



Networking in AWS

Corey Harris Jr., Solutions Architect – chj@amazon.com

Agenda

- Amazon VPC – Virtual Private Cloud
- VPC Building Blocks
- VPC Security
- VPC Connectivity Options
- Connect your Data Center to AWS
- Traffic Distribution

Amazon VPC

Amazon VPC - Virtual Private Cloud

Provision a **logically isolated section** of the AWS Cloud where you can launch AWS resources in a **virtual network that you define**.

Bring your own network



IP Addresses



Subnets



Network Topology

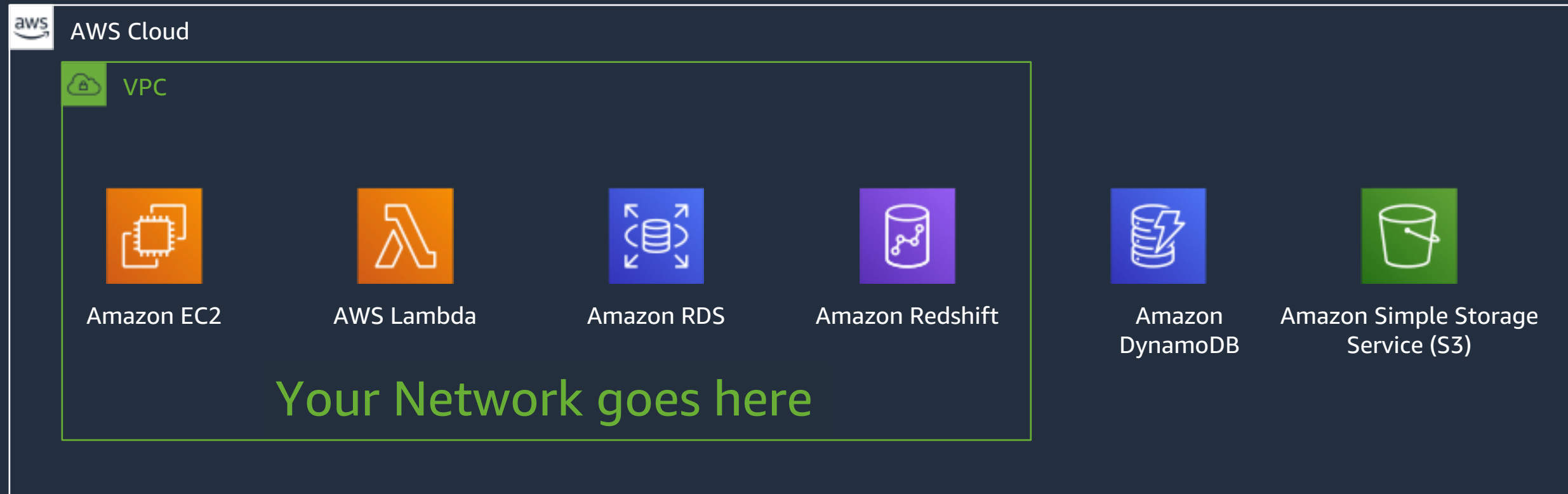


Routing Rules



Security Rules

Amazon Virtual Private Cloud (VPC)

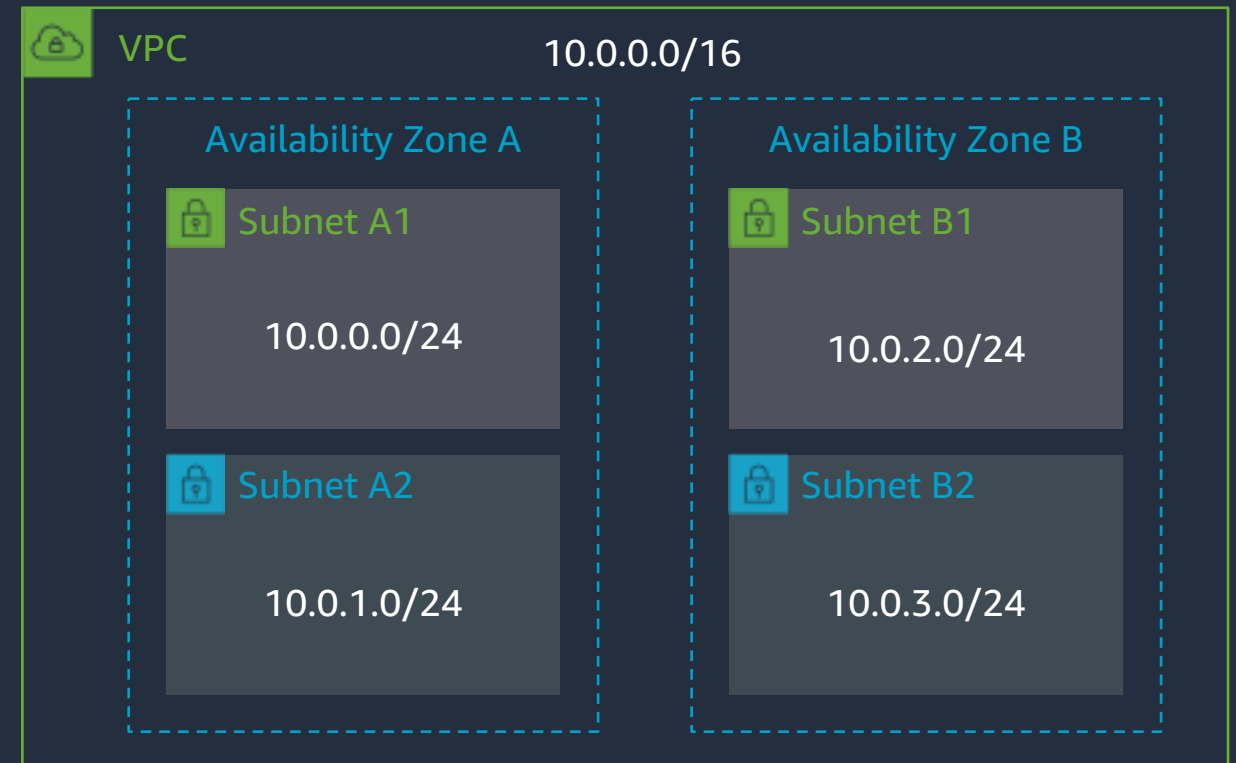


VPC Building Blocks

How to segment my networks inside a VPC?

VPC Subnets

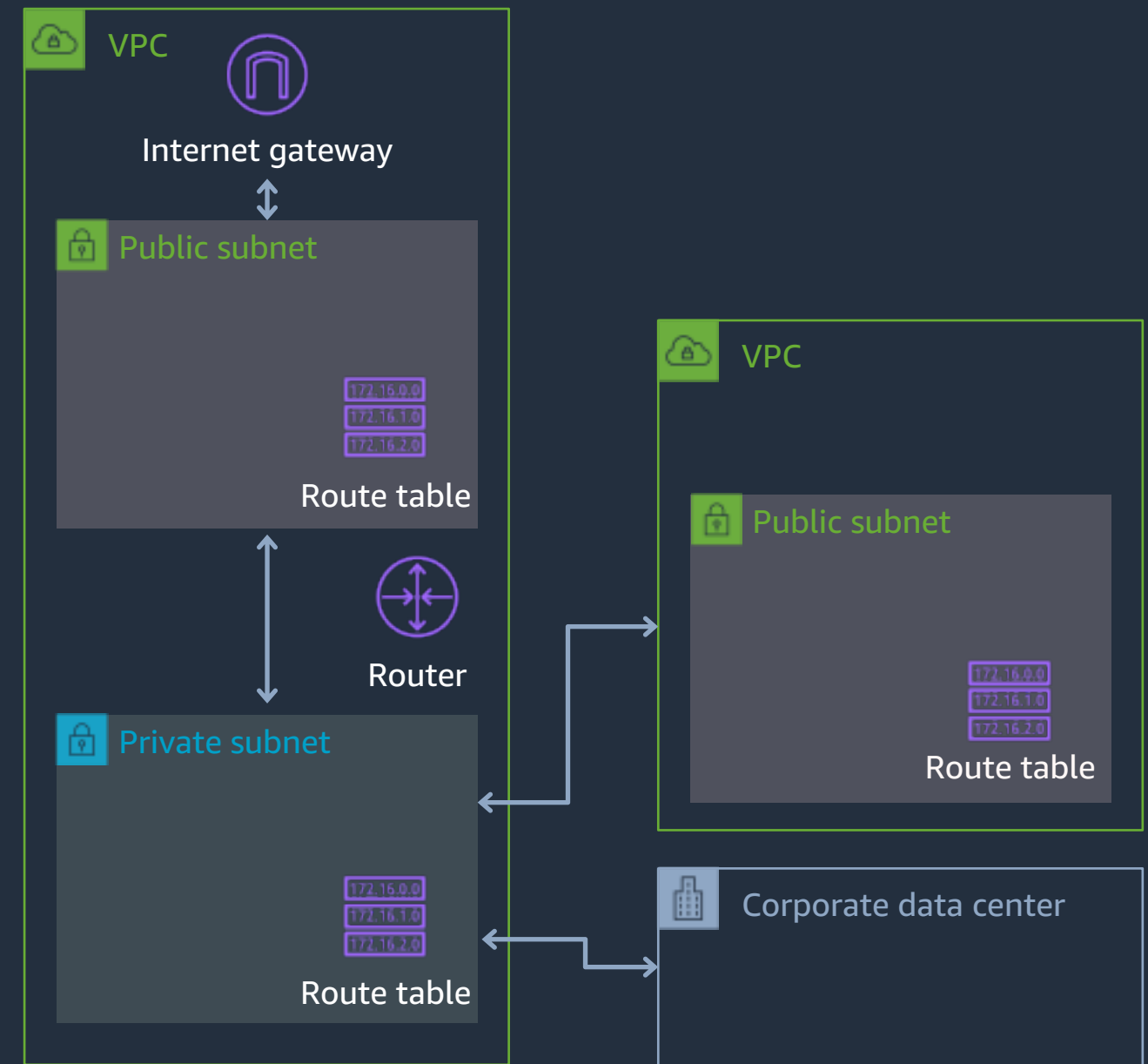
- You can add one or more subnets in each Availability Zone
- AZs provides fault isolations
- Subnets are allocated as a subset of the VPC CIDR range



How to direct traffic out of my Subnets?

Subnets and Route Tables

- Each subnet can have a unique Route Table
- Route Tables direct traffic out of the VPC, towards:
 - Internet Gateway
 - Virtual Private Gateway
 - VPC Endpoints
 - Direct Connect
 - VPC Peering
 - AWS Transit Gateway
- Subnets are named “Public Subnets” when connected to an Internet Gateway



How to connect my VPC to the Internet?

Internet Gateway

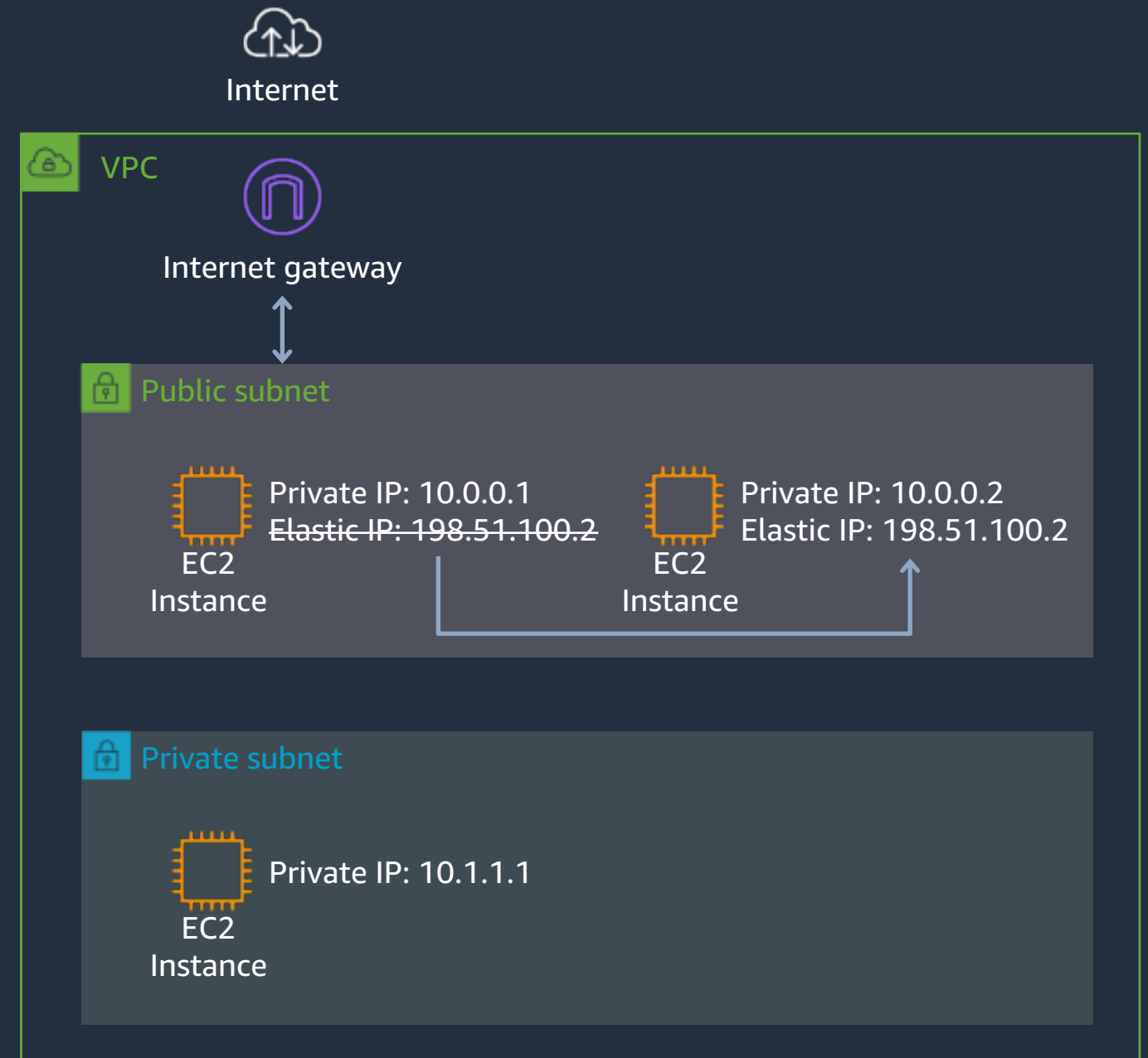
- Horizontally scaled, redundant, highly available VPC component
- Connect your VPC Subnets to the Internet
- Must be referenced on the Route Table
- Performs NAT between Public and Private IP Addresses



How does my instance get an IP address?

Elastic IP Address

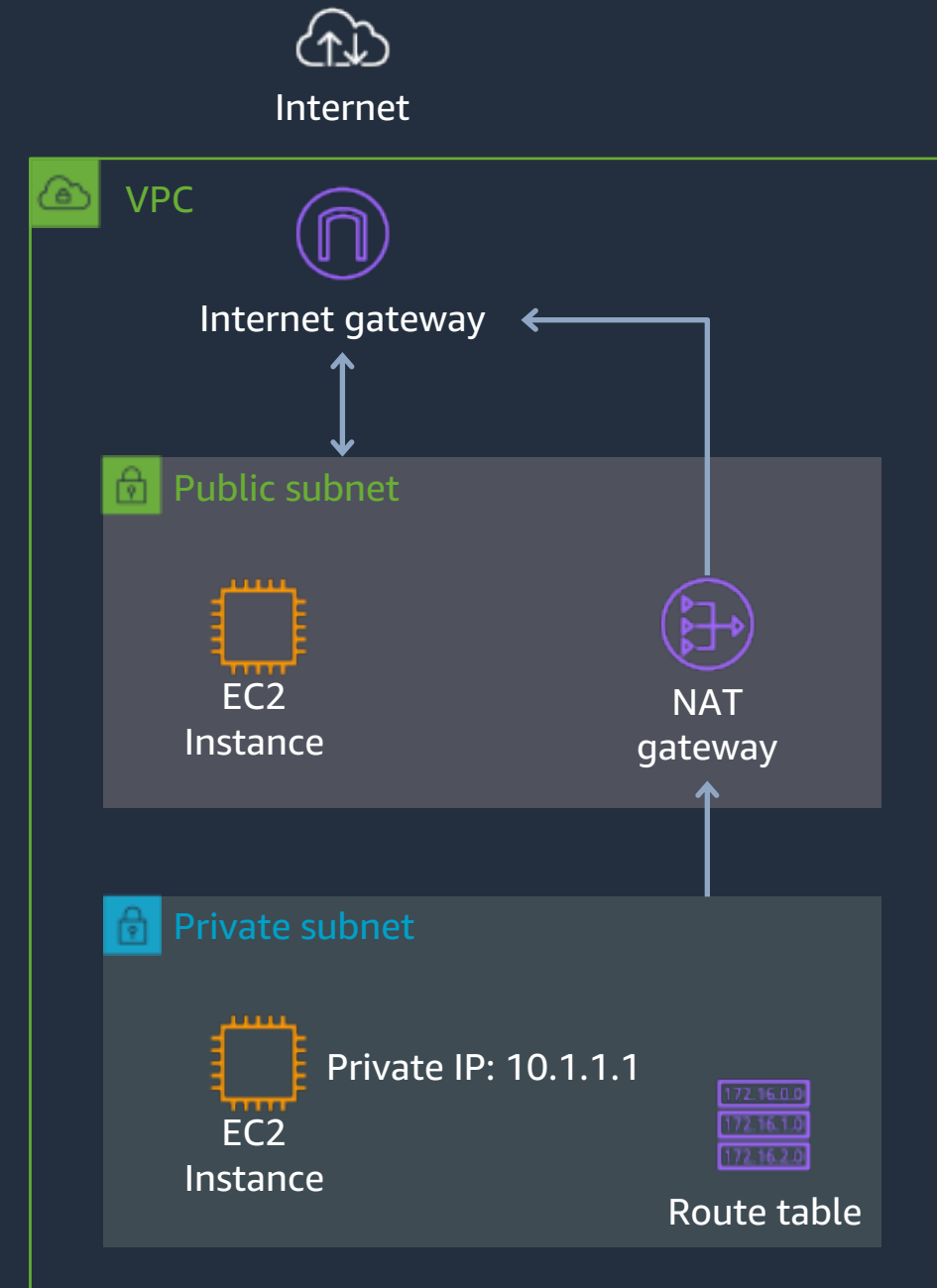
- Static, Public IPv4 address, associated with your AWS account
- Can be associated with an instance or network interface
- Can be remapped to another instance in your account
- Useful for redundancy when Load Balancers are not an option



Can I have outbound only Internet access?

NAT Gateway

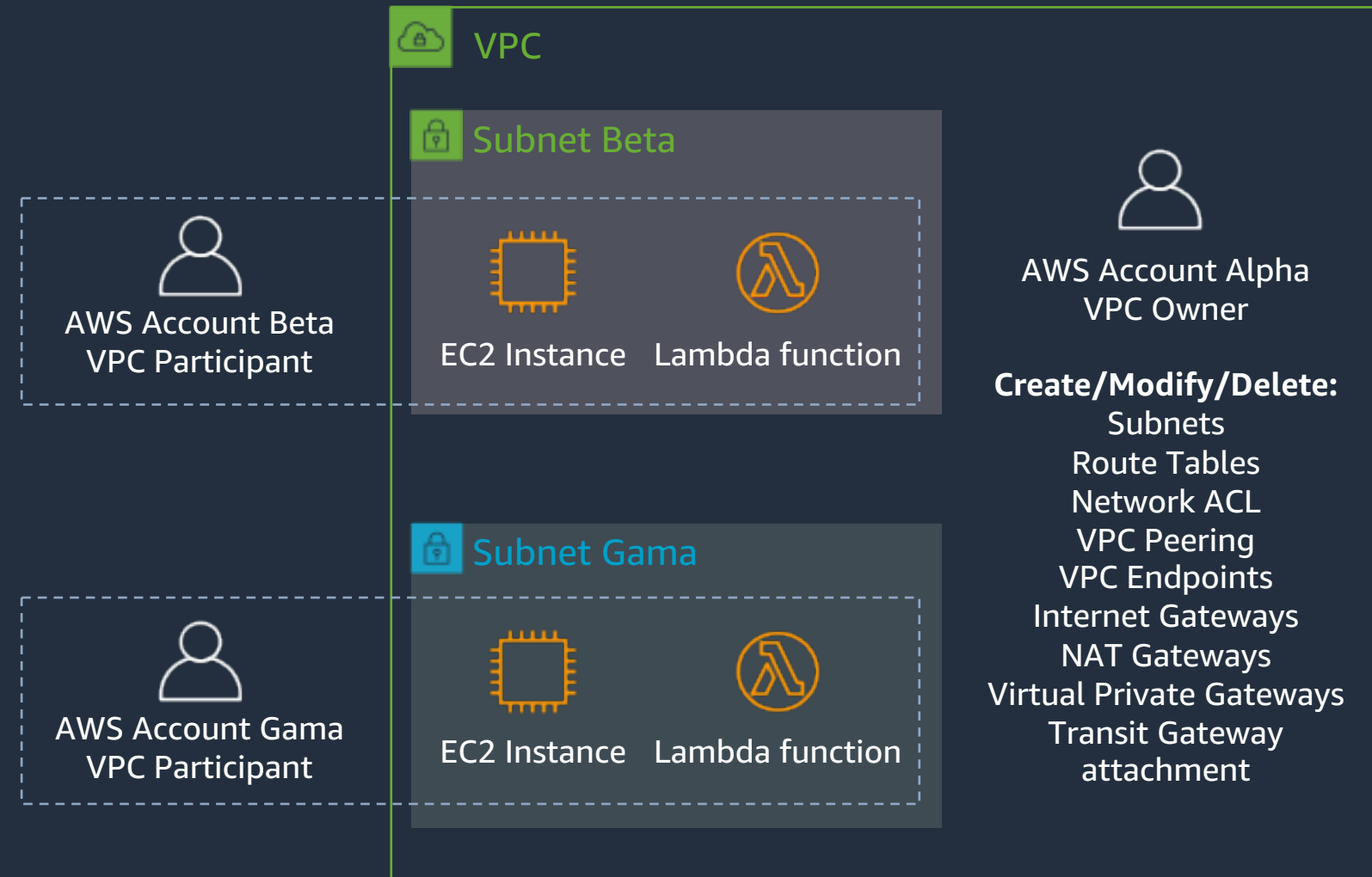
- Enable outbound connection to the internet
- No incoming connection - useful for OS/packages updates, public web services access
- Fully managed by AWS
- Highly available
- Up to 10Gbps bandwidth
- Supports TCP, UDP, and ICMP protocols
- Network ACLs apply to NAT gateway's traffic



Can I have one account owning the VPC, and other using it?

Shared VPC

- VPC Owner can create and edit VPC Components
- VPC Participants can launch resources in their assigned Subnets
- Each participant pays for their own resources and data transfer costs
- Based on AWS Resource Access Manager, under AWS Organizations

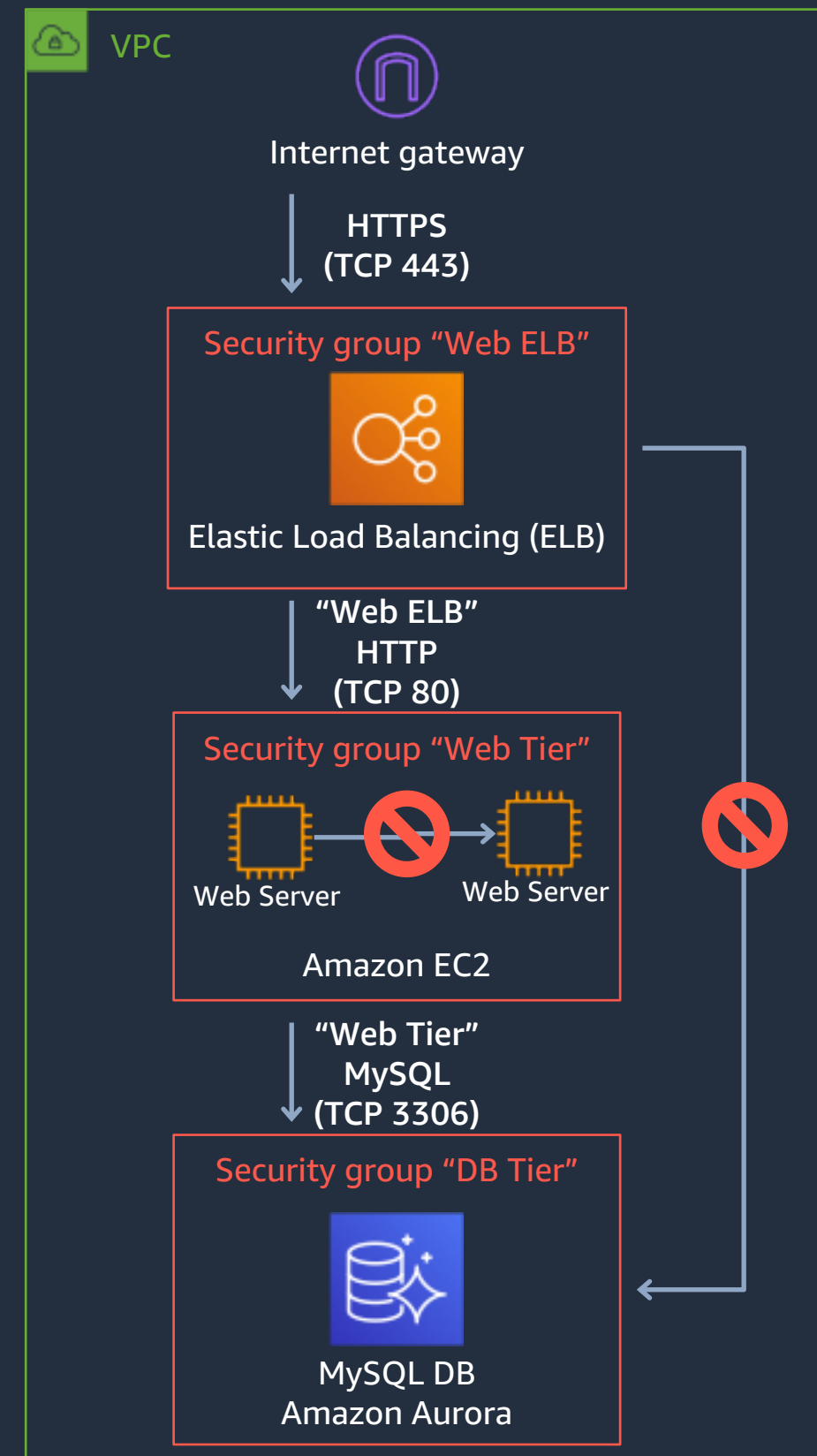


VPC Security

Can I filter traffic reaching my instances?

Security Groups

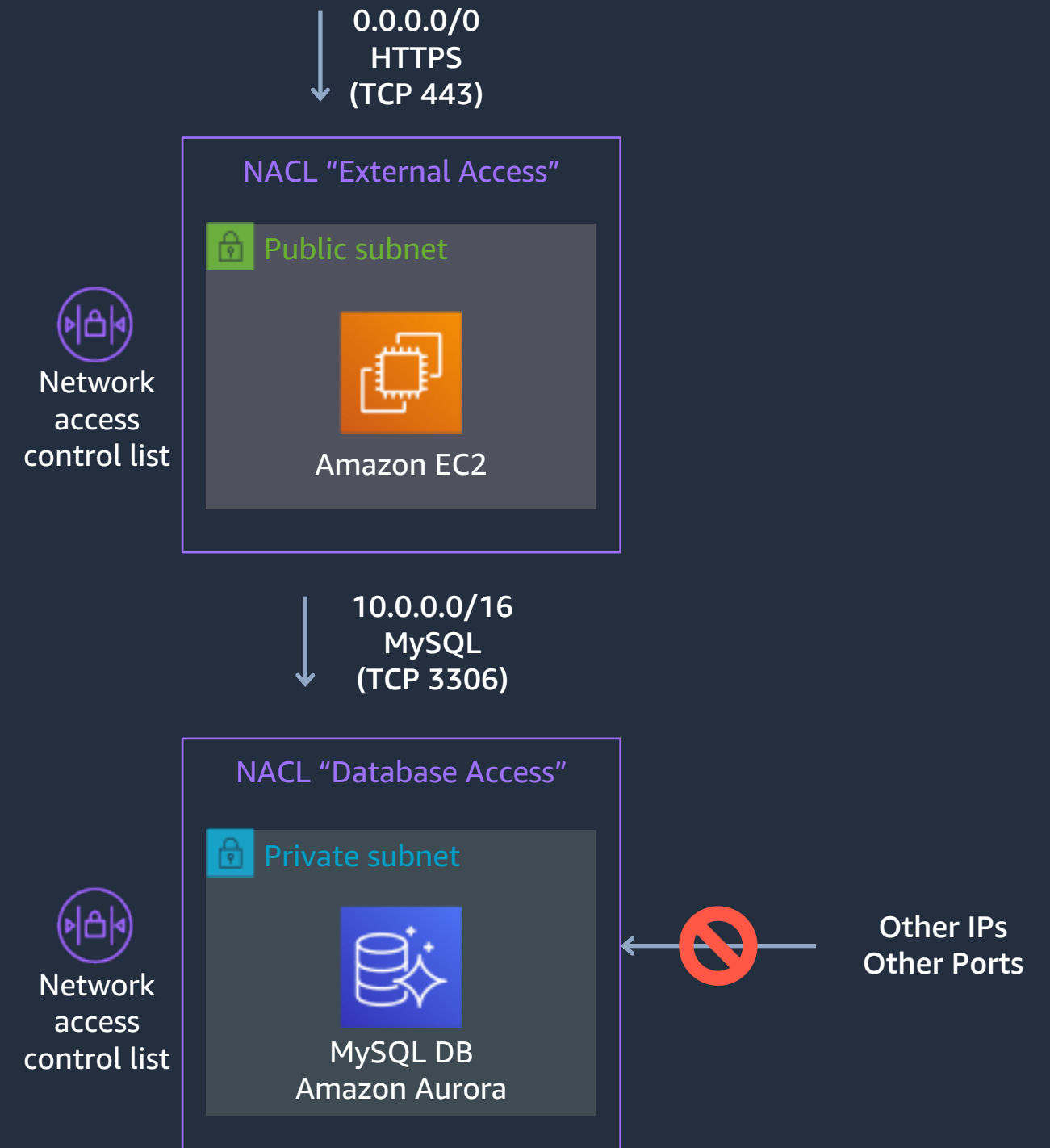
- Virtual stateful firewall
- Inbound and Outbound customer defined rules
- Instance/Interface level inspection
 - Micro segmentation
 - Mandatory, all instances have an associated Security Group
- Can be cross referenced
 - Works across VPC Peering
- Only supports allow rules
 - Implicit deny all at the end



Can I filter traffic on a subnet level?

Network Access Control List

- Inbound and Outbound
- Subnet level inspection
- Optional level of security
- By default, allow all traffic
- Stateless
- IP and TCP/UDP port based
- Supports allow and deny rules
- Deny all at the end

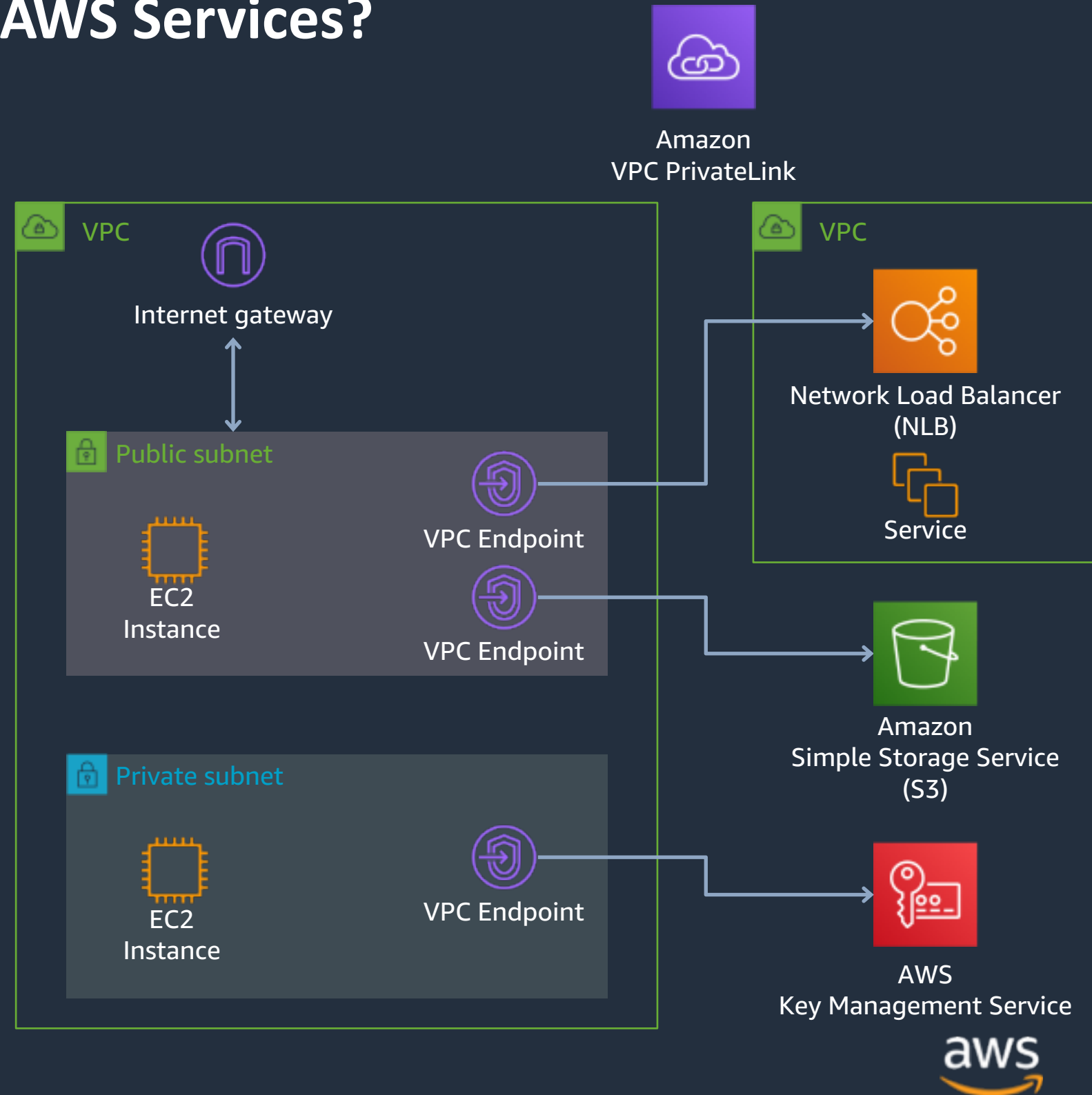


VPC Connectivity Options

How to connect privately to public AWS Services?

VPC Endpoints

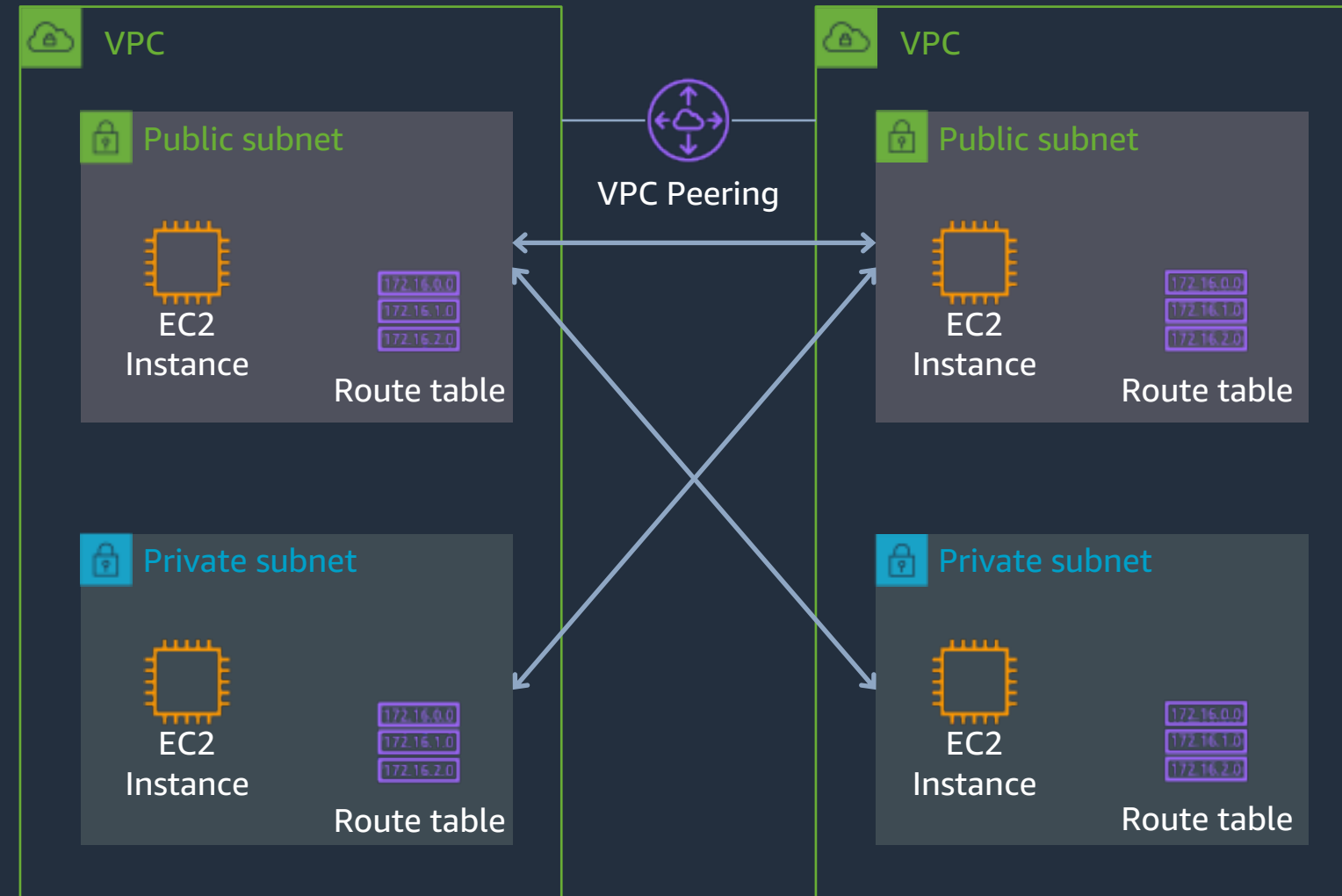
- Connect your VPC to:
 - Supported AWS services
 - VPC endpoint services powered by PrivateLink
- Doesn't require public IPs or Internet connectivity
- Traffic does not leave the AWS network.
- Horizontally scaled, redundant, and highly available
- Robust access control



How to connect directly to other VPCs?

VPC Peering

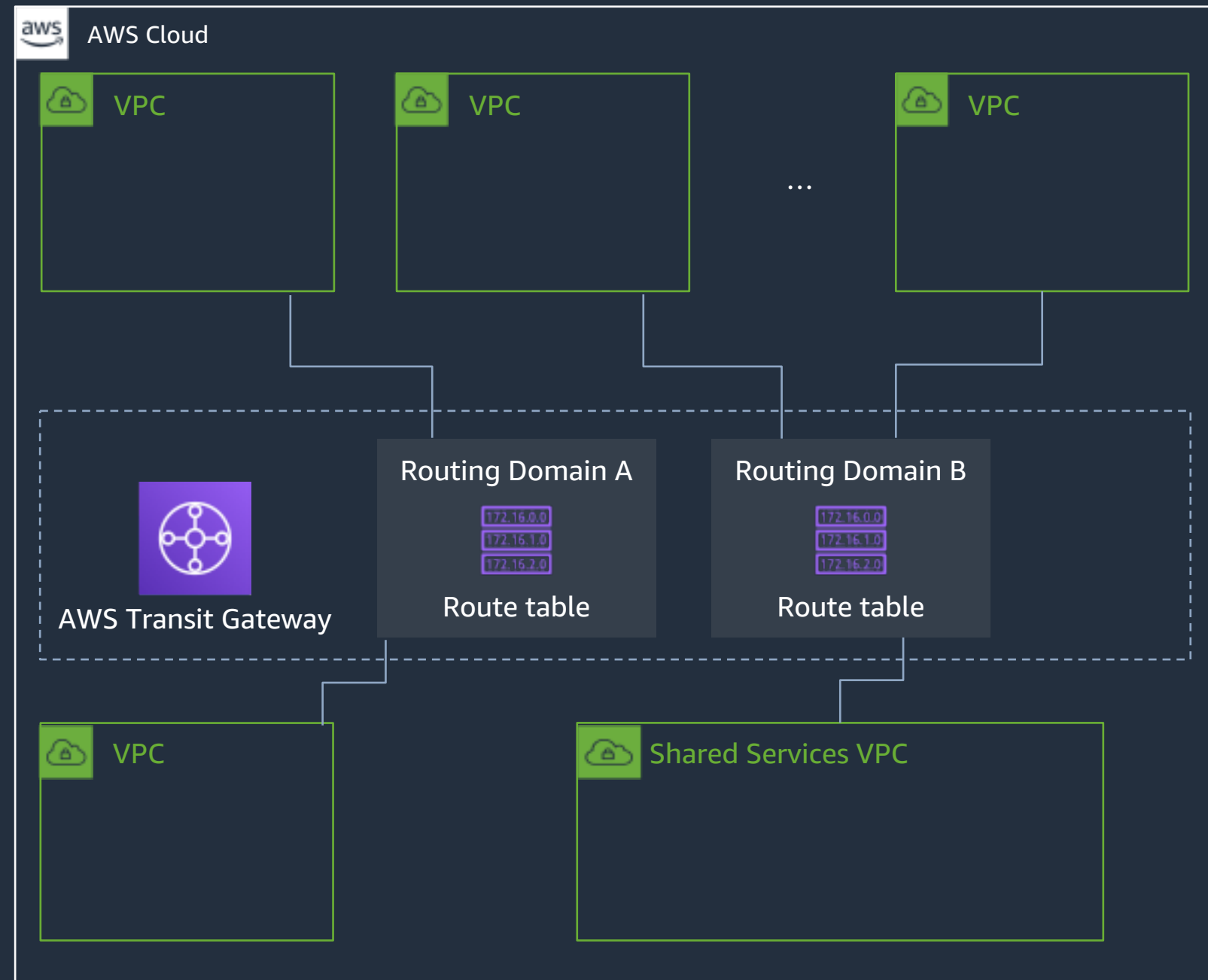
- Scalable and high available
- Inter-account peering
- Same or different AWS Regions
- Bi-directional traffic
- Remote Security groups can be referenced
- Routing policy with Route Tables
 - Not all subnets need to connect to each other
- No transitive routing, requires full-mesh to interconnect multiple VPCs
- No support for overlapping IP addresses



How to connect multiple VPCs together?

AWS Transit Gateway

- Connect thousands of VPC across accounts
- Connect your VPCs and on-premises through a single gateway
- Centralize VPN and AWS Direct Connect connections
- Control segmentations and data flow with Routing Tables
- Hub and Spoke design
- Up to 50 Gbps per VPC connection (burst)

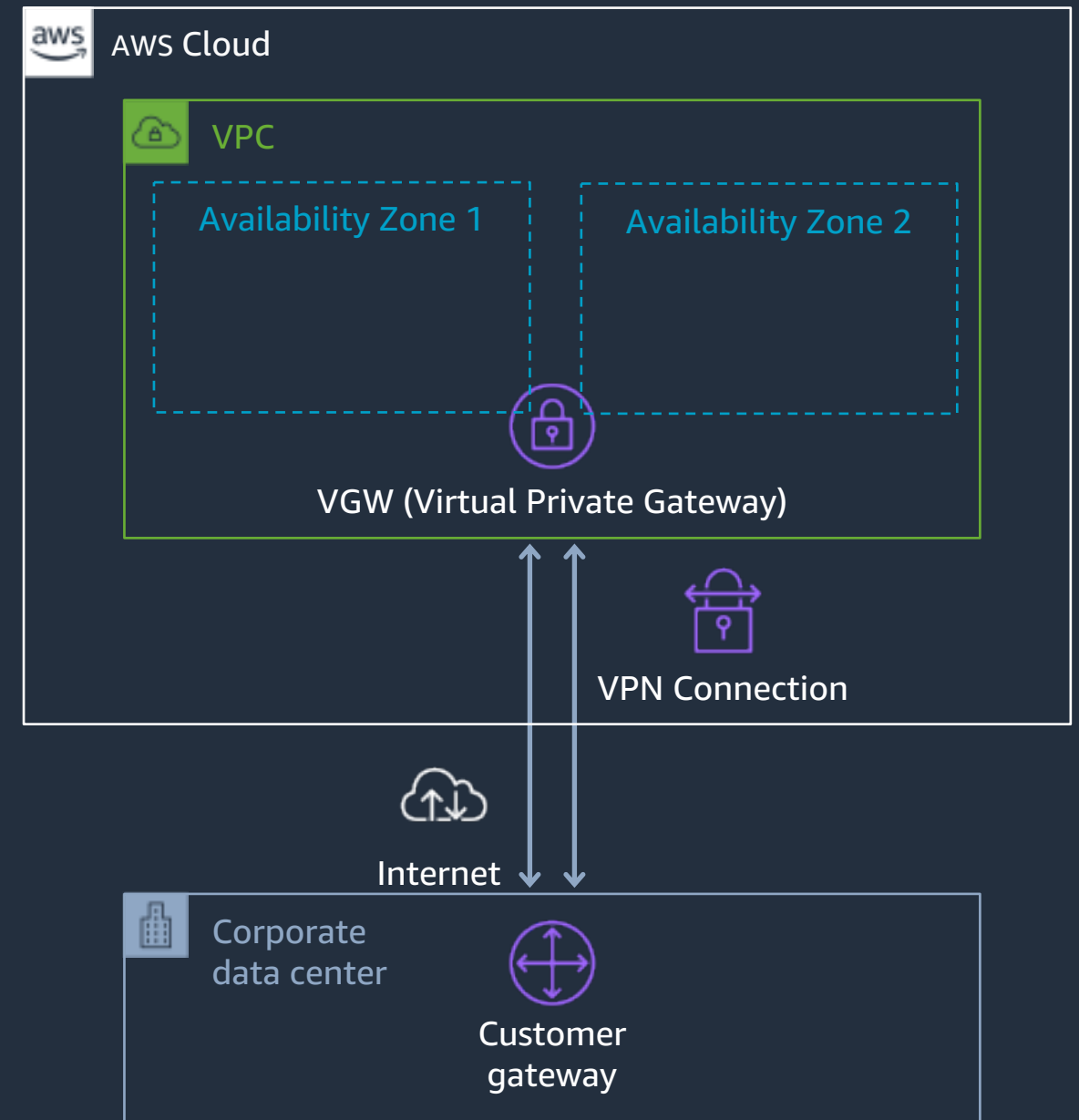


Connect Your Data Center to AWS

How to connect my Datacenter to AWS over the Internet?

AWS Virtual Private Network

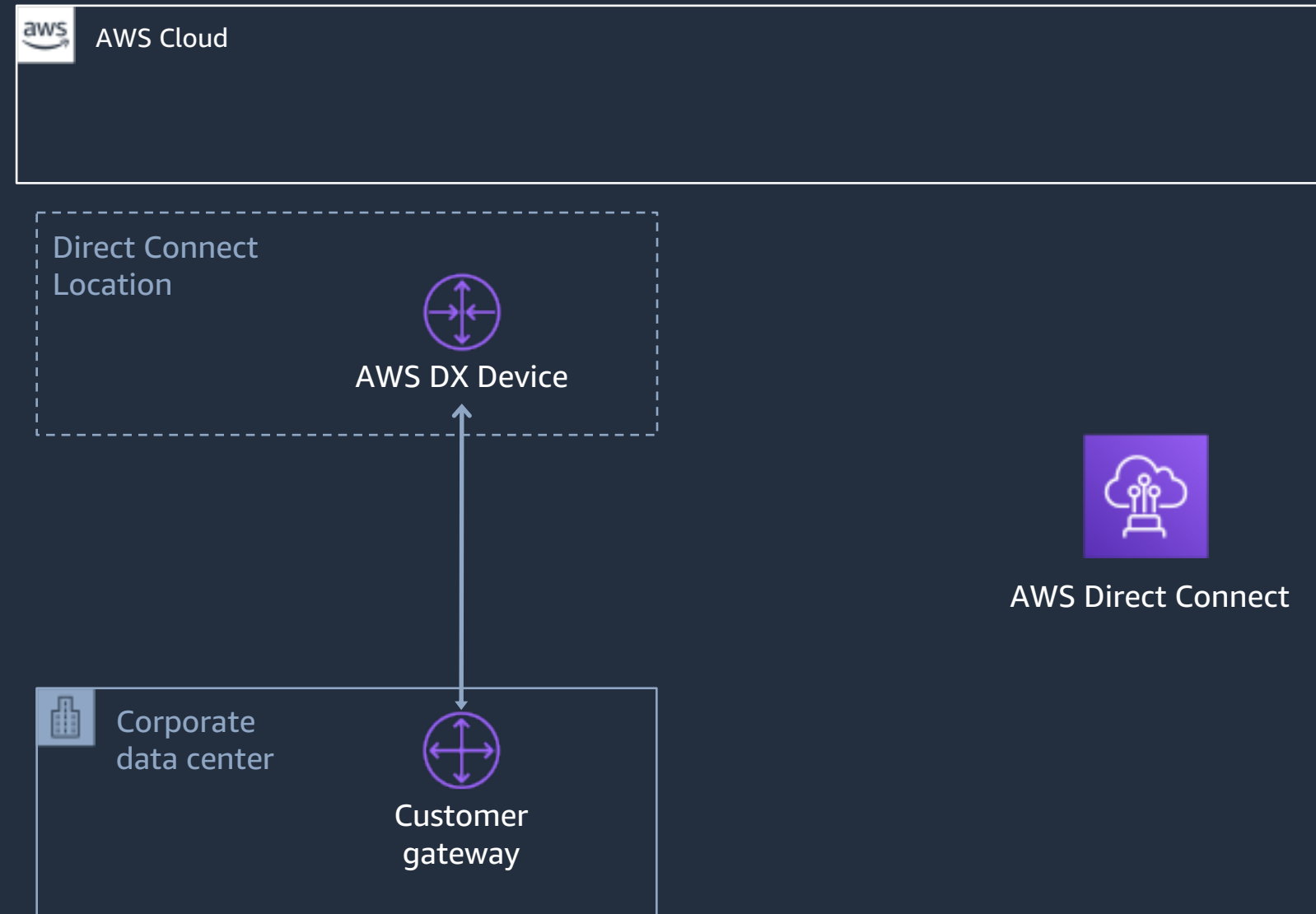
- One VGW (Virtual Private Gateway) per VPC
- Redundant IPSec VPN Tunnels
 - Terminating in different AZs
- IPSec
 - AES 256-bit encryption
 - SHA-2 hashing
- Scalable
- BGP or Static Routing



How to connect my Datacenter to AWS over dedicated circuits?

AWS Direct Connect

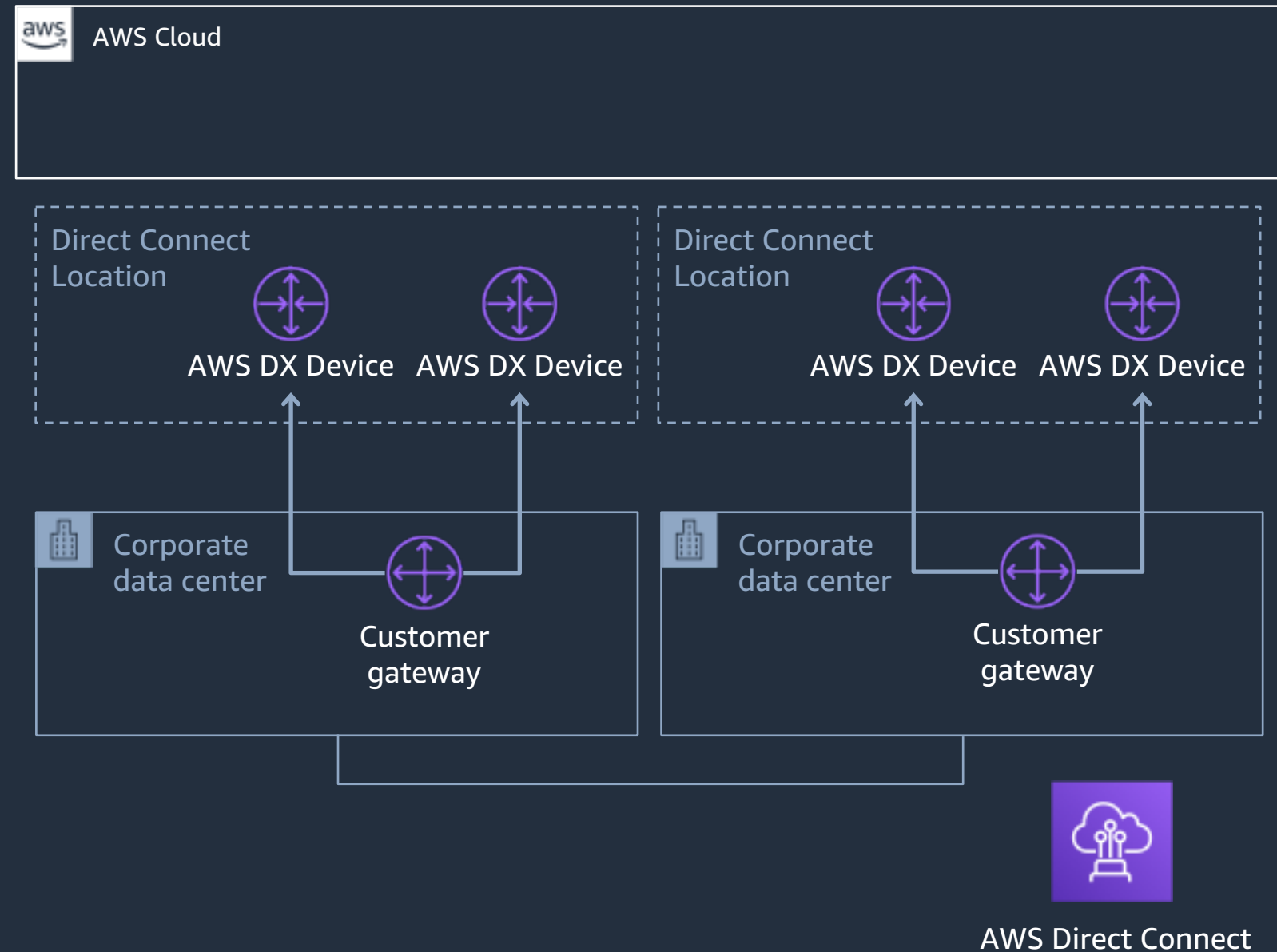
- Dedicated network connection from your premises to AWS
- Dedicated Connection (1/10 Gbps, Multiple VIFs)
- AWS Partner Hosted Connection (50 Mbps to 10 Gbps, Single VIF)
- Consistent Network Performance
- More consistent network experience
- Reduced egress data charges
- Connect to 90+ Direct Connection Locations across the globe



How to add redundancy to my dedicated circuits?

AWS Direct Connect

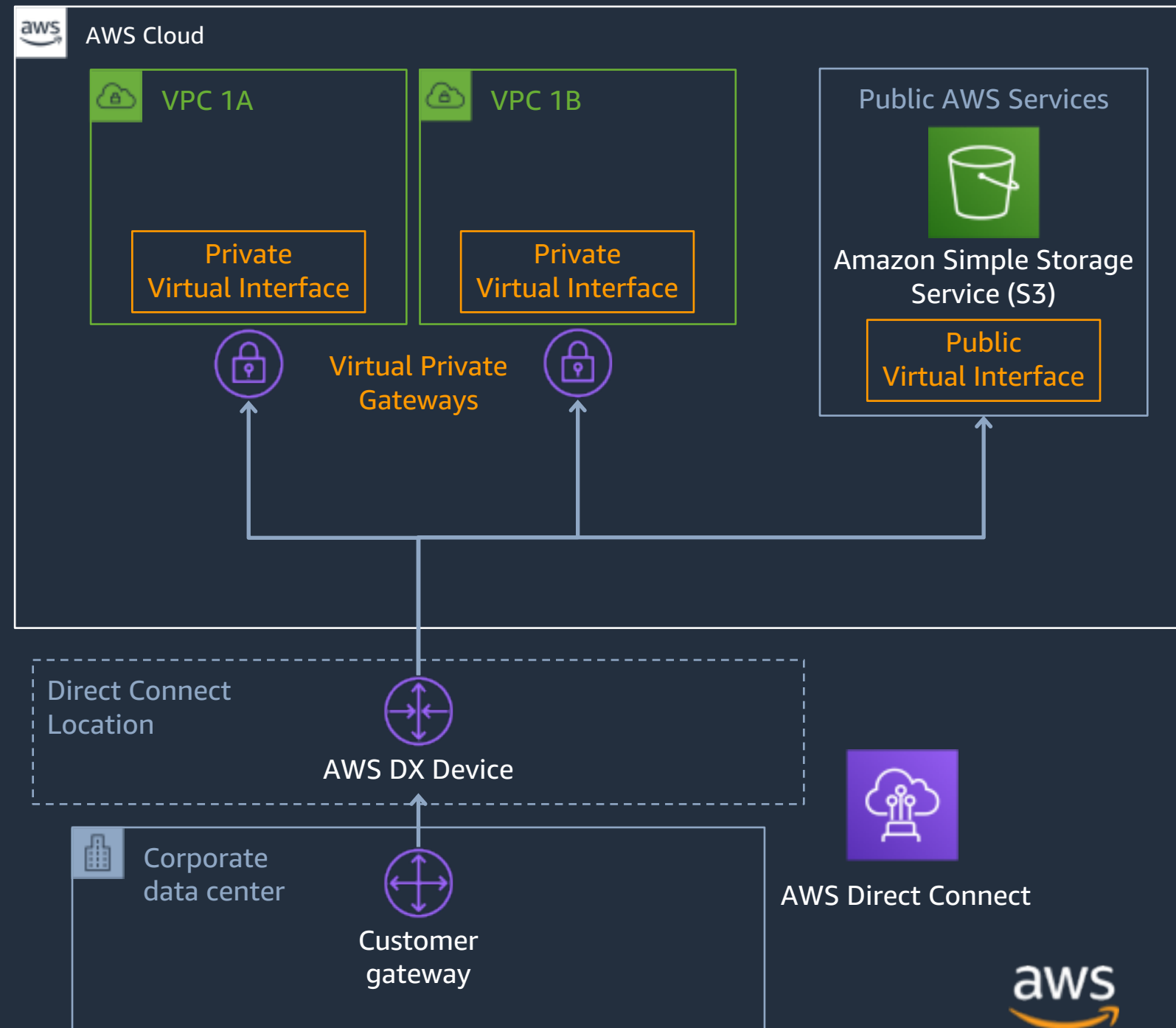
- For redundancy, DX can be deployed with single or multiples:
 - Circuits
 - Providers
 - Customer Gateways
 - Direct Connect Locations
 - Customer data centers
- BGP Routing for redundancy
- AWS VPN can also be used as backup path



How to access my VPCs or AWS Public Services over my DX?

AWS Direct Connect

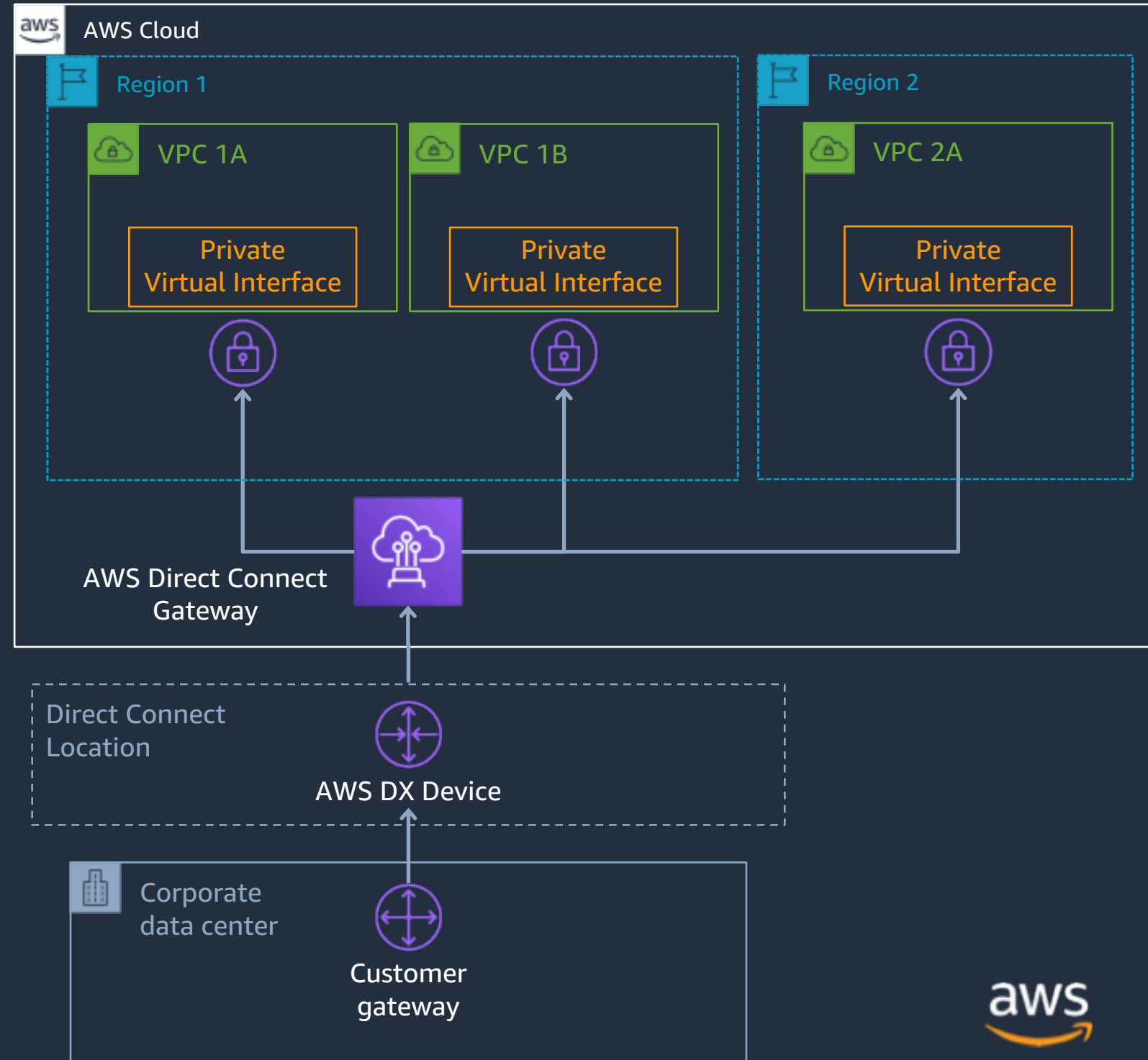
- VIFs: Virtual Interface
- Private VIFs
 - Access to VPC IP address
- Public VIFs
 - Access to AWS Public IP address space



How to connect to multiple AWS Regions/Accounts over DX?

AWS Direct Connect Gateway

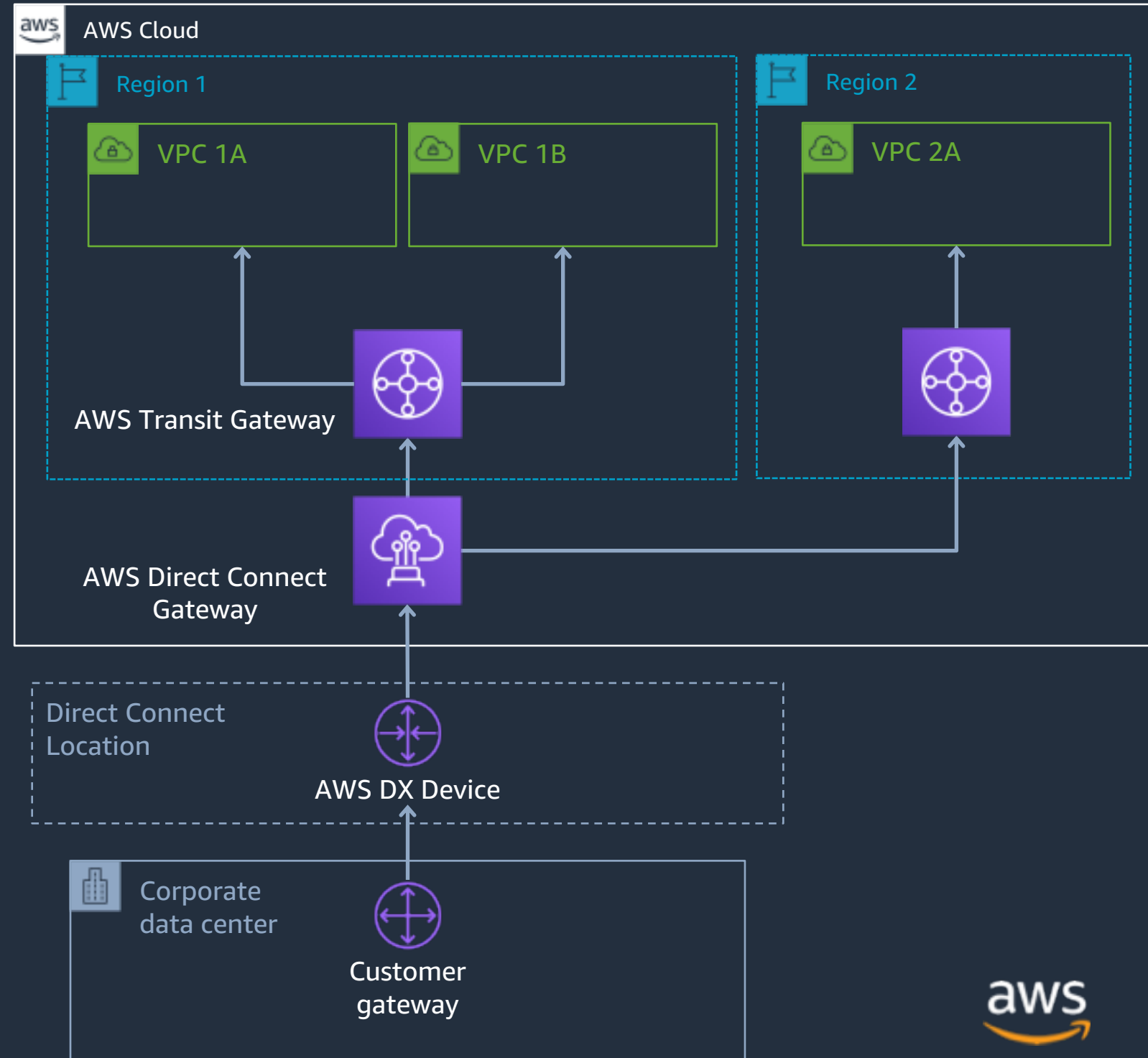
- Global resource
- Connect to multiple VPCs
 - Regions
 - Accounts (same Payer ID)
- Enables traffic flow from the VPC to the DX connection
 - For VPC to VPC Traffic, consider using AWS Transit Gateway



How to connect at scale across accounts/Regions?

AWS DX Gateway + AWS Transit Gateway

- Transit VIF
 - Connects to a AWS Transit Gateway
- Simplify your network architecture and management overhead
- Create a hub-and-spoke model that spans multiple
 - VPCs
 - Regions
 - AWS accounts

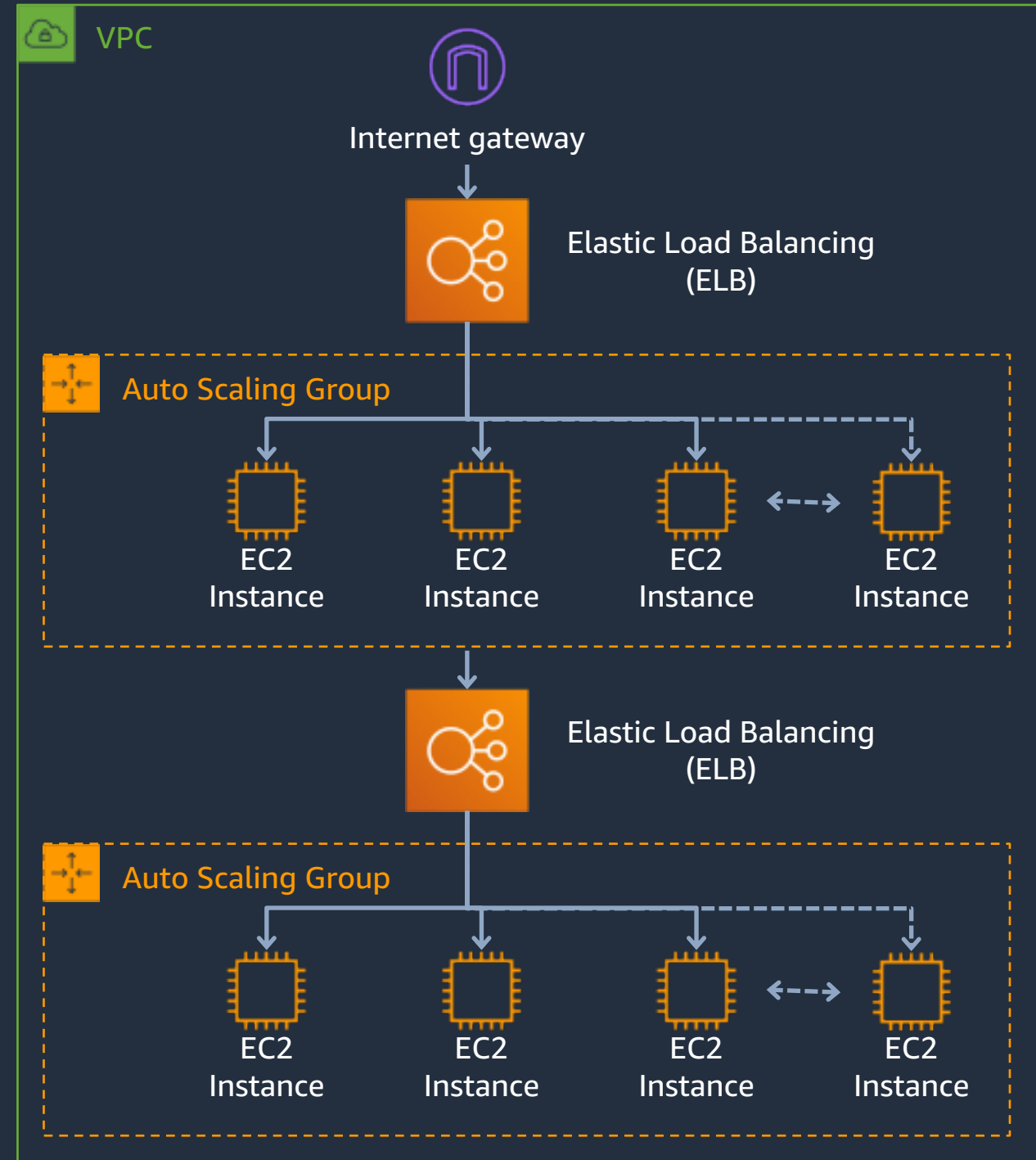


Traffic Distribution

How to scale my app horizontally inside my VPC?

Elastic Load Balancing

- Distributes incoming application or network traffic across multiple targets
 - EC2 instances
 - Containers
 - IP address
- Multiple Availability Zones
- Scales automatically
- Auto Scaling Groups can add or remove instances as required
 - Automatically register to the Load Balancer



Elastic Load Balancing

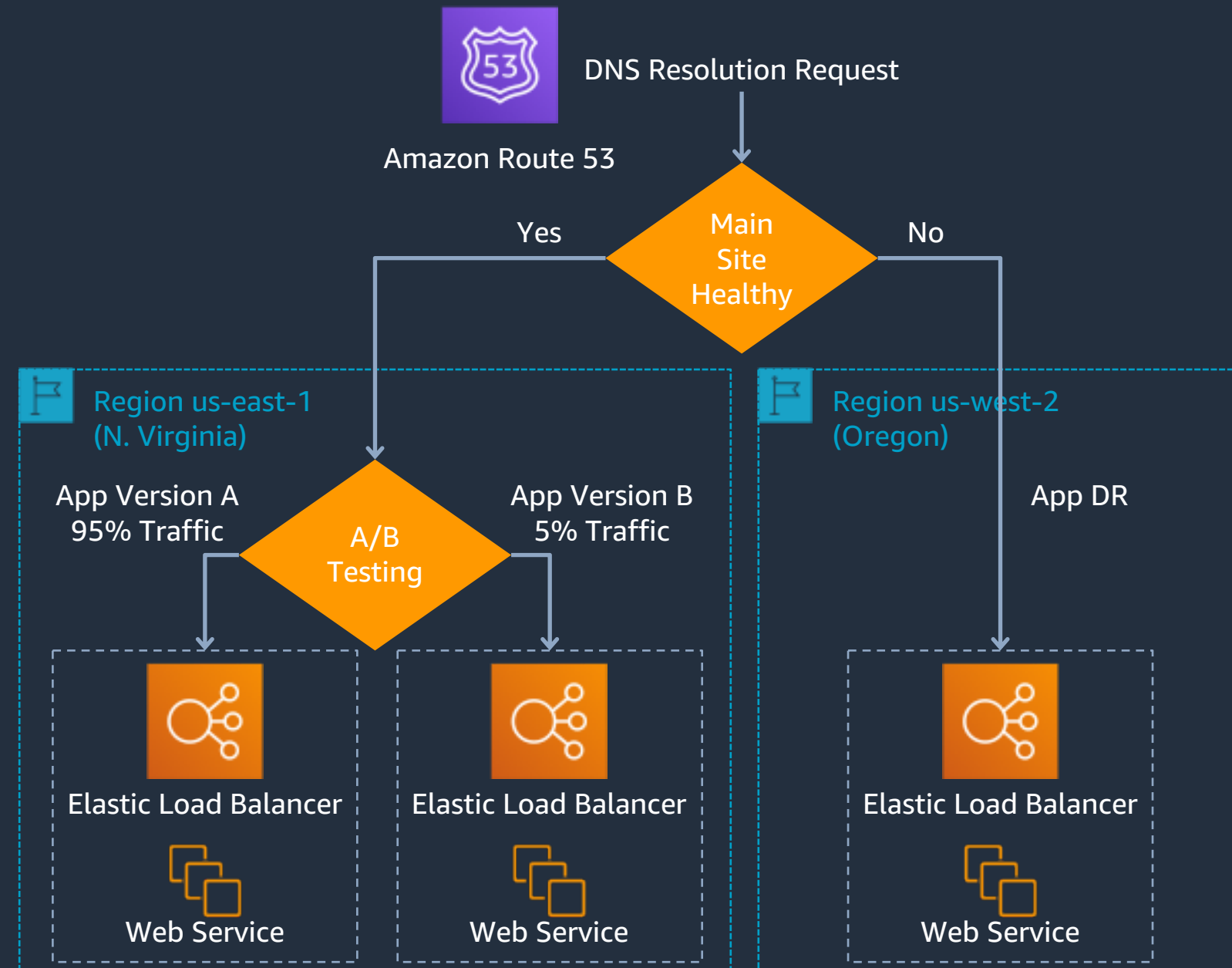
Features Comparison

Feature	Application Load Balancer	Network Load Balancer
Protocols	HTTP, HTTPS	TCP
Platforms	VPC	VPC
Health checks	√	√
CloudWatch metrics	√	√
Logging	√	√
Path-Based Routing	√	
Host-Based Routing	√	
Native HTTP/2	√	
Configurable idle connection timeout	√	
SSL offloading	√	
Server Name Indication (SNI)	√	
Sticky sessions	√	
Back-end server encryption	√	
Static IP		√
Elastic IP address		√
Preserve Source IP address		√

How to solve my Domain Names to IP Address?

Amazon Route 53

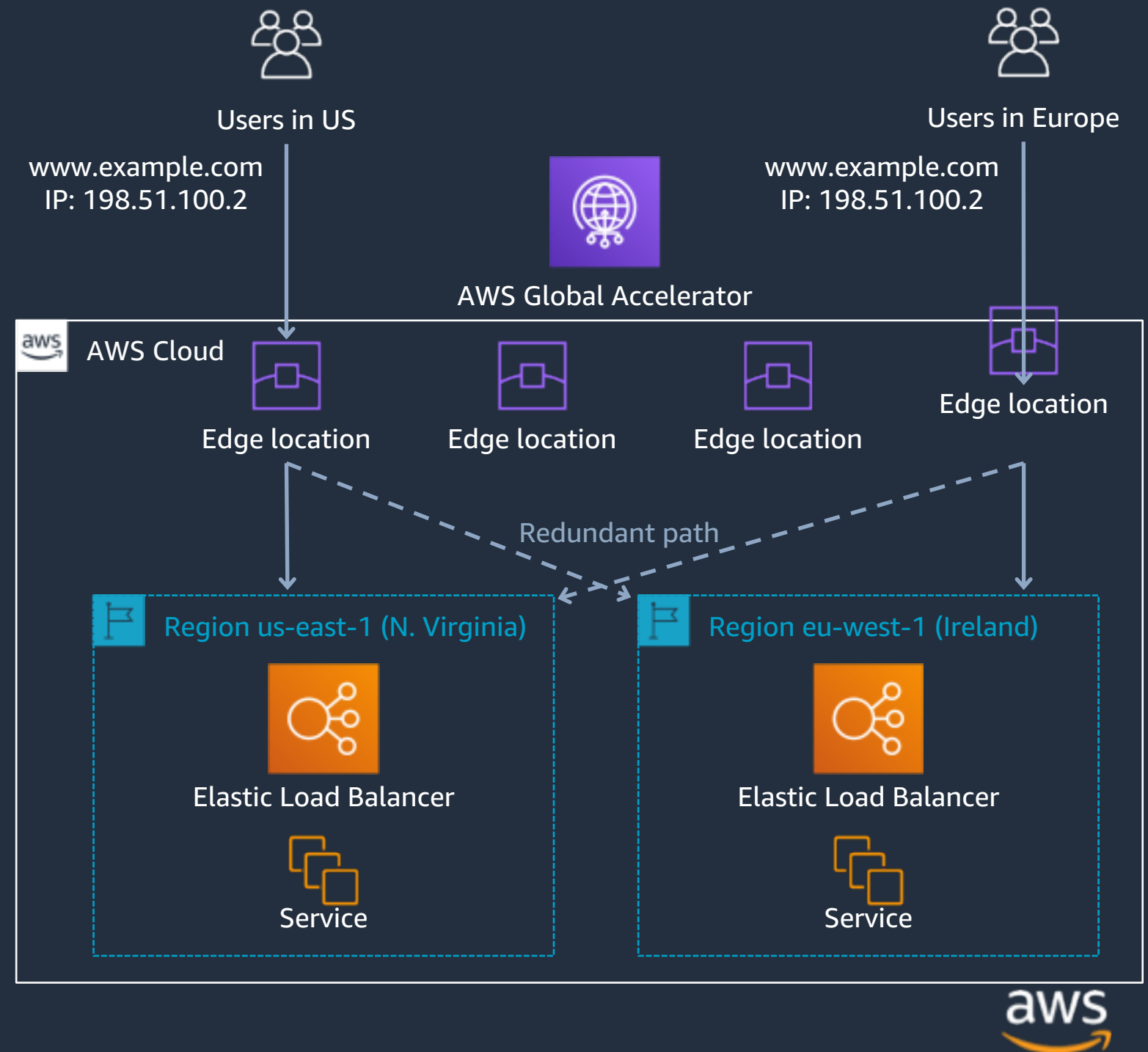
- AWS DNS service
- Domain Registration
- Domain name resolution
- 100% availability SLA
- Health Checks
- DNS Failover
- Latency Based Routing
- Geo Based Routing
- Weighted Round Robin
- Private DNS for VPC



Can I improve availability and performance of my global services?

AWS Global Accelerator

- Uses AWS Global Network from Edge to Region
- Client traffic ingresses via closest available Edge location
- Route client to closest healthy endpoint
- No DNS switchover required, same IP address globally
 - Static IP Anycast



Questions?