168.2.0/24	Dynamic (OMP) (VRF1)	cEdge GCP (Outside - VRF0)

Site to Cloud Route Table		
172.16.1.0/24 172.16.2.0/24	Dynamic (BGP)	cEdge GCP (Inside- VRF1)
0.0.0.0/0	Static (Peering)	Multicloud Defense ILB

Workload Route Tables		
192.168.10/24	Subnet (Peering)	Peering to Security VPC
0.0.0.0/0	Static (Peering)	Multicloud Defense ILB

Branch to OCI Workload VCN Connectivity



Multicloud Defense Route Tables		
192.168.1.0/24 192.168.2.0/24	Static	DRG
172.16.1.0/24 172.16.2.0/24	Static	DRG
0.0.0.0/0	Static	IGW

Service VCN Attachment Route Table		
0.0.0.0/0	Static	ILB

Branch Route Tables		
192.168.1.0/24 192.168.2.0/24	Dynamic (OMP) (VRF1)	cEdge AWS (Outside - VRF0)

cEdge Route Table		
192.168.1.0/24 192.168.2.0/24	Dynamic (BGP) (VRF1)	DRG
172.16.1.0/24 172.16.2.0/24	Dynamic (OMP) (VRF1)	cEdge Branch/DC (Outside - VRF0)
0.0.0.0/0	Static (VRF0)	IGW

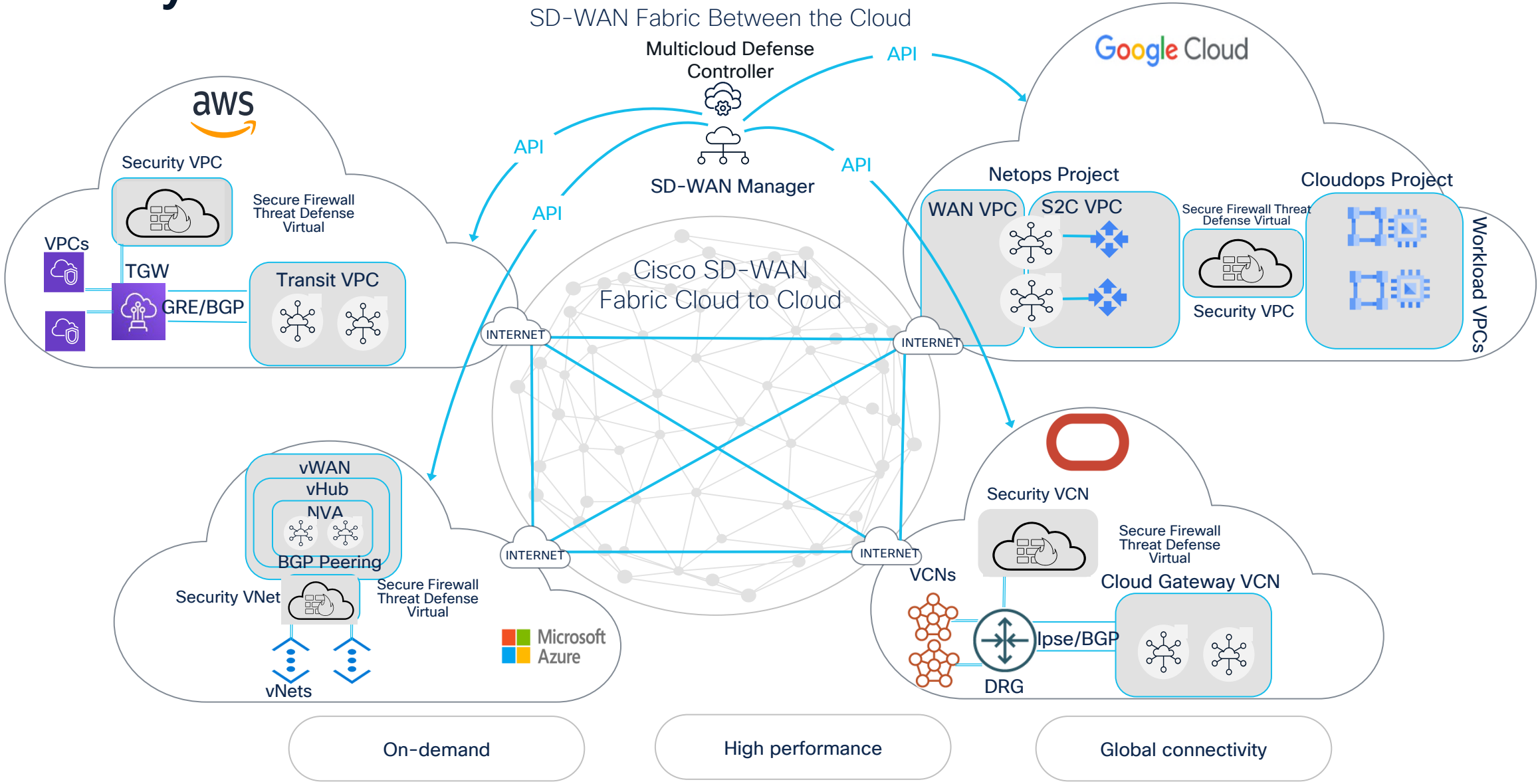
DRG Route Table (Green)		
192.168.1.0/24 192.168.2.0/24	Static	Security VCN

DRG Route Table (Red)		
192.168.1.0/24 192.168.2.0/24	Dynamic (Attachments)	Workload VCNs
172.16.1.0/24 172.16.2.0/24	Dynamic (VPN)	cEdge OCI (Inside - VRF1)

DRG Route Table (Blue)		
0.0.0.0/0	Static	Security VCN

Workload Route Tables		
0.0.0.0/0	Static	DRG

Security Stack Insertion in the Cloud



What’s New?

Multicloud Defense and AI Defense

Cisco AI Defense

AI Security Journey

Safely enable generative AI across your organization

Discovery

Uncover shadow AI workloads, apps, models, and data

Detection

Test for AI risk, vulnerabilities, and adversarial attacks

Protection

Place guardrails and access policies to secure data and defend against runtime threats

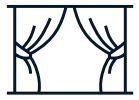
The AI Defense Solution

Complete your session surveys

Complete your surveys in the Cisco Events App.

Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Thank you

cisco Live !


CISCO