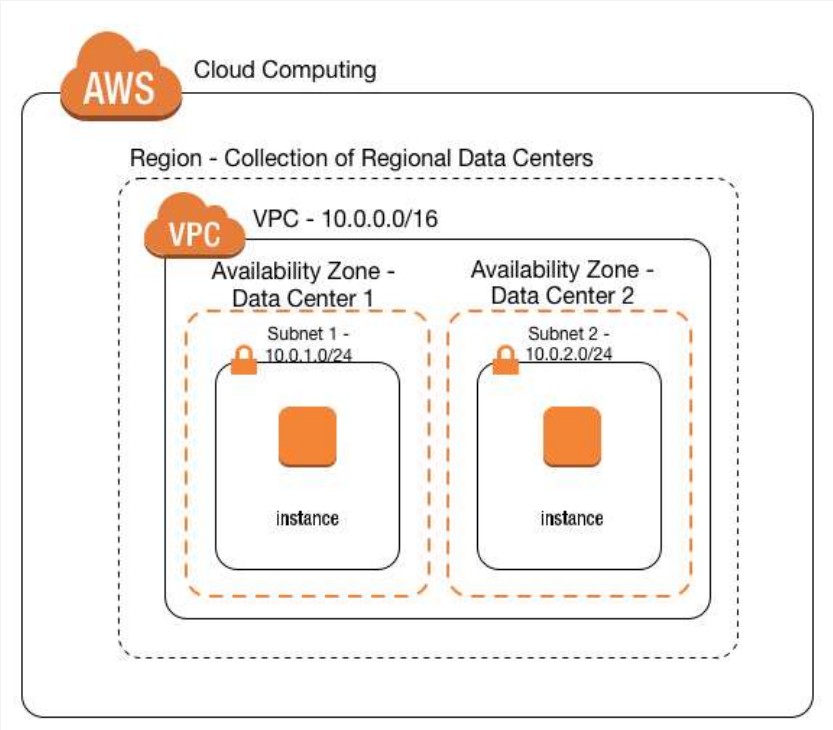
CABLES TO THE CLOUD

Hybrid Network connectivity to AWS

AWS FUNDAMENTALS



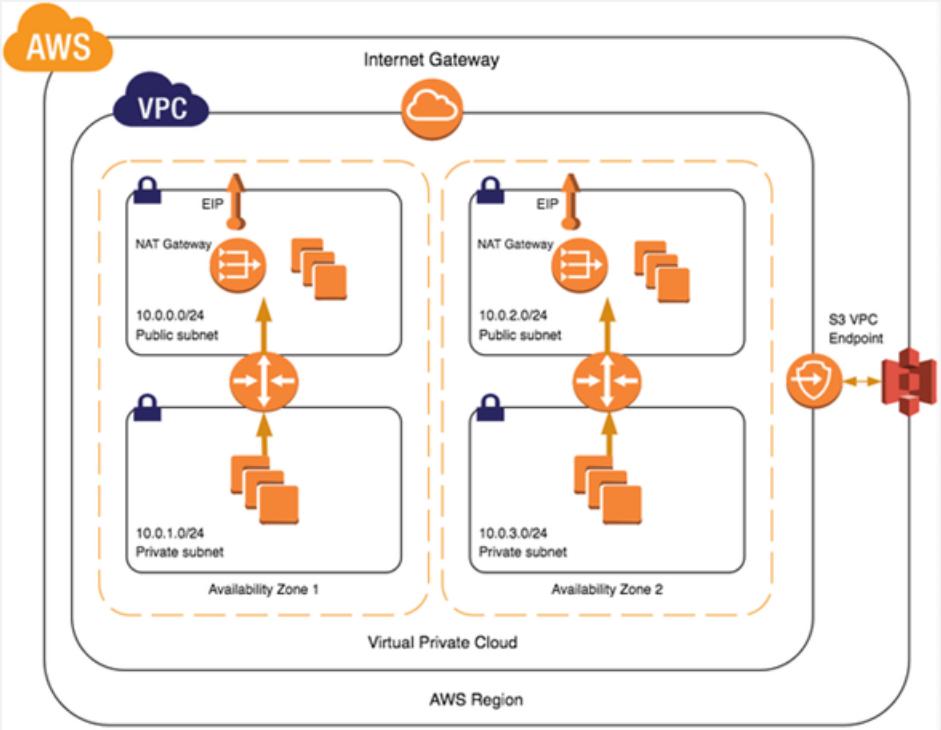
AWS CONNECTIVITY OPTIONS

- Internet
- VPN
  - AWS Managed
  - 3rd Party Solutions
- Direct Connect

INTERNET CONNECTION

- Console access via HTTPS
- Access to S3 buckets and other internet facing services
- Security Groups to permit access over internet to VPC
- Limited in capability
- Good use case if no direct back-end connectivity is required
- No QOS

MULTI-AZ EXAMPLE



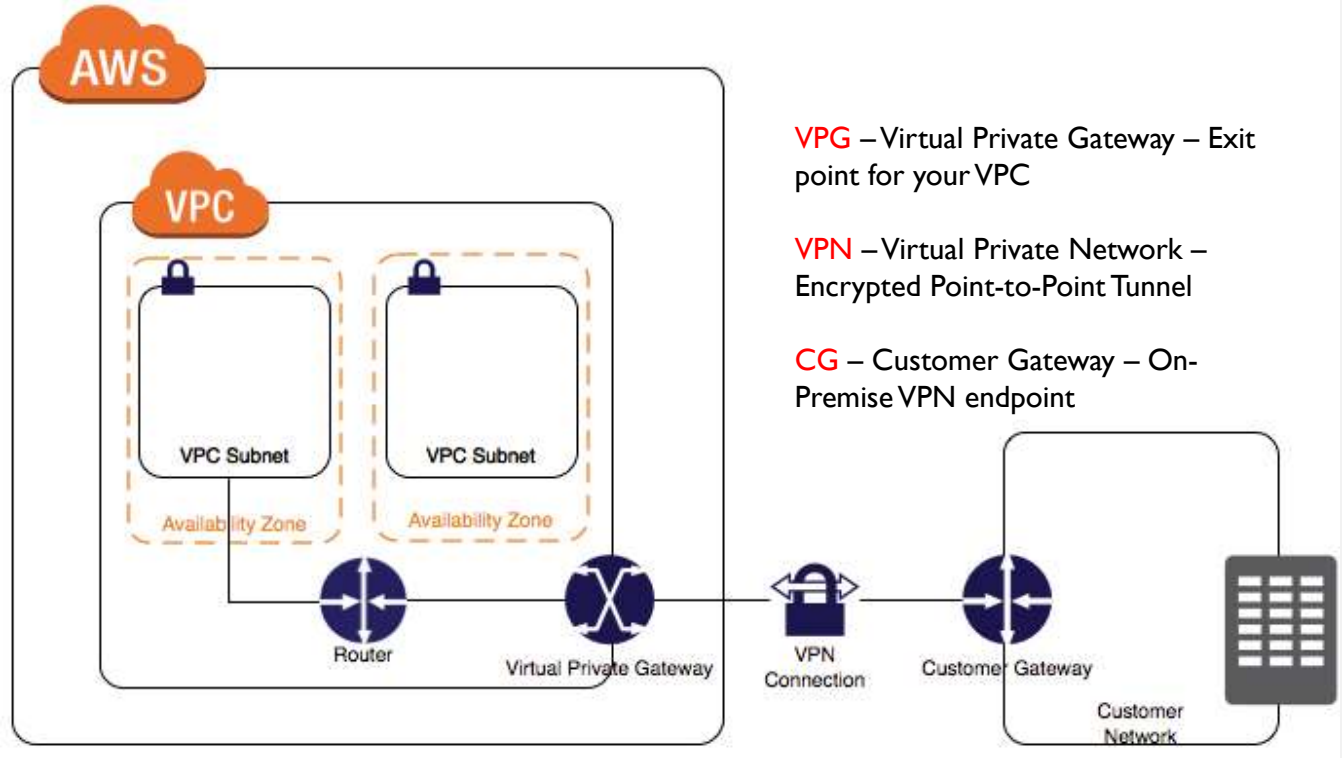
Public and private multi-AZ VPC with NAT gateways

- Two Public subnets with NAT Gateway for outgoing traffic
- Two Private subnets

VPN – AWS MANAGED

- IPSEC VPN from On-Premise to AWS Region
- AWS creates Two Tunnels per VPN Connection
  - Redundancy to two different Availability Zones
- Can use Static Routing or BGP Dynamic Routing
  - Dynamic routing is preferred
- Limited configuration options
- Keepalives must be sent from on-premise in order for tunnels to remain active
- No QOS

VPN – AWS MANAGED

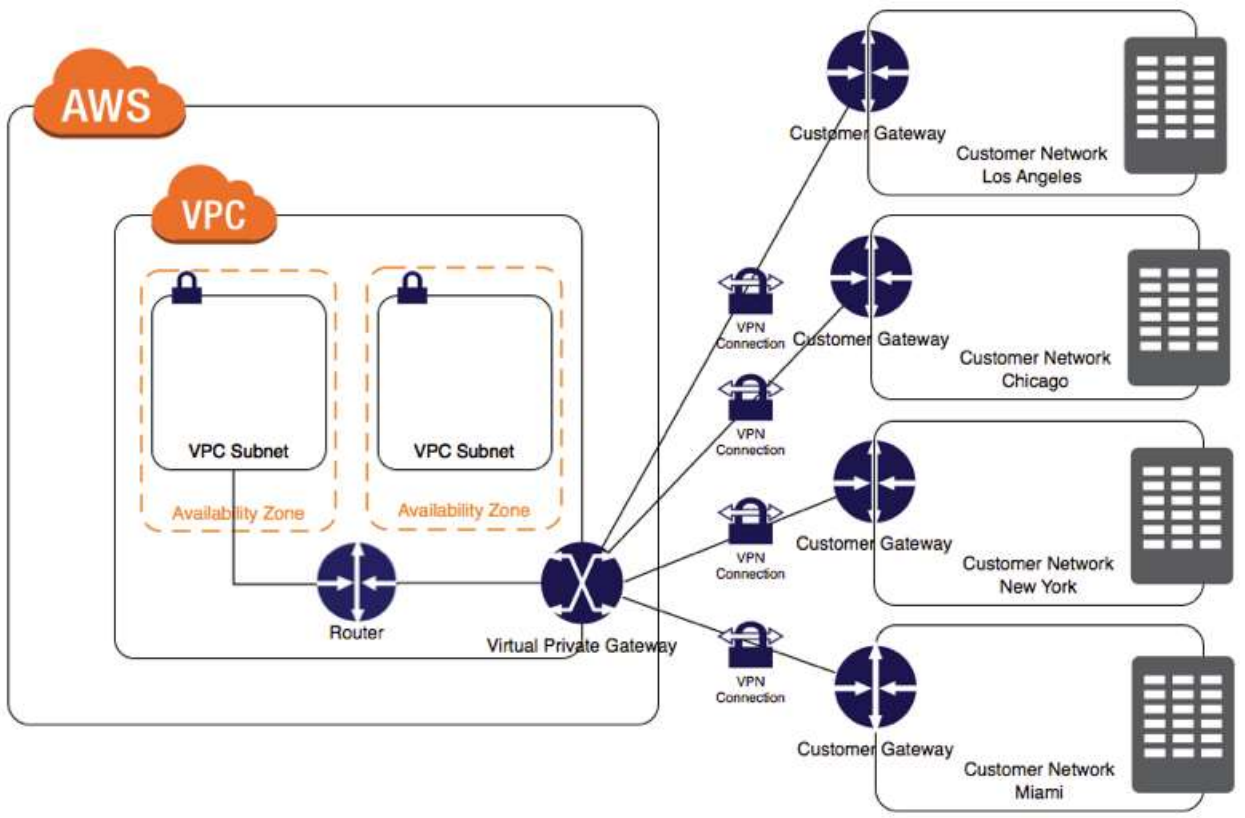


VPG – Virtual Private Gateway – Exit point for your VPC

VPN – Virtual Private Network – Encrypted Point-to-Point Tunnel

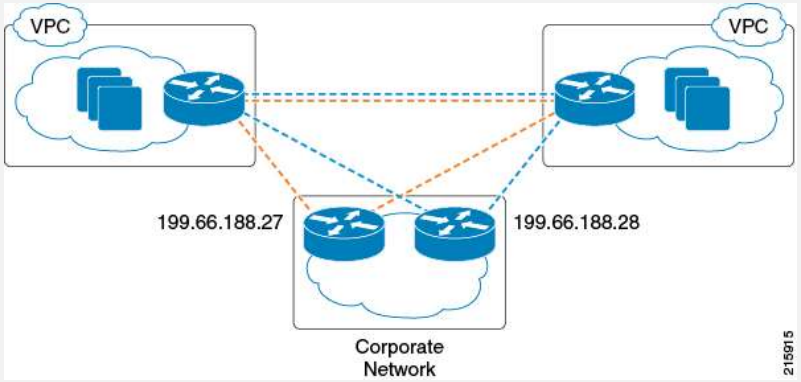
CG – Customer Gateway – On-Premise VPN endpoint

VPN – AWS MANAGED



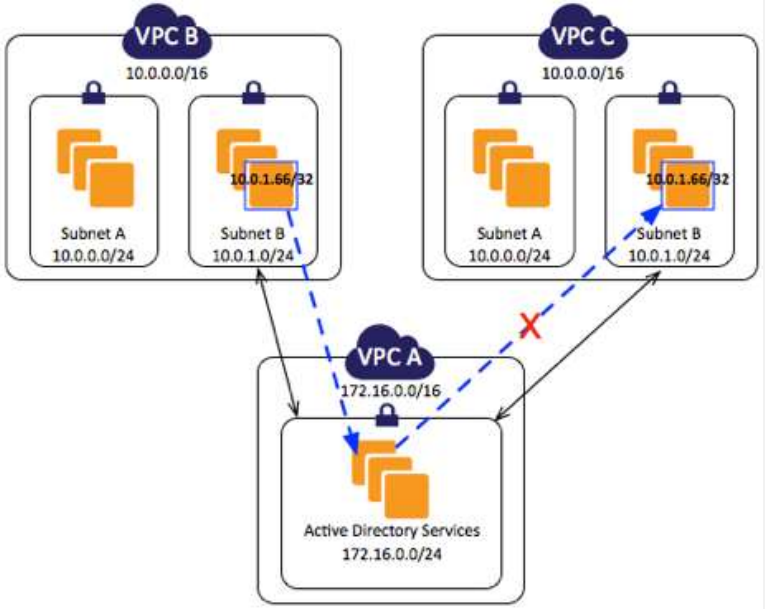
VPN – 3RD PARTY

- Instead of using the AWS managed VPN you can install a 3rd party VPN solution and manage it yourself
- Same concept as the AWS VPN but you have more granular control over the VPN
- Cisco CSR1000V, PFSense, PaloAlto
- Many images are available on the AWS marketplace



VPC PEERING LIMITATIONS

- AWS provides the capability for VPC's to communicate to each other across accounts and regions
- VPC peering connections are non-transative and cannot be used to connect VPN or direct connect to additional VPC.



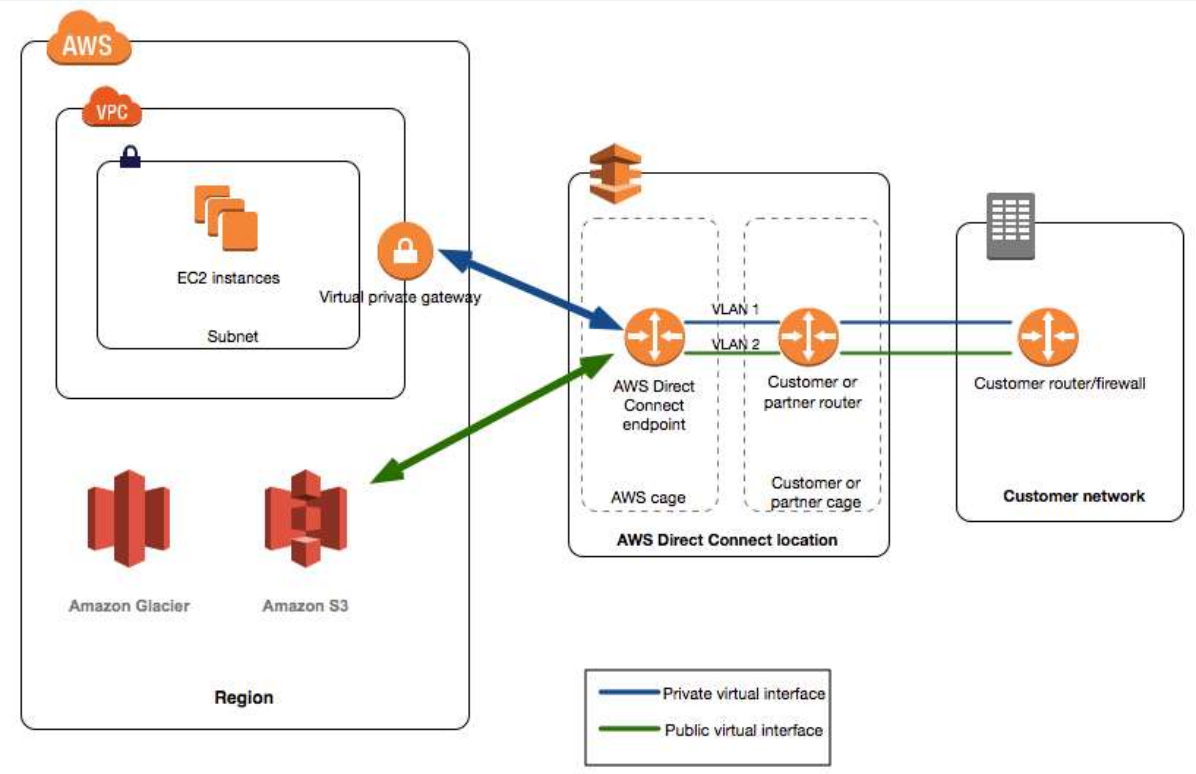
DIRECT CONNECT

- Direct Connect provides high speed connections into AWS regions over either cross connections at specific data centers or over MPLS providers
- Use cases are for working with large data transfers, real-time data feeds, or hybrid environments
- Direct connect provides QOS capabilities not available in any other solution
- Direct connect is also the most expensive solution for connecting to AWS.

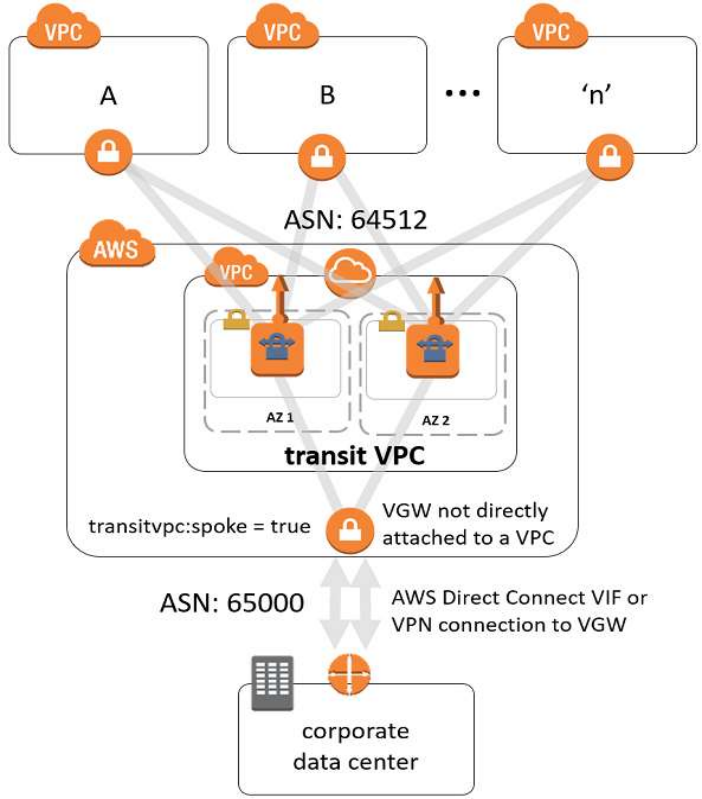
DIRECT CONNECT LOCATIONS

- AWS regions have partner Colocation Providers and Telecom Carriers that can provide cross-connectivity into AWS – e.g. Equinex and Level-3
- Direct Connect provides either sub 1GB, 1Gb or 10Gb connections
- 1GB and 10GB connections can be Layer-2 connected while sub 1Gb are not and can only connect Layer-3 to a VPC.
- https://aws.amazon.com/directconnect/partners/

DIRECT CONNECT SIMPLE EXAMPLE



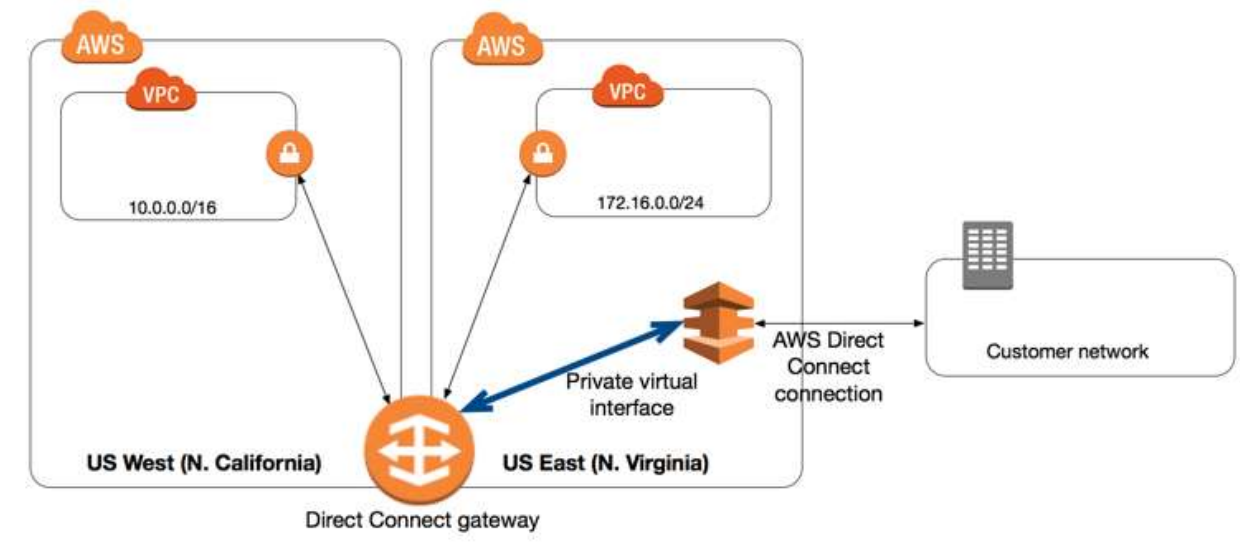
DIRECT CONNECT - TRANSIT VPC



- Overcomes VPC Peering limitations
- Adds complexity and management of 3rd party VPN

DIRECT CONNECT GATEWAYS

- Direct Connect Gateways – Allows for connections between VPCs sharing the same direct connection



SUMMARY

Internet	VPN	Direct-Connect
No direct back-end connectivity	Provides multi-AZ Tunnels	Provides L2 or L3 connectivity to VPCs
Access to public facing services	For AWS VPN keep-alive traffic must be sent from on-prem	Direct connect partner required
Least Expensive	Use AWS managed or 3rd party VPN	High Speed connectivity options
No QOS	Less Configuration for AWS Managed	Transit VPC or direct VPC connections
	VPN must be established to each VPC	Direct Connect Gateway can provide multi-VPC connectivity in same account
	No QOS	Most Expensive
		QOS