

SD-WAN—How to Design Multicloud Networking

cisco Live !

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

Session ID: BRKENS-2561

Agenda

- 01 Introduction to Cloud Networking**
- 02 Infrastructure Transition**
- 03 Cloud Connectivity Options
Cisco Recommended and**
- 04 Automated Cloud
Networking Design**
- 05 Security and Compliance in
Cloud Networking**

Introduction to Cloud Networking

Cloud Models

Public Cloud

Private Cloud

Hybrid Cloud

Multi-Cloud

Cloud Connectivity

Direct Connect

Virtual Private Networks

Express-route

Interconnect Services

SD-WAN Fabric

Cloud-native Networking Services

Virtual Private Clouds

Transit Gateway

AWS Cloud WAN

Virtual Private Network

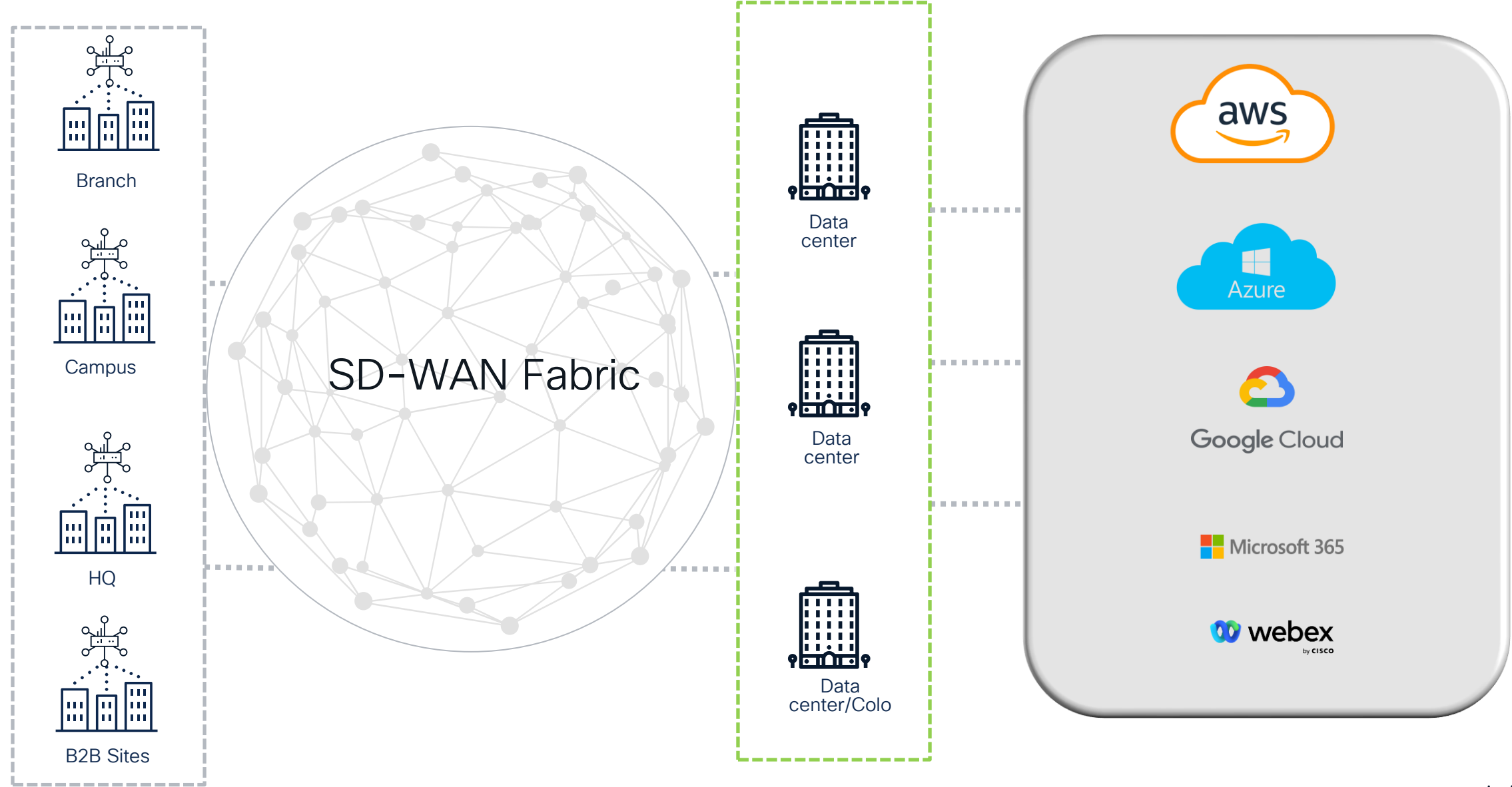
vWAN/vHub

Google Cloud Router

Network connectivity Centre

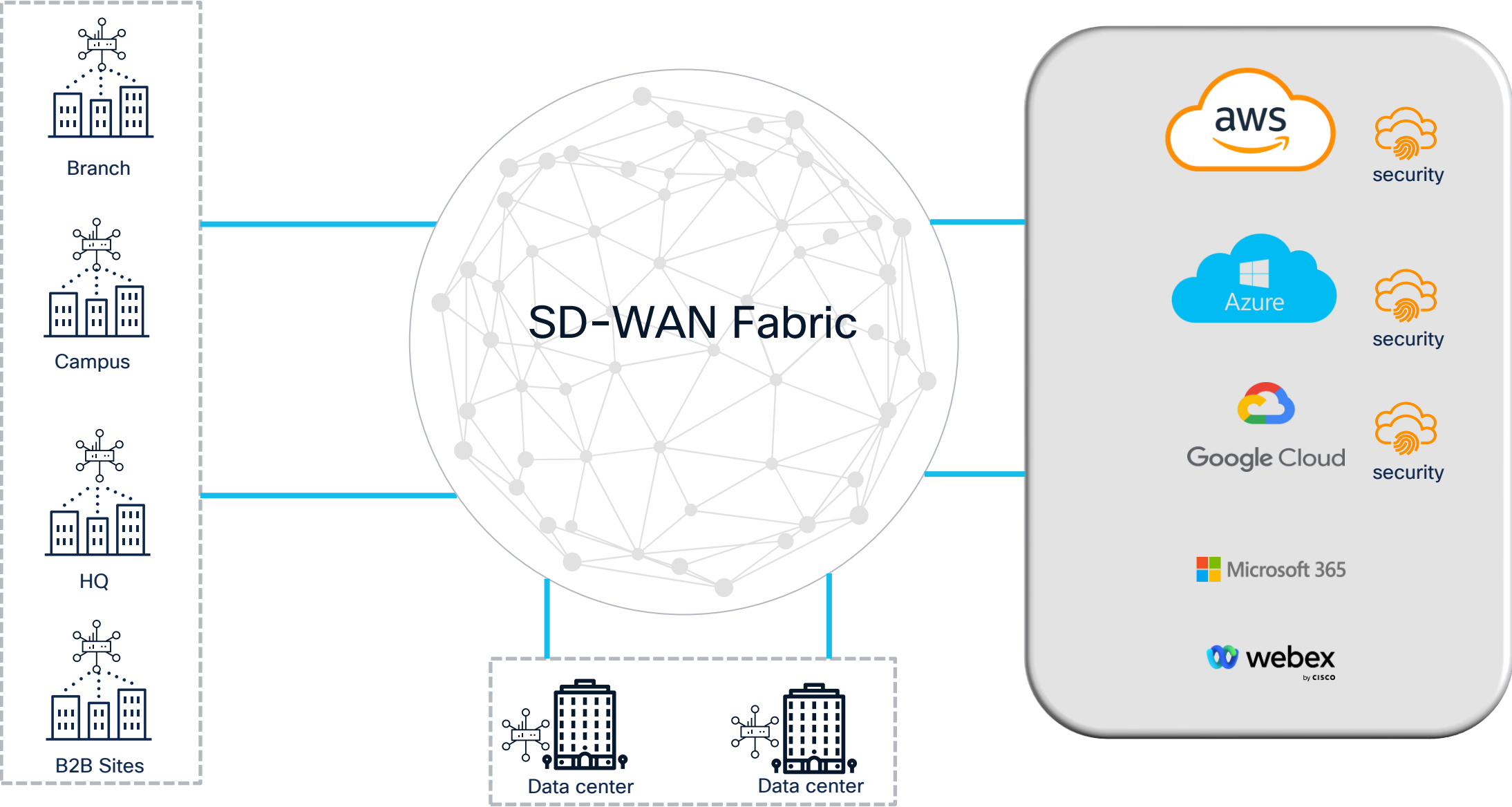
Infrastructure Transition

Infrastructure transition

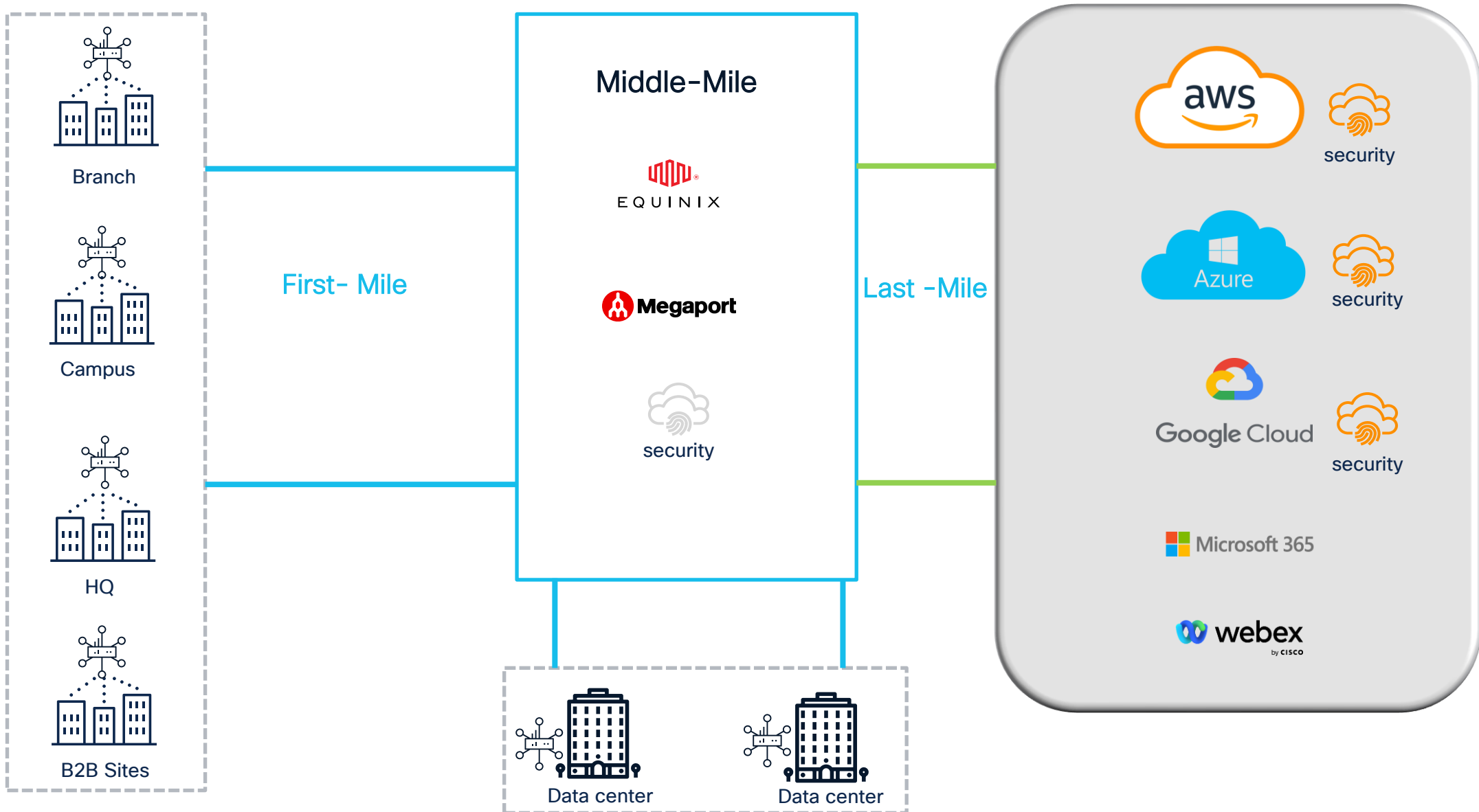


Cloud Connectivity Options

Architecture Option - 1 - Direct access to the Cloud



Architecture Option 2- via Cloud interconnect



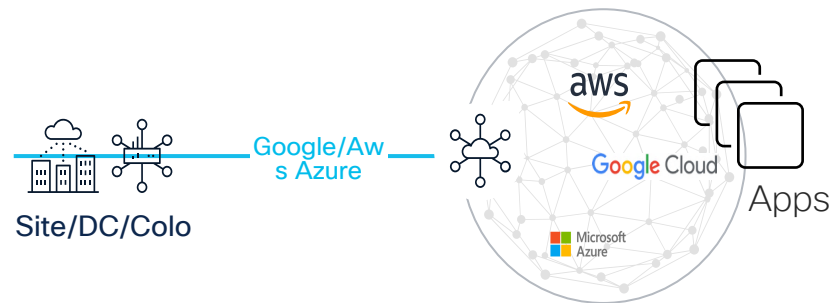
Cisco Recommended and Automated Cloud Networking Design

Cloud Networking & Security Use cases

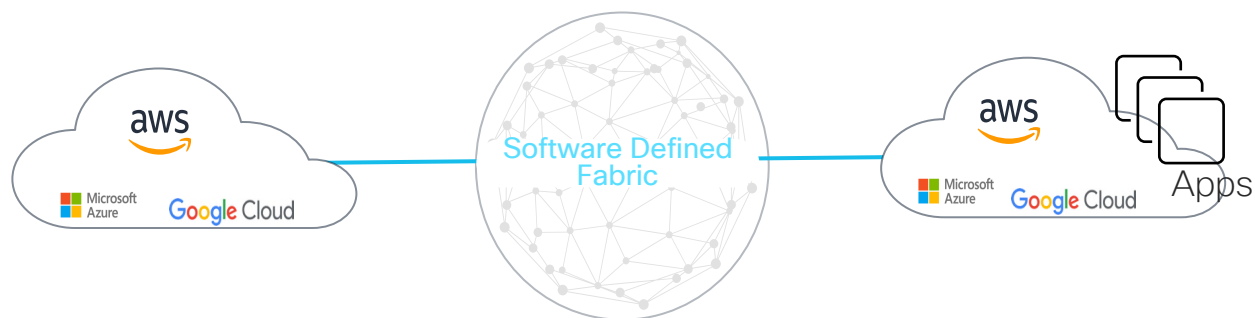
Cisco SD-WAN & Multicloud Defense

-  = Cisco SD-WAN virtual router hosted at Cloud Service Provider POP
-  = Cisco SD-WAN router on-premises
-  = Multicloud Defense

Site to Multicloud



Site to Site



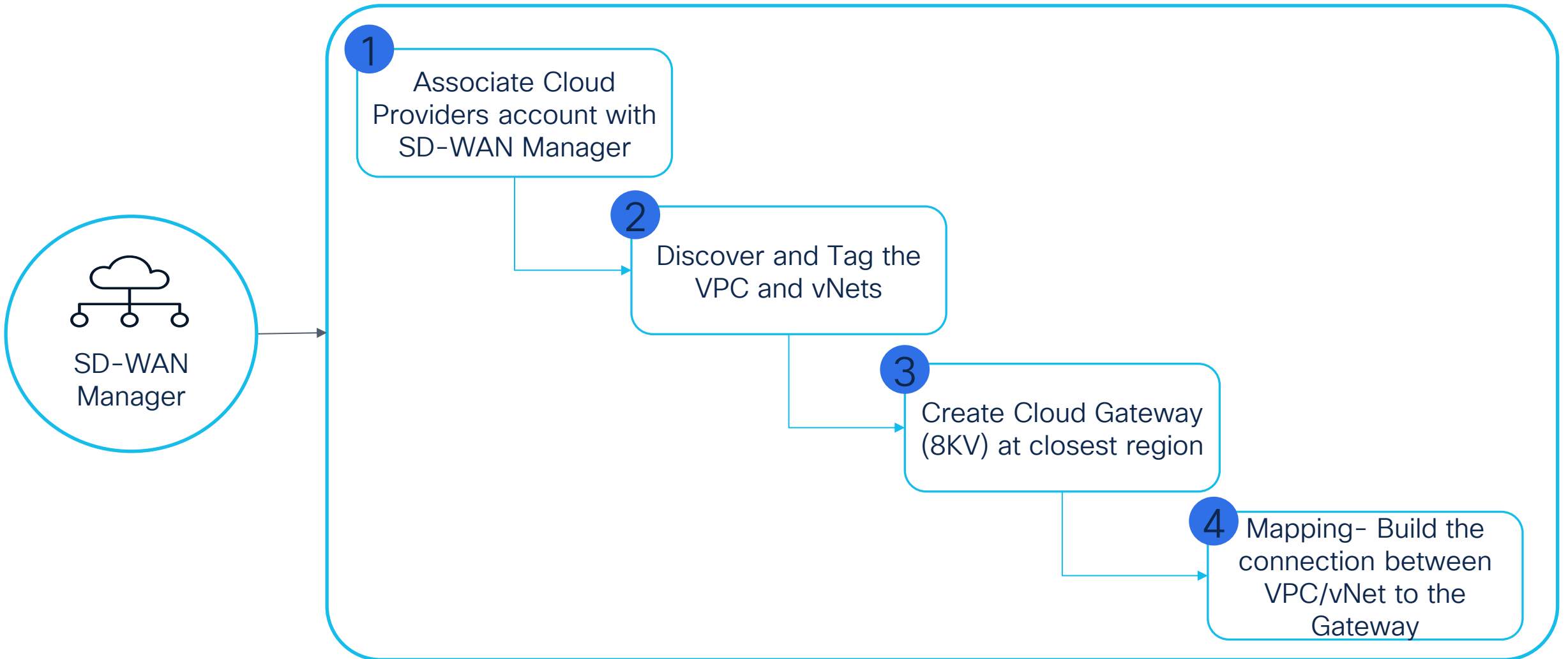
Region to Region & Cloud to Cloud

Inspection In & Between the Cloud



Multicloud Networking Workflow

Secure Connectivity achieved in minutes....



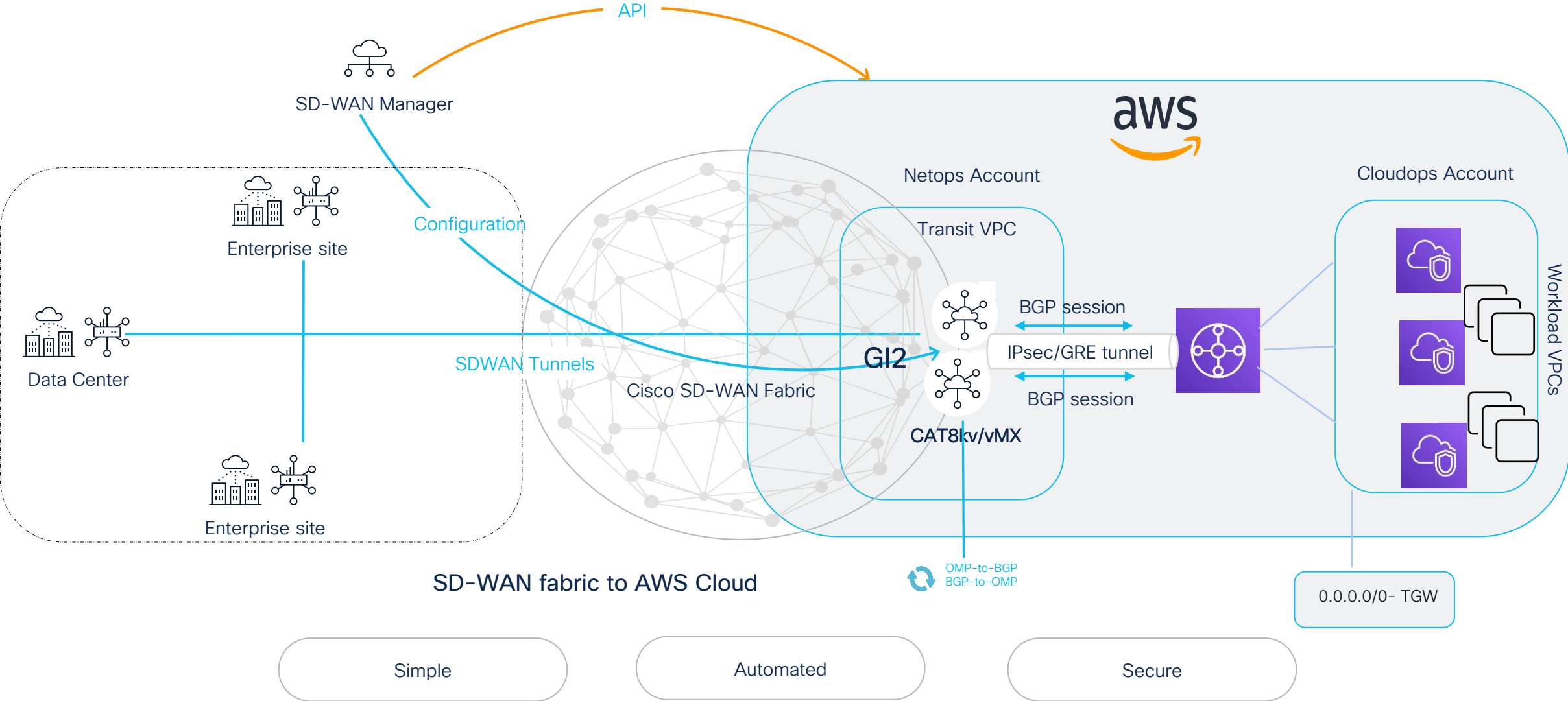
Let's get into details

SDWAN Integration + Design with AWS

Site to Multicloud

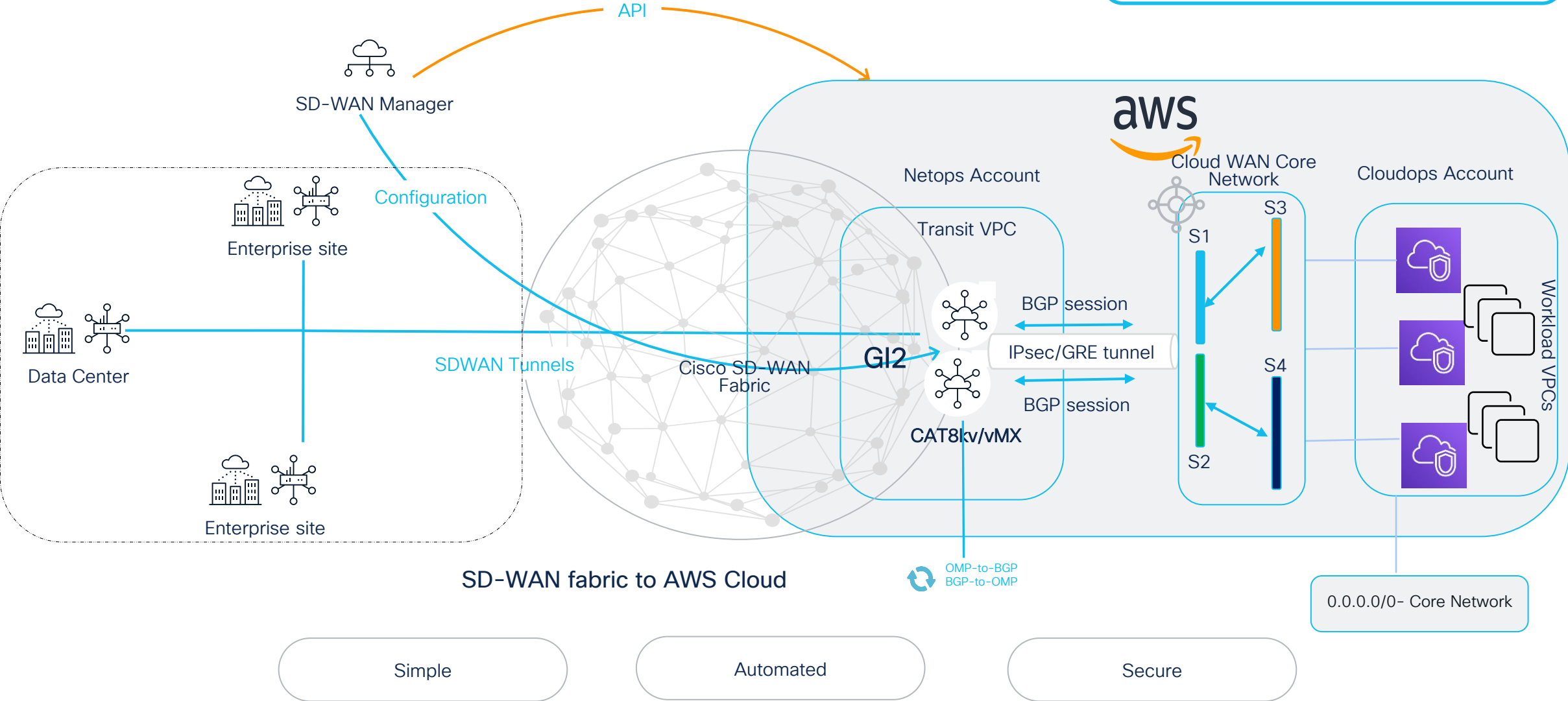
Site-to-Cloud with TGW

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



Site-to-Cloud with Cloud WAN

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



Site-to-Cloud with TGW-Brownfield

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

CiscoCatalyst WANCiti BankMonitorConfigurationToolsMaintenanceAdministrationWorkflowsAnalyticsExplore

Cloud OnRamp for MulticloudCreate Cloud Gateway

1 Select provider

2 Configure site parameters

3 Configure device parameters

4 Summary

Select provider

ProviderAmazon Web Service

Account nameDev-account

Cloud gateway namecgw1

Region

DescriptionValue

Transit gateway (TGW) settings

Create new TGW

Use existing TGW - connect now

Use existing TGW - connect later

Select an existing TGW

TGW-1

Attachment(s) to TGW

SD-WAN VPN

VPN-100

Associated route table

rt-default

+ Add attachments

Reset all

Cancel

All changes saved

Next

Connection diagram

Image description

Host VPC

Host VPC

Host VPC

AWS Transit Gateway

IPSec

Transit VPC

C8000v(s)

Cloud Gateway

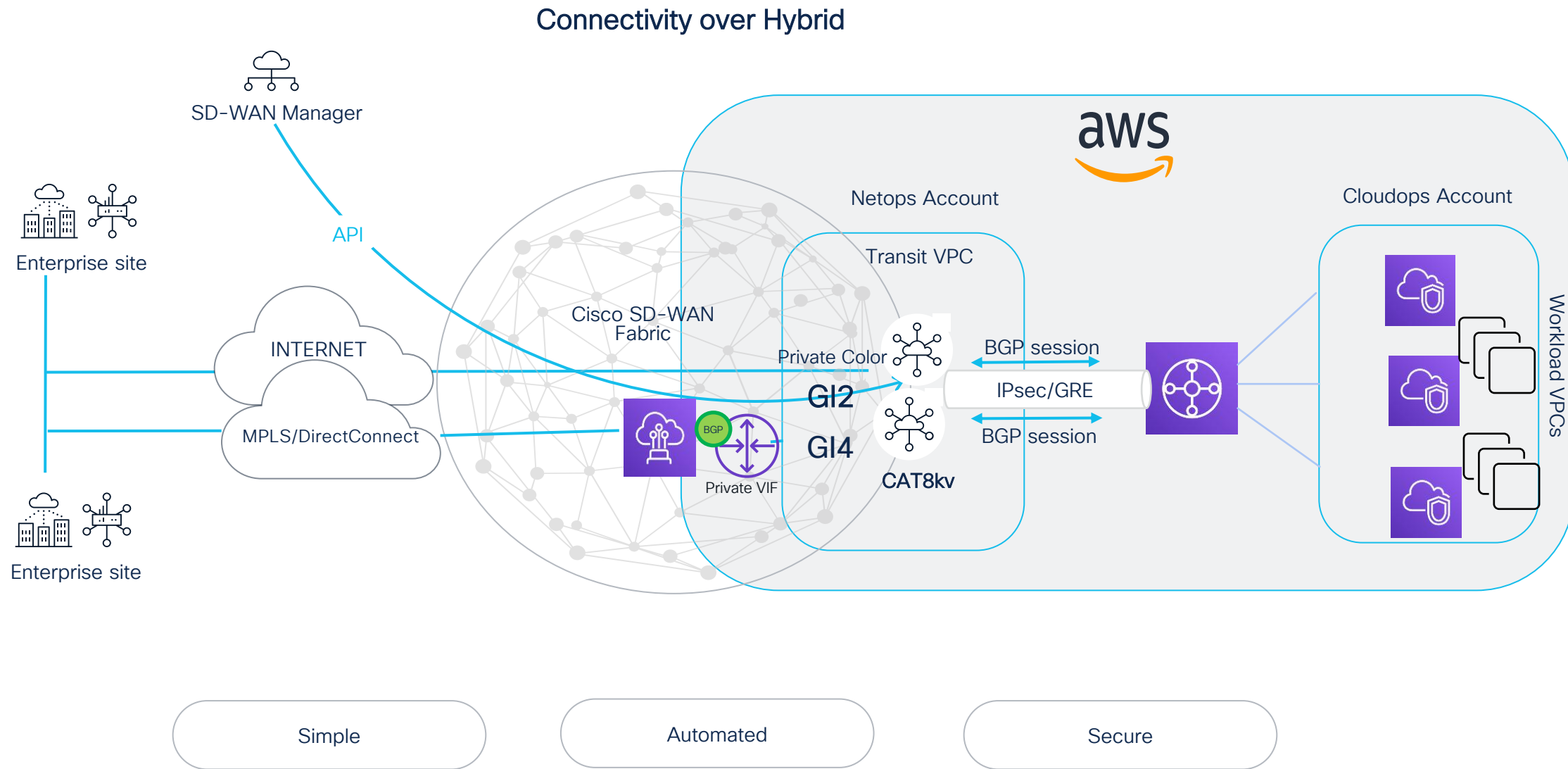
Branches

© 2024 Cisco Systems, Inc.

Privacy policy

Terms of service

On-Prem to AWS- Resilient connectivity

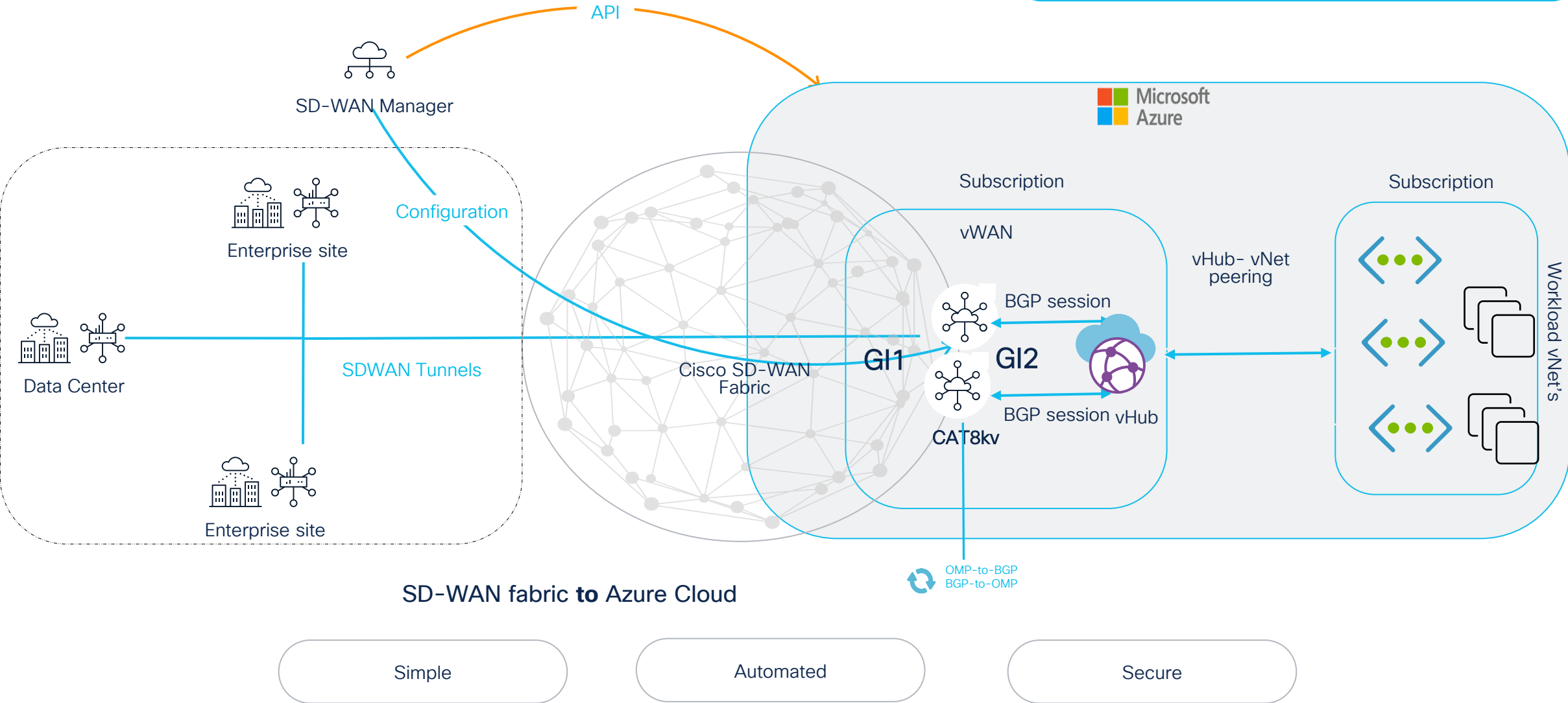


SDWAN Integration + Design with Azure

Site to Multicloud

Azure - Site-to-Cloud

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



SD-WAN fabric to Azure Cloud

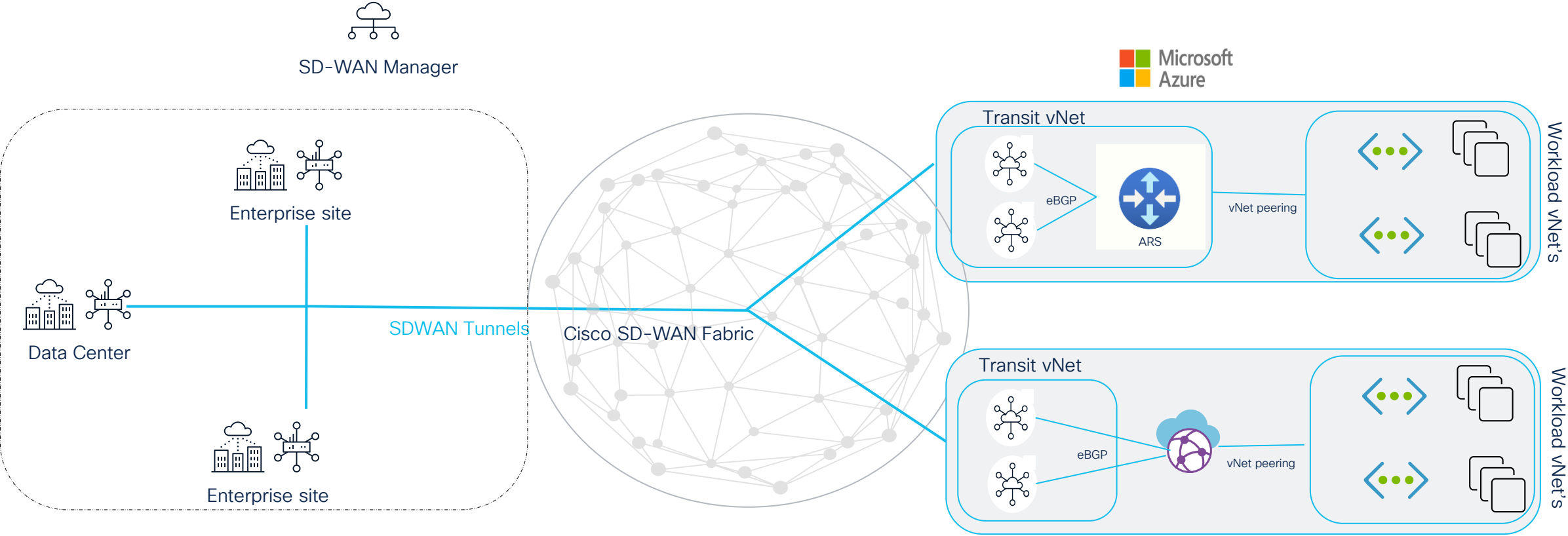
Simple

Automated

Secure

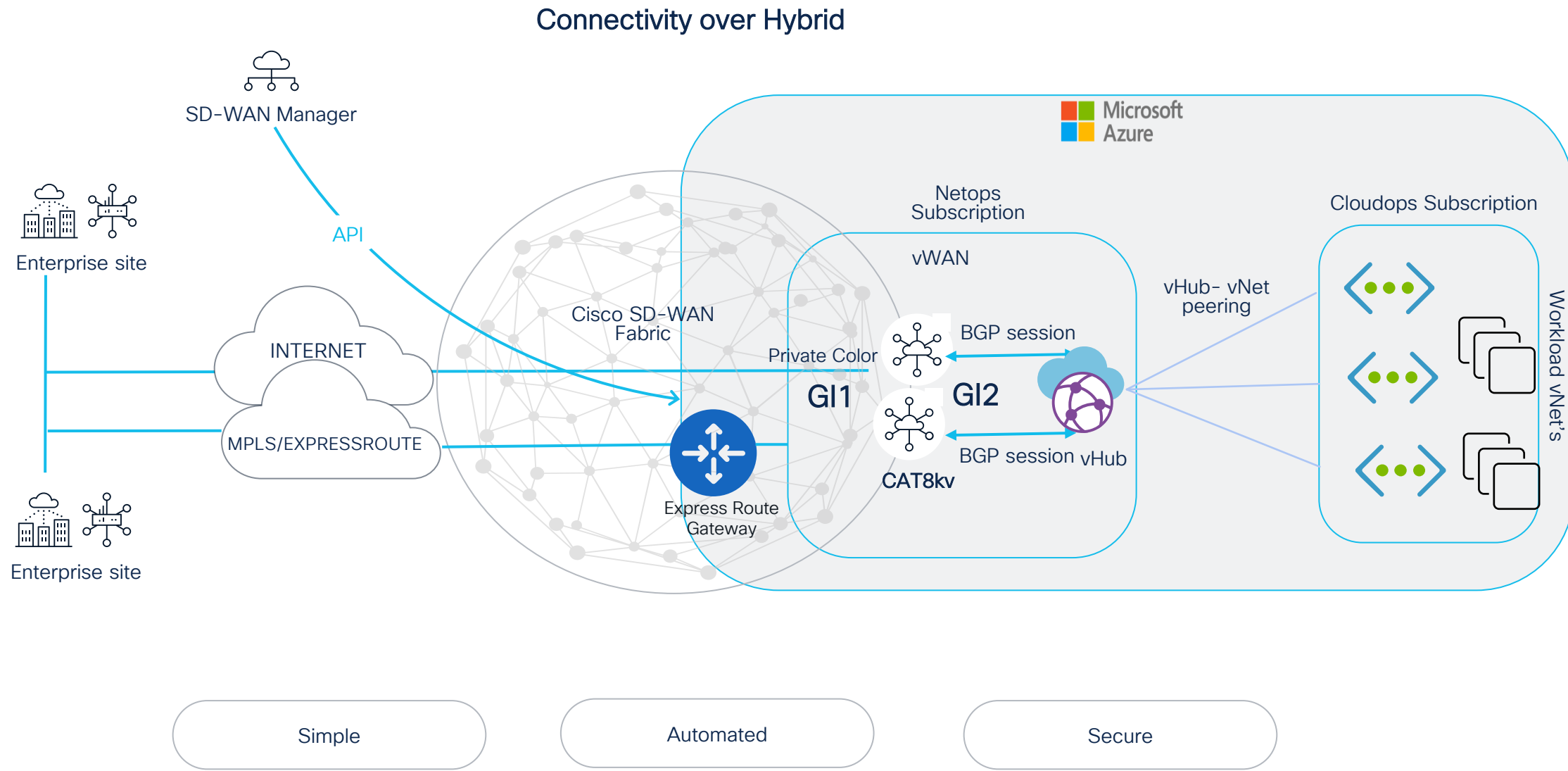
Azure - Site-to-Cloud (Meraki)

vMX Network virtual appliances are hosted in transit vNet



SD-WAN fabric to Azure Cloud

On-Prem to Azure Resilient connectivity

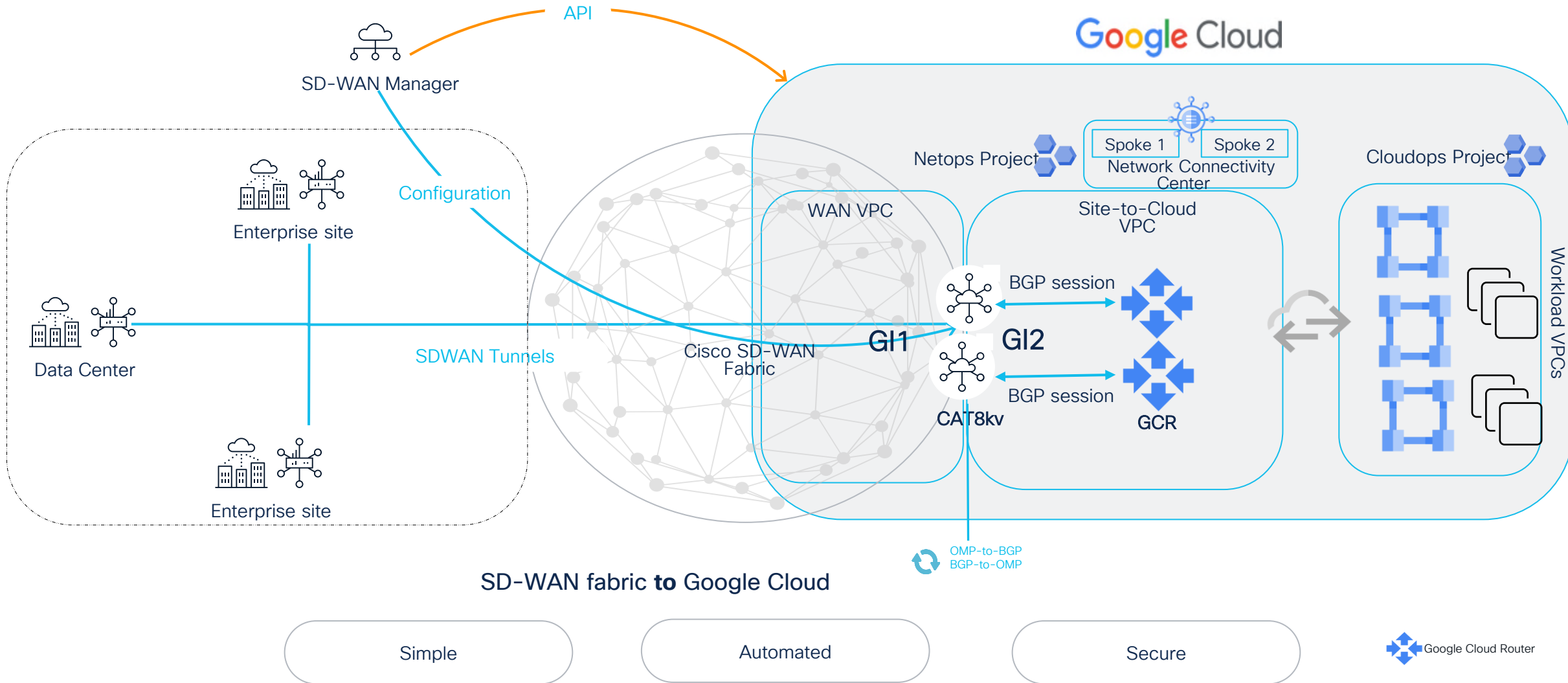


SDWAN Integration + Design with Google Cloud

Site to Multicloud

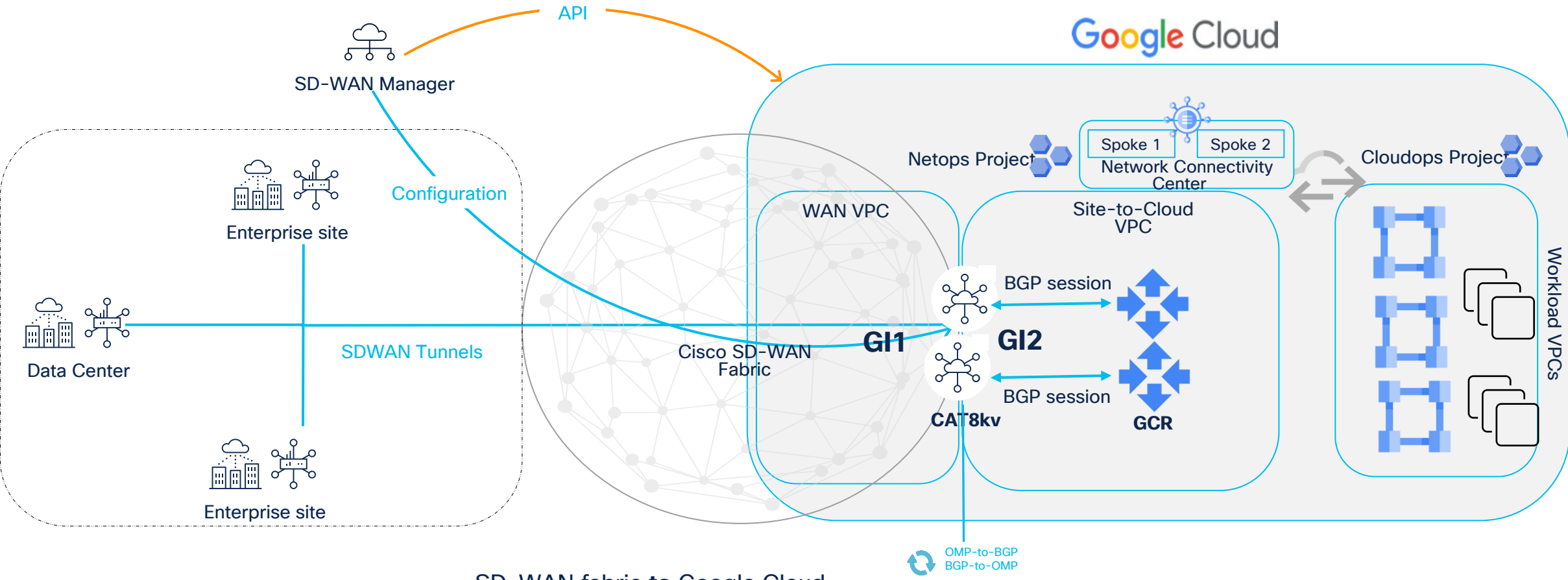
Google Cloud - Site-to-Cloud

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



Google Cloud - Site-to-Cloud

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



SD-WAN fabric to Google Cloud

Simple

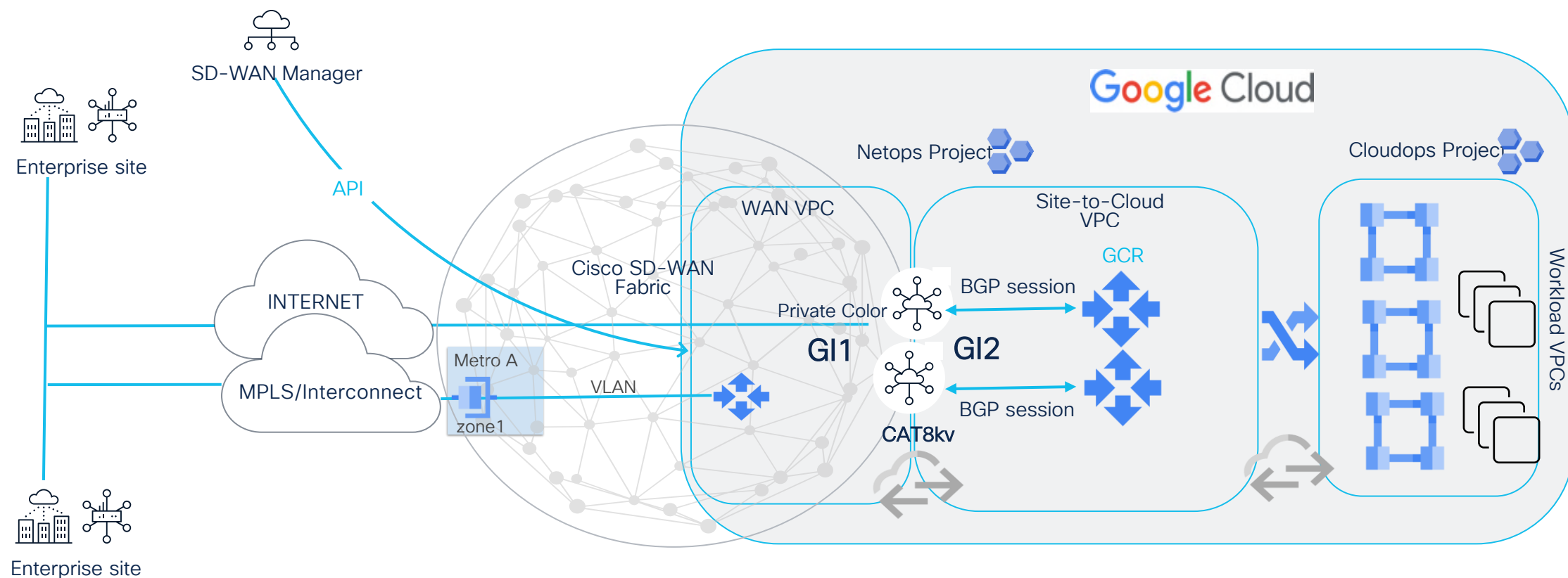
Semi Automated

Secure



On-Prem to Google Resilient connectivity-1

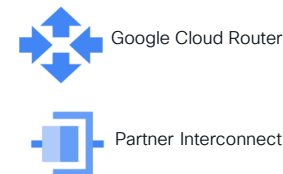
Connectivity over Hybrid



Simple

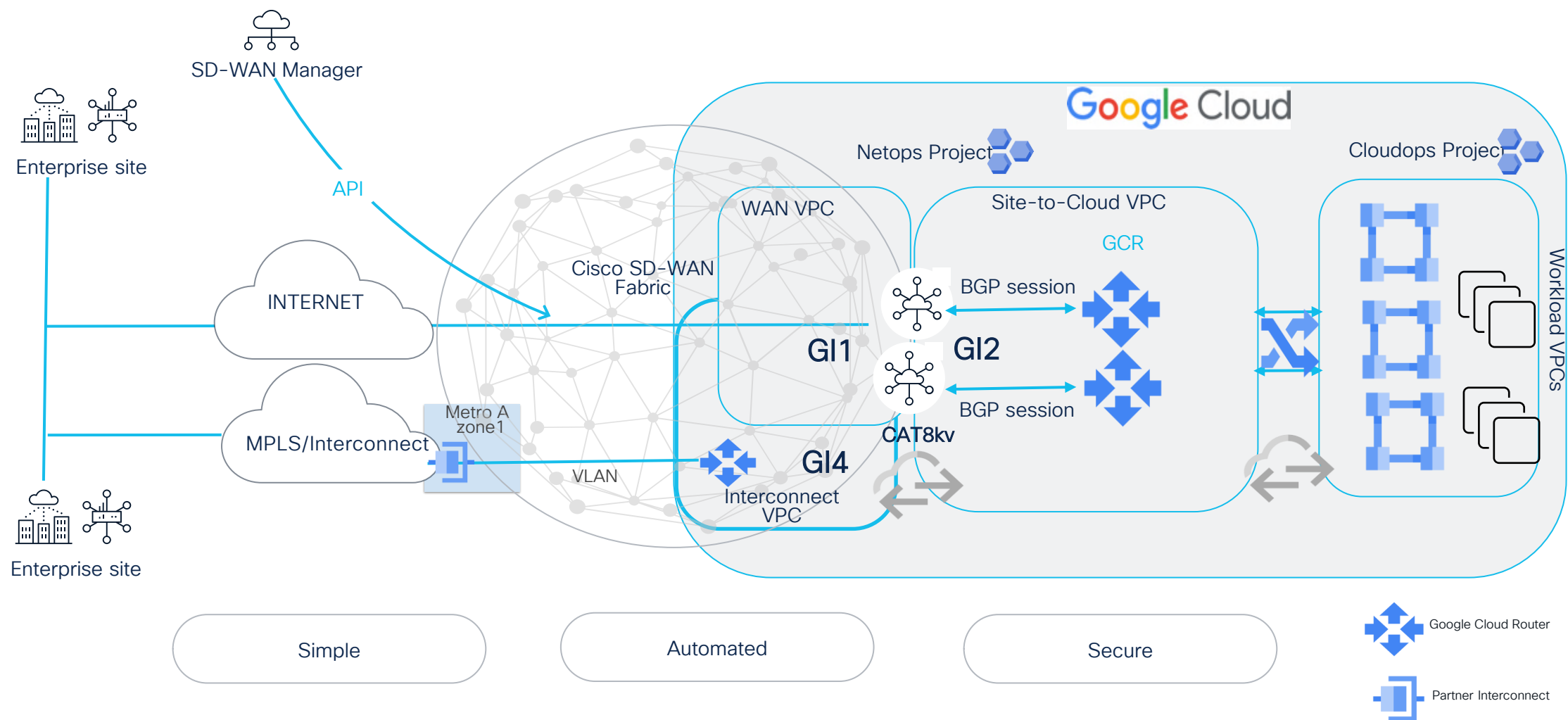
Automated

Secure



On-Prem to Google Resilient connectivity-2

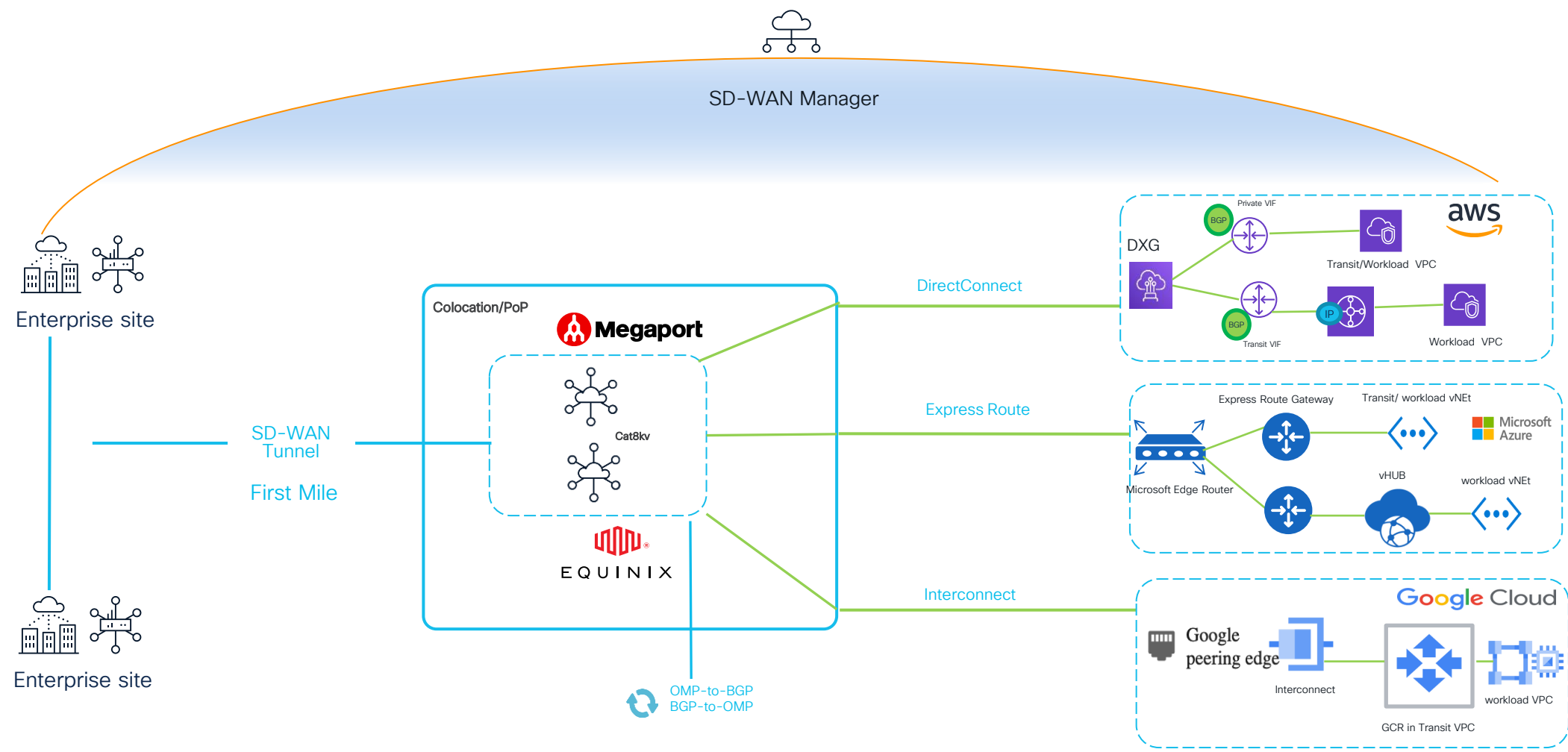
Connectivity over Hybrid



Multicloud connections via Interconnect/Carrier Neutral Facilities

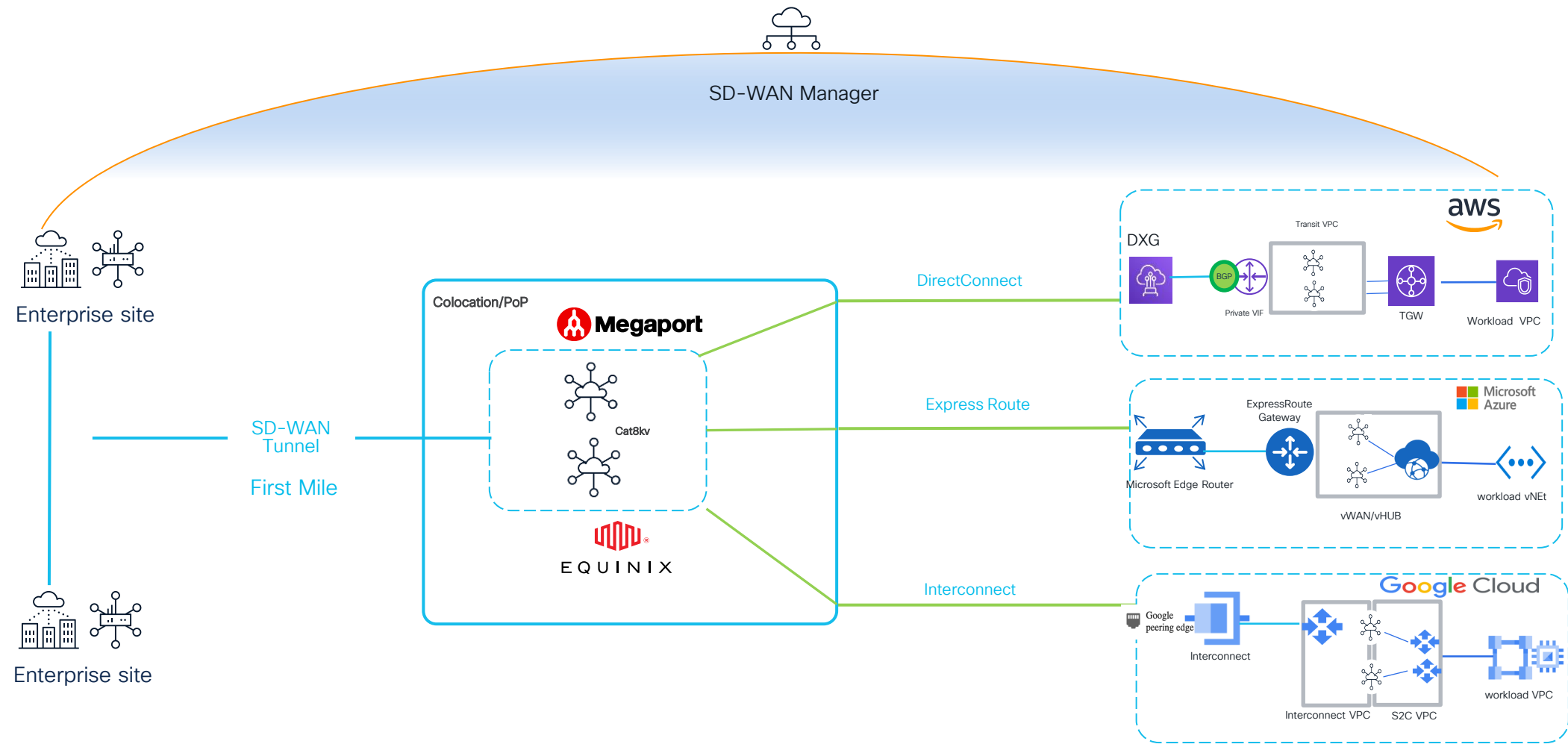
With Megaport & Equinix

Site-to-Multicloud- Megaport or Equinix



Site-to-Multicloud- Megaport or Equinix

Fully Encrypted

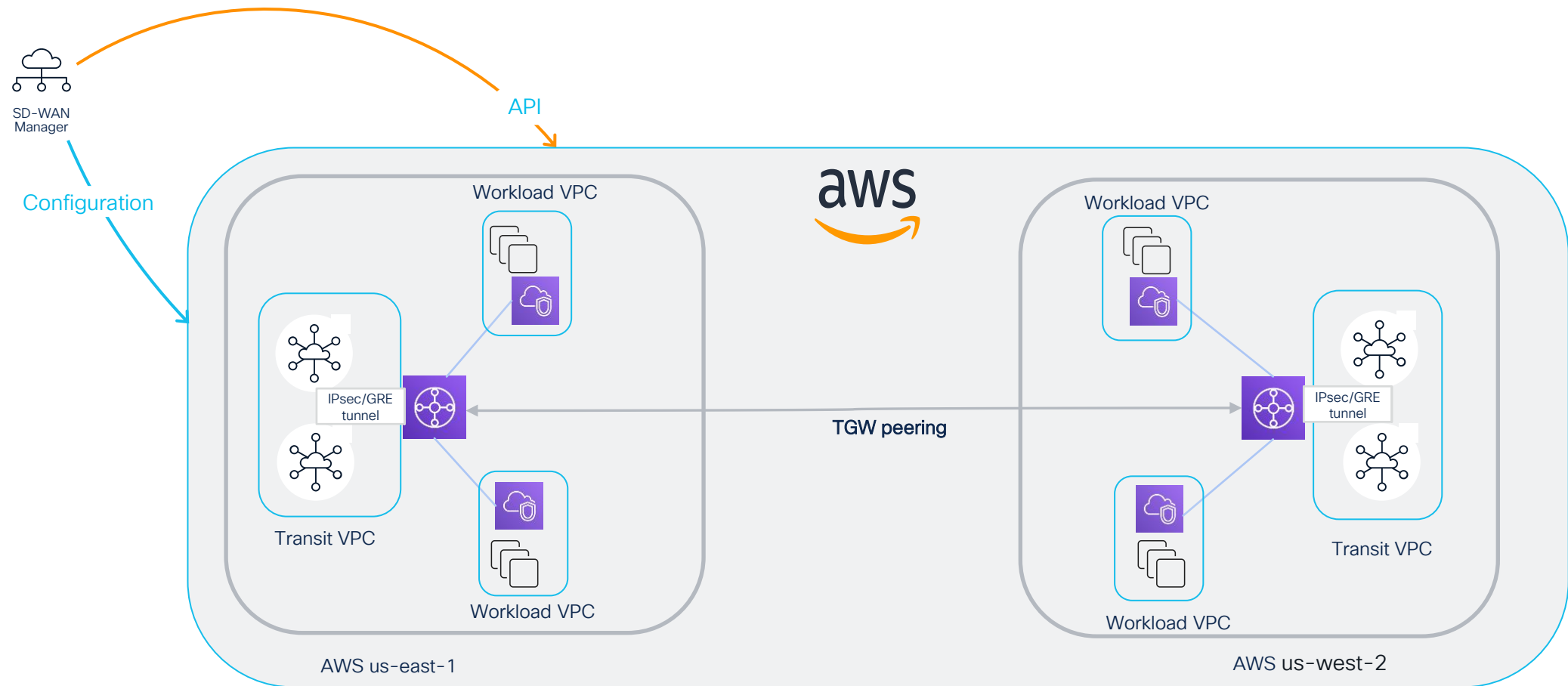




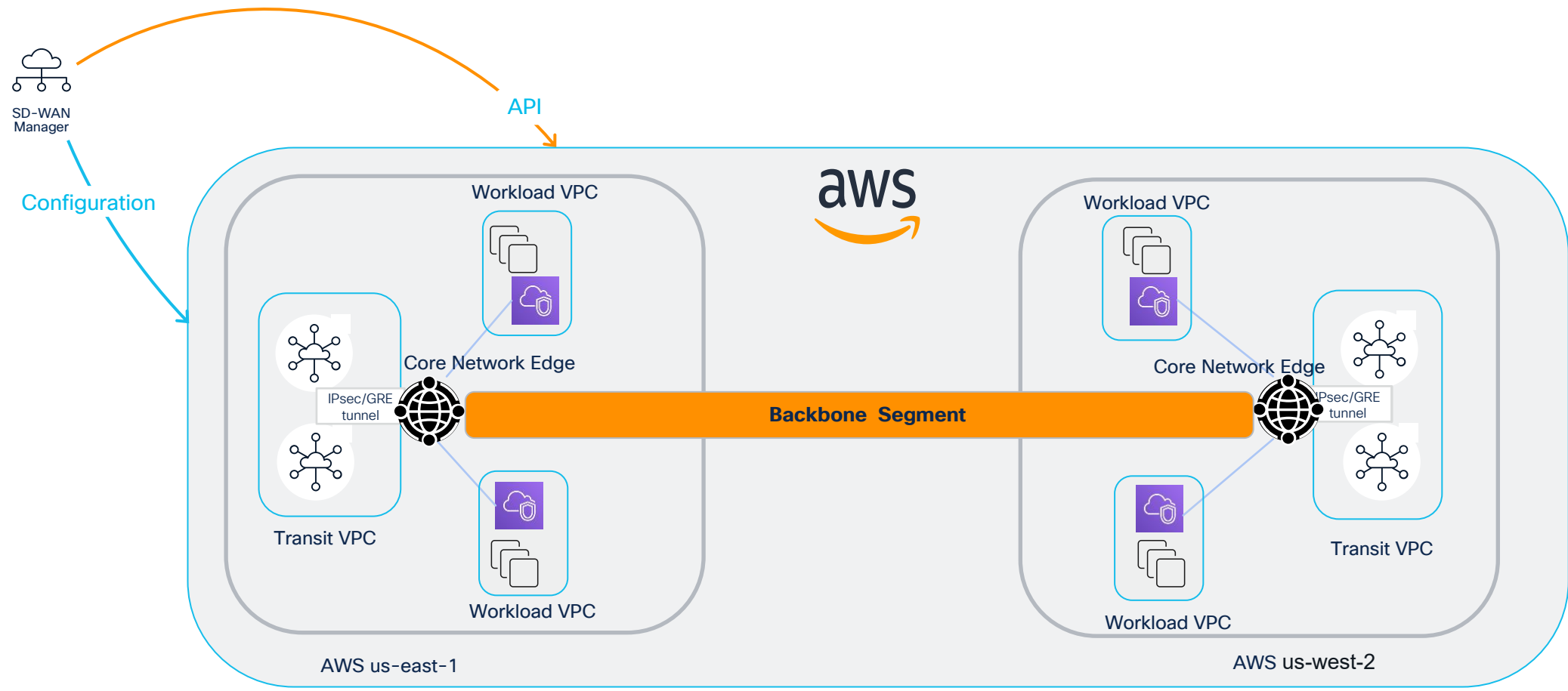
For distributed applications

Region to Region & Cloud to Cloud Connectivity

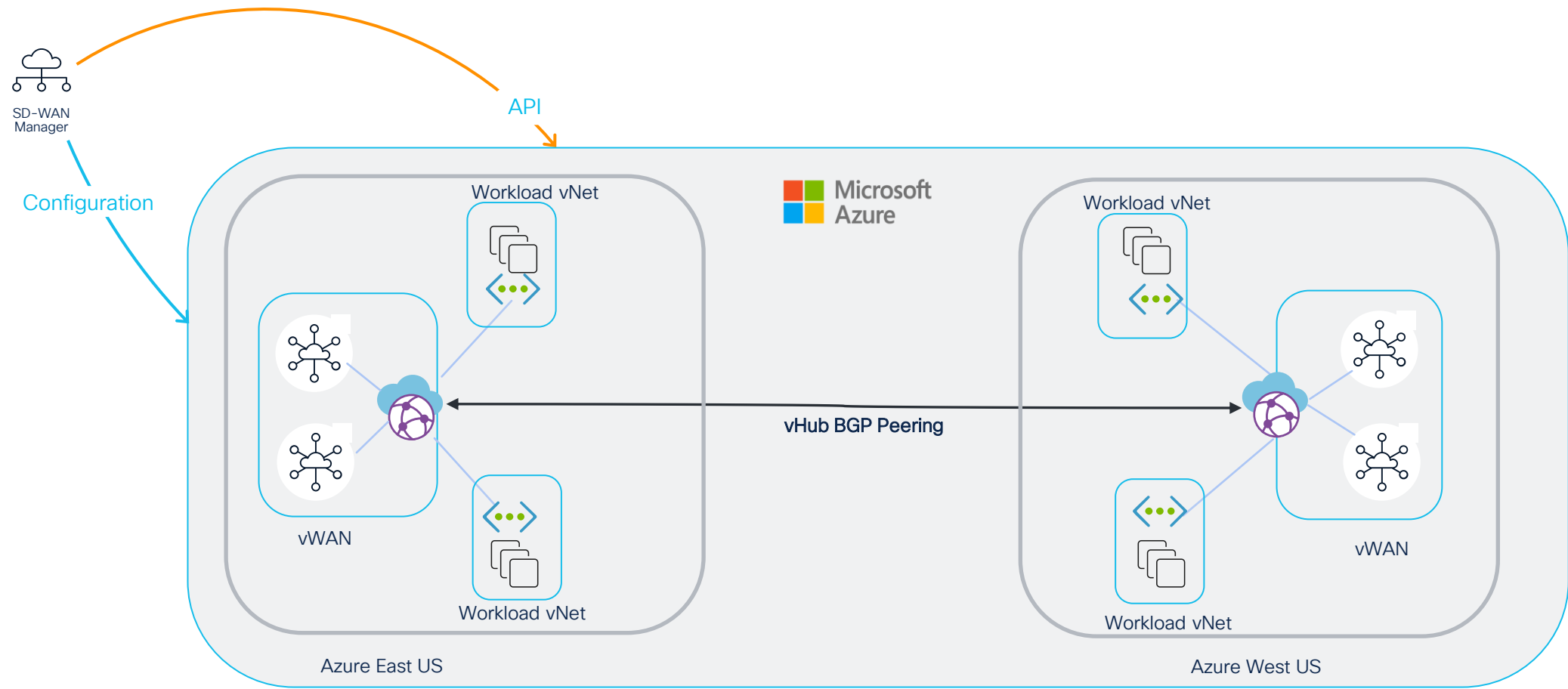
Region to Region with TGW



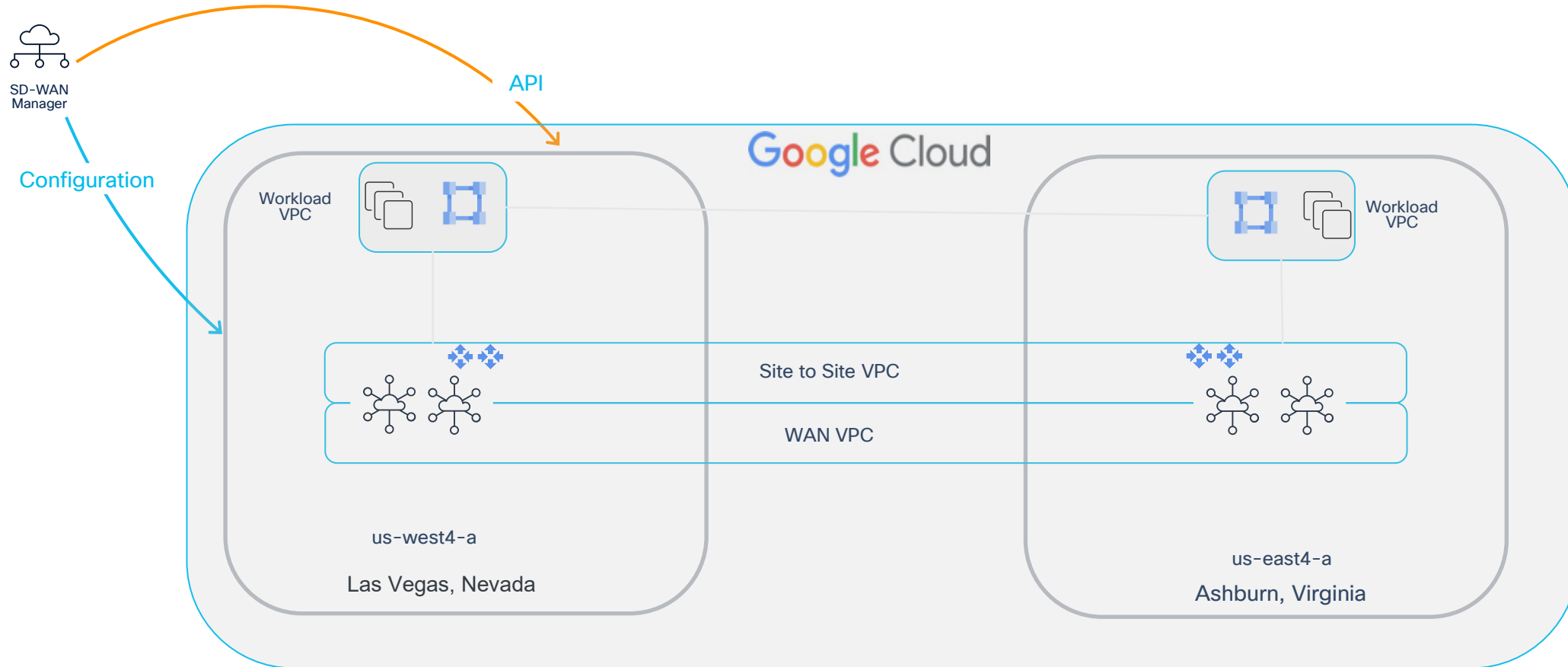
Region to Region with Cloud WAN



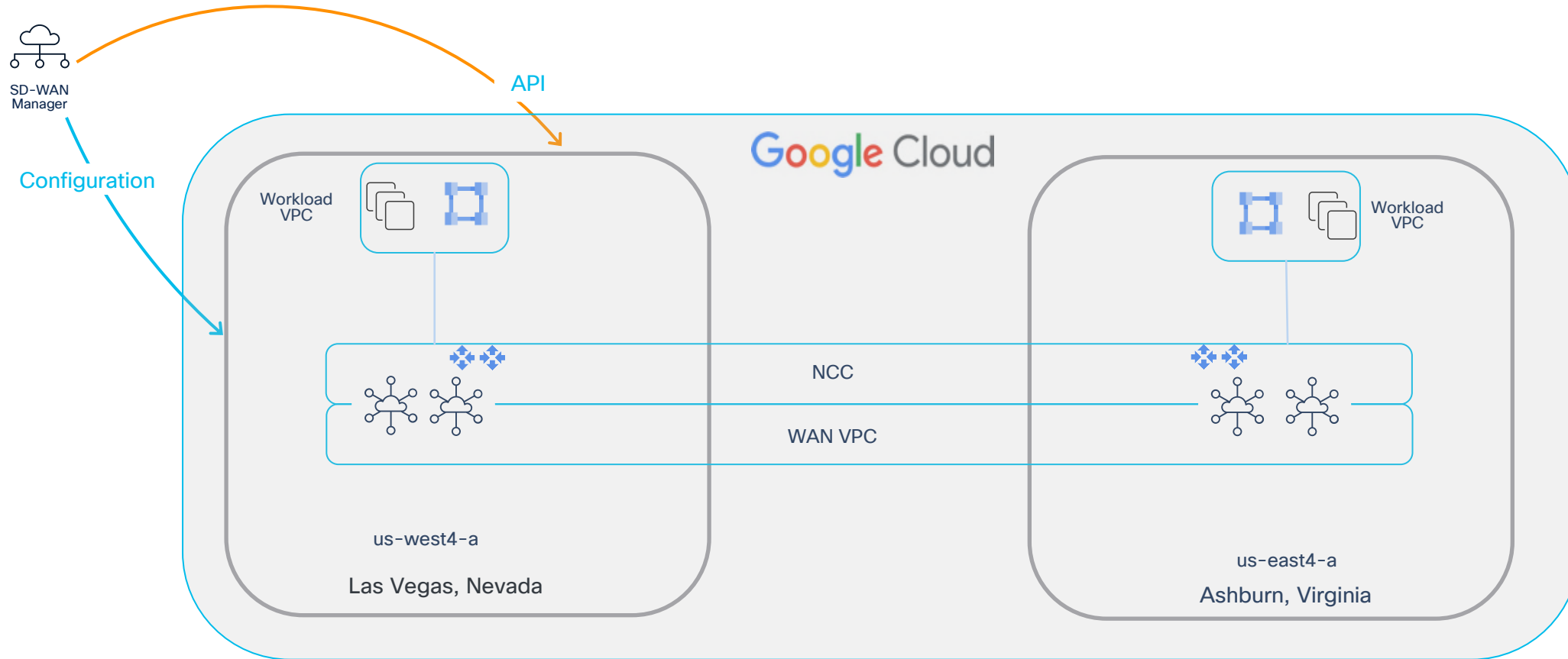
Azure – Region to Region



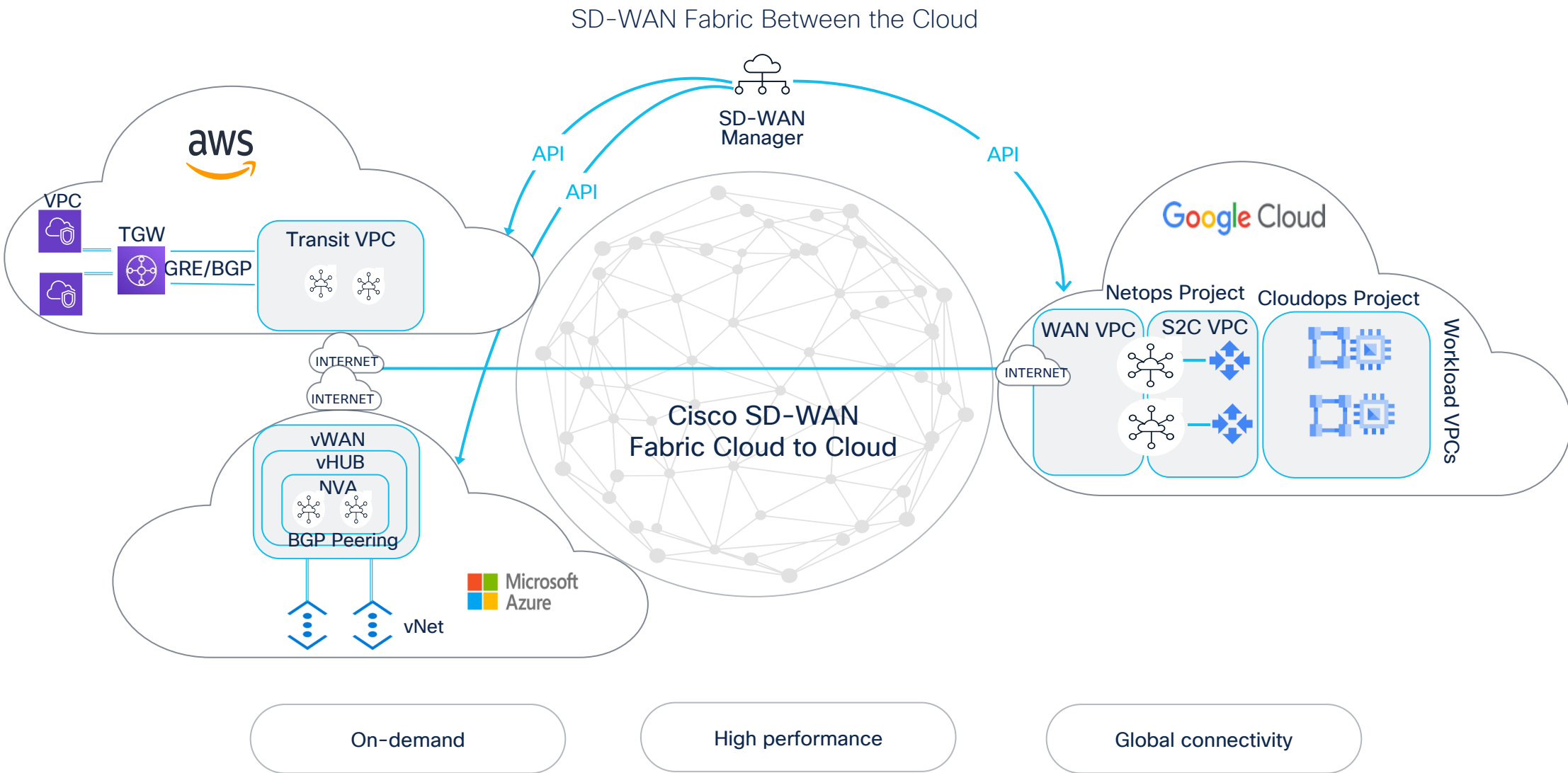
Google Cloud – Region to Region



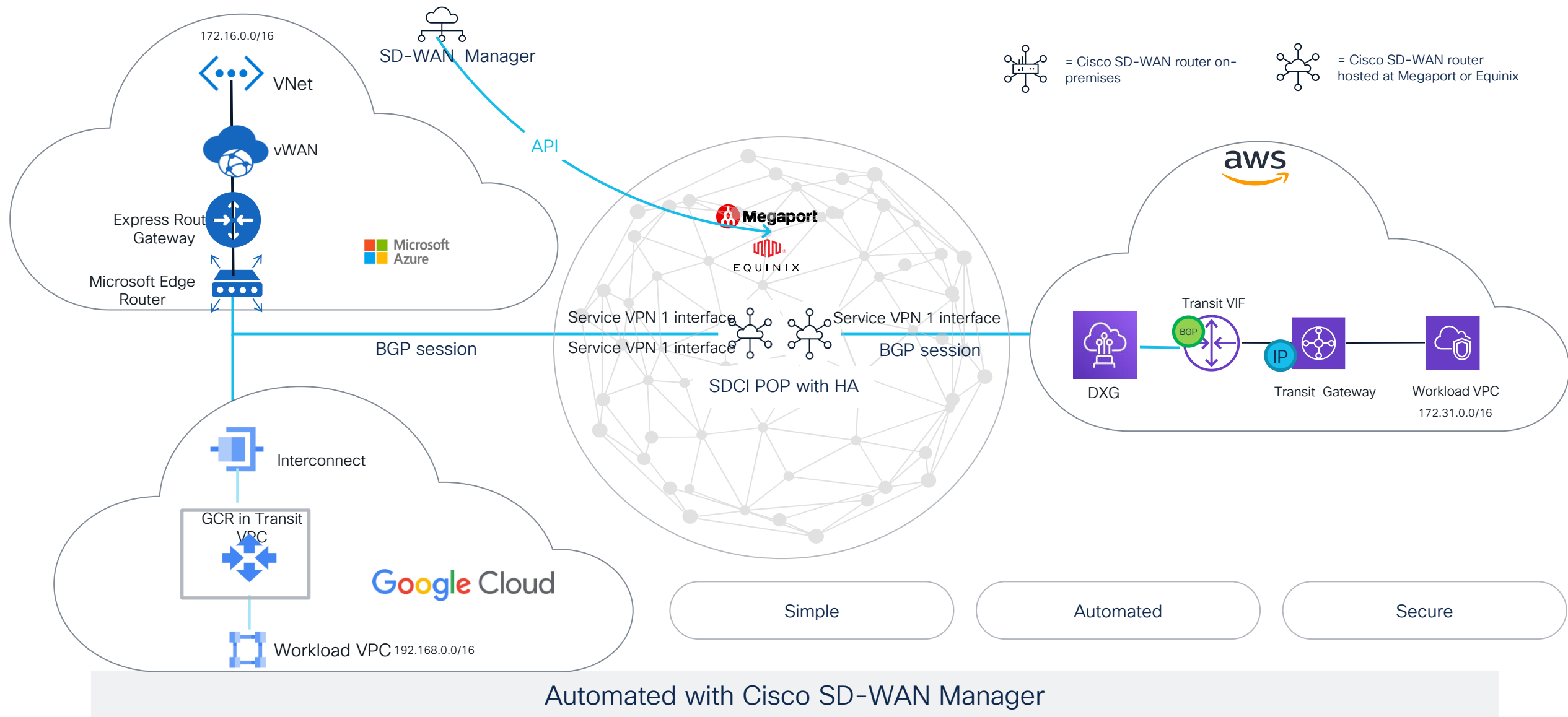
Google Cloud – Region to Region: NCC/Cloud WAN



Cloud to Cloud – Over Internet



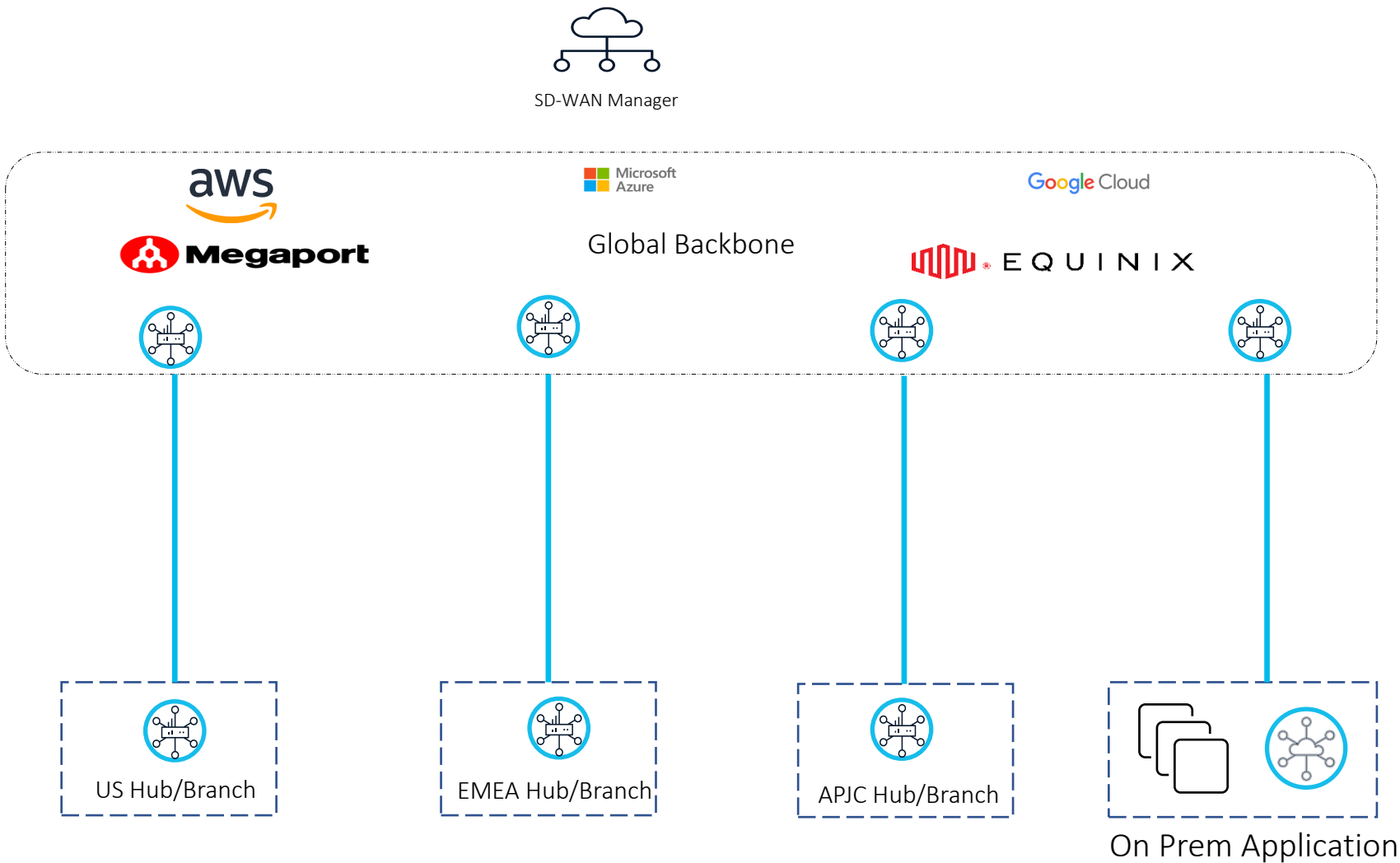
Cloud to Cloud – With Megaport/Equinix



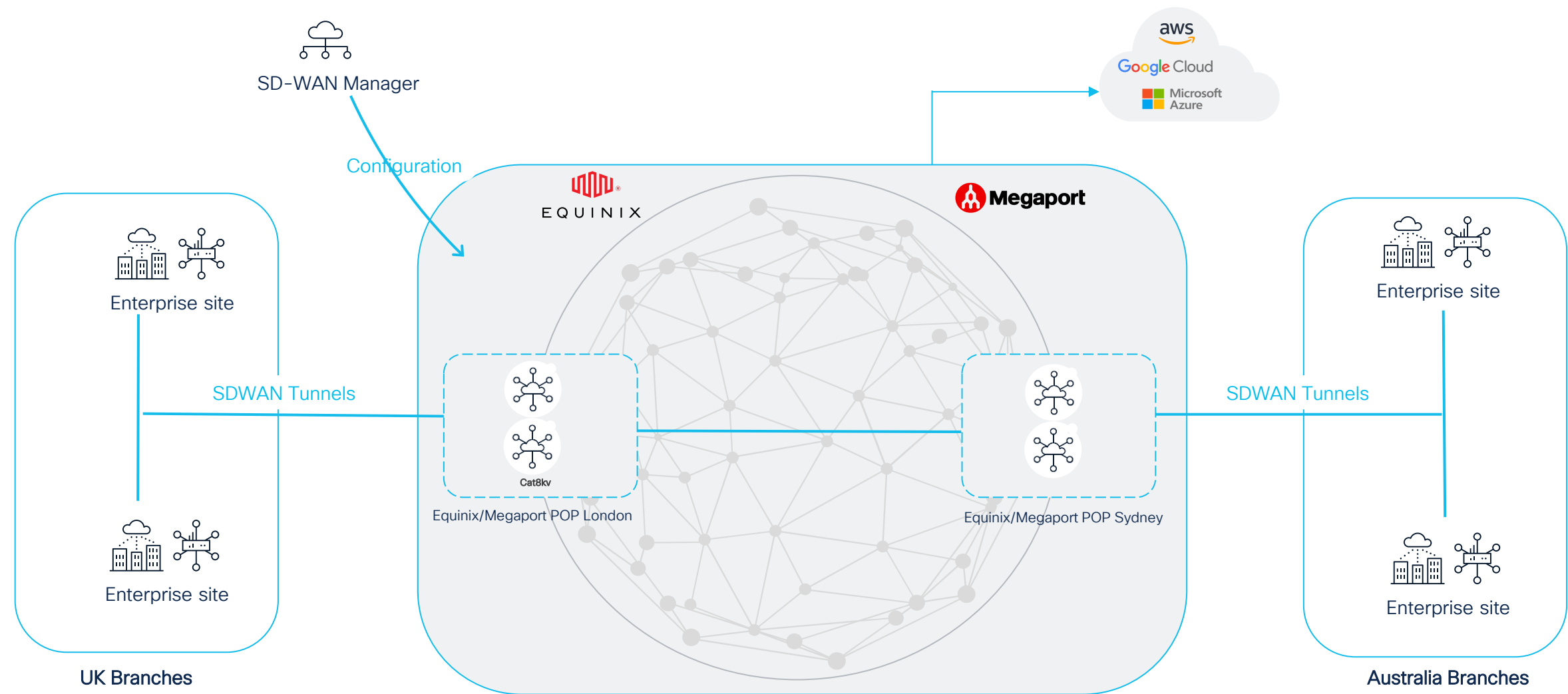
Site to Site

For International sites / Building a
Global backbone

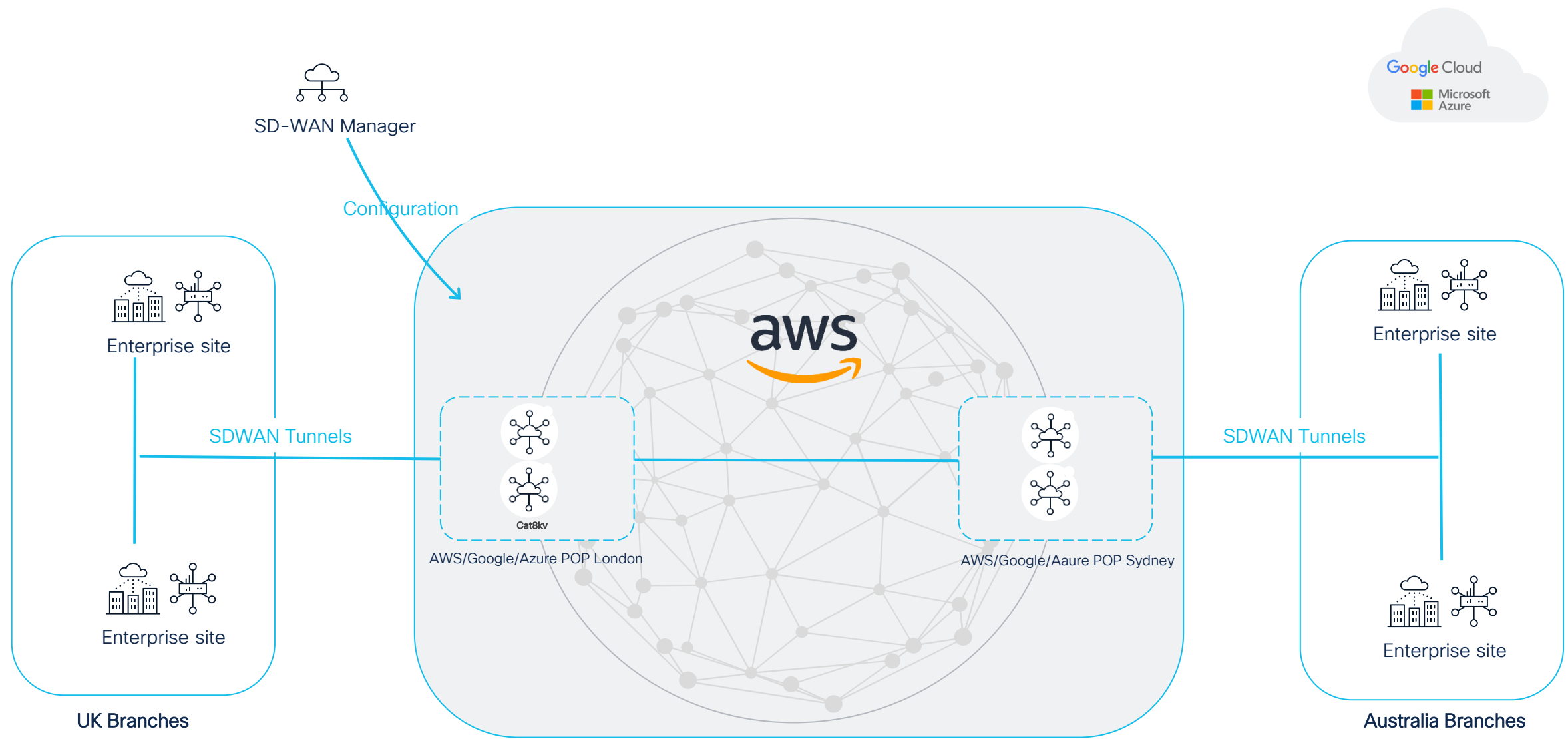
Flexible backbone and connectivity to Cloud



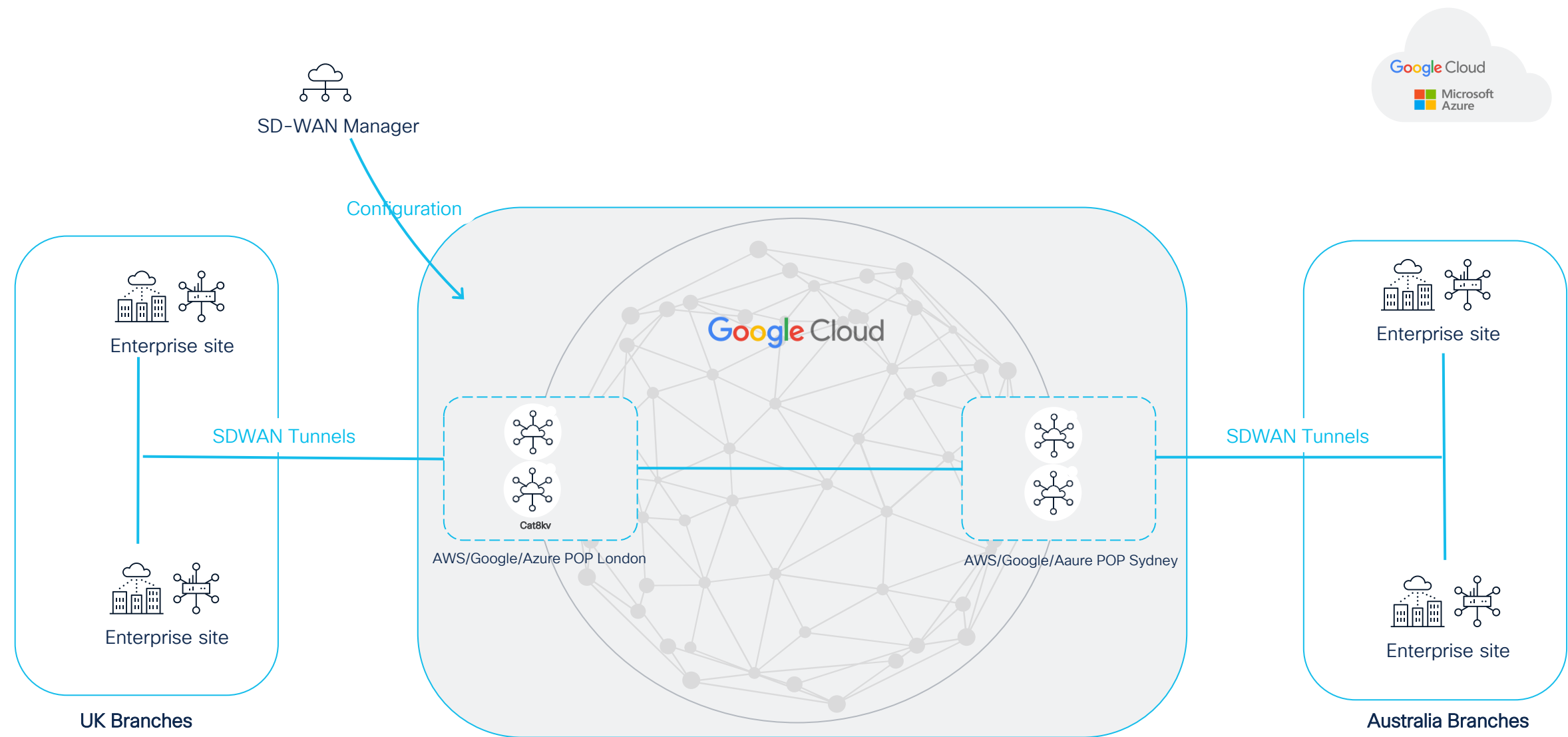
Site-to-Site - Cloud Agnostic



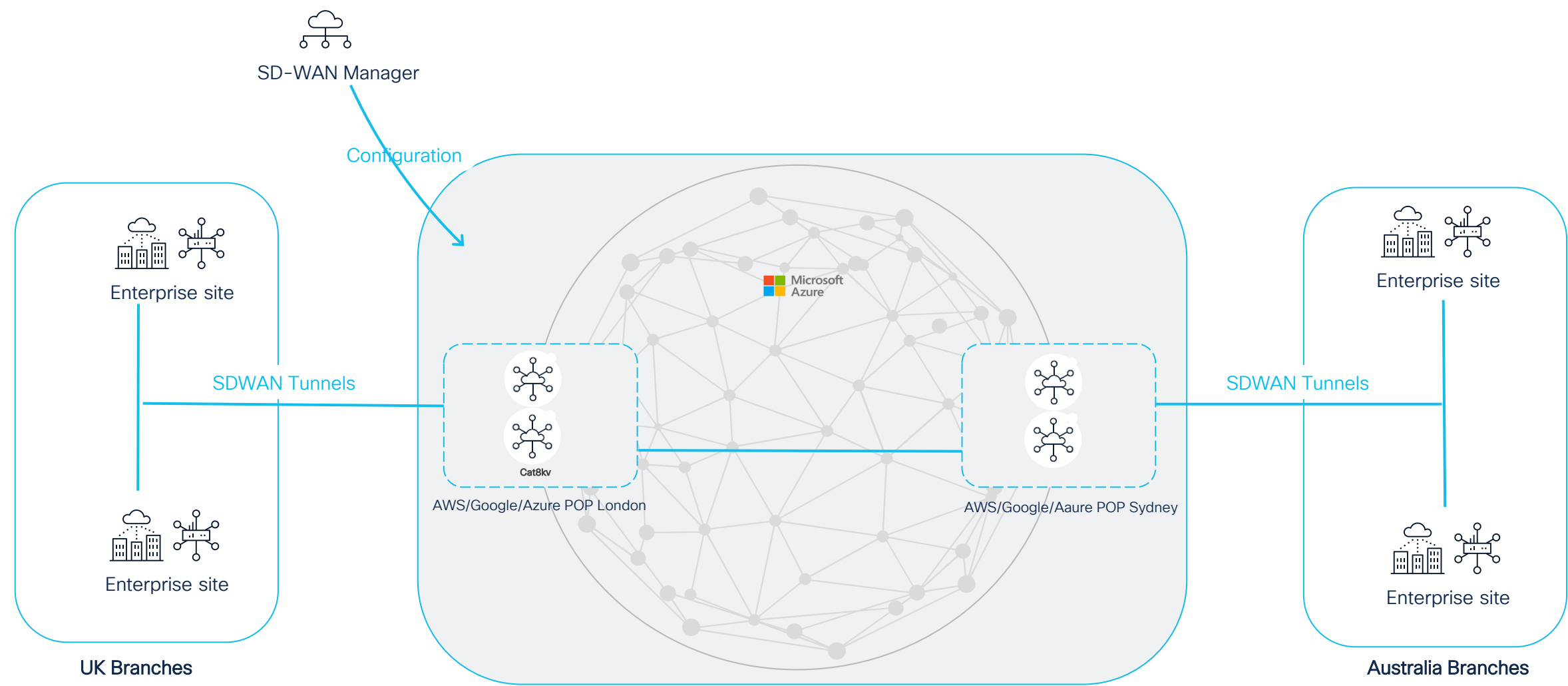
Site-to-Site - CSP Backbone - AWS



Site-to-Site - CSP Backbone- Google Cloud

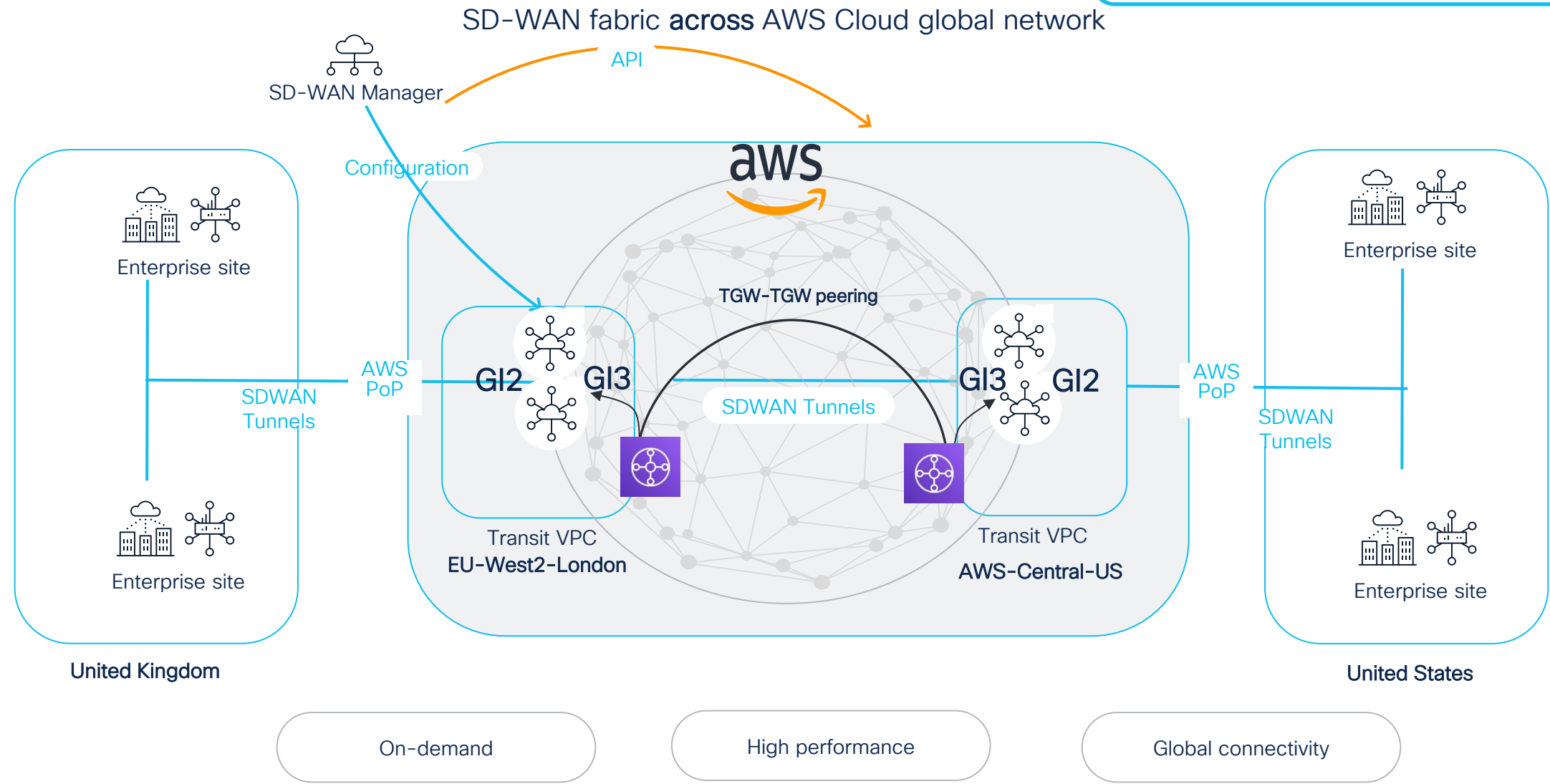


Site-to-Site - CSP Backbone- Azure



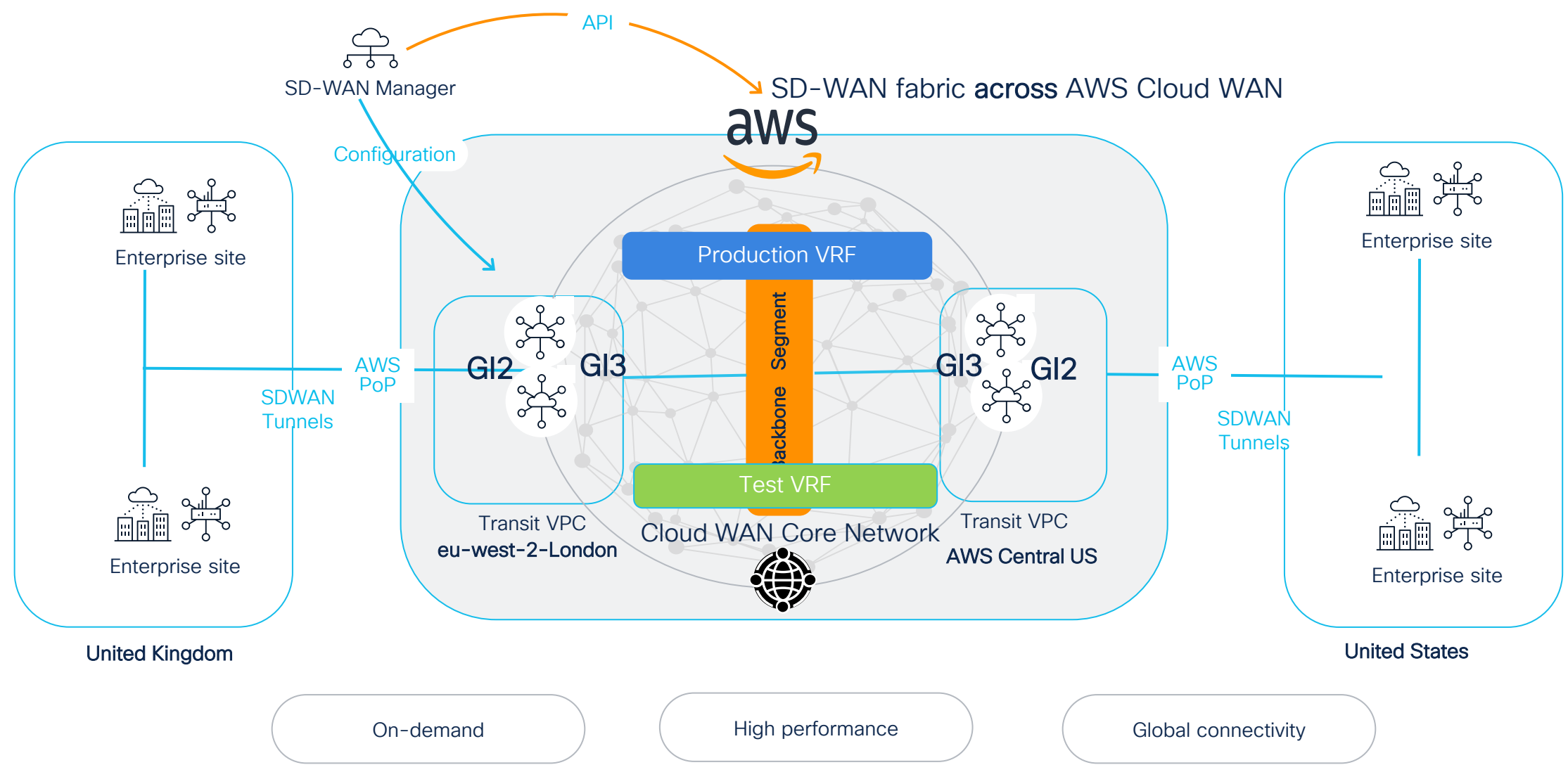
Site-to-Site with TGW

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



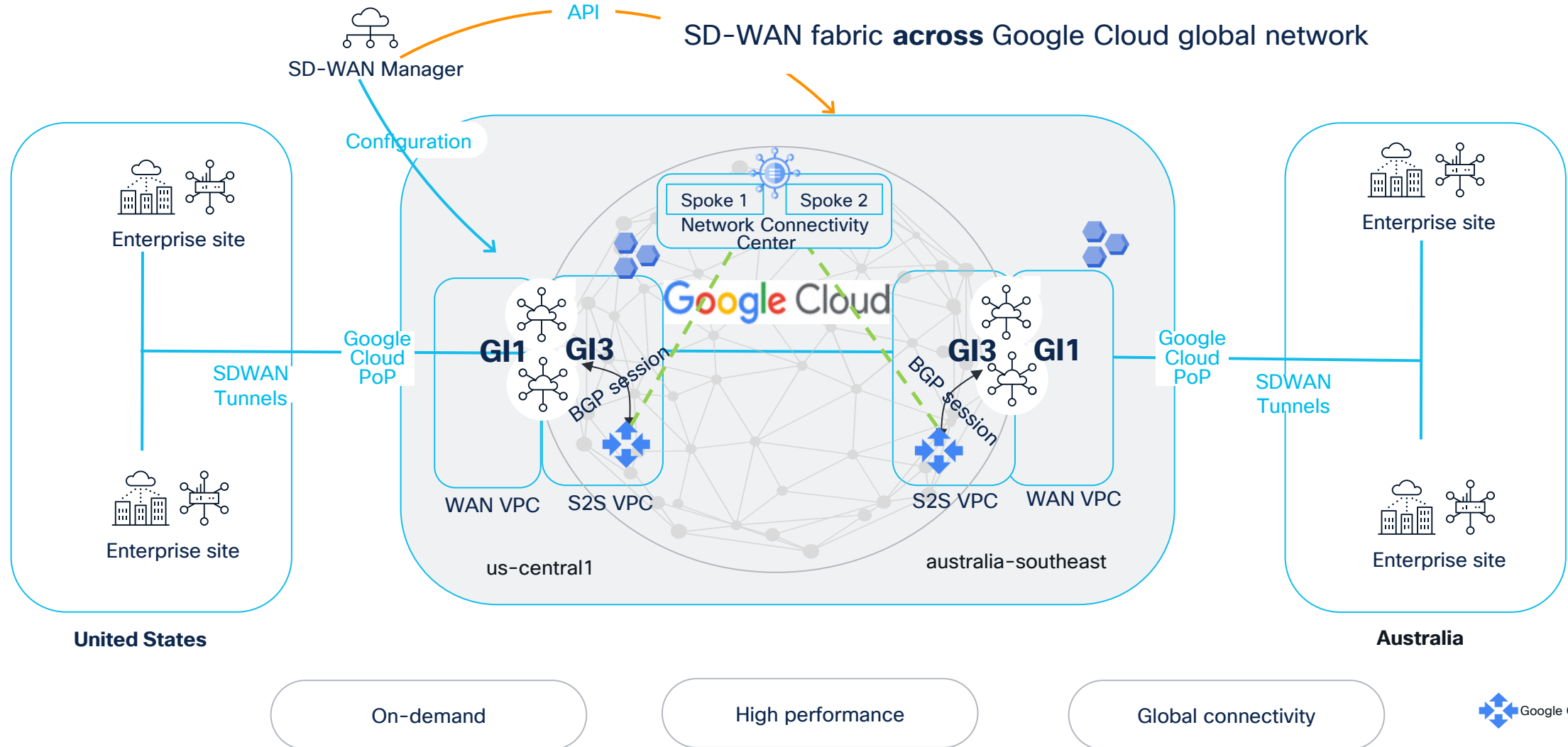
Site-to-Site with Cloud WAN

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



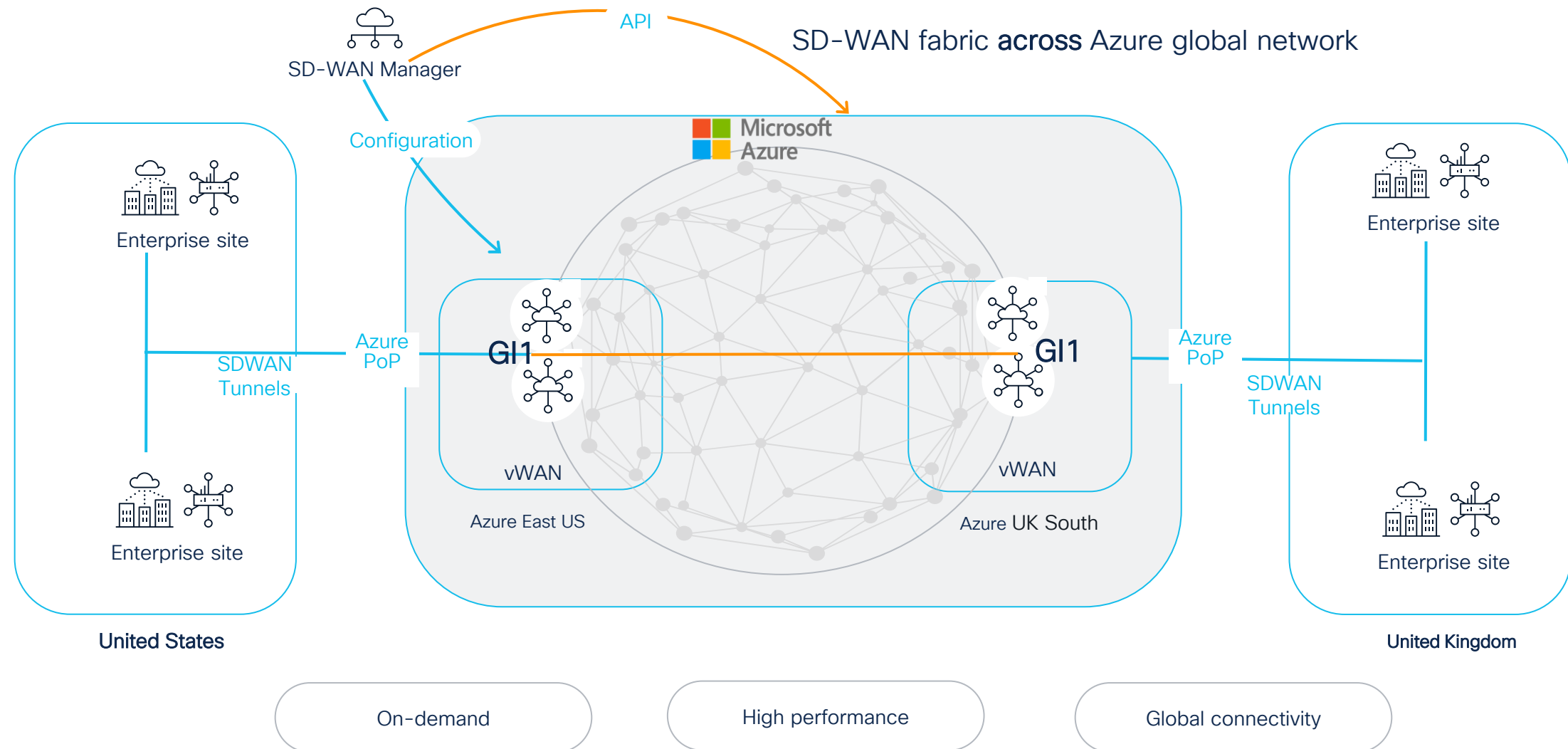
Google Cloud - Site-to-Site

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



Azure - Site-to-Site

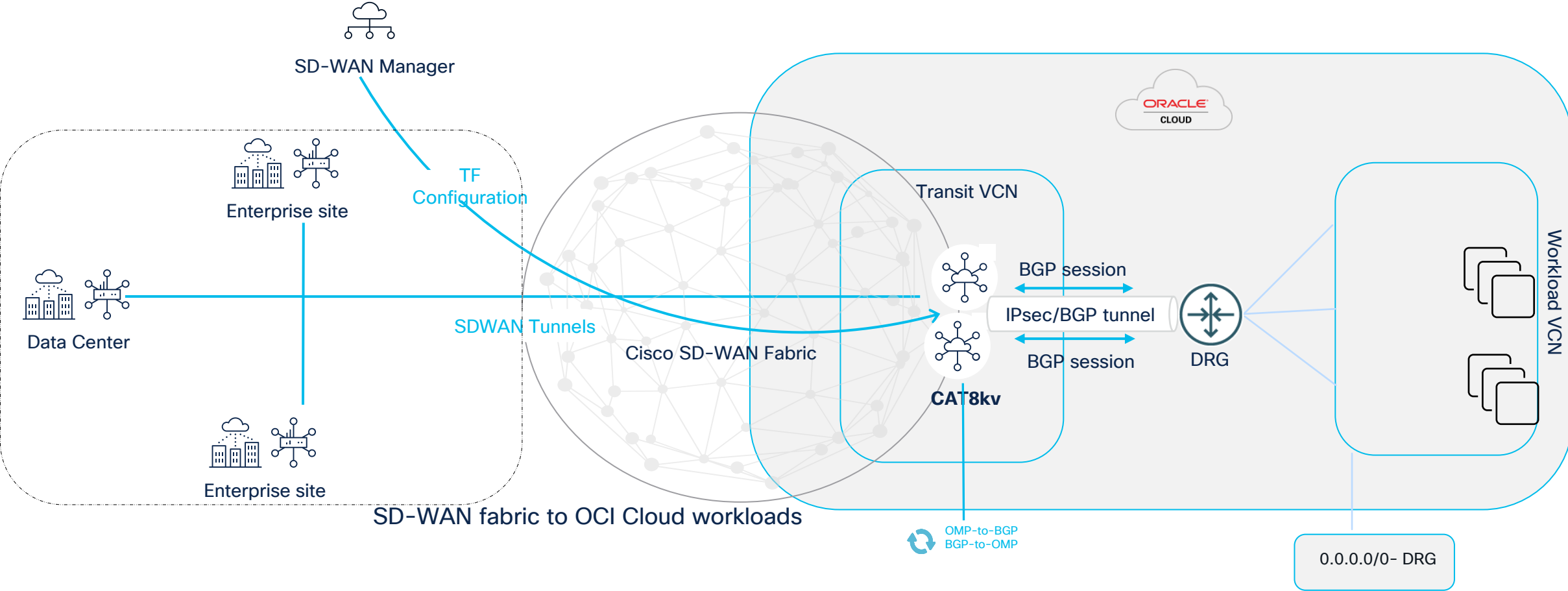
SDWAN tunnels with Azure Public IPs on NVAs go through Azure Backbone. Control policy or Multi region Fabric required for traffic redirection



OCI support

OCI- Site-to-Cloud

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



Simple

Automated

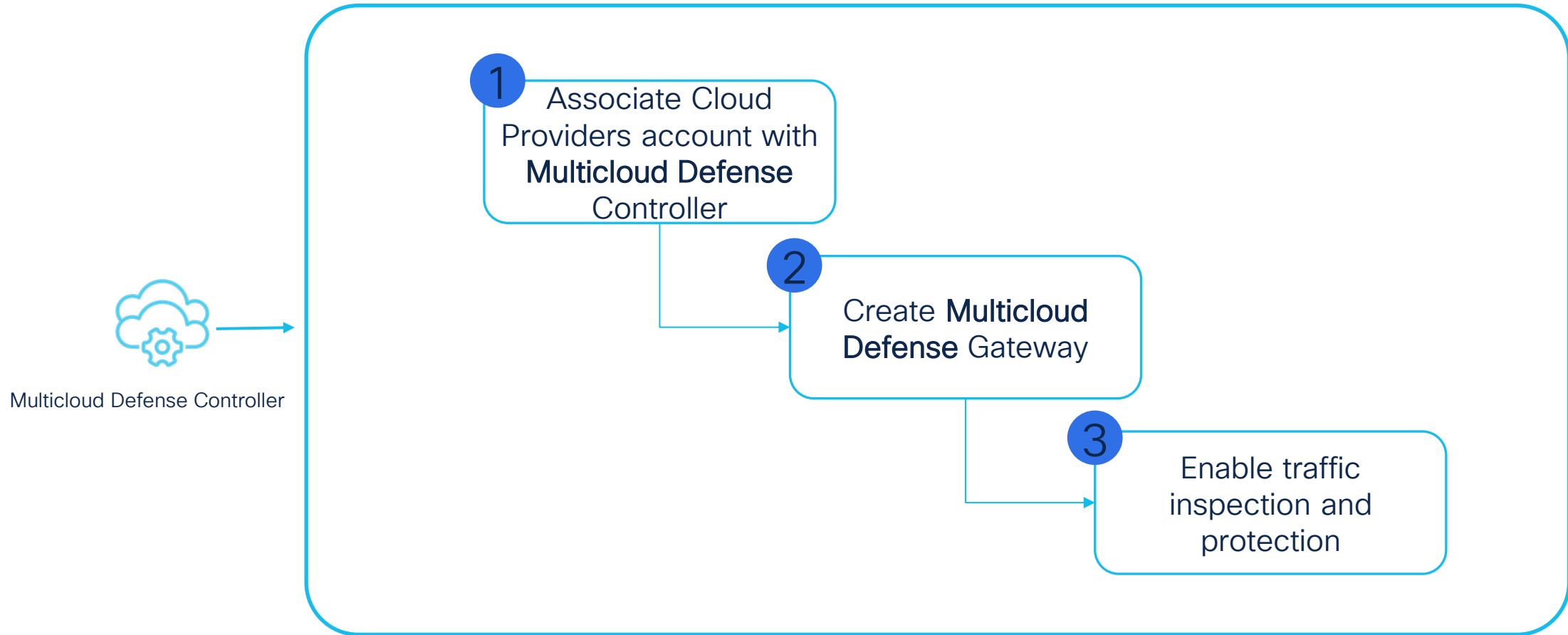
Secure

Security and Compliance with Cloud Networking

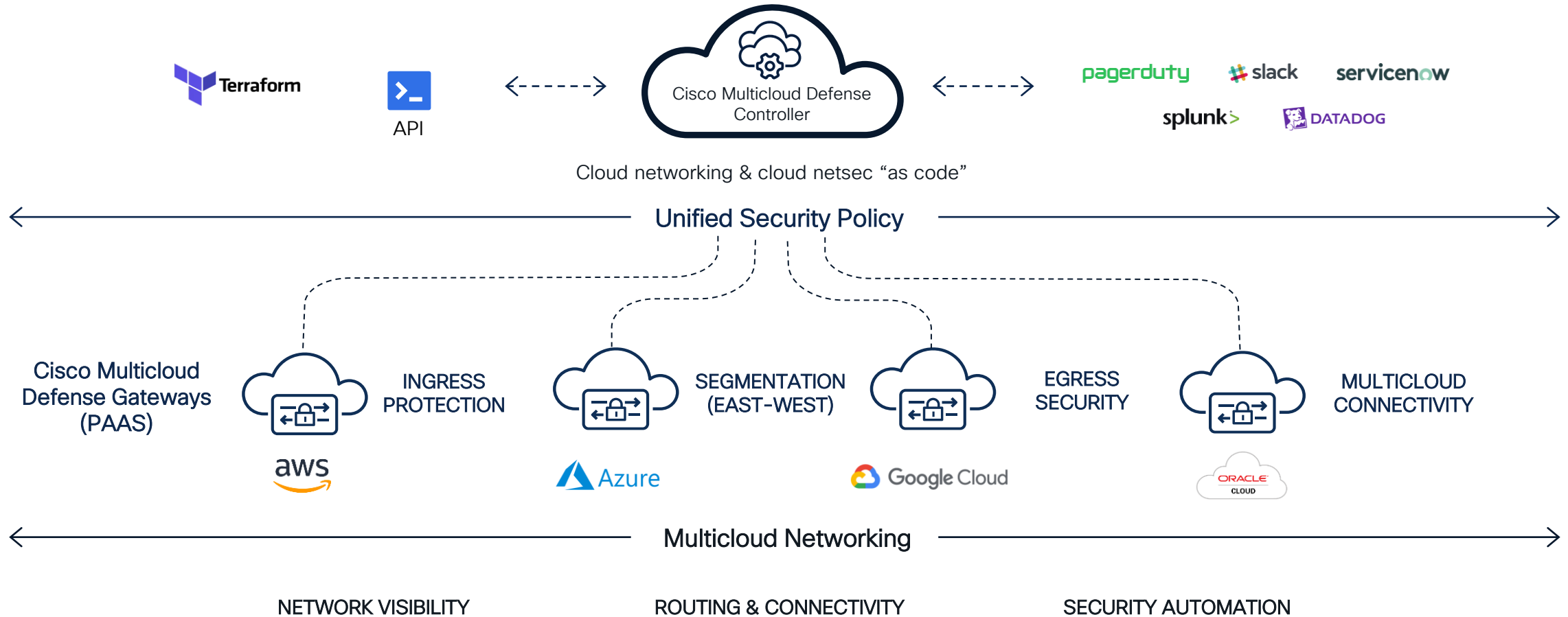
With Cisco Multicloud Defense

Multicloud Defense Workflow

Secure Connectivity achieved in minutes....



Cisco Multicloud Defense



Multicloud Defense Gateways



Ingress Gateway

Ingress

- ✓ Reverse Proxy
- ✓ TLS decrypt
- ✓ WAF – L7 DoS
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Geo IP
- ✓ Malicious IP



Egress Gateway

Egress

- ✓ URL filtering
- ✓ Forward proxy
- ✓ TLS decrypt
- ✓ FQDN filtering
- ✓ FQDN-based firewall policy
- ✓ DLP
- ✓ IDS / IPS
- ✓ Antivirus

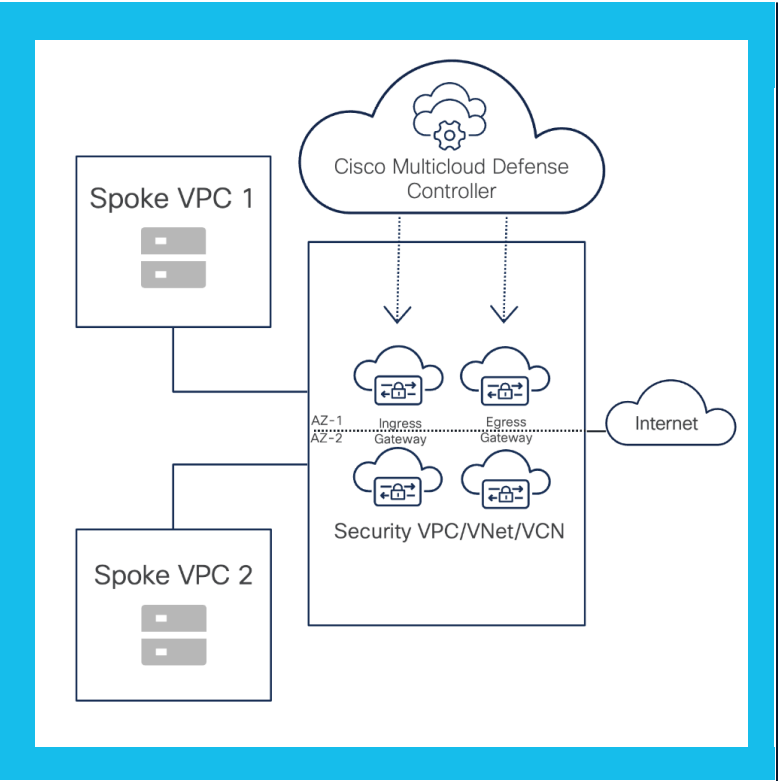
East/West

- ✓ FQDN filtering
- ✓ IPS / IDS
- ✓ Antivirus
- ✓ Segmentation
- ✓ FQDN-based firewall policy
- ✓ TLS decrypt

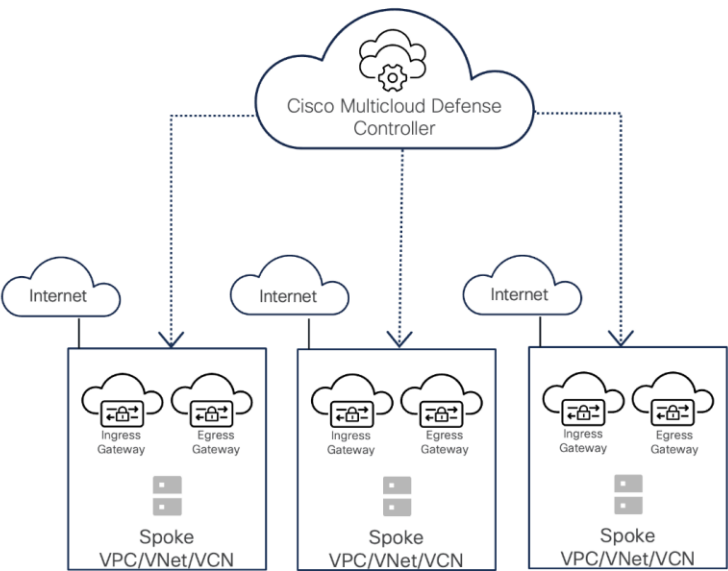
Flexible Single Pass Architecture, Available in AWS, Azure, GCP and OCI

Security Models

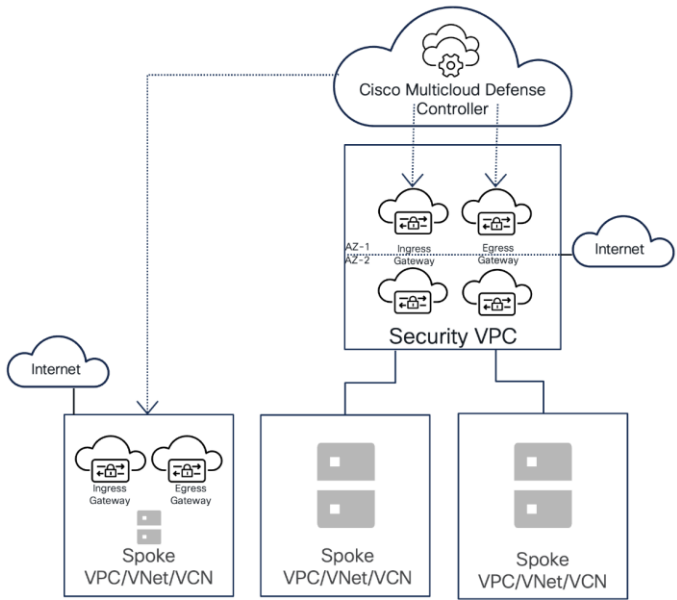
Centralized Security Model



Distributed Security Model



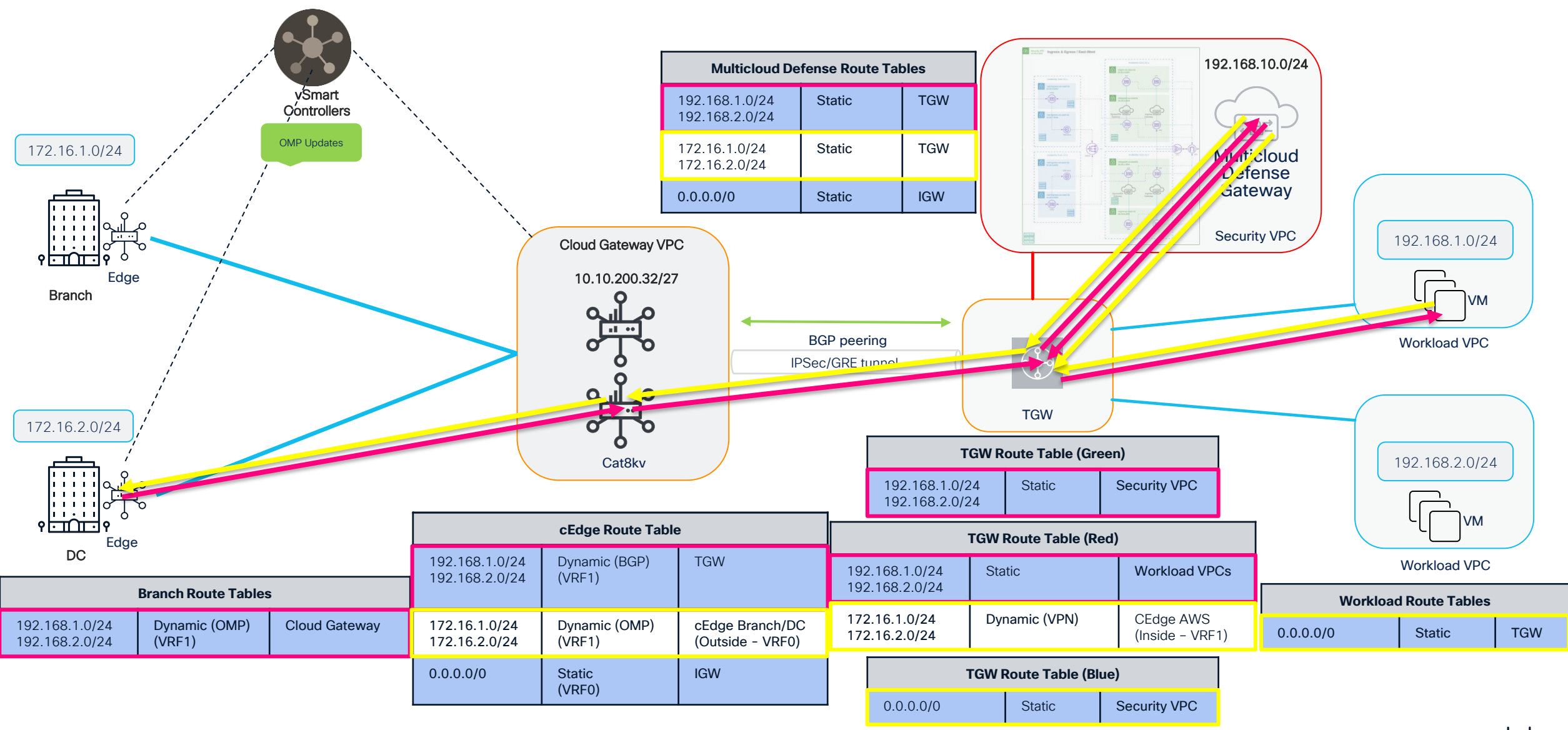
Combined Security Model



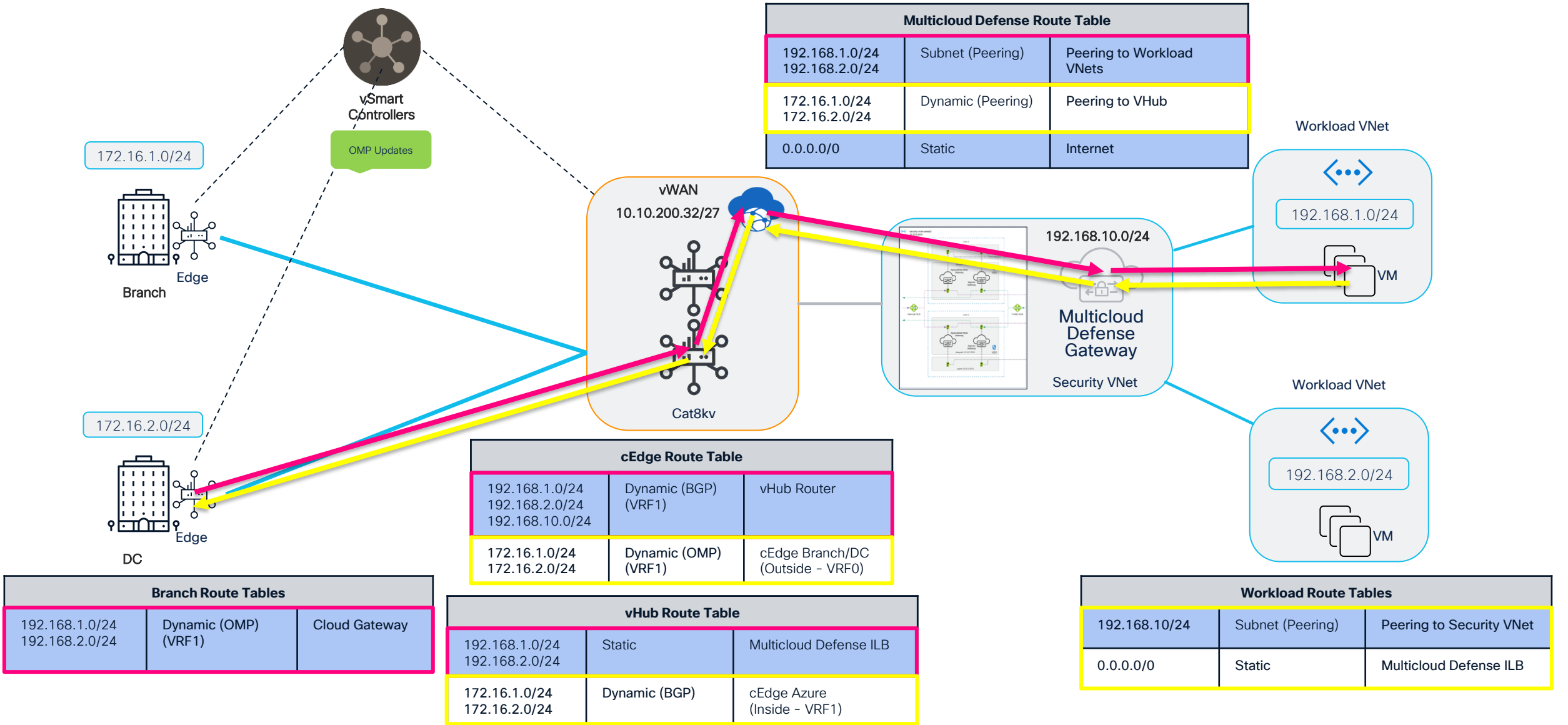
Multicloud Defense + SDWAN

Secure connections

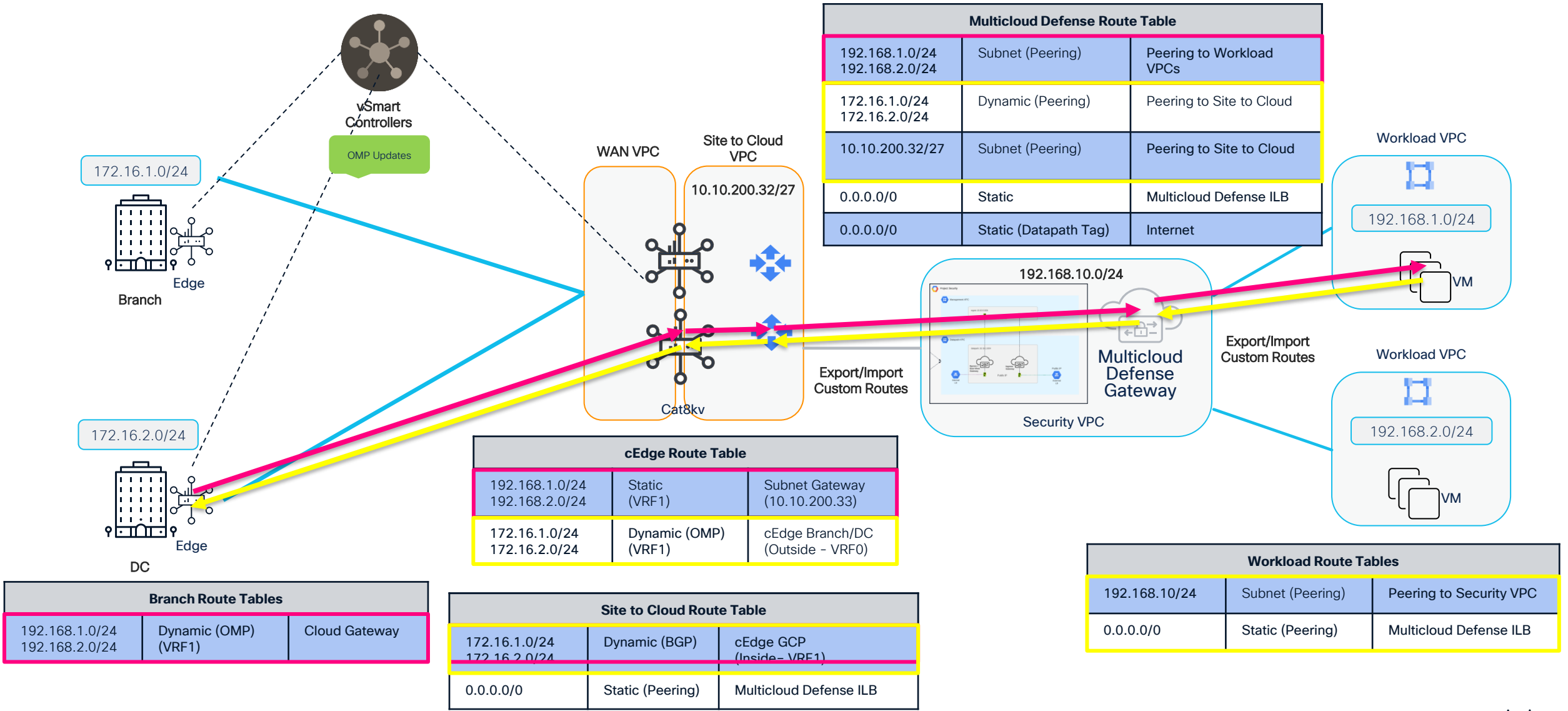
Branch to AWS Workload VPC Connectivity



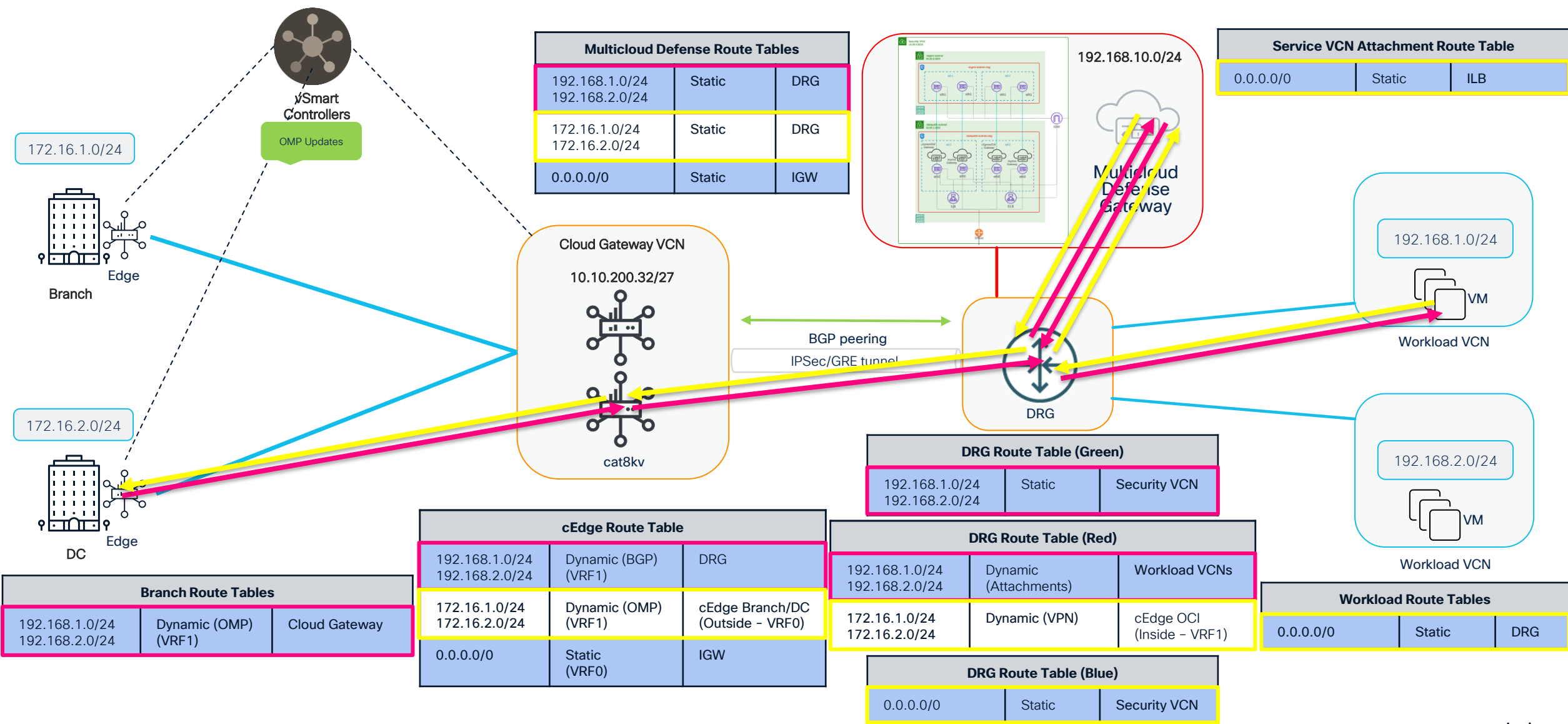
Branch to Azure Workload VNet Connectivity



Branch to GCP Workload VPC Connectivity

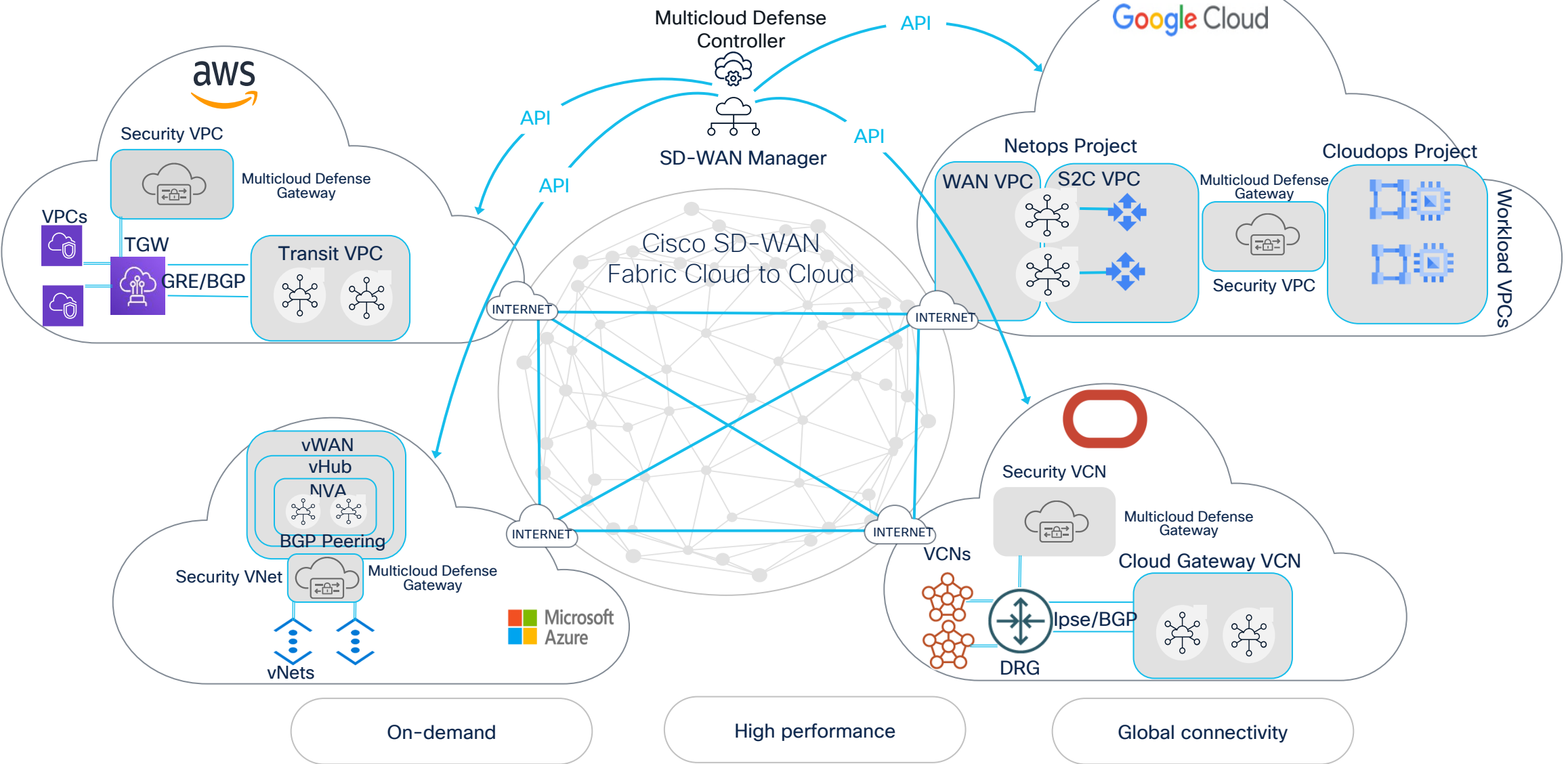


Branch to OCI Workload VCN Connectivity



Security Stack Insertion in the Cloud

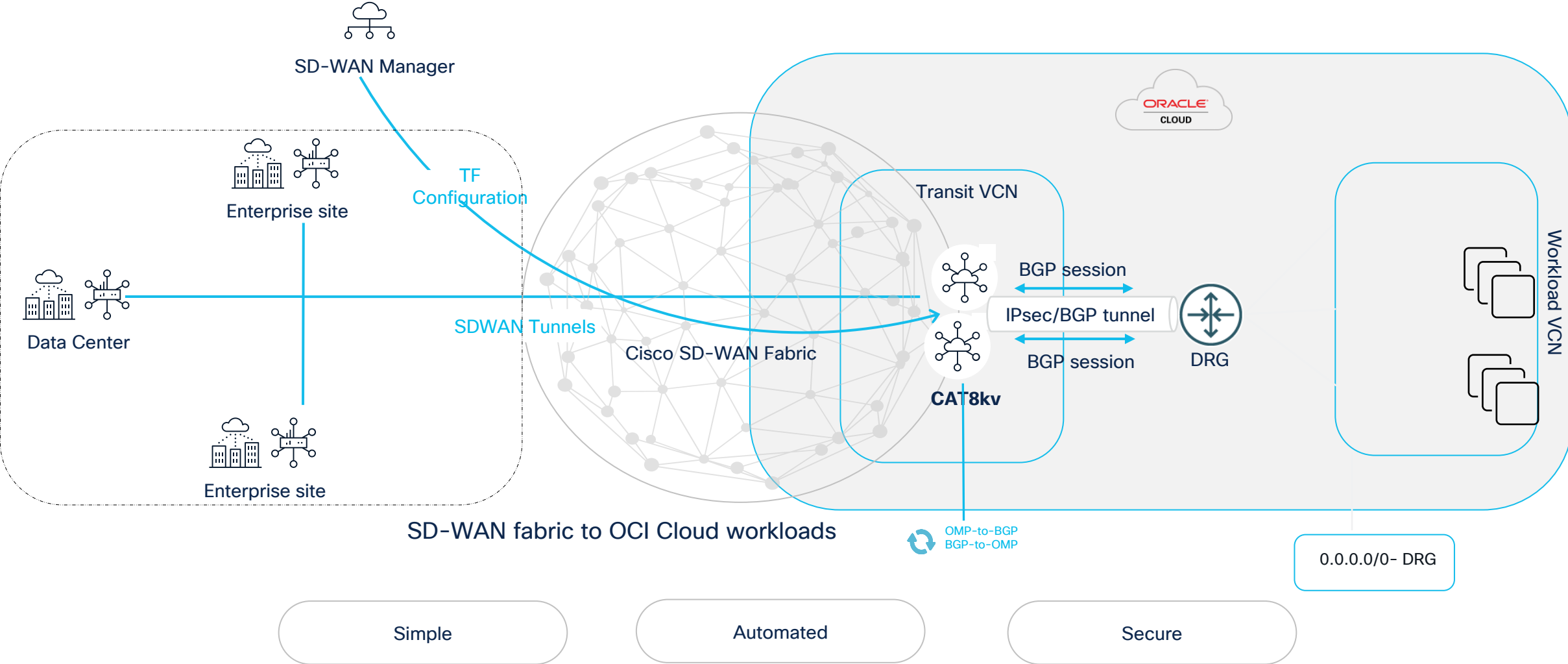
SD-WAN Fabric Between the Cloud



SD-WAN and OCI

SD-WAN - OCI support

SD-WAN Native Integration using IKE IPsec Transit VCN
cat8kv and DRG



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



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



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

Thank you

CISCO Live !

