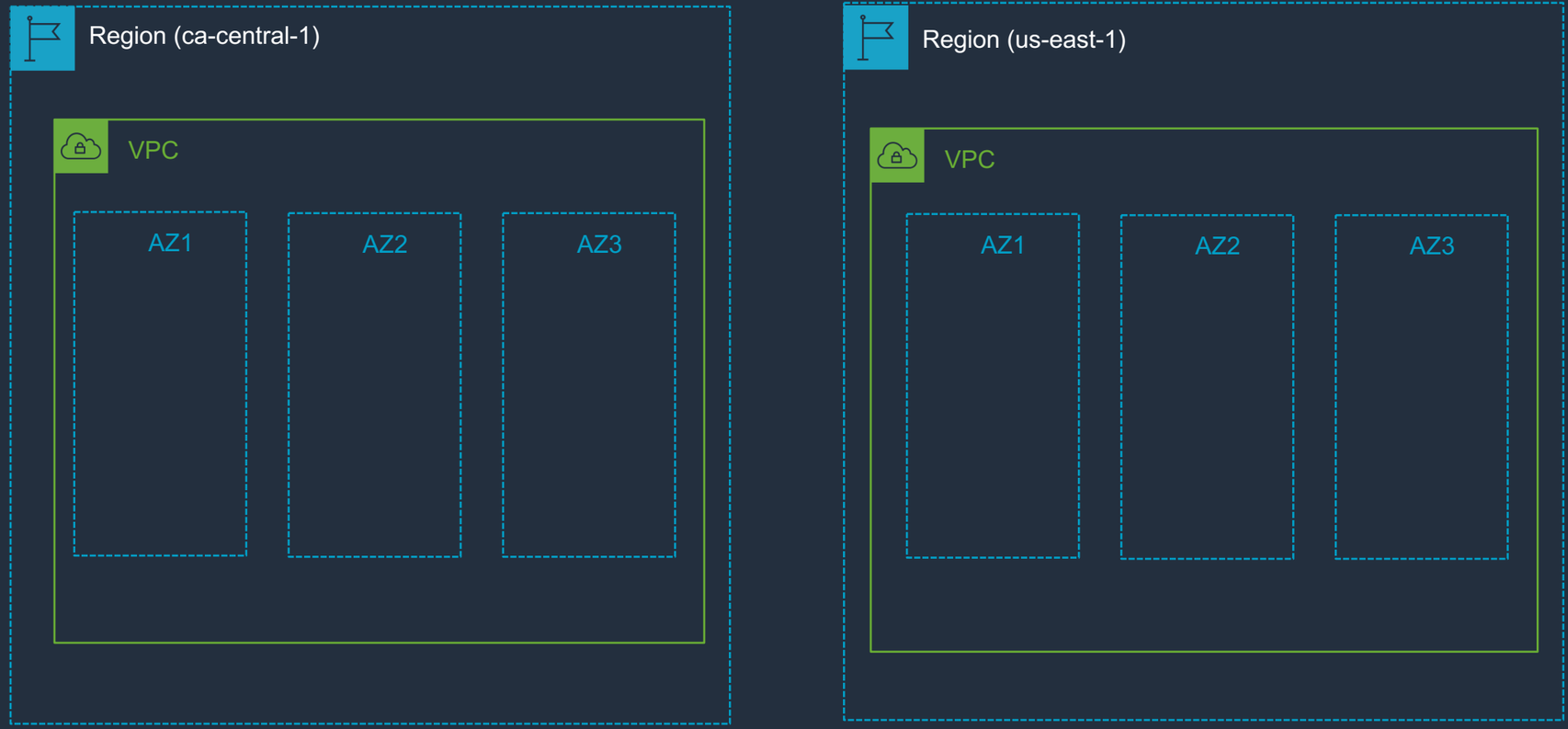
Networking in AWS

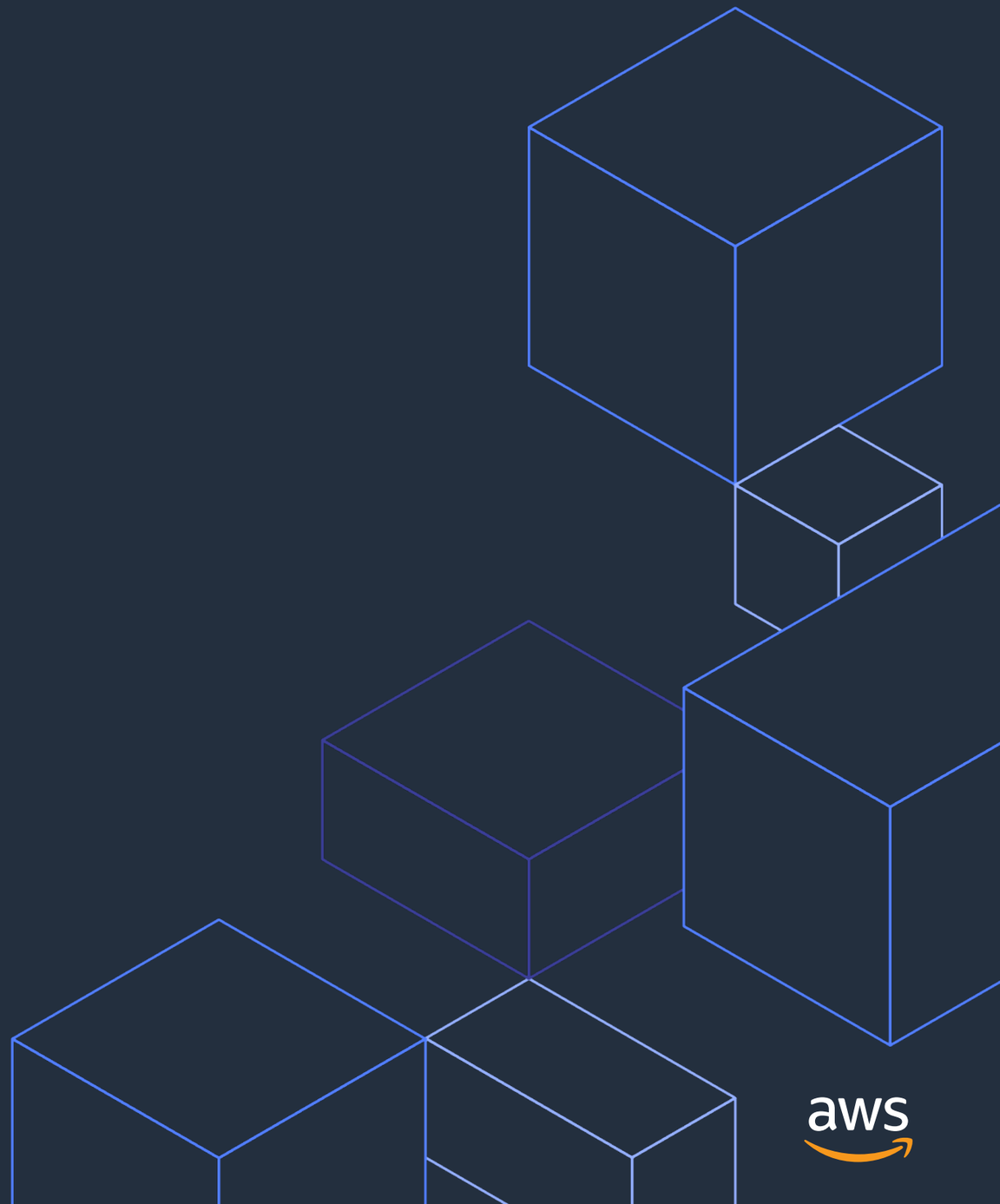
Agenda

- Amazon VPC
- VPC Building Blocks
- VPC Security
- VPC Connectivity Options
- Load Balancers
- Traffic Distribution

AWS Cloud

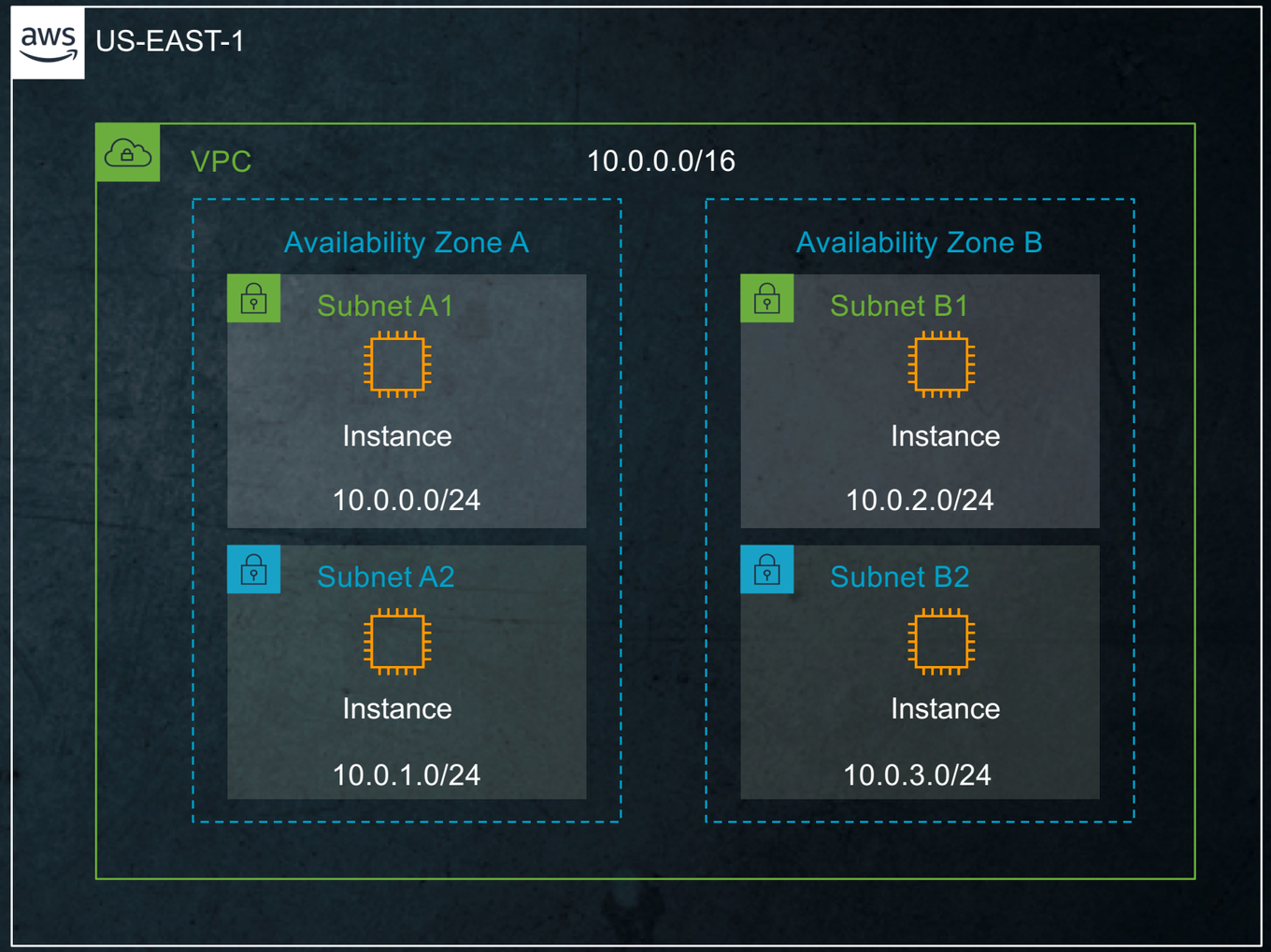


Amazon VPC



Amazon Virtual Private Cloud (VPC) overview

- Virtual network topology that you define
- Your own logically isolated section of AWS
- Complete control of your networking environment
  - IP ranges
  - Subnets
  - Routing tables
  - Gateways
- Multiple Connectivity Options
- Advanced Security Features



aws

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

aws

VPC Subnets

VPC CIDR
10.0.0.0/16 = 65,536 addresses

Note: AWS preserves 5 IP addresses from each VPC

- `10.0.0.0`: Network address.
- `10.0.0.1`: Reserved by AWS for the VPC router.
- `10.0.0.2`: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. For more information, see Amazon DNS Server.
- `10.0.0.3`: Reserved by AWS for future use.
- `10.0.0.255`: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

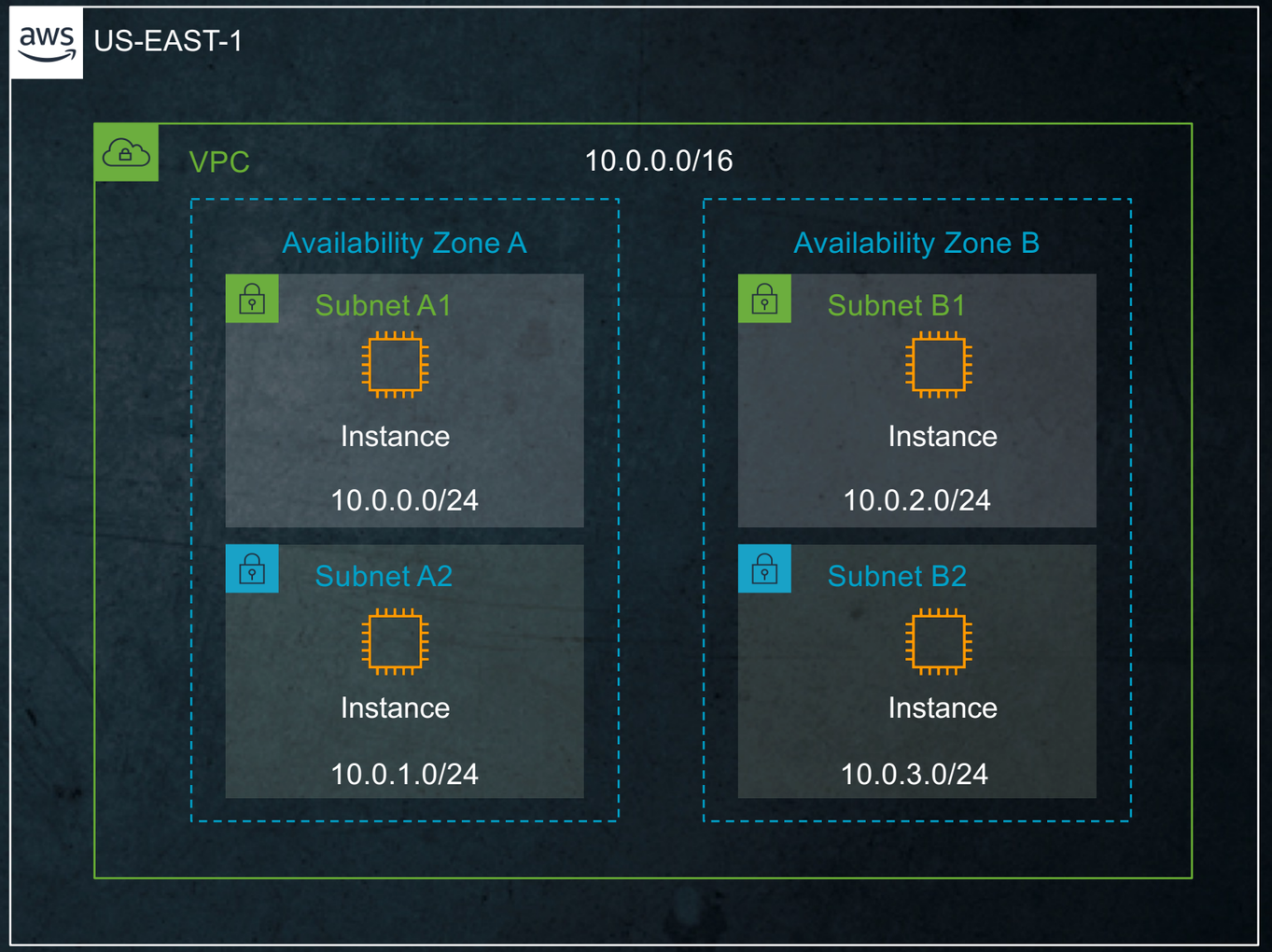
VPC IP addressing considerations

- 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
  - VPC CIDR can be between /16 and /28
  - Overlapping IP spaces = Routing issues in the future

aws

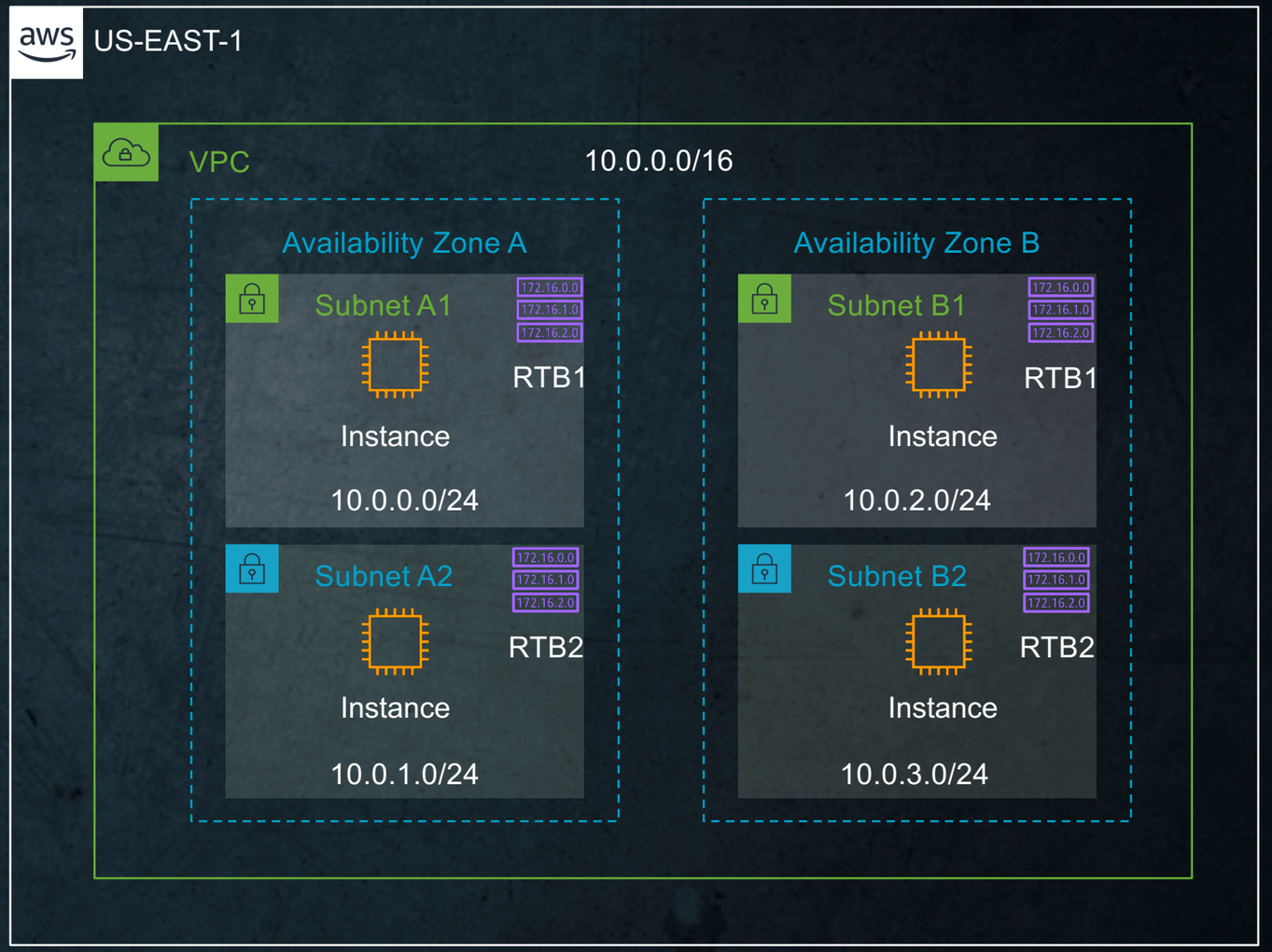
Subnets

- 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



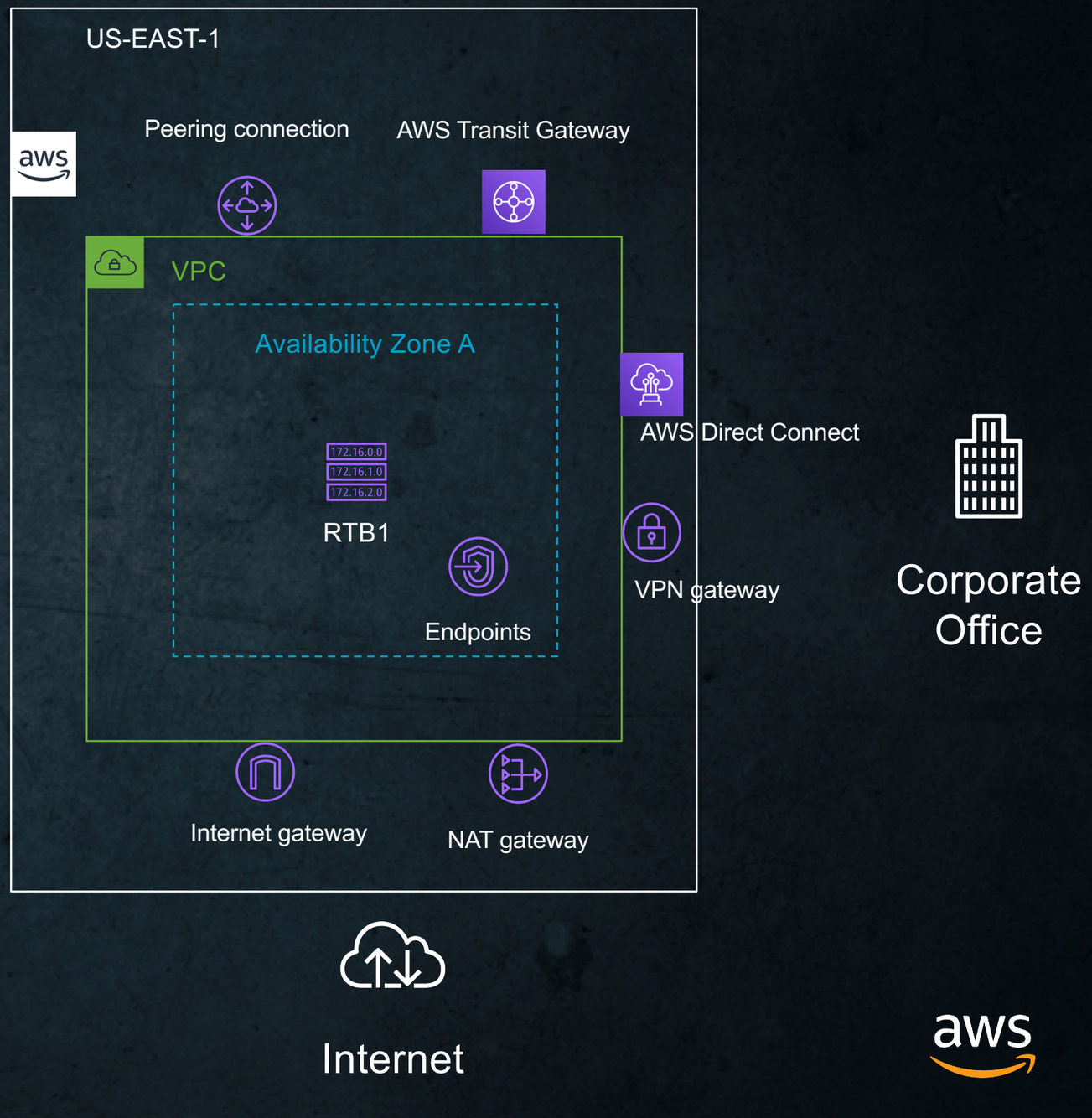
Routing tables

- 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

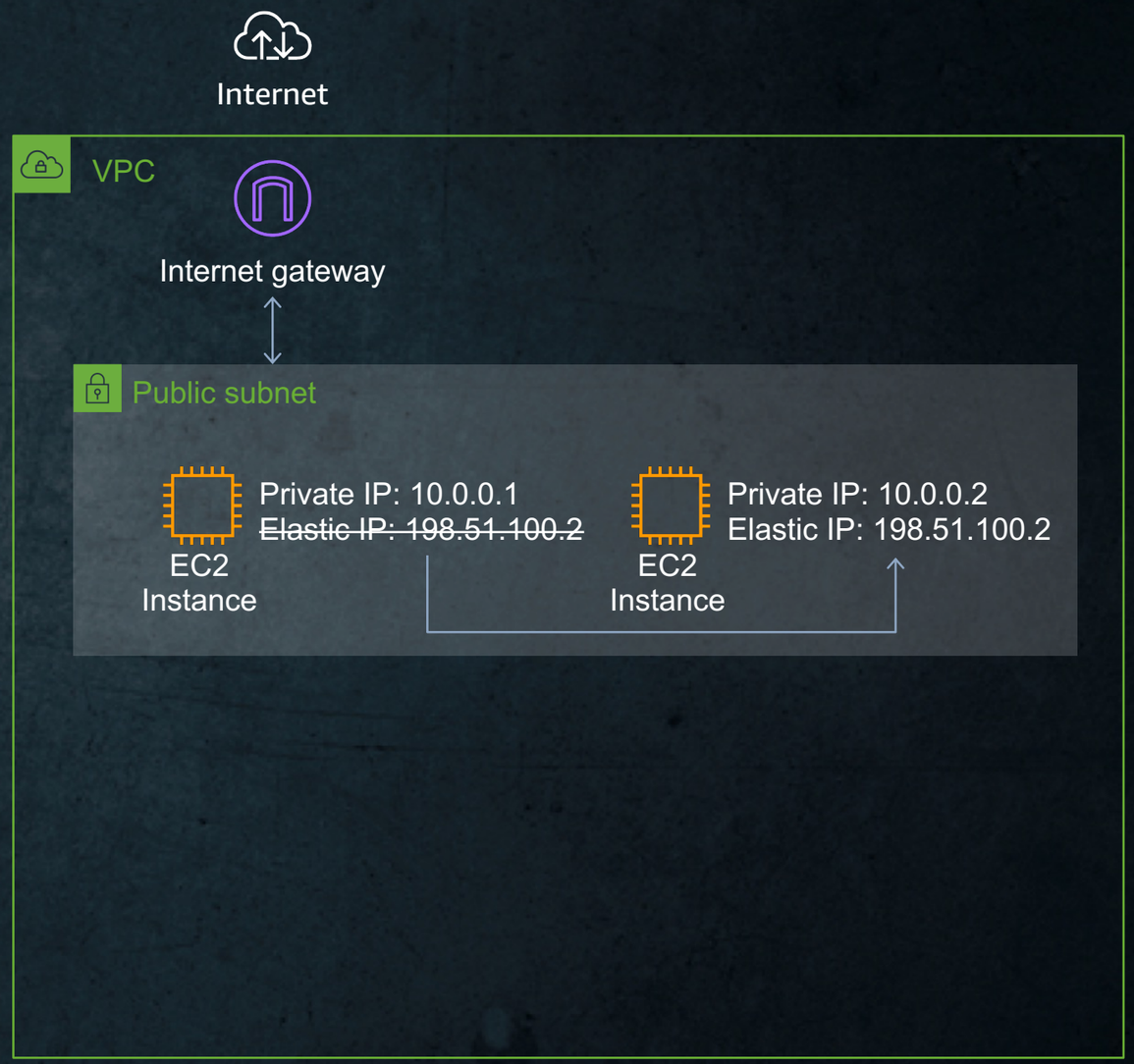


VPC to internet: Internet Gateway

- Horizontally scaled, redundant, highly available VPC component
- Connect your VPC Subnets to the Internet
- Must be referenced on the Route Table
- Performs 1:1 NAT between Public and Private IP Addresses
- No bandwidth limitation.

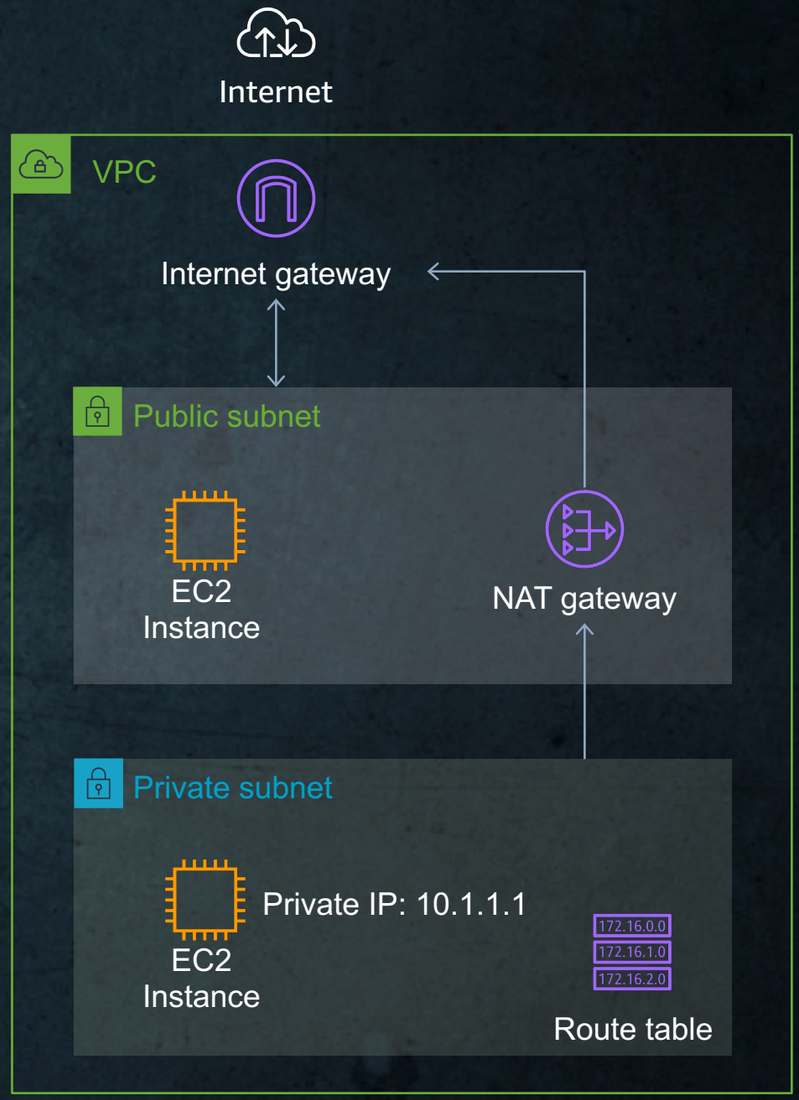
Public IP addressing: Elastic IP Address

- 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

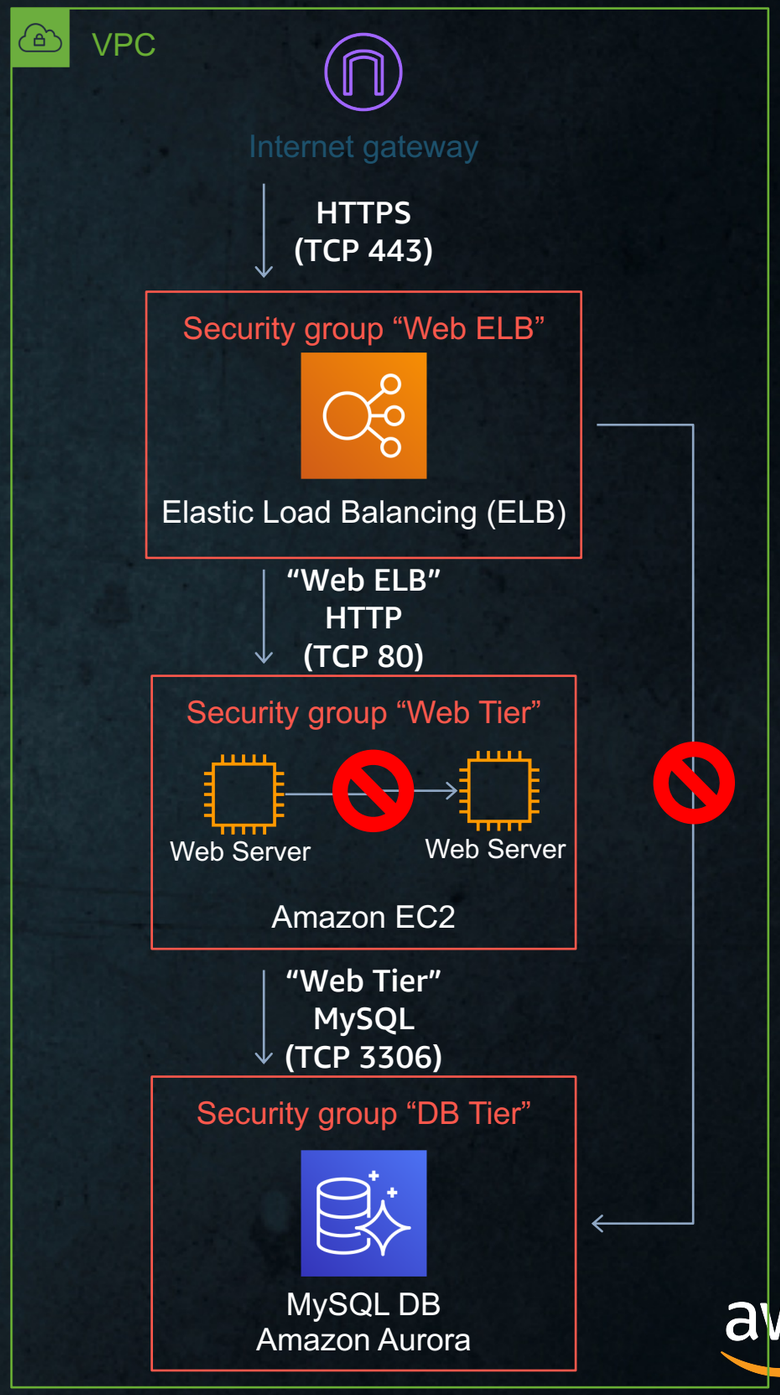


VPC Security

aws

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



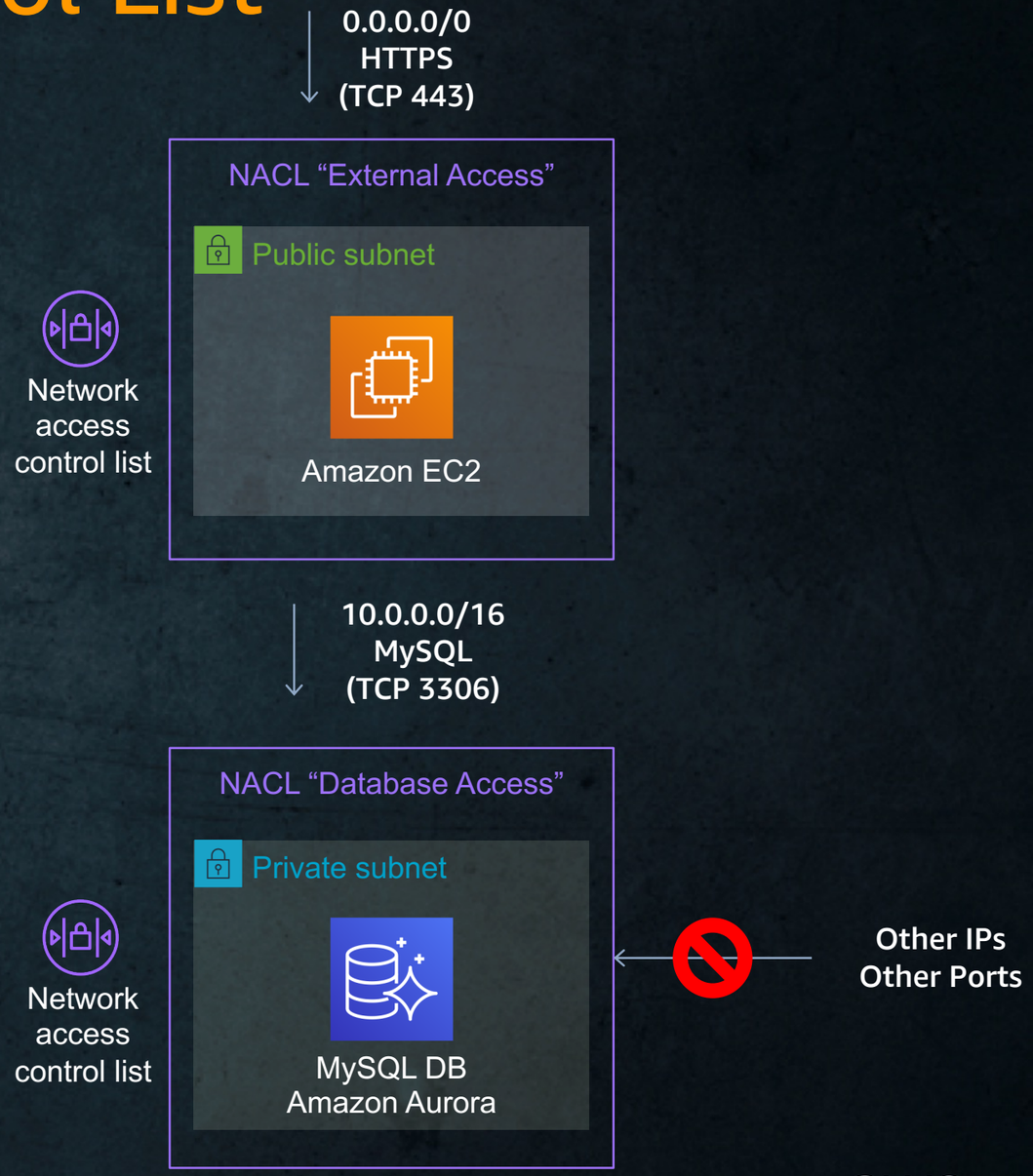
Security Group

Inbound			
Source	**Protocol**	**Port Range**	**Description**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from network interfaces (and their associated instances) that are assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Description**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

aws

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



Network Access Control List (NACL's)

Inbound					
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
101	All IPv6 traffic	All	All	::/0	ALLOW
*	All traffic	All	All	0.0.0.0/0	DENY
*	All IPv6 traffic	All	All	::/0	DENY
Outbound					
Rule #	**Type**	**Protocol**	**Port Range**	**Destination**	**Allow/Deny**
100	All traffic	All	All	0.0.0.0/0	ALLOW
101	All IPv6	All	All	::/0	ALLOW

aws

Poll # 1

What does VPC stands for:

A. Variable Public Cloud
B. Virtual Private Cloud
C. Virtuous Private Cloud
D. Virtual Potential Cloud

Poll # 2

In an AWS VPC subnet how many IPs are reserved?

A. 2

B. 3

C. 5

D. 7

Poll # 3

How many Internet Gateways can be attached to custom VPC?

A. 3
B. 1
C. Need AWS support ticket to attach more than 1
D. 1 per availability zone.

aws

Poll # 4

Which of the following offers the largest range of internal IP addresses?

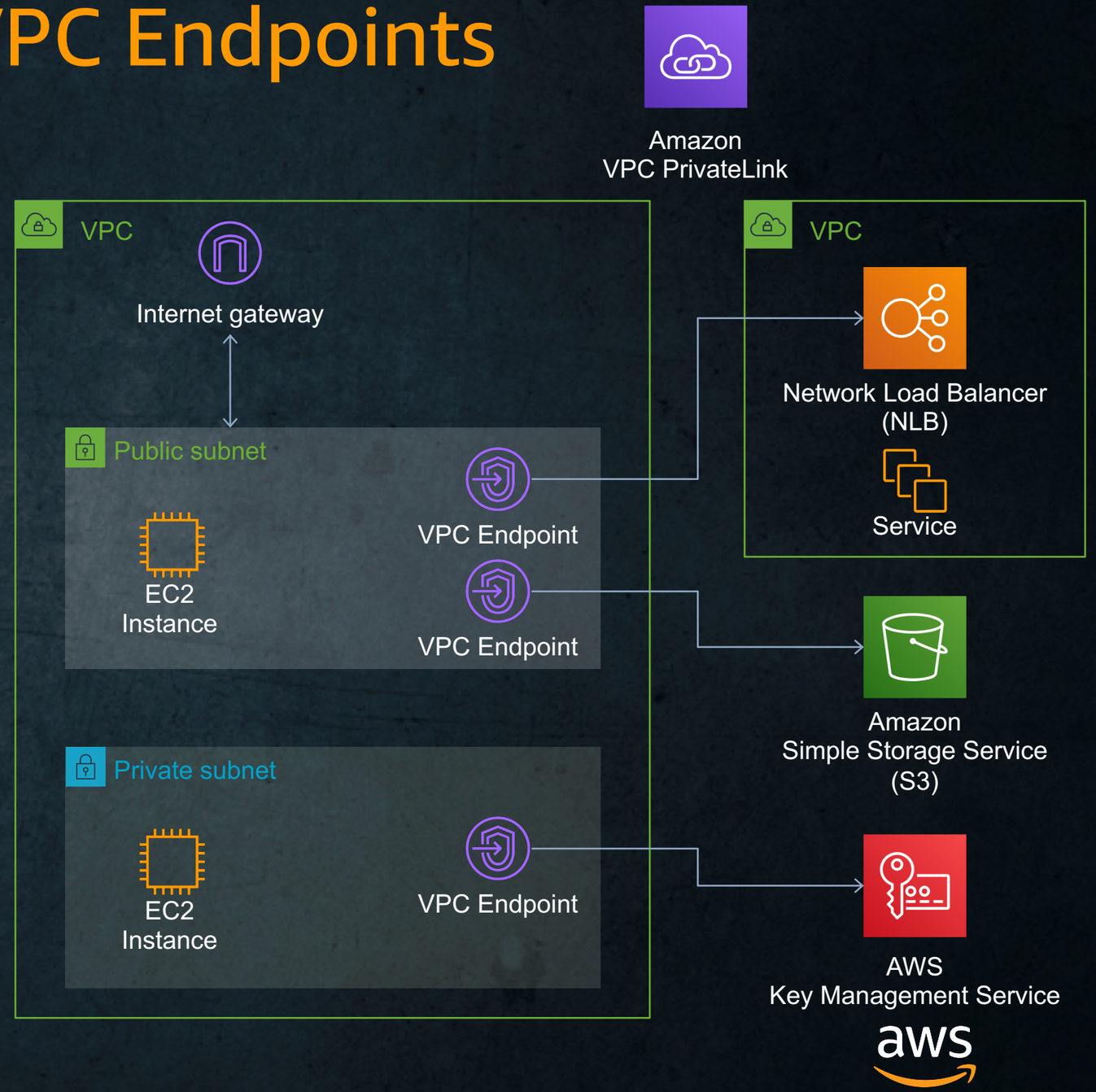
A. /20
B. /16
C. /24
D. /28

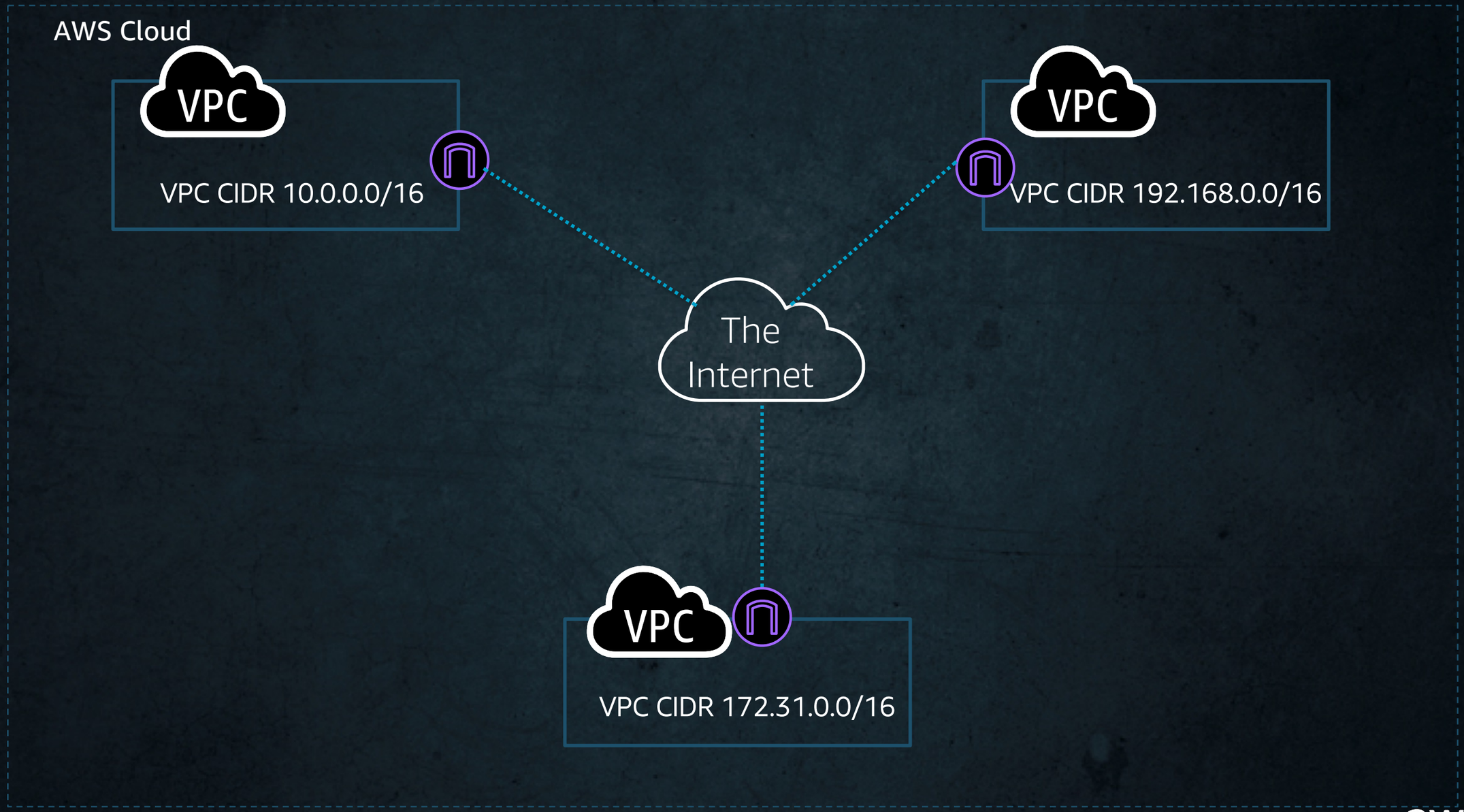
VPC Connectivity Options

aws

Stay on AWS network: VPC Endpoints

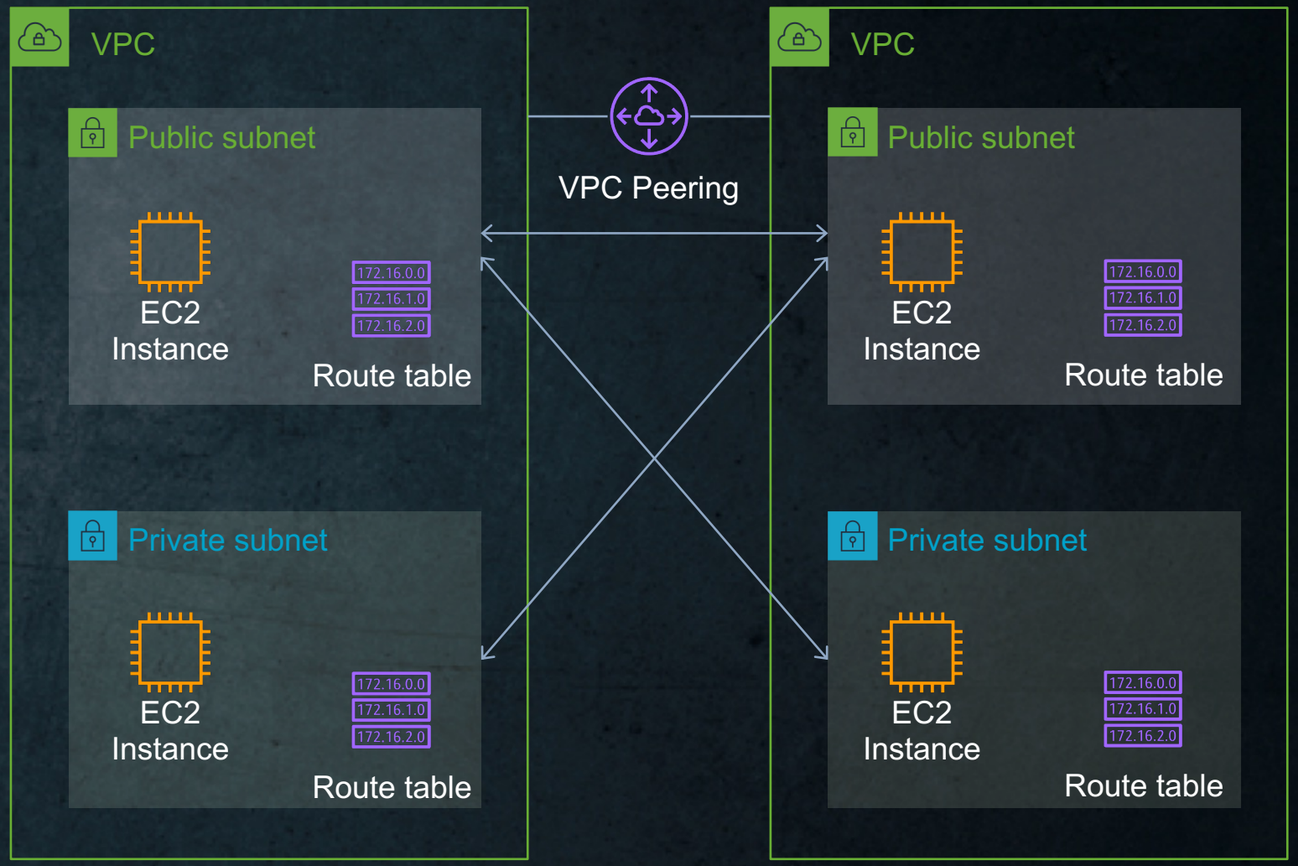
- Connect your VPC to:
  - Supported AWS services
  - VPC endpoint services powered by PrivateLink
- Doesn’t require public IPs or Internet connectivity
- Traffic does not leave the AWS network.
- Horizontally scaled, redundant, and highly available
- Robust access control



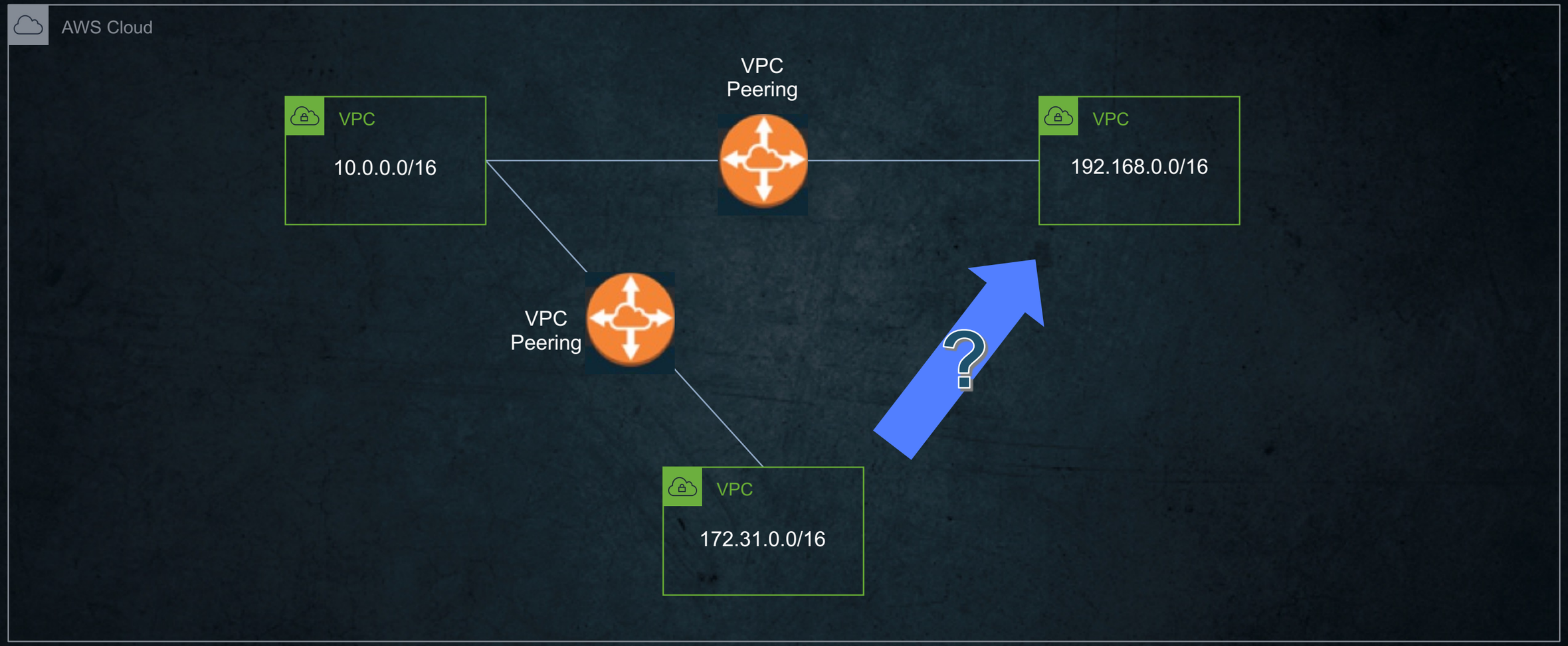


Connect multiple VPCs: VPC Peering

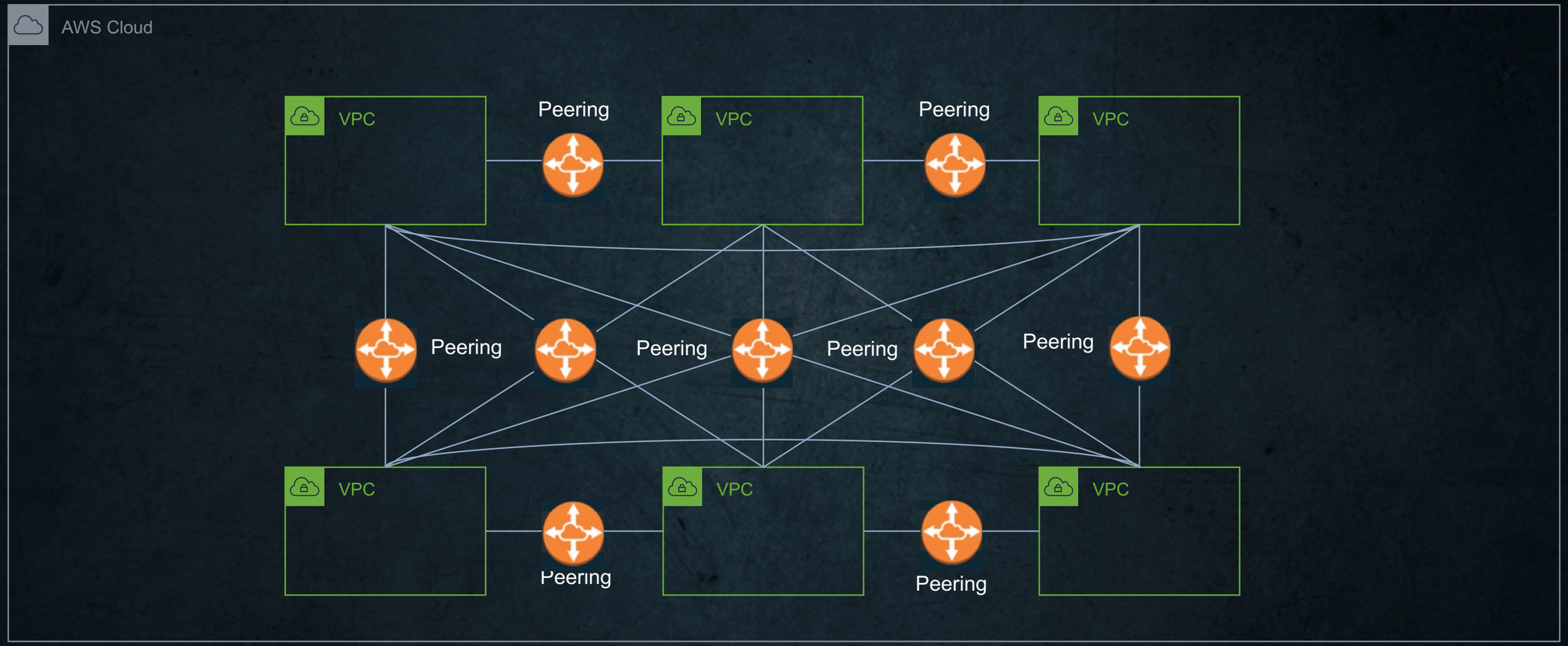
- Scalable and high available
- Supported between AWS accounts
- Supported across AWS Regions
- Bi-directional traffic
- Remote Security groups can be referenced
- Routing policy with Route Tables
    - Not all subnets need to connect to each other
- No overlapping IP addresses
- No transitive routing



Connect multiple VPCs: VPC Peering

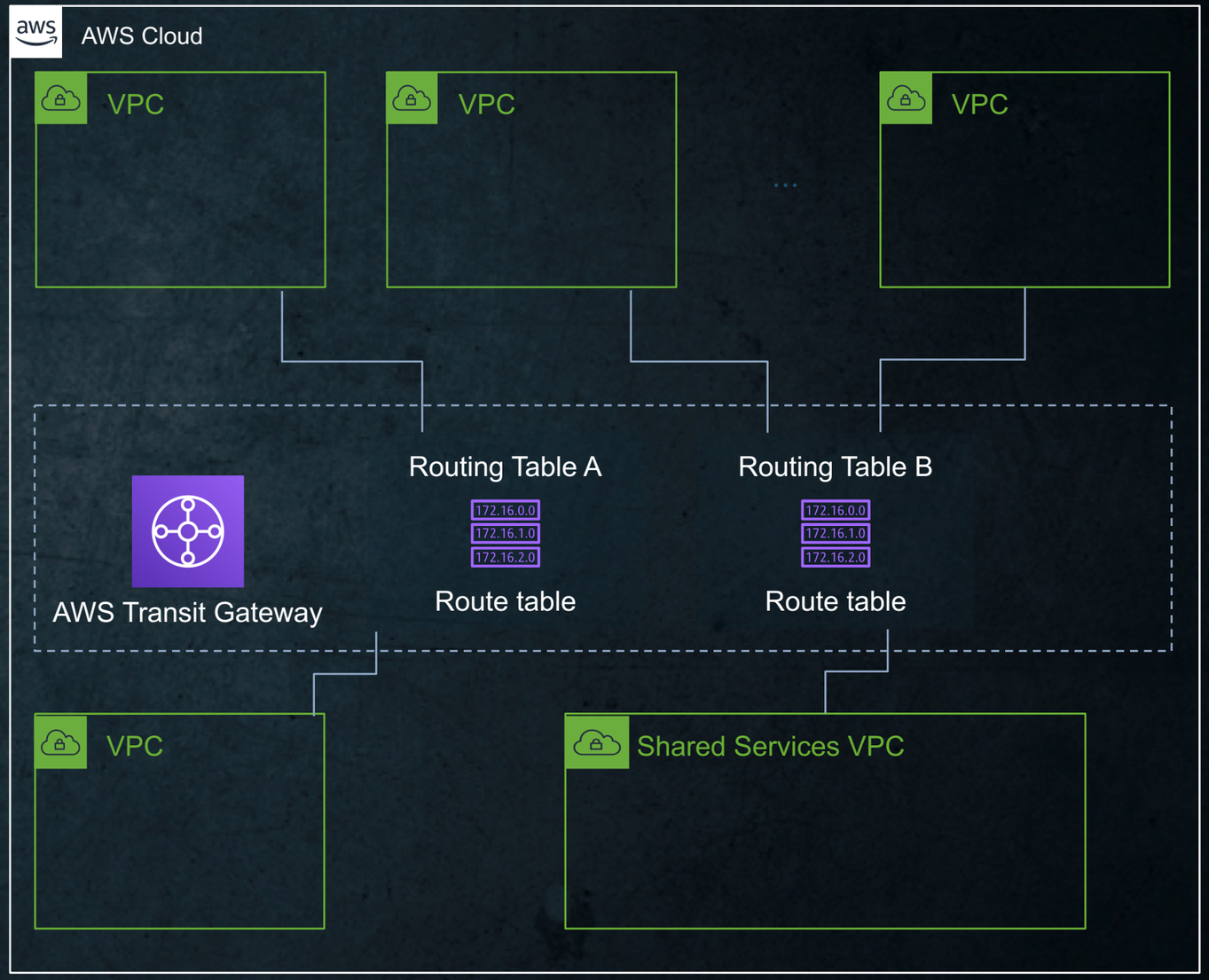


Connect multiple VPCs: VPC Peering at scale



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)



AWS Transit Gateway

Limit	Default
Number of AWS Transit Gateway attachments	5,000
Maximum bandwidth per VPN connection*	1.25 Gbps
Maximum bandwidth (burst) per VPC, Direct Connect gateway, or peered Transit Gateway connection	50 Gbps
Number of AWS Transit Gateways per account	5
Number of AWS Transit Gateway attachments per VPC	5
Number of routes	10,000
Number of Direct Connect gateways per AWS Transit Gateway	20

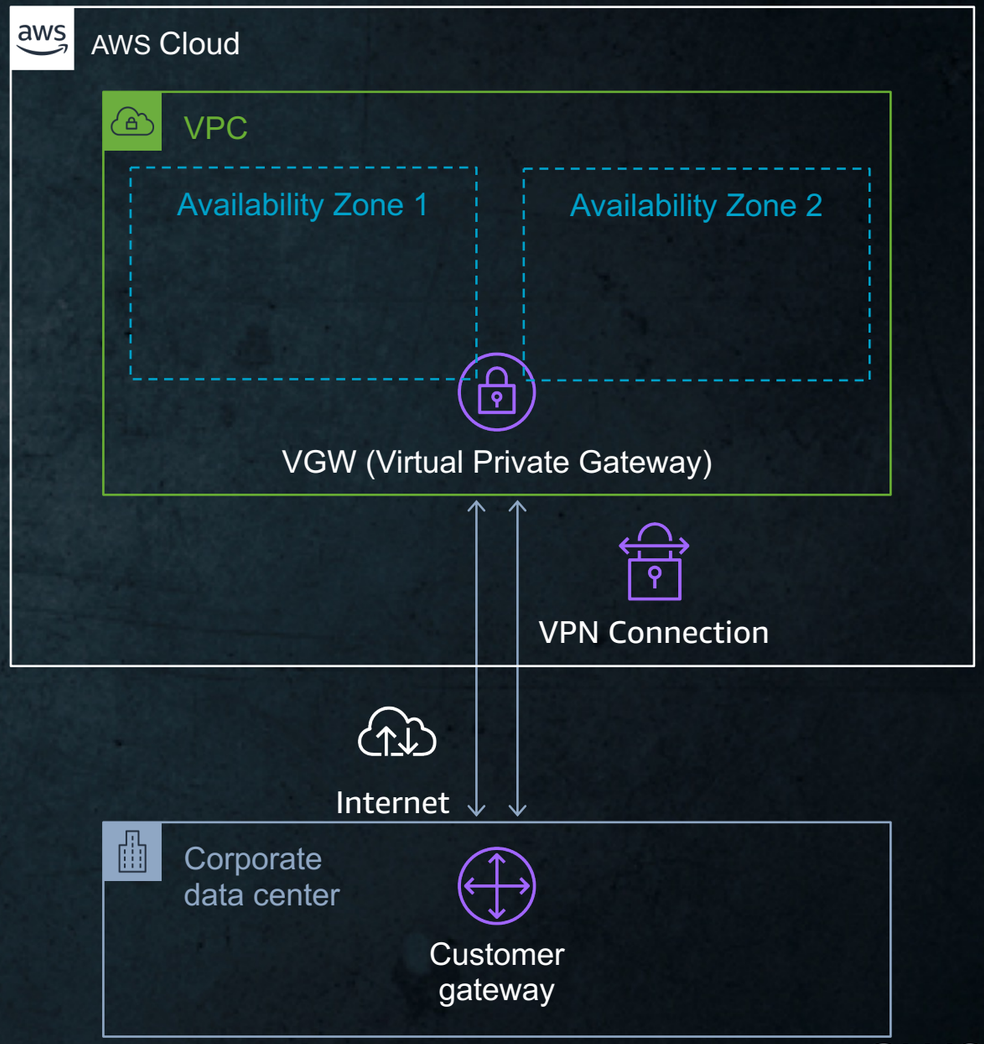
aws

Connect Your Data Center to AWS

aws

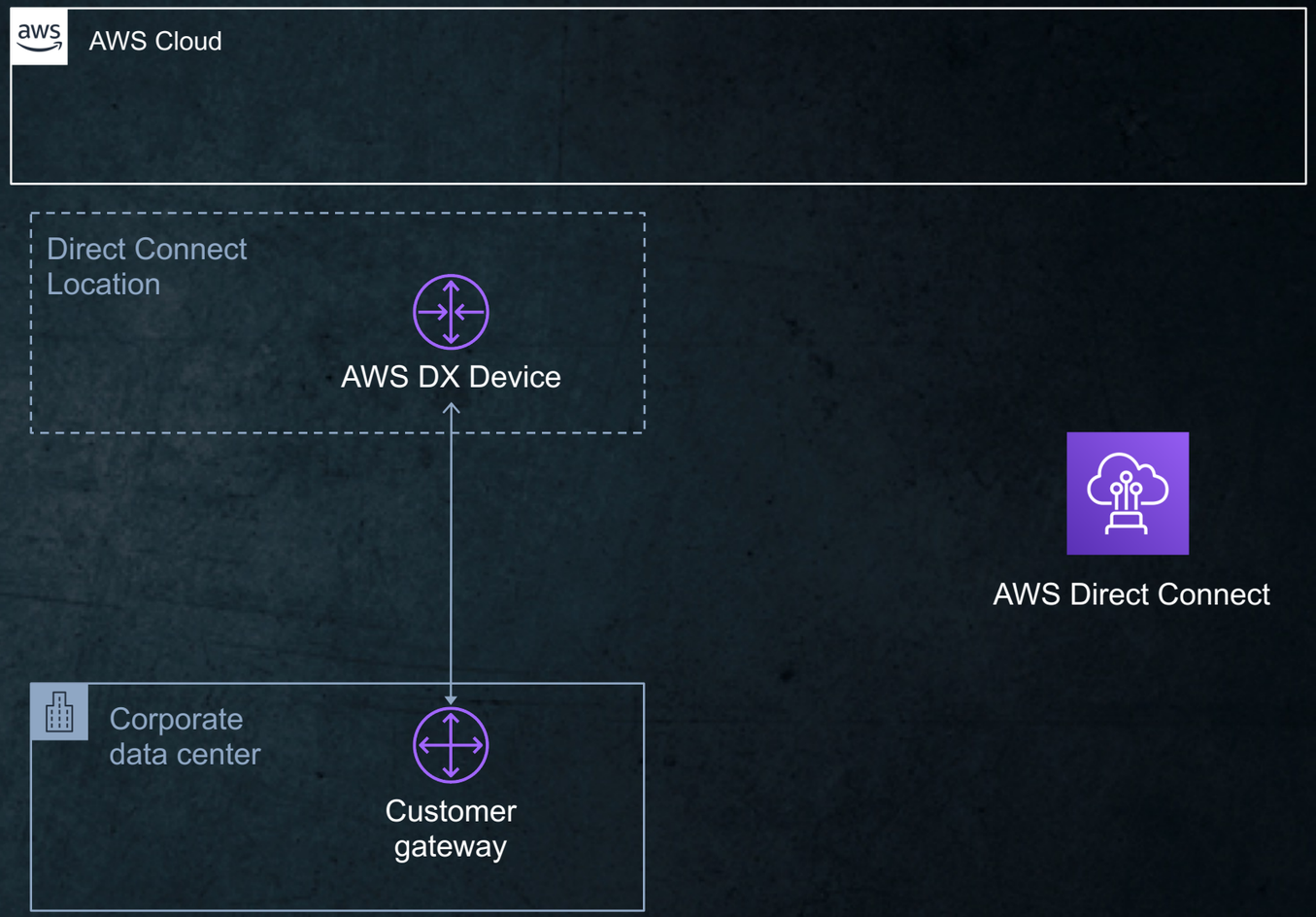
VPN to AWS: Virtual Private Gateway

- 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

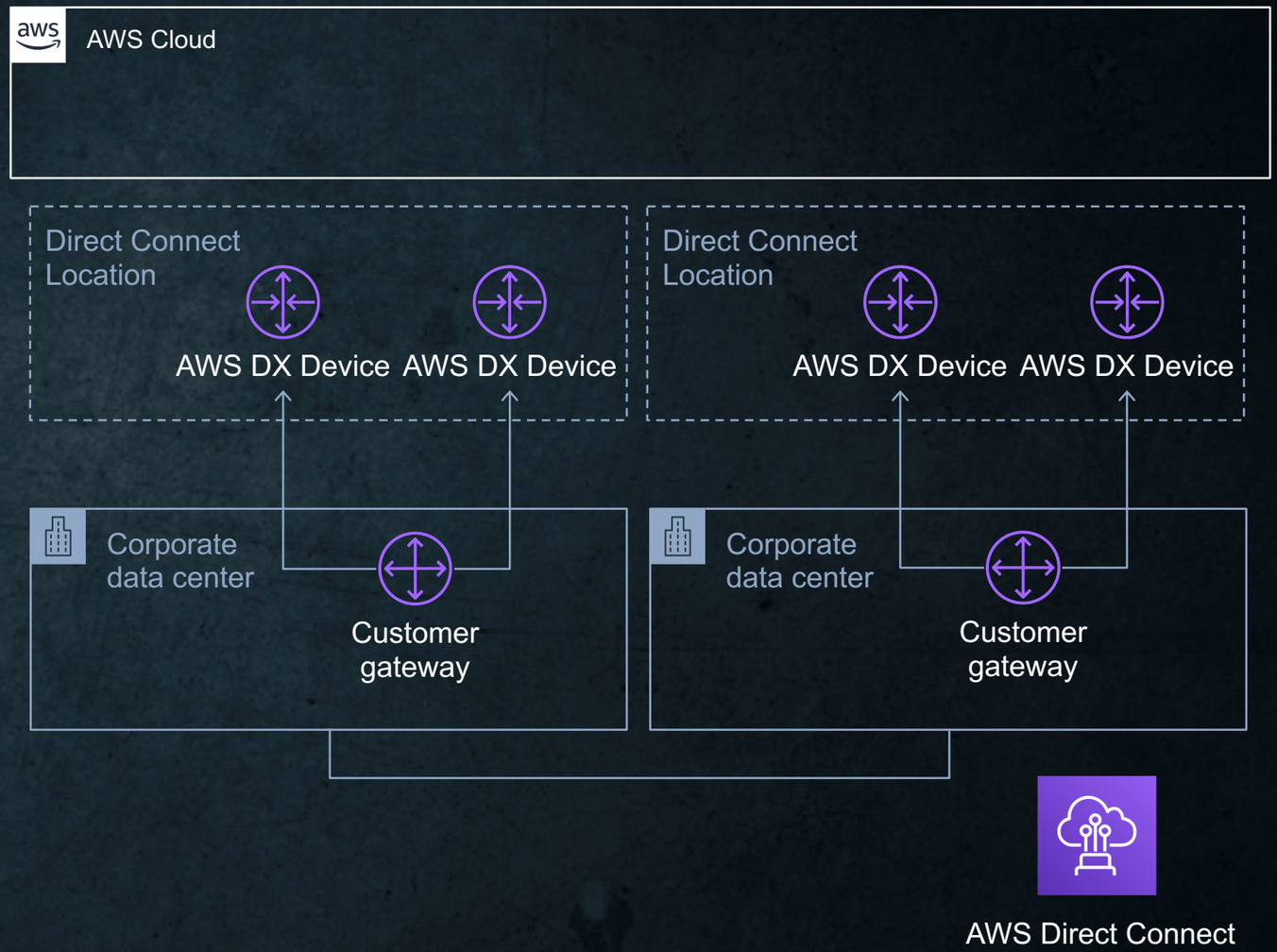
- Dedicated network connection from your premises to AWS
- Dedicated Connection (1 or 10 Gbps, Supports multiple VIFs)
- AWS Partner Hosted Connection (50 Mbps to 10 Gbps, Single VIF)
- Consistent Network Performance
  - Dedicated bandwidth
  - Low latency
- Reduced egress data charges
- Connect to 97+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



AWS Direct Connect

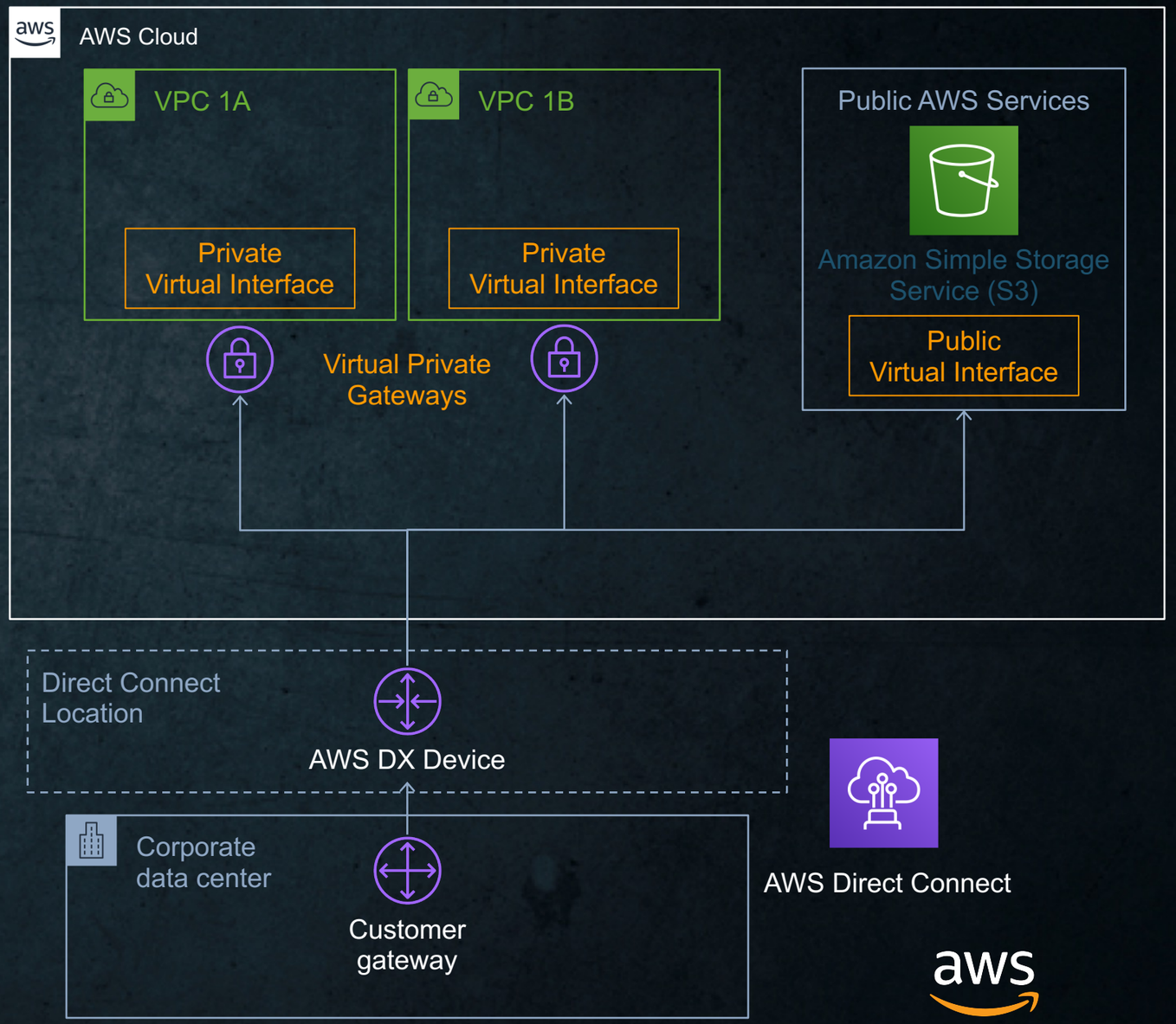
Dedicated link to AWS: AWS Direct Connect

- 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



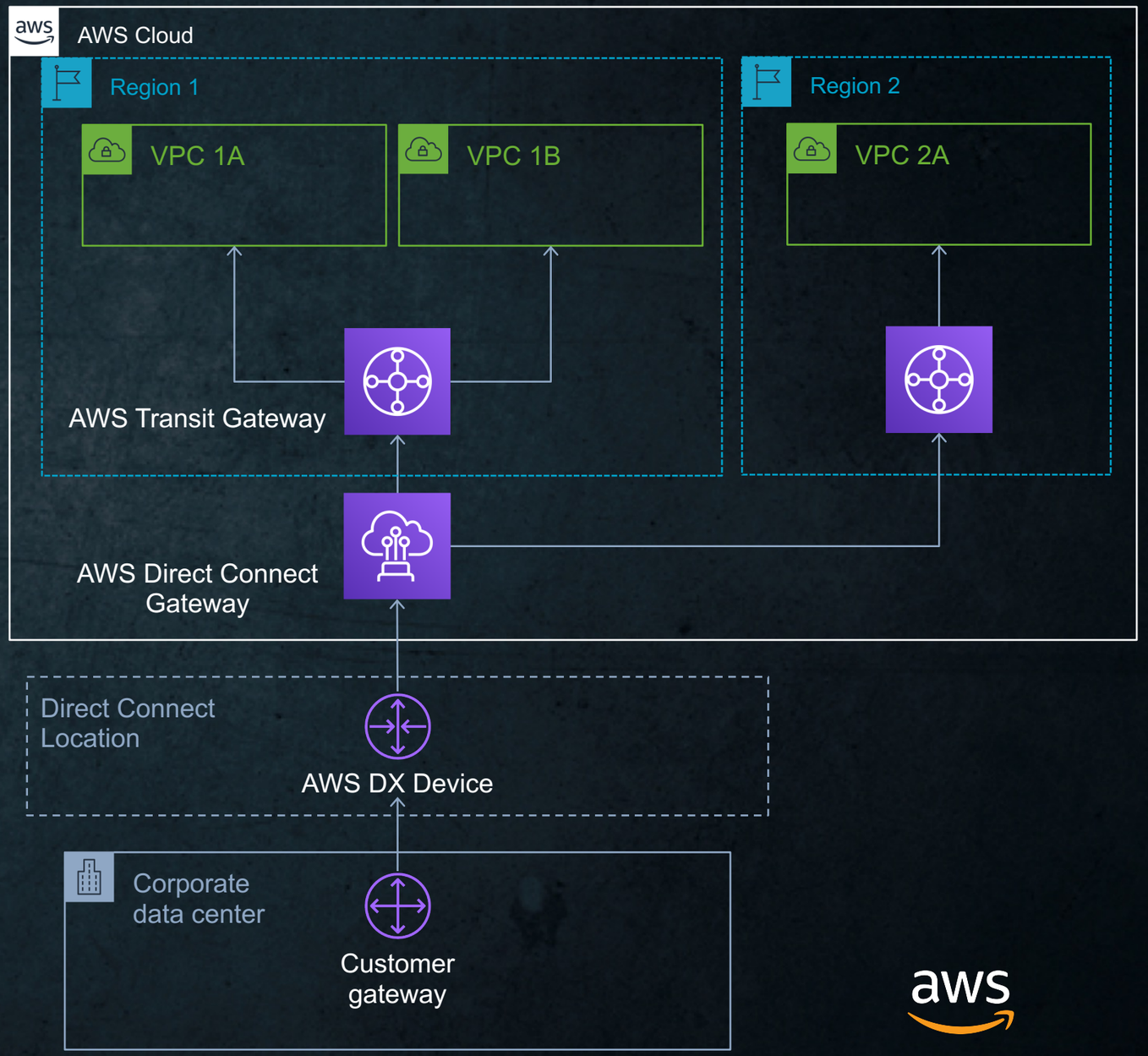
Dedicated link to AWS: AWS Direct Connect

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



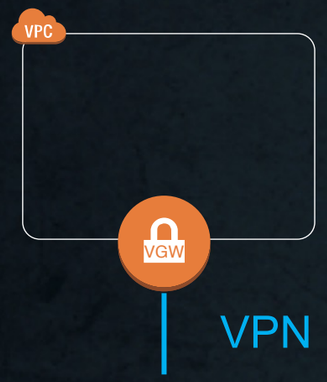
Connect at global scale: DX Gateway + Transit Gateway

- 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



Connecting to on-premises

Virtual Private Gateway VPN

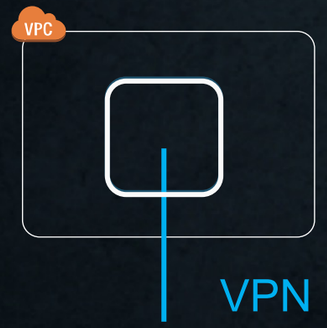


- Per VPC
- 1.25 Gbps per tunnel
- Encrypted in transit

AWS Direct Connect

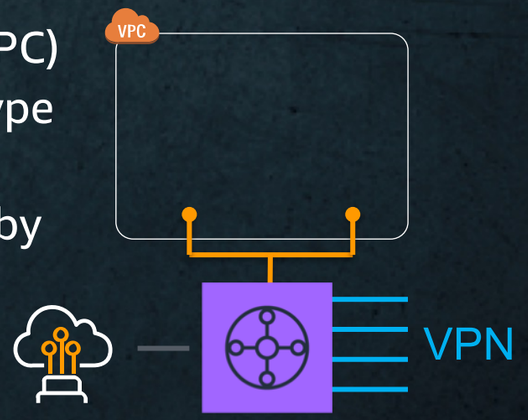
- Per VPC (50 per port)
- Multiple VPCs with DX gateway
- No bandwidth restraint

Amazon EC2 Customer VPN



- Per VPC or multiple (Transit VPC)
- Bandwidths vary by instance type
- AWS Marketplace options
- Scalability is generally limited by management complexity

AWS Transit Gateway VPN / DX



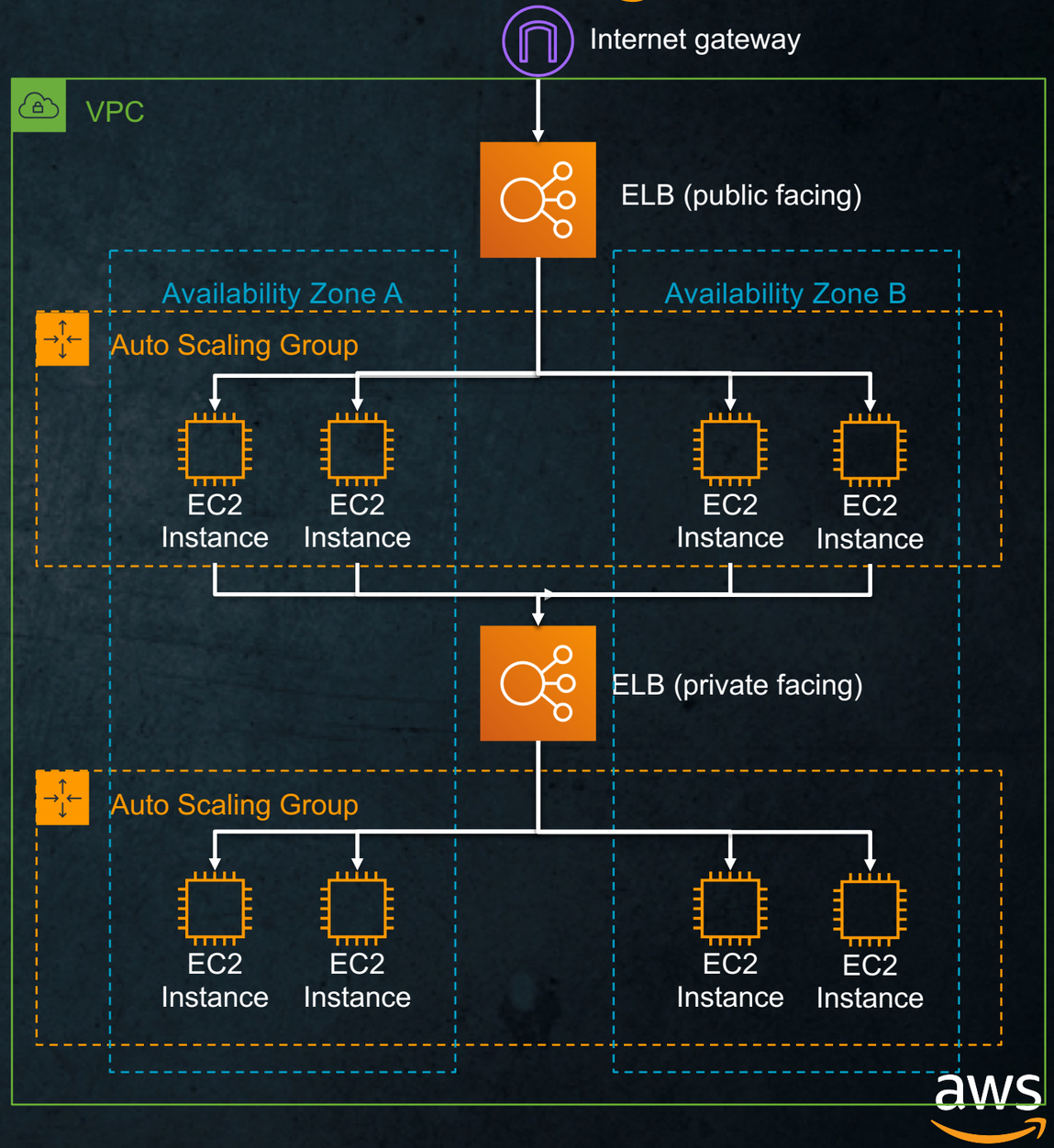
- Multiple VPCs
- Add VPNs as needed
- 1.25 gbps per tunnel
- Native DX support

Traffic Distribution

aws

Horizontal scaling: Elastic Load Balancing

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



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
- IP addresses as Targets

Application Load Balancer (ALB)

- Layer 7 Load Balancing
- Content-Based Routing (host and path based)
- Containerized Application Support (ECS, EKS)
- HTTP/2 Support
- Request Tracing
- Web Application Firewall (WAF) integration

- WebSocket Support
- Deletion Protection

aws

Features Comparison

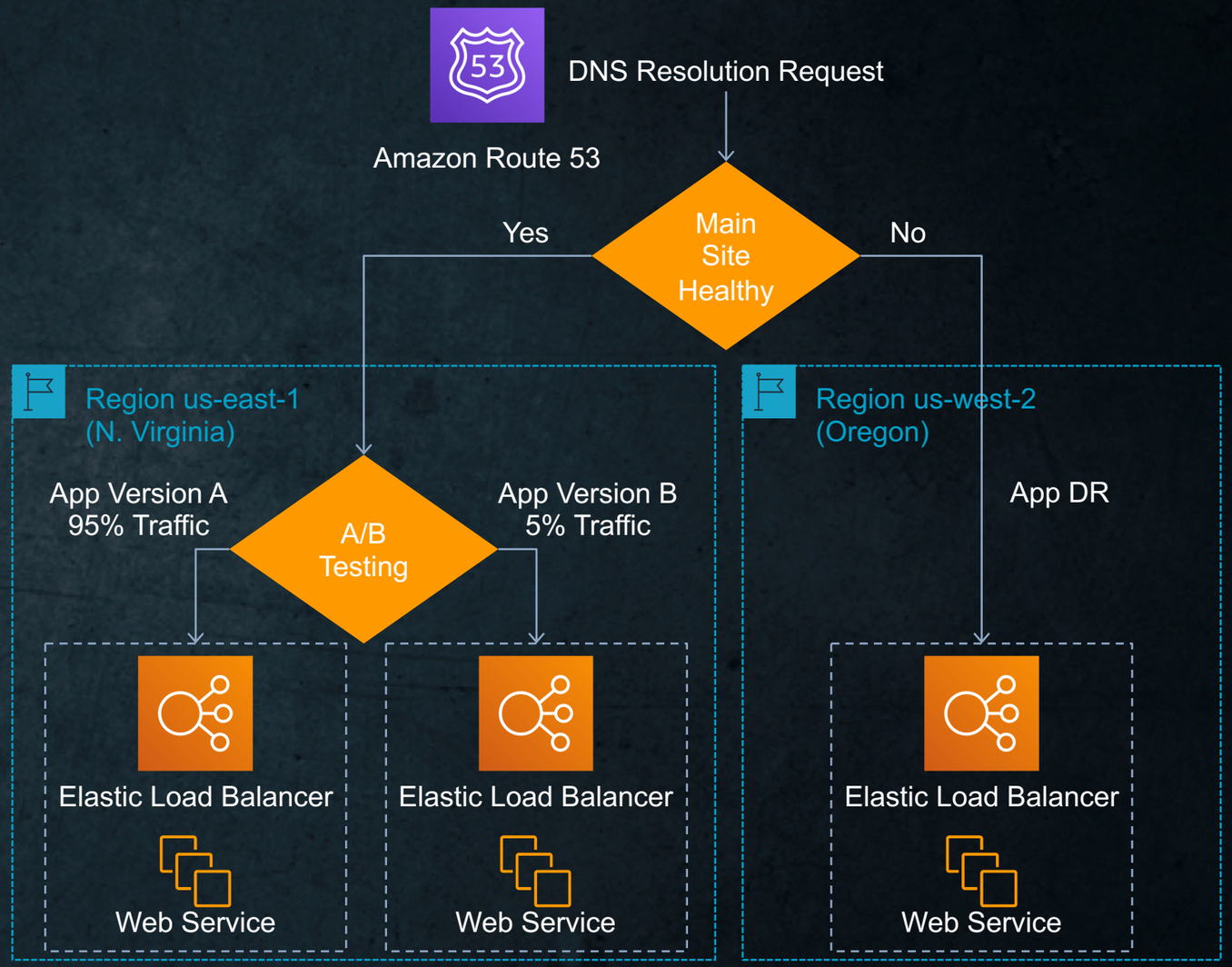
Feature	Application Load Balancer	Network Load Balancer
Protocols	HTTP, HTTPS	TCP
Platforms	VPC	VPC
Health checks	√	√
CloudWatch metrics	√	√
Logging	√	√
Path-Based Routing	√	
Host-Based Routing	√	
Native HTTP/2	√	
Configurable idle connection timeout	√	
SSL offloading	√	
Server Name Indication (SNI)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

Route 53

How to solve my Domain Names to IP Address?

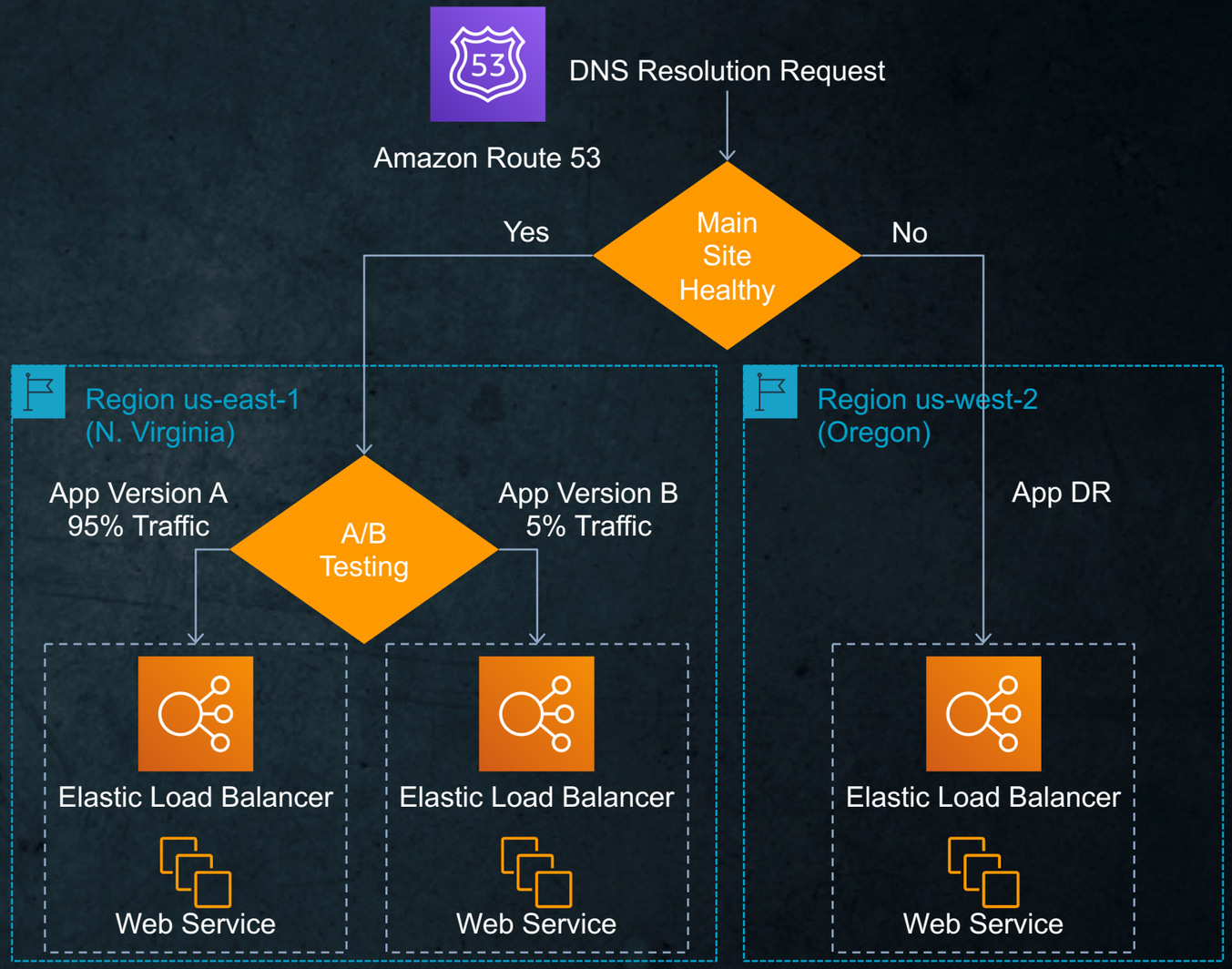
Amazon Route 53

- AWS DNS service
- Domain Registration (default is 20)
- Domain name resolution
- 100% availability SLA
- Zone Apex integration
- Public and private DNS



Policy based routing for Amazon Route 53

- Global routing:
  - Health Checks
  - DNS Failover
  - Latency Based Routing
  - Geo Based Routing
  - Weighted Round Robin



Poll # 5

Route 53 is named so because _____.

A. Route 66 is taken by Microsoft
B. The idea of DNS was invented in 1953
C. The DNS Port is on Port 53 and Route 53 is a DNS service
D. Only AWS Marketing team know the reason

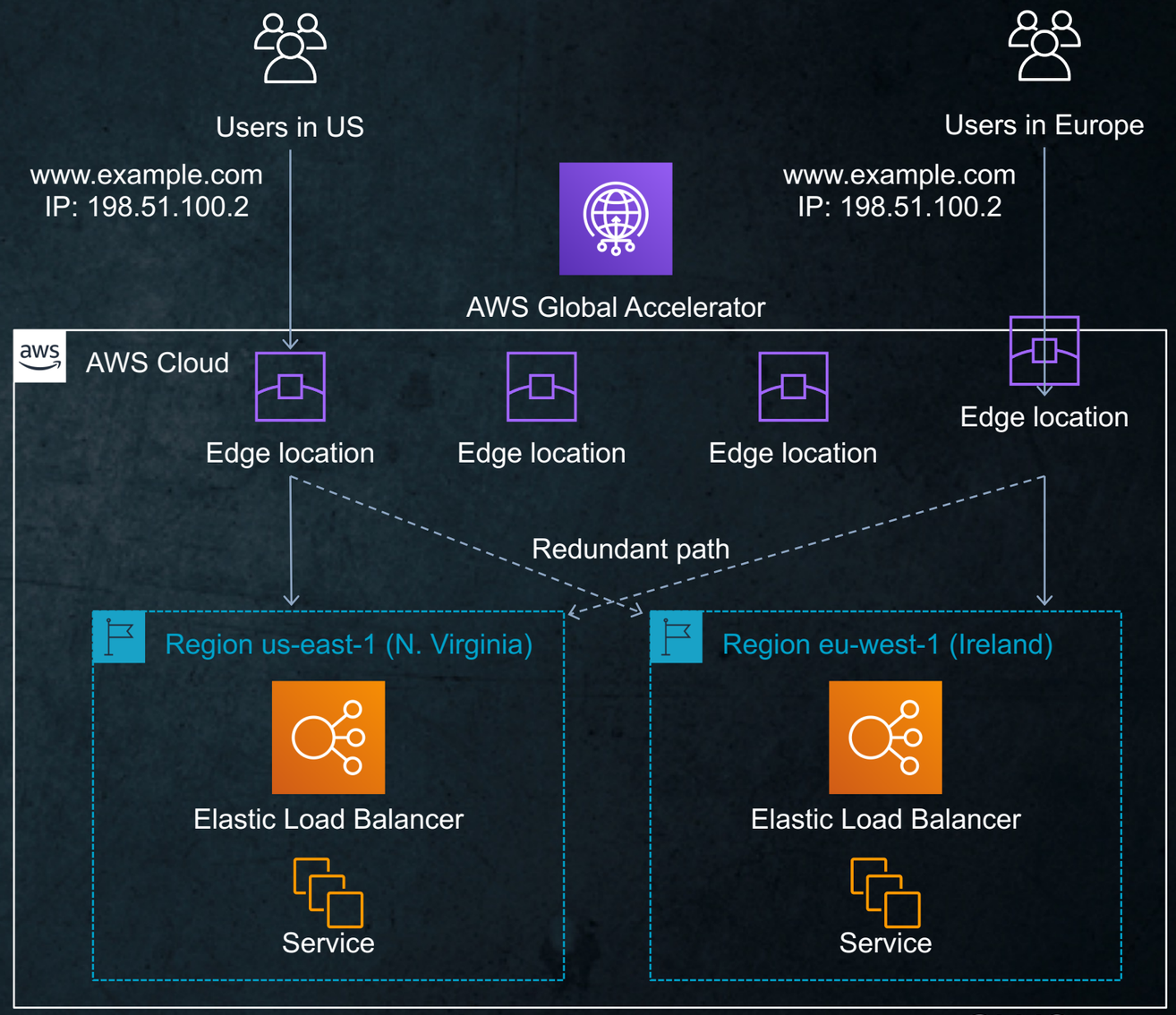
Poll # 6

For regulatory compliance, your application may only provide data to requests coming from the United States. Which of the following routing policies can be configure to do this?

A. Simple
B. Latency
C. Geolocation
D. Multi-value

Anycast instead of DNS: AWS Global Accelerator

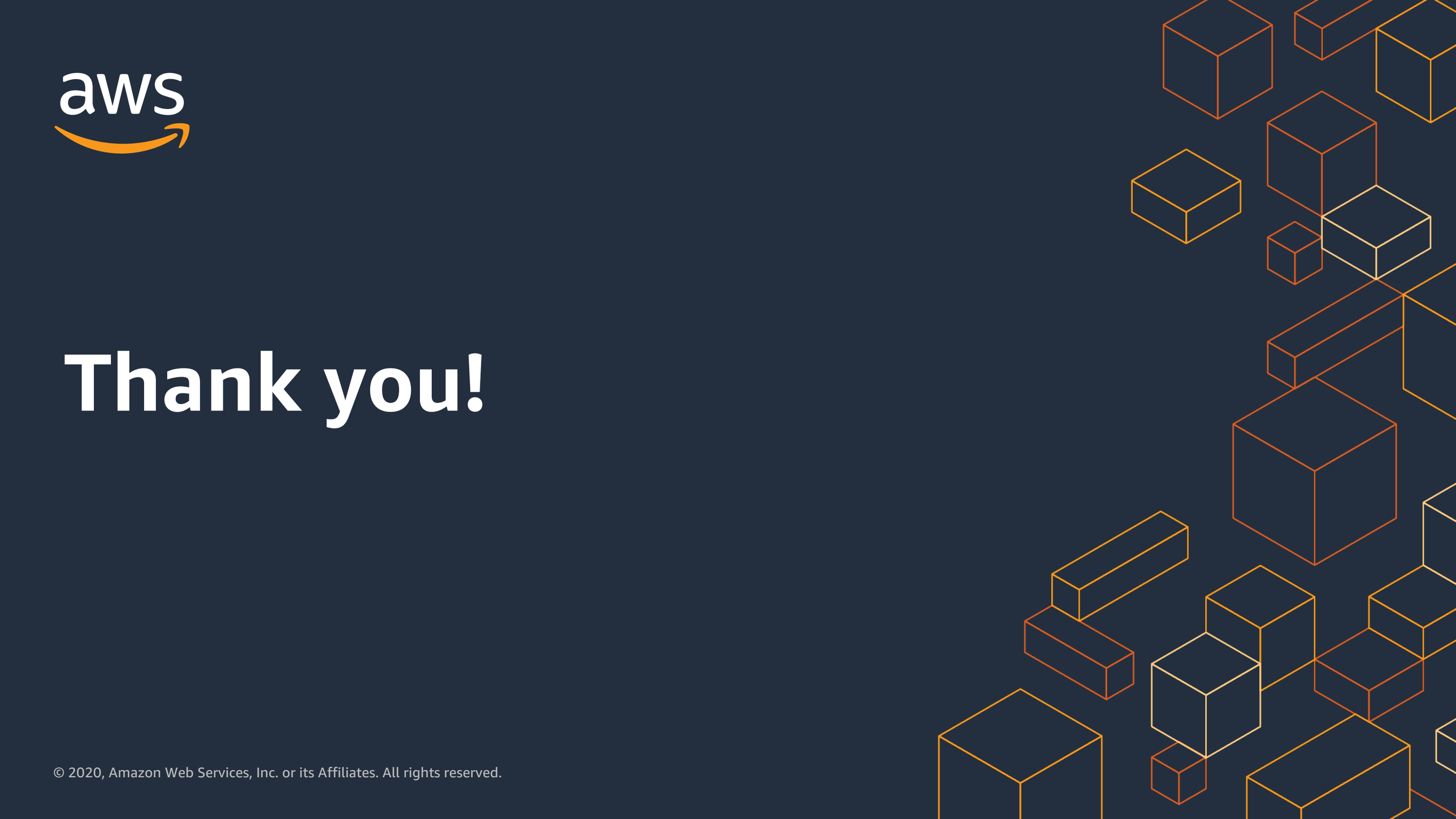
- Uses AWS Global Network from Edge to Region
- Client traffic ingresses via closest available Edge location
- Route client to closest healthy endpoint
- No DNS switchover required, same IP address globally
    - Static IP Anycast



Reference Documentation

1. VPC FAQ
2. Route53 FAQ
3. Elastic Load Balancing FAQ
4. VPN FAQ
5. Direct Connect FAQ
6. Building a Scalable and Secure Multi-VPC AWS Network Infrastructure Whitepaper
7. Well-Architected Framework Whitepaper

aws



Thank you!

Trivia time!

Poll # 7

Route 53 is Amazon’s DNS service

A. True
B. False

Poll # 8

What networking feature can you use to provide connectivity between multiple VPCs?

A. A NAT Gateway
B. An Internet Gateway
C. A Transit Gateway
D. This capability isn’t available in AWS at this time

Poll # 9

You have created a new subdomain for your popular website and you need this subdomain to an ELB using route 53. Which DNS record set type could you create? (Choose 2)

A. MX
B. AAAA
C. A
D. CNAME
E. Alias

aws

Poll # 10

You have been tasked with auditing the security of your VPC. As part of this process, you need to start by analyzing what traffic is allowed to and from various EC2 instances. What two parts of the VPC do you need to check to accomplish this task?

A. NACLs and Subnets
B. Security Groups and Internet Gateways
C. NACLs and Route Tables
D. Security Groups and NACLs

aws

Poll # 11

There is a limit to the domain names that you can manage using Rt 53.

A. True. There's a hard limit of 10 domain names. You can not go above this number.

B. True and False. In Rt 53, there is a default limit of 20 domain names. But, you can increase this limit with a support ticket.

C. False. By default, you can support as many as needed.

aws

Poll # 12

If you need a dedicated, low-latency connection to AWS from your on-premises data center, what solution should you choose?

A. AWS VPN
B. AWS Storage Gateway
C. AWS VPG
D. AWS Direct Connect

Poll # 13

An Application Load Balancer operates at which OSI layer?

A. Layer 4,
B. Layer 2,
C. Layer 7,
D. Layer 3,

aws

Poll # 14

You keep getting an error when you try to attach an IGW to a VPC. What is the most likely cause of the error?

A. The IGW isn't in the same Availability Zone as the VPC.
B. An IGW is already attached to the VPC.
C. The IGW is most likely broken and a new one should be created.
D. The IGW needs to be associate with a route table before it can be attached to a VPC.

aws

Poll # 15

Which of the following describes the advantages of an AWS Direct Connection? (Choose all that apply)

A. A DX connection is a dedicated, private network connection
B. It can be used to reduce data transfer costs
C. Data delivered over a Direct Connection traverses the Internet
D. Data transfer speeds are the same as with a VPN connection

Poll # 16

A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region. Test is peered to both Prod and Dev. All VPCs have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to Prod to speed up time to market. Which of the following options helps the company accomplish this?

A. Create a new peering connection Between Prod and Dev along with appropriate routes.
B. Create a new entry to Prod in the Dev route table using the peering connection as the target.
C. Attach a second gateway to Dev. Add a new entry in the Prod route table identifying the gateway as the target.
D. The VPCs have non-overlapping CIDR blocks in the same account. The route tables contain local routes for all VPCs.

aws