
aws
SUMMIT
INDIA | MAY 25, 2023

GSAWS005

Networking considerations for a scalable architecture

Avanish Yadav
Senior Specialist Solutions Architect – Networking
AWS India

Swapnil Tiwari
Associate Solutions Architect
AWS India

Motivation for moving to multi - region architecture?

- Disaster recovery requirements
- Application global presence for decreased latency
- Data regulations or Compliance

Agenda

- Network connectivity patterns
- SD-WAN integration with AWS Cloud
- Simplifying the multi-region connectivity with Cloud-wan
- DNS & Endpoint failover
- Summary

Network connectivity design principles

Single or Multi-region architecture

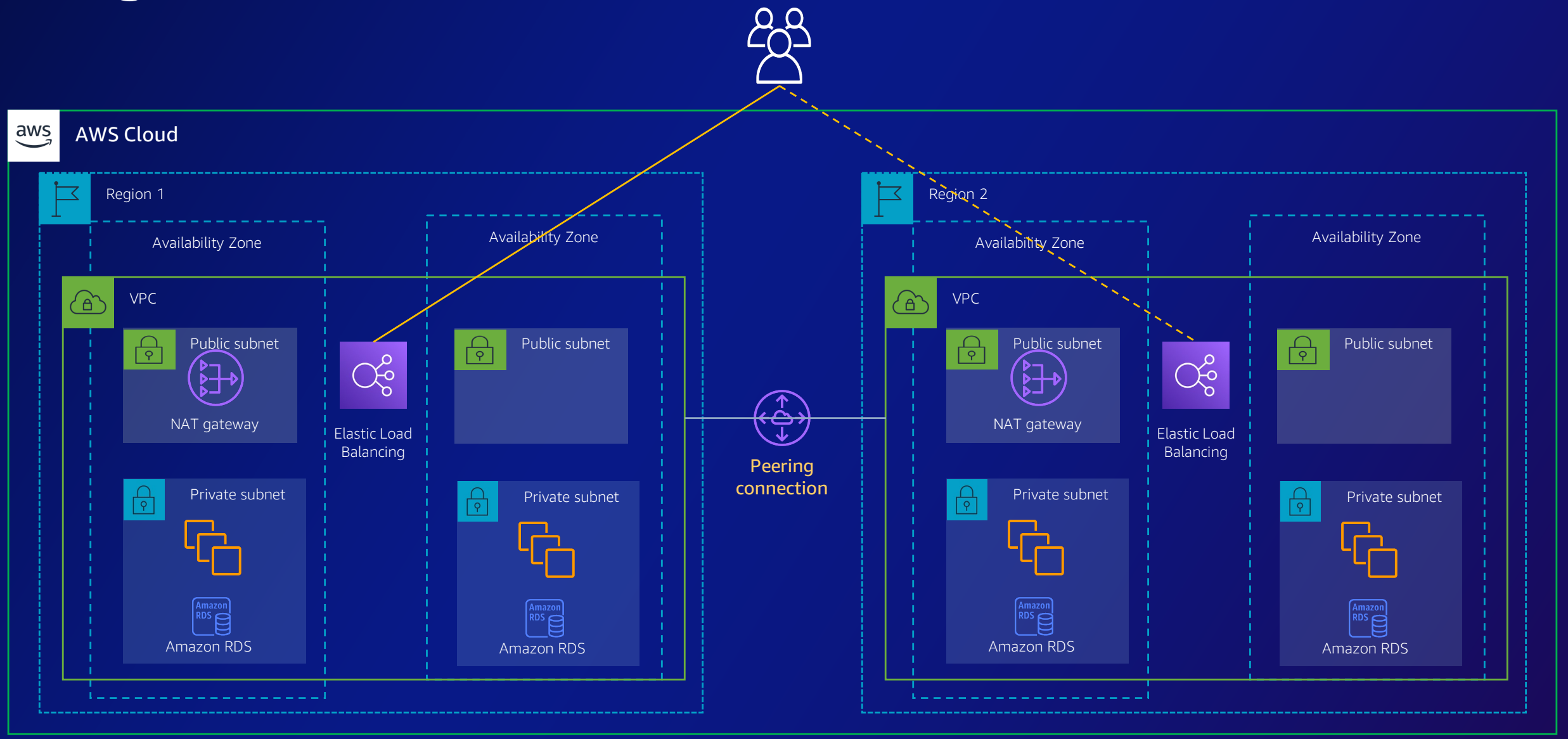
How do you plan your Network topology?

Networking		
	VPC, route tables, Security group, NACL, NAT Gateway, VPC end points, Transit gateway, Virtual private gateway, VPN, Elastic load balancer (ELB)	Regional scope
	Route 53, Direct connect gateway, Cloud front, Global accelerator	Global scope

- Use highly available AWS global backbone connectivity for your workload
- Provision redundant connectivity between private networks in the cloud and on-premises environments
- Prefer hub-and-spoke topologies over many-to-many mesh
- Enforce non-overlapping private IP address ranges

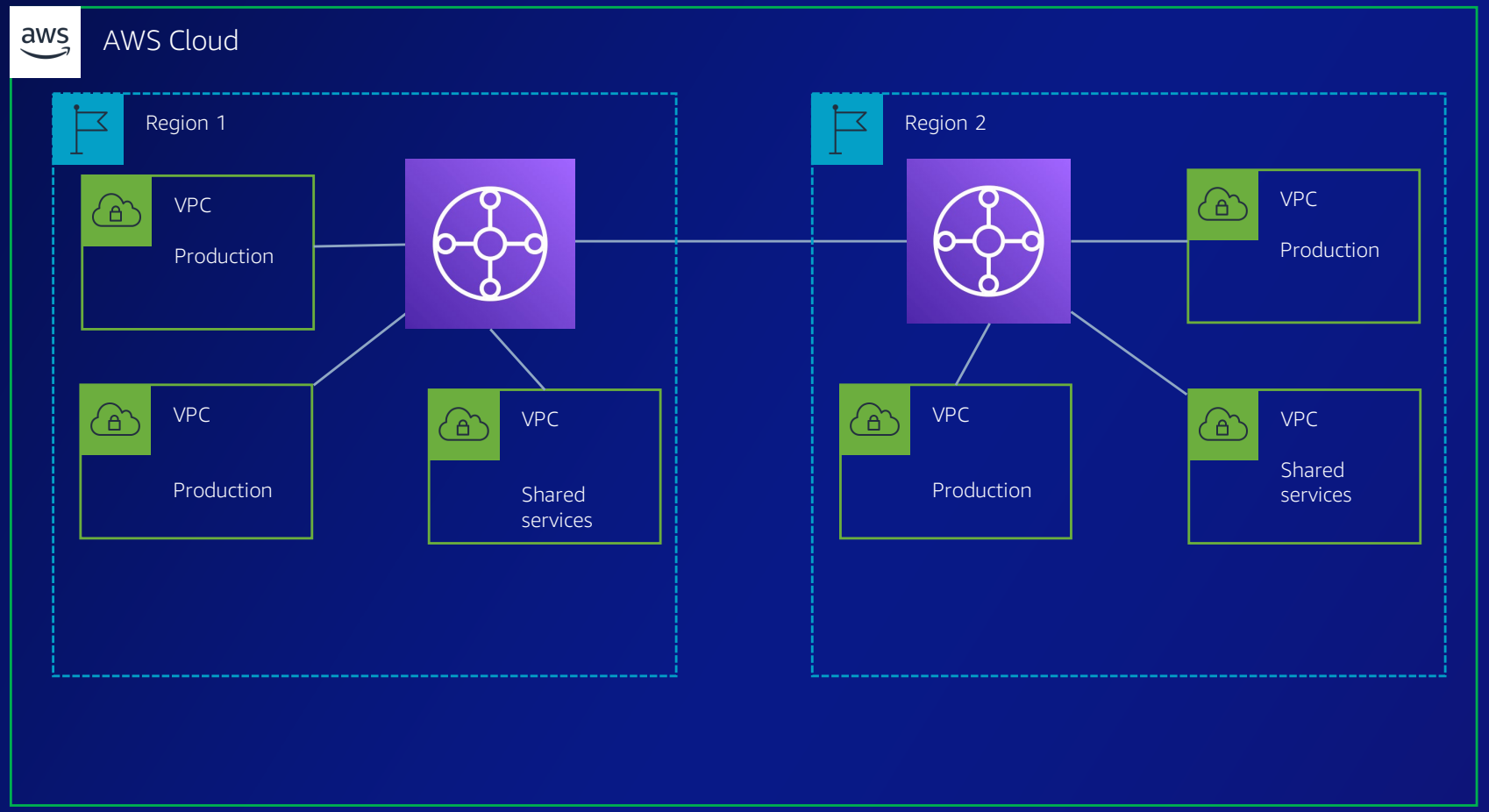
Single VPC architecture

Single VPC



Multi VPC and multi region architectures

Multi VPC – TGW peering



Key considerations

- TGW is used for inter-VPC communication in single region
- TGW peering* for inter region communication

* Traffic between the peered transit gateways requires static routes

Key considerations VPC's connectivity

- Non-overlapping IP addresses
- Use VPC Peering (Inter or Intra) for fewer number of VPCs, if you have more VPCs or plan to have more number of VPCs, use TGW and TGW Peering.
- Decision for number of VPCs depends on type of Network Level isolation
- Provision Core services in the 2nd region, if its your DR region.
- Outbound traffic EIPs might need to be white listed
- During DR event, inbound endpoints update in upstream CDN/External WAF/ DNS

Connectivity to data centers, branches and corporate offices

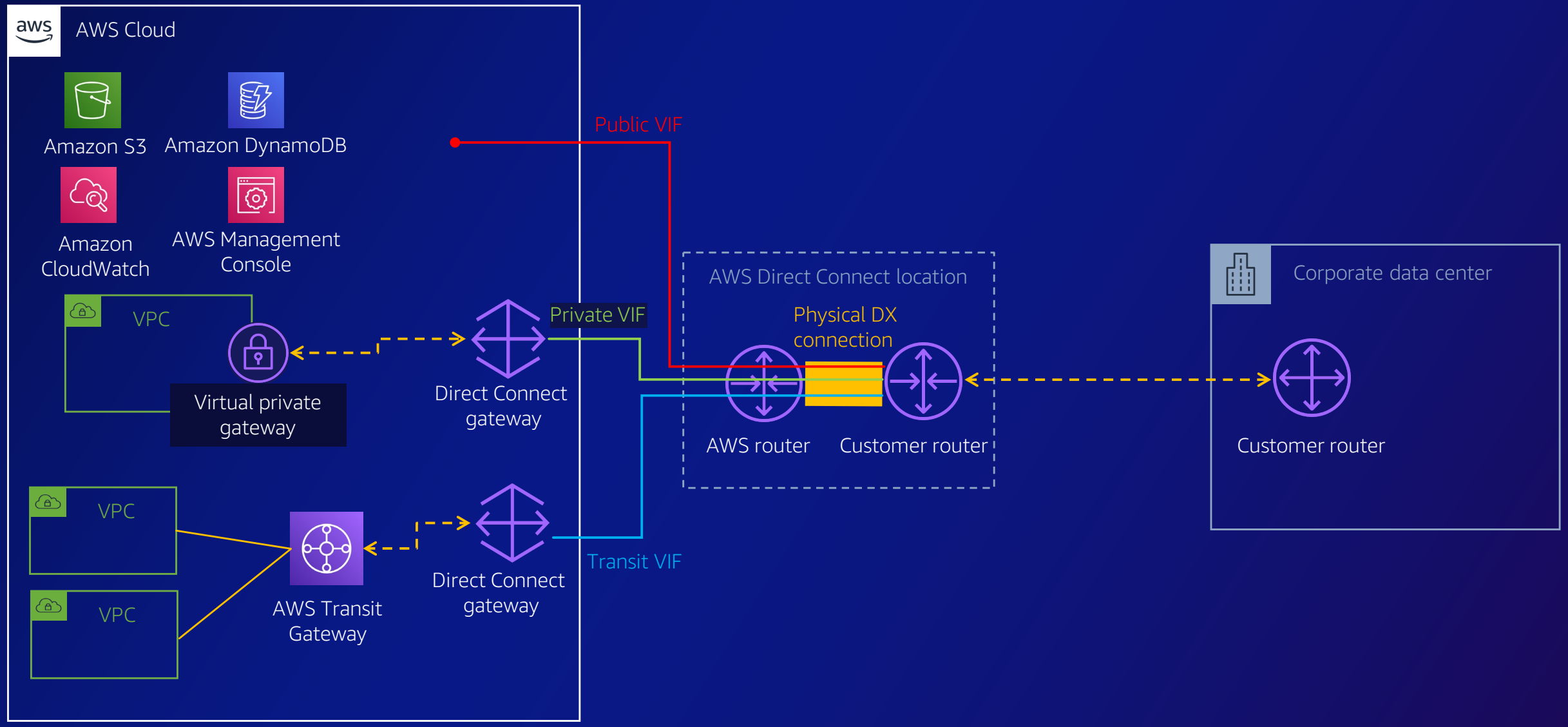
Hybrid connectivity options

Options for privately connecting your on premises Network with AWS:

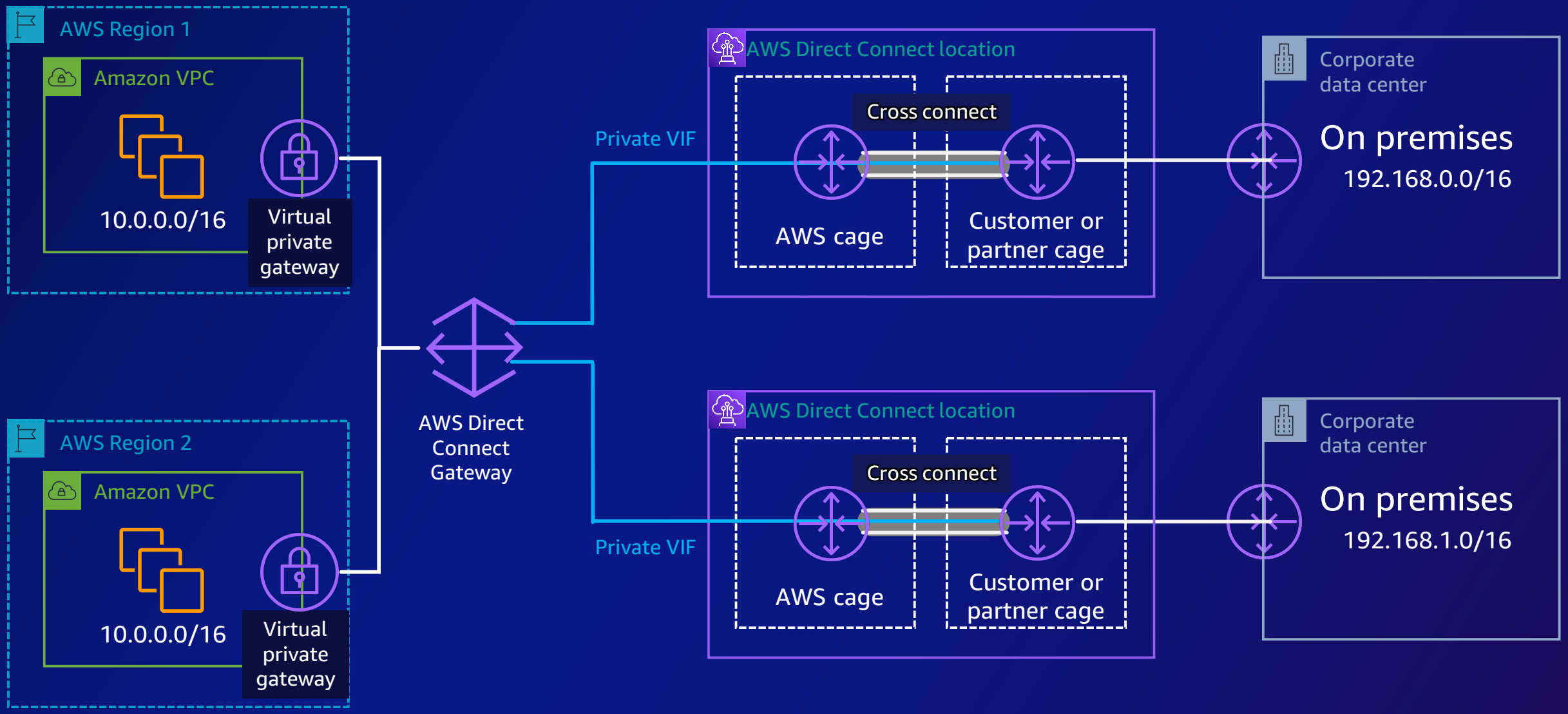
- AWS Direct Connect or,
- VPN or,
- SD-WAN over Direct Connect or Internet

Hybrid connectivity – Direct connect

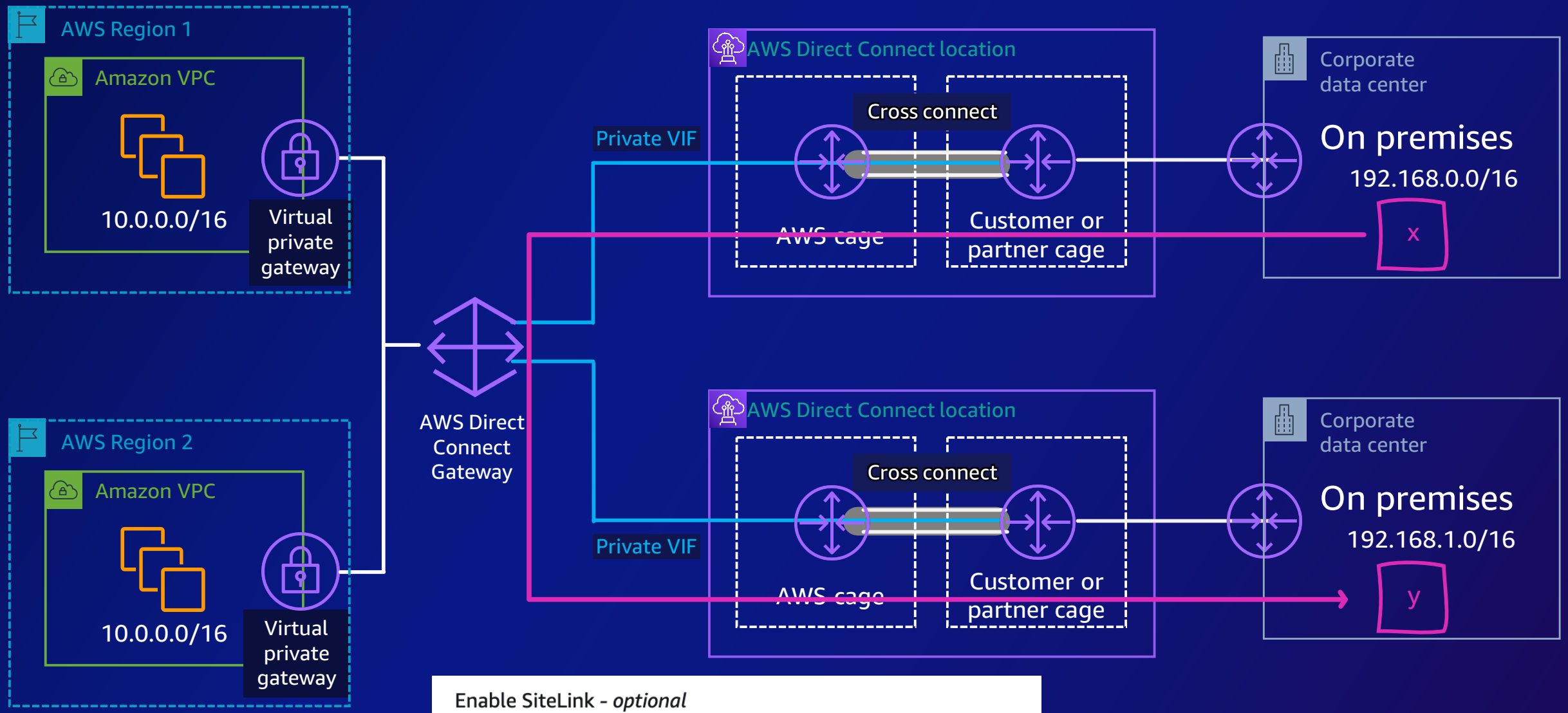
Direct connect – VIFs



Multi - region architecture – DXGW and VGW



AWS direct connect SiteLink

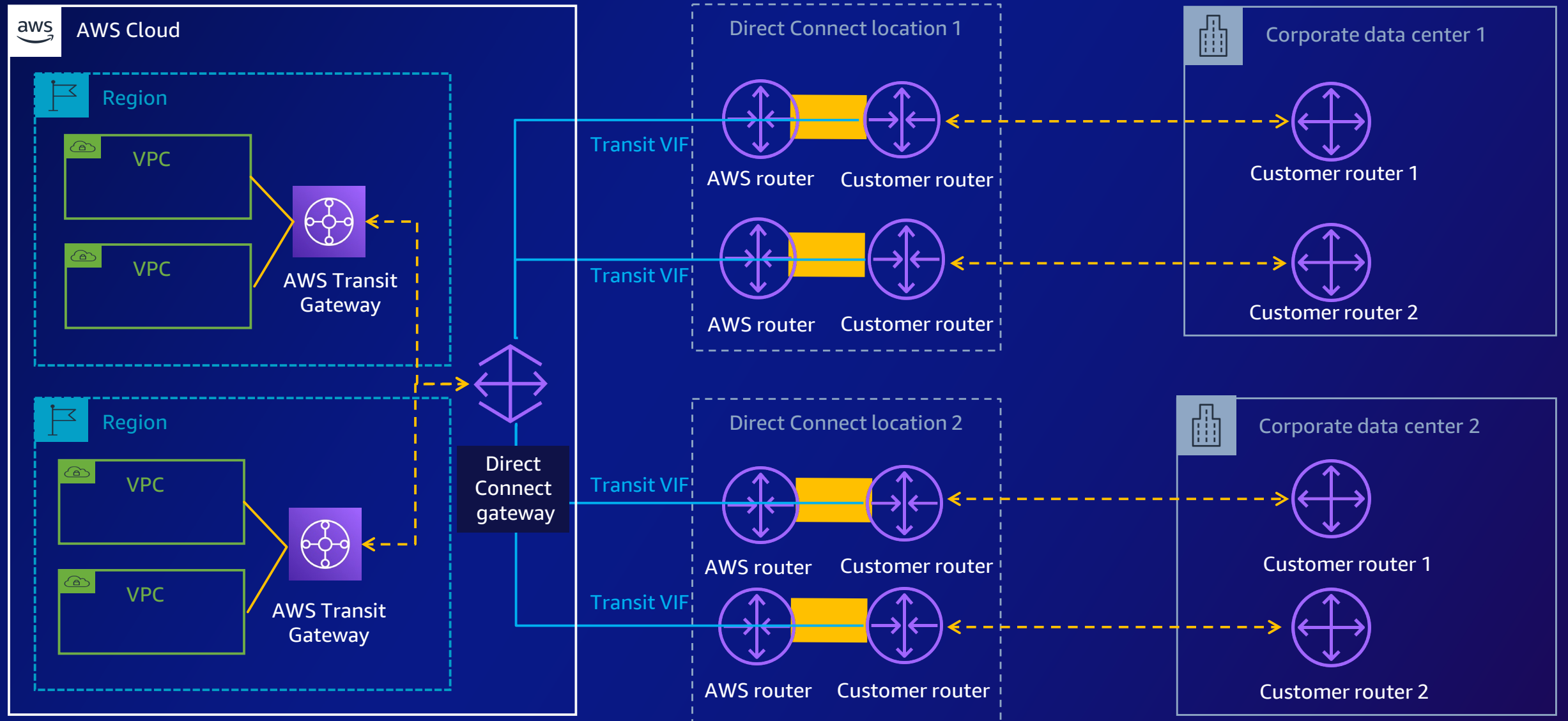


Enable SiteLink - *optional*

Enable direct connectivity between Direct Connect points of presence.

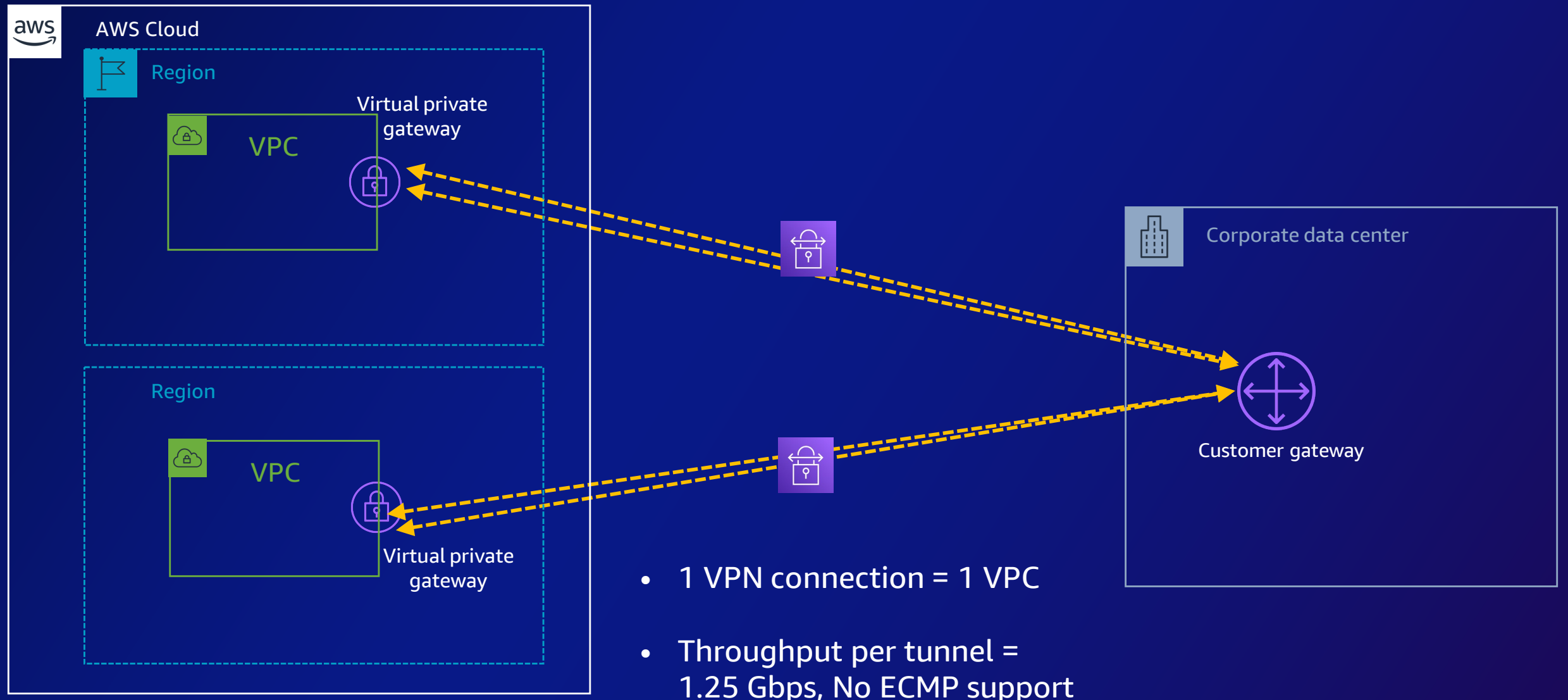
☑ Enabled

Multi - region architecture – DXGW and TGW



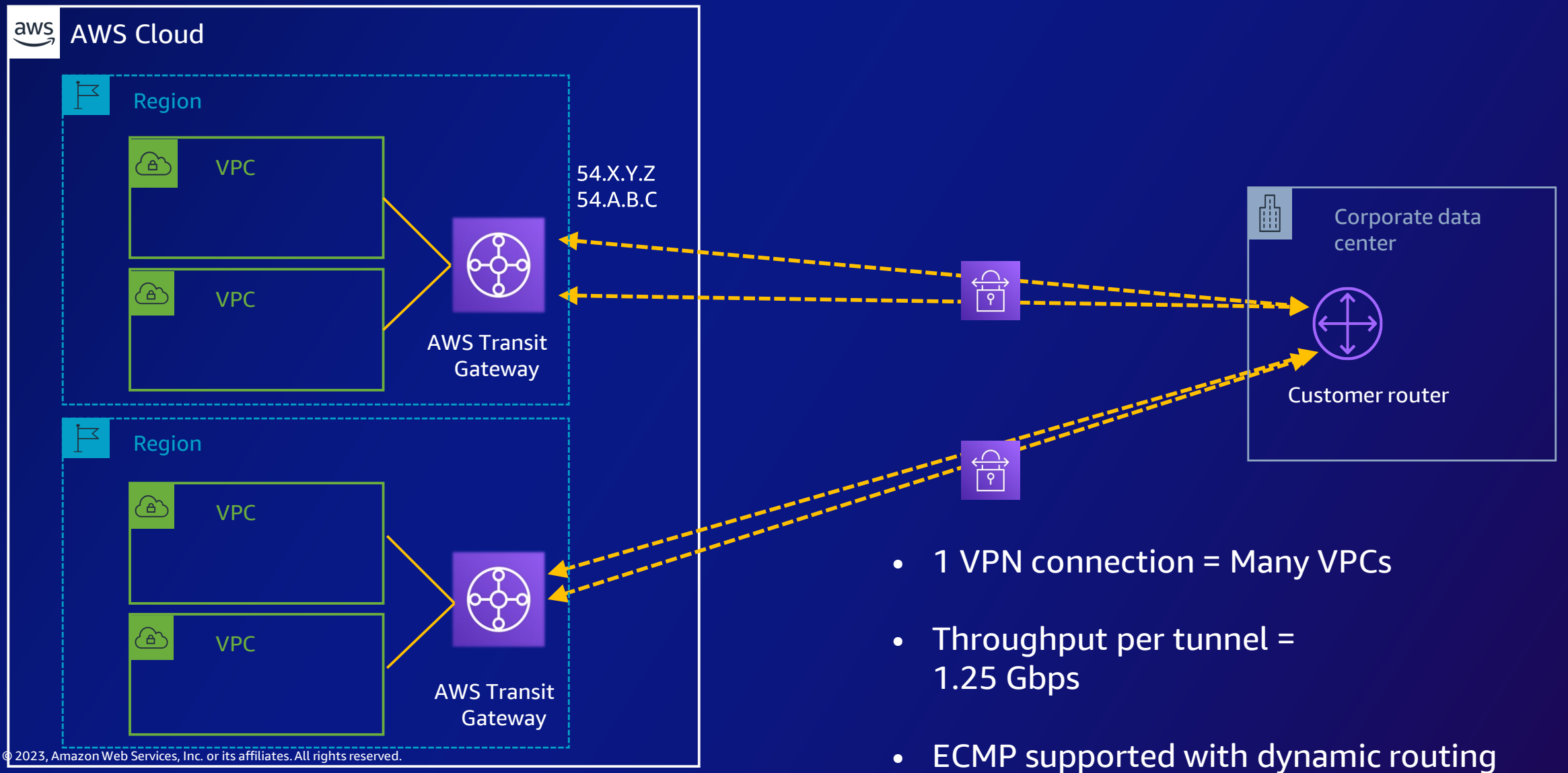
Hybrid connectivity – Site-to-Site VPN

Site-to-Site VPN: Virtual private gateway



- 1 VPN connection = 1 VPC
- Throughput per tunnel = 1.25 Gbps, No ECMP support

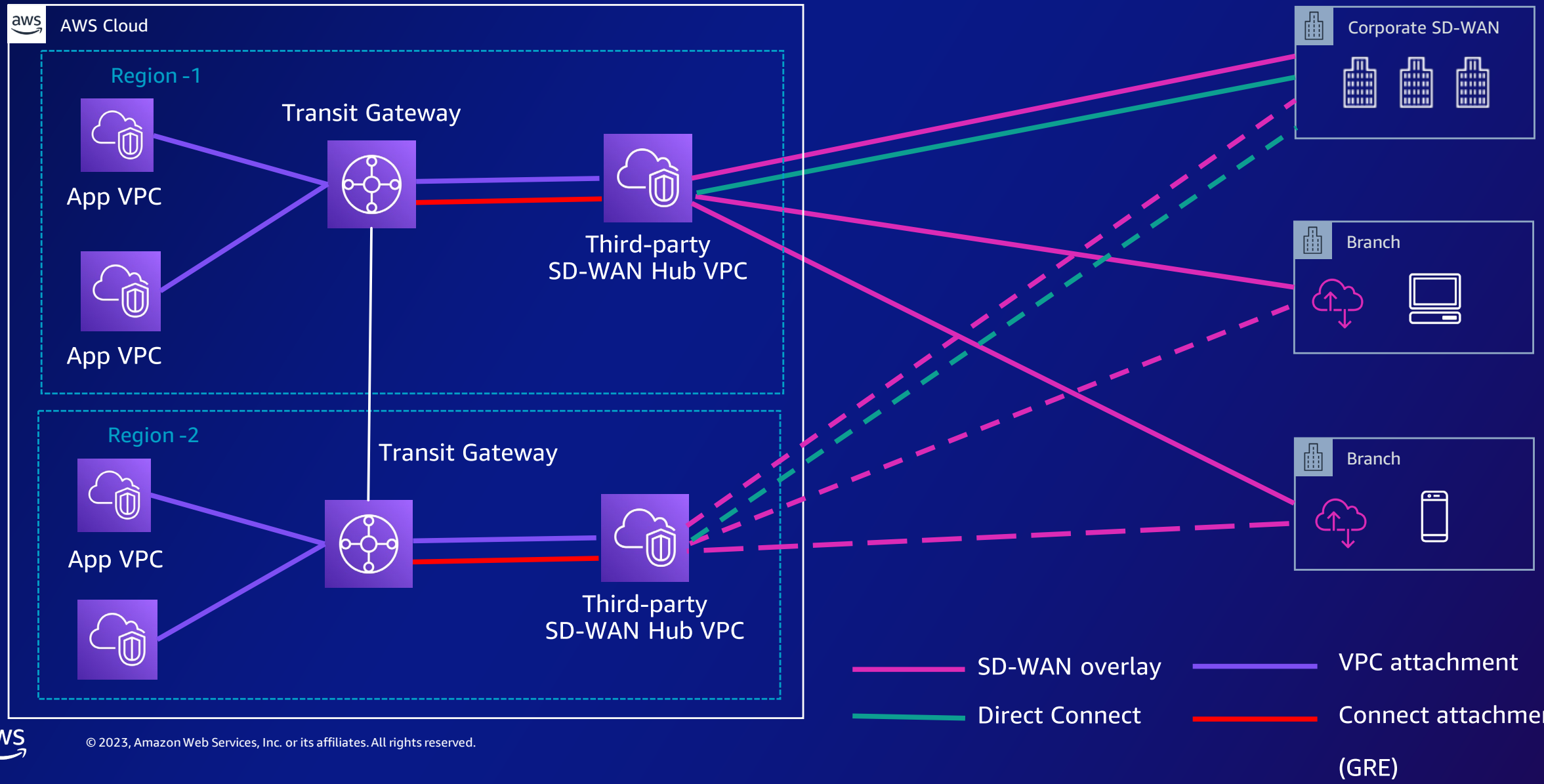
Connectivity using AWS Site-to-Site VPN with TGW



- 1 VPN connection = Many VPCs
- Throughput per tunnel = 1.25 Gbps
- ECMP supported with dynamic routing

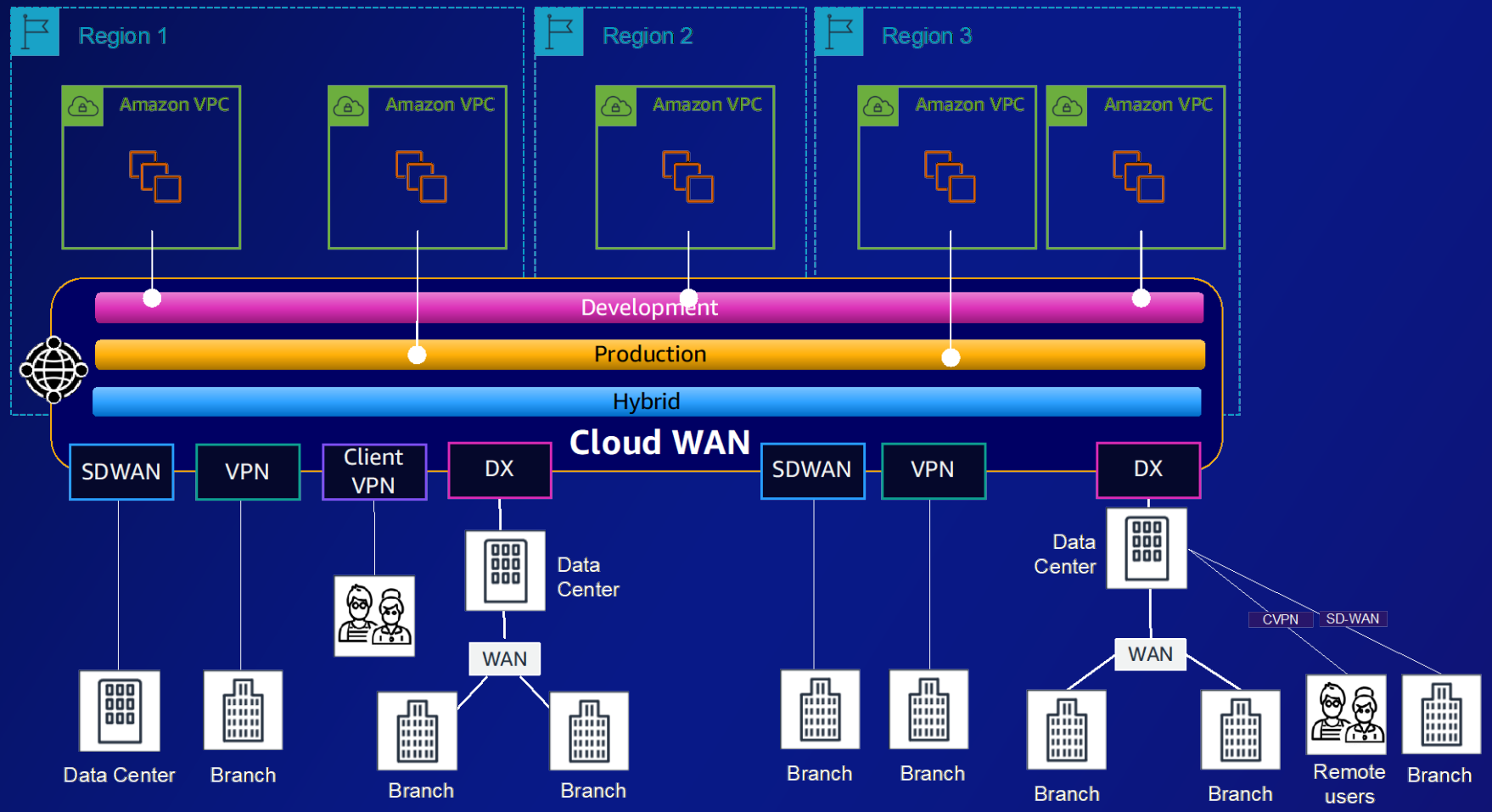
SD WAN integration with multi - region architecture

Transit gateway connect (SD-WAN/GRE)



On-premises and global connectivity

AWS cloud WAN: Global connectivity



Global

- Create connectivity across AWS Regions

Managed

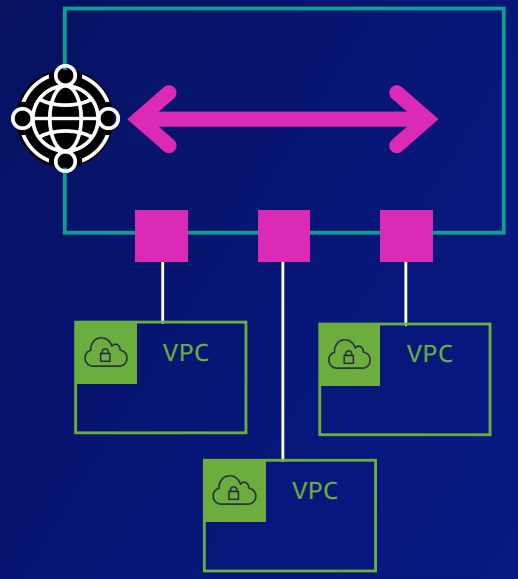
- Dynamic routing
- Built-in automation

Attach your things

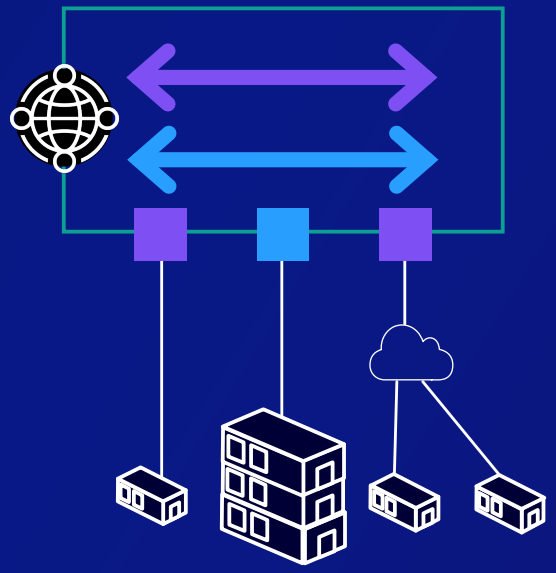
- VPCs
- VPNs
- SD-WAN
- Client VPN
- Firewalls

Last-mile equipment and equipment on customer premises doesn't change

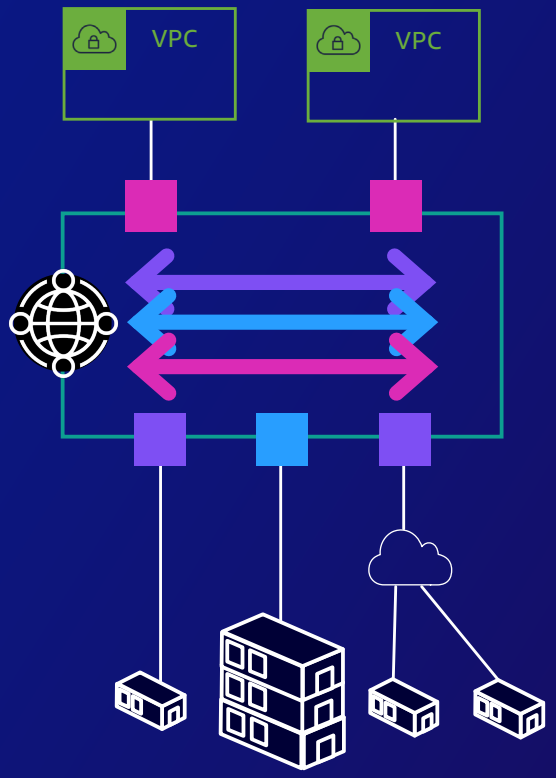
AWS cloud WAN use cases



Between VPCs



WAN



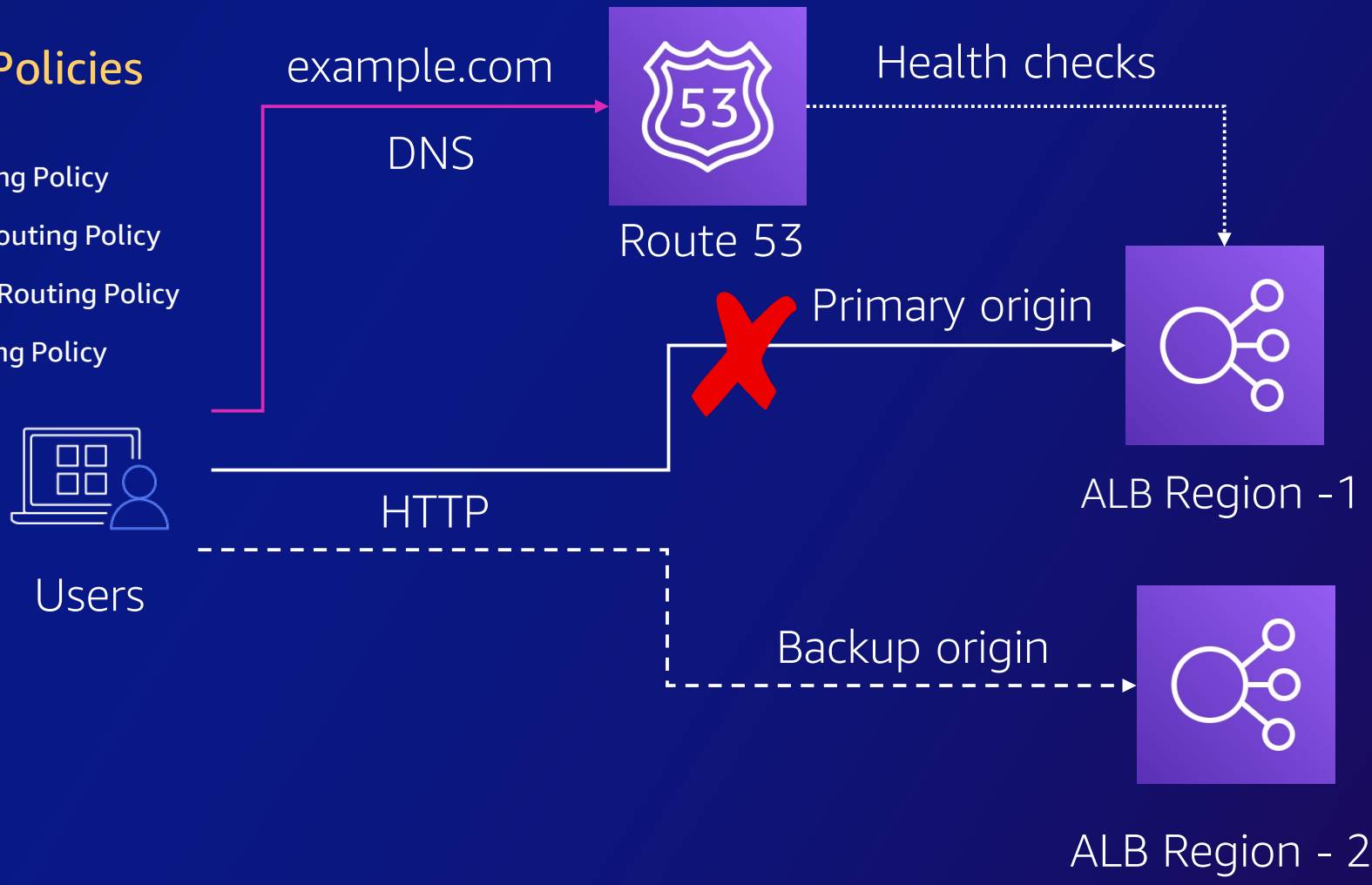
Hybrid

Amazon Route 53

Multi - region disaster recovery scenarios

Amazon Route 53 – Internet to multi-region architecture

- Health Checks
  - Health Check can monitor one of the following:-
  - Specific resource, such as a web server
  - Status of other health checks
  - Status of an Amazon CloudWatch alarm
- Routing Policies
  - Failover Routing Policy
  - Geolocation Routing Policy
  - Geoproximity Routing Policy
  - Latency Routing Policy
  - …

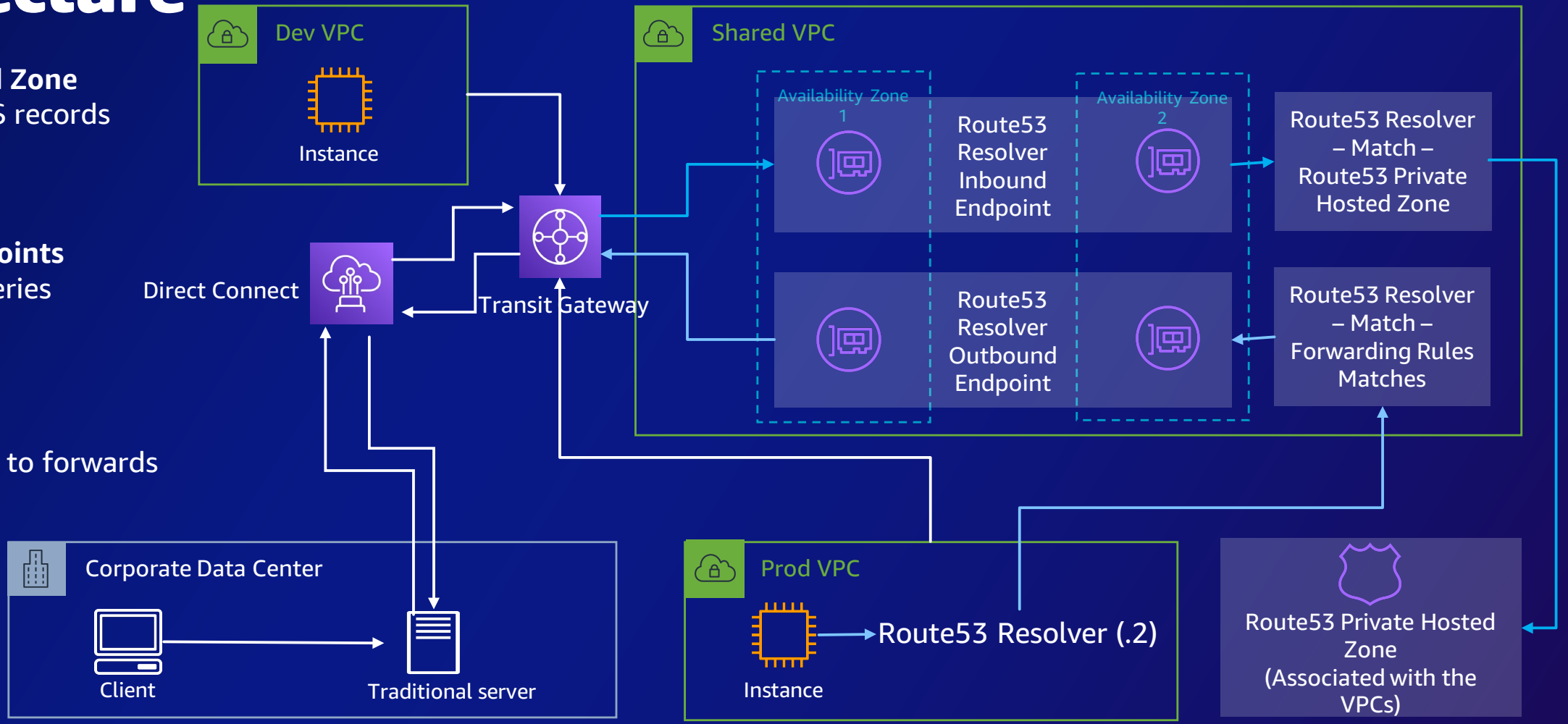


Amazon Route 53 – DNS Resolution in Hybrid Architecture

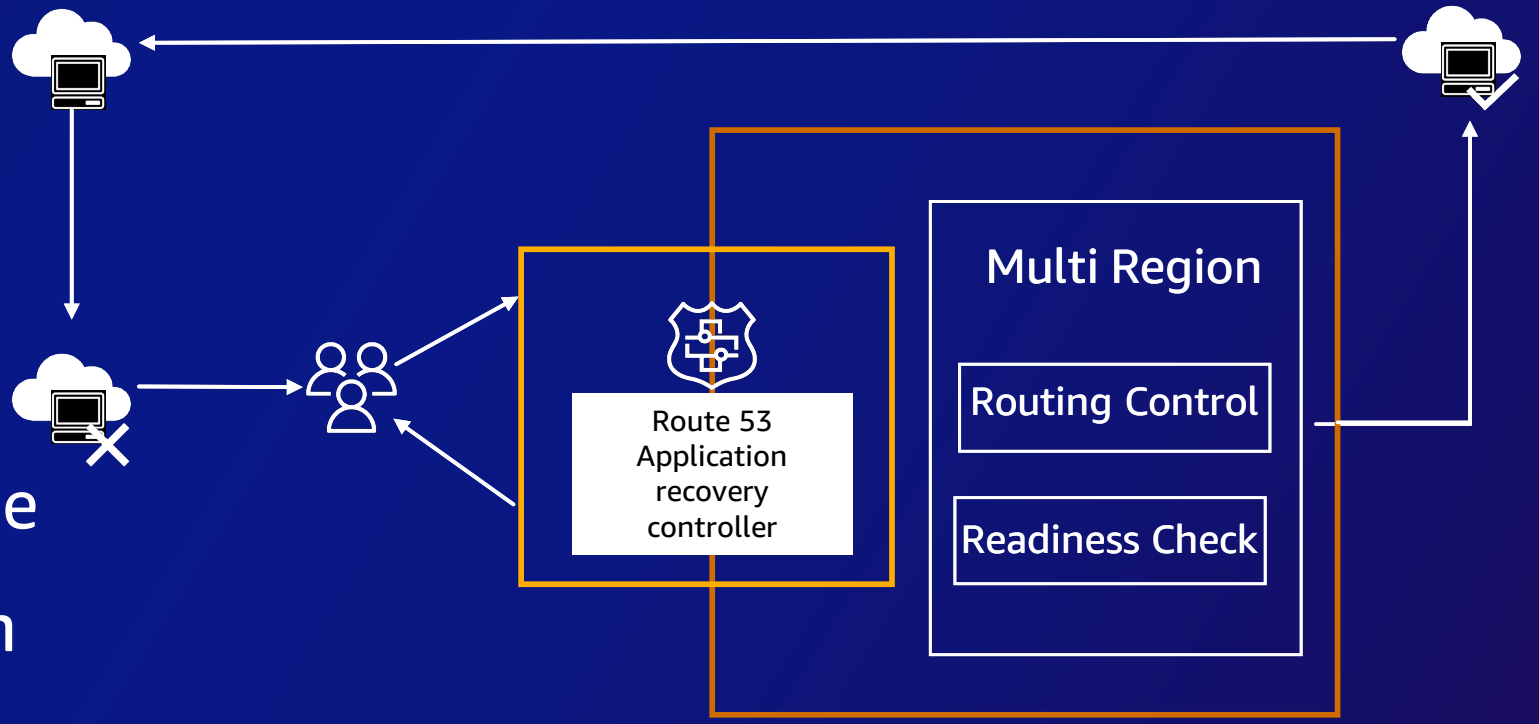
1. Private Hosted Zone
Host internal DNS records

2. Resolver Endpoints
Forward DNS Queries

3. Resolver Rules
To decide queries to forwards



Amazon Route 53 Application Recovery Controller



Centralized, safe, and reliable way to manage cross-region and cross-AZ recovery

Summary

- Motivation towards multi-region architecture
- Single VPC and multi VPC multi-region architecture
- Hybrid connectivity options
- Amazon Route 53

Resources

Networking Workshop

CloudWAN Workshop

Case Studies and Blogs

Thank you!

Please complete the session survey

Avanish Yadav
Senior Specialist Solutions Architect – Networking
AWS India

Swapnil Tiwari
Associate Solutions Architect
AWS India