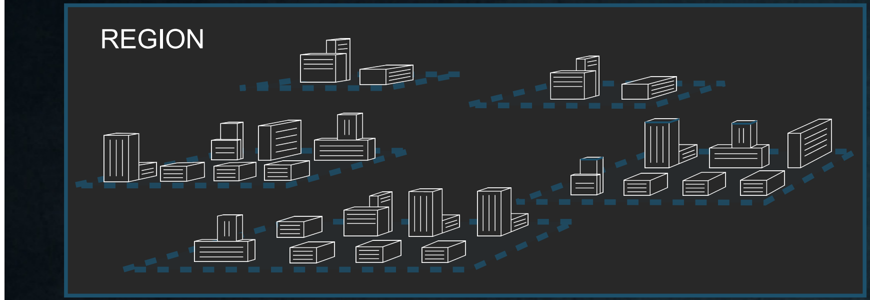
Networking in AWS

Agenda

- The VPC construct
- Connecting VPC to the internet
- Securing resources in the VPC
- Load Balancing incoming traffic
- Connecting multiple VPCs to each other
- Connecting to on-premises datacenters
- Routing traffic

Amazon VPC

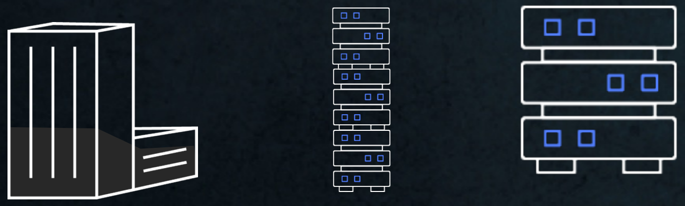
Amazon Virtual Private Cloud (VPC) overview

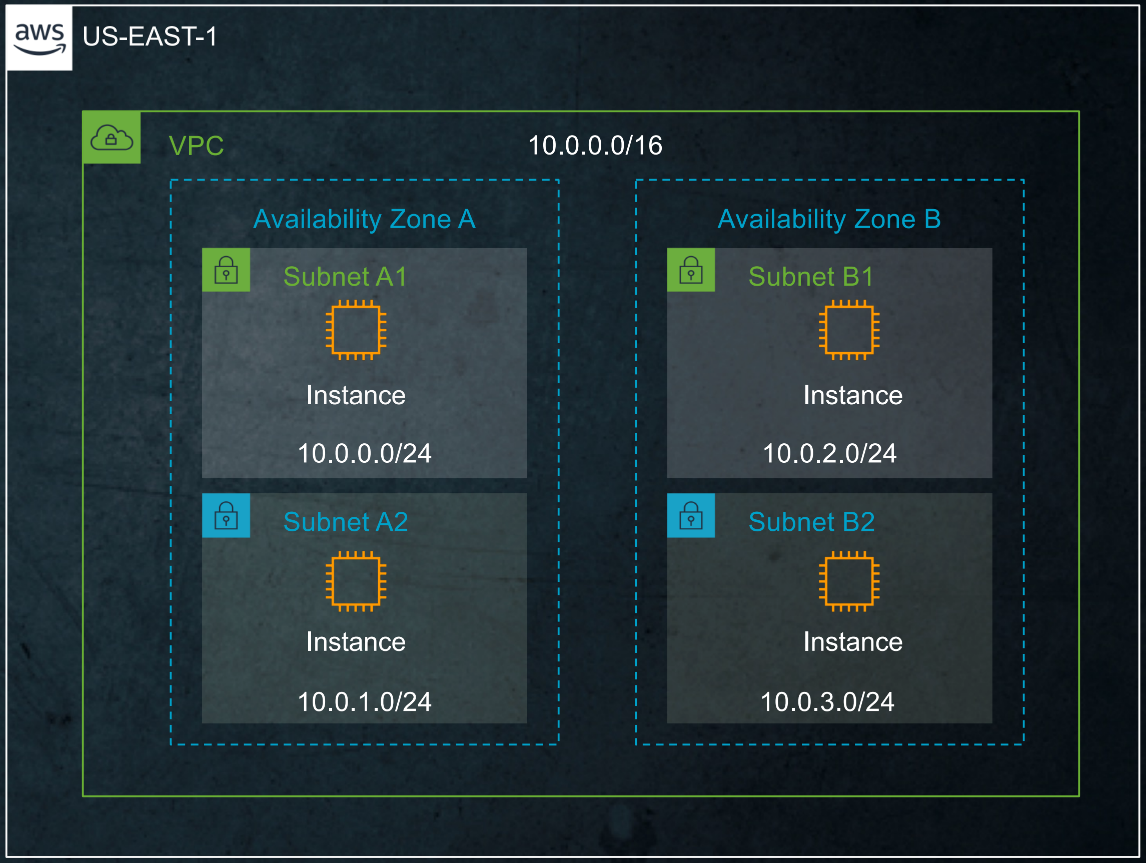


REGION

AVAILABILITY ZONE

DATA CENTER, RACK, HOST





US-EAST-1

VPC

10.0.0.0/16

Availability Zone A

Subnet A1

Instance

10.0.0.0/24

Subnet A2

Instance

10.0.1.0/24

Availability Zone B

Subnet B1

Instance

10.0.2.0/24

Subnet B2

Instance

10.0.3.0/24

VPC IP addressing

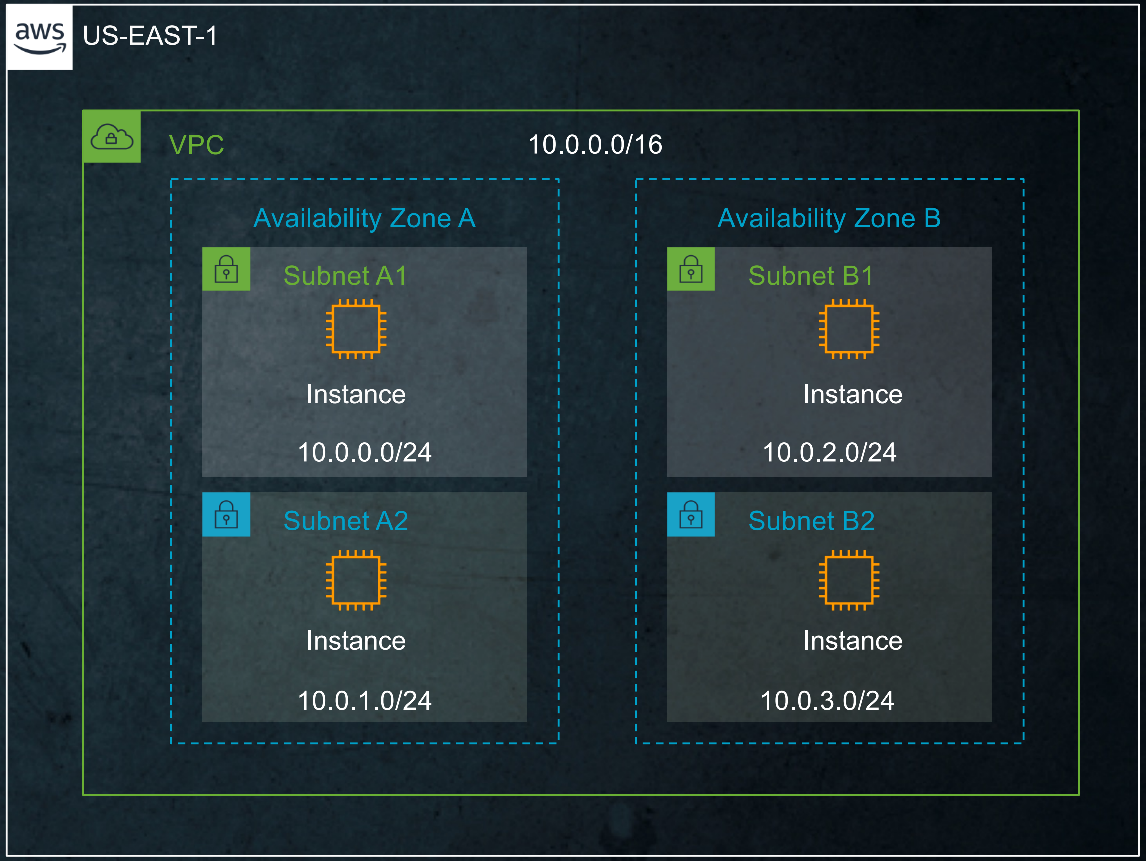
- Internal to VPC
    - VPCs can be between /16 and /28
    - VPCs support subnetting
    - VPC CIDRs cannot be modified once created
    - Additional CIDRs can be added to a VPC
- External
    - Support IPv4 and IPv6
    - Support bringing your own IP space

VPC IP addressing considerations

- Plan your IP space before creating it
  - Overlapping IP spaces = future headache
  - Consider using multiple VPCs
  - Consider future AWS region expansion
  - Consider future connectivity to corporate networks
  - Consider subnet design

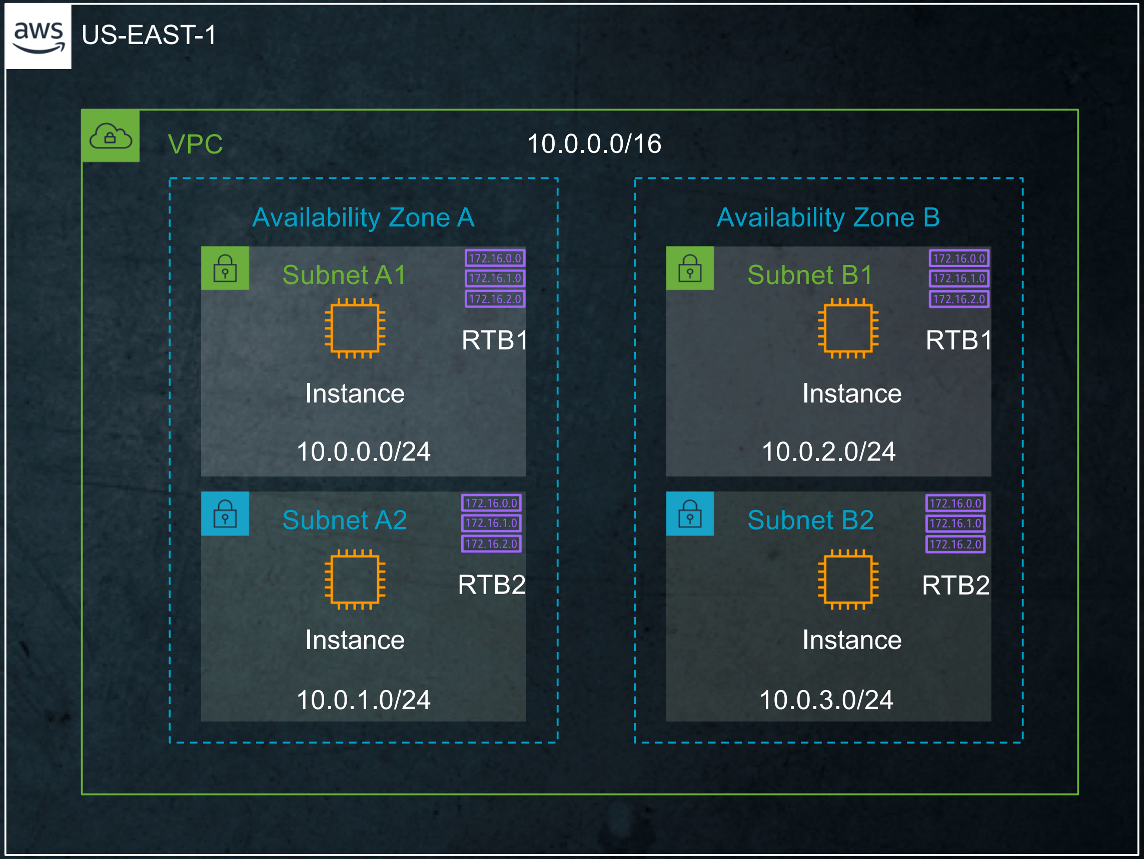
Subnets

- VPCs span a region
- Subnets are allocated as a subset of the VPC CIDR range and span a specific AZ
- You can have multiple subnets in each VPC and each AZ
- Implicit route between all subnets within a VPC



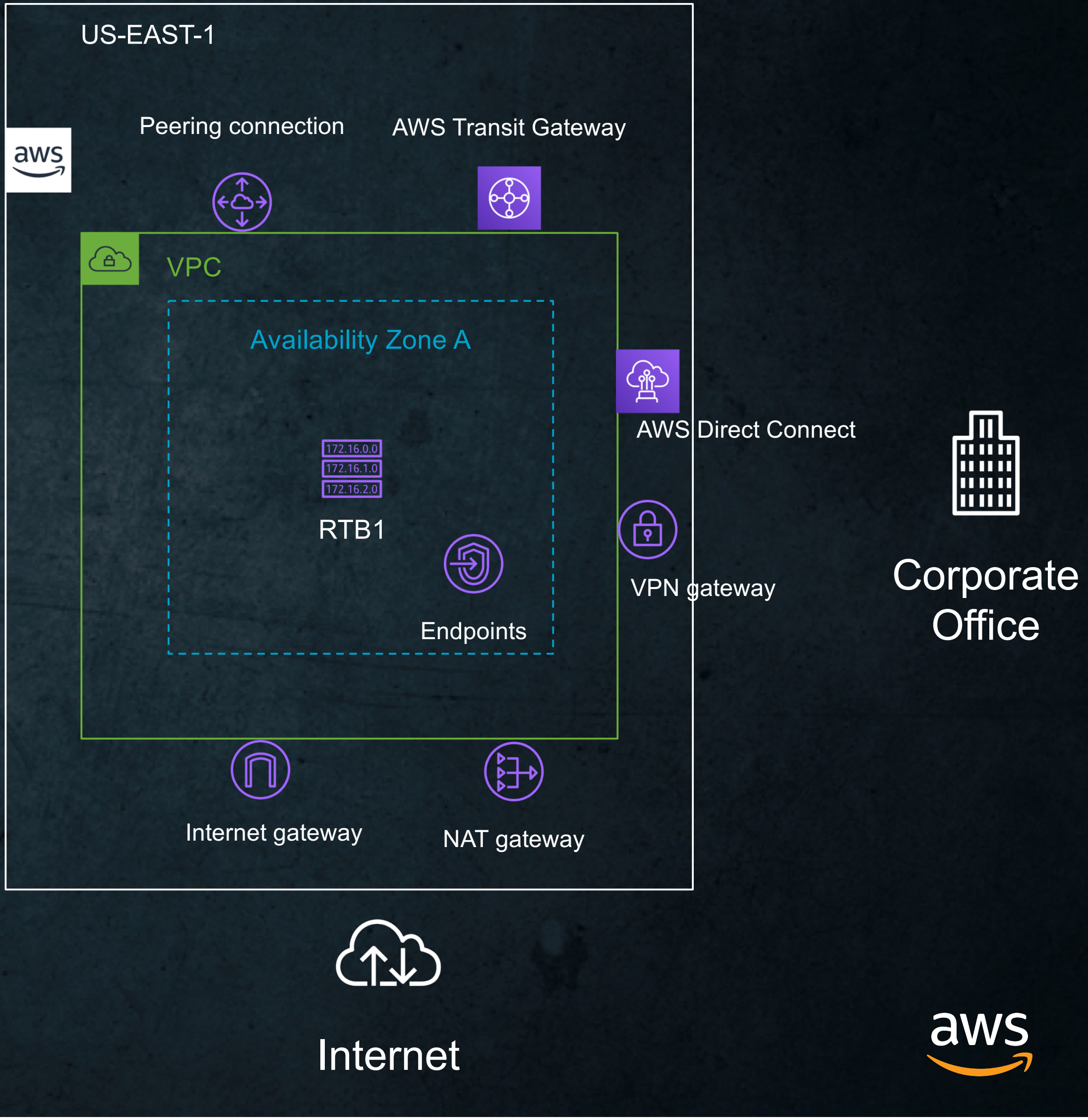
Routing tables

- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets



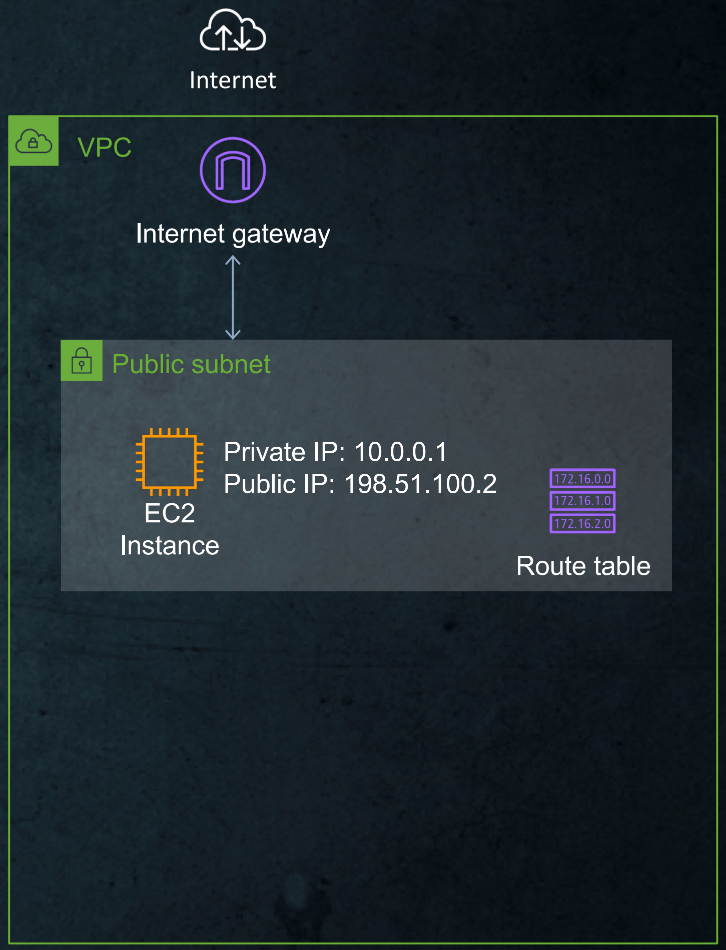
Routing

- Route Tables direct traffic towards:
  - Internet / NAT Gateway
  - VPC Endpoints
  - VPC Peering / AWS Transit Gateway
  - VPN Gateway / Direct Connect
- Subnets are referred to as “Public Subnets” when there is a route to an Internet Gateway



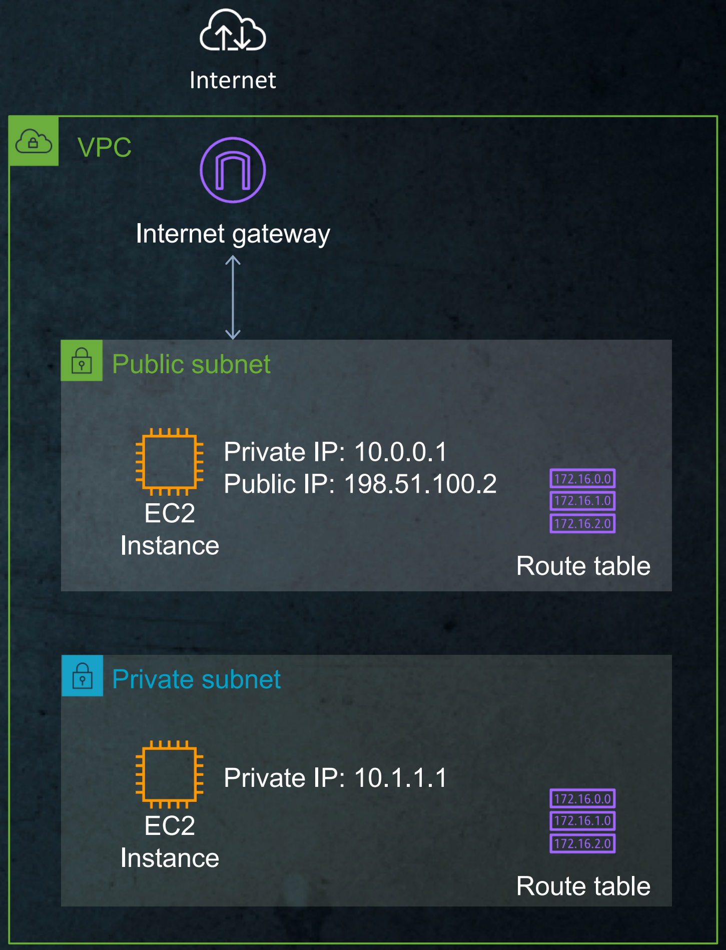
VPC to internet: Internet Gateway

- 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



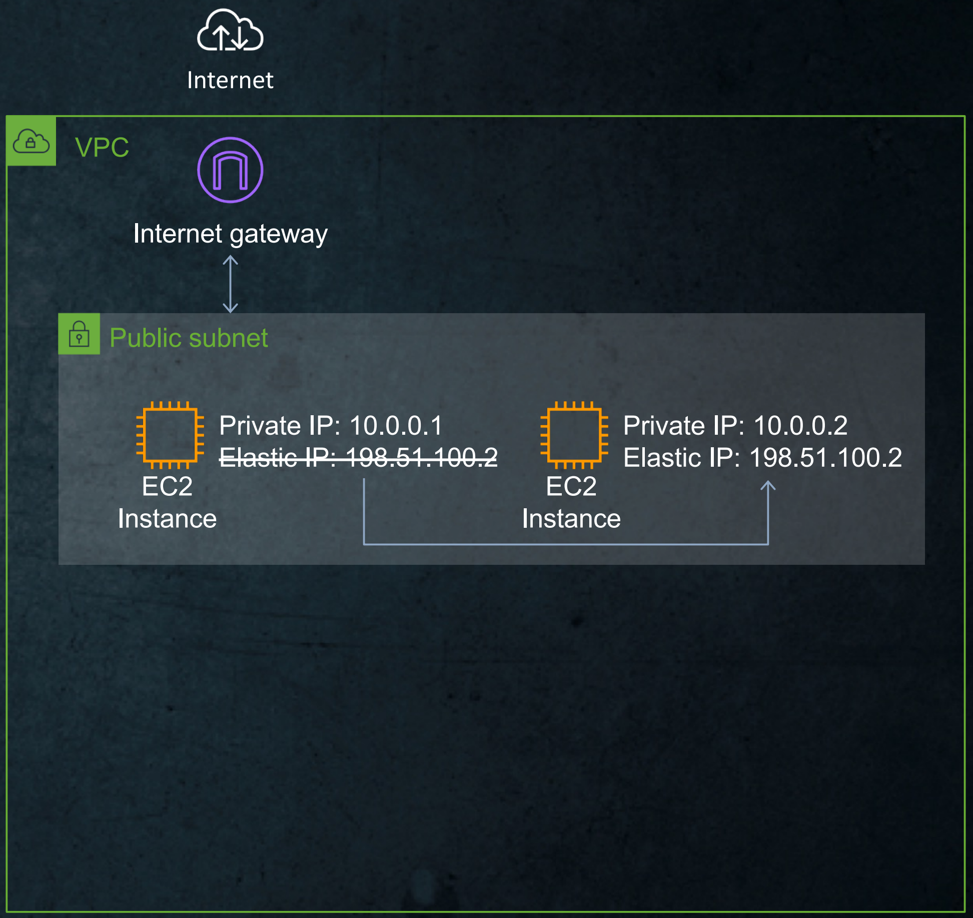
VPC to internet: Internet Gateway

- Horizontally scaled, redundant, highly available VPC component
- Connect your VPC Subnets to the Internet
- Must be referenced on the Route Table
- Performs 1:1 NAT between Public and Private IP Addresses



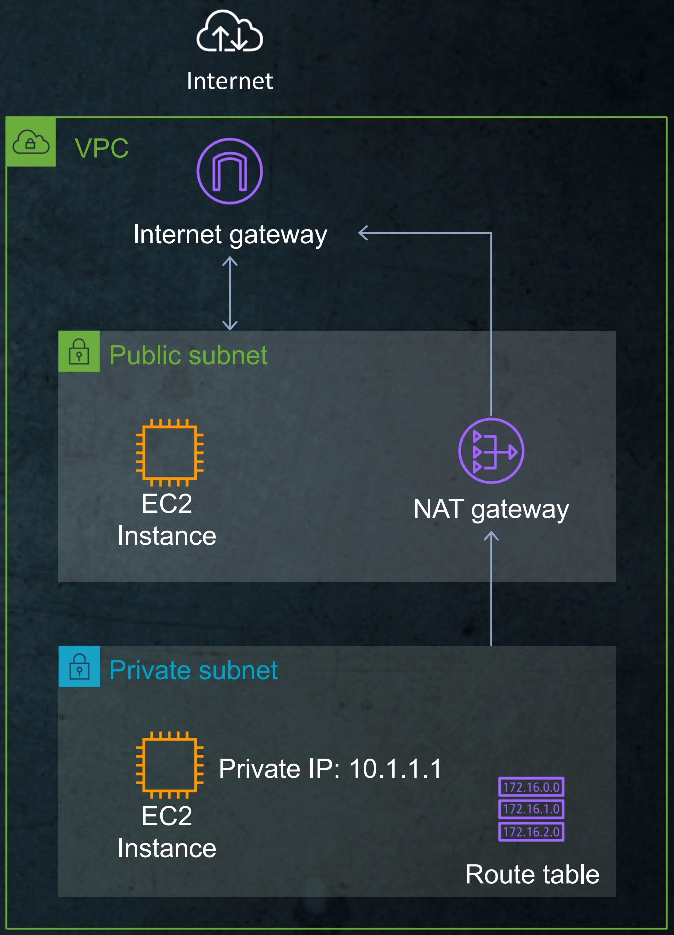
Public IP addressing: Elastic IP Address

- Static, Public IPv4 address, associated with your AWS account
- Dynamically assigned
- Specific to a region
- 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



Outbound only traffic: NAT Gateway

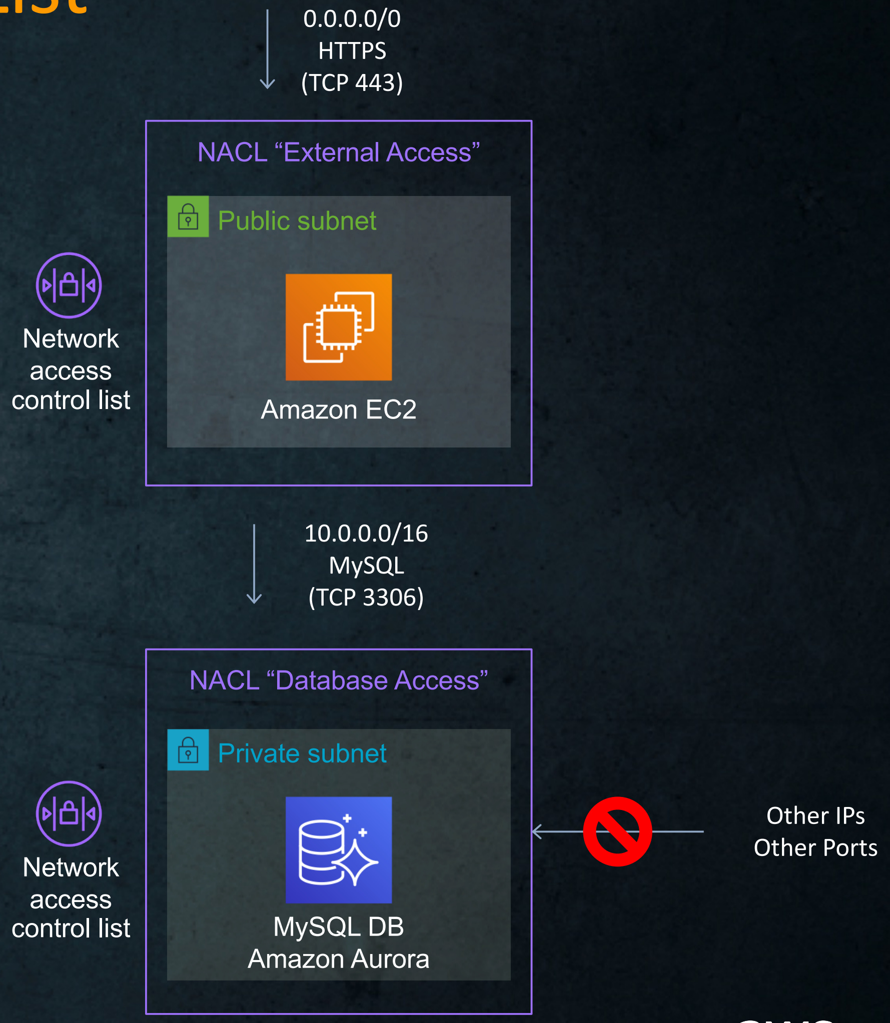
- Enable outbound connection to the internet
- No incoming connection - useful for OS/packages updates, public web services access
- Fully managed by AWS
- Highly available
- Up to 45Gbps aggregate bandwidth
- Supports TCP, UDP, and ICMP protocols
- Network ACLs apply to NAT gateway traffic



VPC security

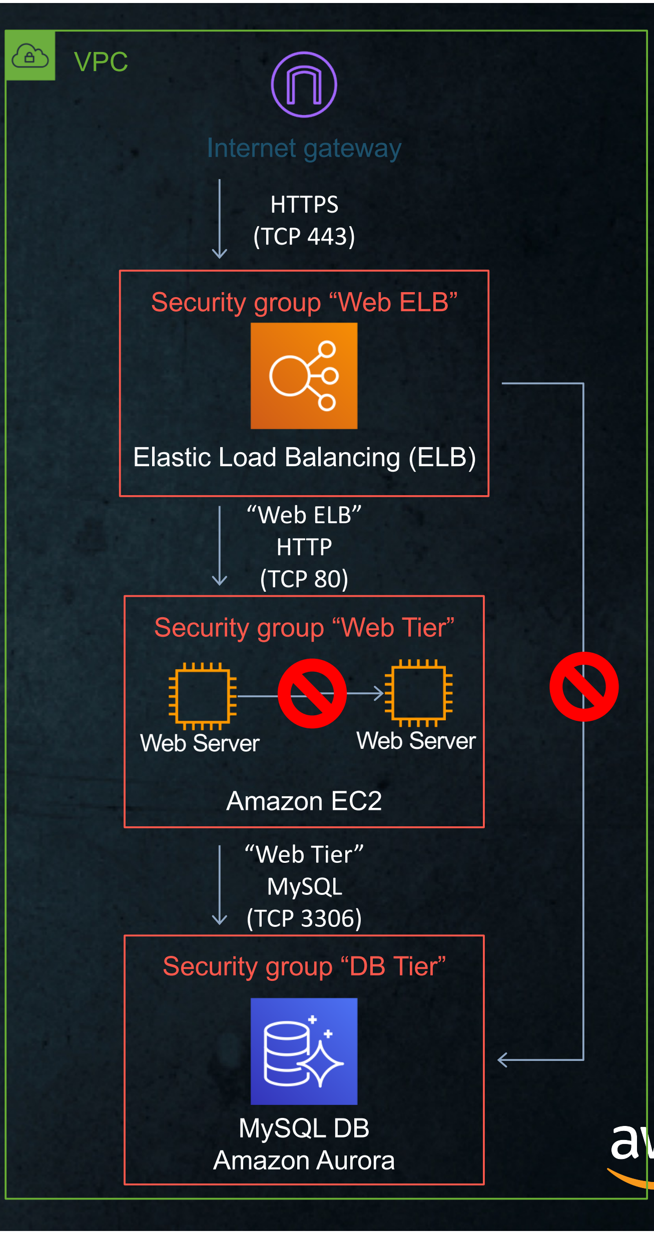
IP FW: Network Access Control List

- 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



Resource FW: Security Groups

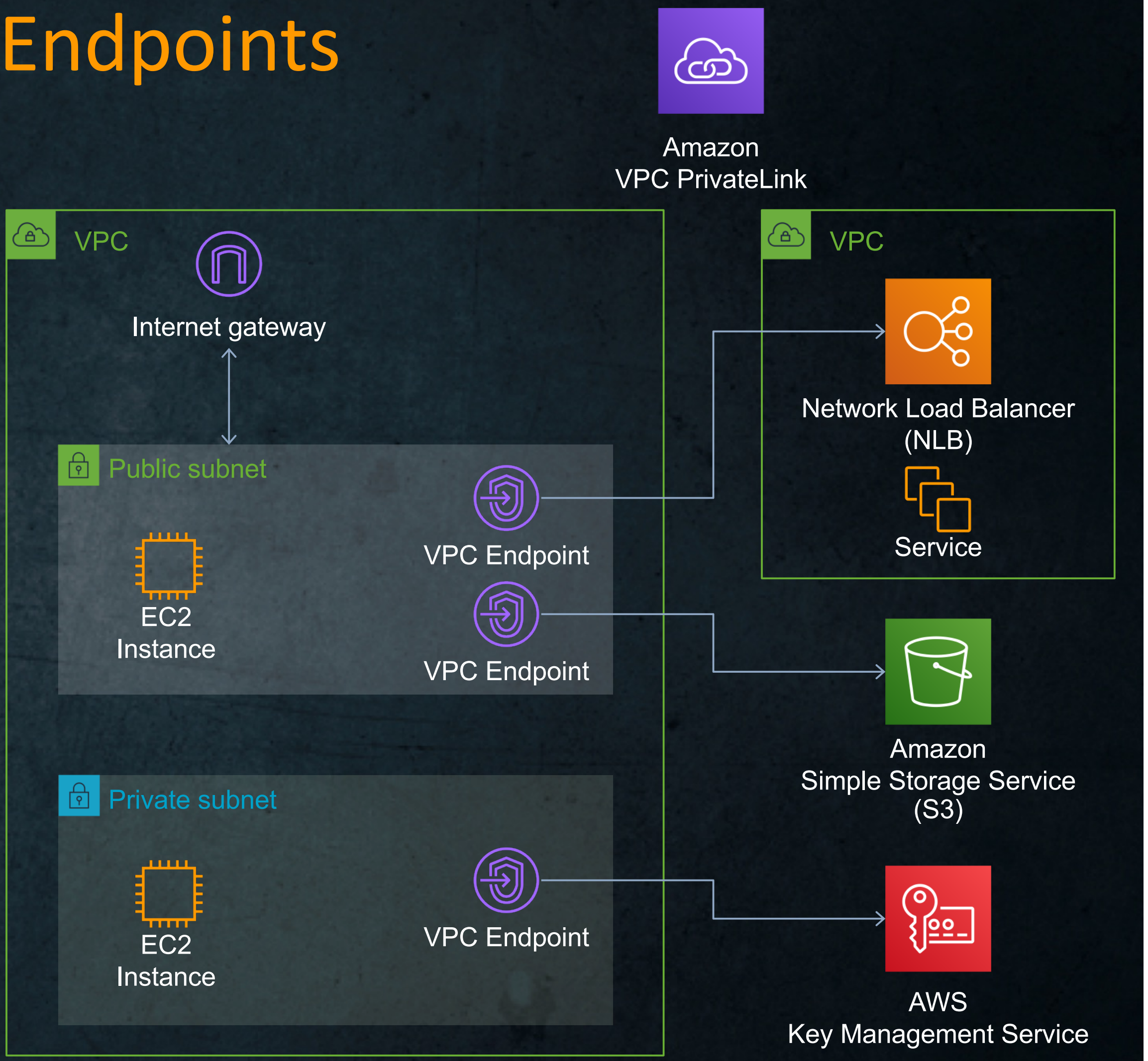
- Stateful firewall
- Inbound and Outbound customer defined rules
- Instance/Interface level inspection
  - Micro segmentation
  - Mandatory, all instances have an associated Security Group
- Can be cross referenced
  - Works across VPC Peering
- Only supports allow rules
  - Implicit deny all if not allowed



VPC connectivity options

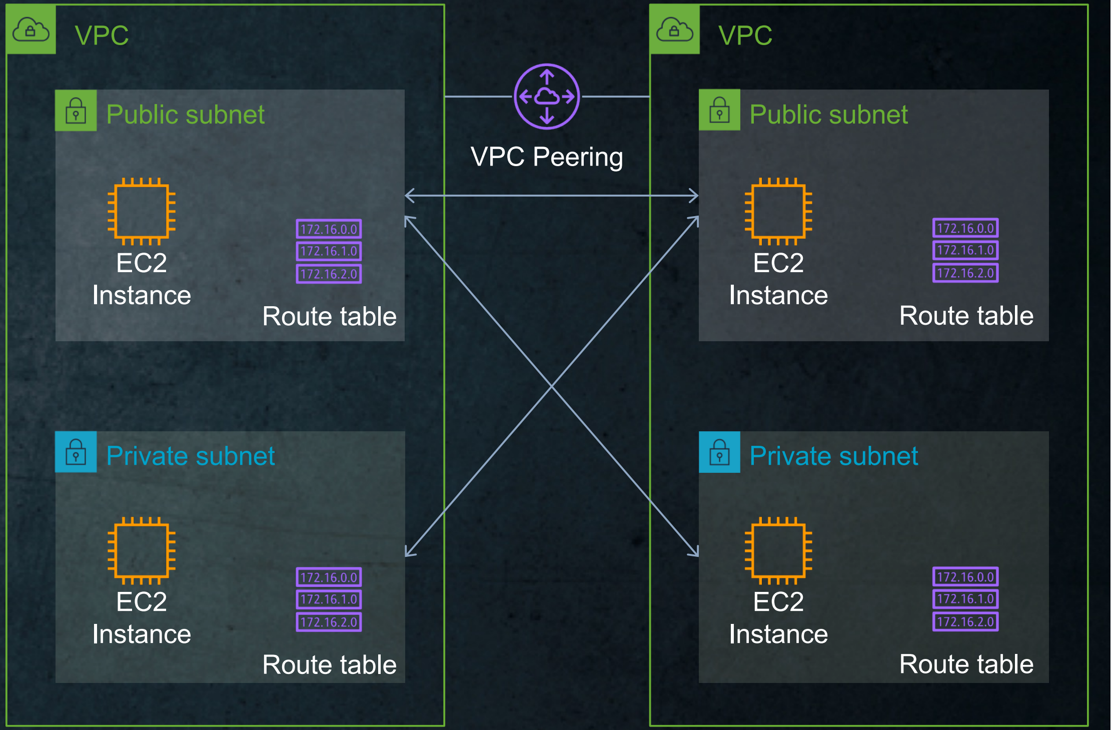
Stay on AWS network: VPC Endpoints

- 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

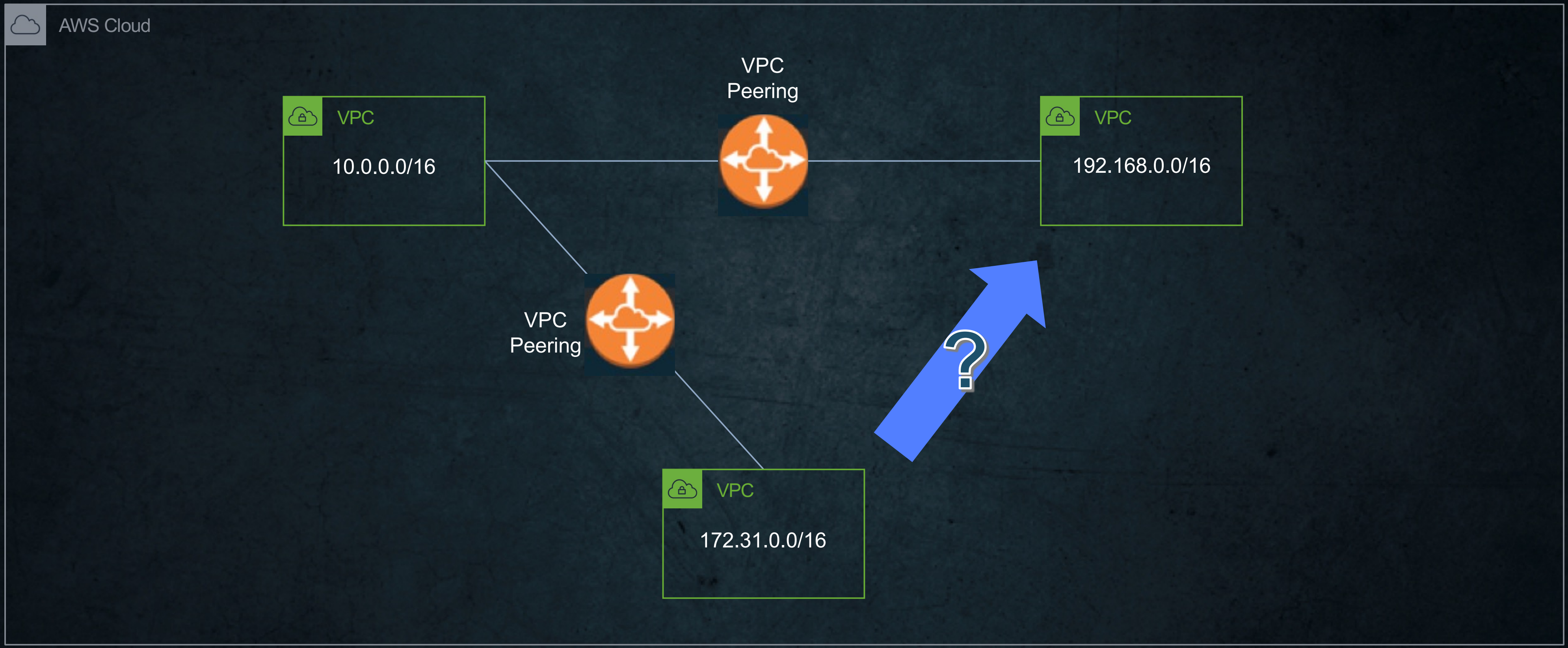


Connect multiple VPCs: VPC Peering

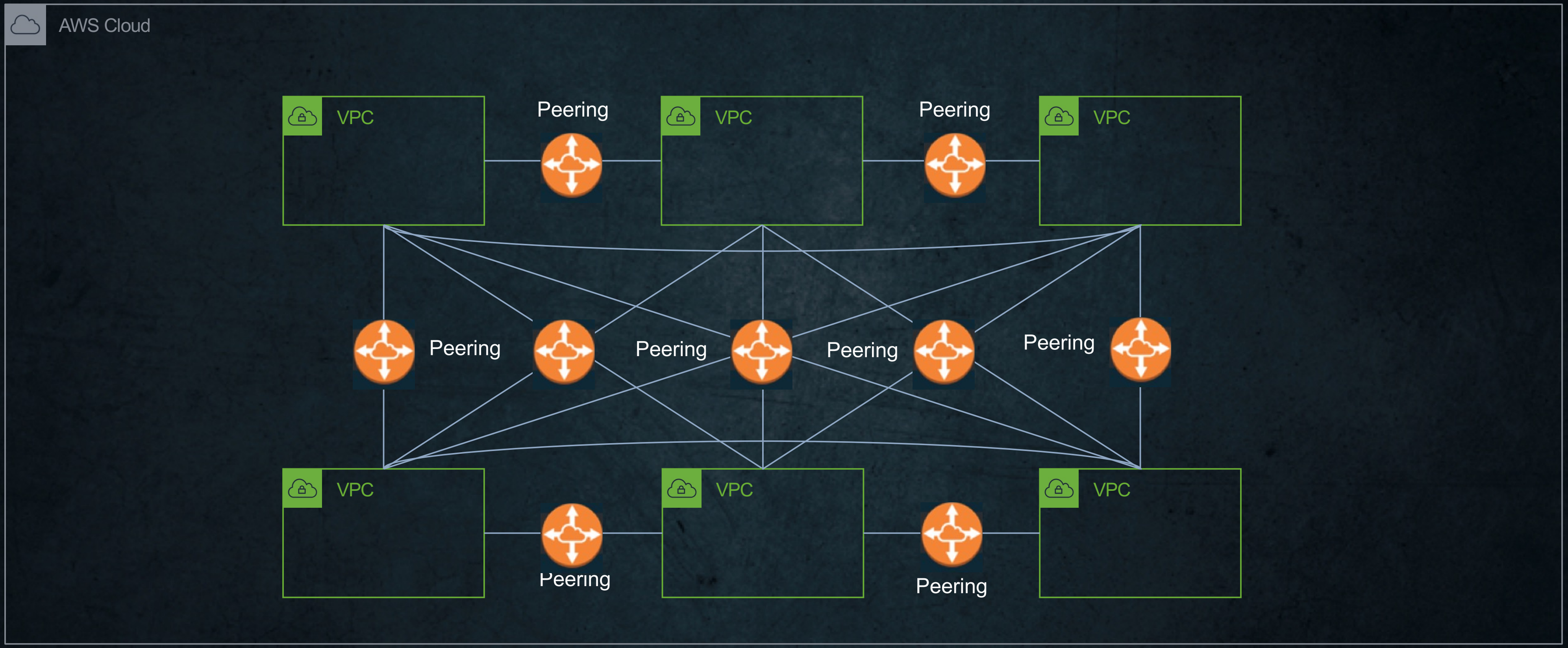
- Scalable and high available
- Supported between AWS accounts
- Supported across AWS Regions
- Bi-directional traffic
- Remote Security groups can be referenced
- Routing policy with Route Tables
    - Not all subnets need to connect to each other
- No overlapping IP addresses
- No transitive routing



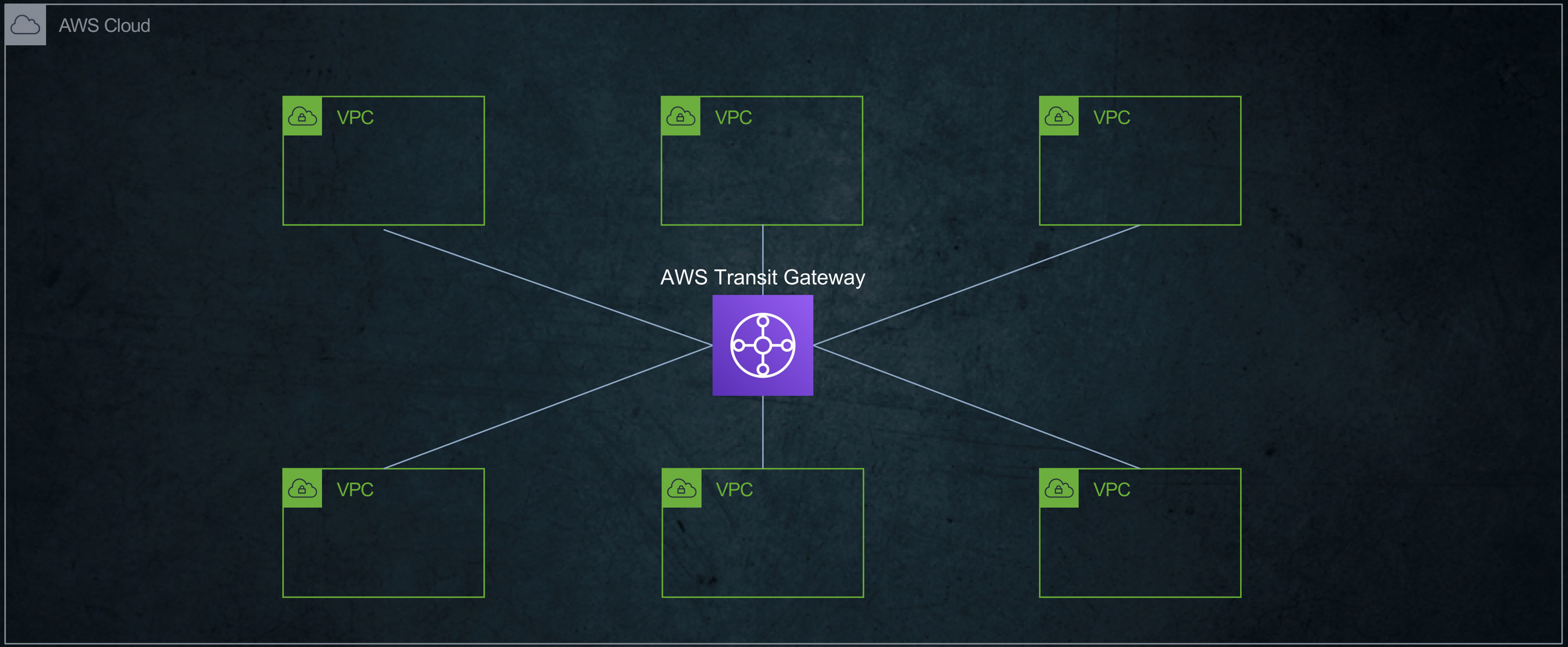
Connect multiple VPCs: VPC Peering



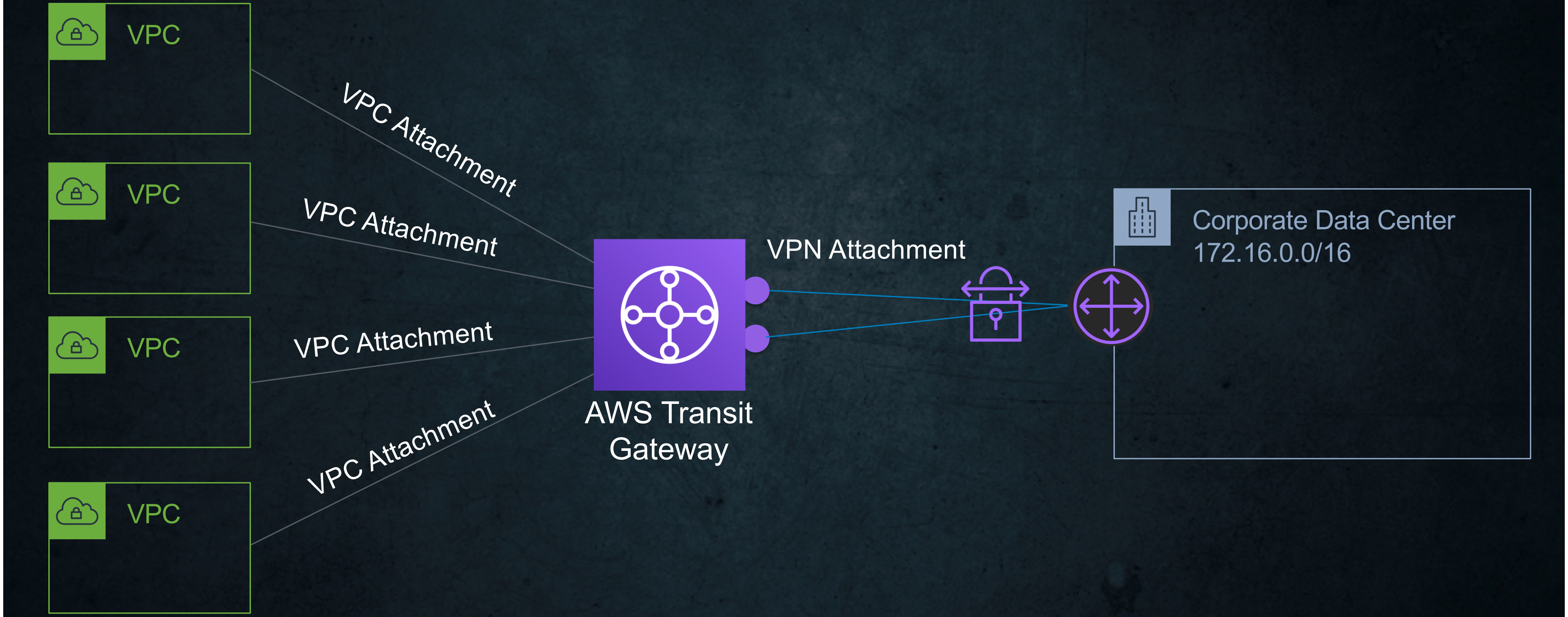
Connect multiple VPCs: VPC Peering at scale



Multiple VPCs access models – AWS Transit Gateway

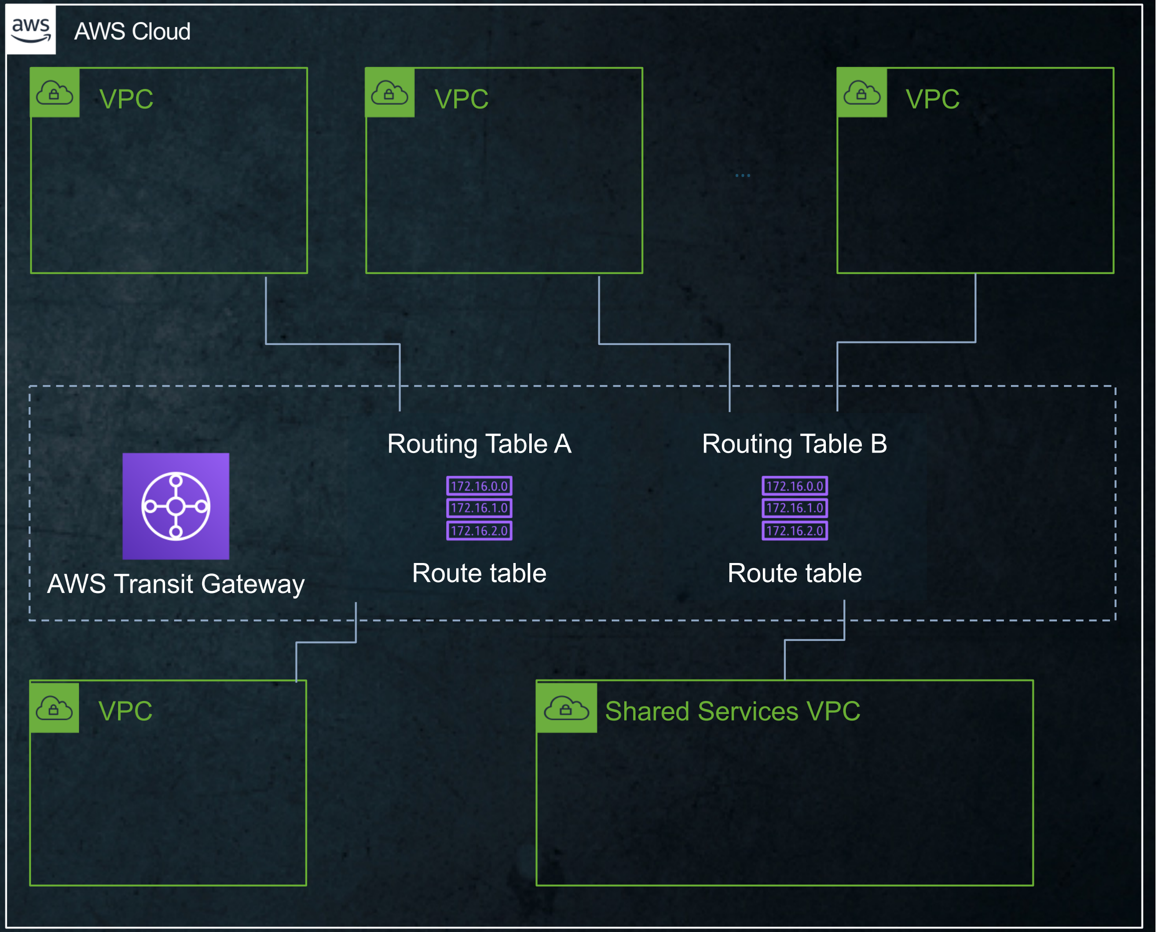


AWS Transit Gateway with AWS site-to-site VPN



Connect multiple VPCs: Transit Gateway

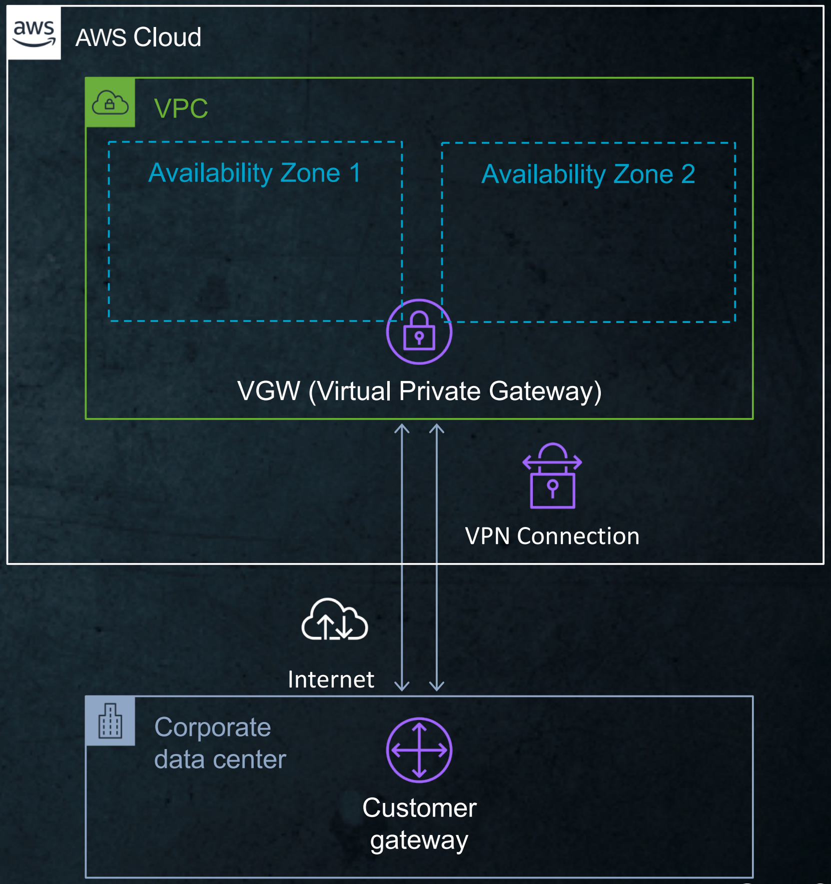
- Connect thousands of VPC across accounts within a region
- Connect your VPCs and on-premises through a single transit gateway
- Centralize VPN and AWS Direct Connect connections
- Control segmentation and data flow with Route Tables
- Hub and Spoke design
- Up to 50 Gbps per attachment (burst)



Connecting to on-premises

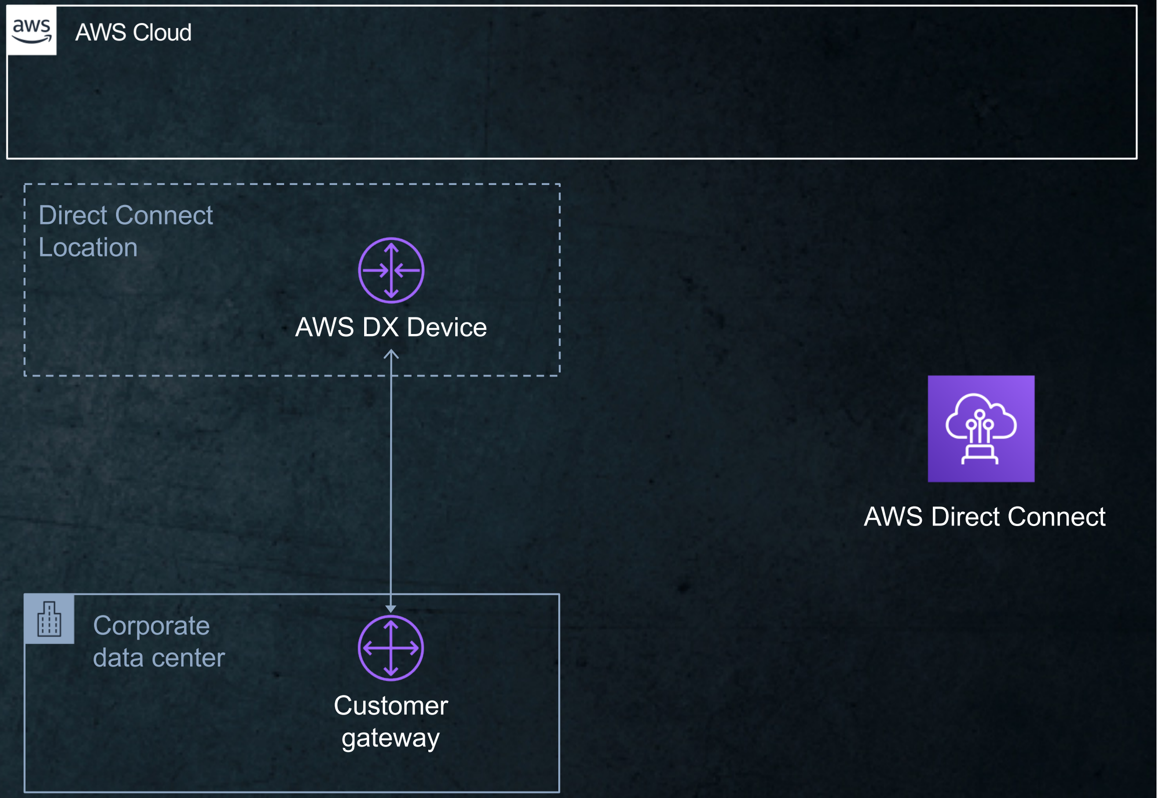
VPN to AWS: Virtual Private Gateway

- Fully managed VPN endpoint device
- One Virtual Private Gateway per VPC
- Redundant IPSec VPN Tunnels
  - Terminating in different AZs
- IPSec
  - AES 256-bit encryption
  - SHA-2 hashing
- Scalable
- Dynamic (BGP) or Static Routing
- Default 10 Site-to-Site VPN connections per VGW – can increase limit



Dedicated link to AWS: AWS Direct Connect

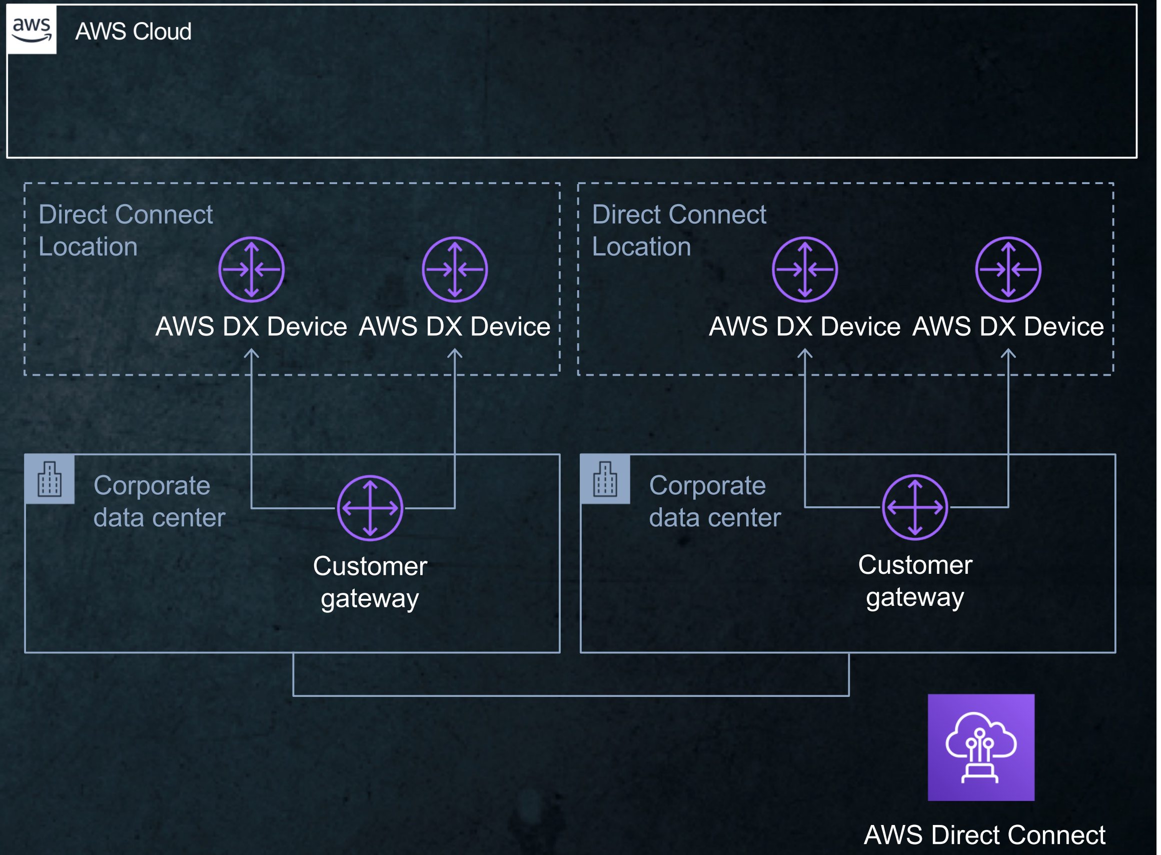
- Dedicated network connection from your premises to AWS
- Dedicated Connection (1 or 10 Gbps, Supports multiple VIFs)
- AWS Partner Hosted Connection (50 Mbps to 10 Gbps, Single VIF)
- Consistent Network Performance
  - Dedicated bandwidth
  - Low latency
- Reduced egress data charges
- Connect to 97+ Direct Connection Locations across the globe



AWS Direct Connect

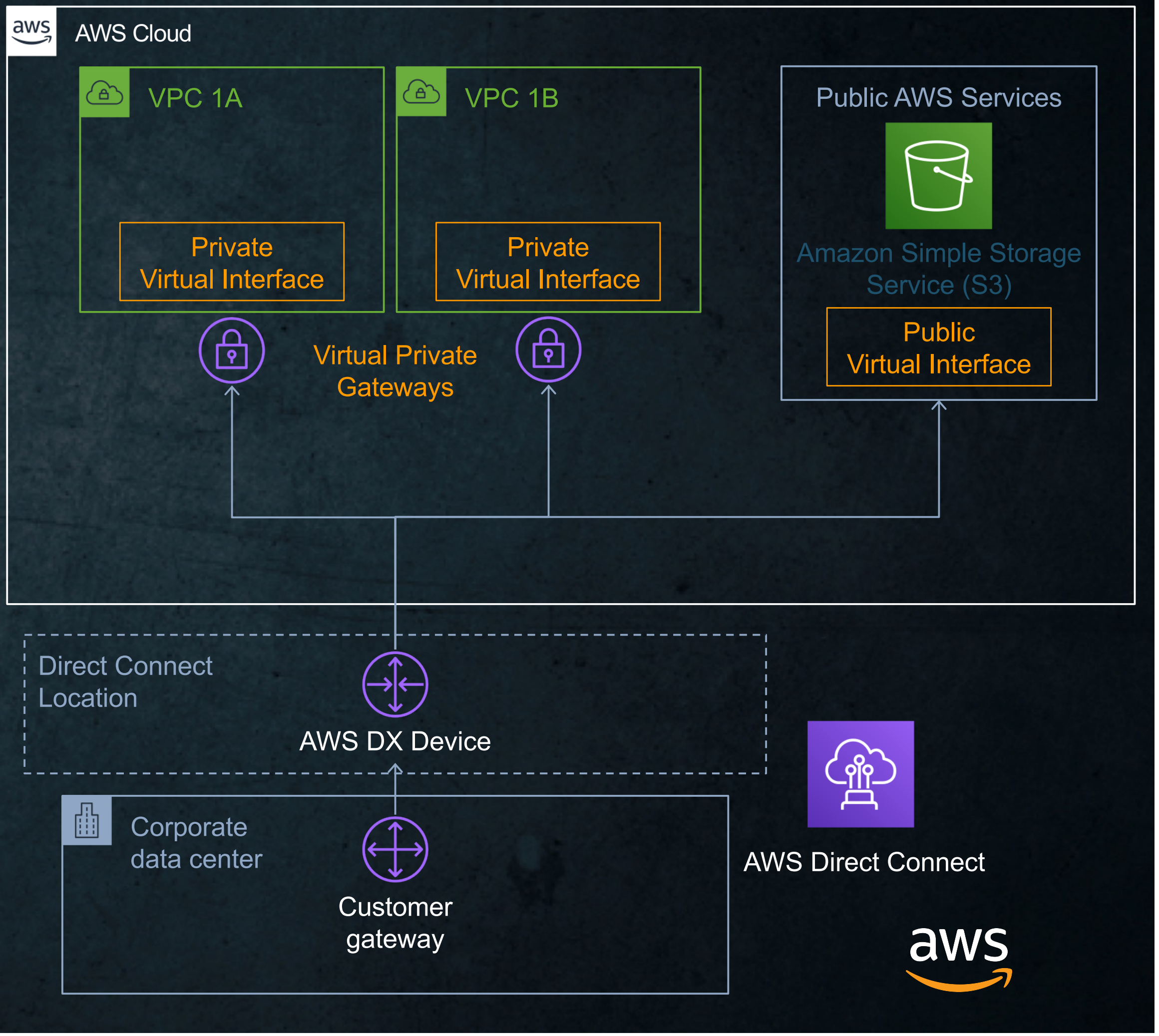
Dedicated link to AWS: AWS Direct Connect

- For redundancy, DX can deployed with single or multiples:
  - Circuits
  - Providers
  - Customer Gateways
  - Direct Connect Locations
  - Customer data centers
- BGP Routing for redundancy
  - AS Path Prepend
  - Scope BGP Communities
  - Local Preference BGP Communities



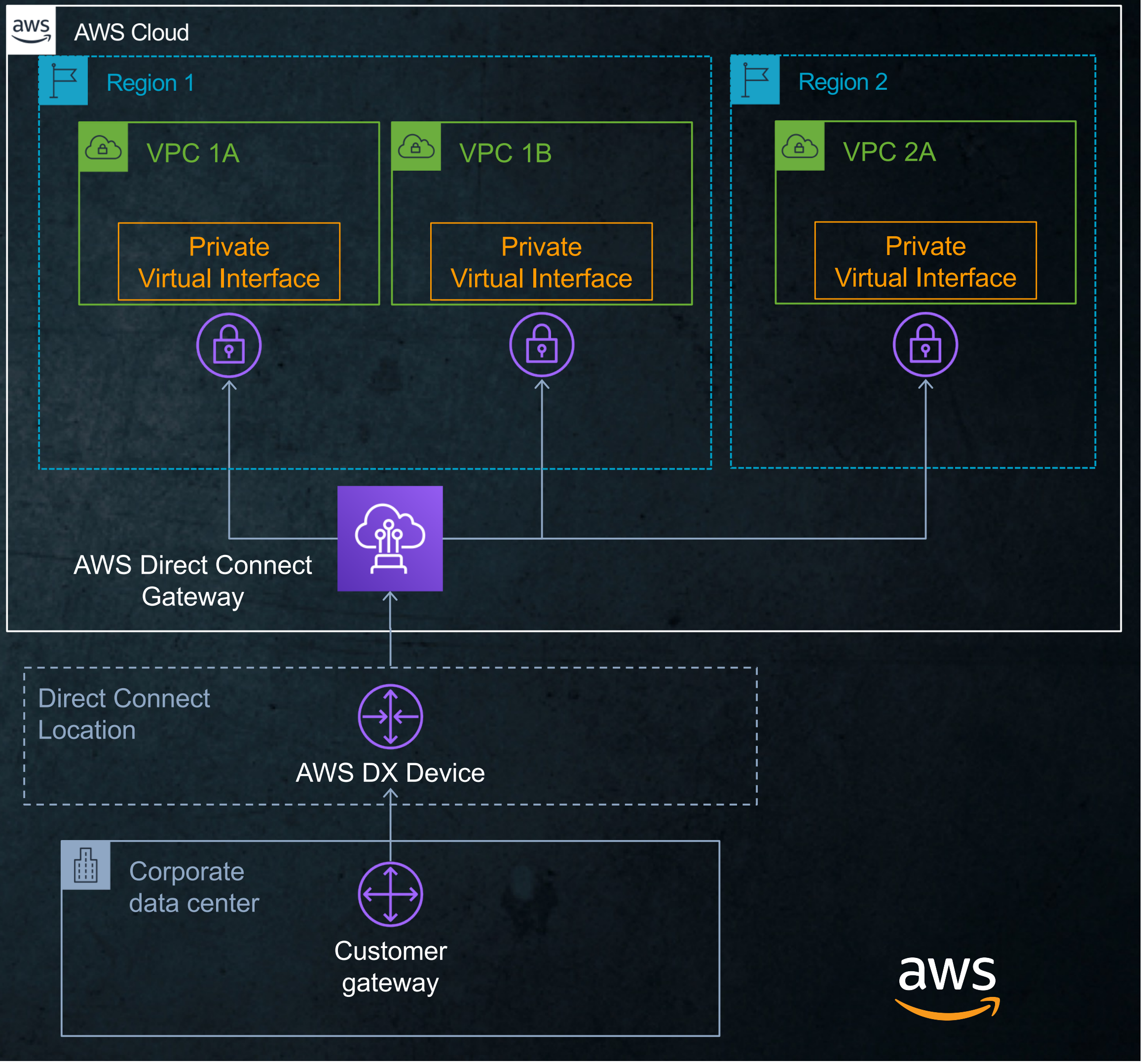
Dedicated link to AWS: AWS Direct Connect

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



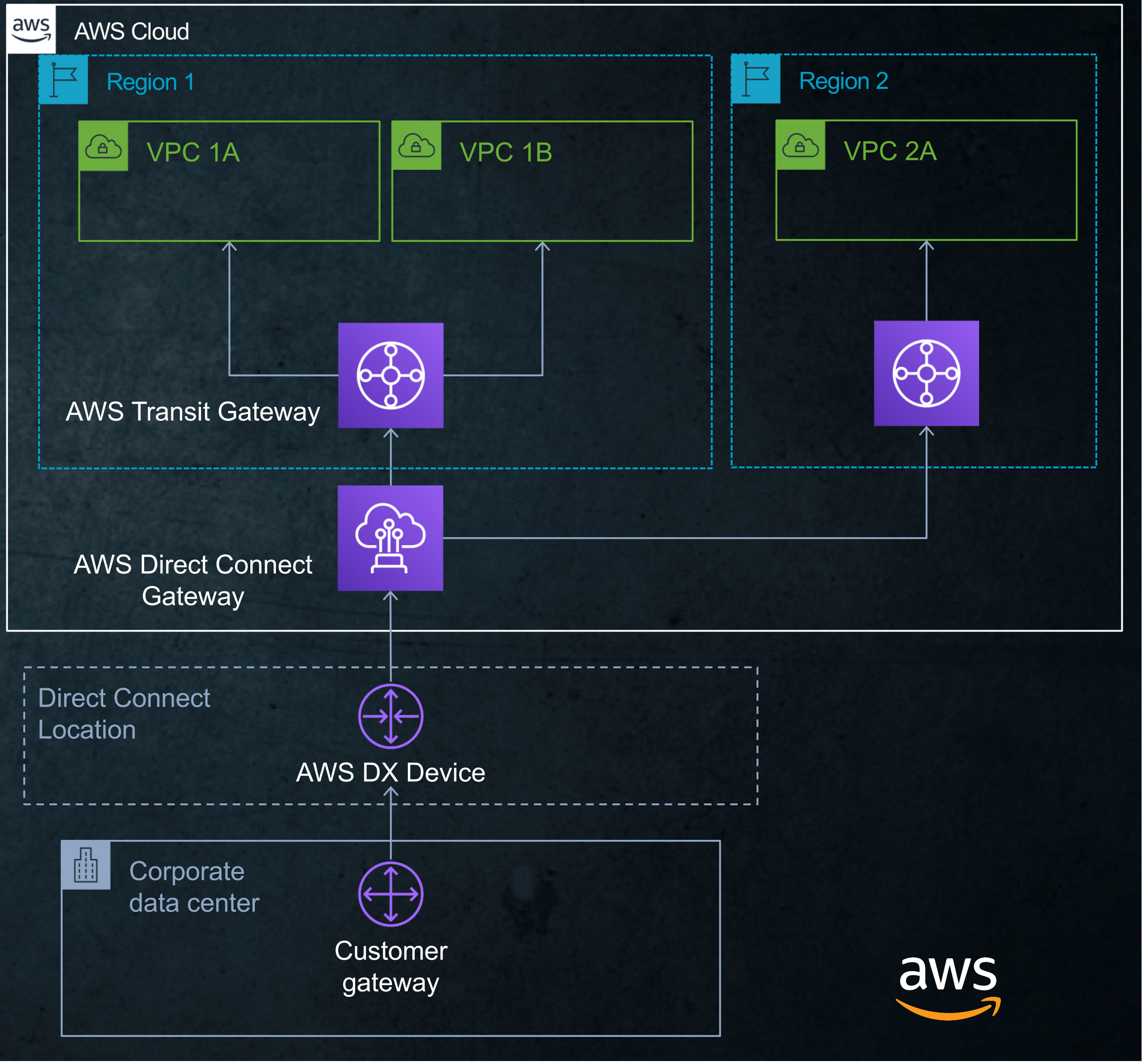
Dedicated link to AWS: AWS Direct Connect

- Global resource
- Connect to multiple VPCs
- VPCs can be on same or different
  - 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



Connect at global scale: DX Gateway + 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



Questions?