AWS re:Invent

NOV. 27 – DEC. 1, 2023 | LAS VEGAS, NV

NTA307

AWS networking foundations

Mike Cornstubble
(he/him)
Sr. Solutions Architect
AWS

Anoop Talluri
(he/him)
Solutions Architect
AWS

Nayan Karumuri
(he/him)
Sr. Solutions Architect
AWS

Agenda

AWS global infrastructure

Getting started in single VPC

Expanding to multiple VPCs and beyond

Hybrid connectivity to on-premise environments

AWS Networking Competency Partners

AWS global infrastructure

AWS global infrastructure

32 GEOGRAPHICAL REGIONS, 102 AVAILABILITY ZONES, 550+ POPS

AWS Region and number of Availability Zones (AZs)

GovCloud (US)
US-East (3), US-West (3)

US West
Oregon (4)
Northern California (3)

US East
N. Virginia (6), Ohio (3)

Canada
Central (3)

South America
São Paulo (3)

Africa
Cape Town (3)

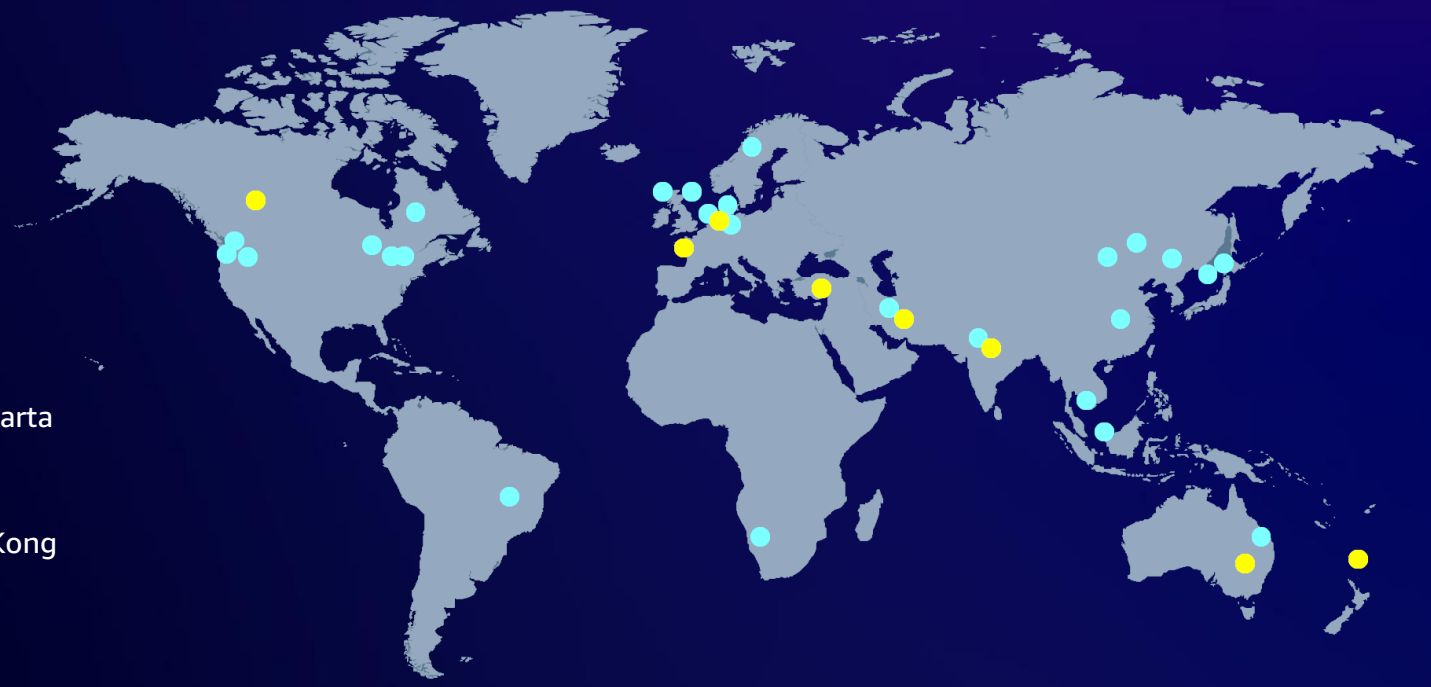
China
Beijing (2), Ningxia (3)

Europe
Frankfurt (3), Paris (3),
Ireland (3), Stockholm (3),
London (3), Milan (3)

Middle East
Bahrain (3)

Asia Pacific
Singapore (3), Sydney (3), Jakarta (3),
Tokyo (4), Osaka (3)
Seoul (4), Mumbai (3), Hong Kong (3)

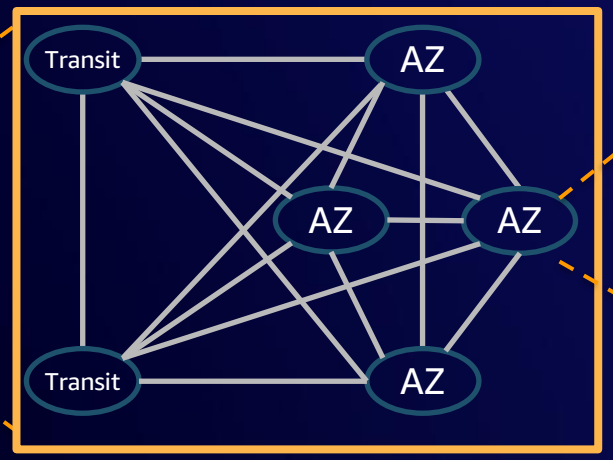
Australia
Sydney (3), Melbourne (3)



AWS Region design

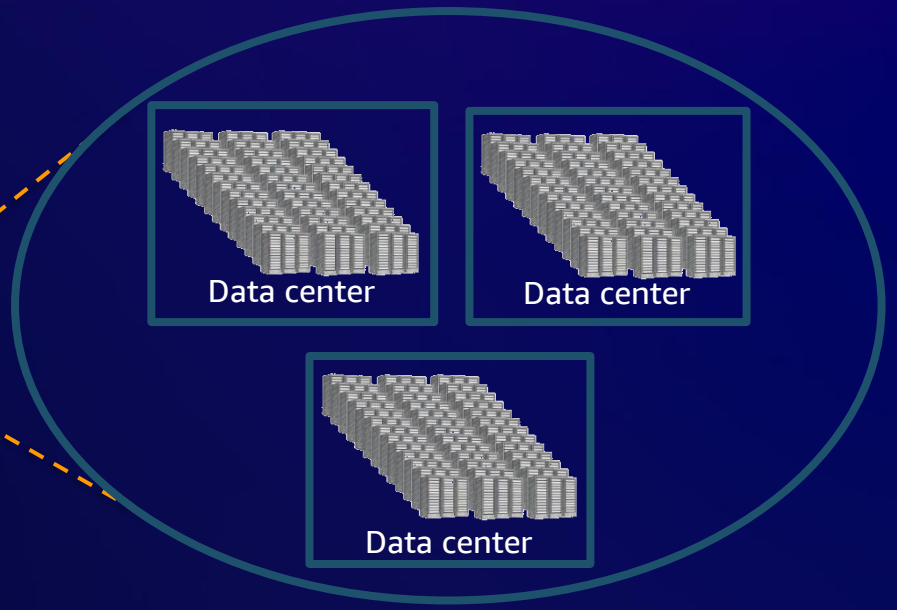
AWS Regions are composed of multiple AZs for **high availability, high scalability, and high fault tolerance.** Applications and data are replicated in real time and consistent in the different AZs.

AWS Region



A **Region** is a physical location in the world where AWS has multiple **Availability Zones**

AWS Availability Zone (AZ)

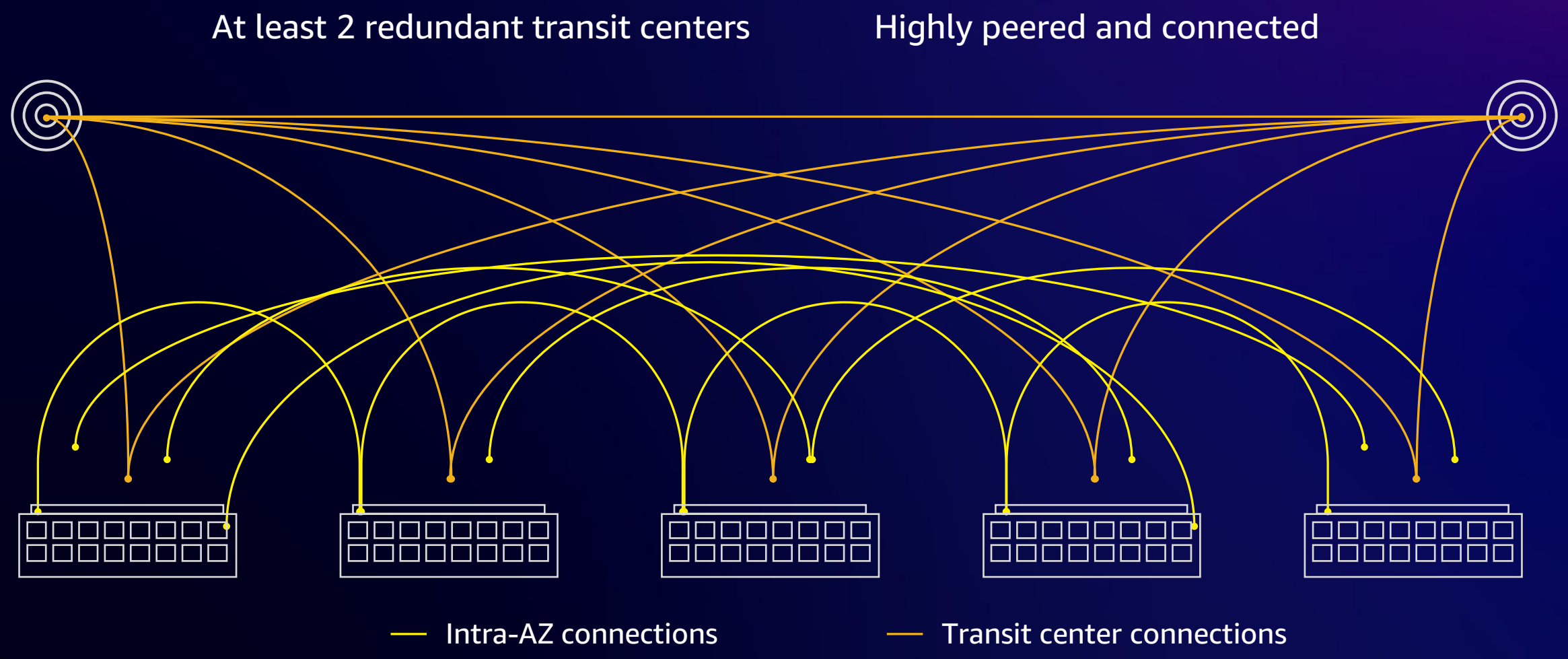


Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities

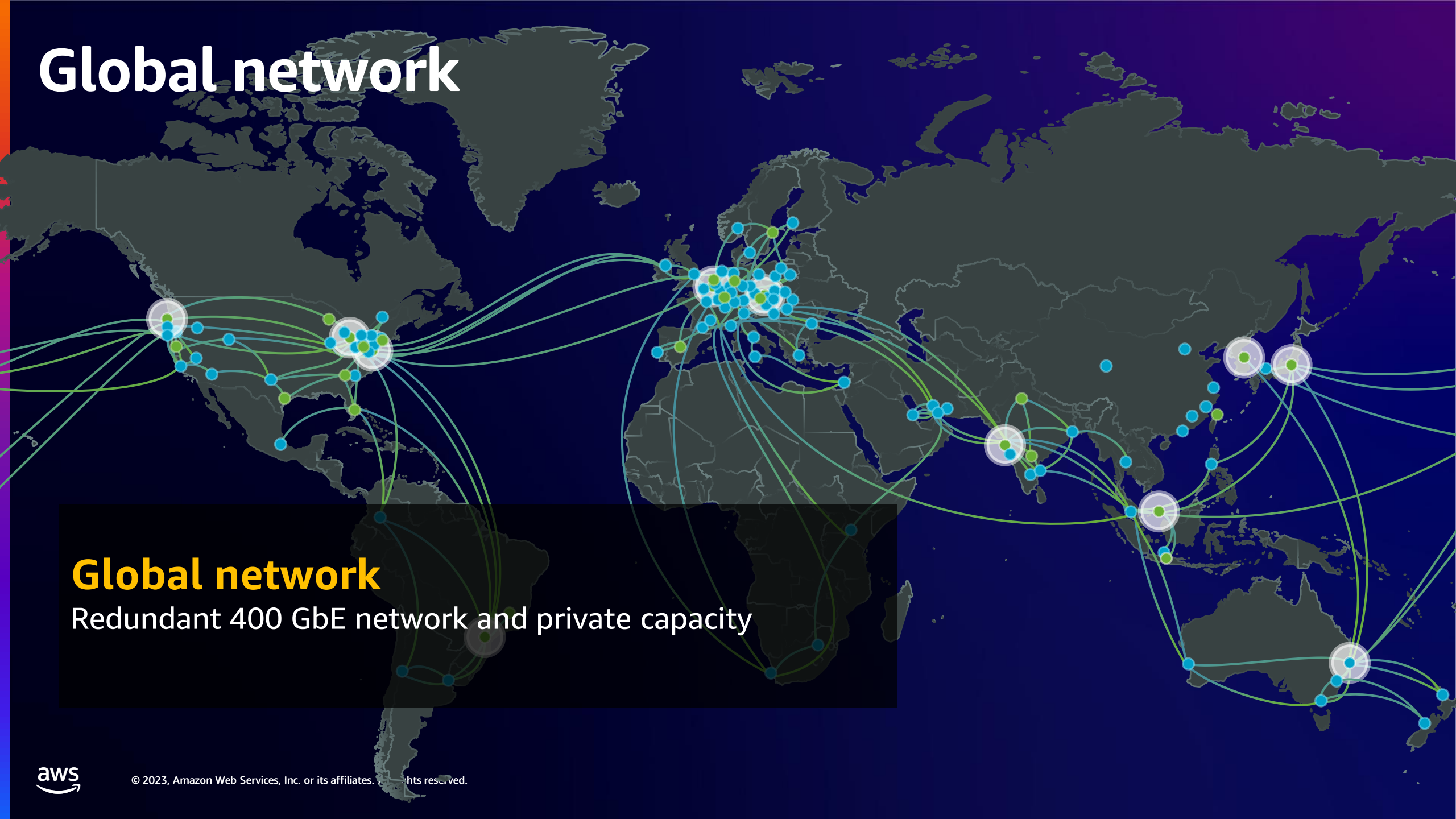
AWS Availability Zone (AZ) design

- Fully isolated infrastructure with one or more datacenters
- Meaningful distance of separation
- Unique power infrastructure
- Many 100Ks of servers at scale
- Datacenters connected via fully redundant and isolated metro fiber

AWS network design



Global network

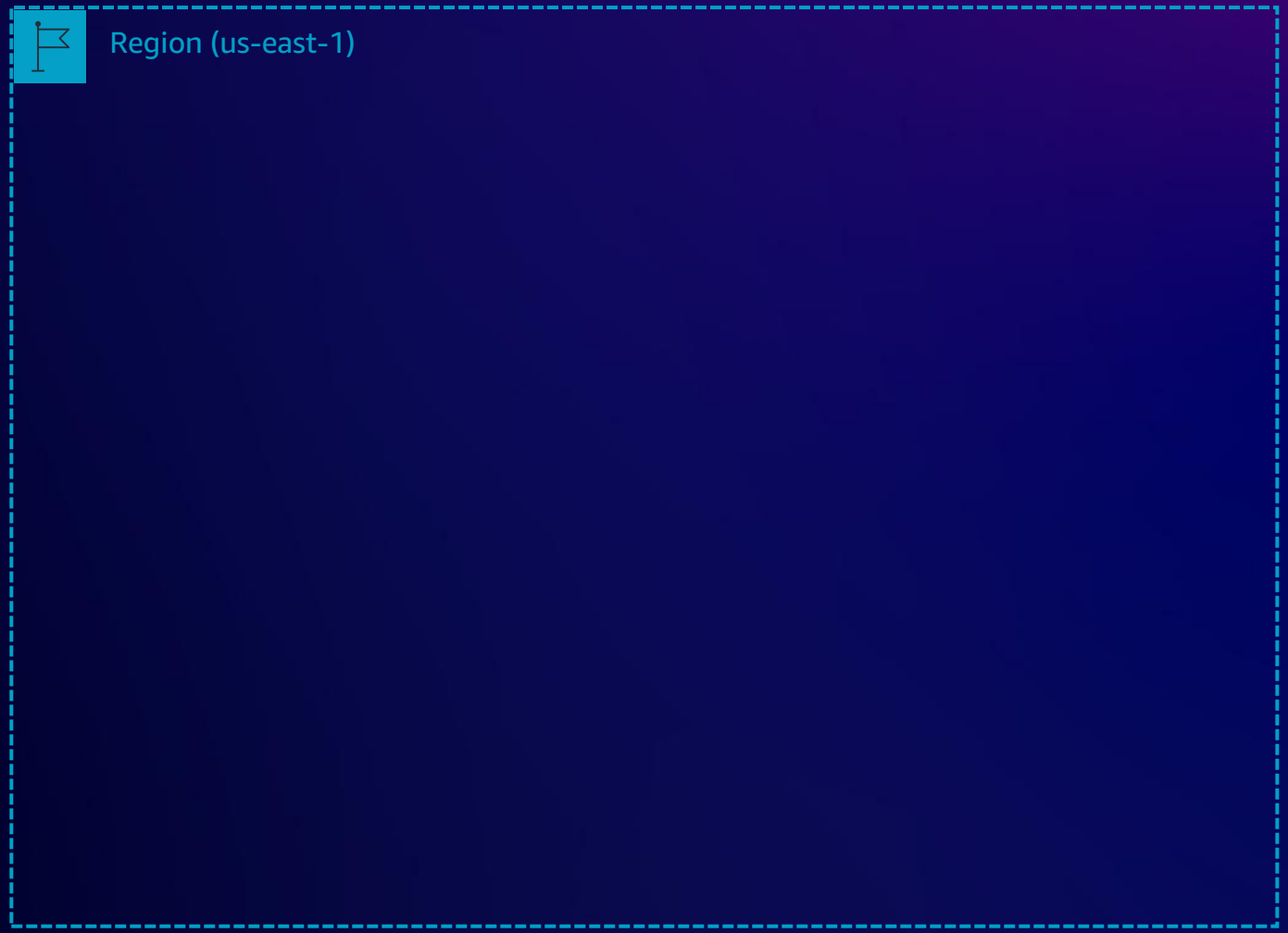


Global network

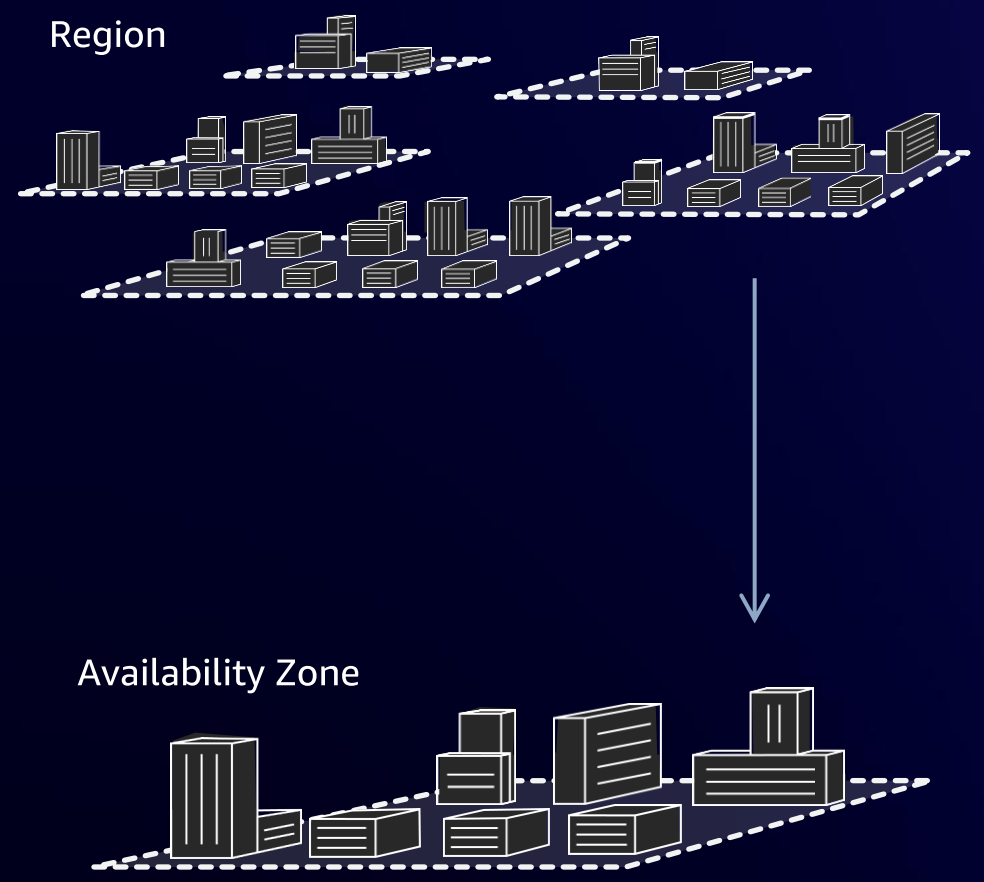
Redundant 400 GbE network and private capacity

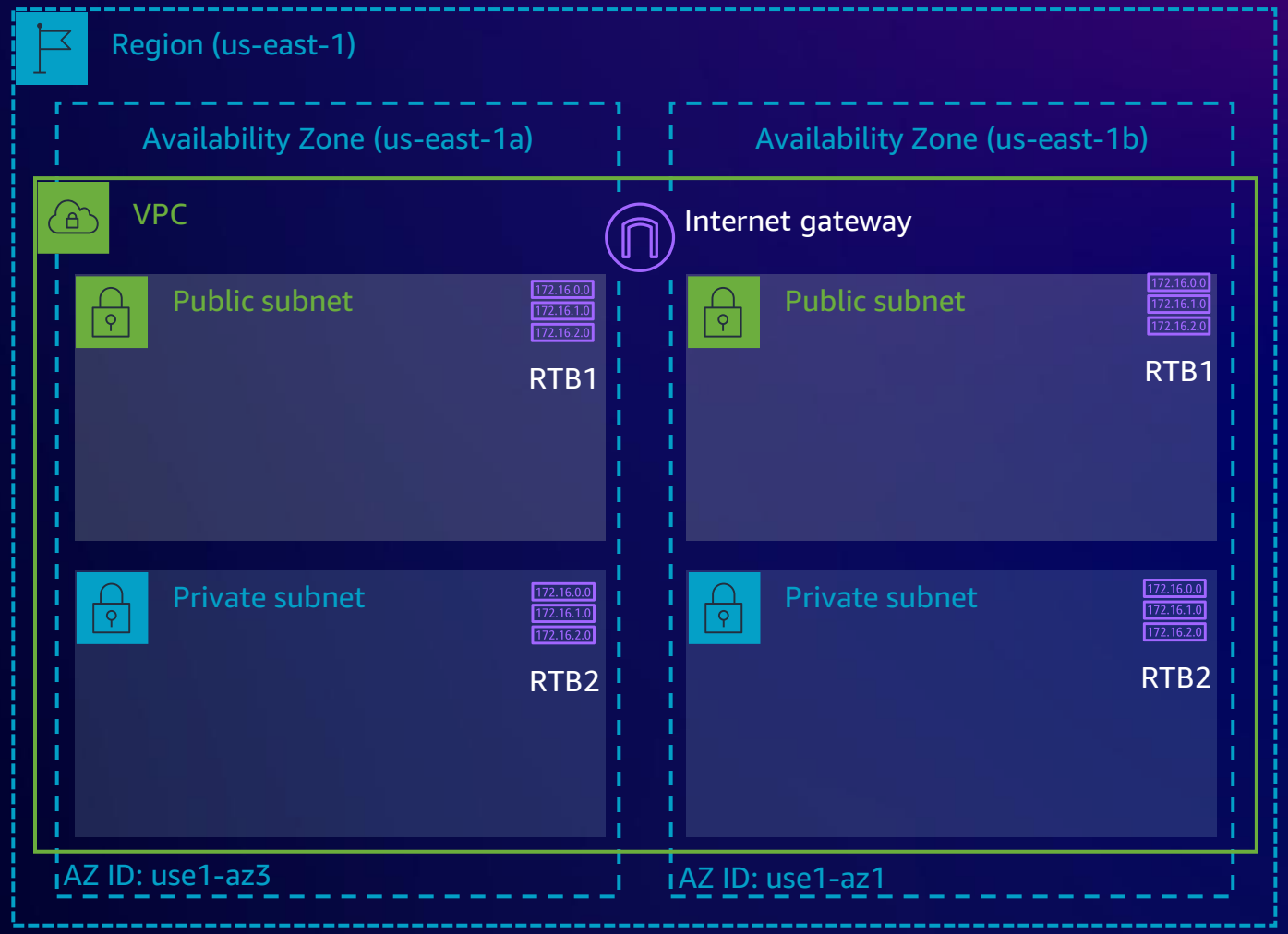
Getting started in single VPC

Building a VPC

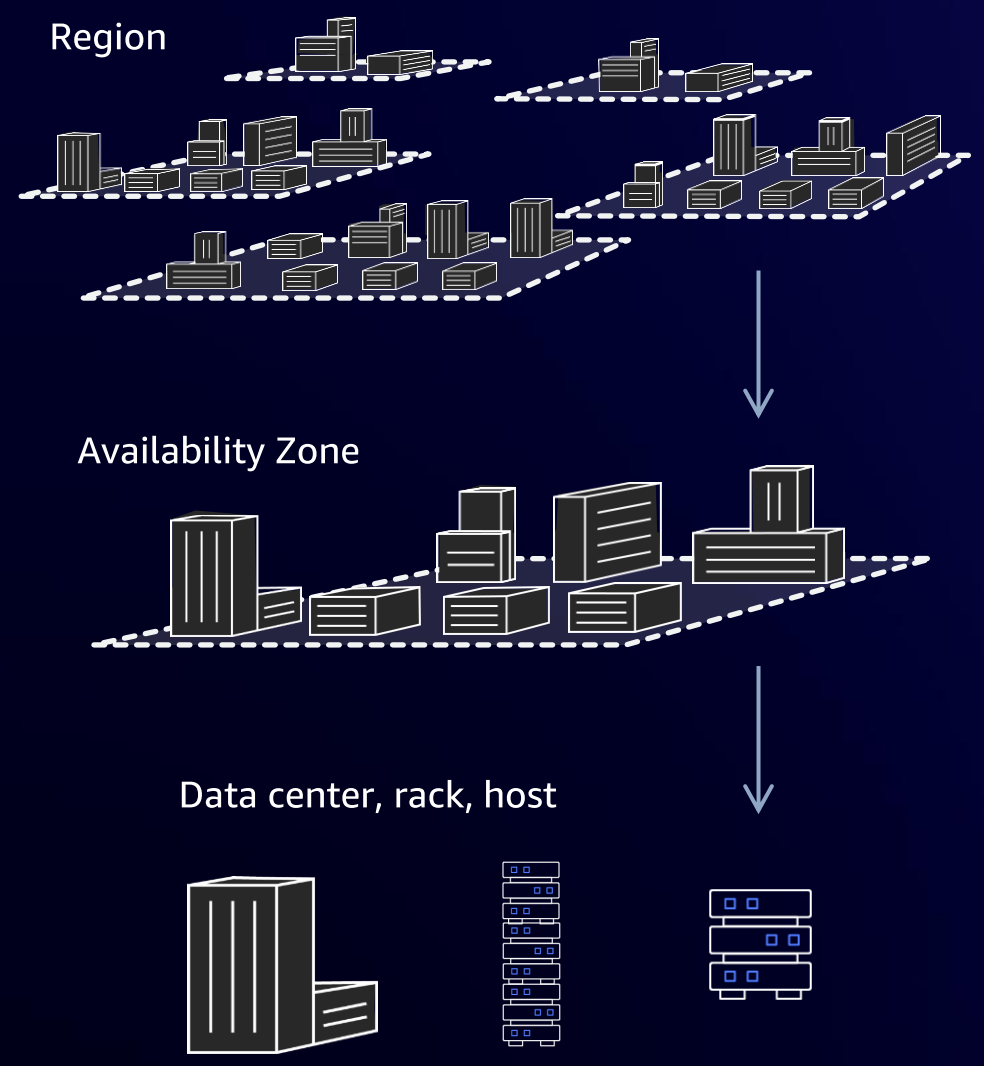


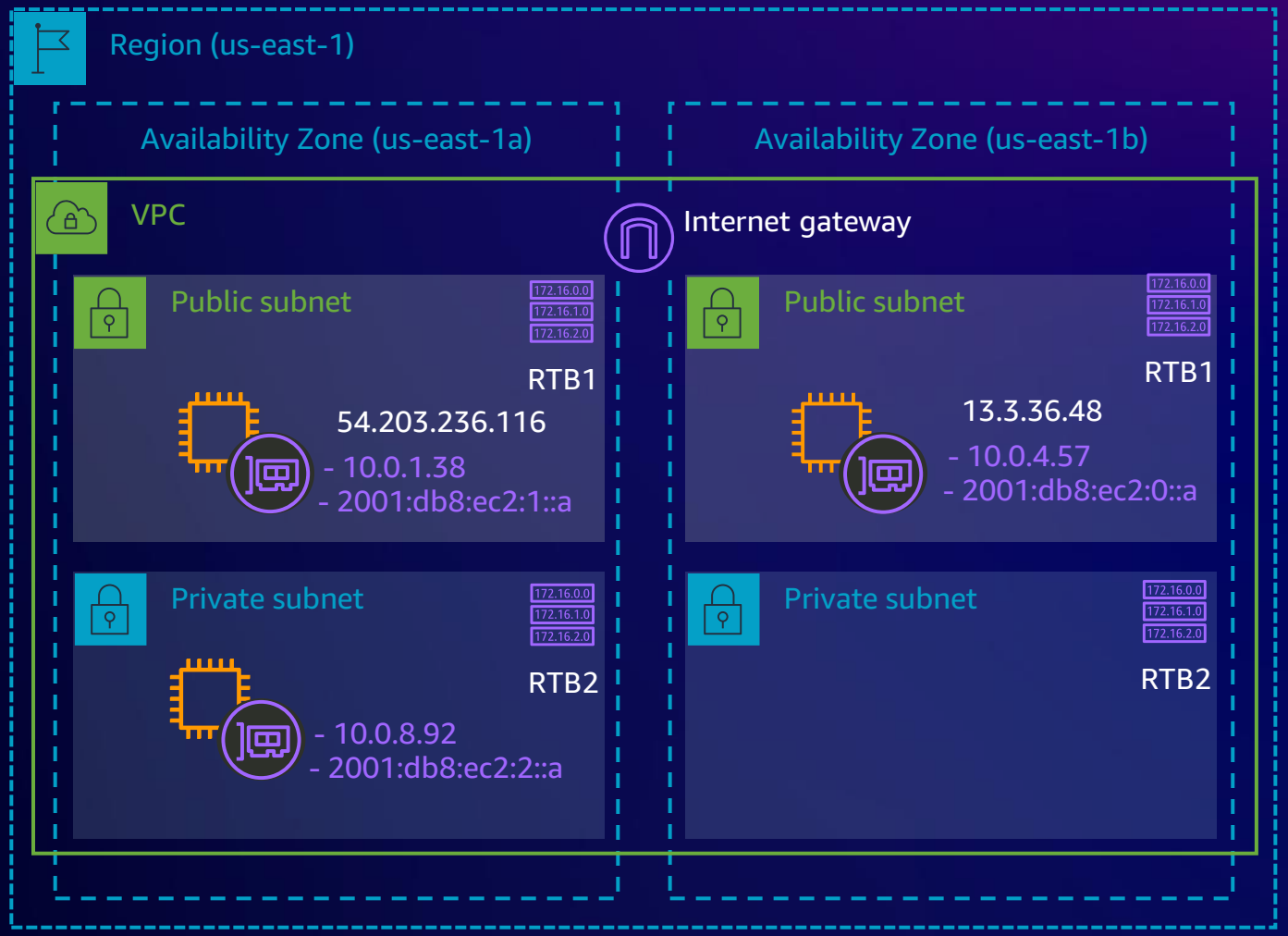
Building a VPC





Building a VPC





What is a VPC?

A VPC is a virtual network that closely resembles a traditional network that you'd operate in your own data center

- Support IPv4 and IPv6
  - IPv4: VPC IPv4 CIDR can be between /16 and /28
  - IPv6: VPC IPv6 CIDR is fixed at /56
- VPCs support subnetting
- VPC CIDRs cannot be modified once created
- Additional CIDRs can be added to a VPC
- Contiguous IPv6 CIDR blocks available

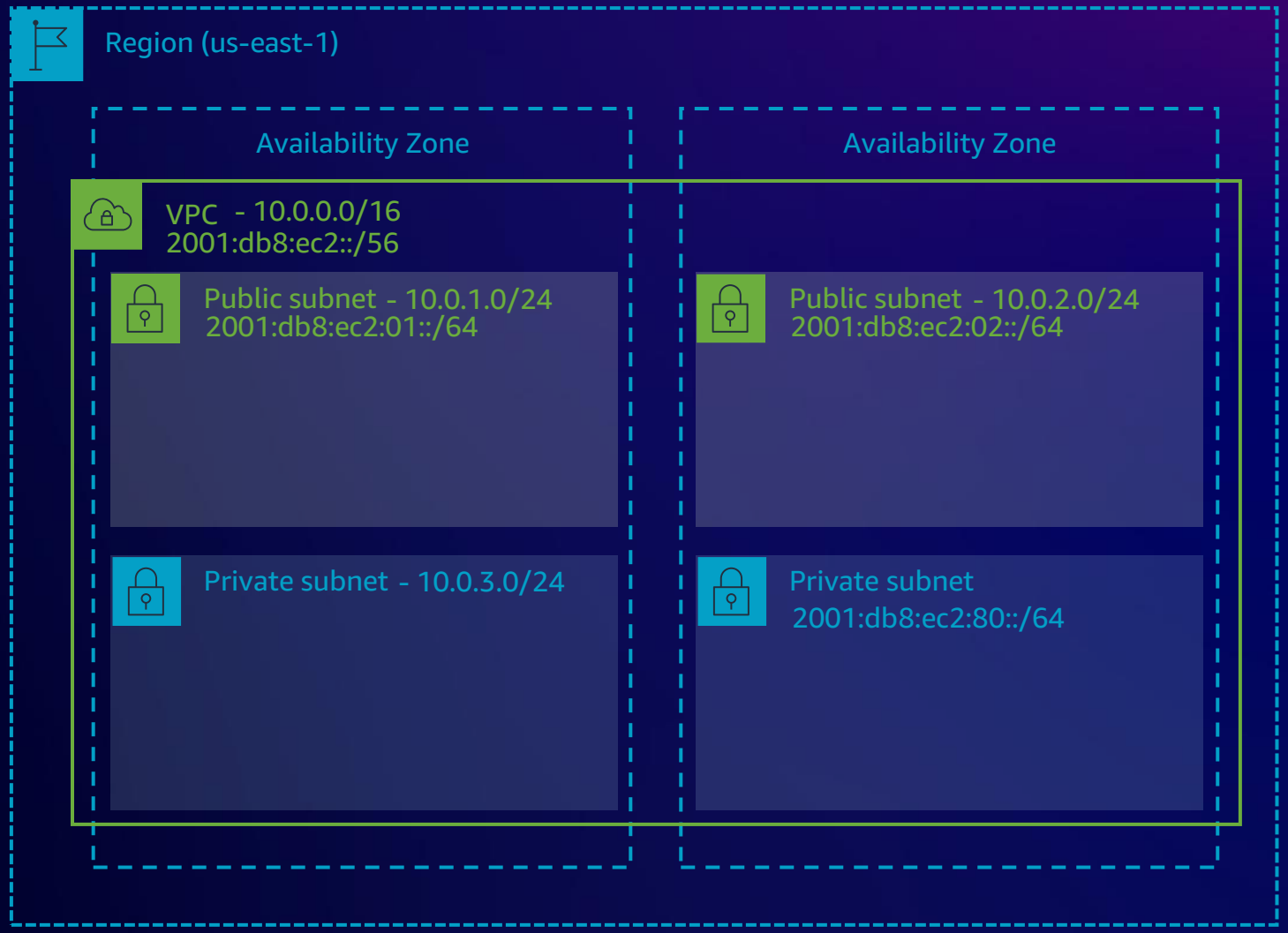
VPC IP addressing considerations

Plan your IP space before creating it

- Consider using multiple VPCs
- Consider future AWS Region expansion
- Consider future connectivity to corporate networks
- Overlapping IP spaces = future headache

Subnets – IPv4 and IPv6 addressing

- VPCs span a Region
- Subnets are allocated as a subset of the VPC IPv4 or IPv6 CIDR range and span a specific AZ
- You can have up to 200 subnets per VPC
- Implicit route between all subnets within a VPC
- Subnets are public subnets when there is a route to an internet gateway



Network access control list

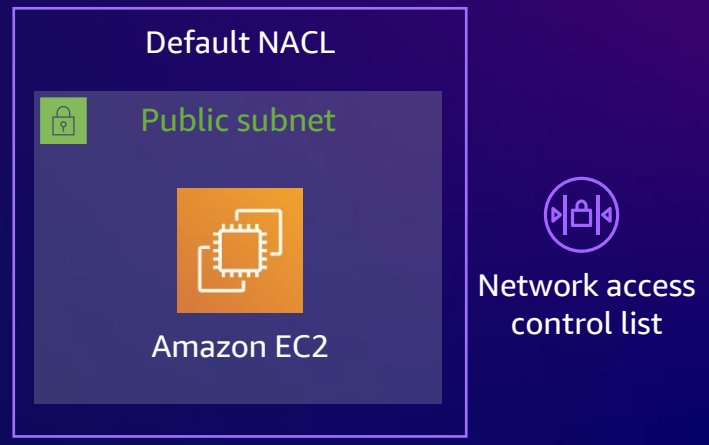
A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level

- Subnet-level inspection
- Inbound and outbound
- Stateless
- Based on IP and TCP/UDP ports
- Supports allow and deny rules
- Deny all at the end
- By default, allow all traffic

Network access control list

A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level

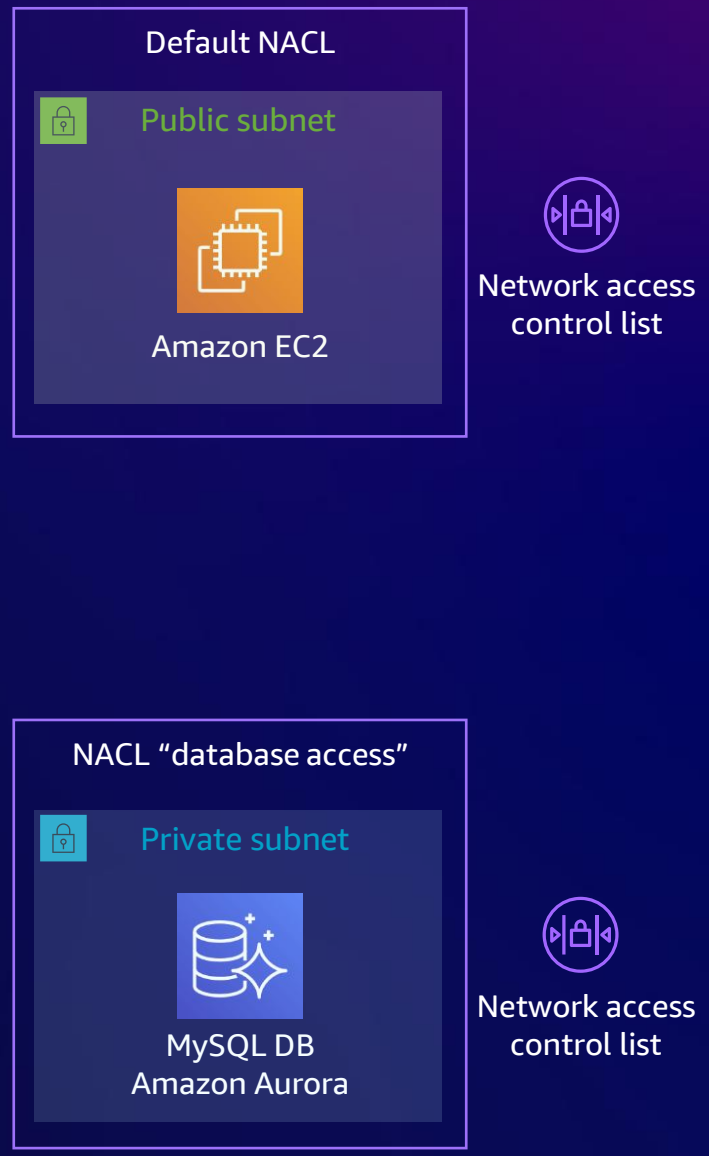
- Subnet-level inspection
- Inbound and outbound
- Stateless
- Based on IP and TCP/UDP ports
- Supports allow and deny rules
- Deny all at the end
- By default, allow all traffic



Network access control list

A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level

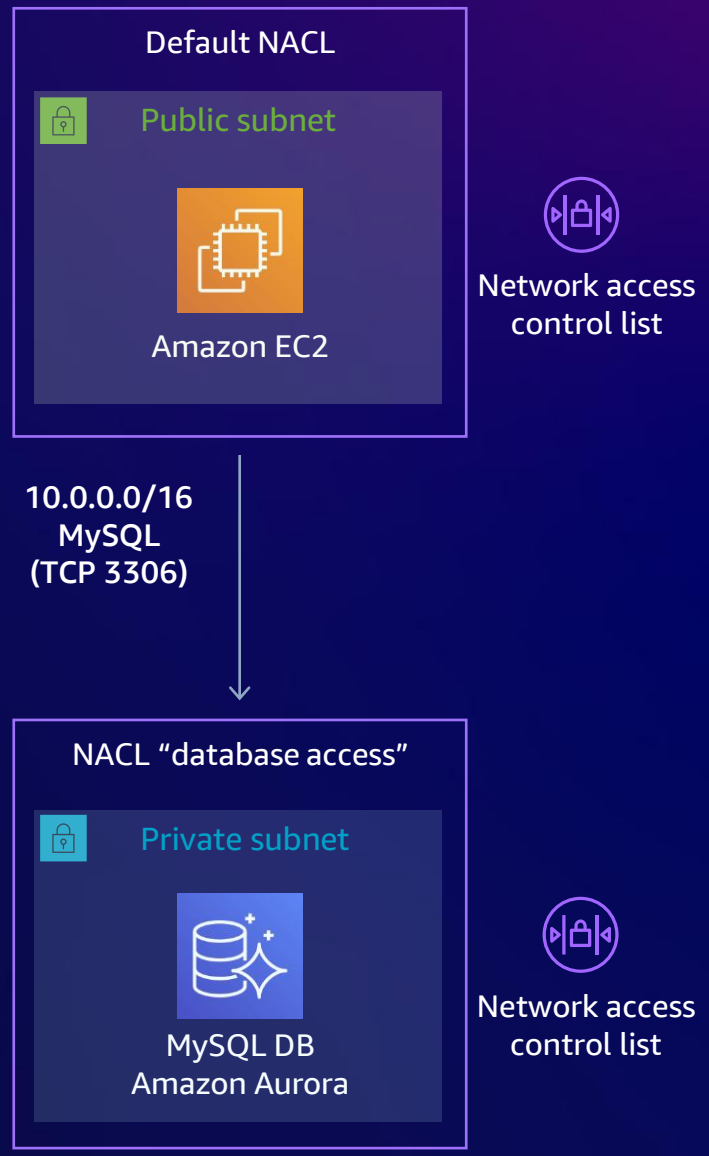
- Subnet-level inspection
- Inbound and outbound
- Stateless
- Based on IP and TCP/UDP ports
- Supports allow and deny rules
- Deny all at the end
- By default, allow all traffic



Network access control list

A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level

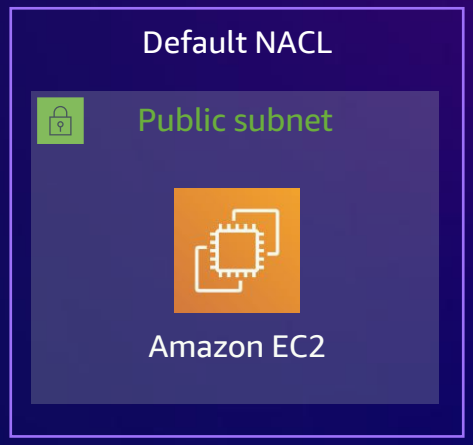
- Subnet-level inspection
- Inbound and outbound
- Stateless
- Based on IP and TCP/UDP ports
- Supports allow and deny rules
- Deny all at the end
- By default, allow all traffic



Network access control list

A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level

- Subnet-level inspection
- Inbound and outbound
- Stateless
- Based on IP and TCP/UDP ports
- Supports allow and deny rules
- Deny all at the end
- By default, allow all traffic



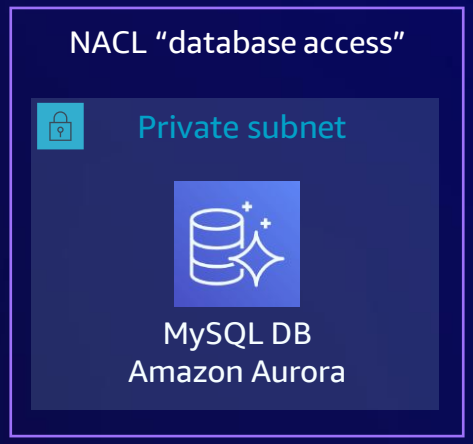
Network access control list

Inbound rules (3)

Edit inbound rules

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	MySQL/Aurora (3306)	TCP (6)	3306	10.0.0.0/16	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

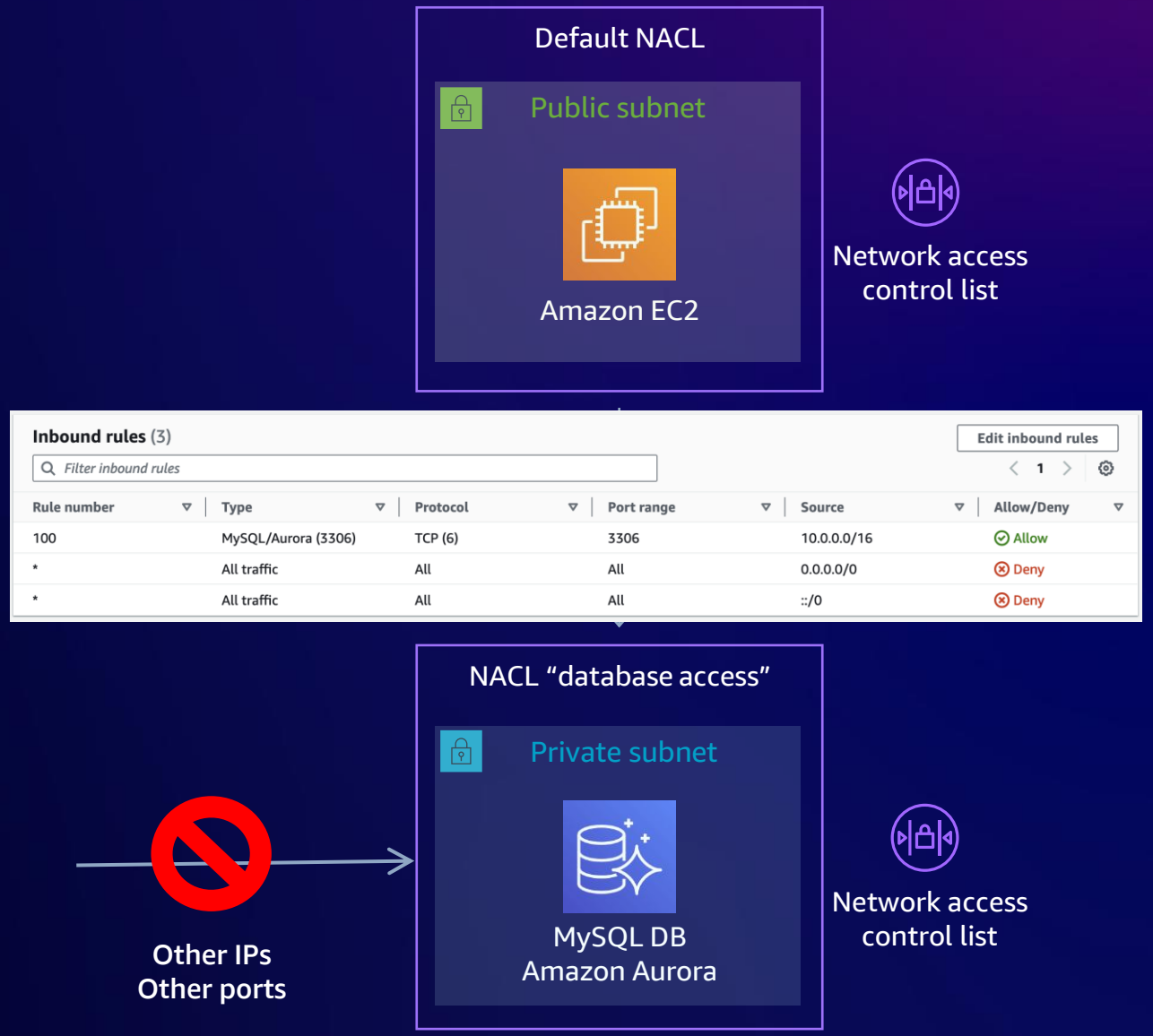


Network access control list

Network access control list

A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level

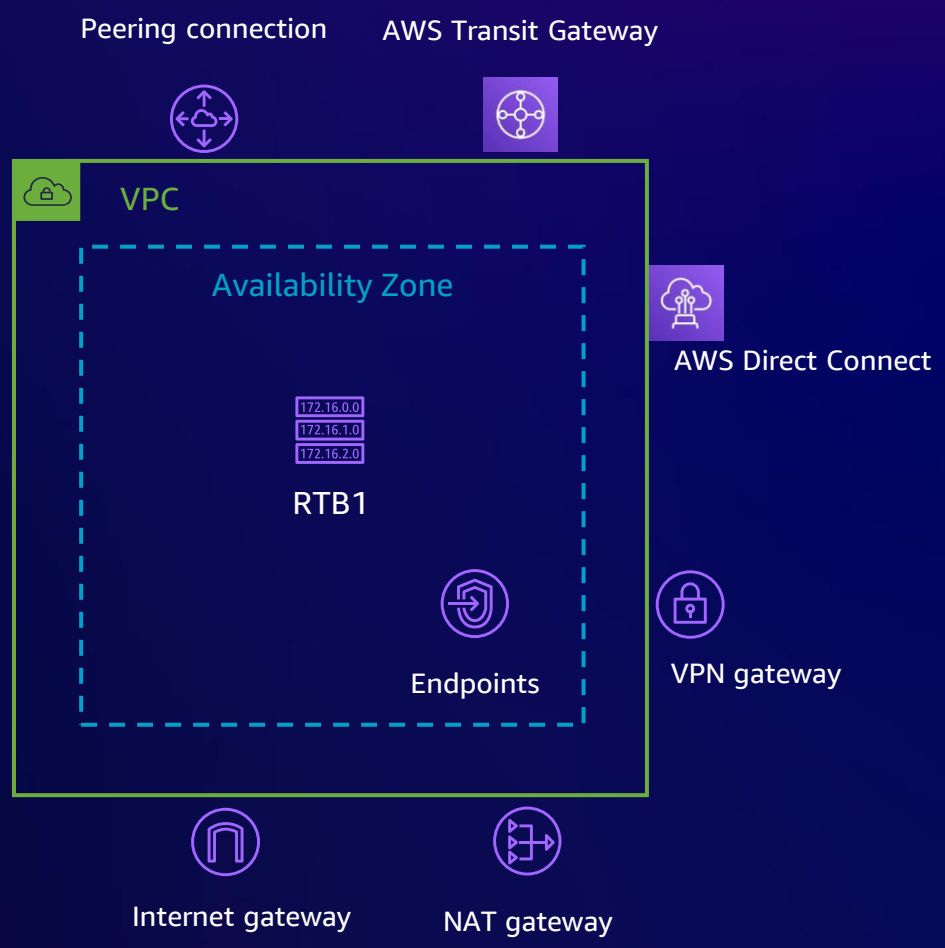
- Subnet-level inspection
- Inbound and outbound
- Stateless
- Based on IP and TCP/UDP ports
- Supports allow and deny rules
- Deny all at the end
- By default, allow all traffic



Route tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

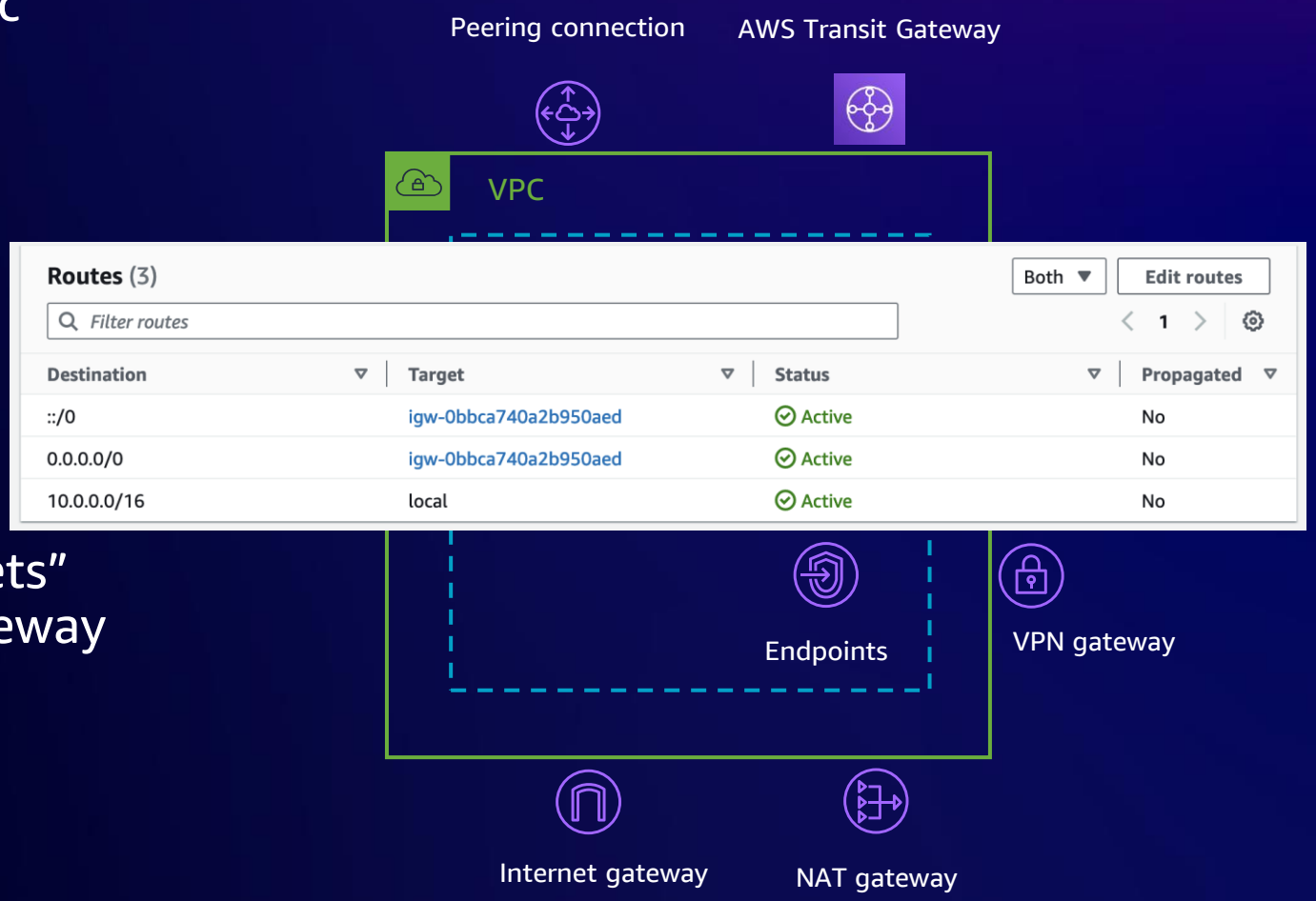
- Route tables direct traffic toward:
  - Internet/NAT gateway
  - Gateway endpoint
  - VPC peering/AWS Transit Gateway
  - VPN gateway/Direct Connect
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Route tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

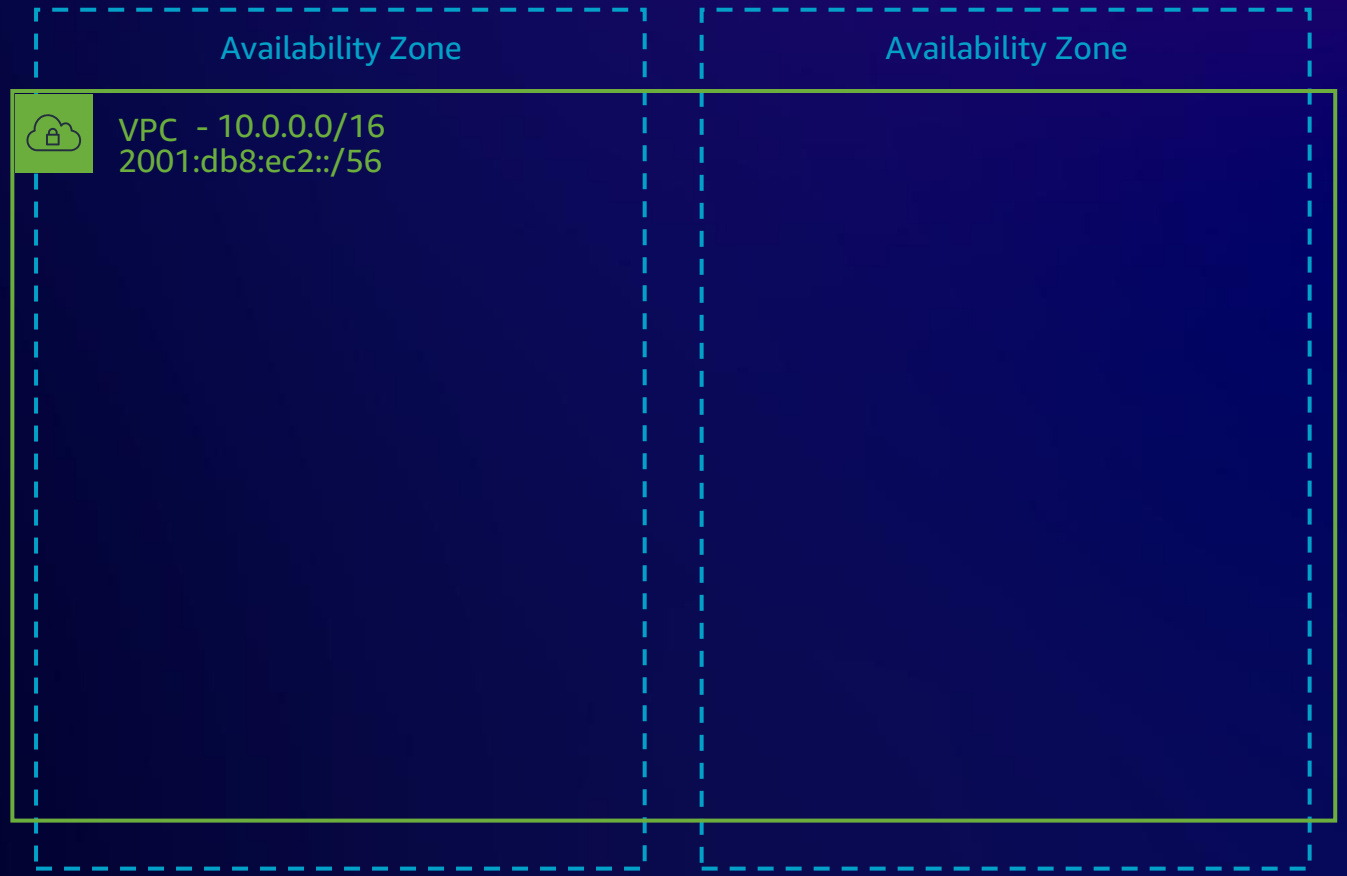
- Route tables direct traffic toward:
  - Internet/NAT gateway
  - Gateway endpoint
  - VPC peering/AWS Transit Gateway
  - VPN gateway/Direct Connect
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Routing tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

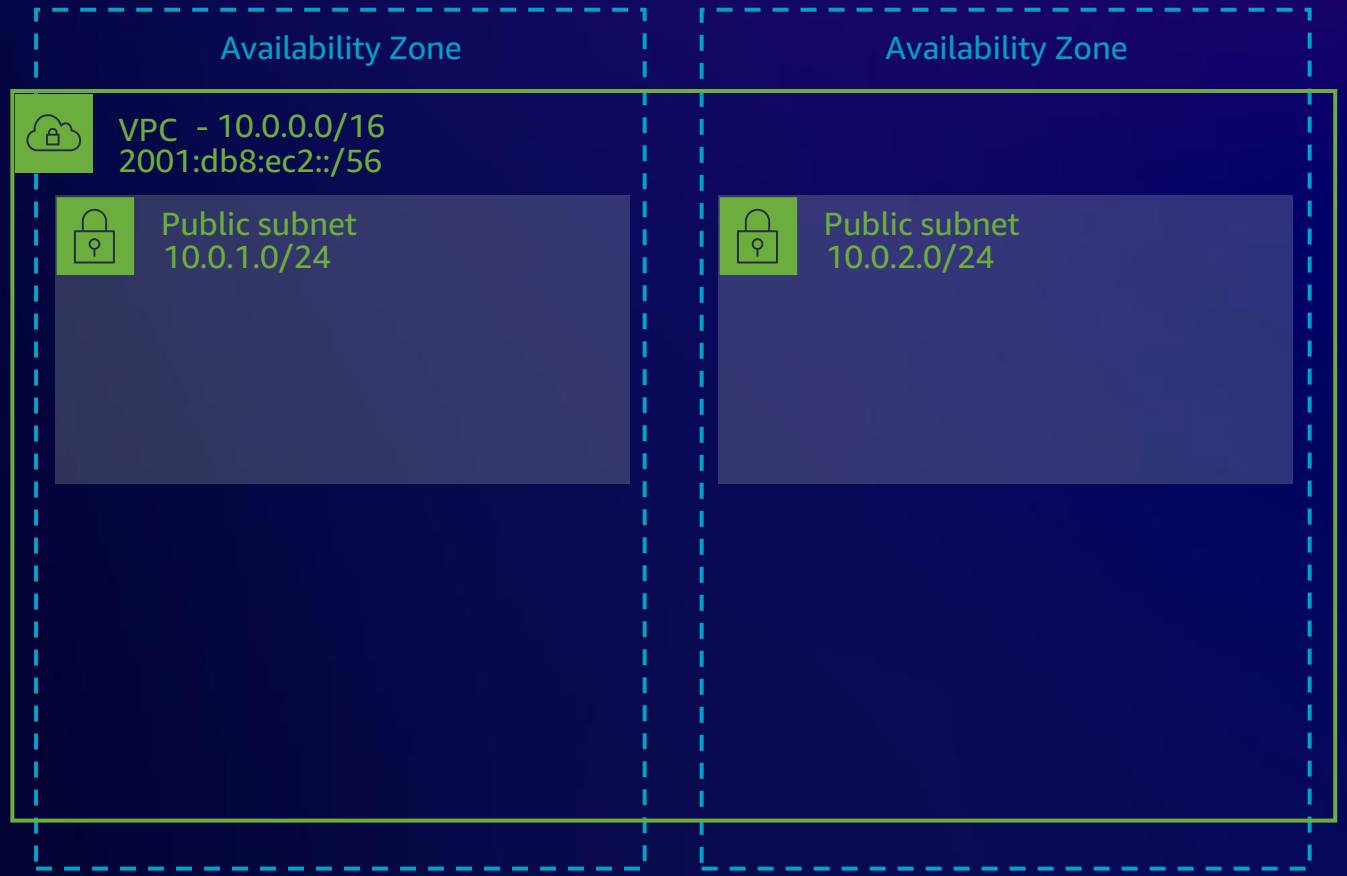
- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Routing tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

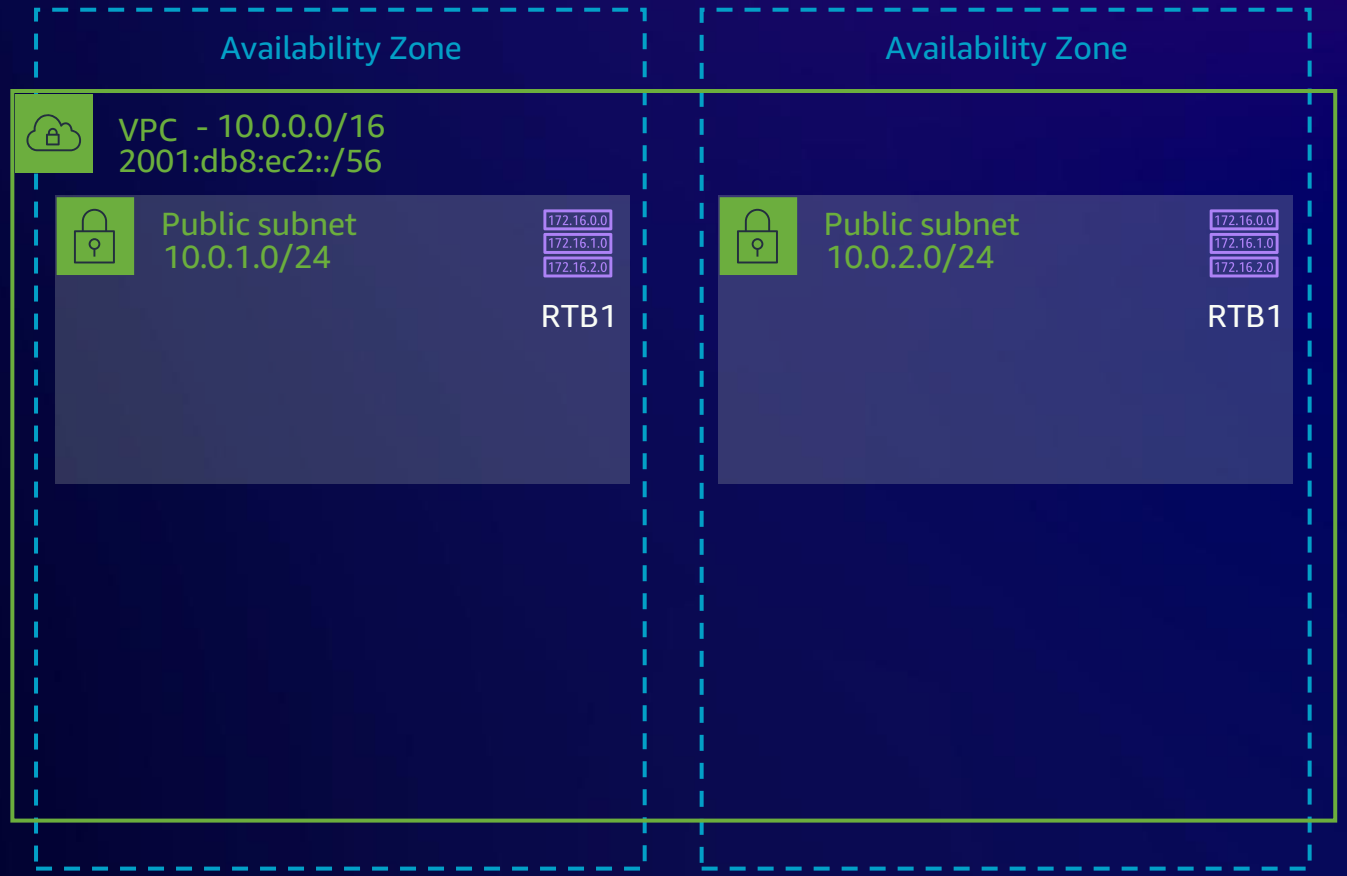
- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Routing tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

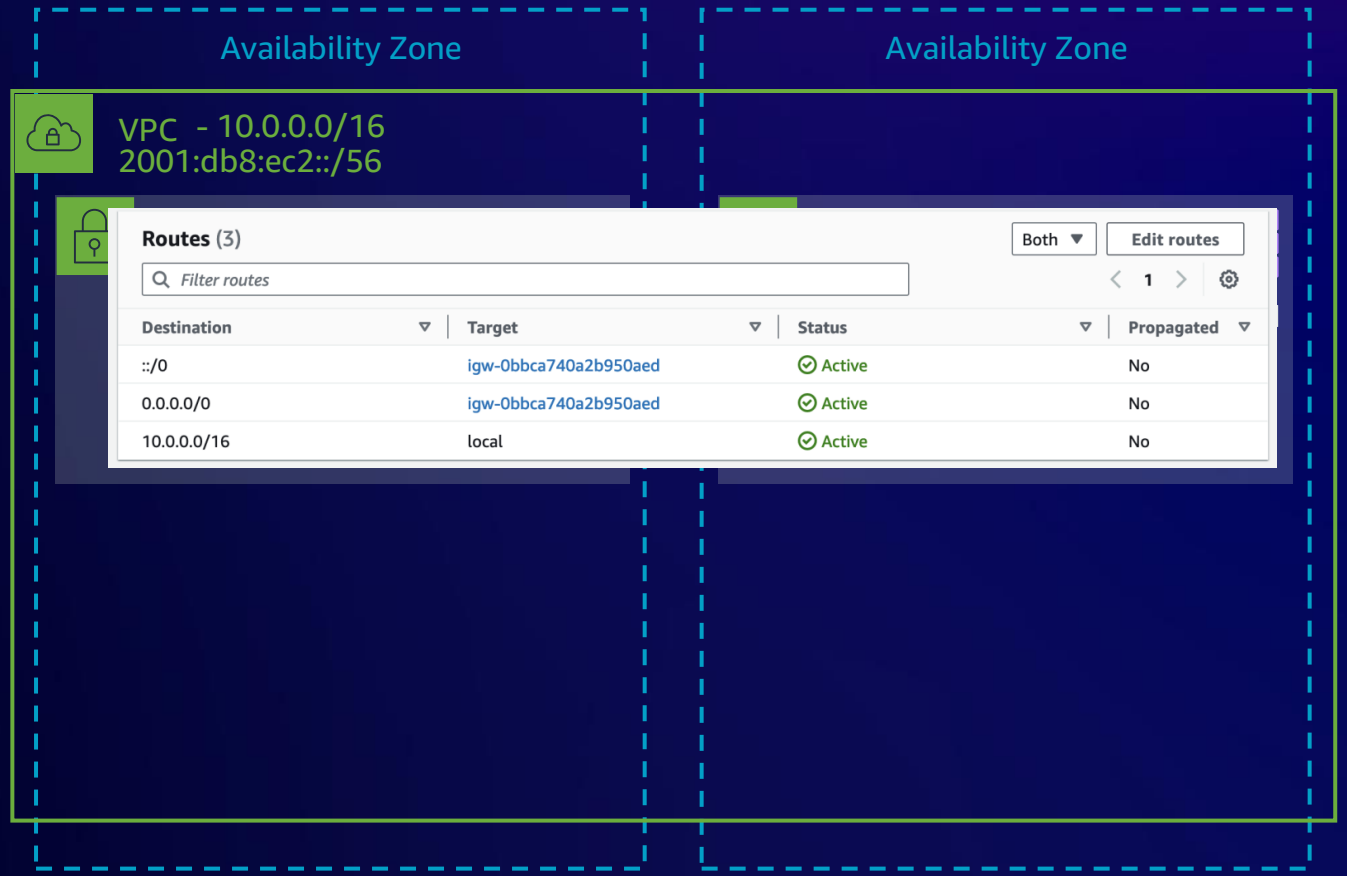
- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Routing tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

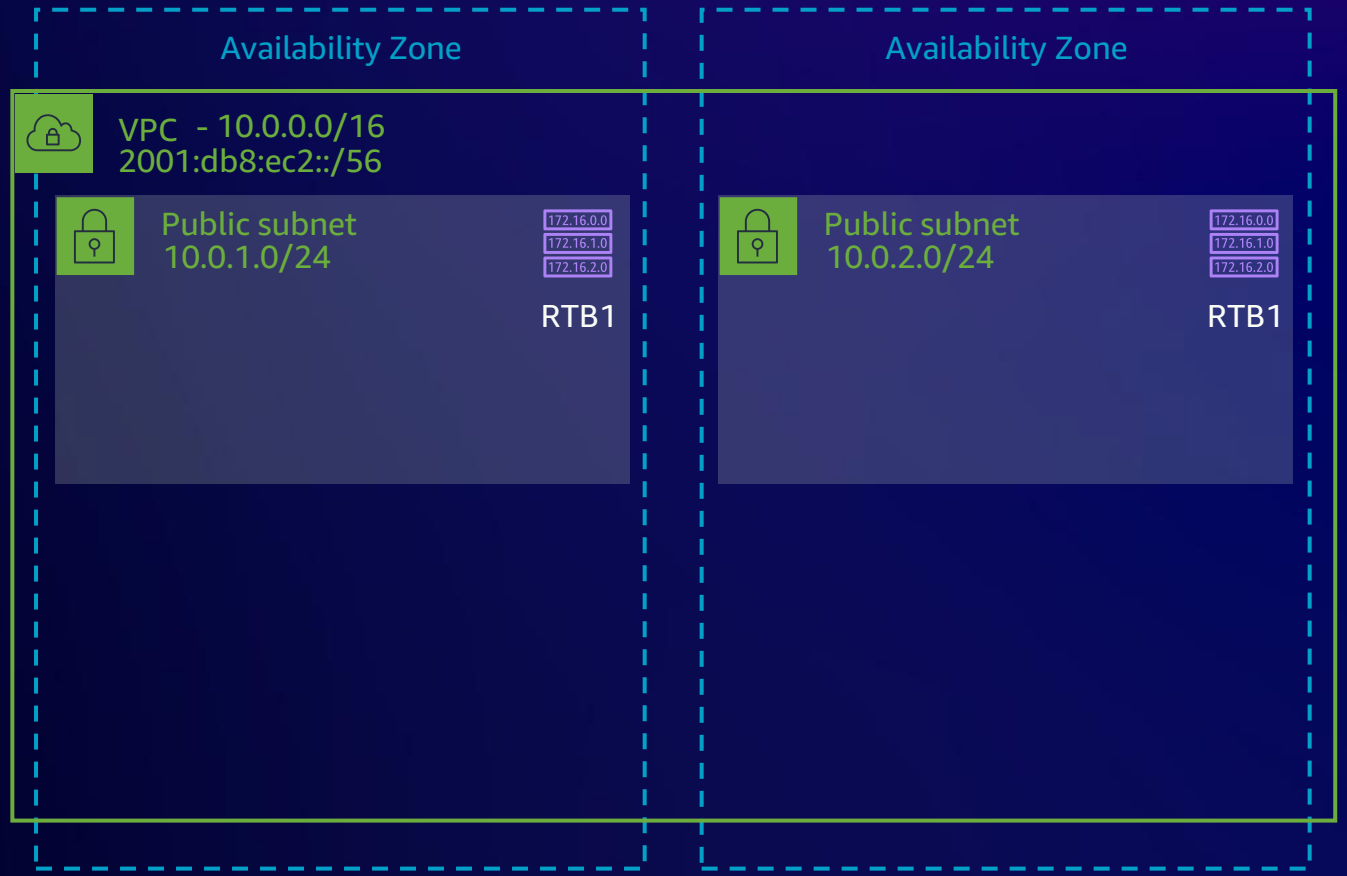
- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Routing tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Routing tables

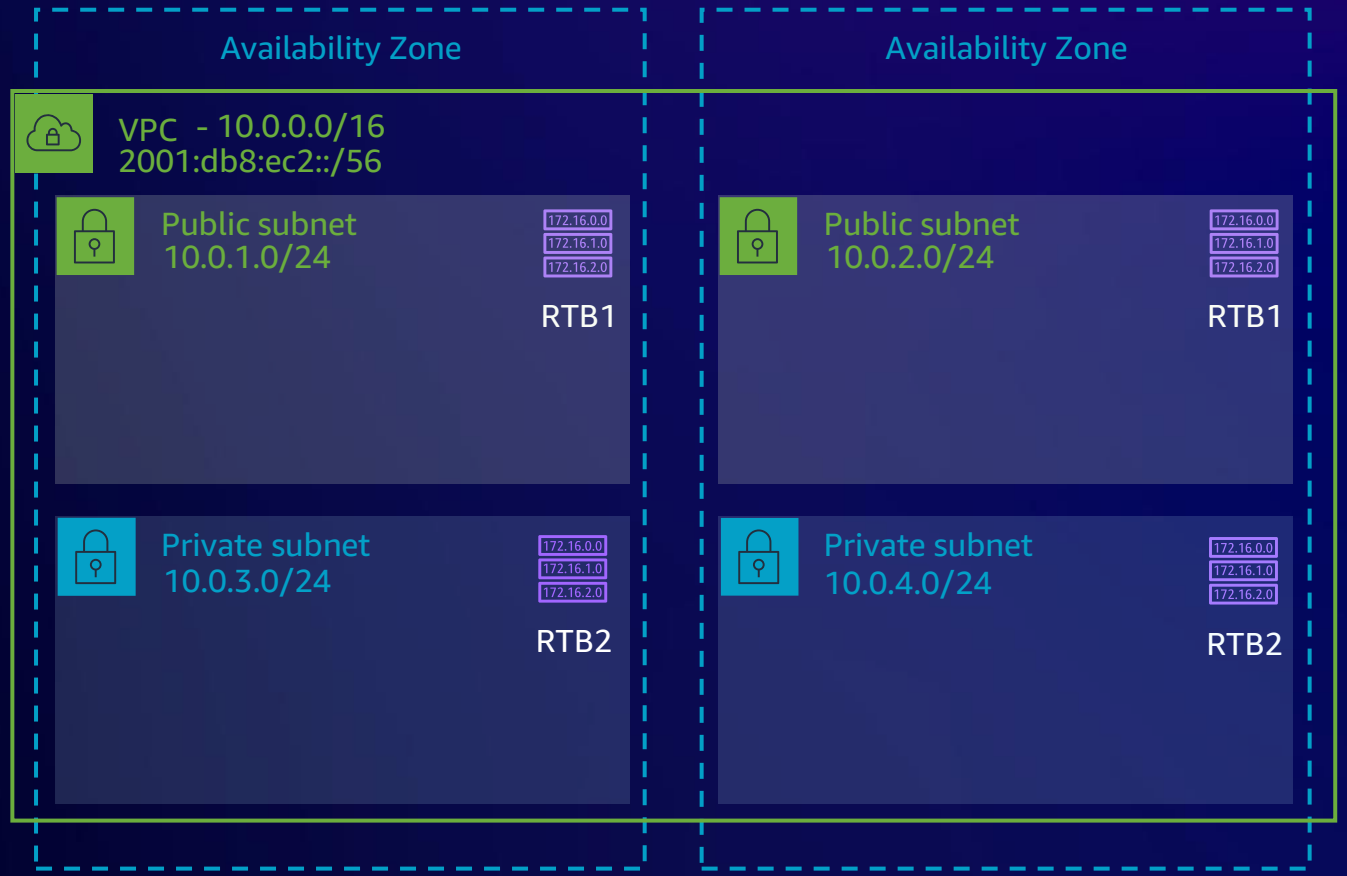
A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway

Routing tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Routing tables

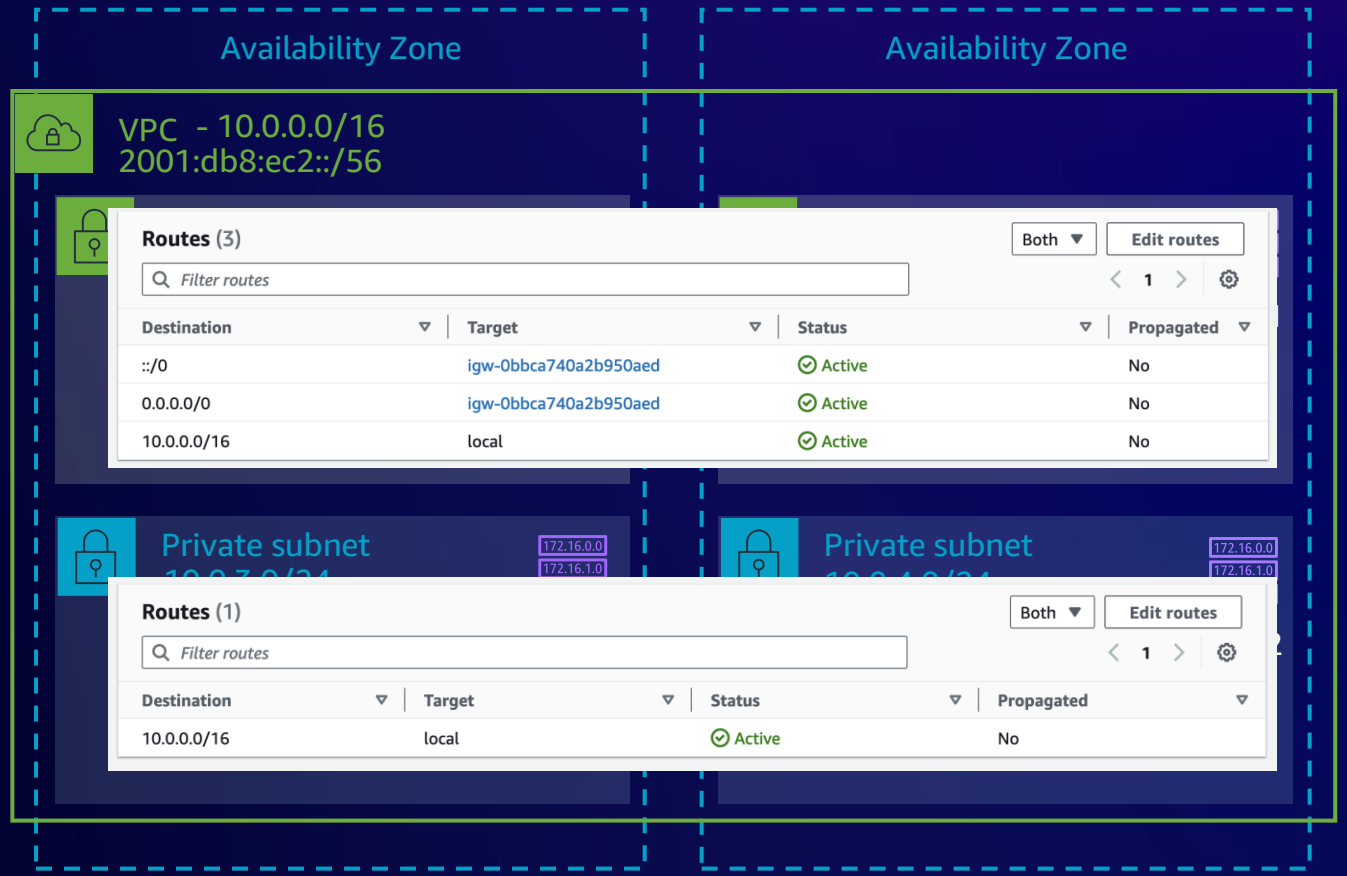
A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway

Routing tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet is directed.

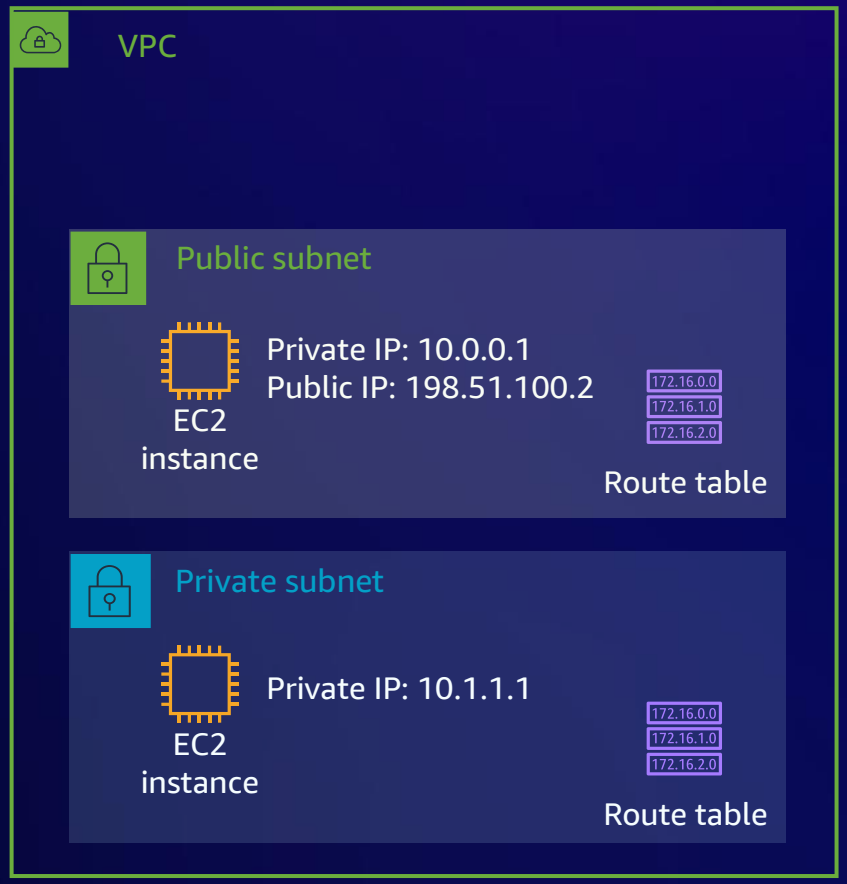
- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- 50 routes per route table by default
- Route quotas enforced separately for IPv4 and IPv6
- Subnets are referred to as “public subnets” when there is a route to an internet gateway



Internet gateway

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet

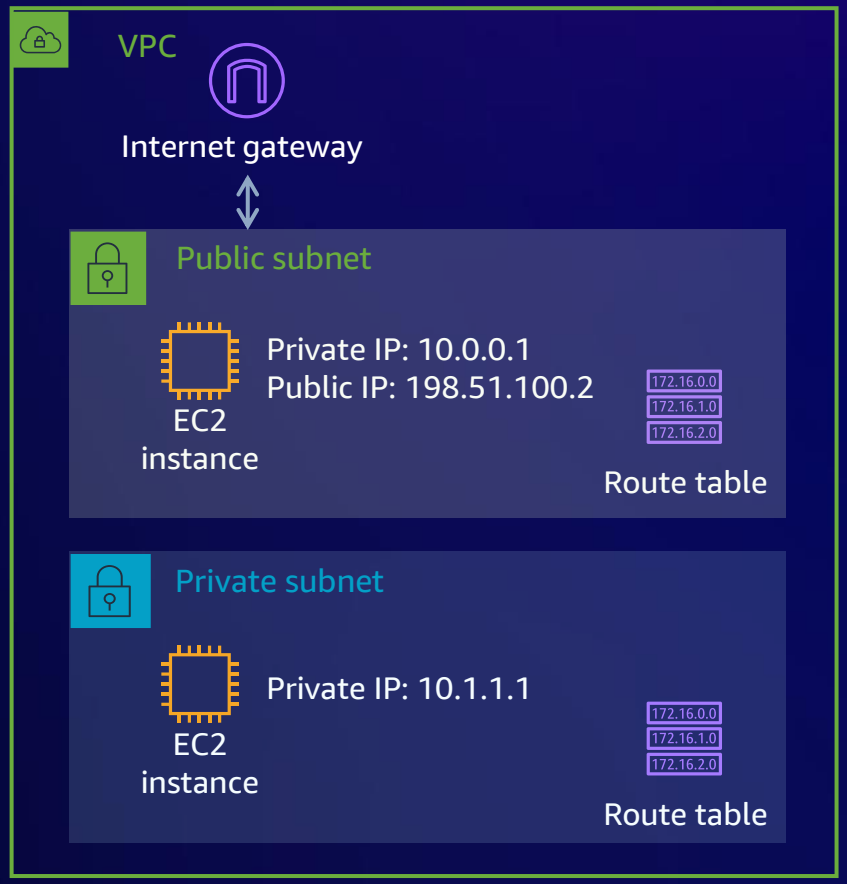
- Supports IPv4 and IPv6
- Connects your VPC subnets to the internet
- Must be referenced on the route table
- Subnets are referred to as “public subnets” when there is a route to an internet gateway
- No bandwidth constraints



Internet gateway

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet

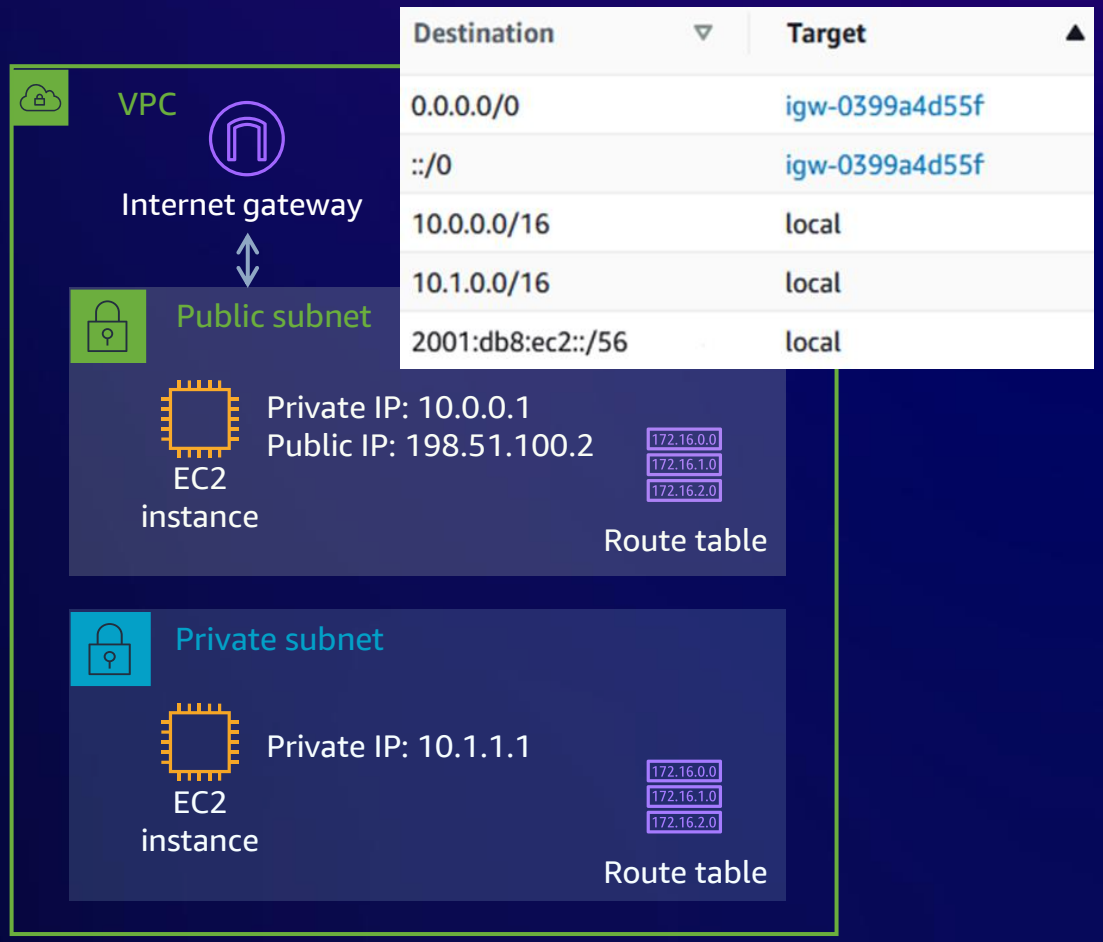
- Supports IPv4 and IPv6
- Connects your VPC subnets to the internet
- Must be referenced on the route table
- Subnets are referred to as “public subnets” when there is a route to an internet gateway
- No bandwidth constraints



Internet gateway

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet

- Supports IPv4 and IPv6
- Connects your VPC subnets to the internet
- Must be referenced on the route table
- Subnets are referred to as “public subnets” when there is a route to an internet gateway
- No bandwidth constraints

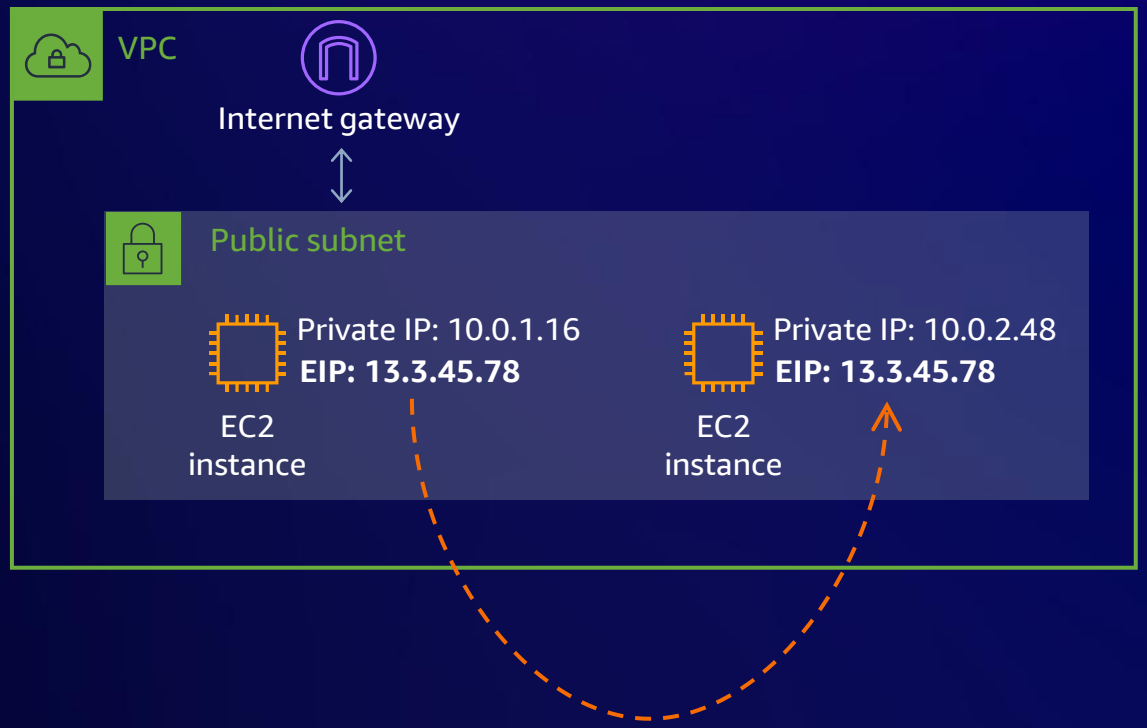


Destination	Target
0.0.0.0/0	igw-0399a4d55f
::/0	igw-0399a4d55f
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local

Public IP addressing: Elastic IP address

An elastic IP address is a static IPv4 address designed for dynamic cloud computing

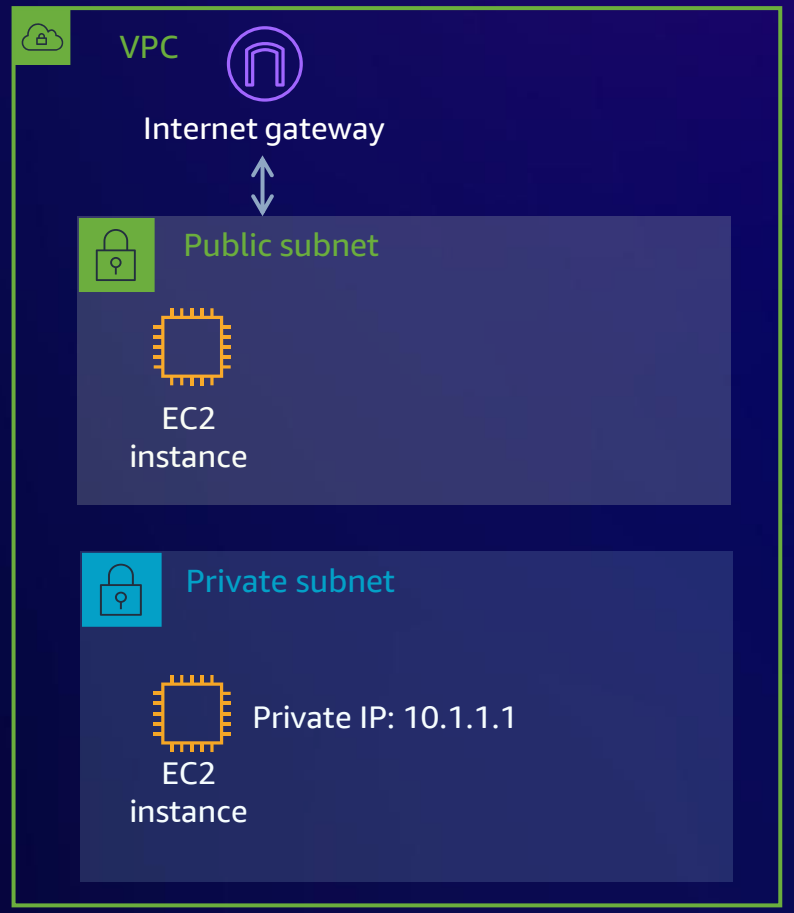
- Static, public IPv4 address, associated with your AWS account
- Dynamically assigned
- Specific to a Region
- Can be associated with an instance or network interface
- Can be remapped to another instance in your account



Outbound traffic: NAT gateway

A NAT gateway is a network address translation (NAT) service

- Enable outbound connection to the internet
- No incoming connection
- Fully managed by AWS
- Highly available
- Up to 45 Gbps aggregate bandwidth
- Supports TCP, UDP, and ICMP protocols
- Private NAT supported



Outbound traffic: NAT gateway

A NAT gateway is a network address translation (NAT) service

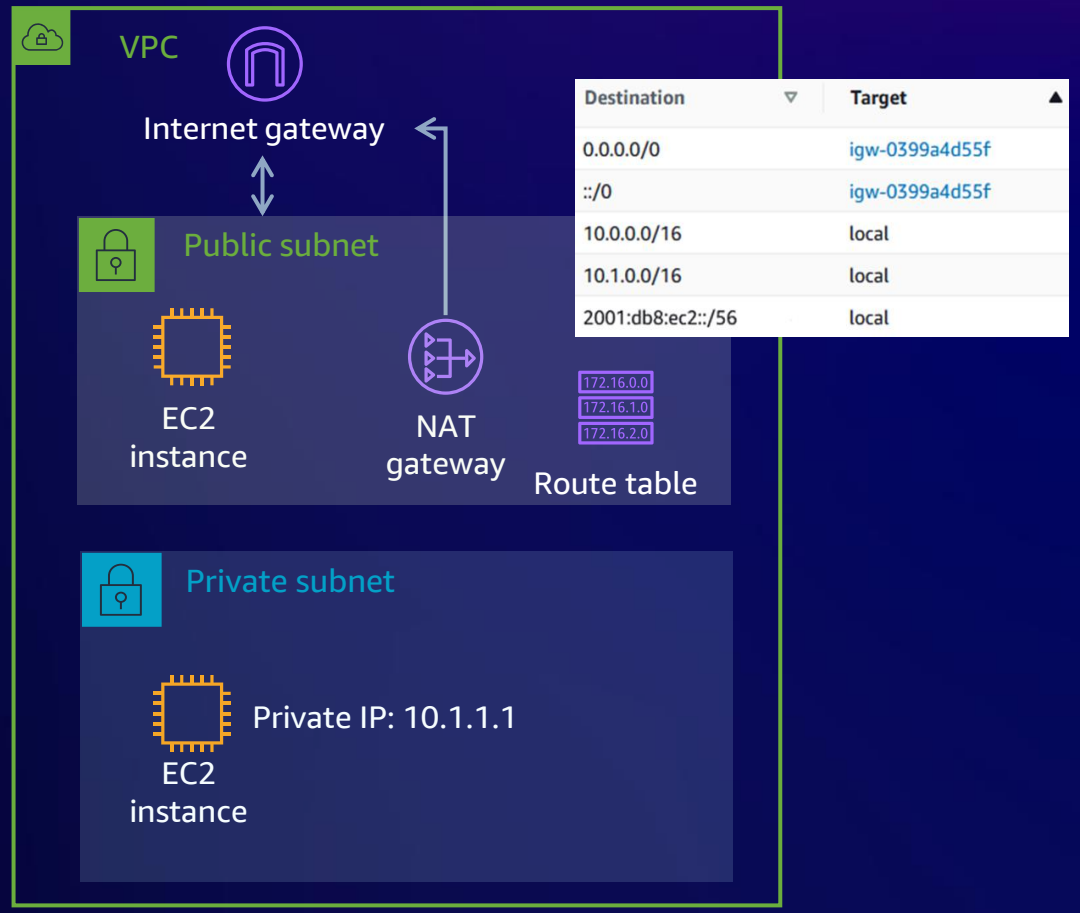
- Enable outbound connection to the internet
- No incoming connection
- Fully managed by AWS
- Highly available
- Up to 45 Gbps aggregate bandwidth
- Supports TCP, UDP, and ICMP protocols
- Private NAT supported

Destination	Target
0.0.0.0/0	igw-0399a4d55f
::/0	igw-0399a4d55f
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local

Outbound traffic: NAT gateway

A NAT gateway is a network address translation (NAT) service

- Enable outbound connection to the internet
- No incoming connection
- Fully managed by AWS
- Highly available
- Up to 45 Gbps aggregate bandwidth
- Supports TCP, UDP, and ICMP protocols
- Private NAT supported

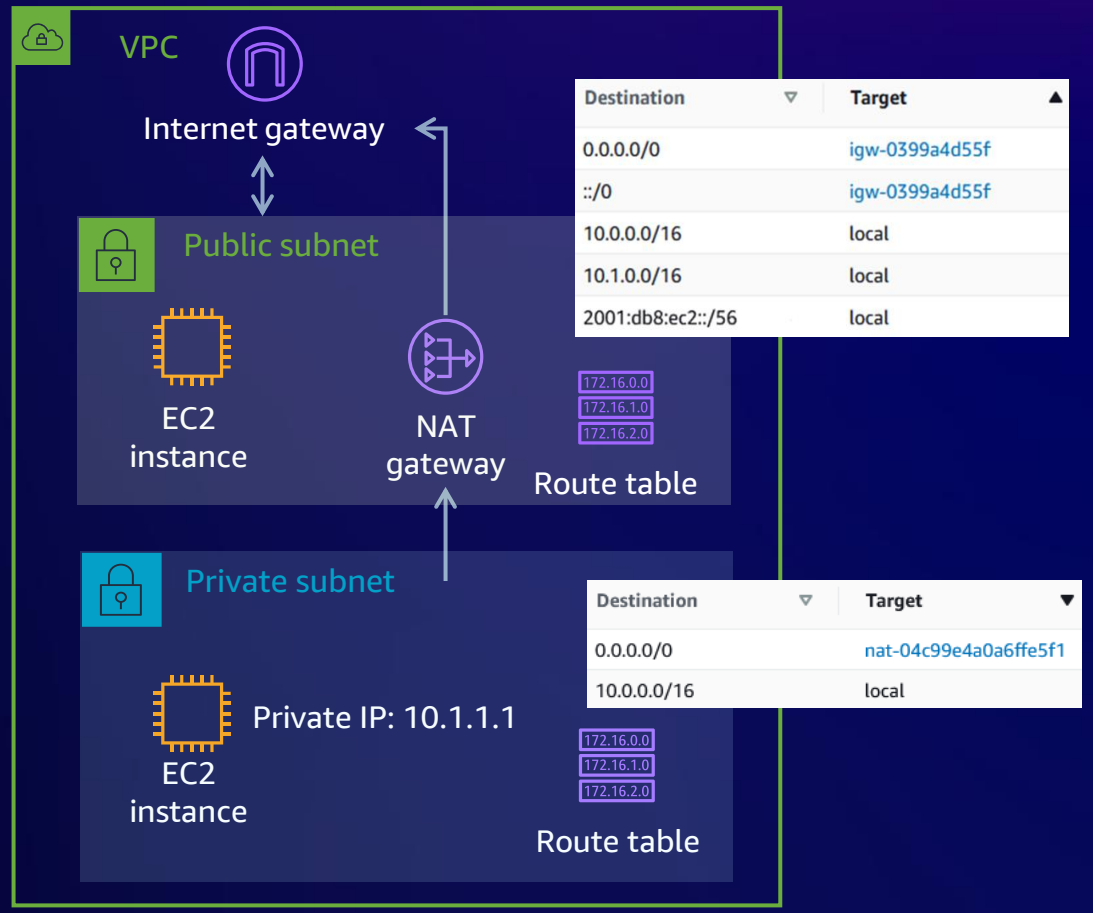


Destination	Target
0.0.0.0/0	igw-0399a4d55f
::/0	igw-0399a4d55f
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local

Outbound traffic: NAT gateway

A NAT gateway is a network address translation (NAT) service

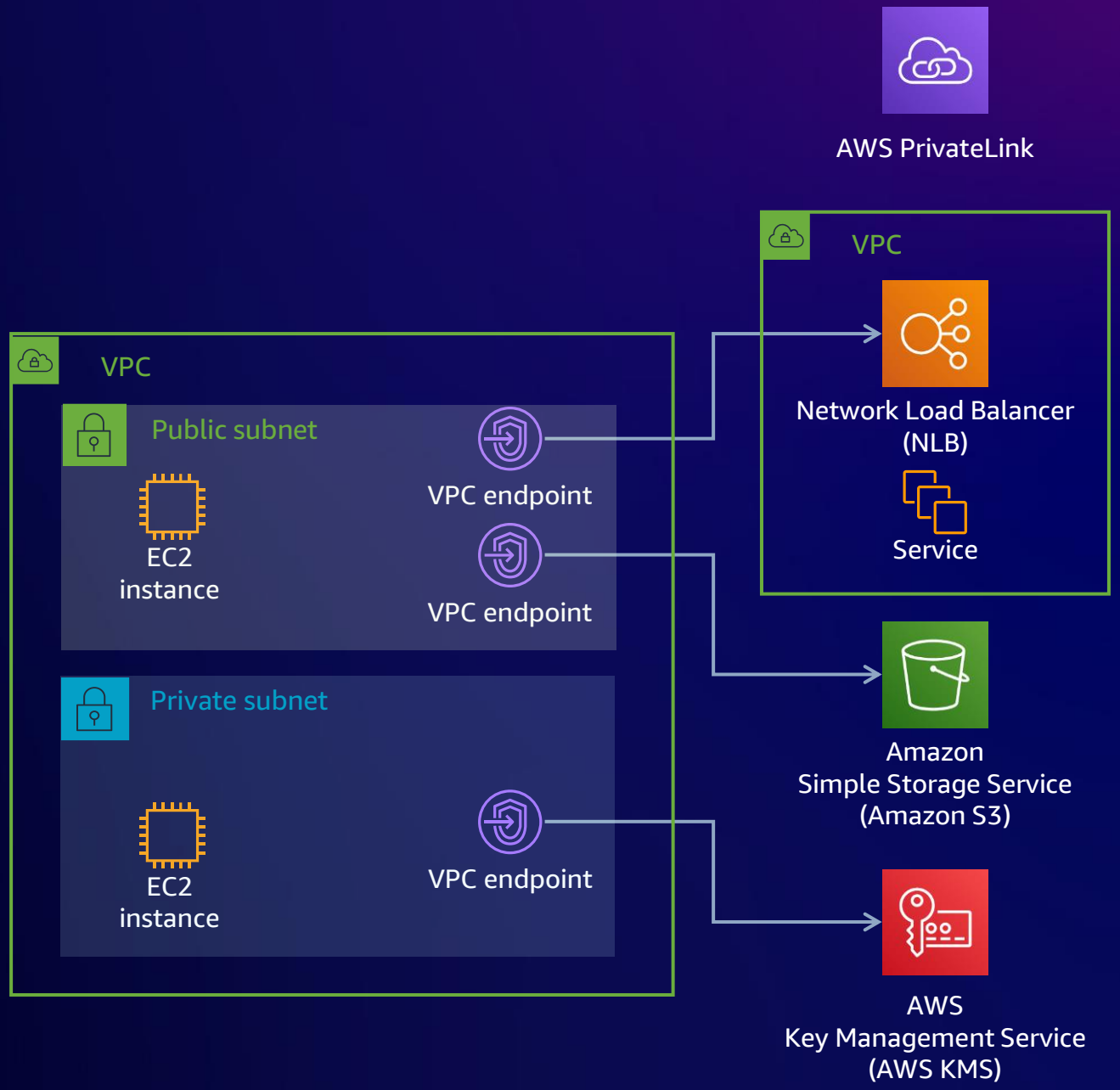
- Enable outbound connection to the internet
- No incoming connection
- Fully managed by AWS
- Highly available
- Up to 45 Gbps aggregate bandwidth
- Supports TCP, UDP, and ICMP protocols
- Private NAT supported



VPC endpoints

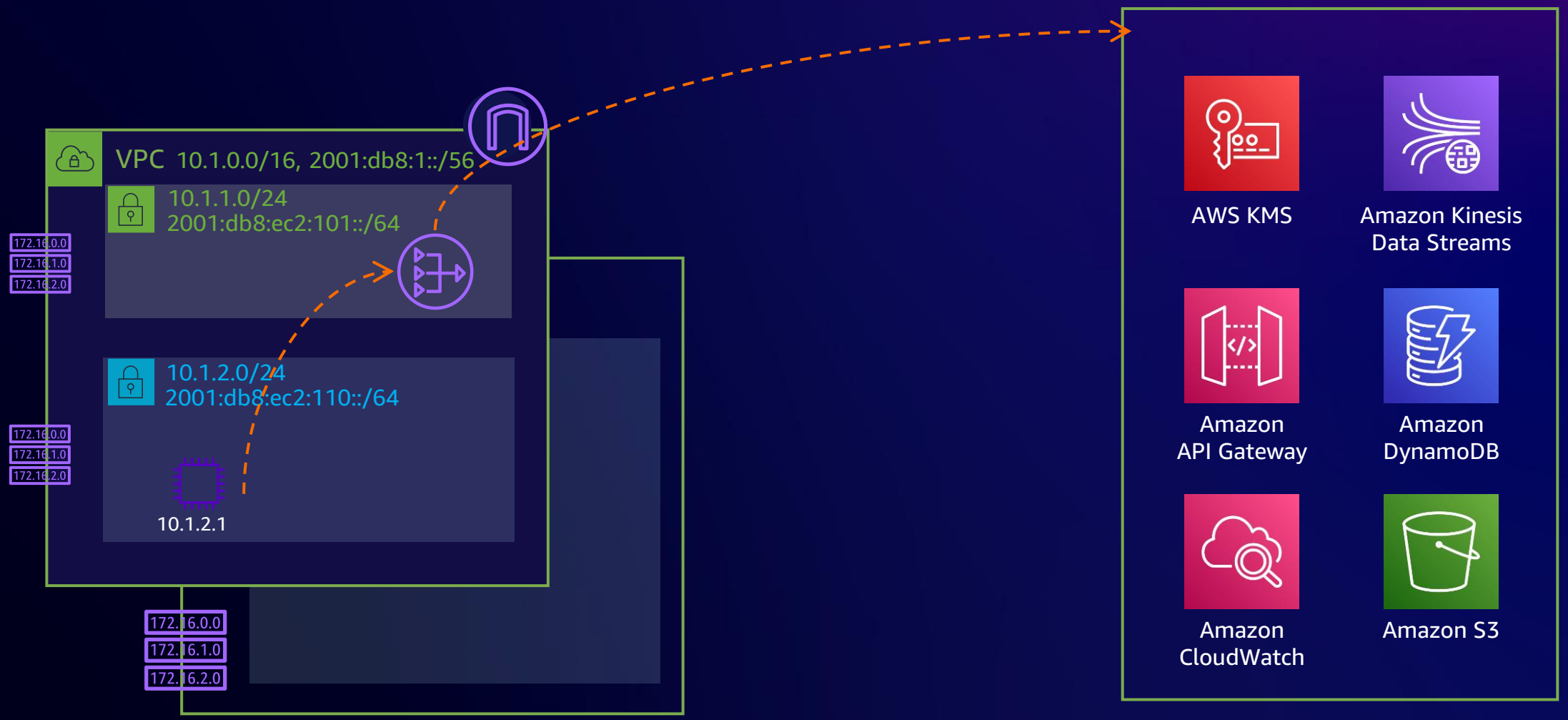
A VPC endpoint enables customers to privately connect to supported AWS services and VPC endpoint services powered by AWS PrivateLink

- Doesn't require public IPs or internet connectivity
- Horizontally scaled, redundant, and highly available
- Robust access control



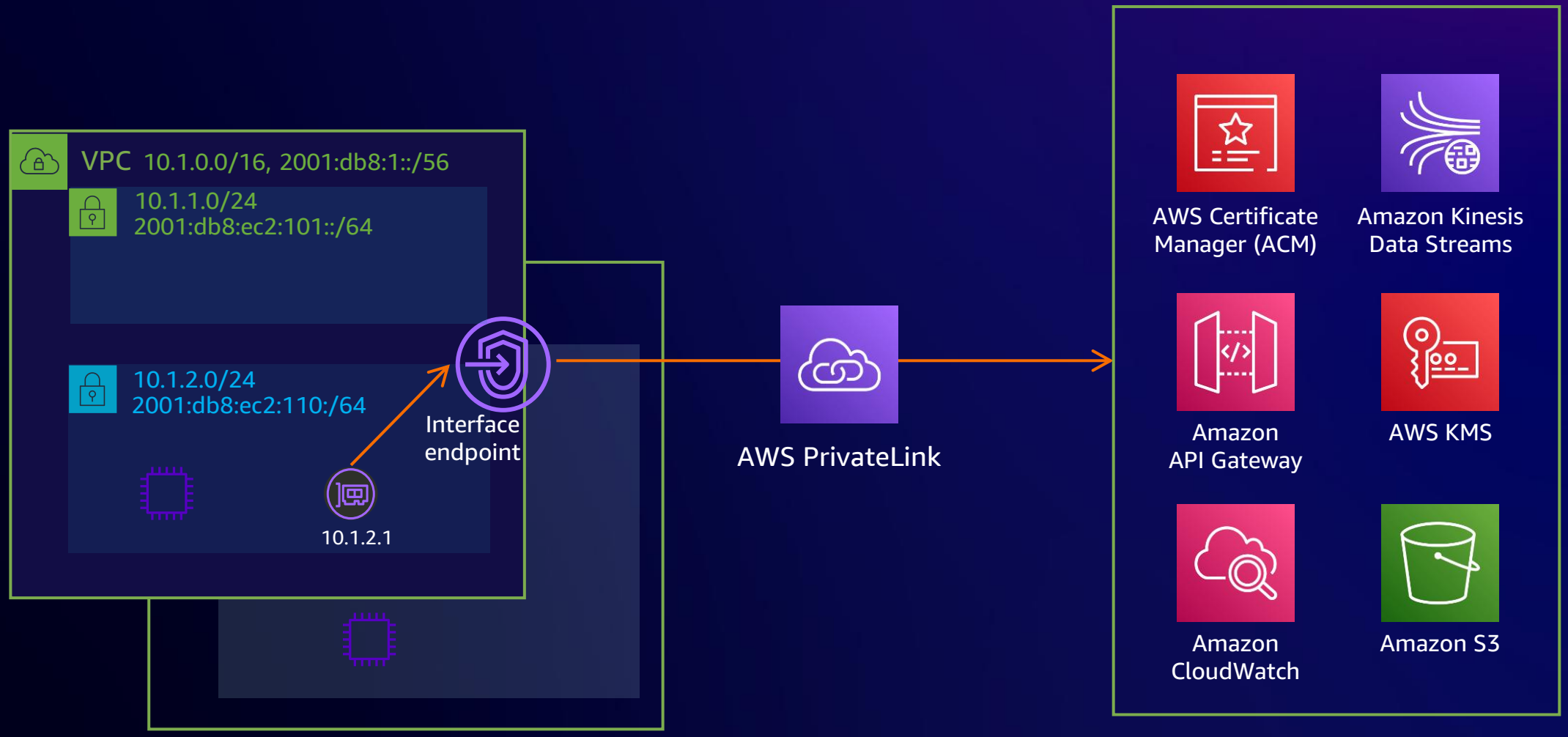
Accessing AWS services

WITHOUT VPC ENDPOINTS



Accessing AWS services

WITH VPC ENDPOINTS



AmazonProvidedDNS for VPC

AmazonProvidedDNS

- VPC+2 resolver
- 169.254.169.253
- fd00:ec2::253

DNS host names

- Private DNS name
- Resource-based private DNS name
- Public DNS name

VPC 10.0.0.0/16, 2001:db8:ec2::/56

Instance

ip-10-0-0-12.us-east-2.compute.internal

i-0e718ecec005e295e.us-east-2.compute.internal

ec2-3-3-3-3.us-east-2.compute.amazonaws.com

10.0.0.2 / fd00:ec2::253
AmazonProvidedDNS

VPC ID	State	DNS hostnames	DNS resolution
vpc-0f61364f7d544be00	Available	Enabled	Enabled

Route 53 private hosted zones

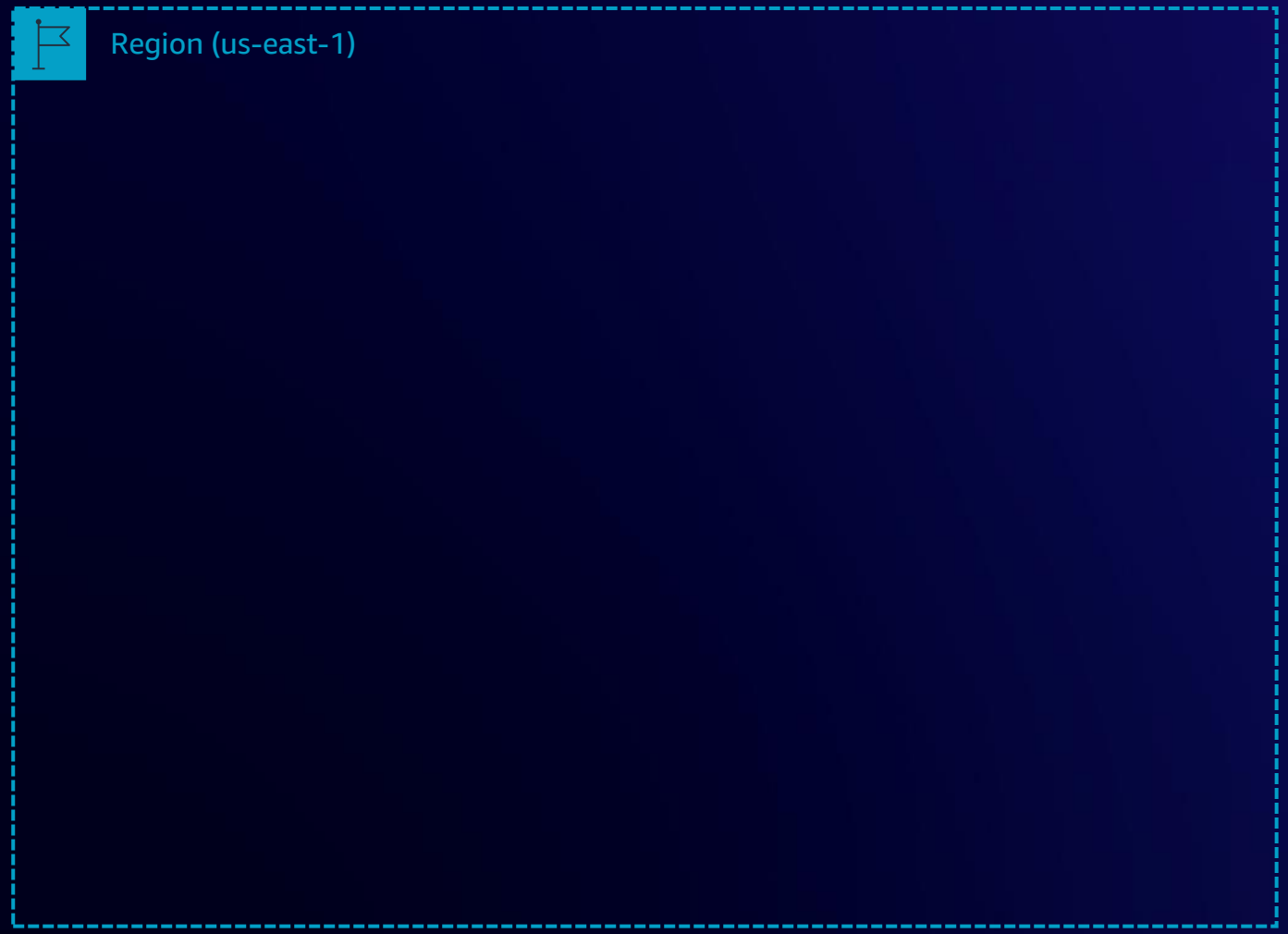
DNS records

db.example.aws
A 10.0.0.1
AAAA 2001:db8:ec2::1

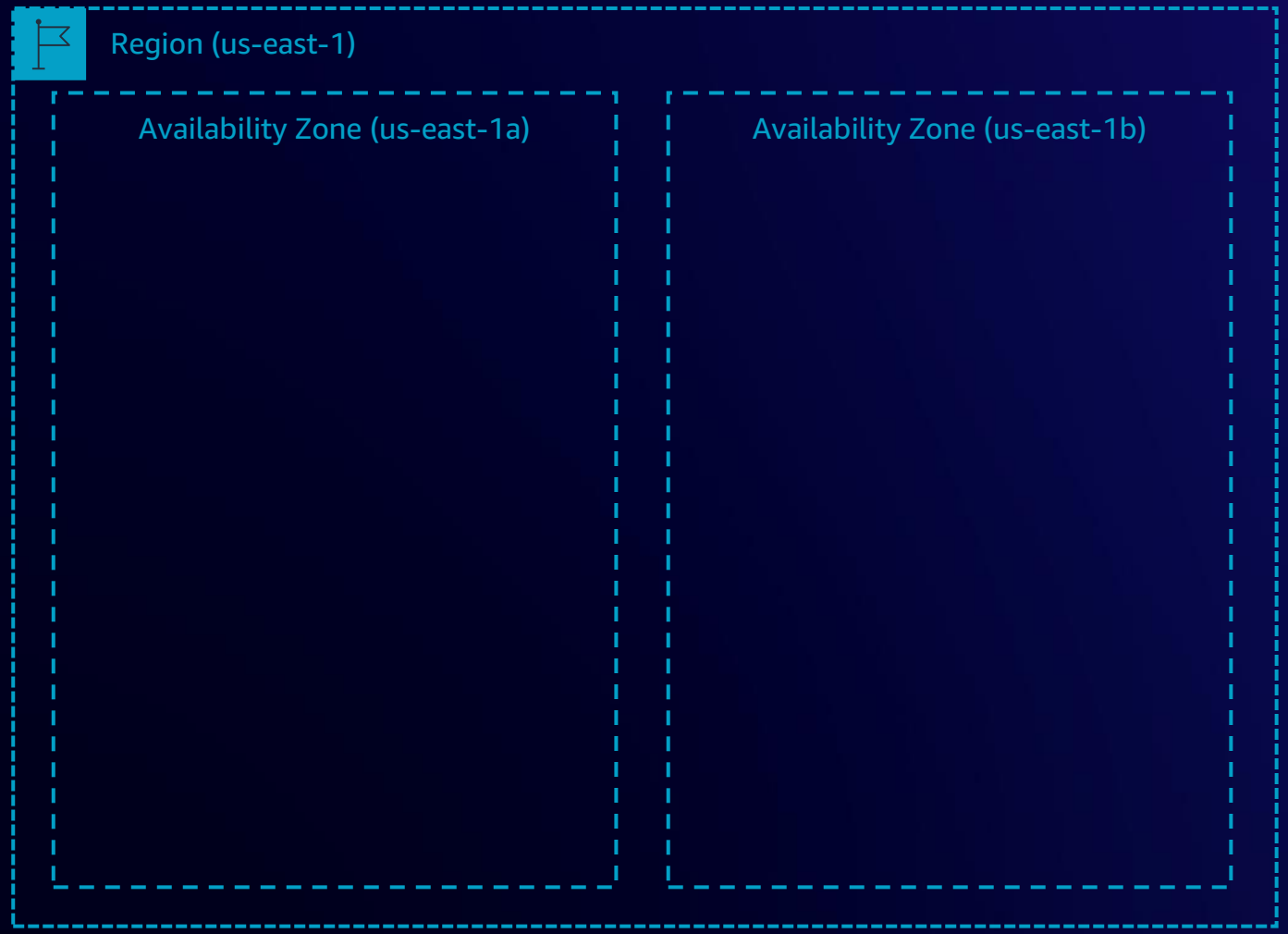
10.0.0.2
Route 53 Resolver

Private hosted zone: example.aws

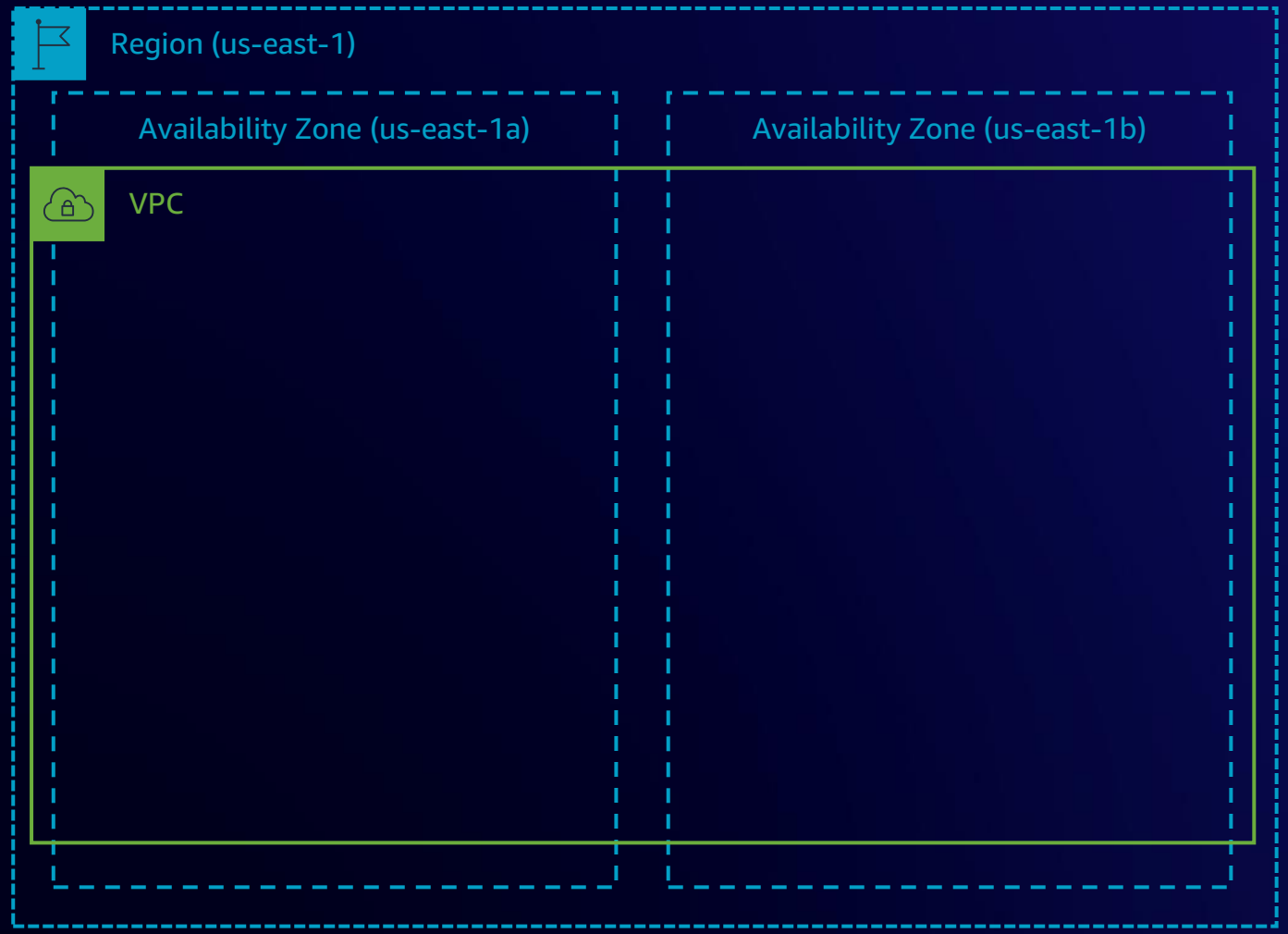
Bringing it together: Your single VPC



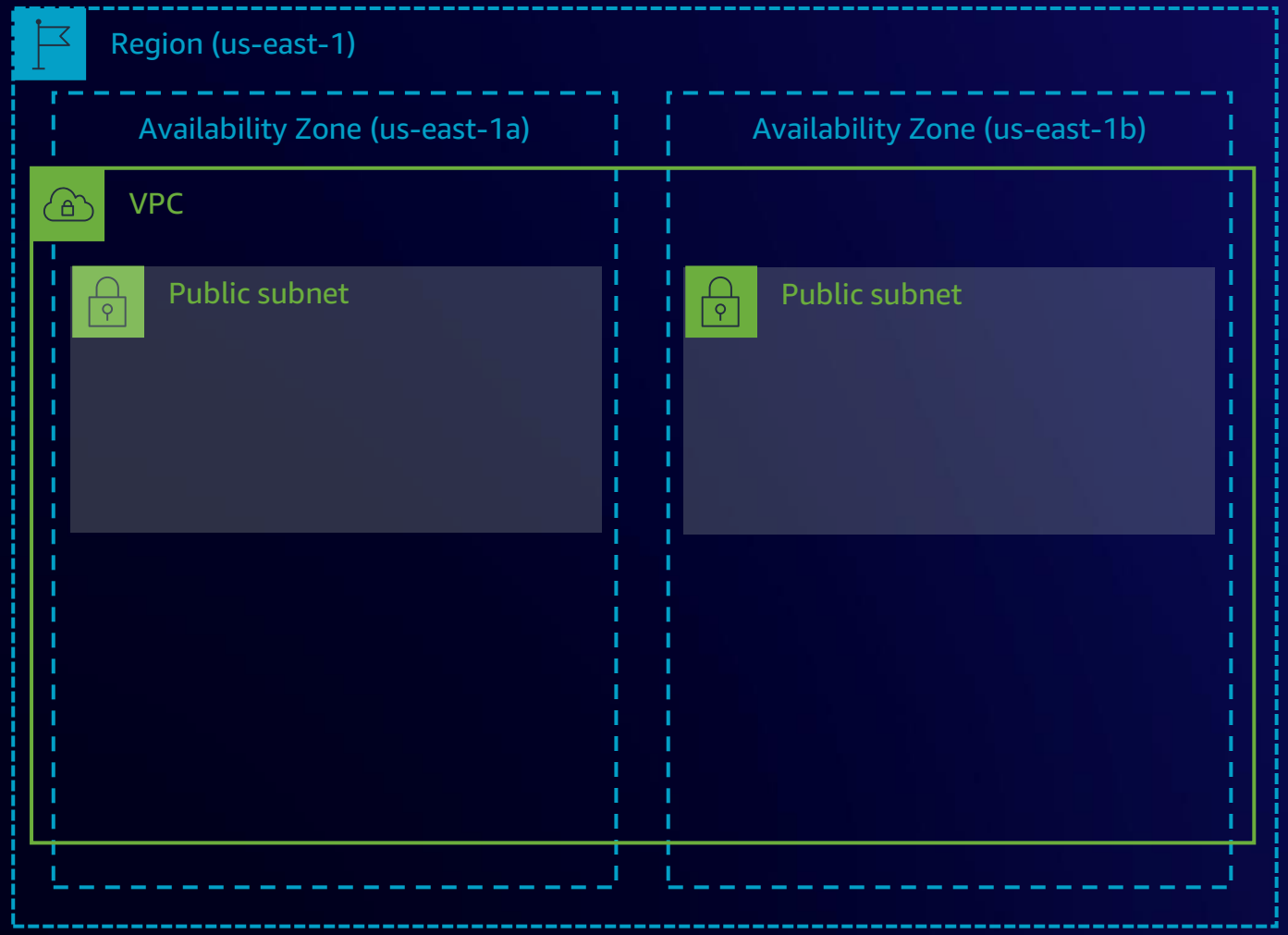
Bringing it together: Your single VPC



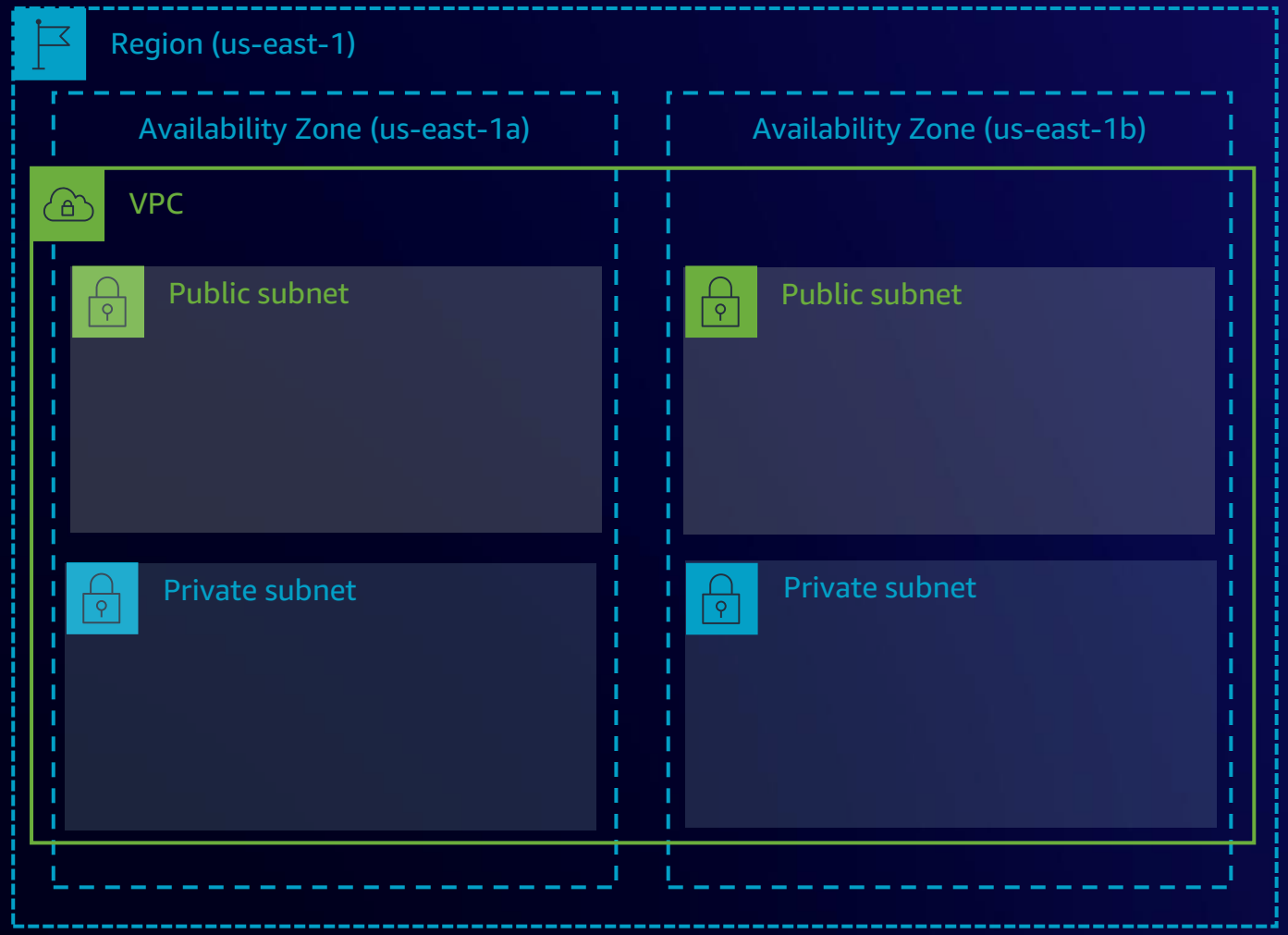
Bringing it together: Your single VPC



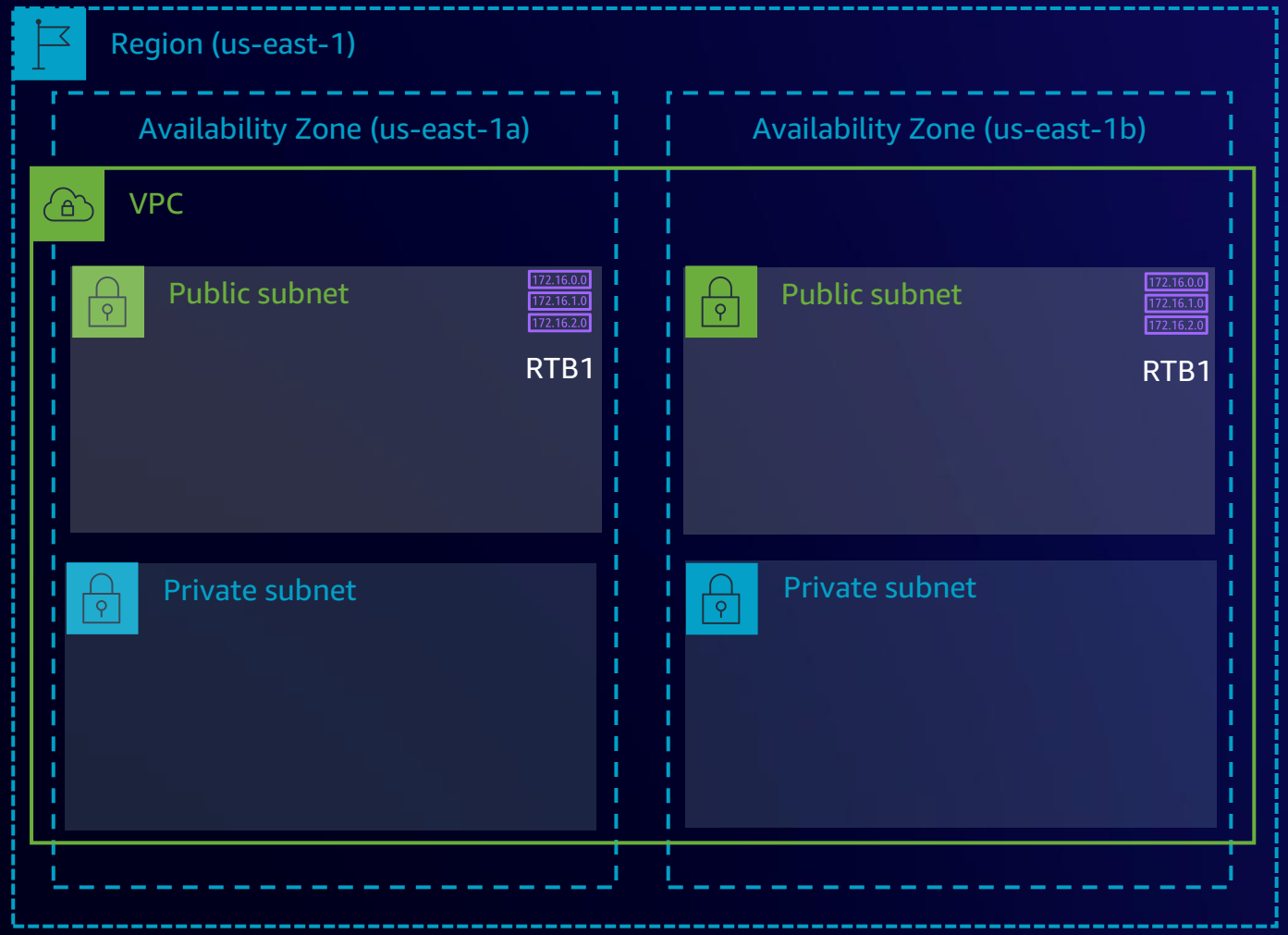
Bringing it together: Your single VPC



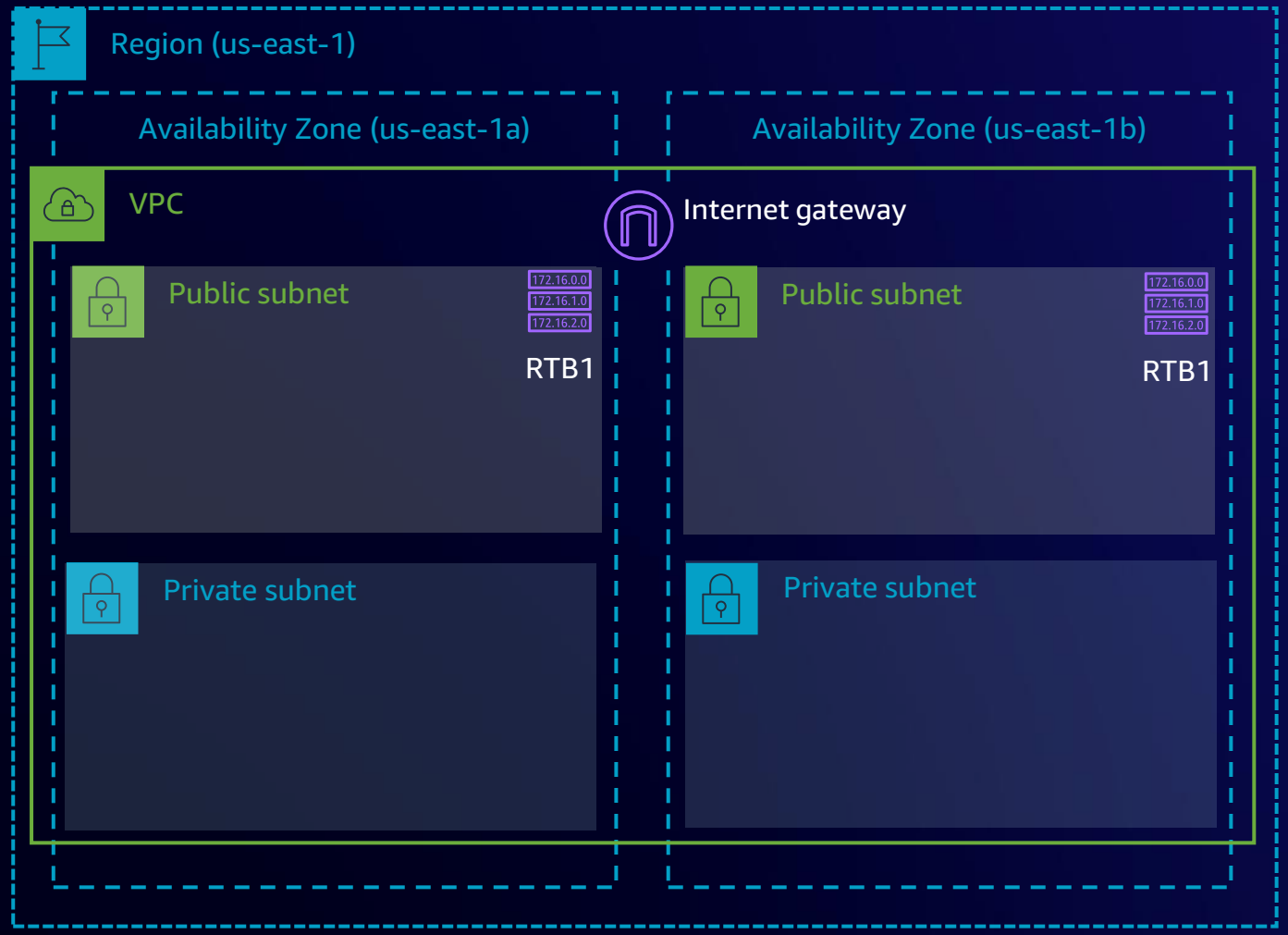
Bringing it together: Your single VPC



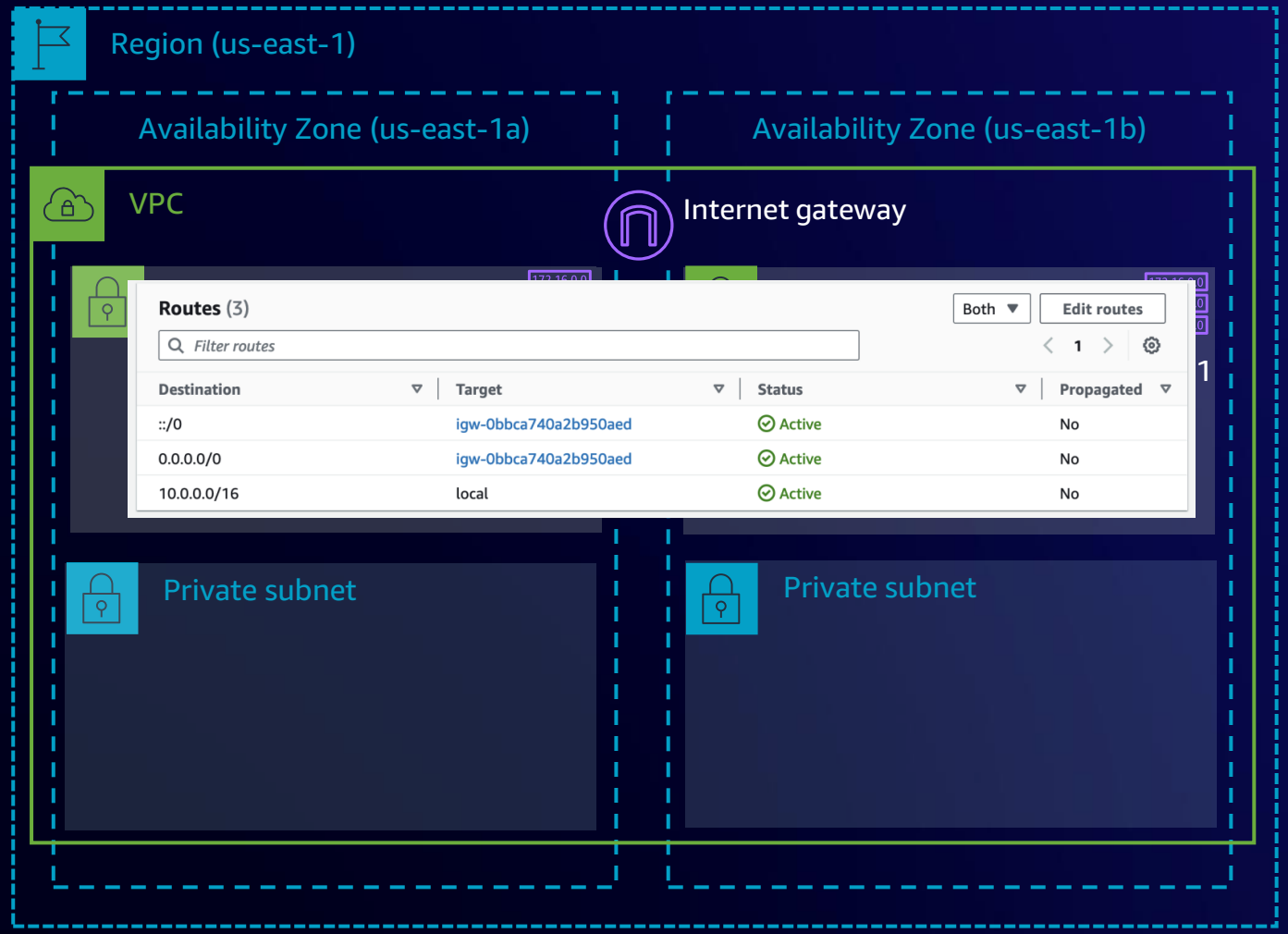
Bringing it together: Your single VPC



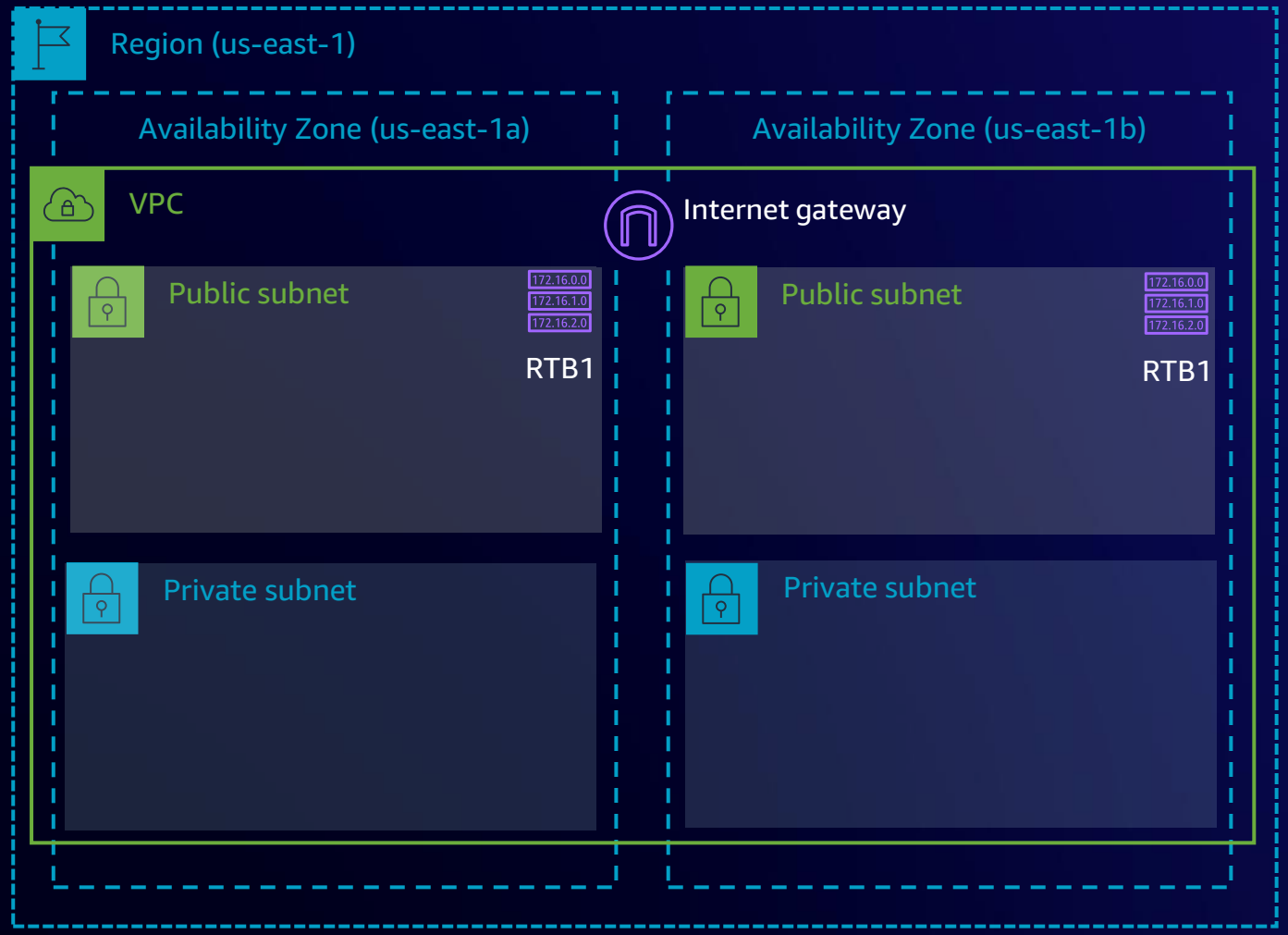
Bringing it together: Your single VPC



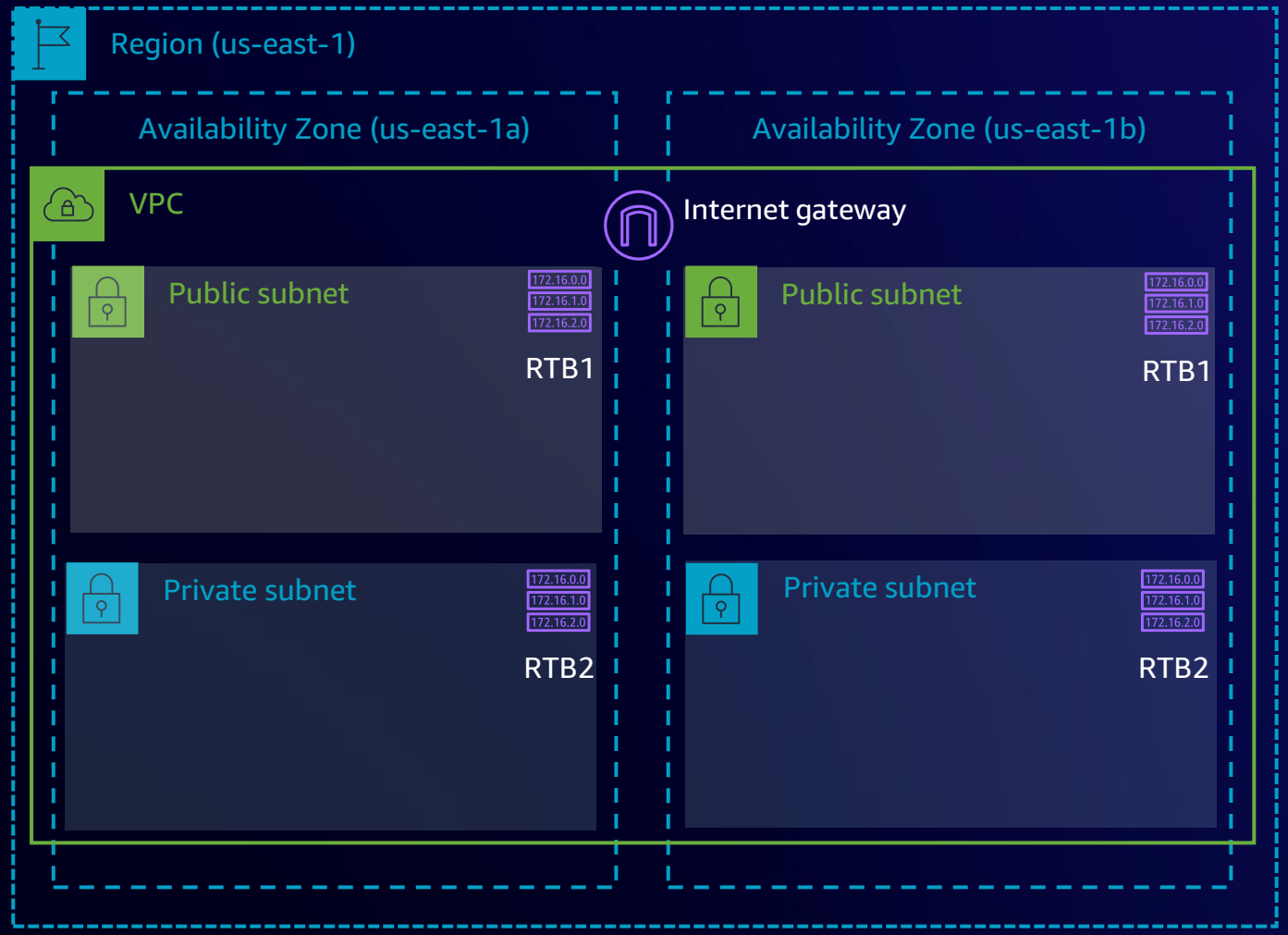
Bringing it together: Your single VPC



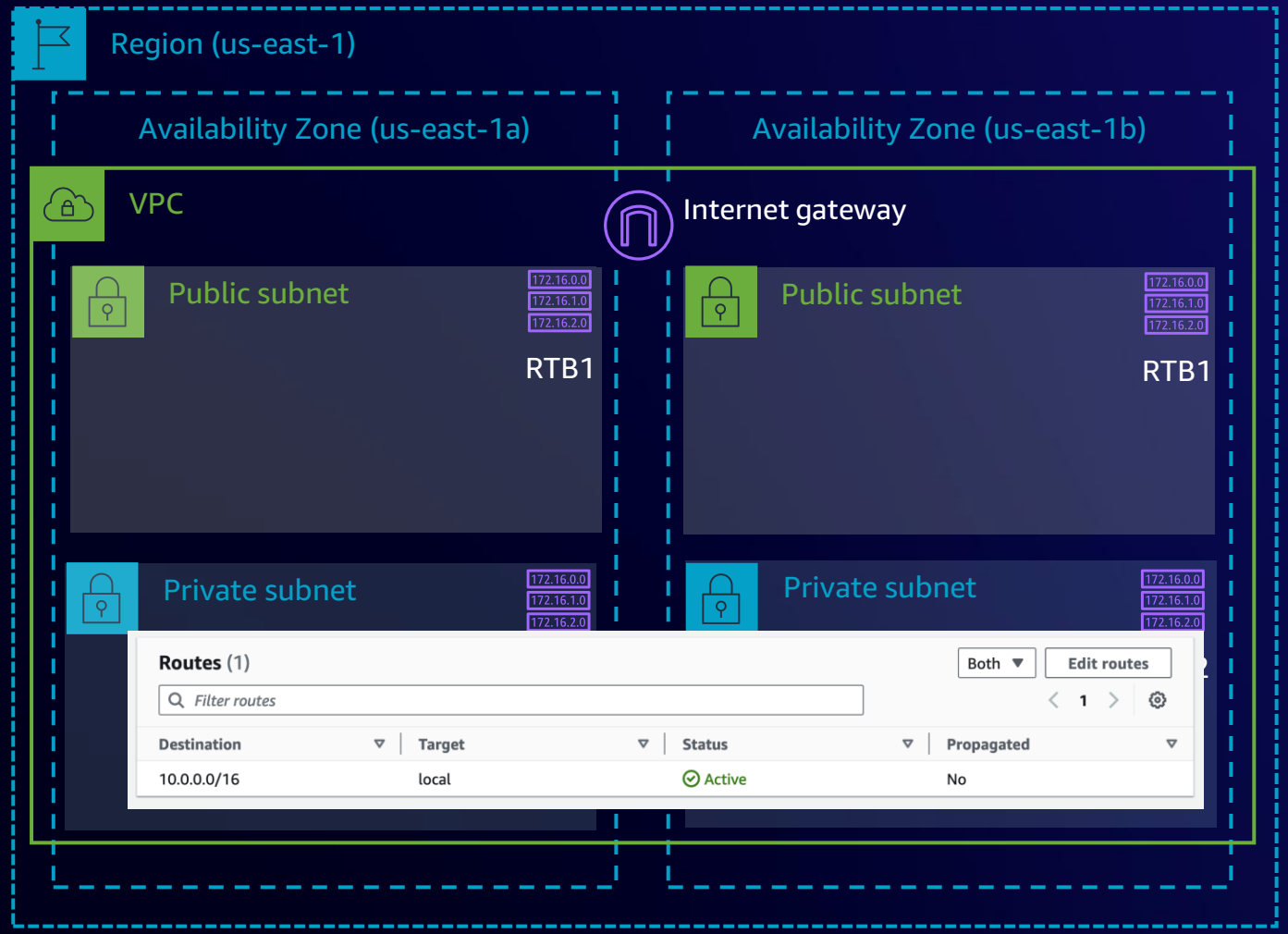
Bringing it together: Your single VPC



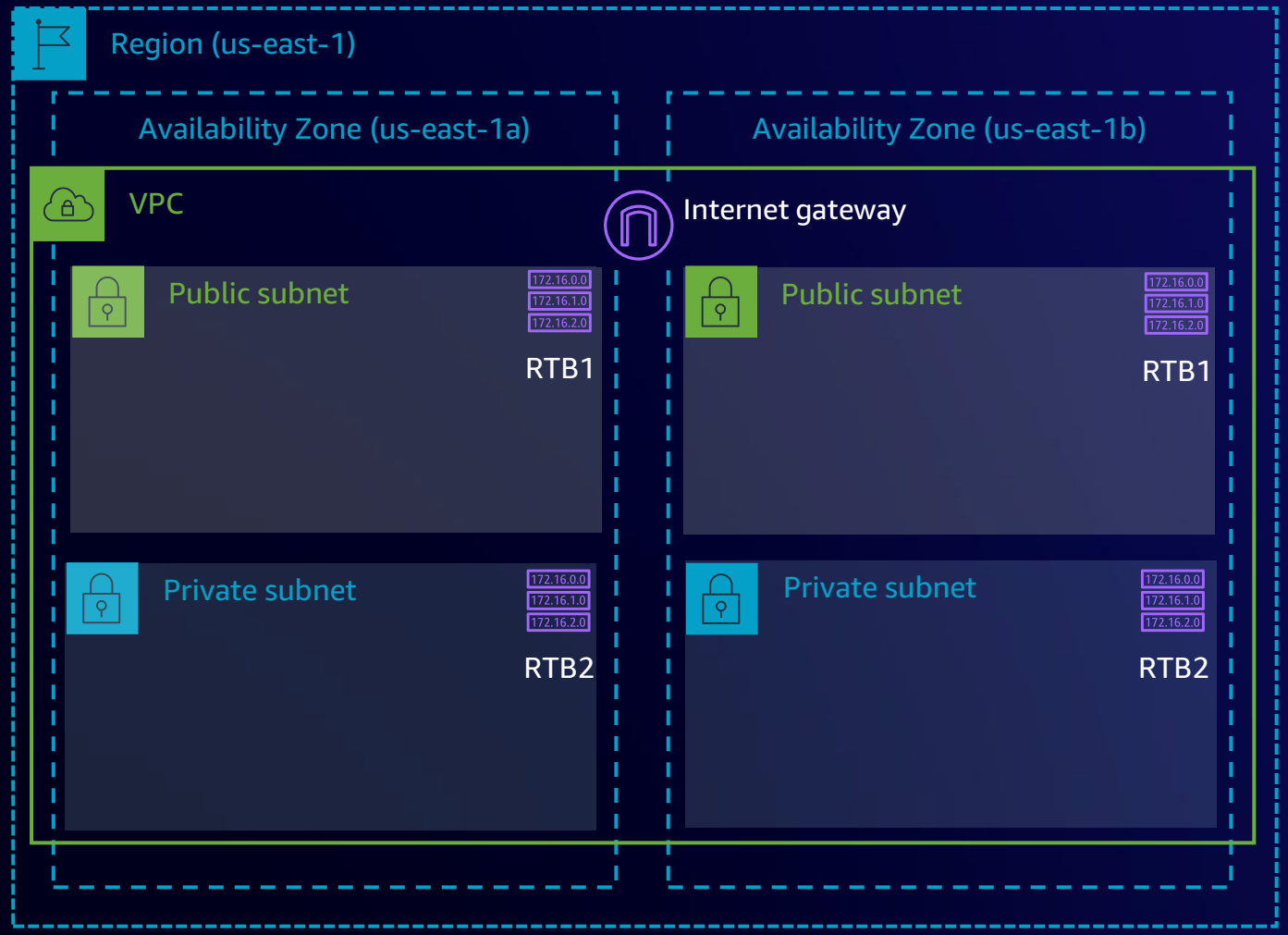
Bringing it together: Your single VPC



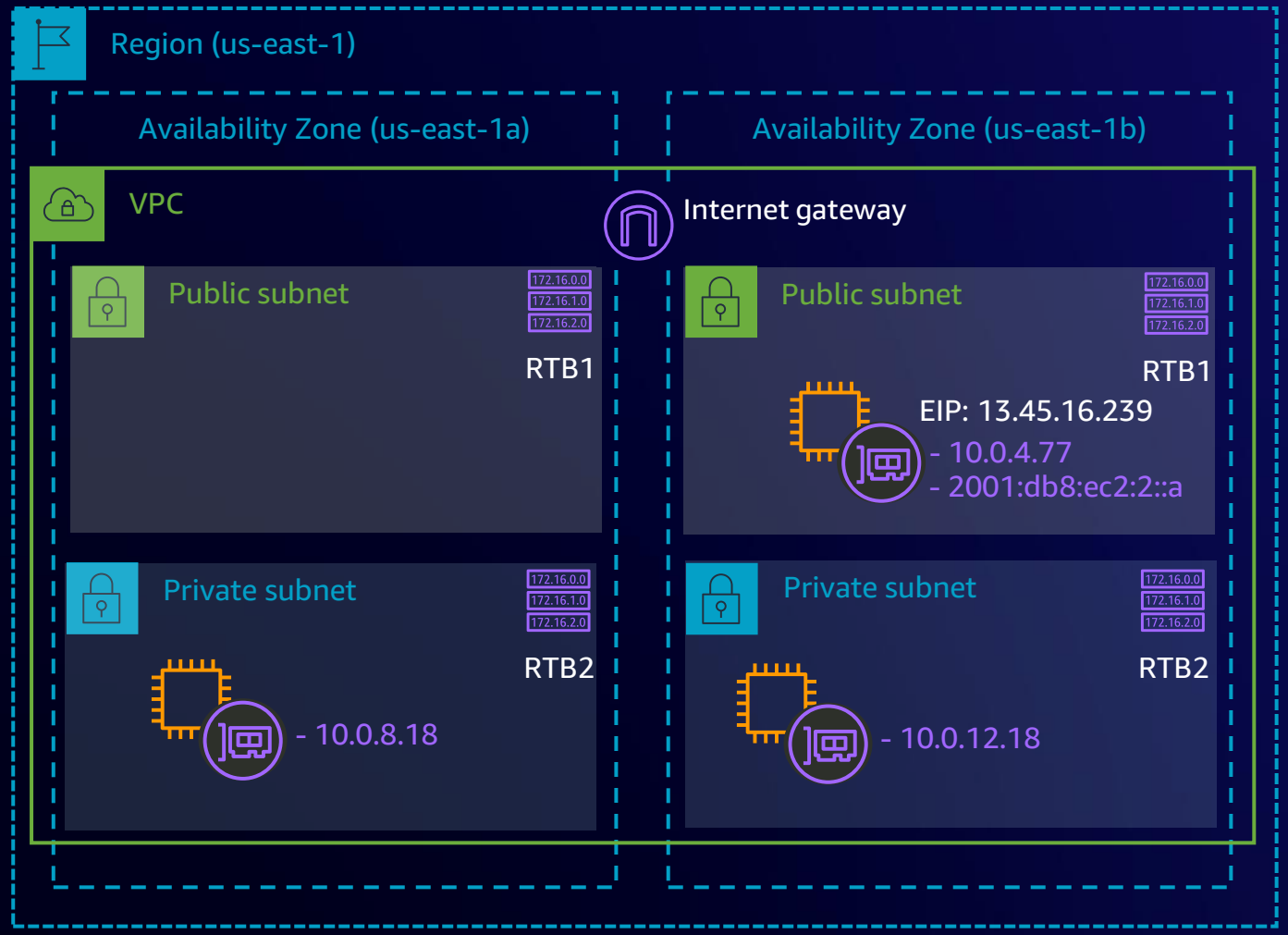
Bringing it together: Your single VPC



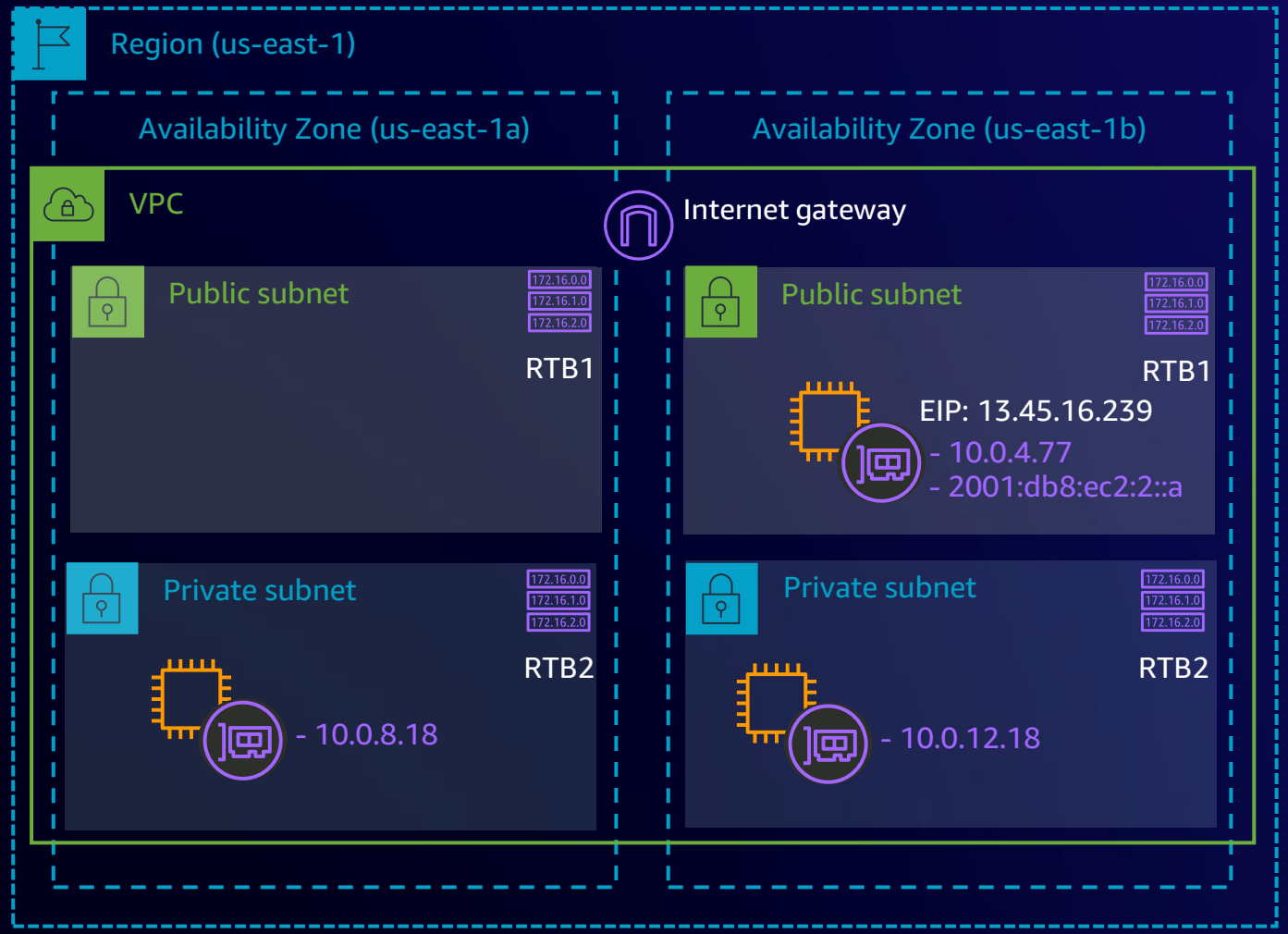
Bringing it together: Your single VPC

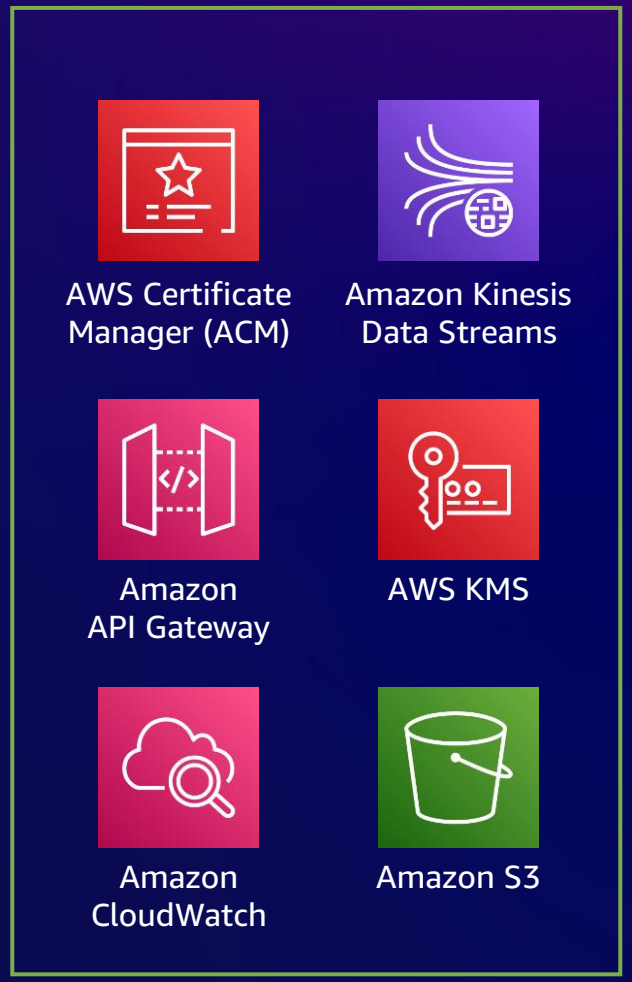


Bringing it together: Your single VPC

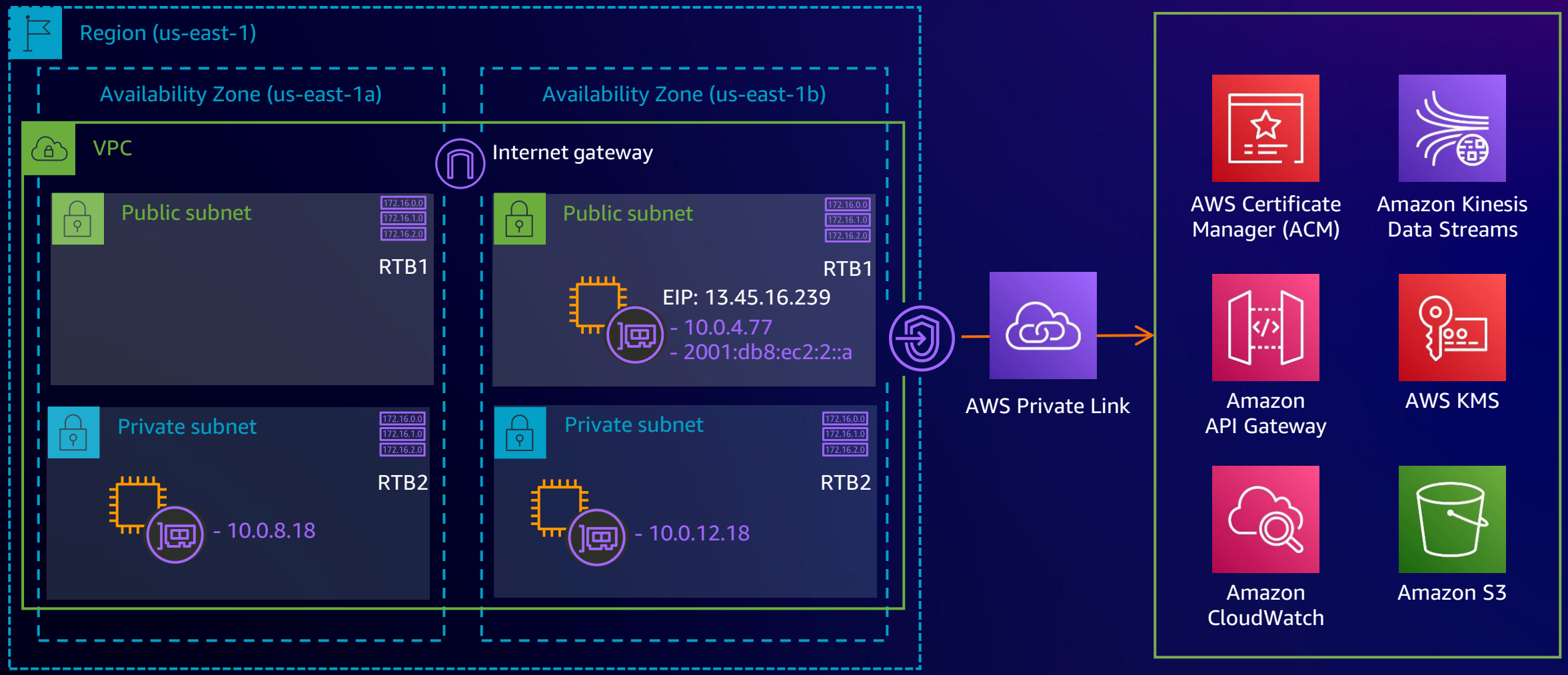


Bringing it together: Your single VPC





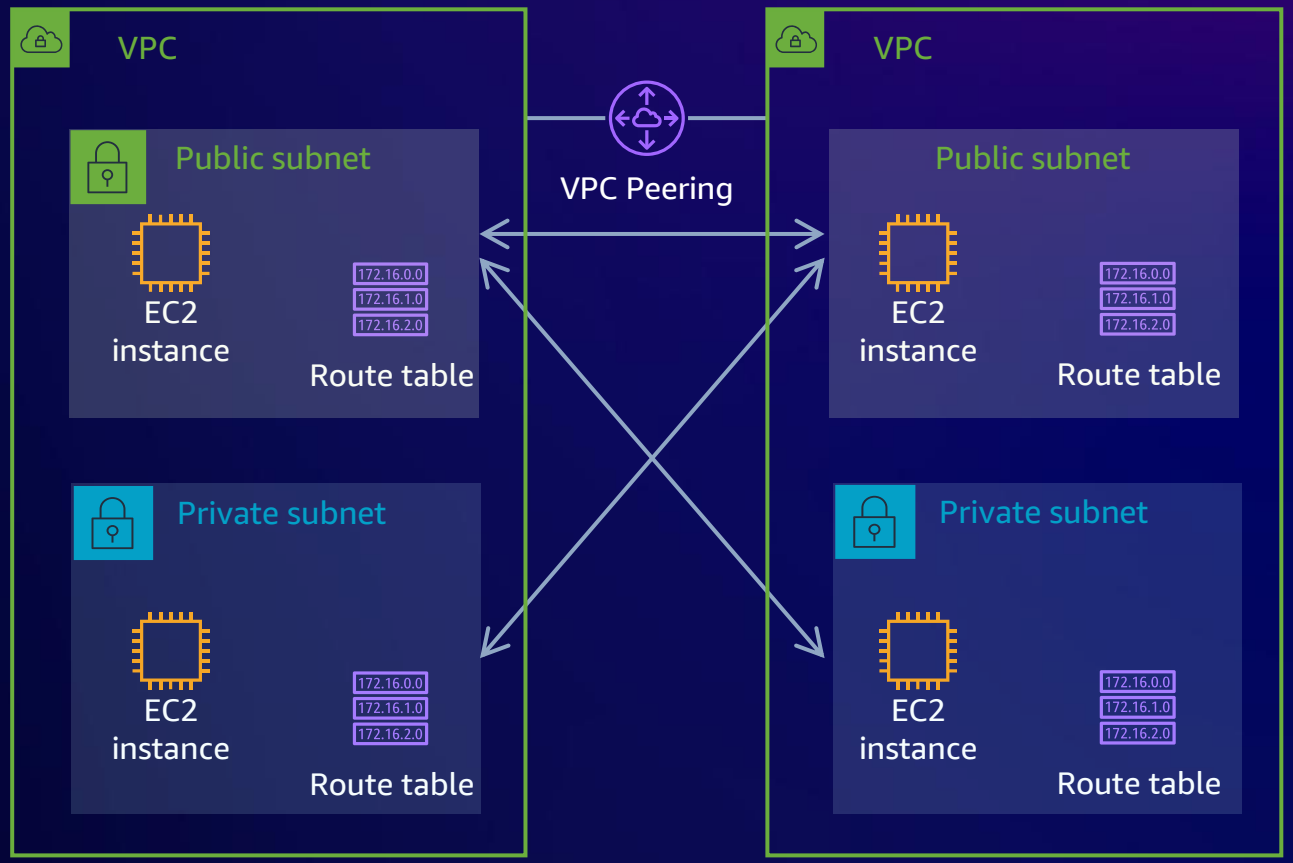
Bringing it together: Your single VPC



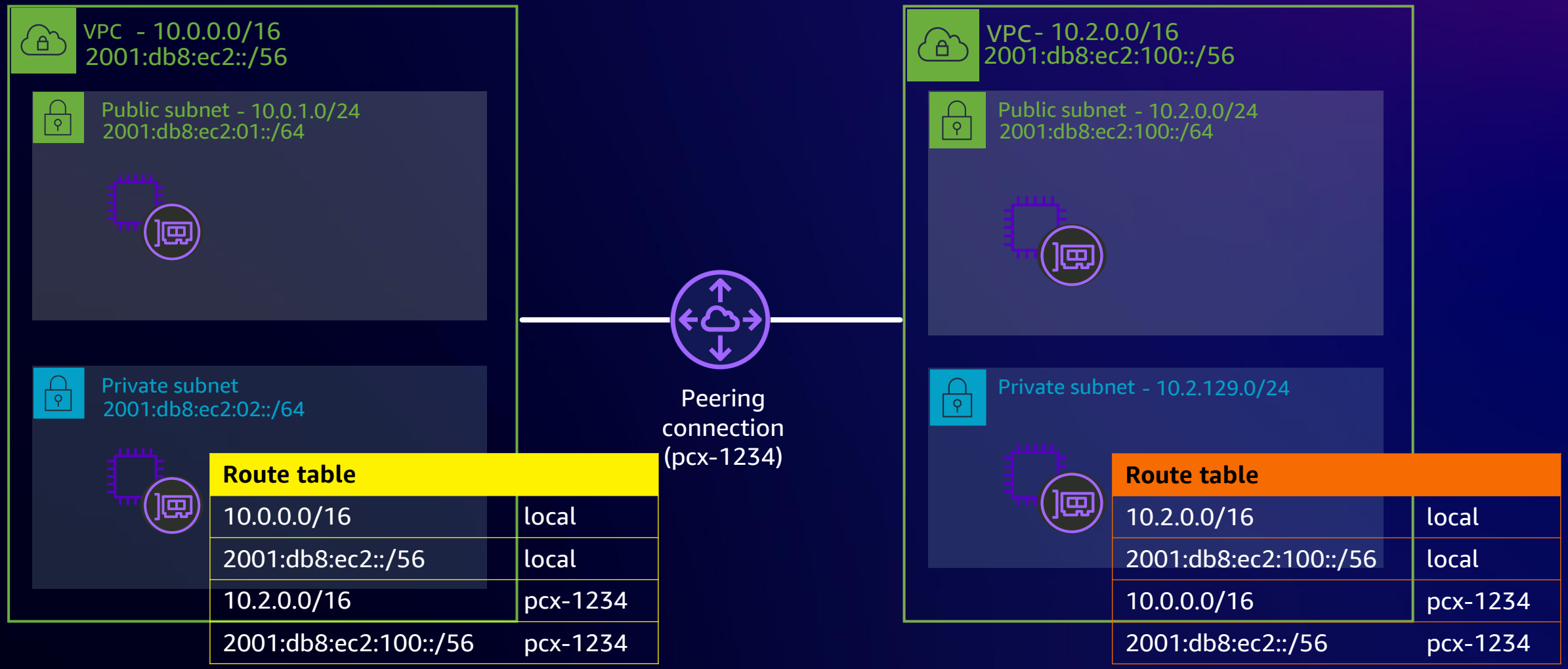
Expanding to multiple VPCs and Regions

Connect multiple VPCs: VPC peering

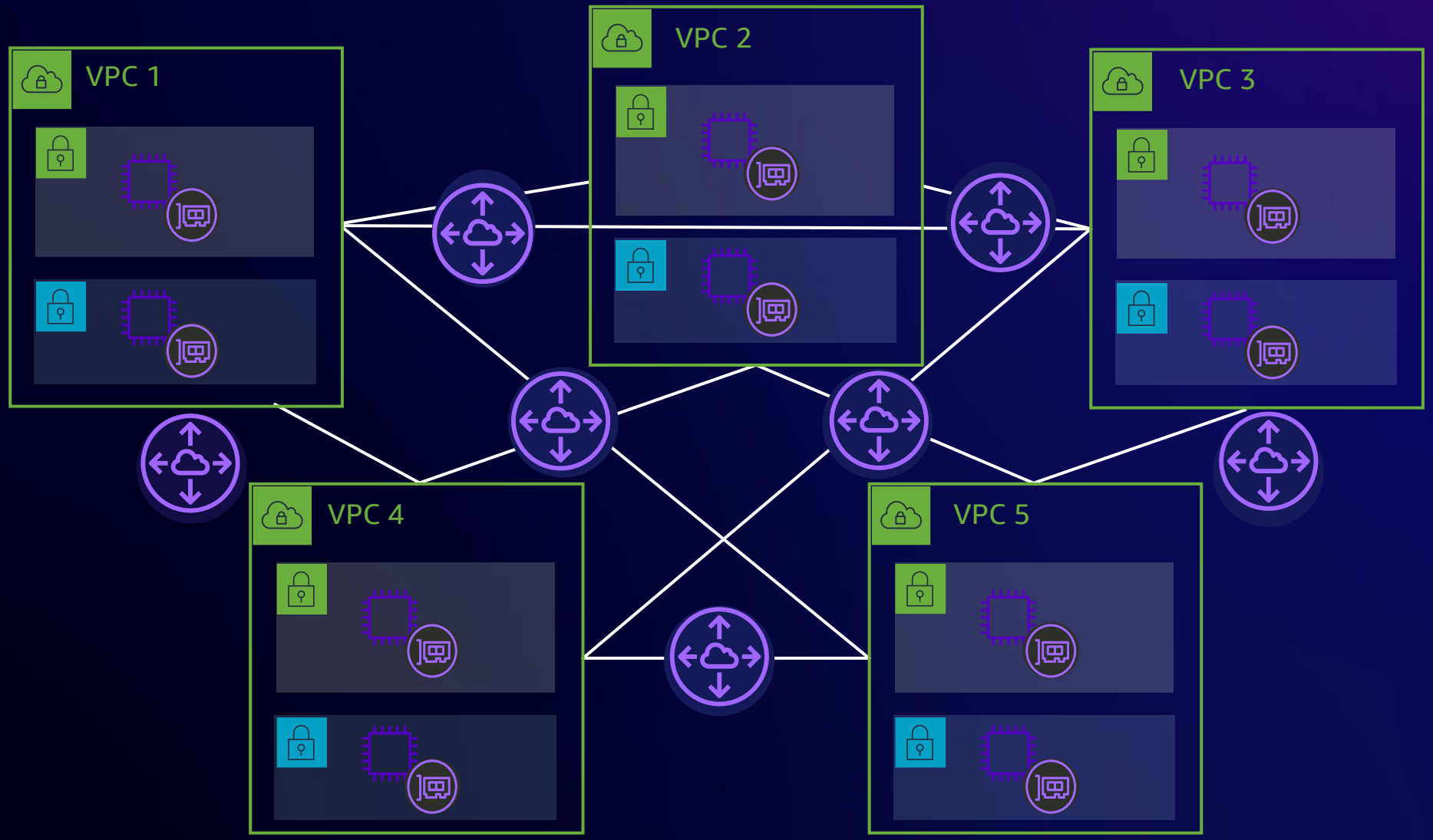
- Scalable and high available
- Supported between AWS accounts
- Supported across AWS Regions
- Bi-directional traffic
- Remote security groups can be referenced
- Routing policy with route tables
  - Not all subnets need to connect to each other
- No overlapping IP addresses
- No transitive routing



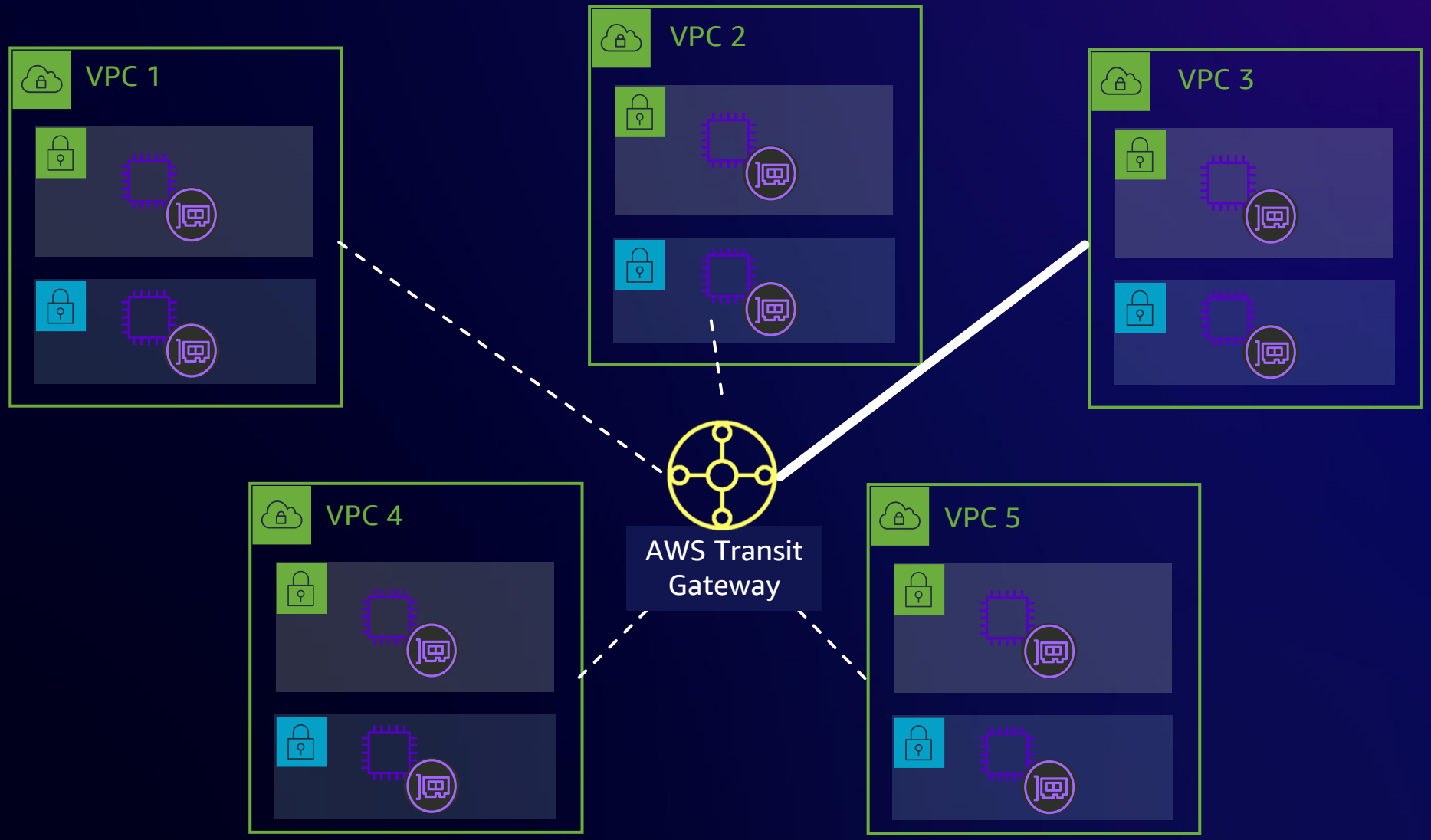
VPC peering



VPC peering

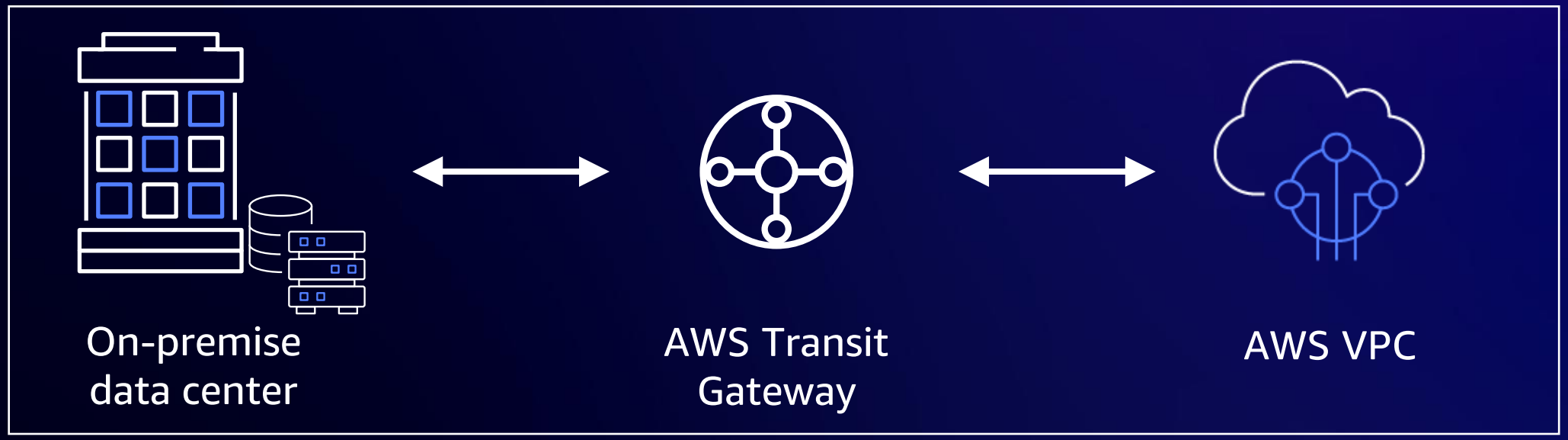


AWS Transit Gateway



AWS Transit Gateway

Easily connect Amazon VPCs, AWS accounts, and on-premises networks to a single gateway

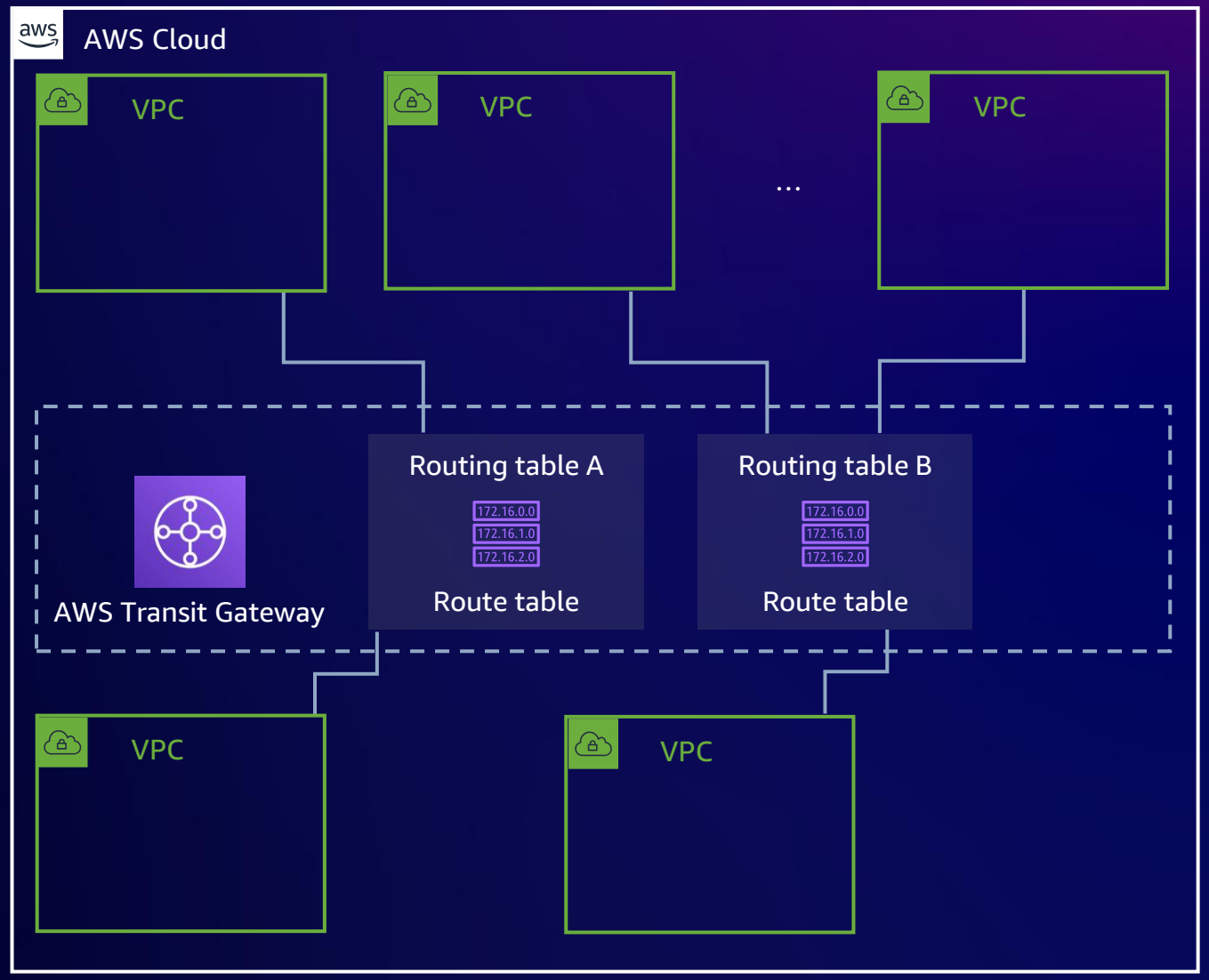


AWS Transit Gateway: Key features and benefits

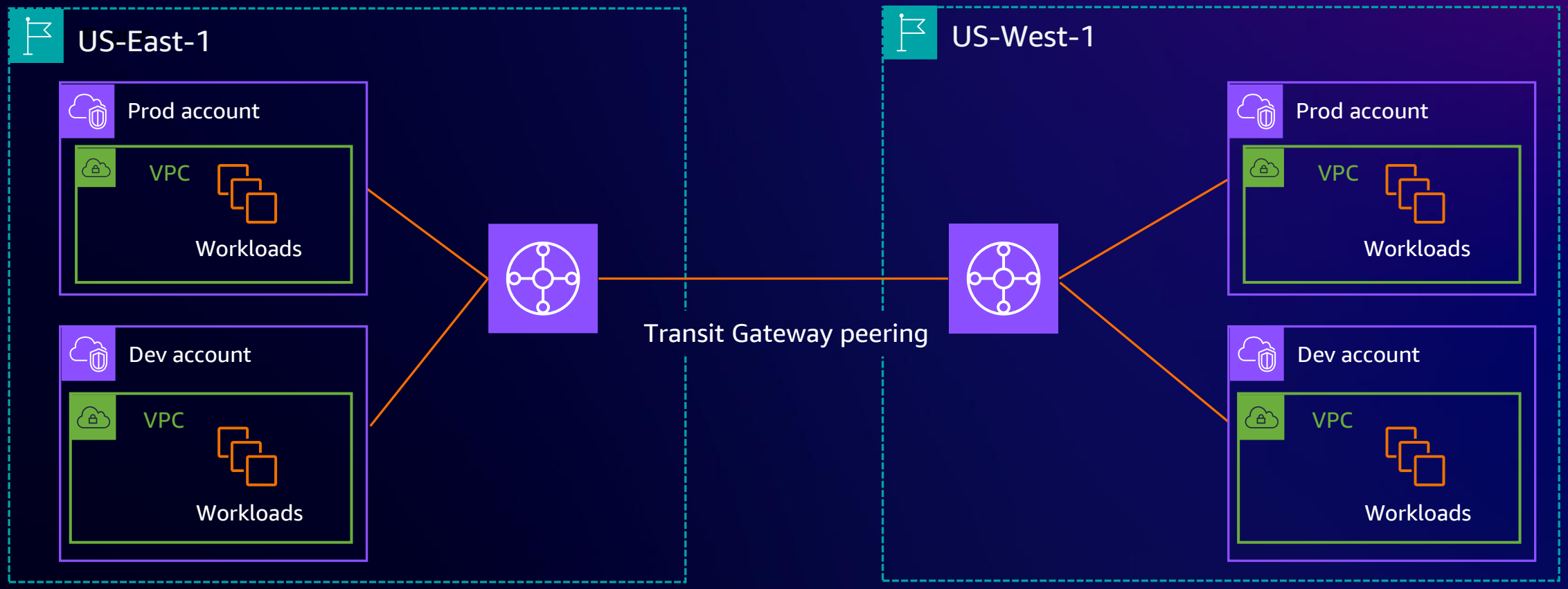
- Fully managed and highly available
- Scales to support thousands of VPCs across multiple accounts
- Centralized routing polices across VPCs and on-premises
- Peer Transit Gateway instances to provide inter-Region VPC connectivity
- Hybrid connectivity via Direct Connect, VPN, and SD-WAN
- Flexible segmentation and routing rules
- Route multicast traffic between VPCs in the same Region
- Simplified management and network visibility

Connect multiple VPCs: Transit Gateway

- Connect thousands of VPCs across accounts within a Region
- Connect your VPCs and on-premises through a single Transit Gateway instance
- Centralize VPN and AWS Direct Connect connections
- Control segmentation and data flow with route tables
- Hub and spoke design
- Up to 100 Gbps per attachment (burst)



Multi-VPC/multi-Region connectivity

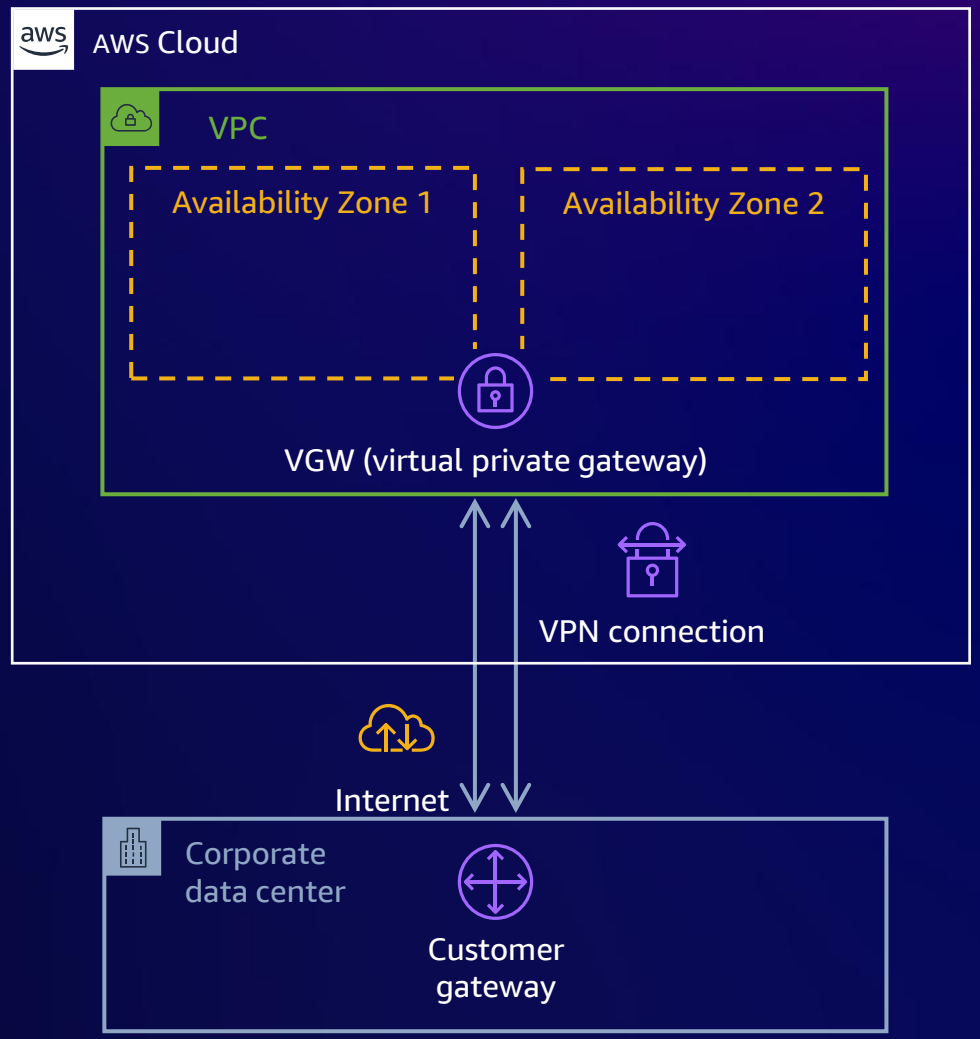


Transit Gateway inter-Region peering

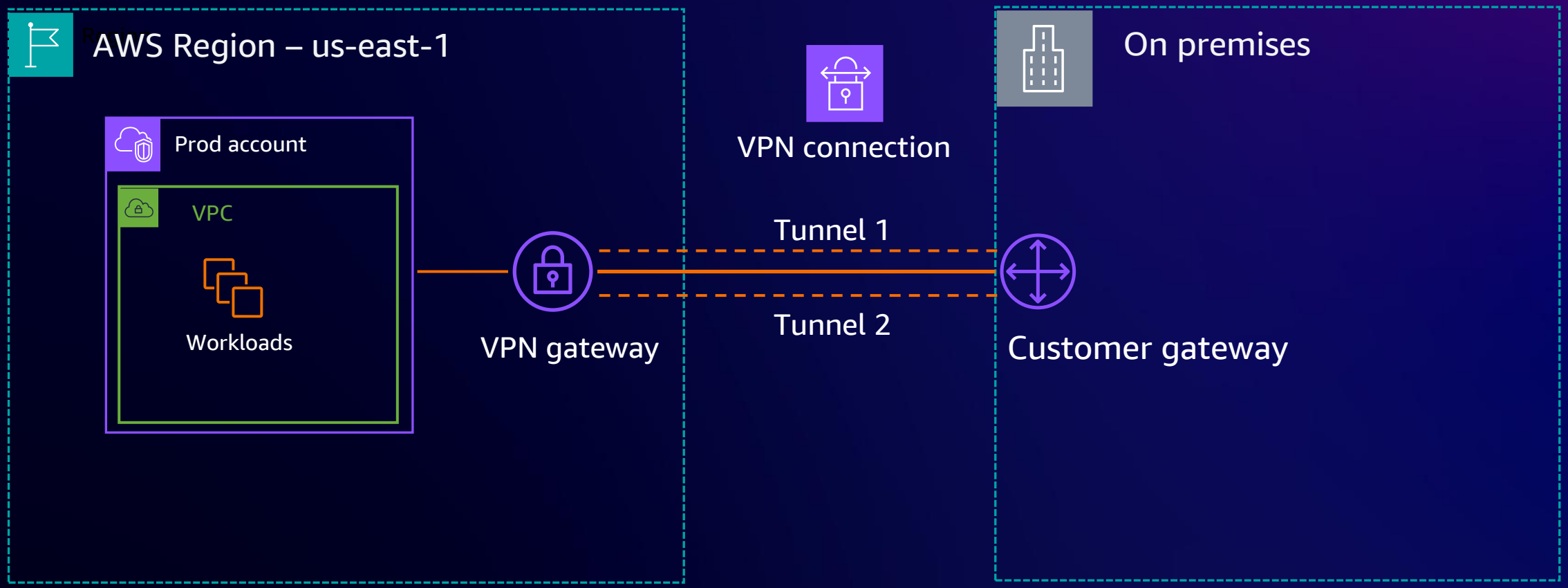
Hybrid connectivity

VPN to AWS: Virtual private gateway (VGW)

- 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

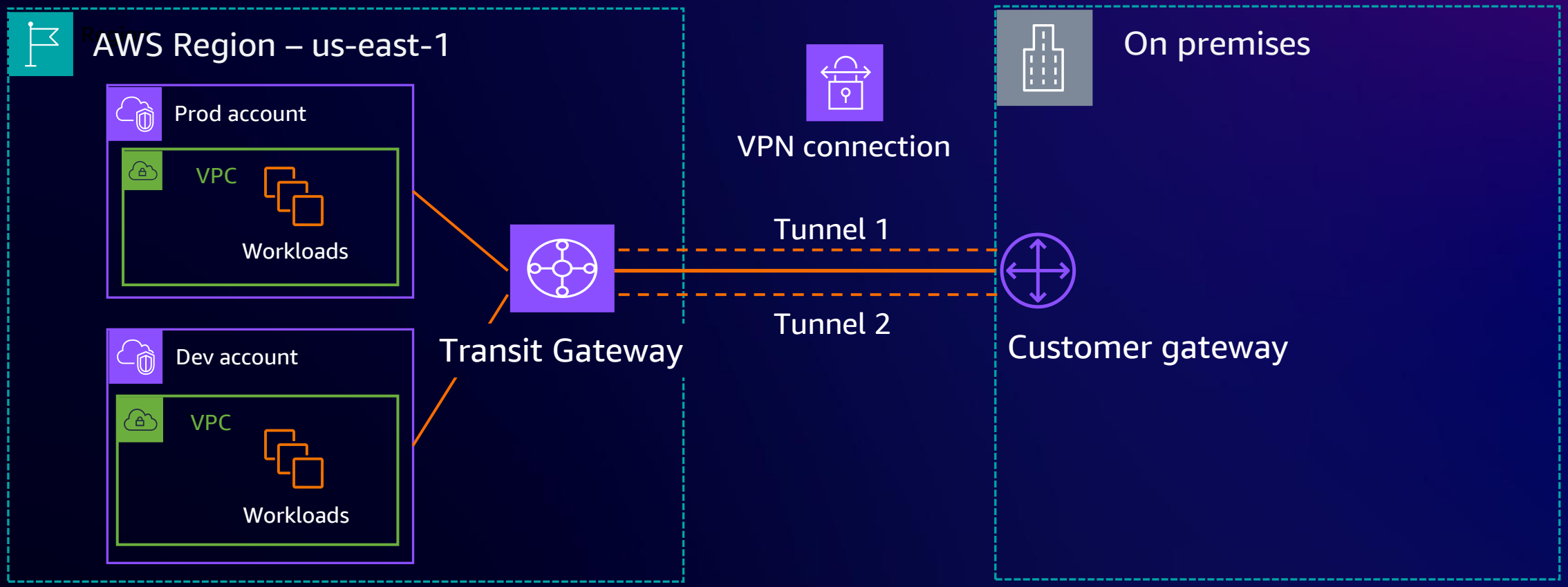


VPN



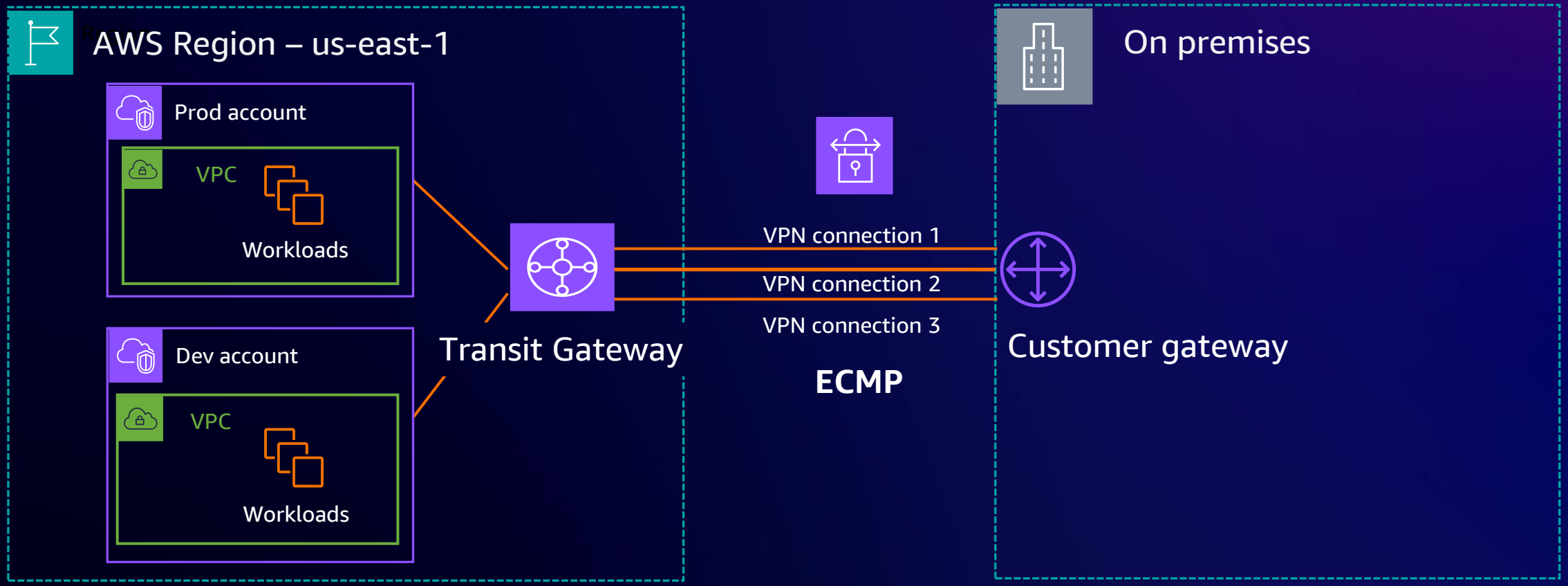
Virtual private gateway (VPN) connection

How to achieve multi-VPC, hybrid VPN connectivity

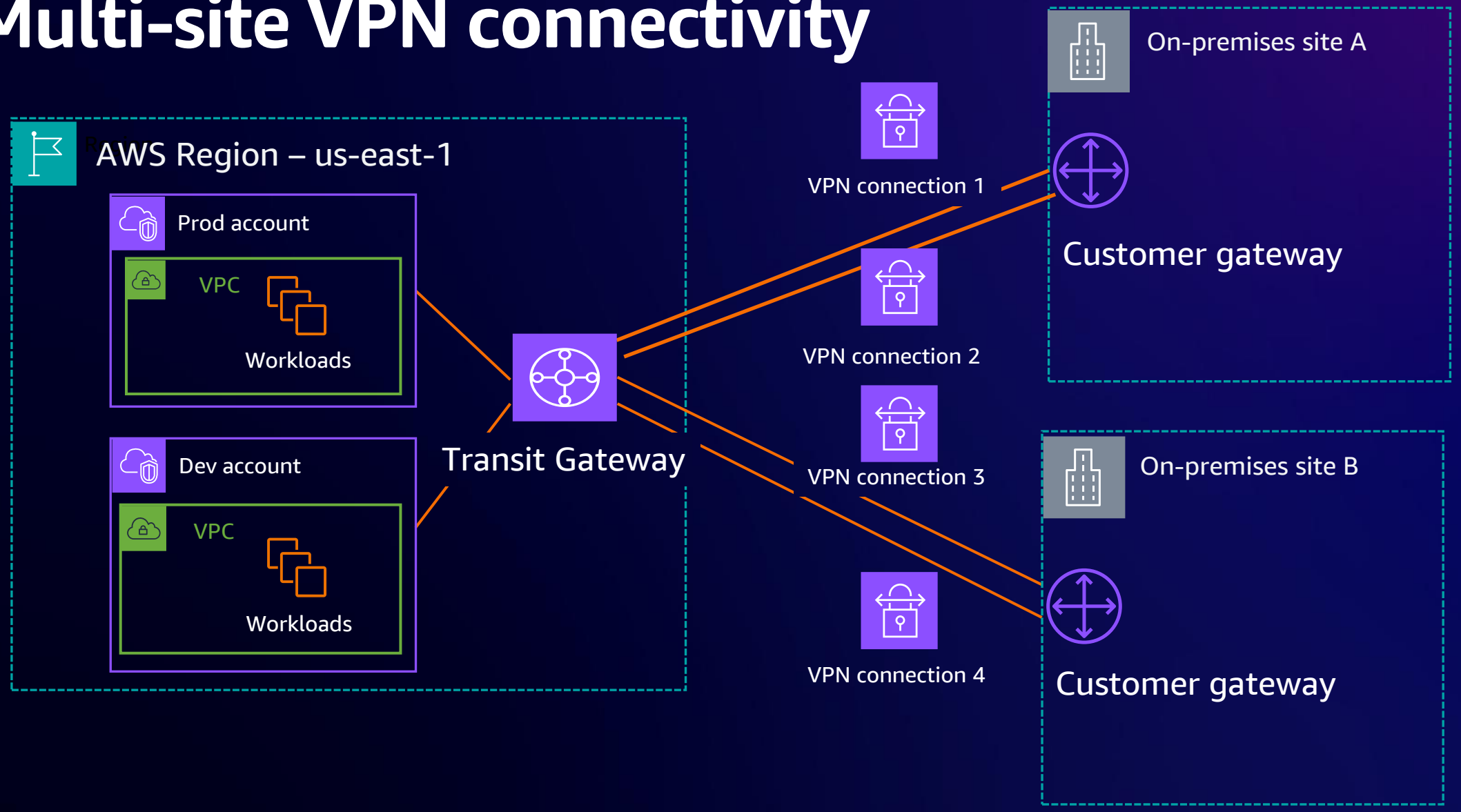


Virtual private gateway (VPN) connection

VPN throughput scalability

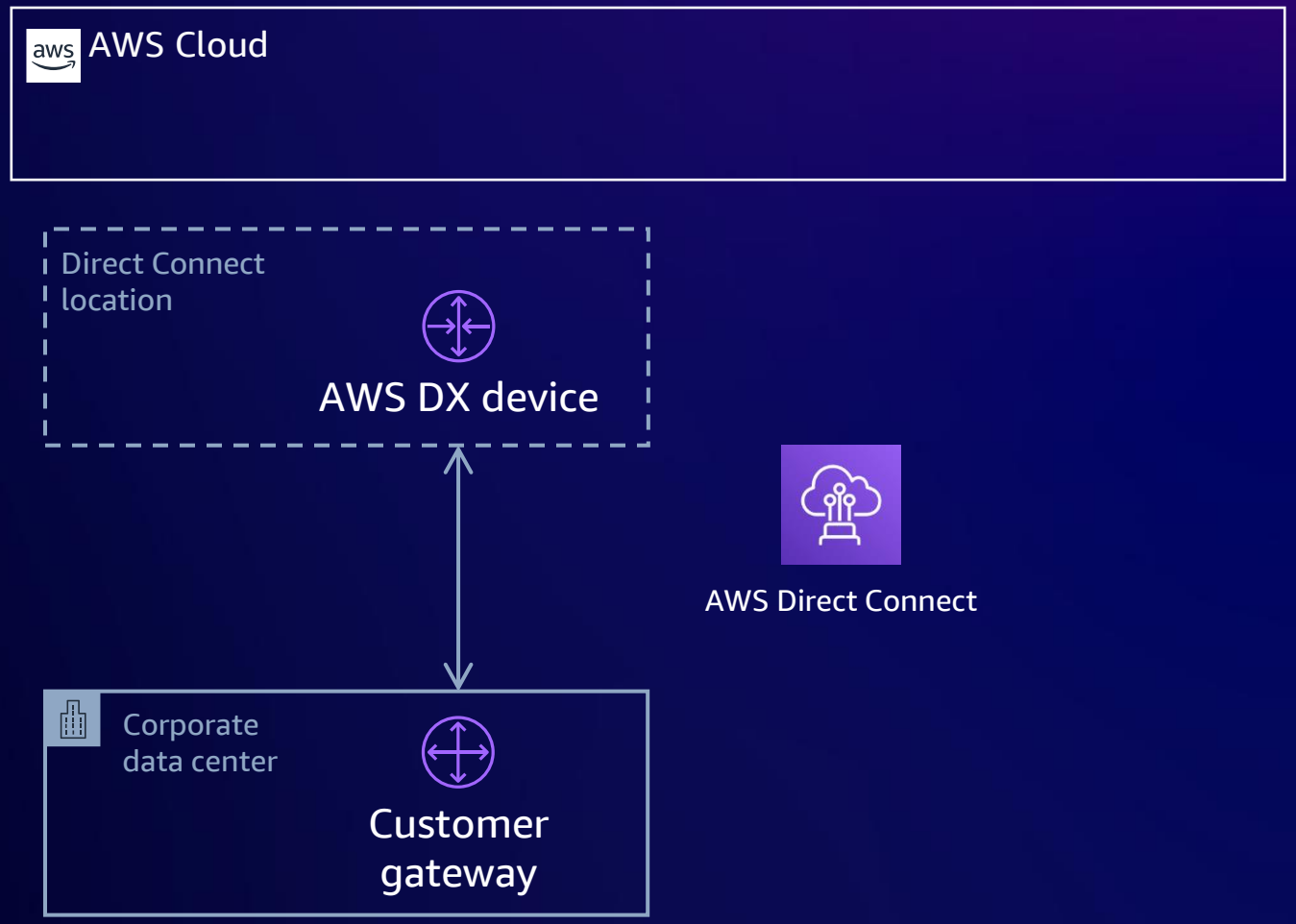


Multi-site VPN connectivity

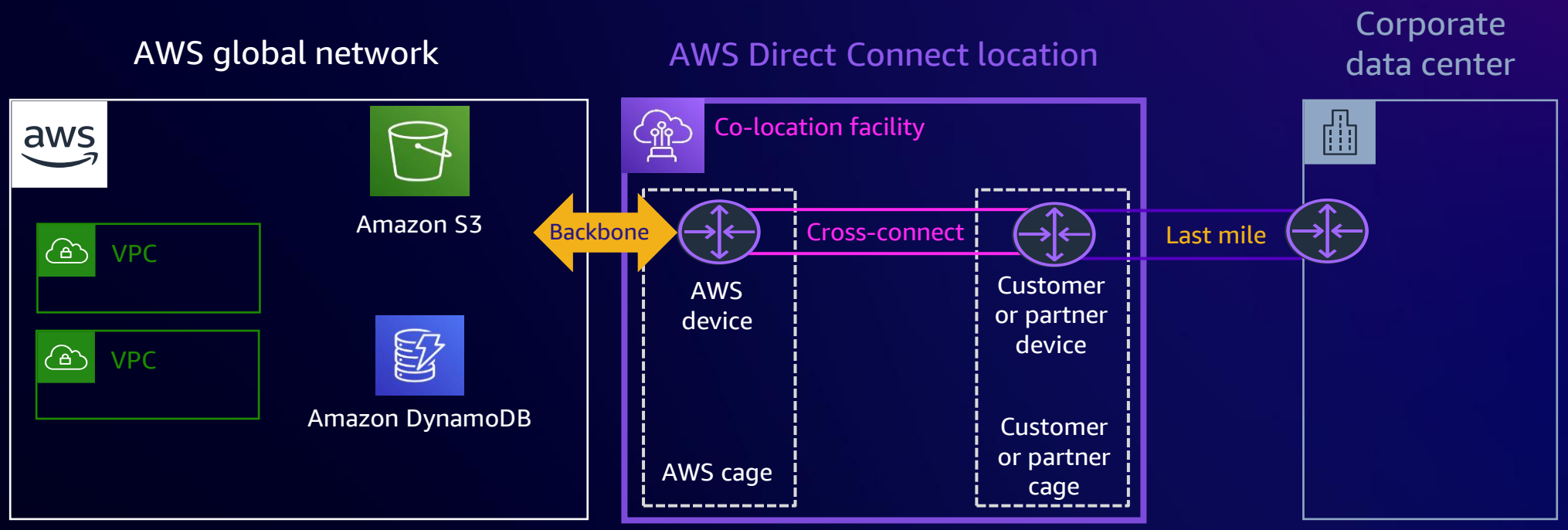


Dedicated link to AWS: AWS Direct Connect

- Dedicated network connection from your premises to AWS
- 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
- > 100 Direct Connection locations across the globe



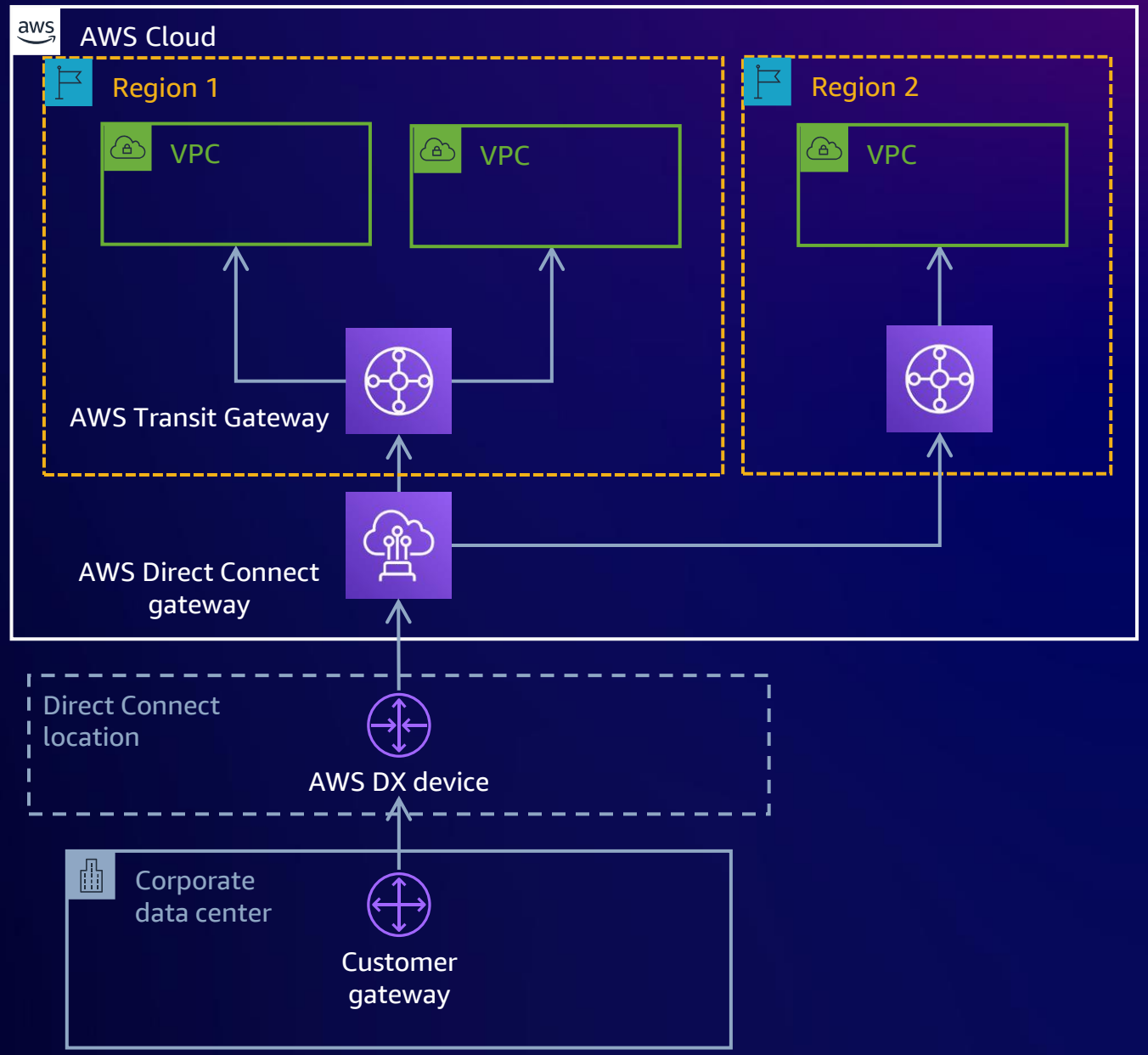
High throughput and consistent hybrid connectivity



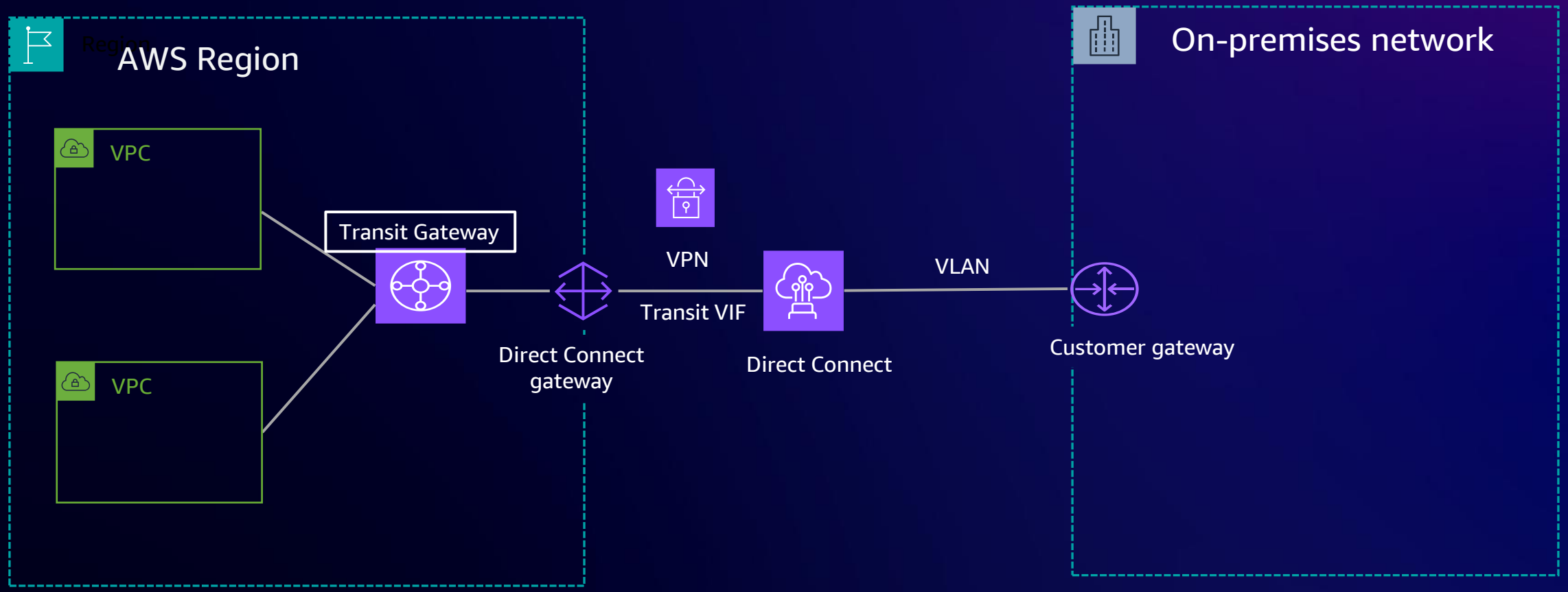
Direct Connect architecture

Connect at global scale: DX Gateway and 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

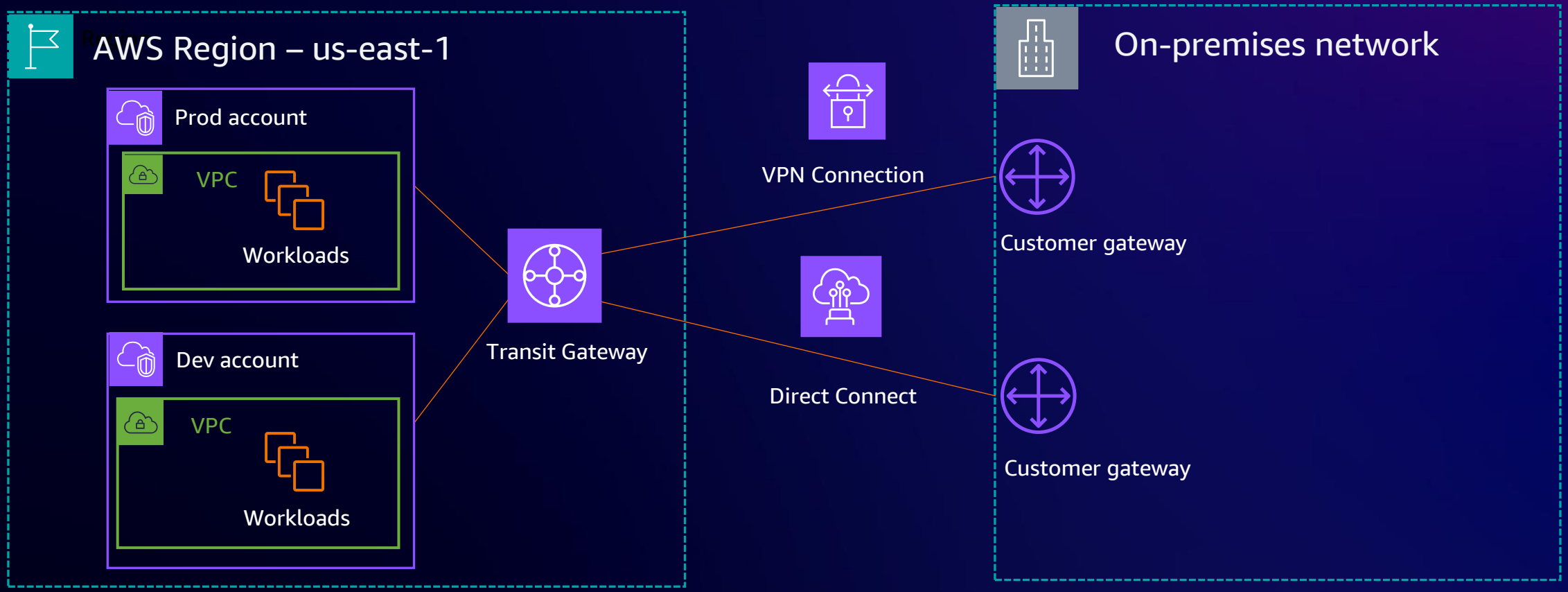


Securing traffic over direct connect



Private VPN over Direct Connect

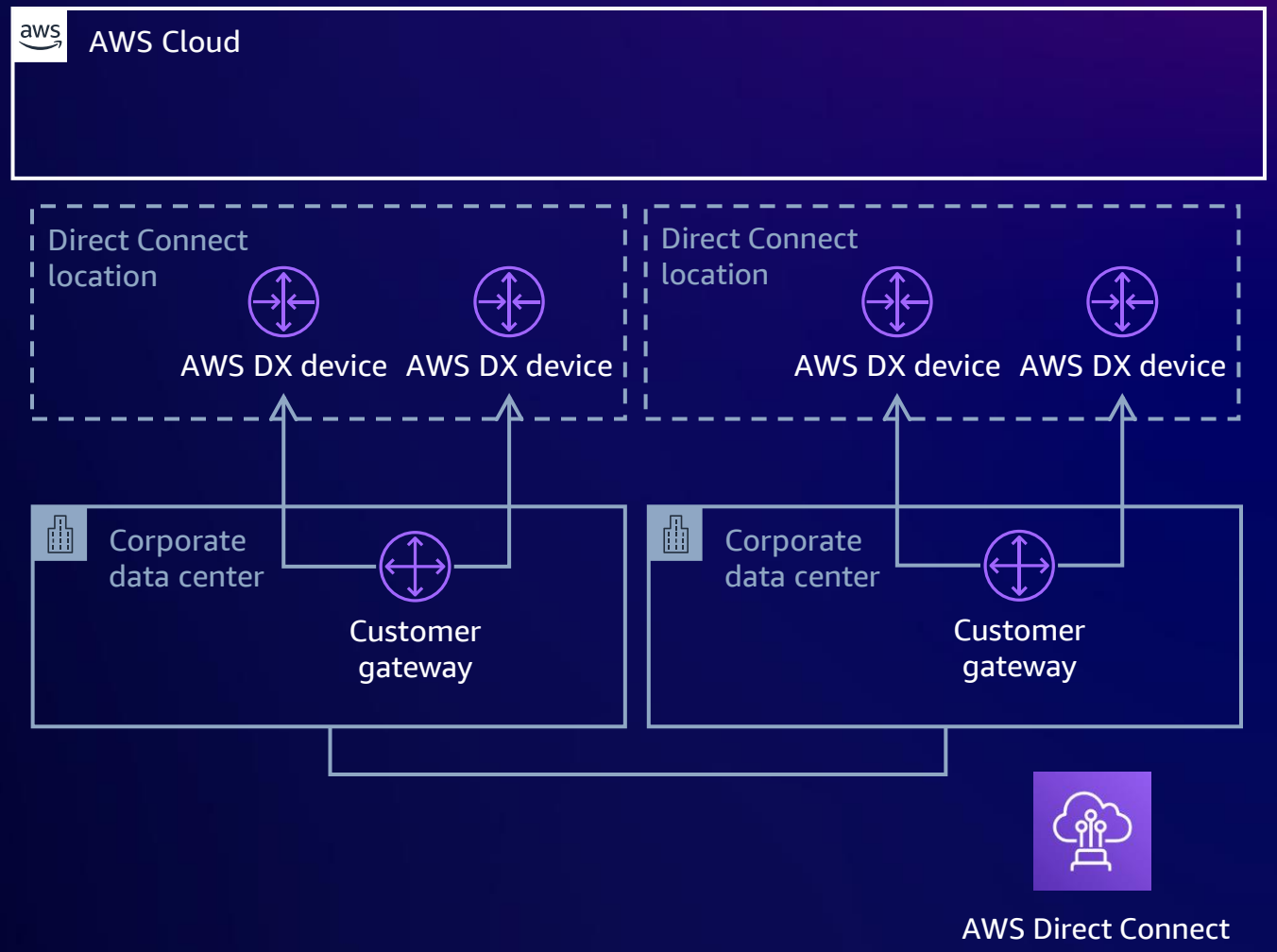
Direct Connect VPN backup



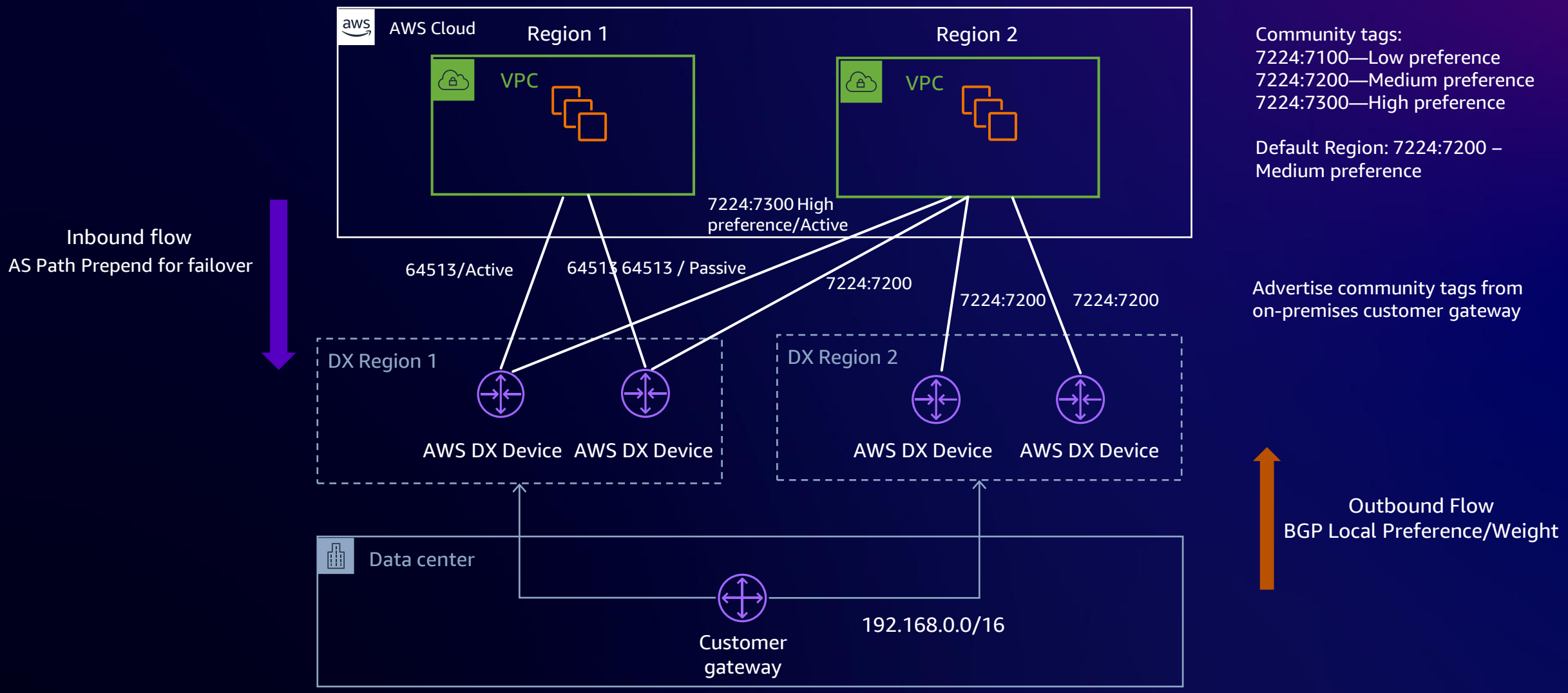
Direct Connect VPN Backup

Dedicated link to AWS: AWS Direct Connect

- For redundancy, DX can deployed with single or multiple:
  - Circuits
  - Providers
  - Customer gateways
  - Direct Connect locations
  - Customer data centers
- BGP routing for redundancy
  - AS_PATH prepend
  - Scope BGP communities
  - Local preference BGP communities



Routing failover and community tags

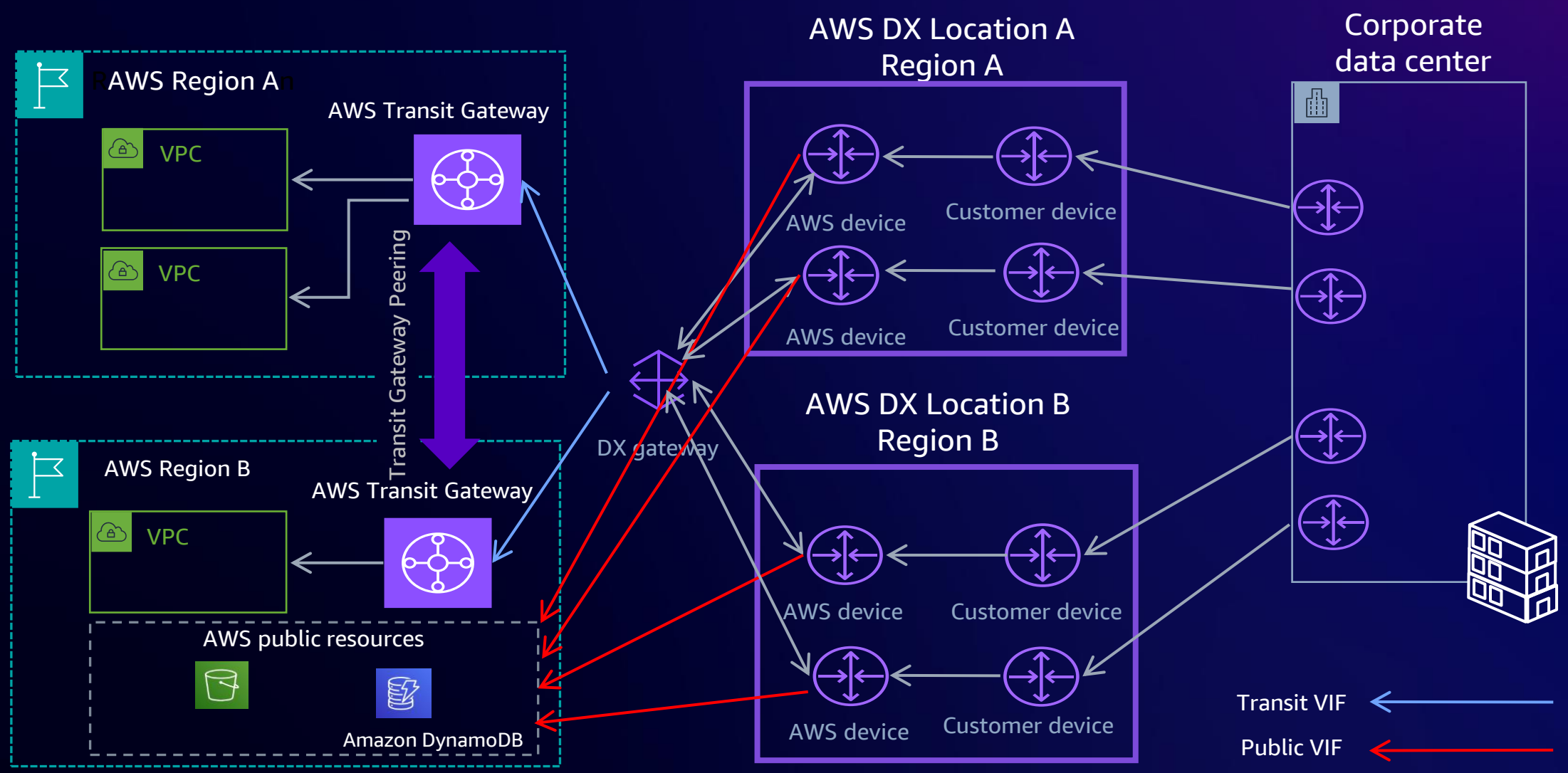


Community tags:
7224:7100—Low preference
7224:7200—Medium preference
7224:7300—High preference

Default Region: 7224:7200 – Medium preference

Advertise community tags from on-premises customer gateway

Direct Connect highly available multi-Region connectivity



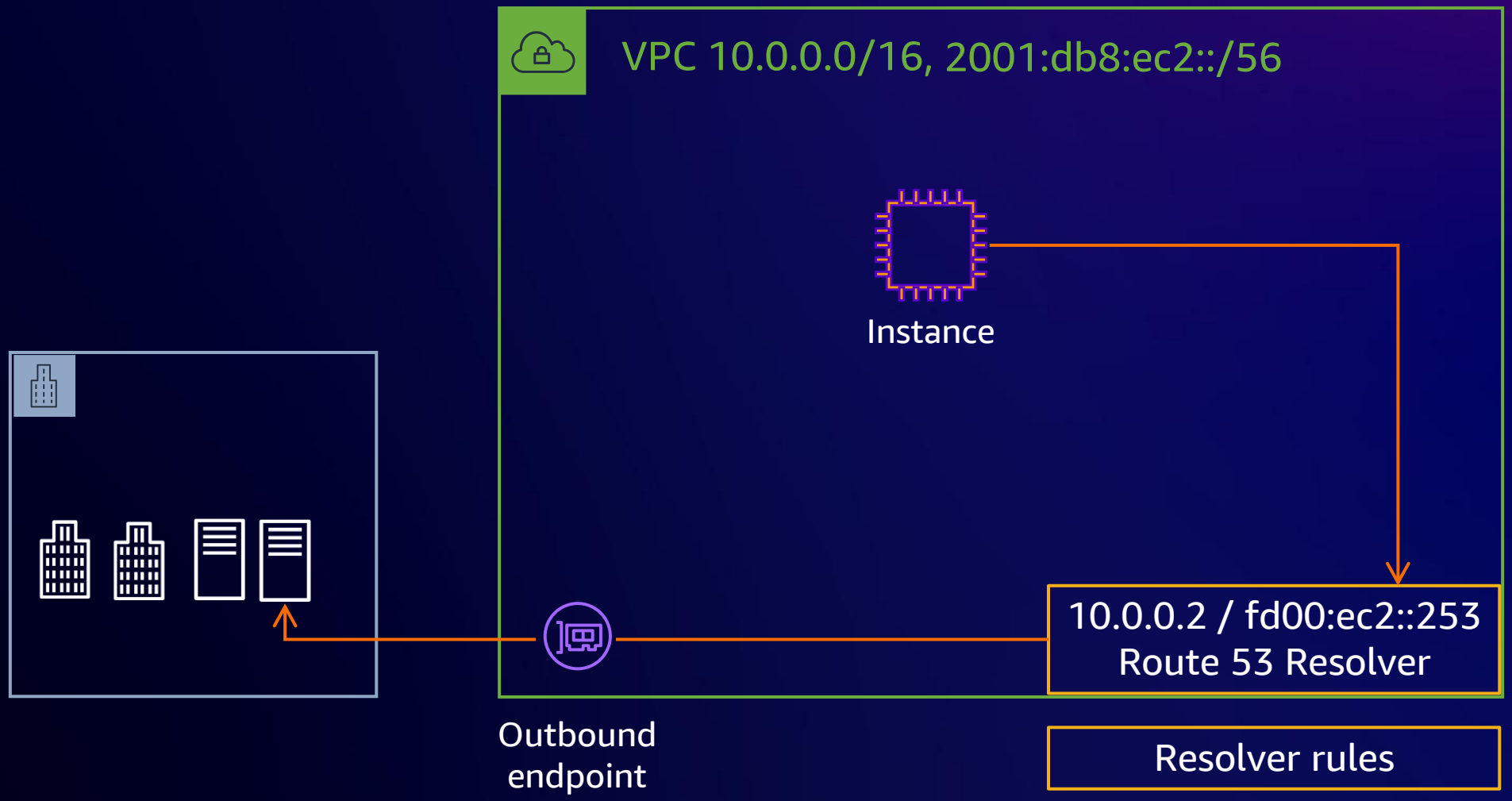
Route 53 Resolver

Managed DNS resolver service from Route 53

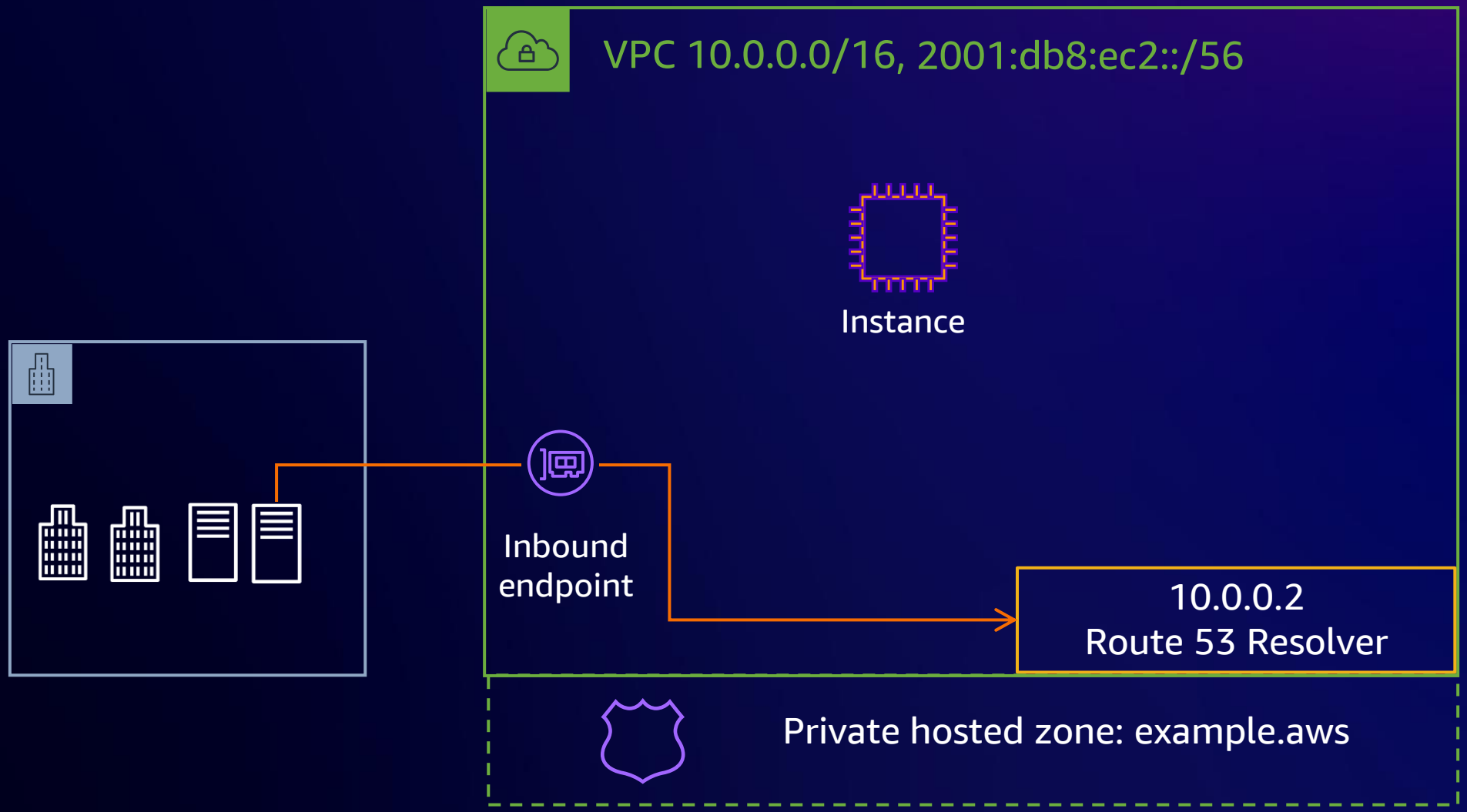
Create conditional forwarding rules to re-direct query traffic

Enables hybrid connectivity over AWS Direct Connect and managed VPN

Route 53 Resolver endpoints

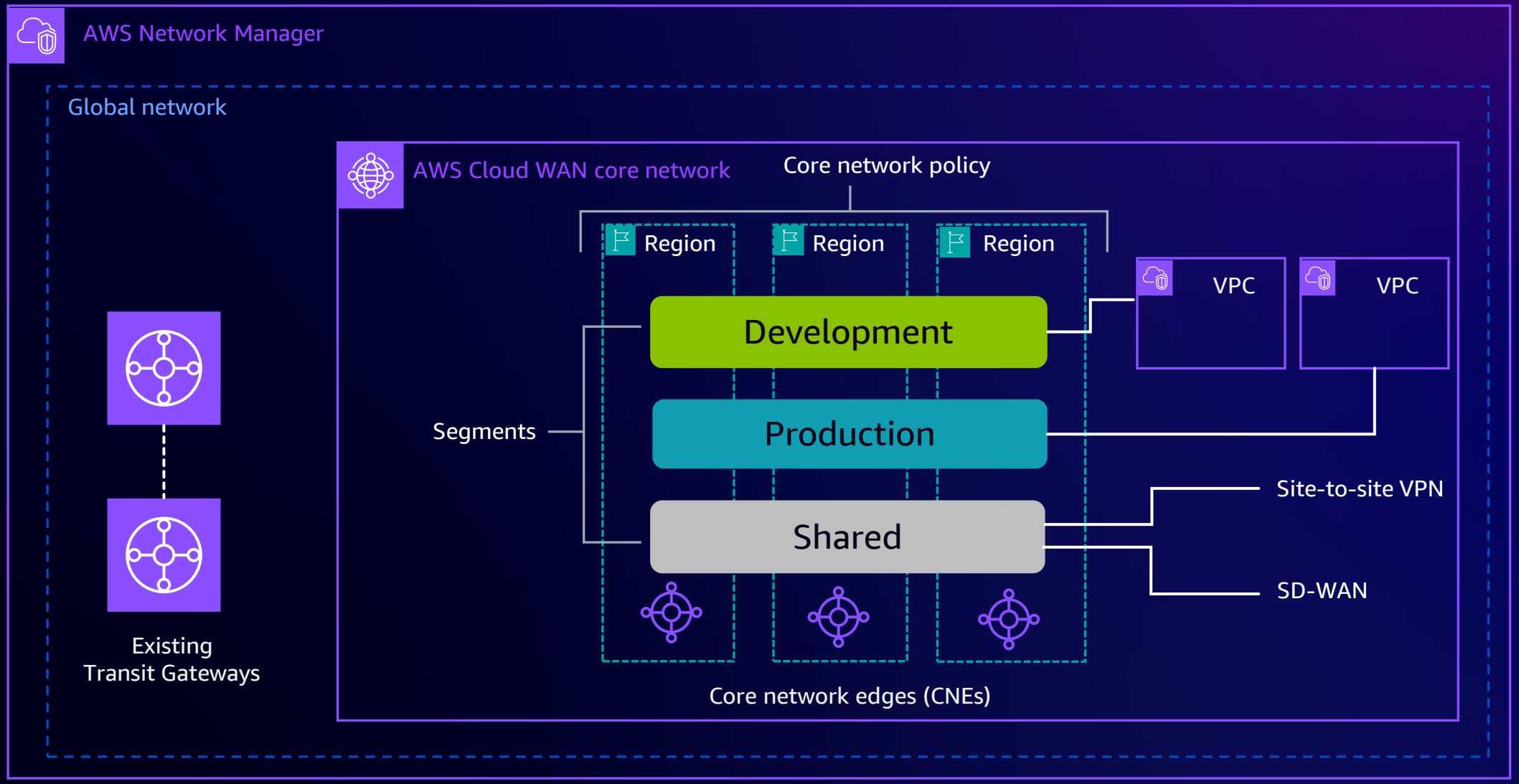


Route 53 Resolver endpoints



WAN

Integrate WAN and Simplify Interconnectivity



CloudWAN

AWS Networking Competency Partners

AWS Networking Competency Partners

AWS Direct Connect (DX) Integrated Partners

Provide Direct Connect connectivity to customers, including hosted connections, port-based connectivity, and software-defined networking functions

AWS Direct Connect (DX) Infrastructure Partners

Provide Direct Connect connectivity to customers, including network connectivity and infrastructure, such as fiber interconnections

Engage with AWS Partners

partners.amazonaws.com

Drive innovation and unlock greater business value with AWS Specialization Partners that have deep technical knowledge and proven customer success

SMB re:Invent Mobile Treasure Hunt

Join in the fun and prizes!

Play our SMB re:Invent Mobile Treasure Hunt

Earn gems as you explore and learn at re:Invent! Take in a session, stop by our kiosk, attend our gala party . . . you can collect gems at a variety of SMB activities!

At the end of re:Invent is a random drawing for fun prizes! The more gems you earn, the more chances you have to win!

Start earning gems today!

Thank you!

Please complete the session survey in the mobile app

Mike Cornstubble
mcornstu@amazon.com

Anoop Talluri
talanoop@amazon.com

Nayan Karumuri
nayanpk@amazon.com