



Networking in AWS

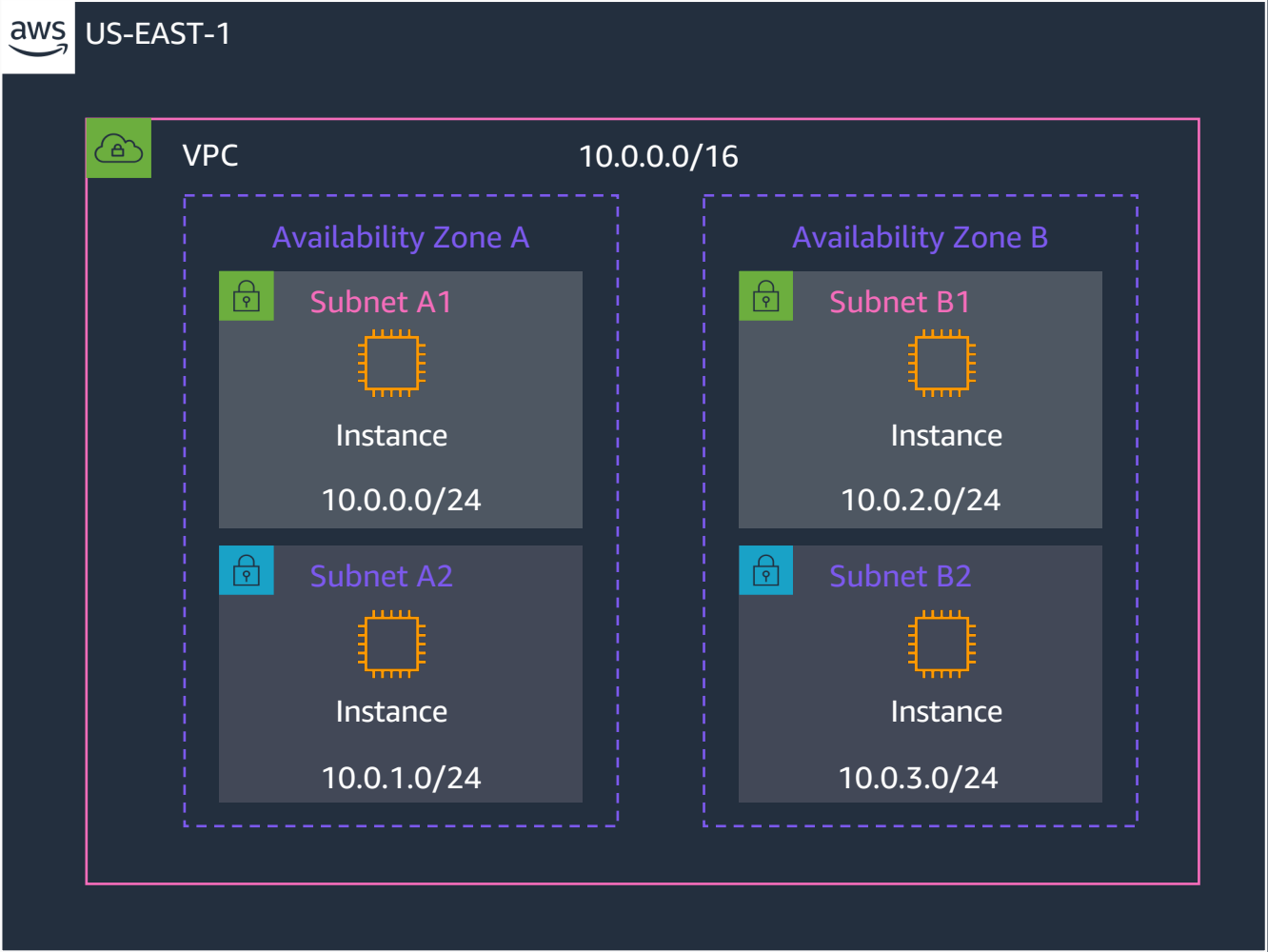
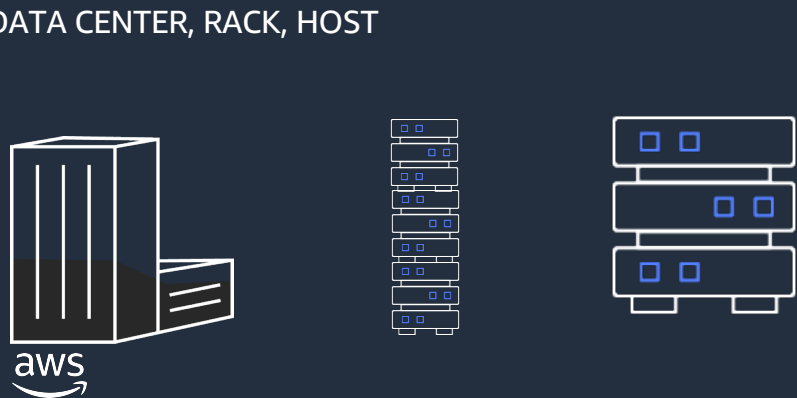
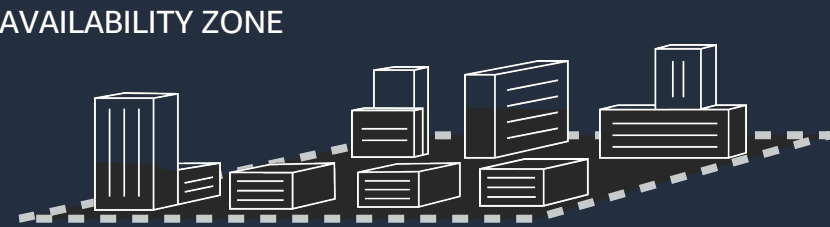
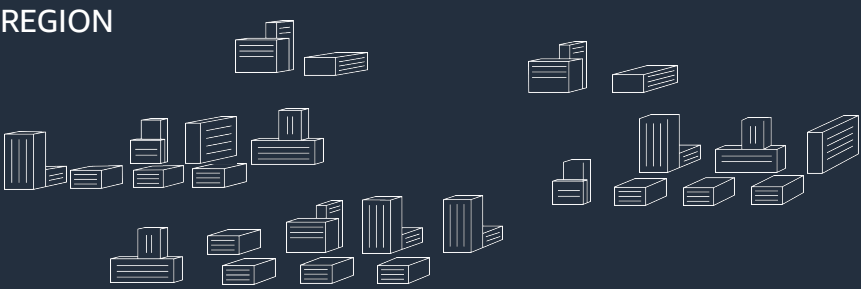
Agenda

- 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
- Domain name resolution

Amazon VPC



Amazon Virtual Private Cloud (VPC) overview



VPC IP addressing

- Support IPv4 and IPv6
 - IPv4: VPCs can be between /16 and /28
 - IPv6: /56 for VPC's & /64 for subnets (fixed)
- VPCs support subnetting
- VPC CIDRs cannot be modified once created
- Additional CIDRs can be added to a VPC
- Supports bringing your own IP space in the newly launched regions too
- AWS announced Amazon-provided contiguous IPv6 CIDR blocks

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
- The VPC IP Address Manager (IPAM) feature can be leveraged to plan, track, and monitor IP addressing in AWS
- Amazon VPC IP Address Manager (IPAM) now manages IP Addresses in your network outside your AWS Organization
- Amazon VPC IP Address Manager introduces a customizable dashboard with new insights

Amazon VPC IP Address Manager (IPAM)

Plan, track, and monitor IP addresses across
AWS accounts and AWS Regions

Works for IPv4 and IPv6



Automate IP assignments

Automate across multiple
Regions and accounts based on your
application's unique networking and
security needs



Monitor across the network

Avoid downtime with overlap detection,
tracking IPs in compliance with security
policy, and utilization trends

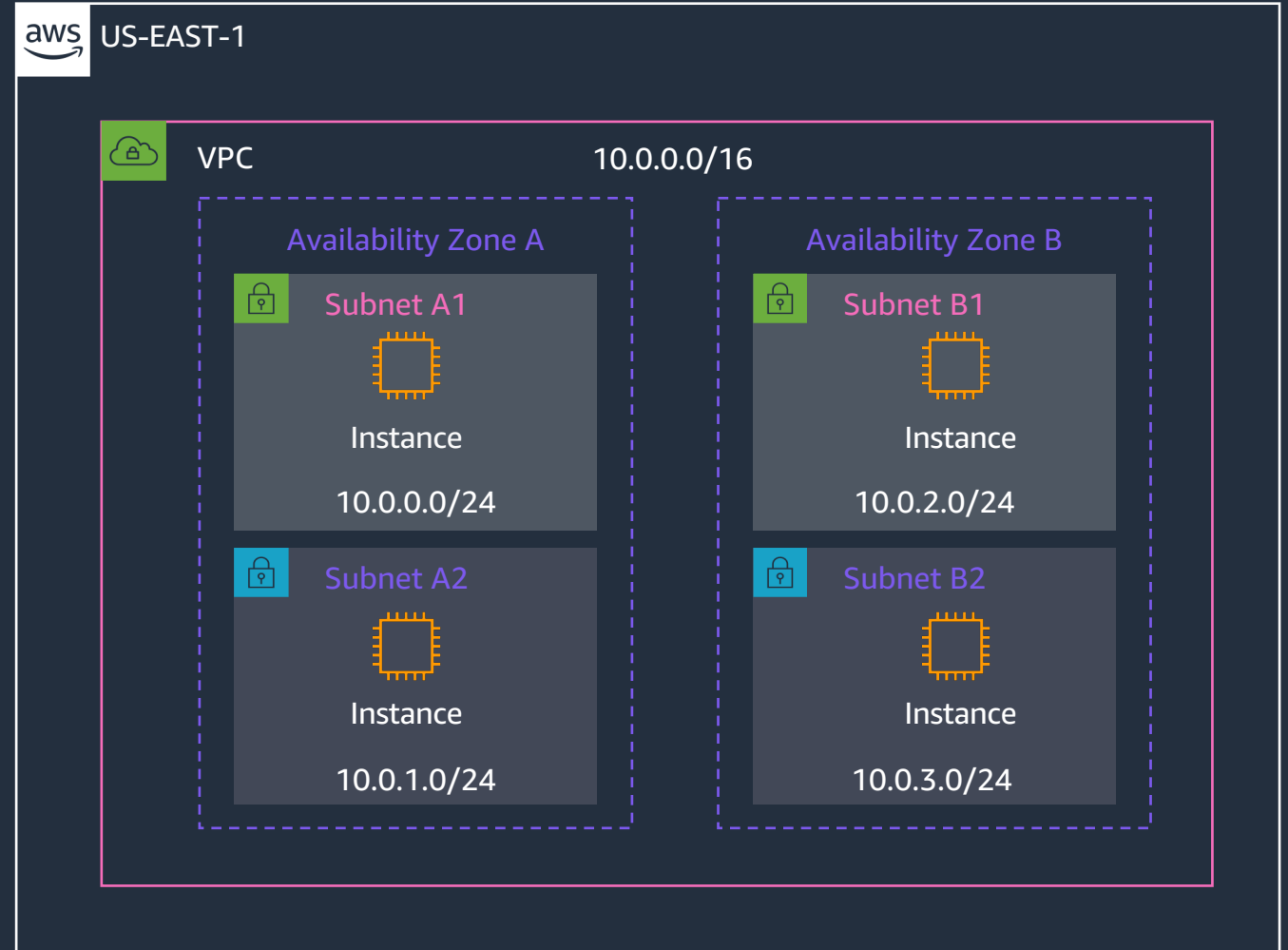


Retrospective analysis

Faster troubleshooting
and auditing

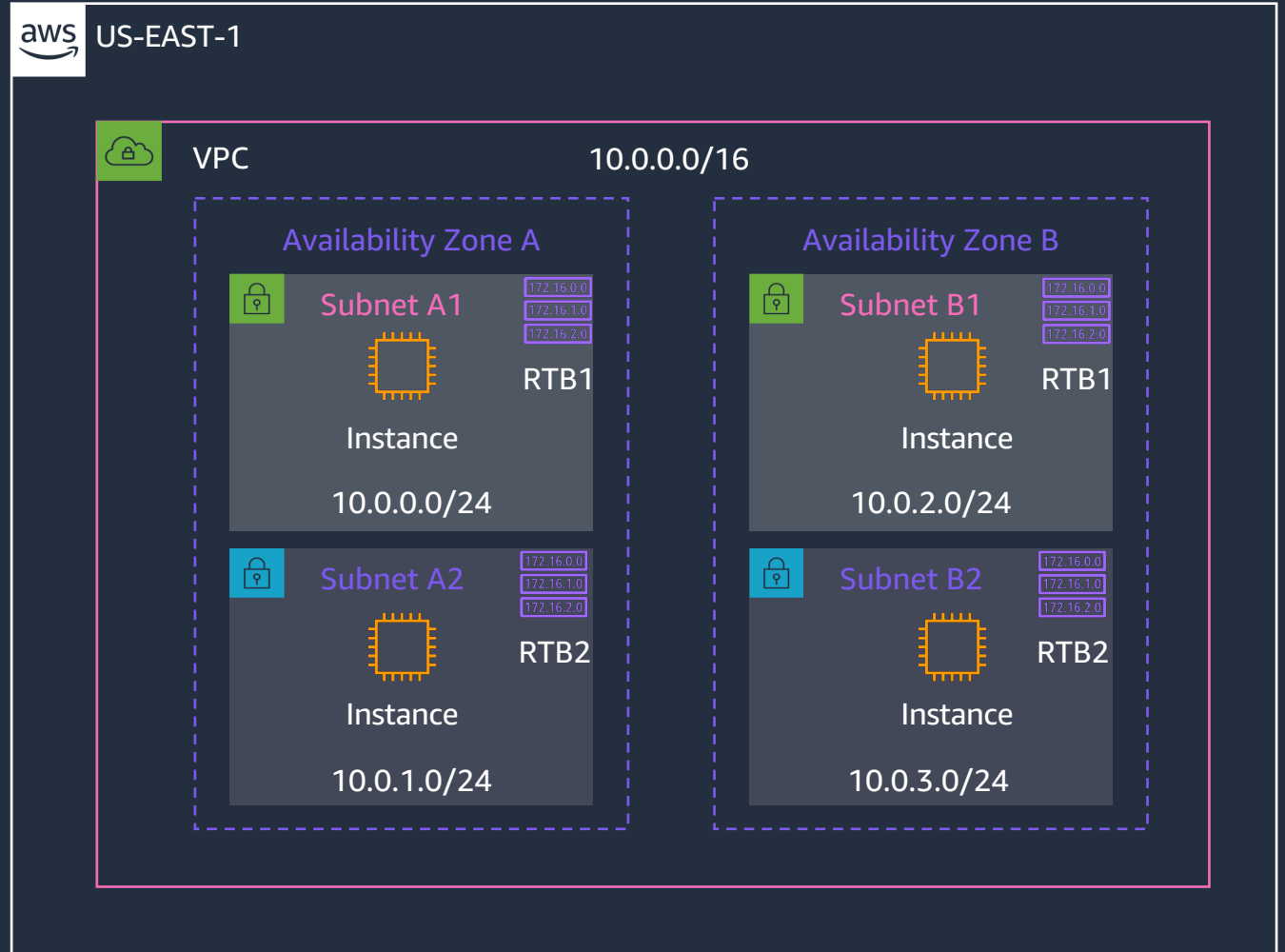
Subnets

- VPCs span a region
- Subnets are allocated as a subset of the VPC CIDR range and span a specific AZ
- You can have up to 200 subnets per VPC.
- Implicit route between all subnets within a VPC



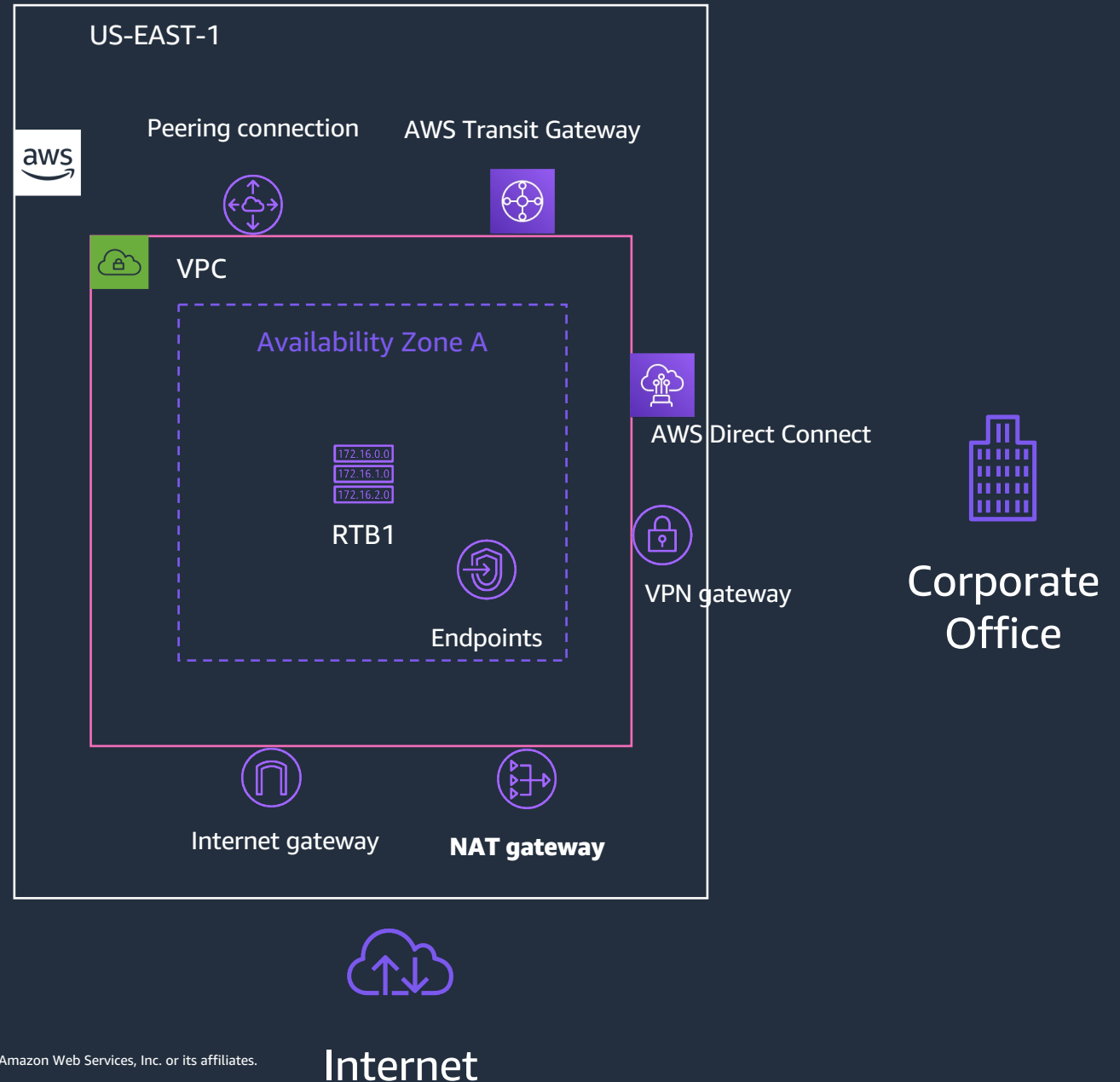
Routing tables

- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- You can have 50 routes per route table.



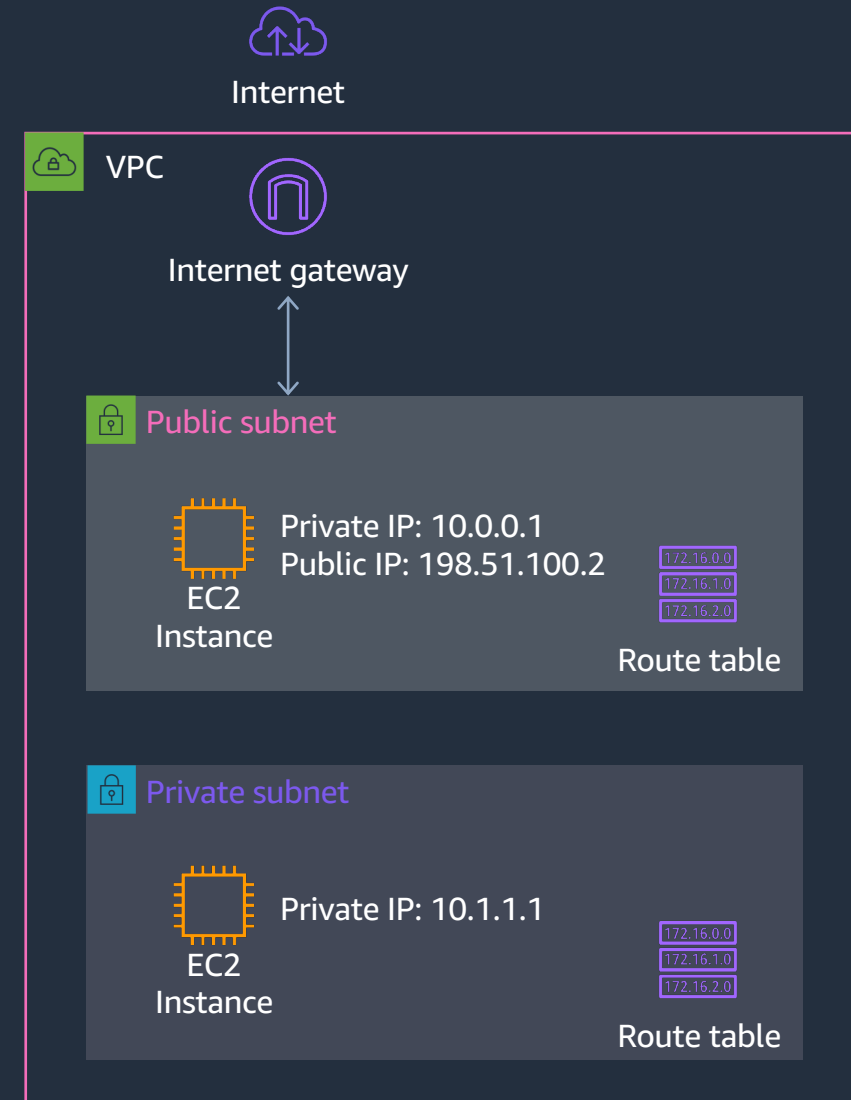
Routing

- Route Tables direct traffic towards:
 - Internet / NAT Gateway
 - Gateway Endpoint
 - 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



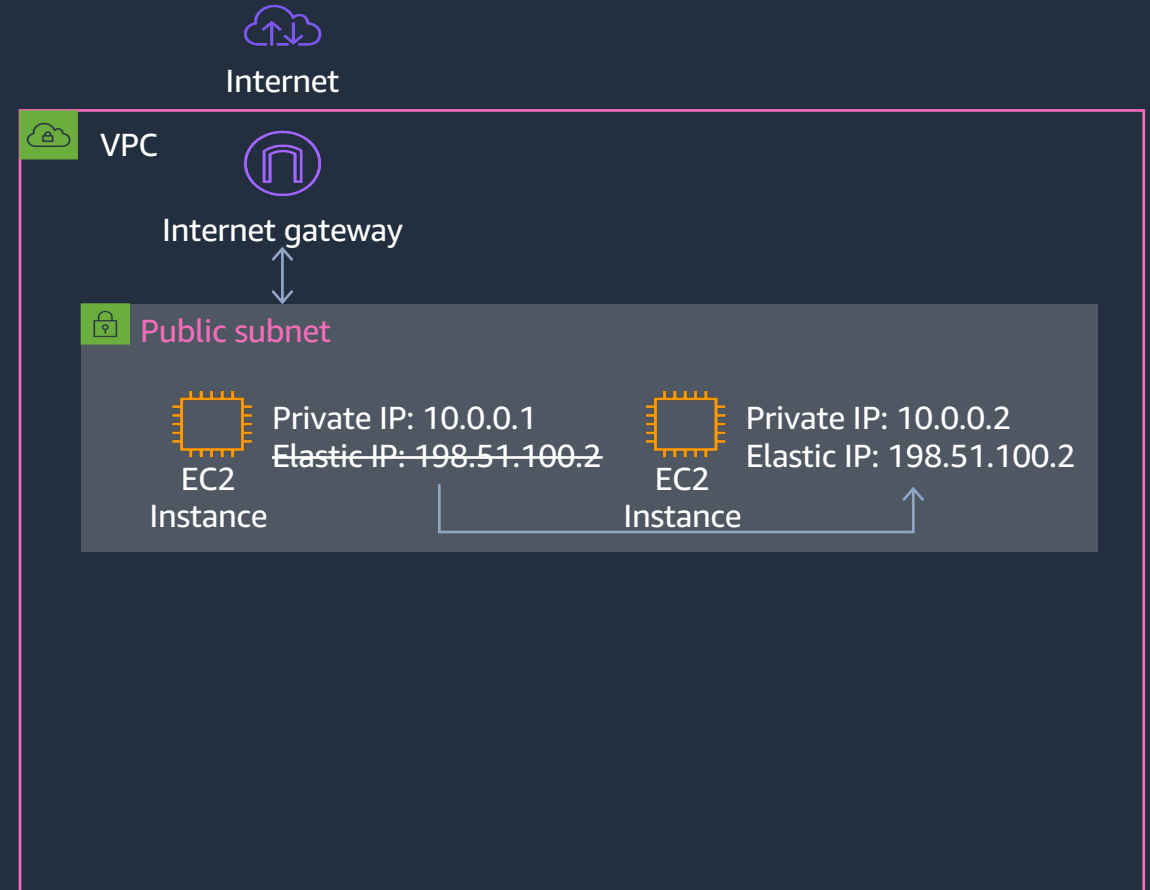
VPC to internet: Internet Gateway

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



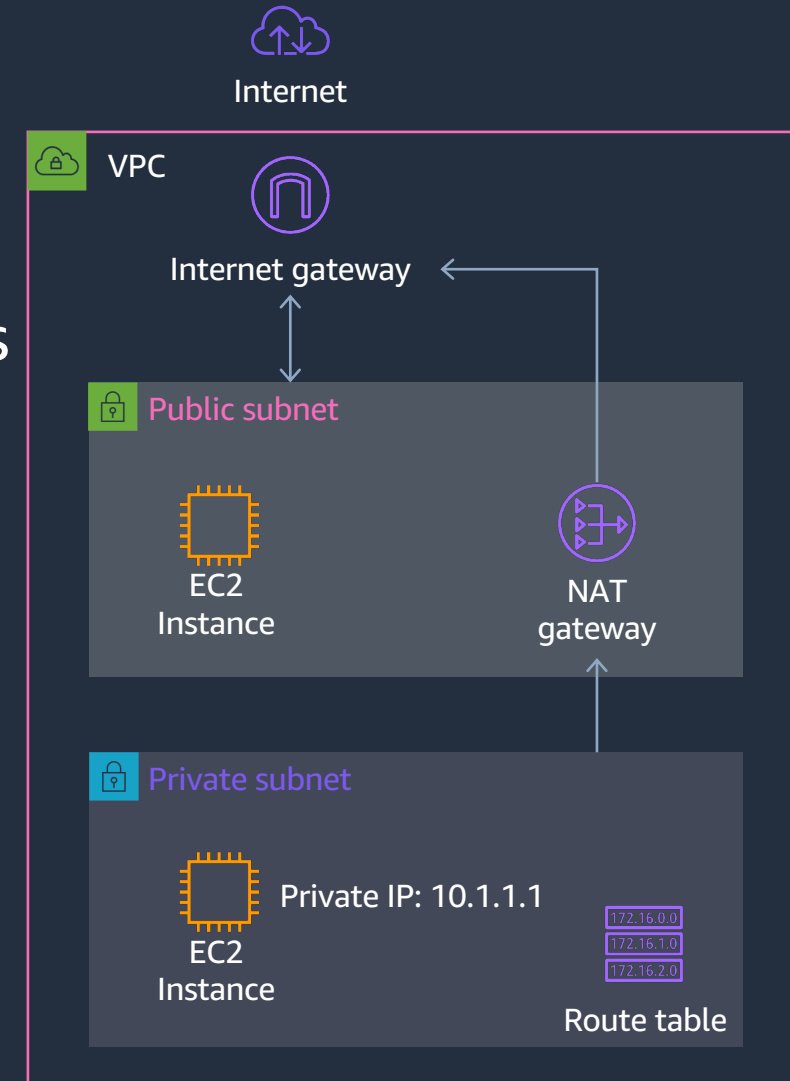
Public IP addressing: Elastic IP Address

- 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

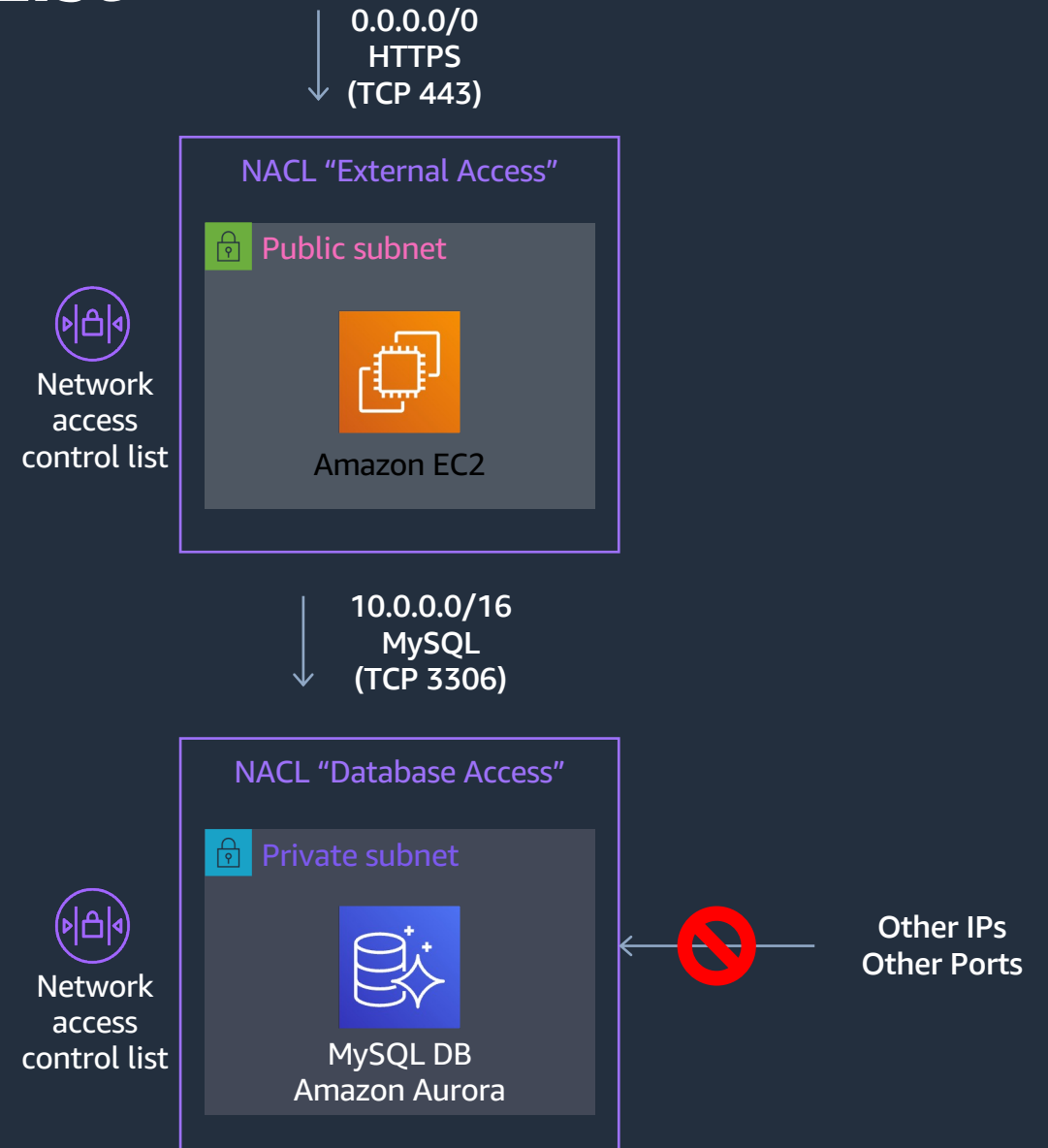


VPC Security



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

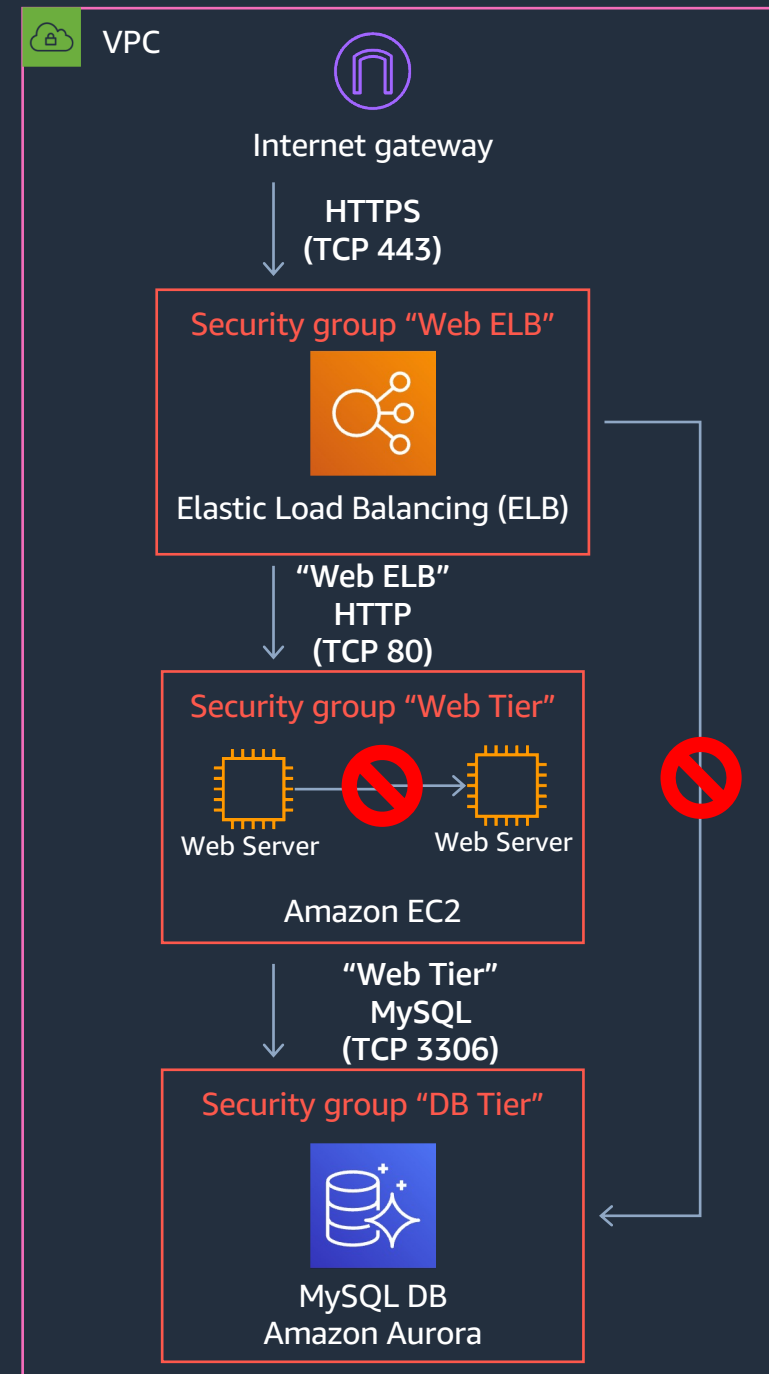
Micro segmentation

Mandatory, all instances have an associated Security Group

- Can be cross referenced

Works across VPC Peering

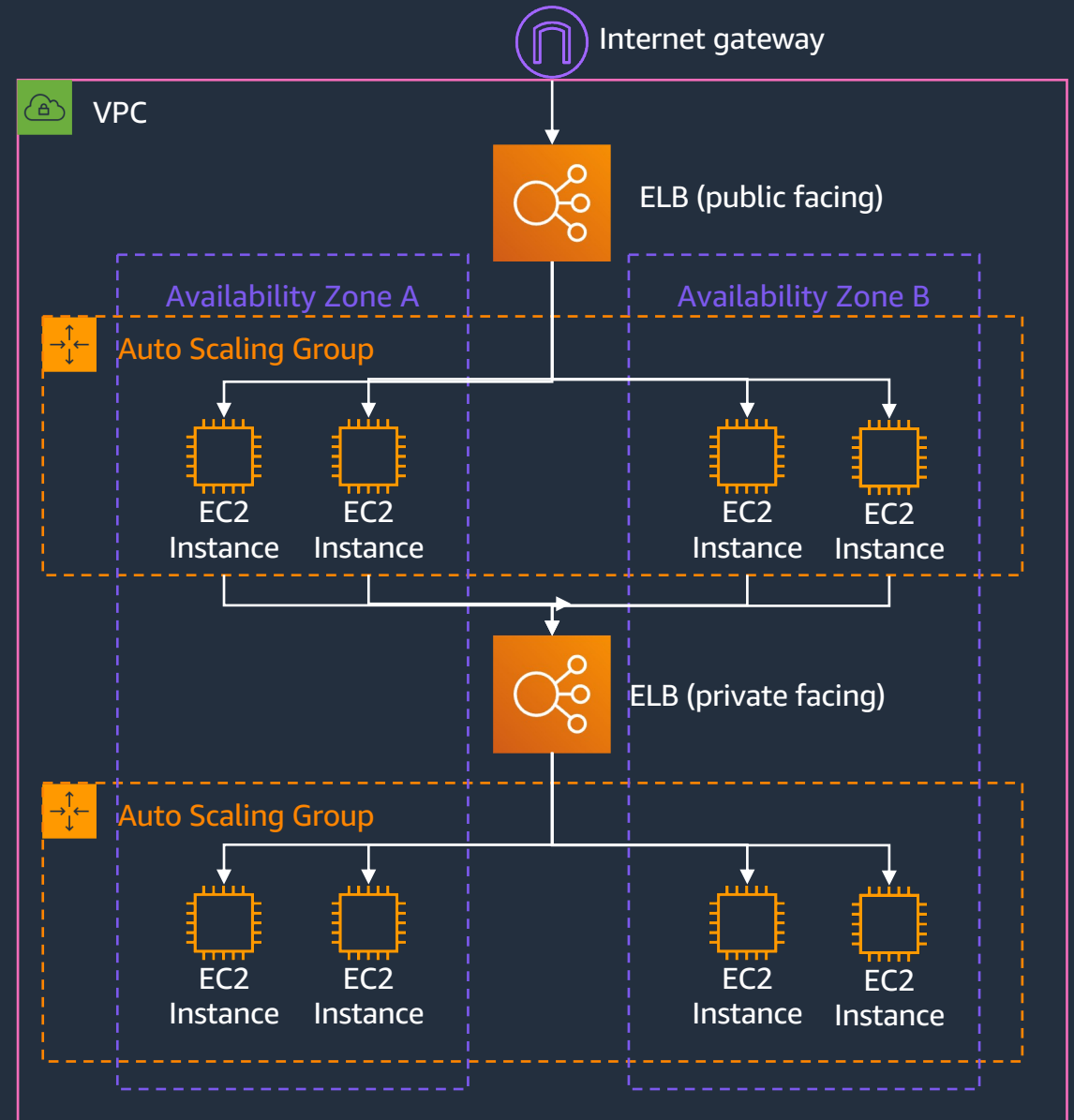
- Only supports allow rules
- Implicit deny all if not allowed
- AWS Verified Access adds a new logging functionality to improve troubleshooting



Load Balancing

Horizontal scaling: Elastic Load Balancing

- Distribute traffic to multiple targets
 - EC2 instances
 - Containers
 - IP addresses
 - Lambda
- Multiple Availability Zones
- ELB Scales automatically
- Support Auto Scaling Groups
 - Automatically (de)register instances to the ELB based on health checks.



Types of ELB: NLB / ALB

Network Load Balancer (NLB)

- Layer 4 Load Balancing
- Connection-based Load Balancing
- High Throughput
- Low Latency
- Preserve source IP address
- Static IPs
- Long-lived TCP Connections
- Supports Security groups

Application Load Balancer (ALB)

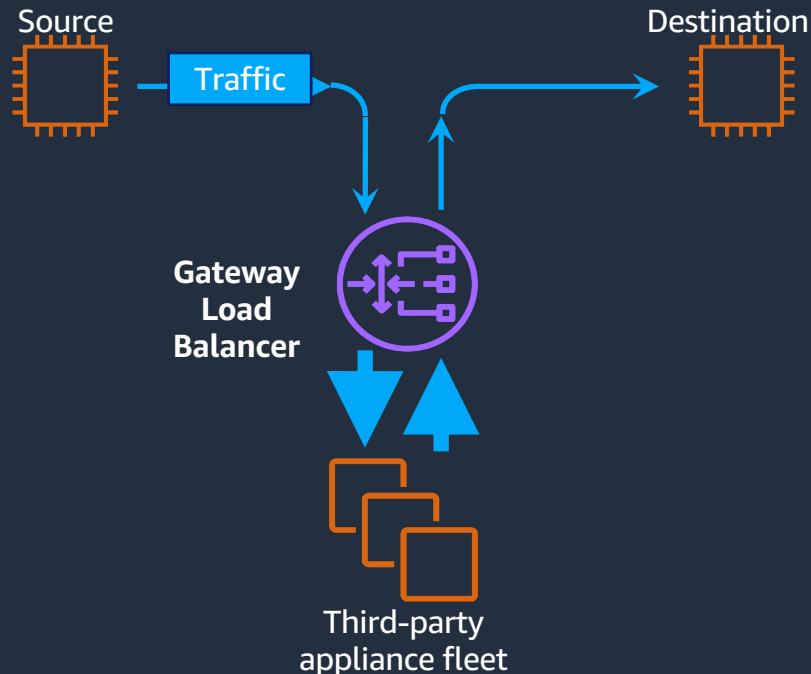
- Layer 7 Load Balancing
- Content-Based Routing (host and path based)
- HTTP/2 Support
- Request Tracing
- Web Application Firewall (WAF) integration
- Application Load Balancer now supports TLS 1.3

Supported by both

- Cross-zone load balancing
- WebSocket Support
- Deletion Protection

Gateway Load Balancer (GWLB)

- Deploy and manage fleets of virtual appliances in elastic, fault-tolerant, and transparent manner
- Available to customers and technology partners

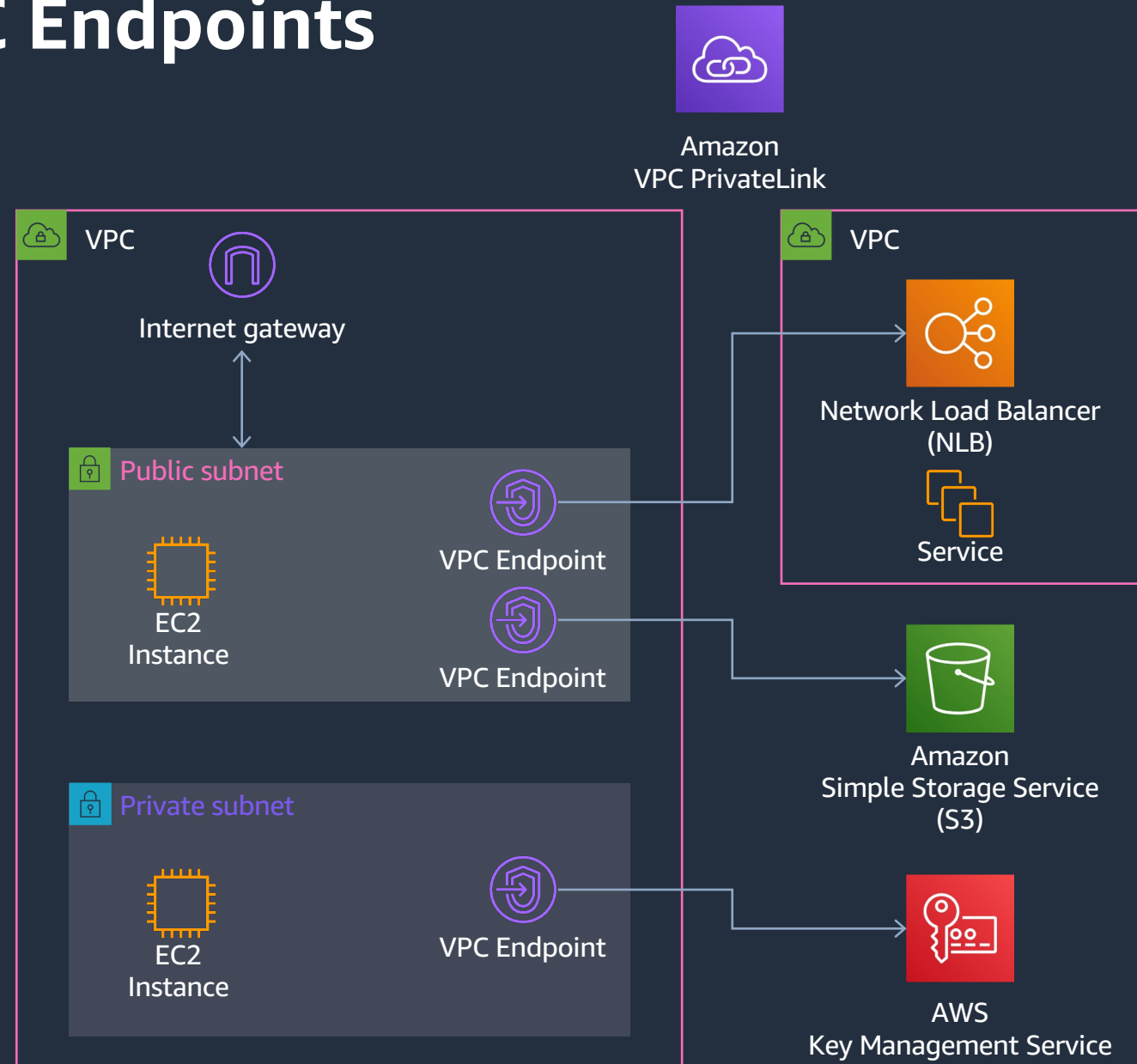


VPC Connectivity Options



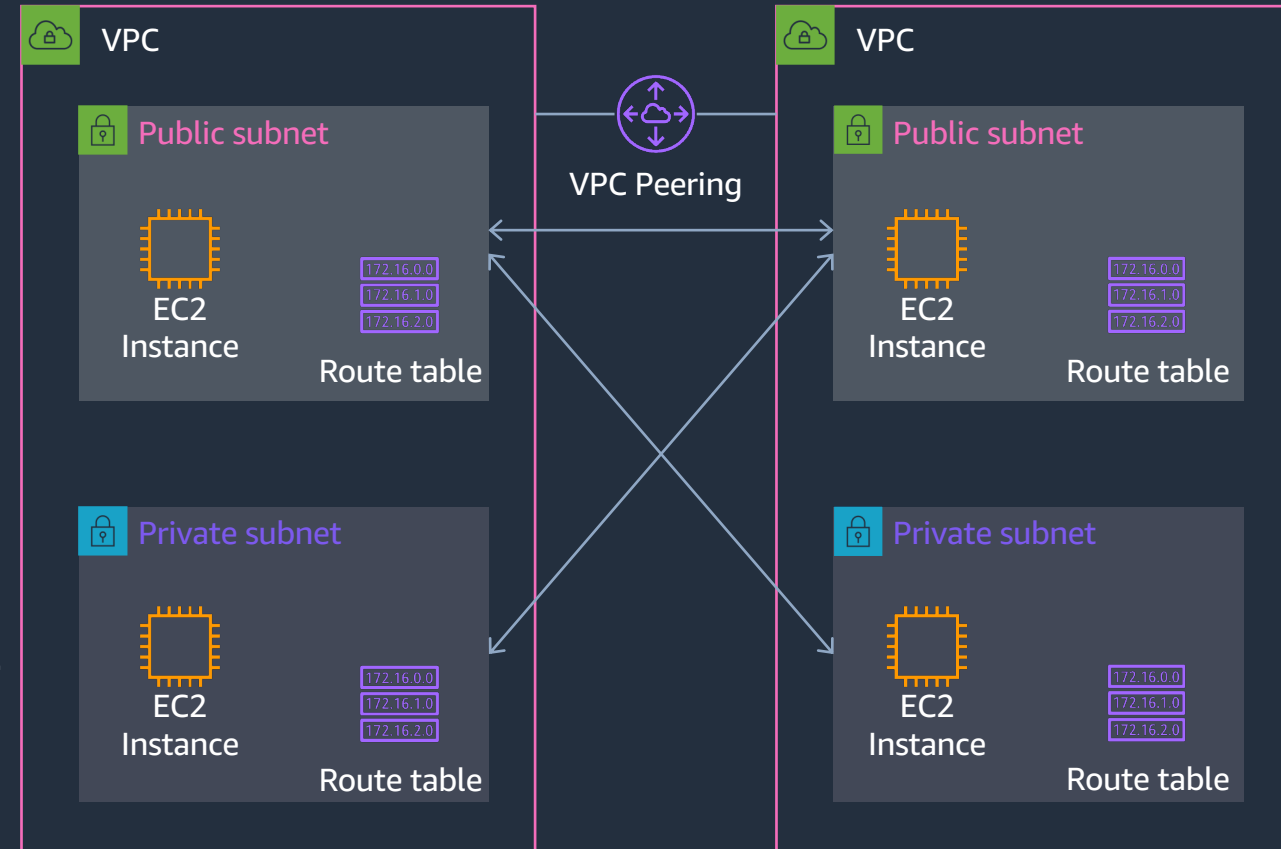
Stay on AWS network: VPC Endpoints

- Connect your VPC to:
 - Supported AWS services
 - VPC endpoint services powered by PrivateLink
- Doesn't require public IPs or Internet connectivity
- Horizontally scaled, redundant, and highly available
- Robust access control
- Metrics for traffic visibility

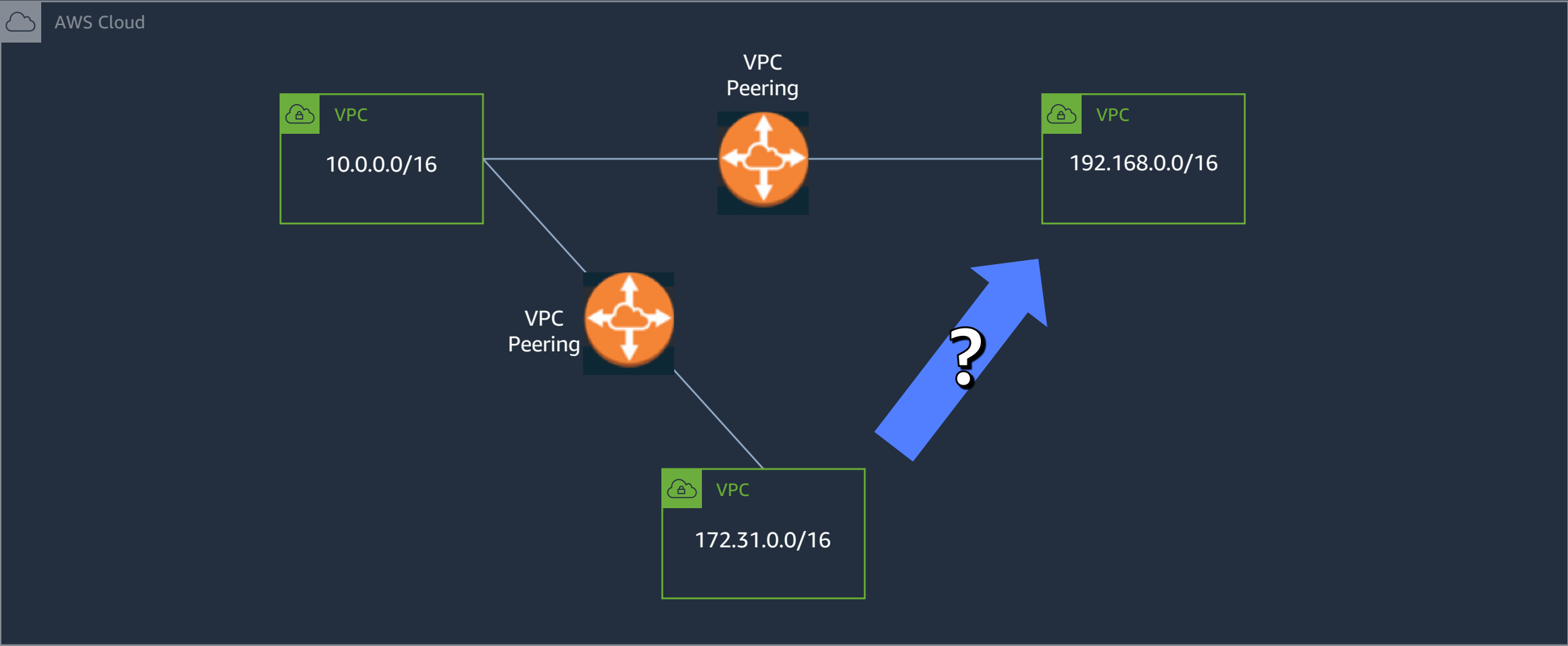


Connect multiple VPCs: VPC Peering

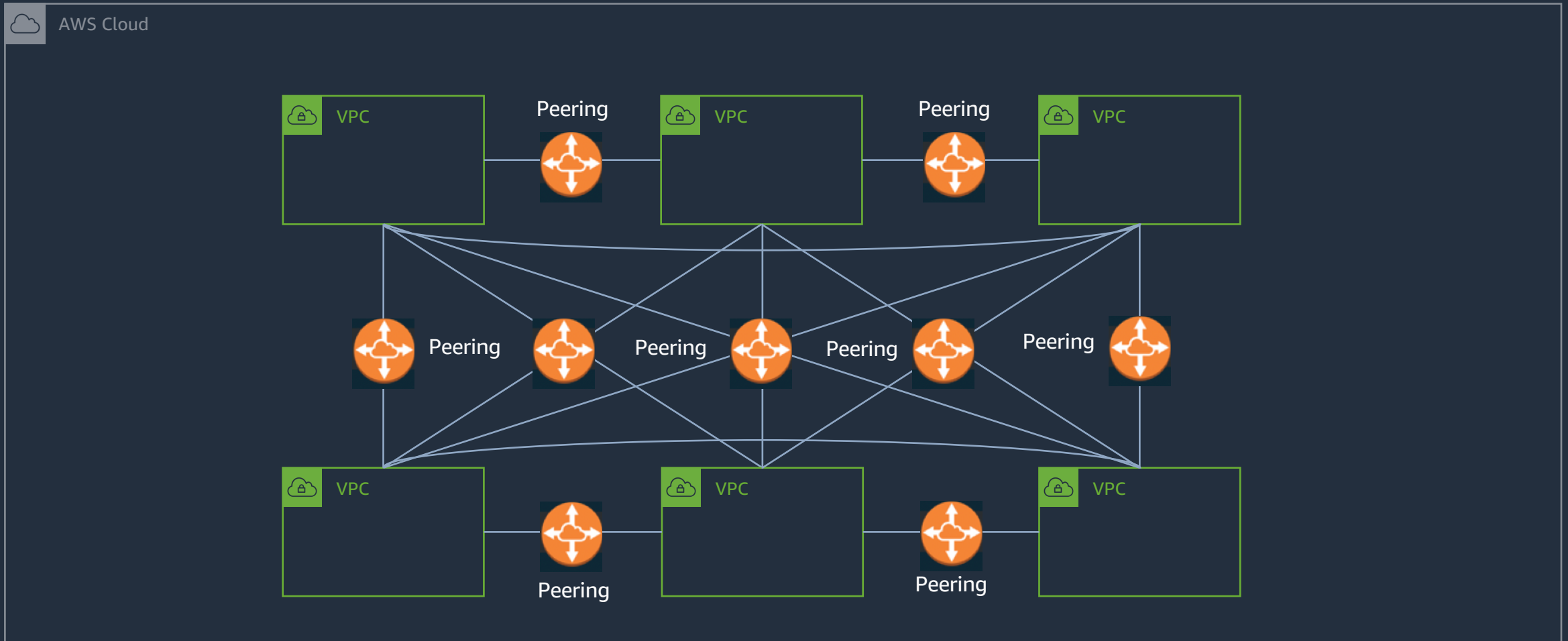
- Scalable and high available
- Supported between AWS accounts
- Supported across AWS Regions
- Bi-directional traffic
- Remote Security groups can be referenced
- Routing policy with Route Tables
 - Not all subnets need to connect to each other
- No overlapping IP addresses
- No transitive routing



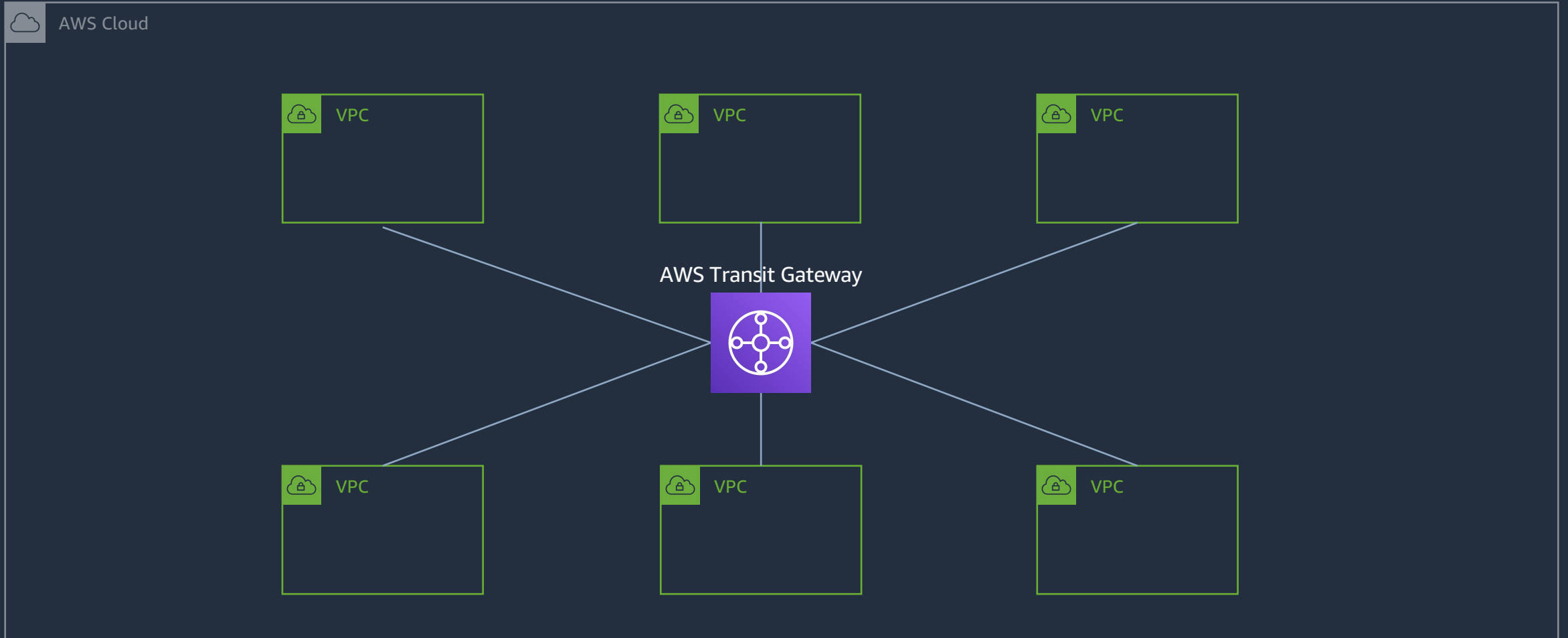
Connect multiple VPCs: VPC Peering



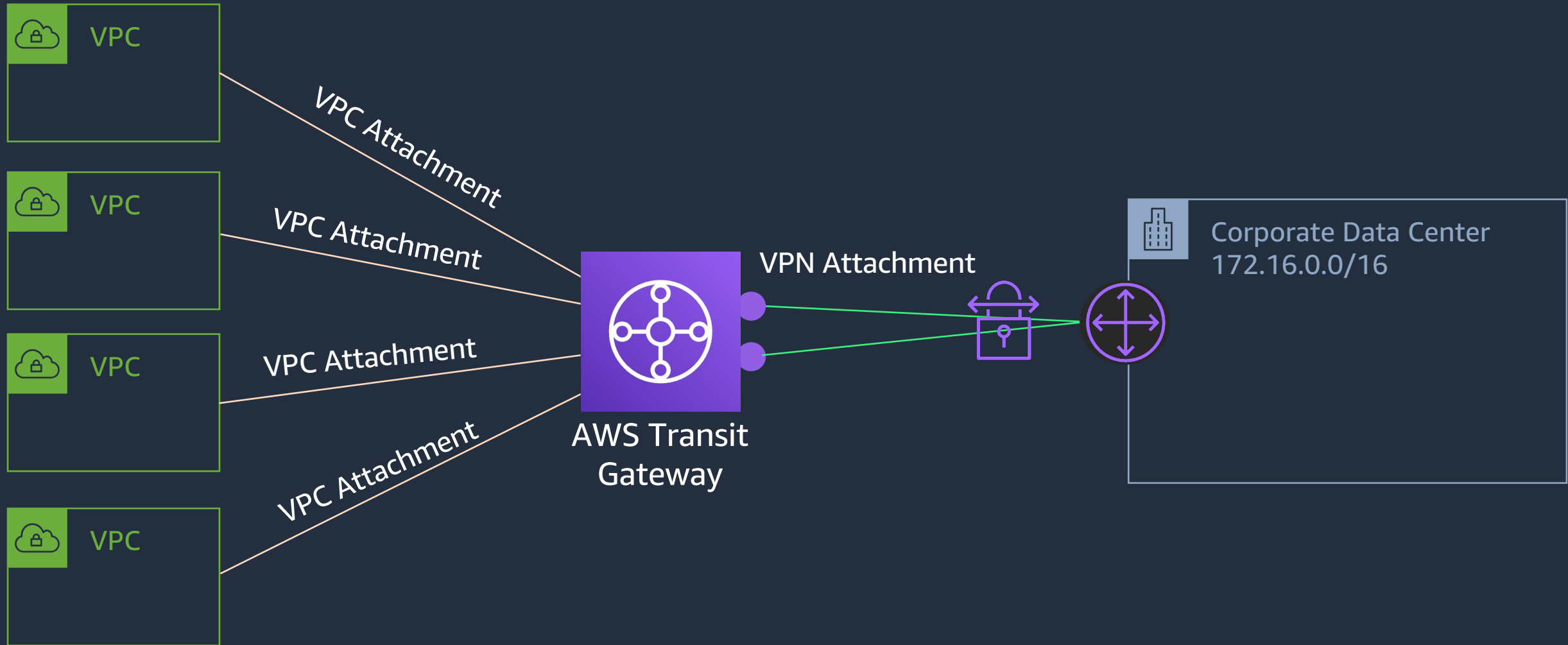
Connect multiple VPCs: VPC Peering at scale



Multiple VPCs access models – AWS Transit Gateway

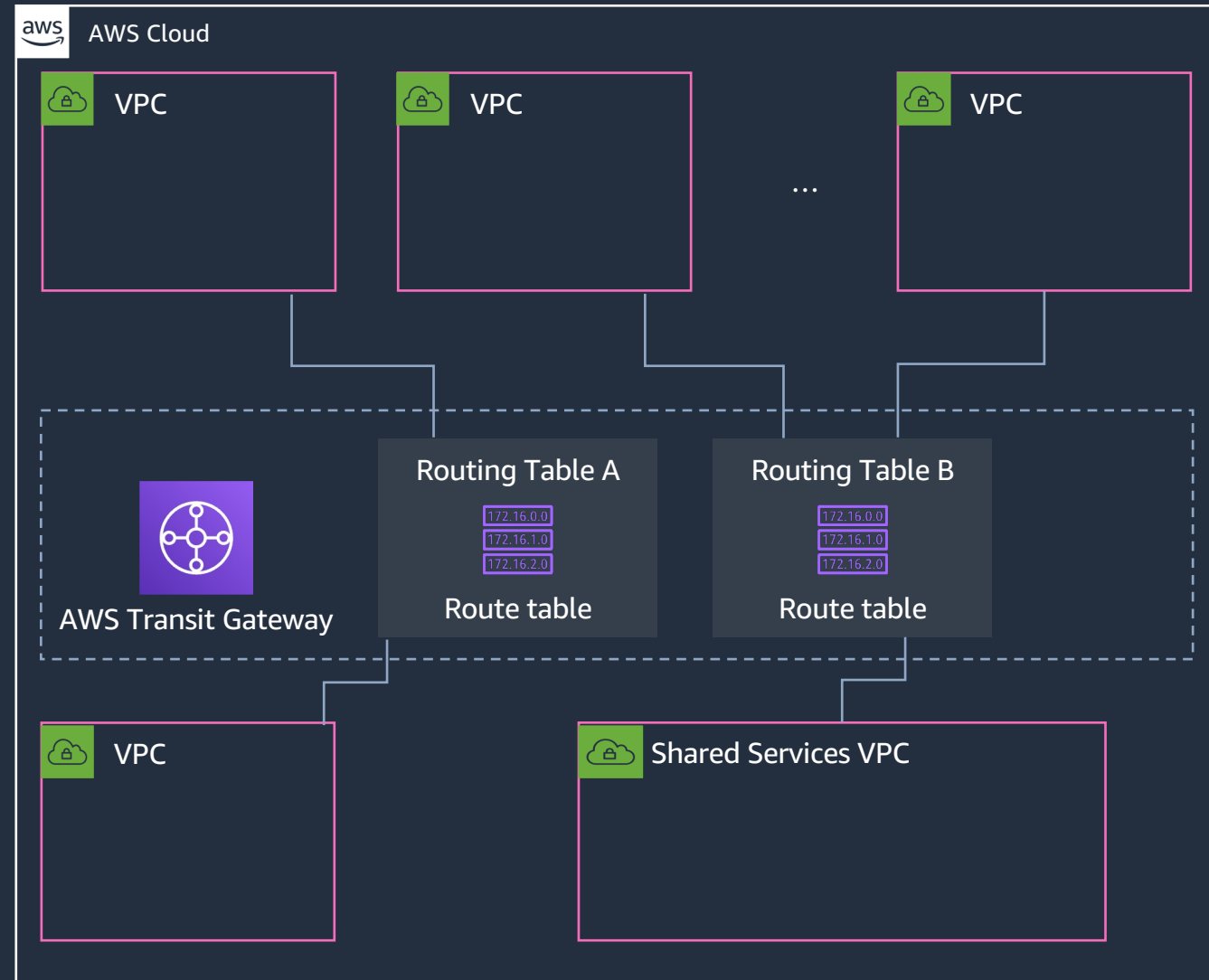


AWS Transit Gateway with AWS site-to-site VPN



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)

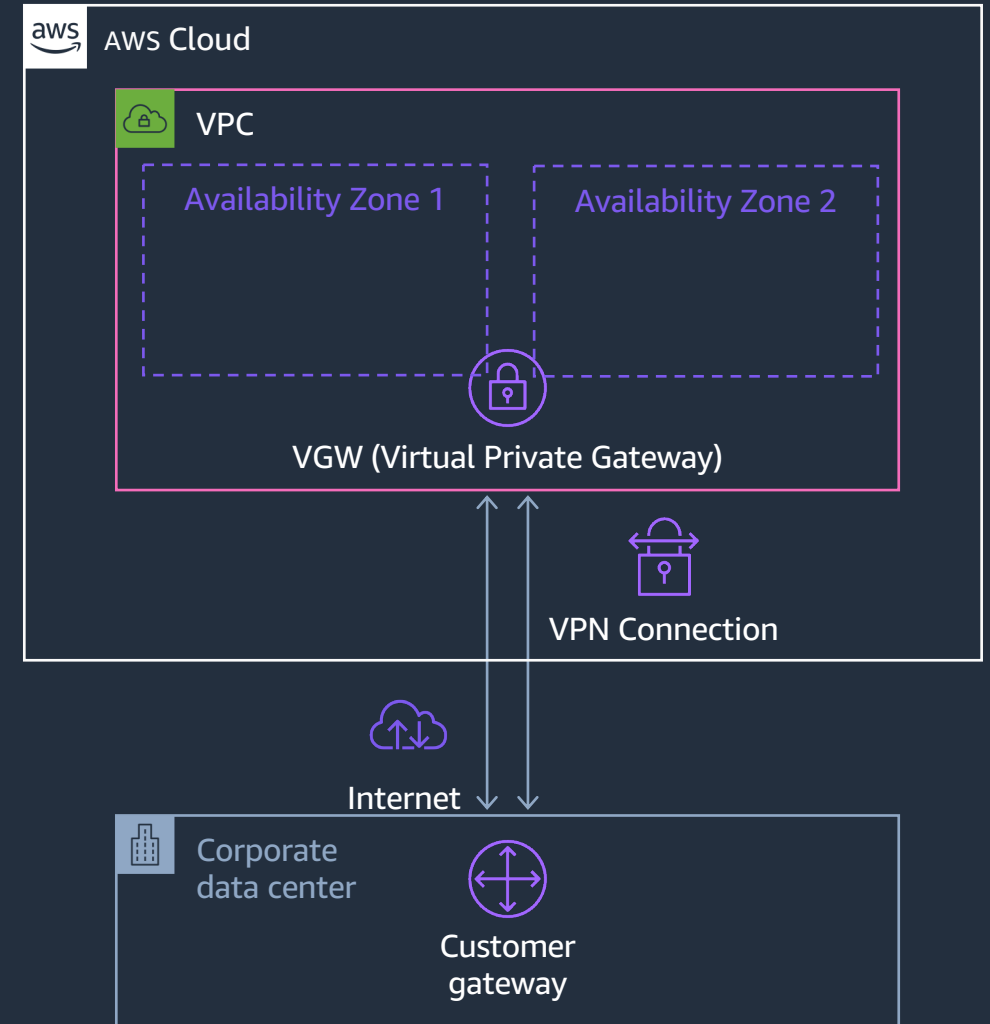


Connecting to On-premises



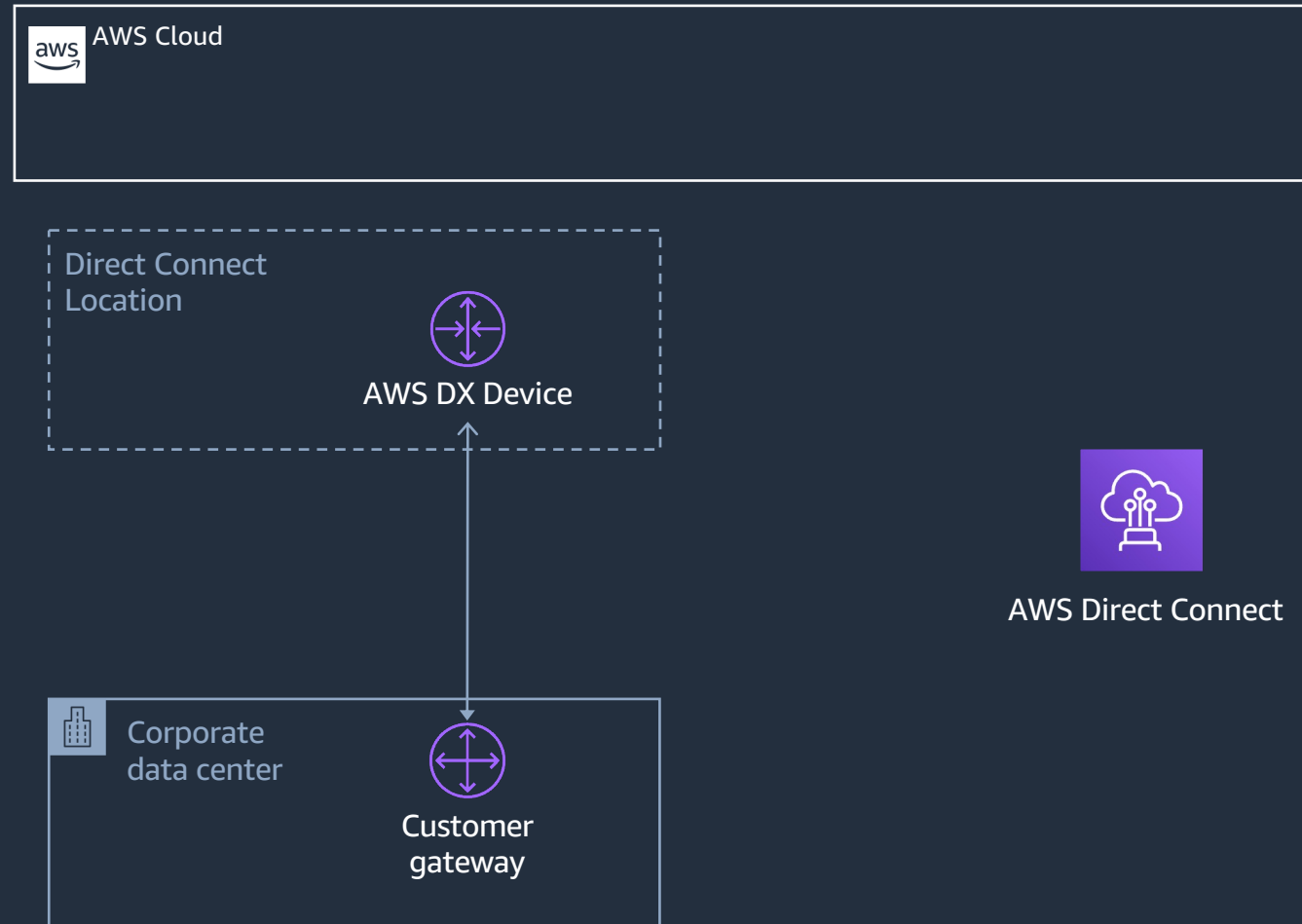
VPN to AWS: Virtual Private Gateway

- 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



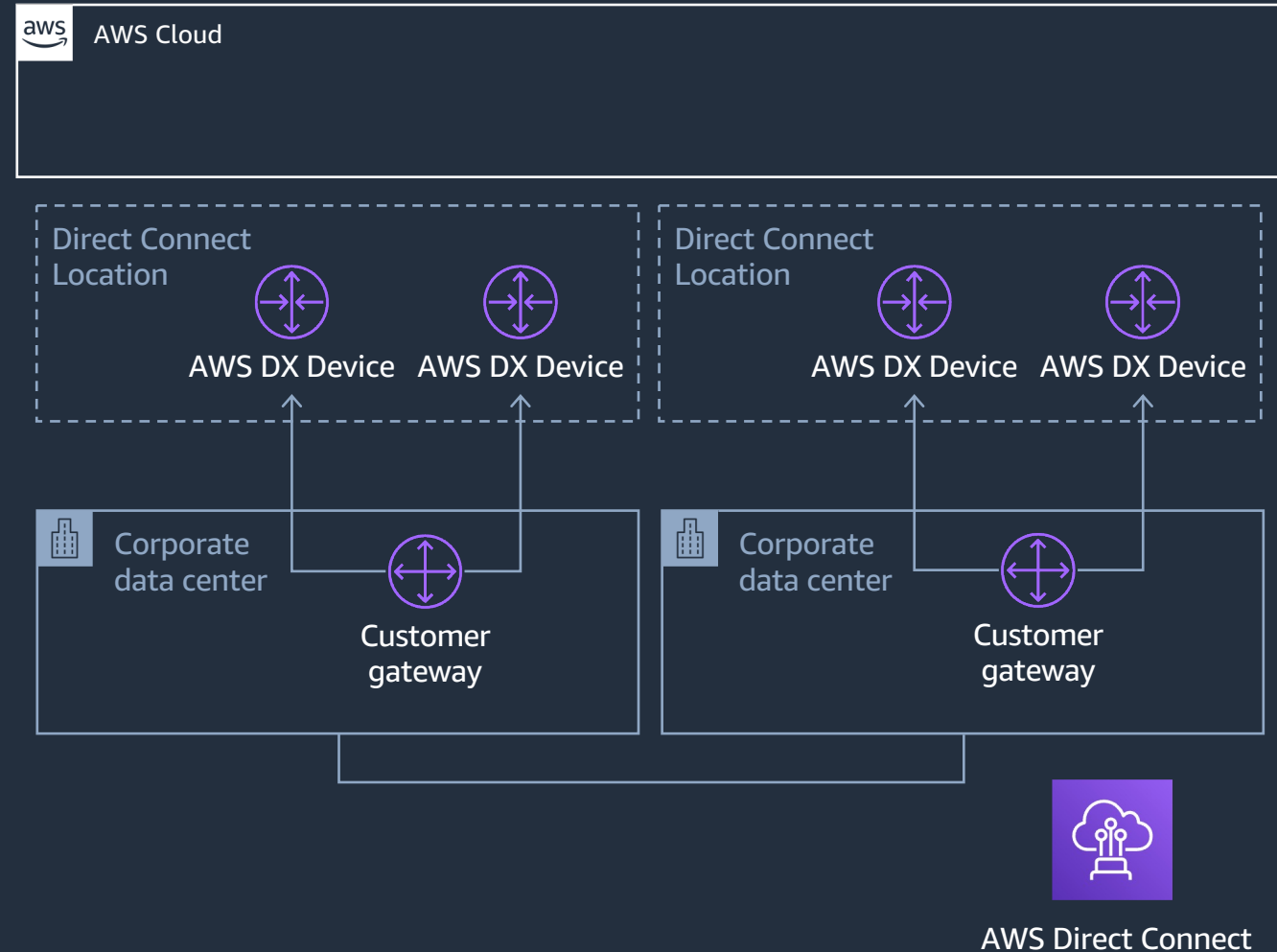
Dedicated link to AWS: AWS Direct Connect

- Dedicated network connection from your premises to AWS
- AWS Dedicated Local Zones
- Dedicated Connection (1,10 or 100 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 108 Direct Connection Locations across the globe



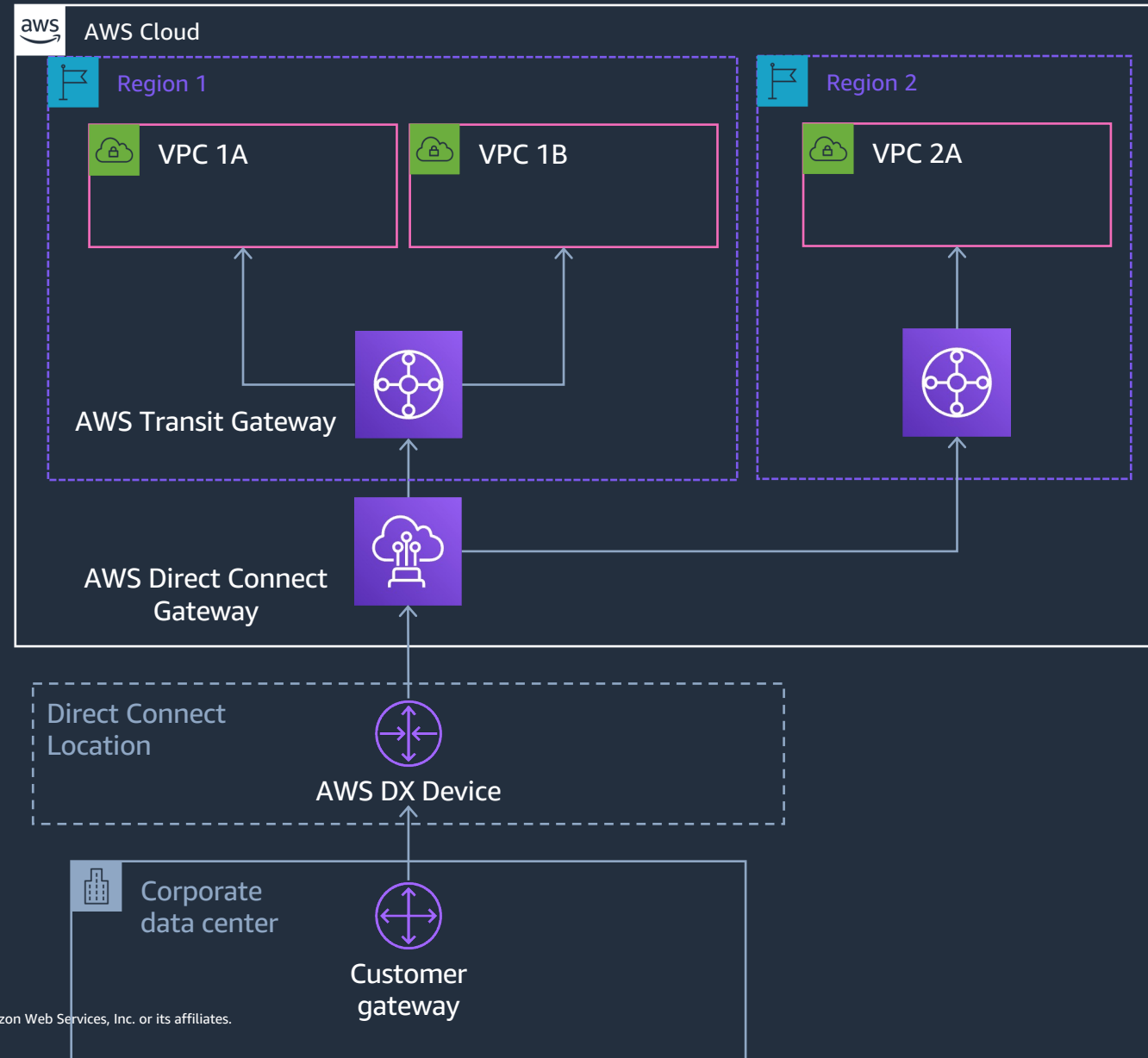
Dedicated link to AWS: AWS Direct Connect

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



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



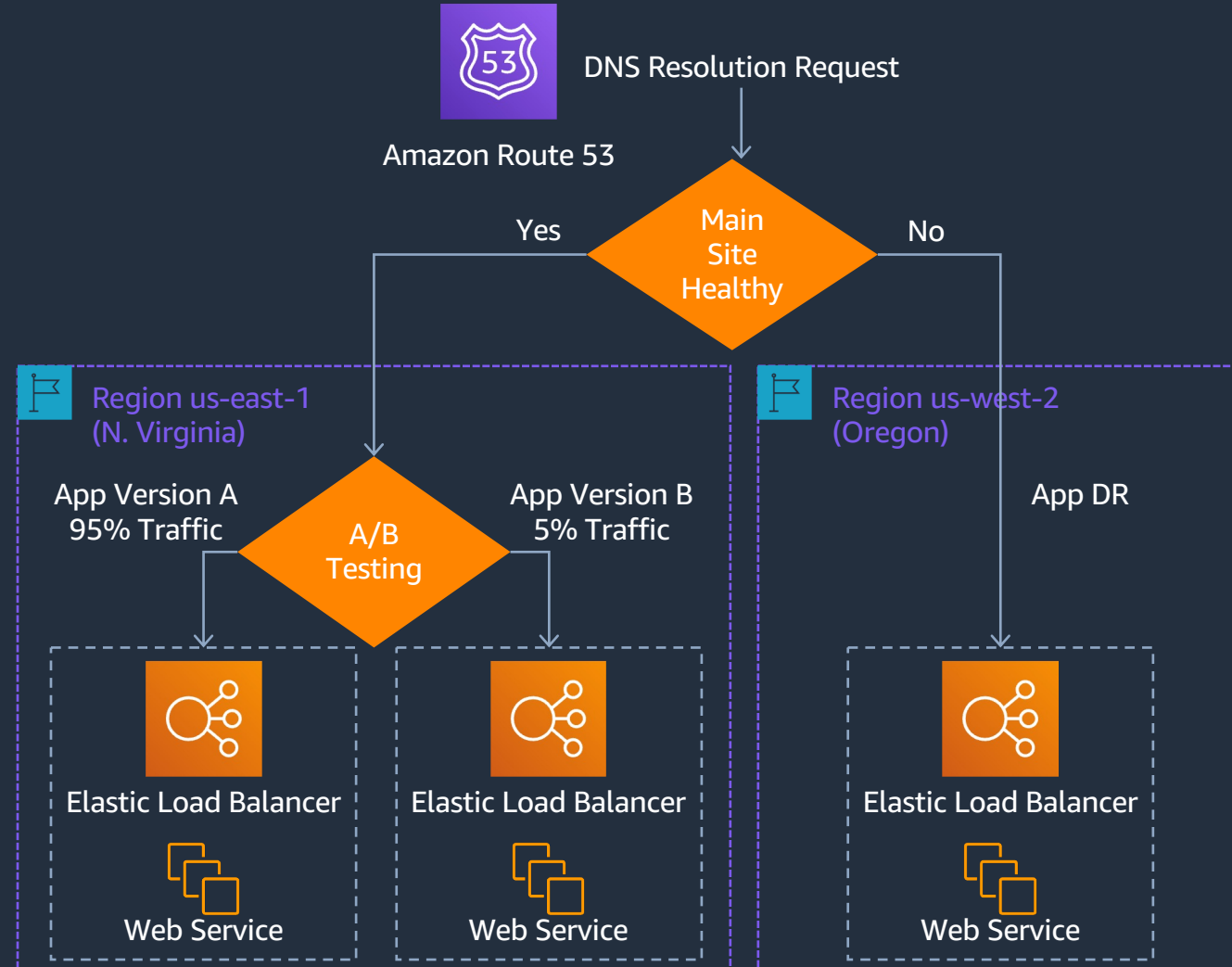
Domain Name Resolution



How to solve my Domain Names to IP Address?

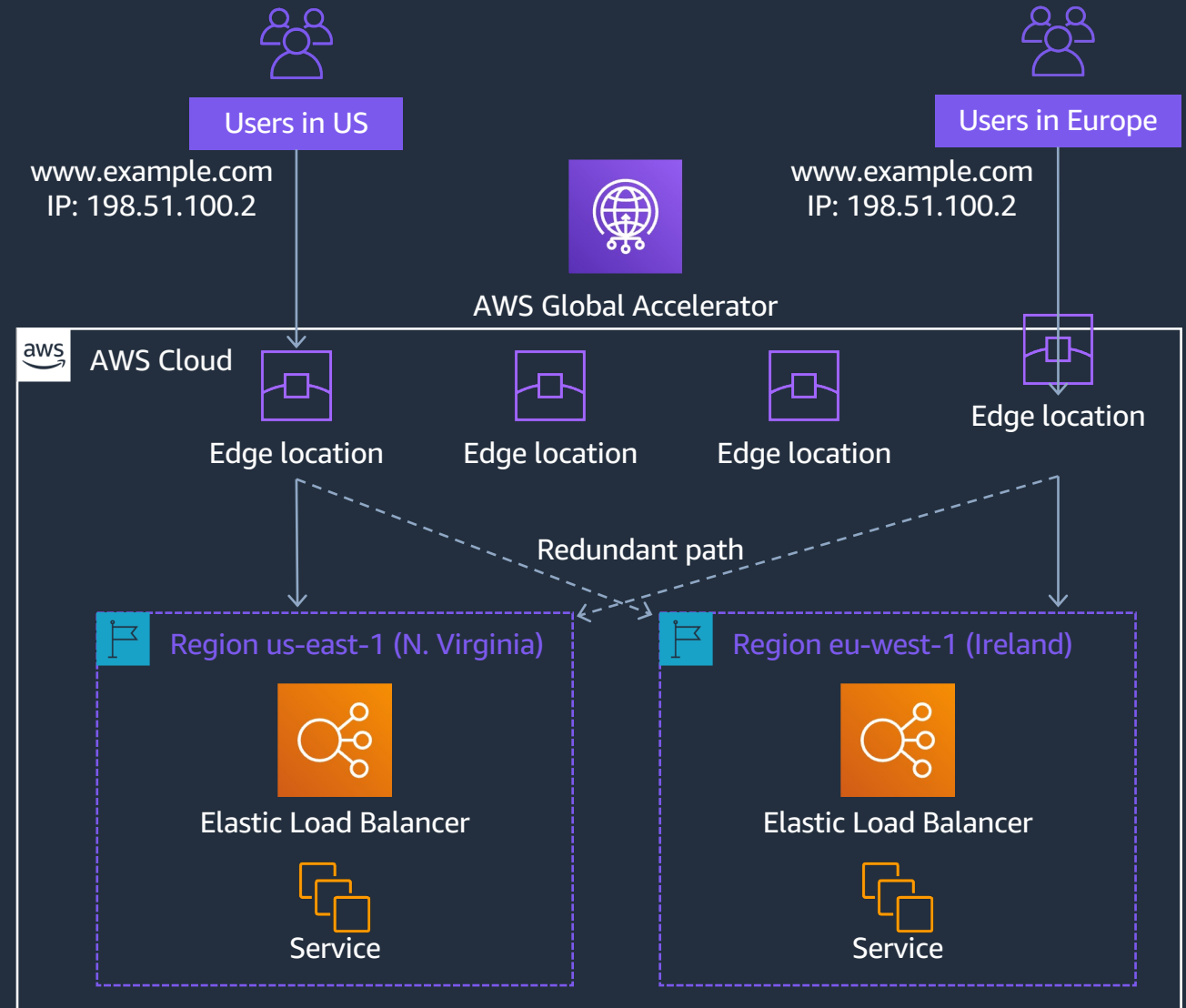
Amazon Route 53

- AWS DNS service
- Domain Registration
- Domain name resolution
- 100% availability SLA
- Global routing:
 - Health Checks
 - DNS Failover
 - Methods: Latency, Geography, IP/CIDR, Weighted Round Robin and Multivalue answer
- Zone Apex integration
- Public and private DNS
- Supports AWS-managed prefix lists for health checks



Anycast instead of DNS: 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)



More networking

- IPv6
- Egress-only Internet Gateway
- VPC flow logs
- Traffic Mirroring
- Elastic Network Interfaces (ENI)
- Instance types and Bandwidth
- ...

Questions?





Thank you!