AWS re:Invent

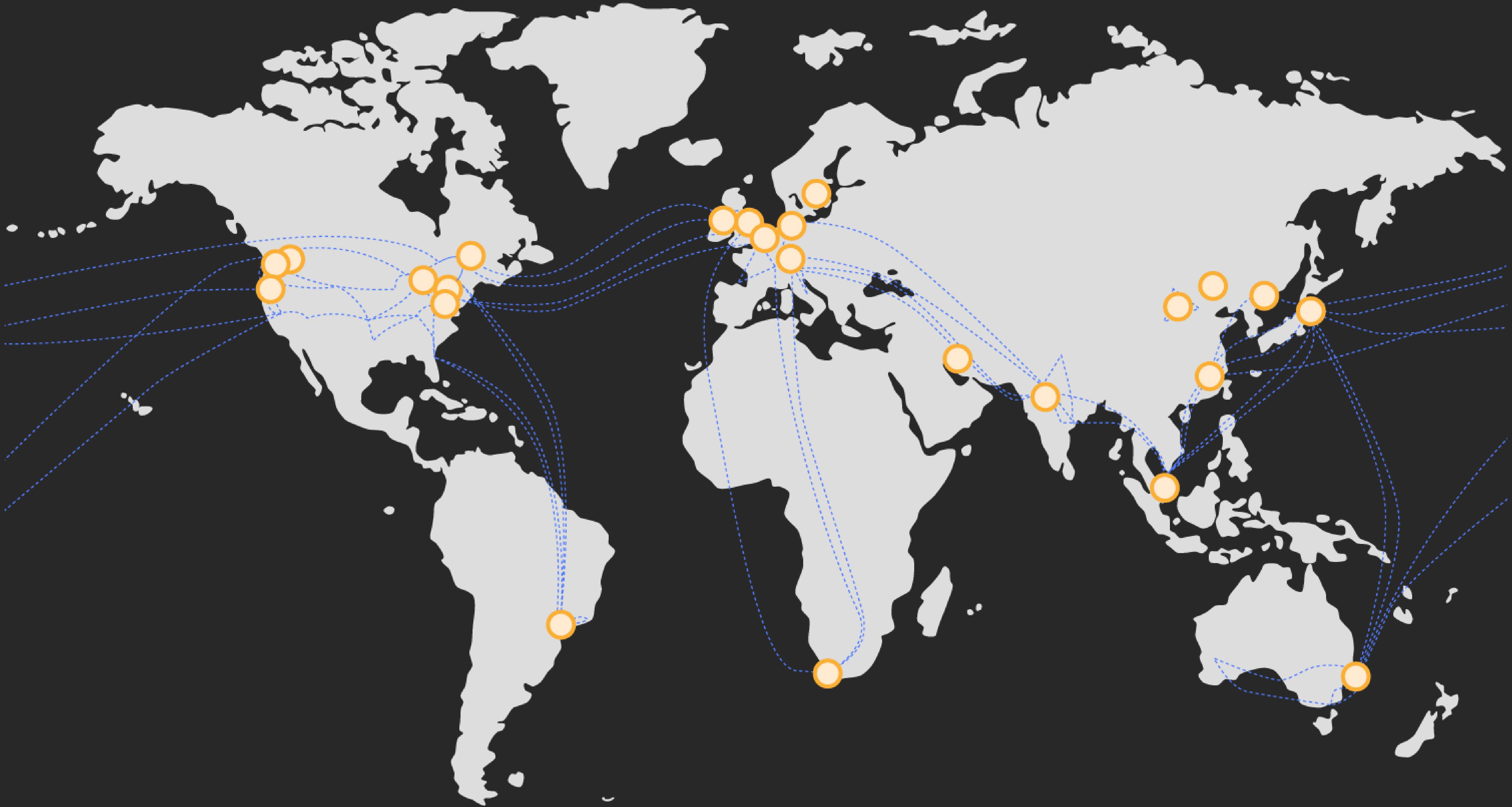
NET201-R

AWS networking fundamentals

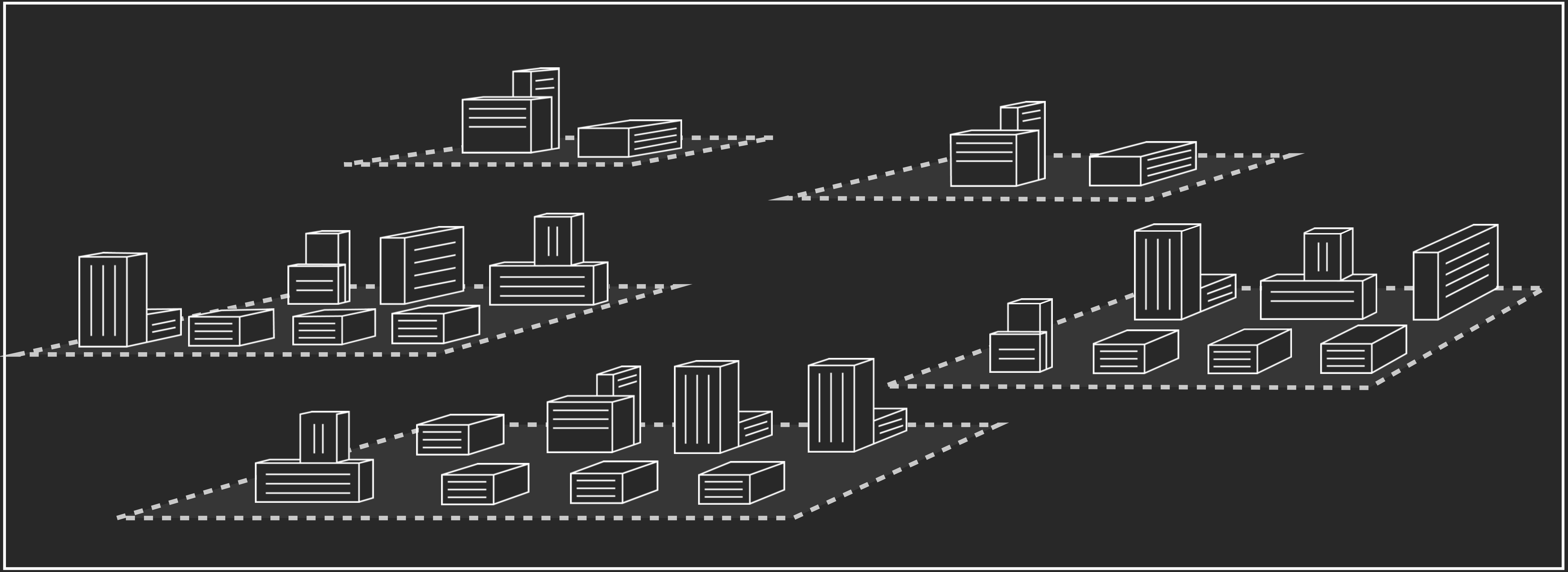
Alan Halachmi
Director, Public Sector
AWS Solutions Architecture
Amazon Web Services

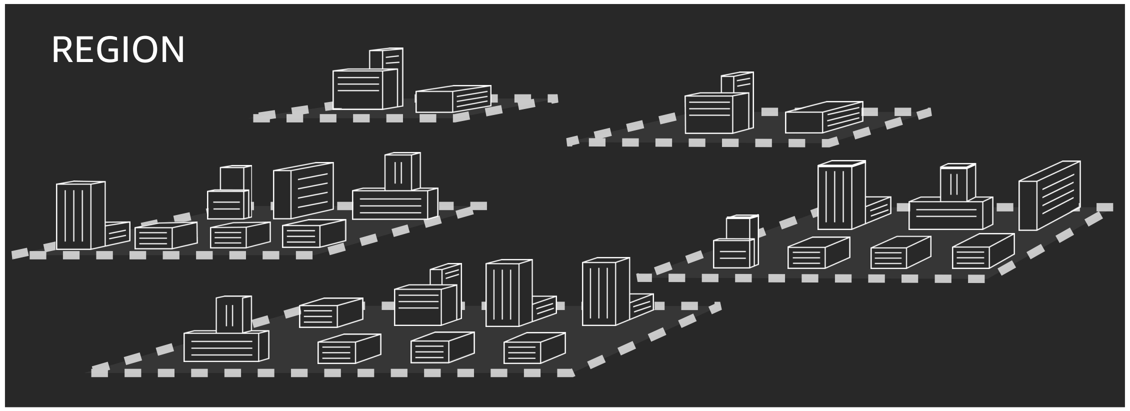
Steve Seymour
WW Tech Leader, Networking
AWS Solutions Architecture
Amazon Web Services

AWS global infrastructure



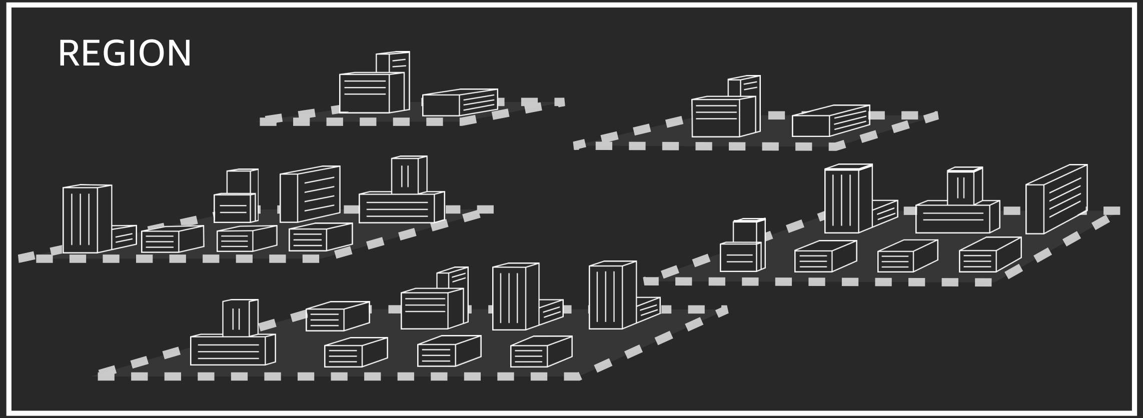
AWS Region



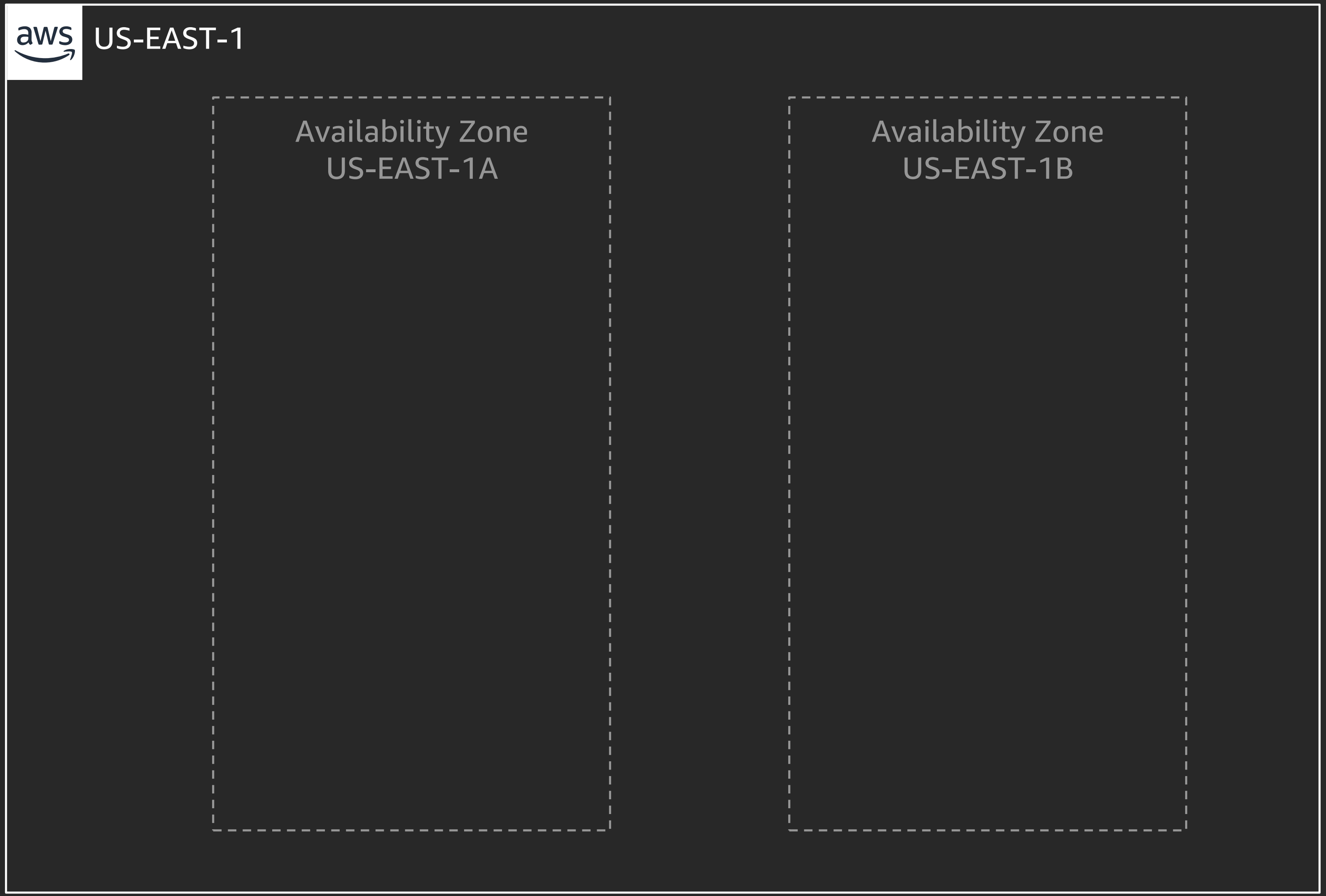


US-EAST-1

Availability Zone (AZ)



AVAILABILITY ZONE

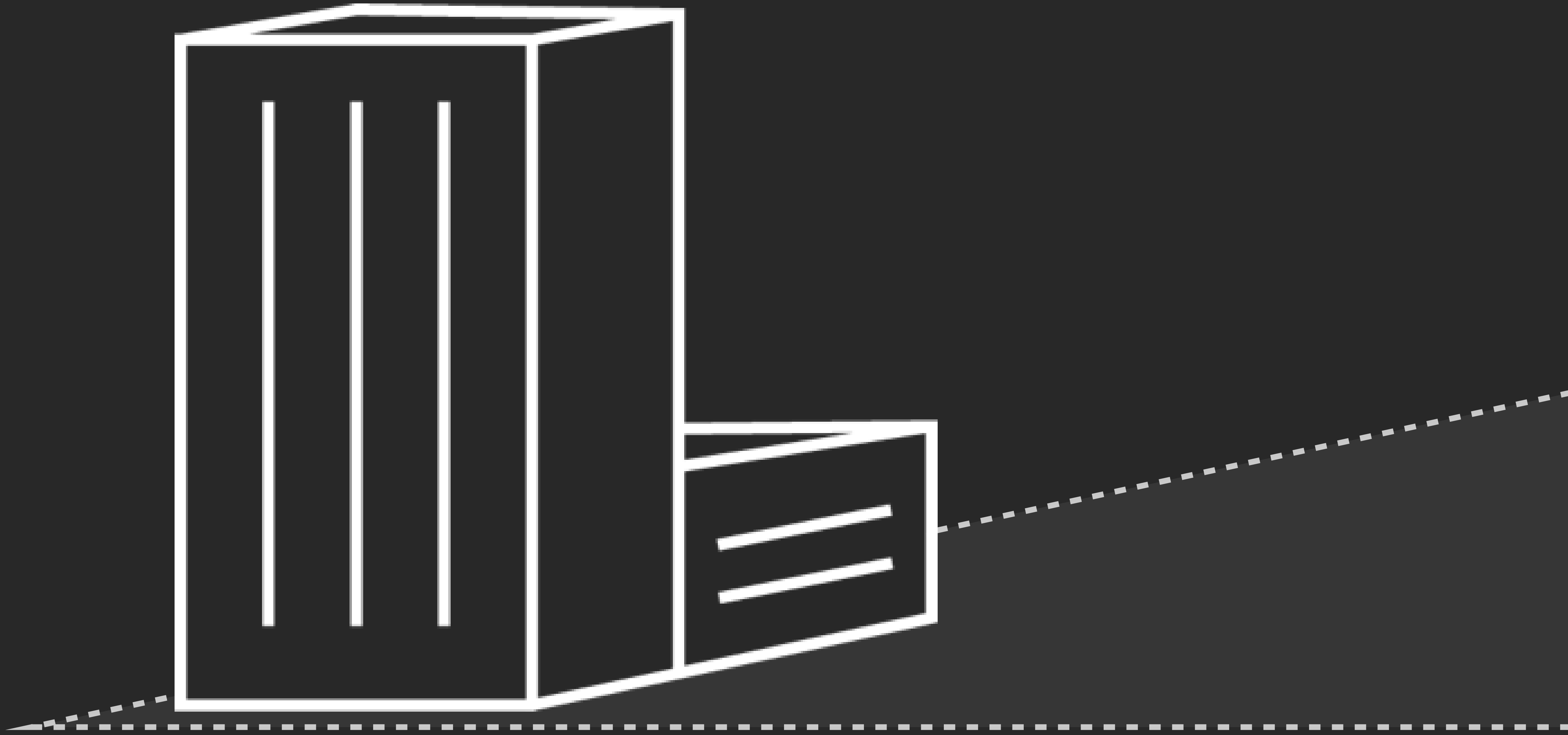


US-EAST-1

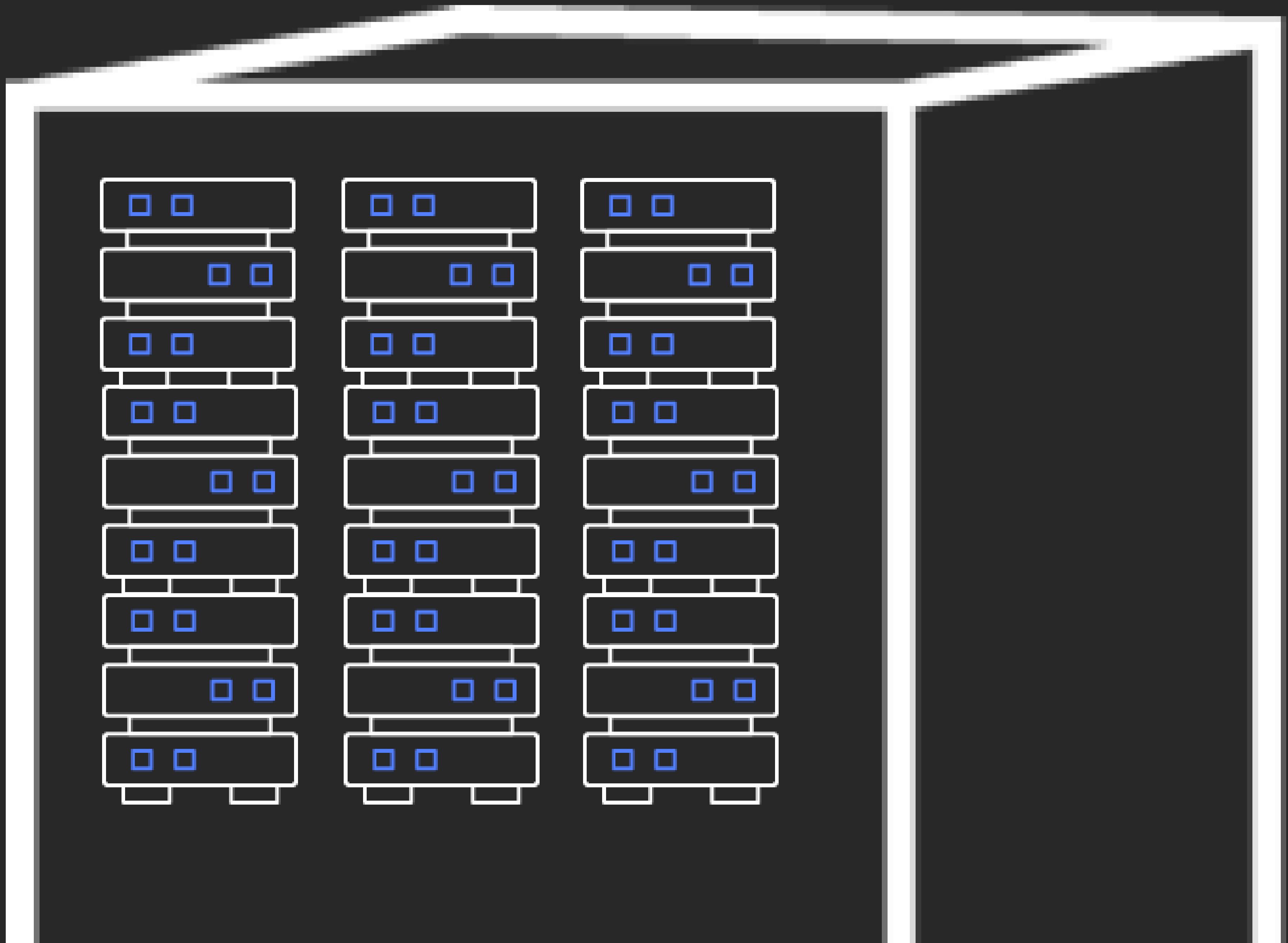
Availability Zone
US-EAST-1A

Availability Zone
US-EAST-1B

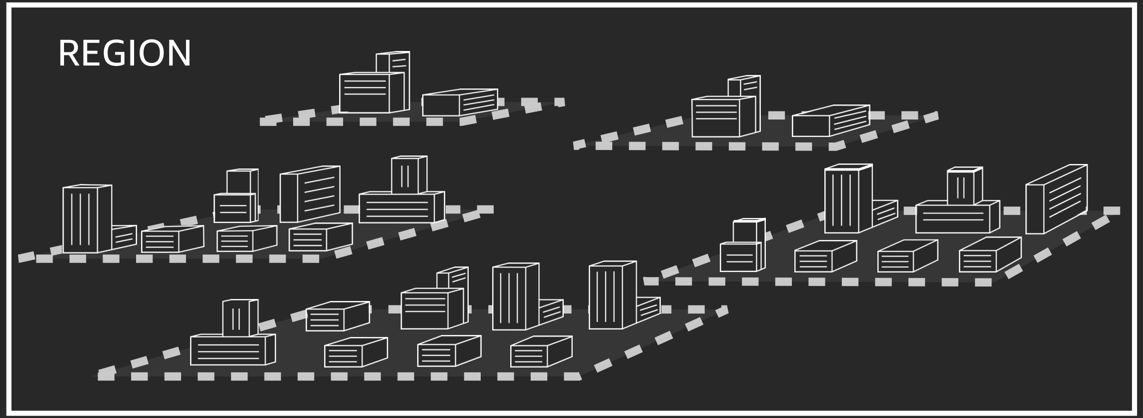
Data center



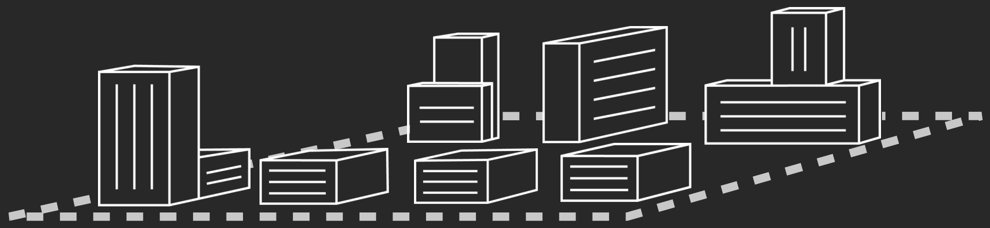
Rack, host, EC2 instance



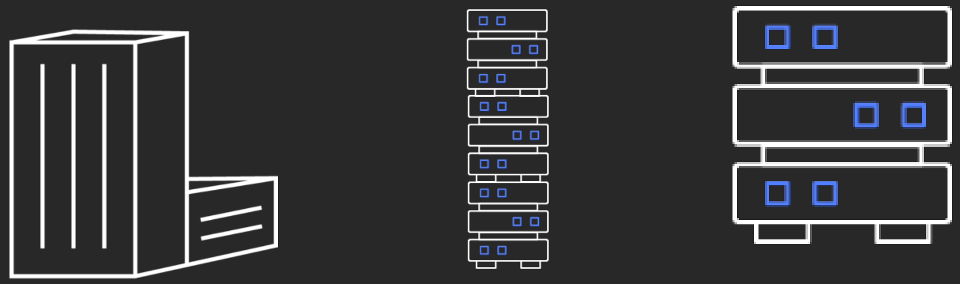
REGION

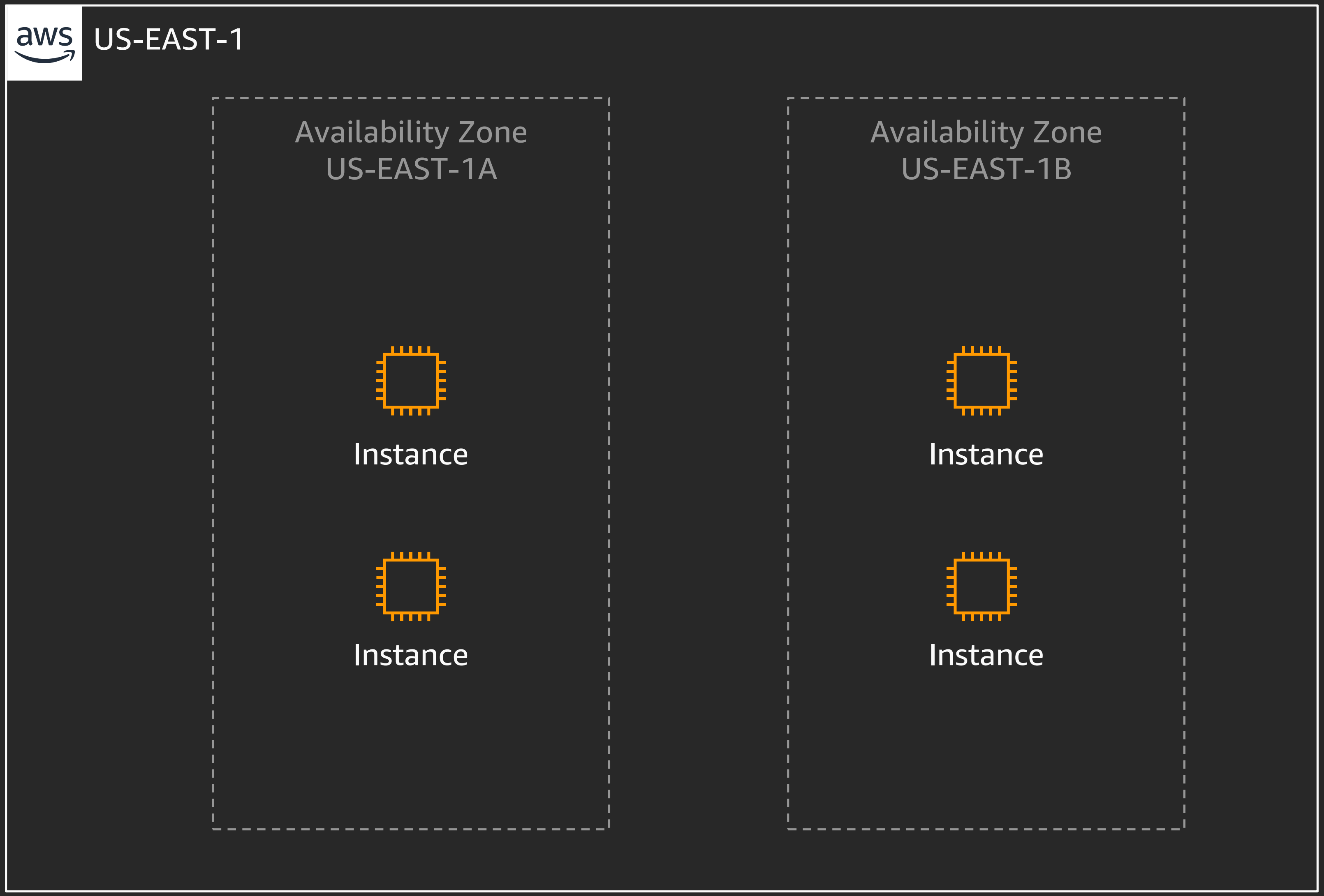


AVAILABILITY ZONE

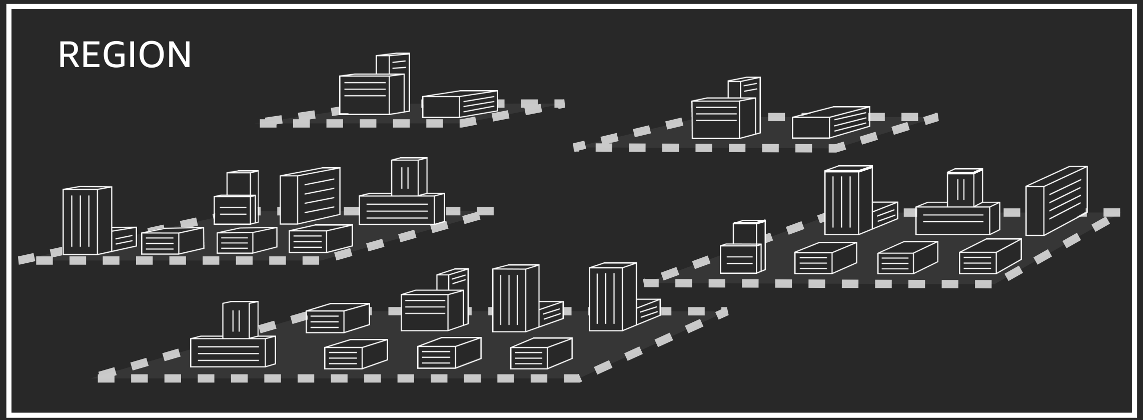


DATA CENTER, RACK, HOST

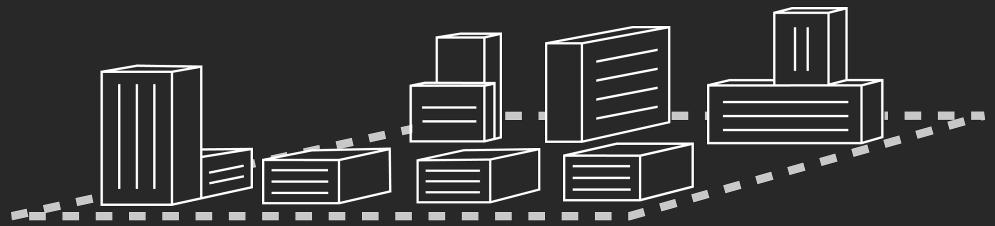




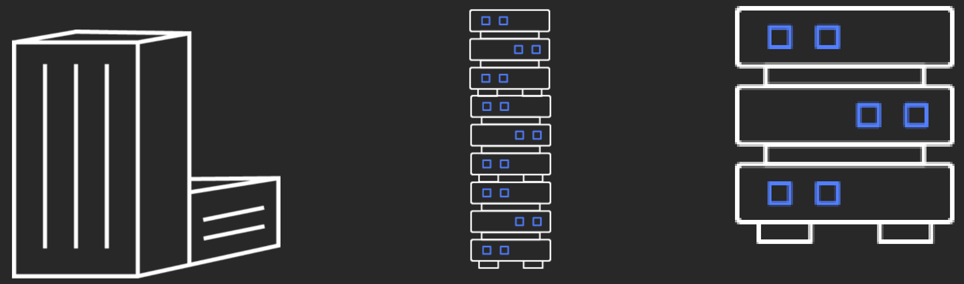
REGION

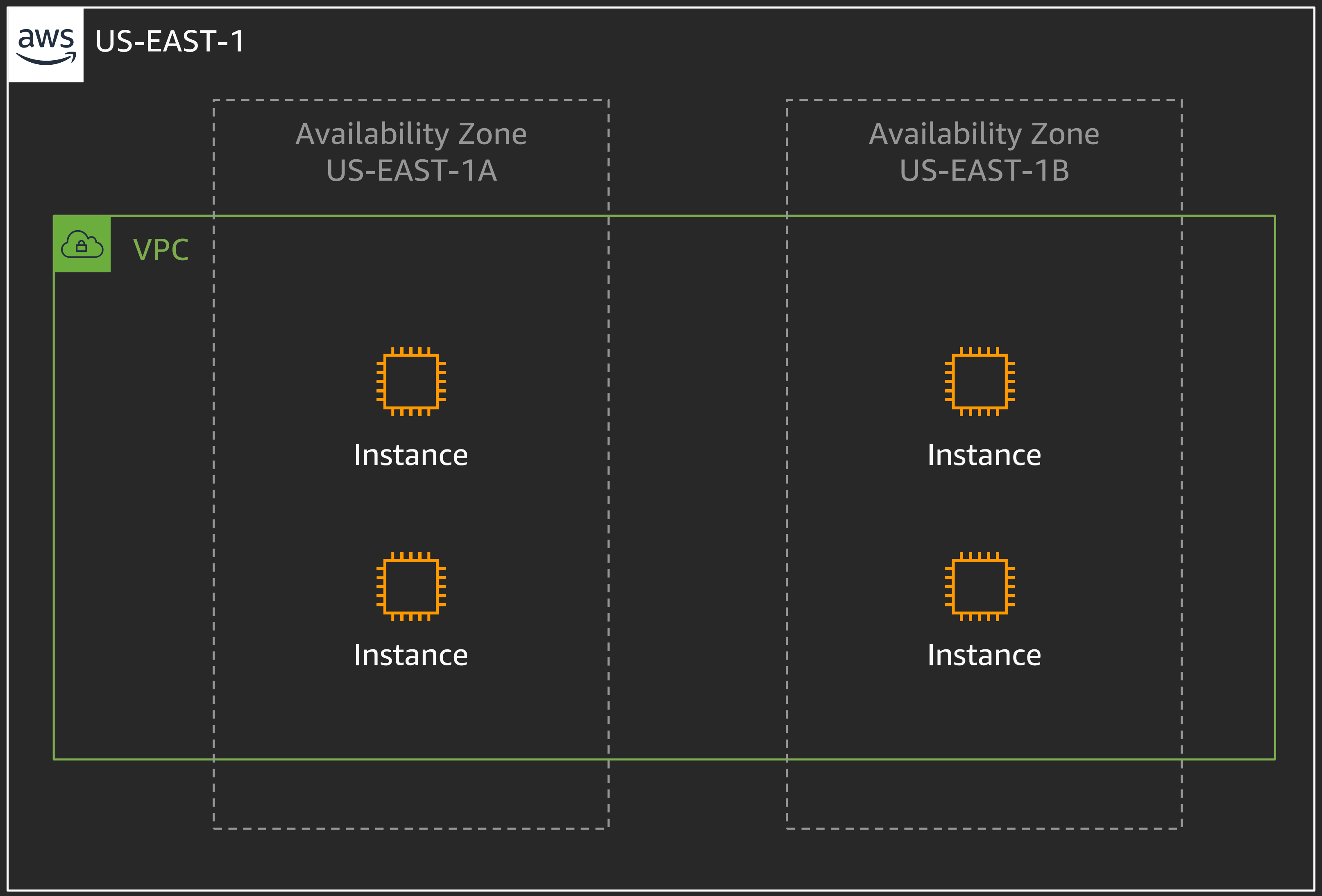


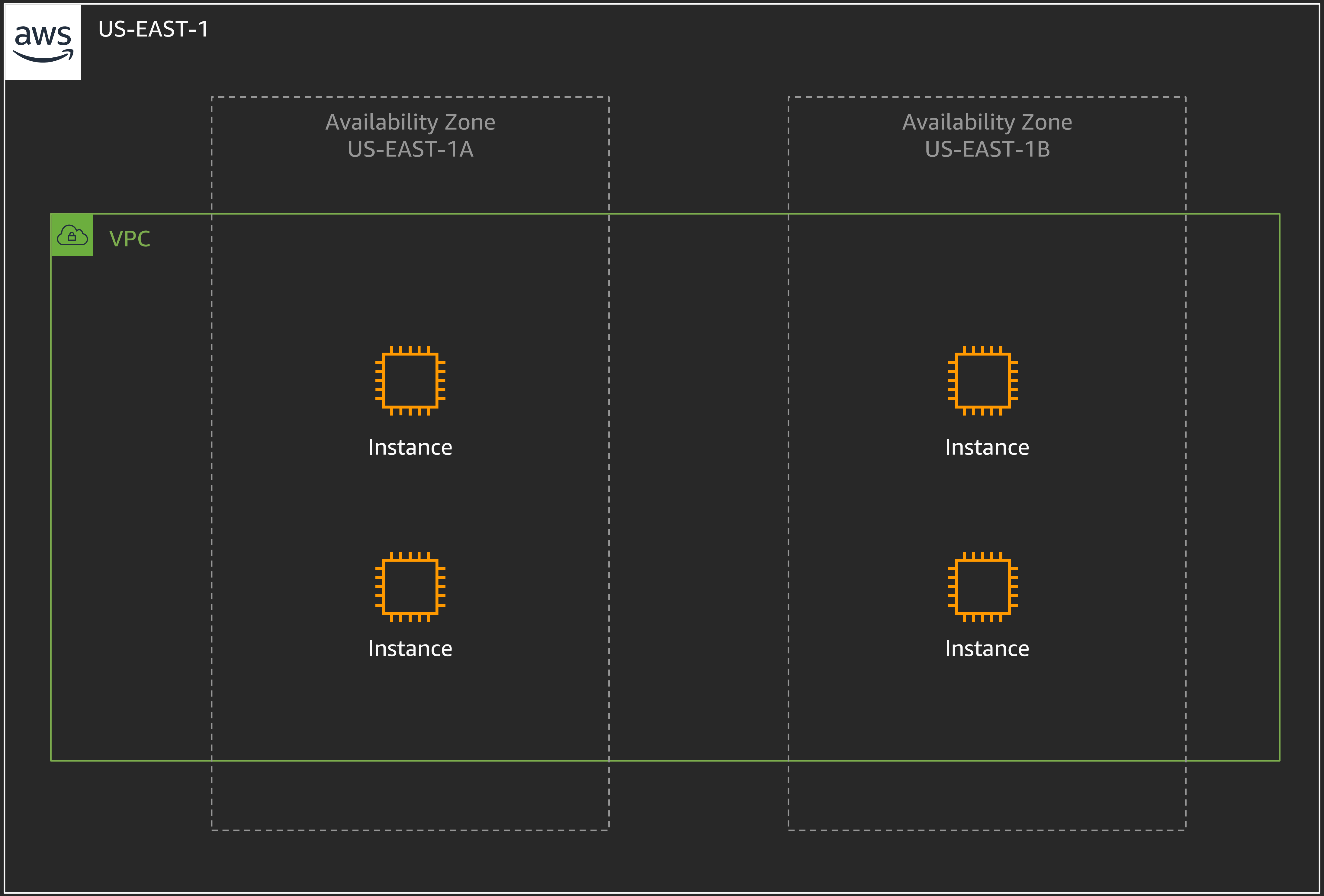
AVAILABILITY ZONE



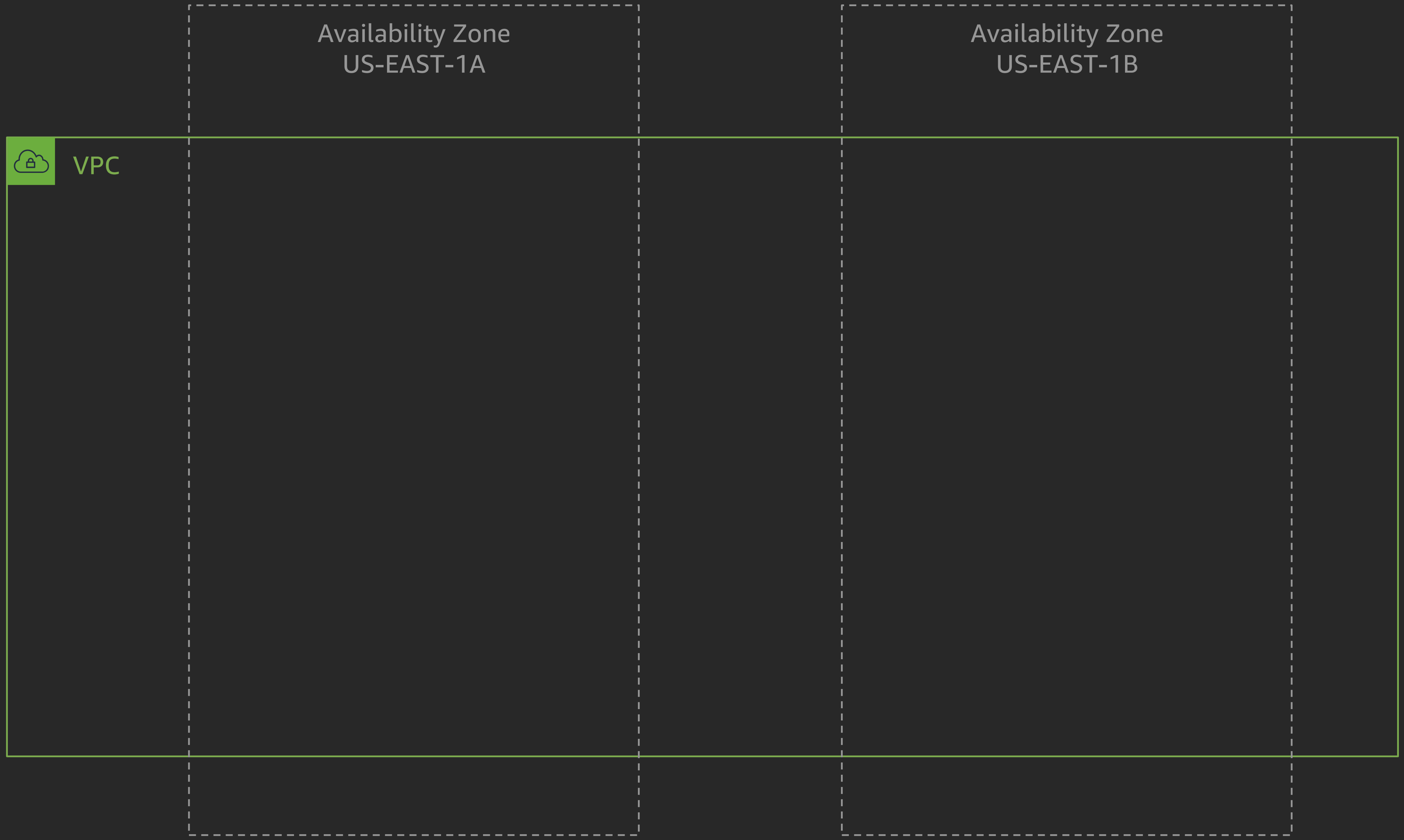
DATA CENTER, RACK, HOST



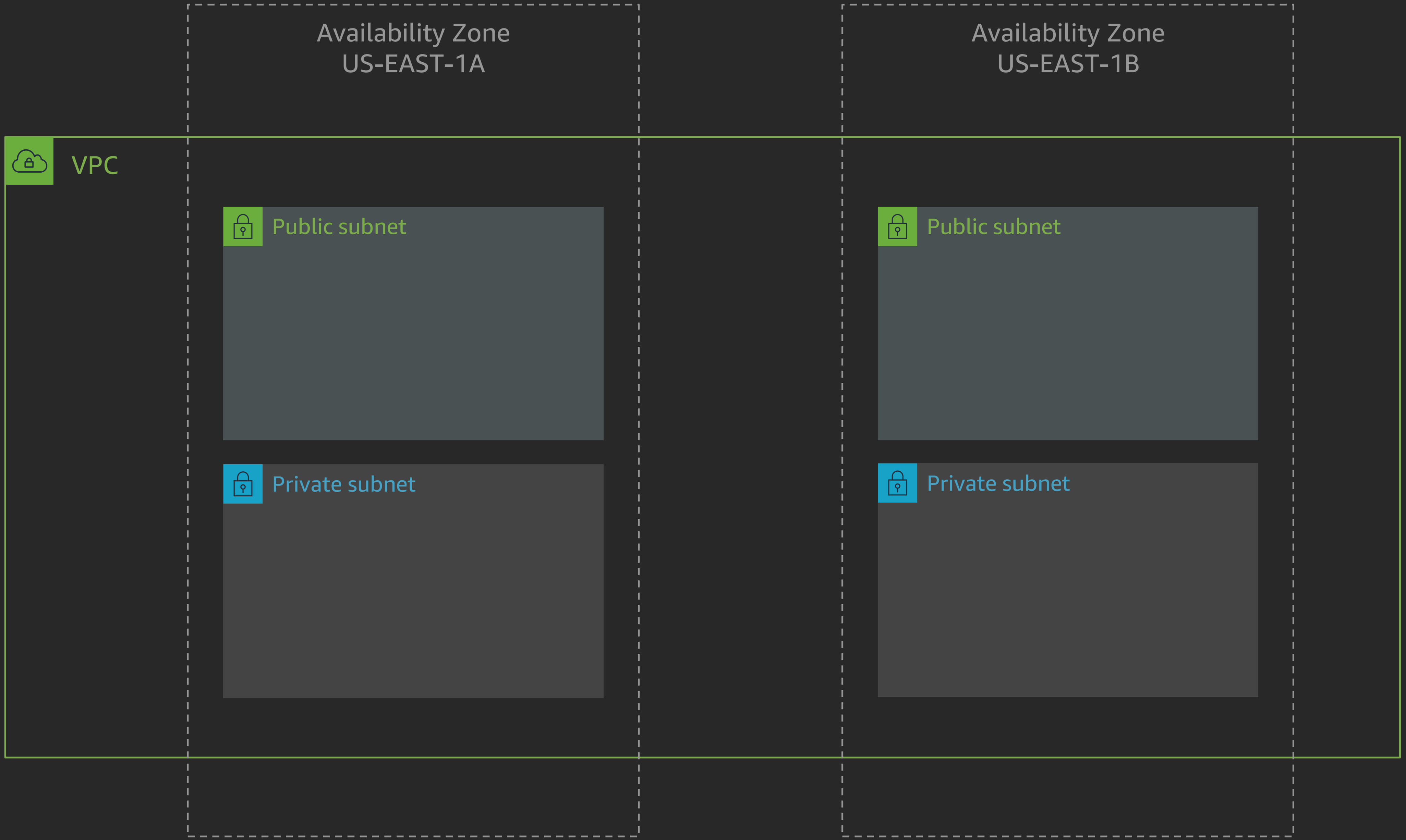



aws
US-EAST-1
Availability Zone
US-EAST-1A
Availability Zone
US-EAST-1B
VPC
Instance
Instance
Instance
Instance

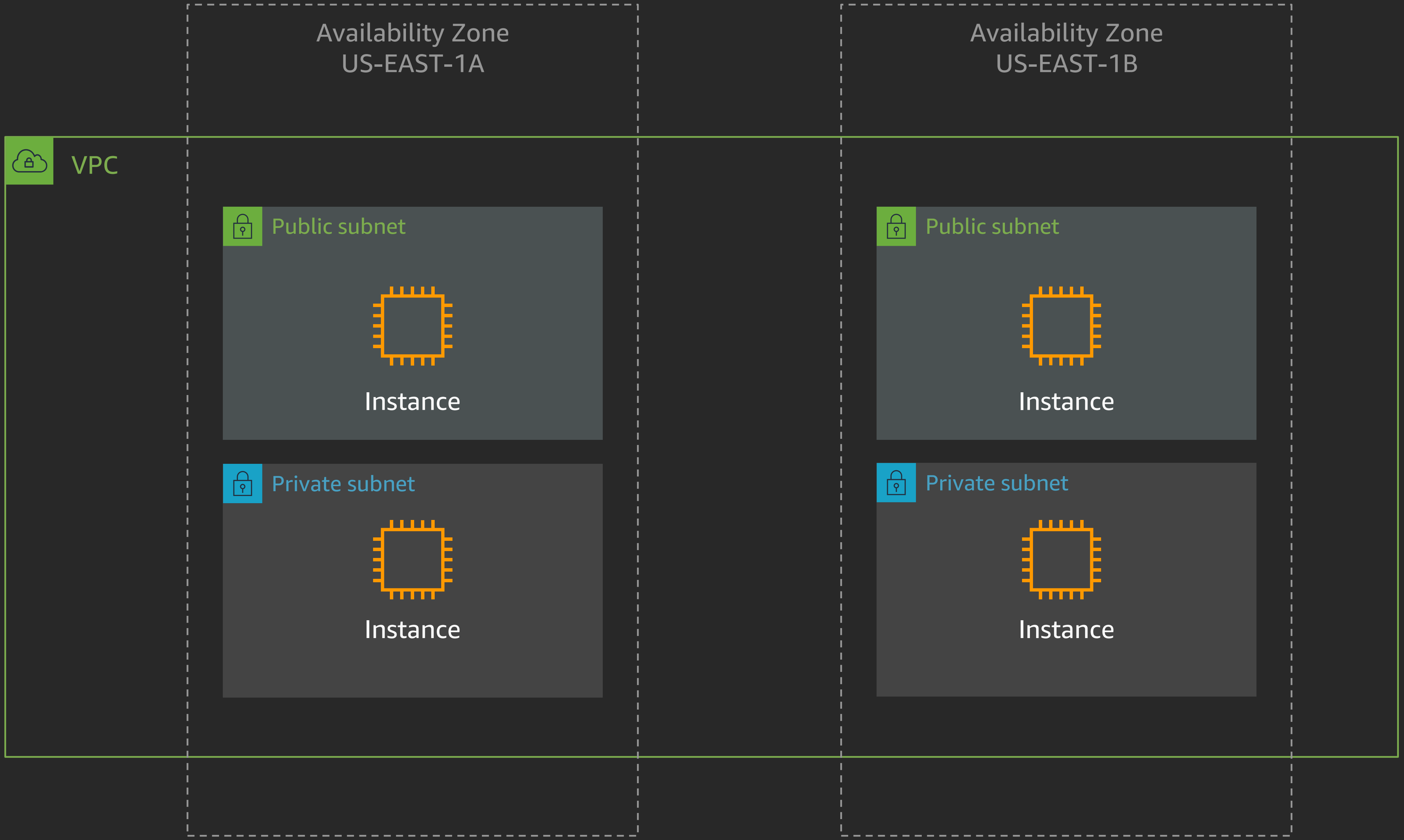
Amazon Virtual Private Cloud (Amazon VPC)



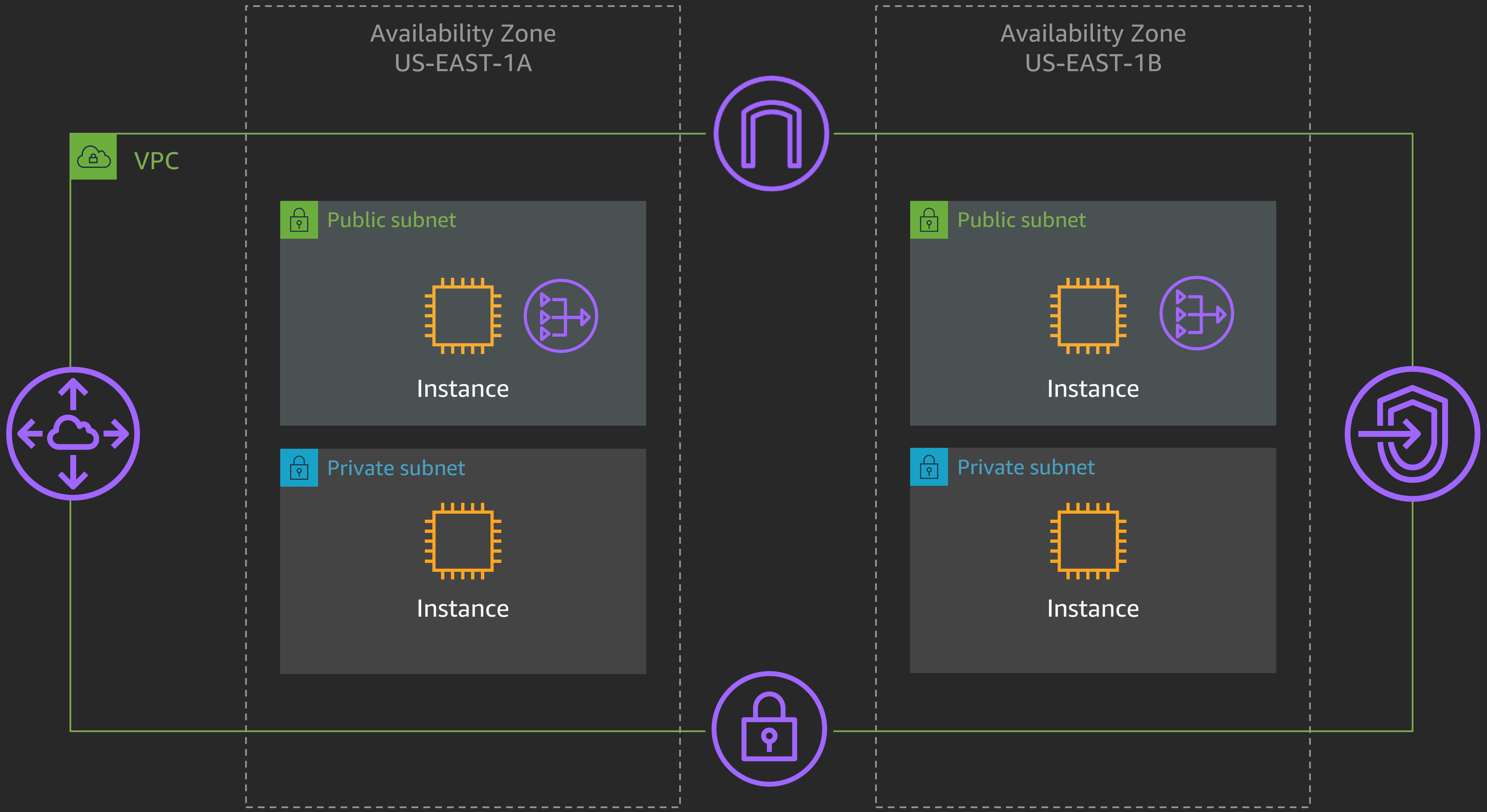
Subnets


Availability Zone
US-EAST-1A
Availability Zone
US-EAST-1B
VPC
Public subnet
Public subnet
Private subnet
Private subnet

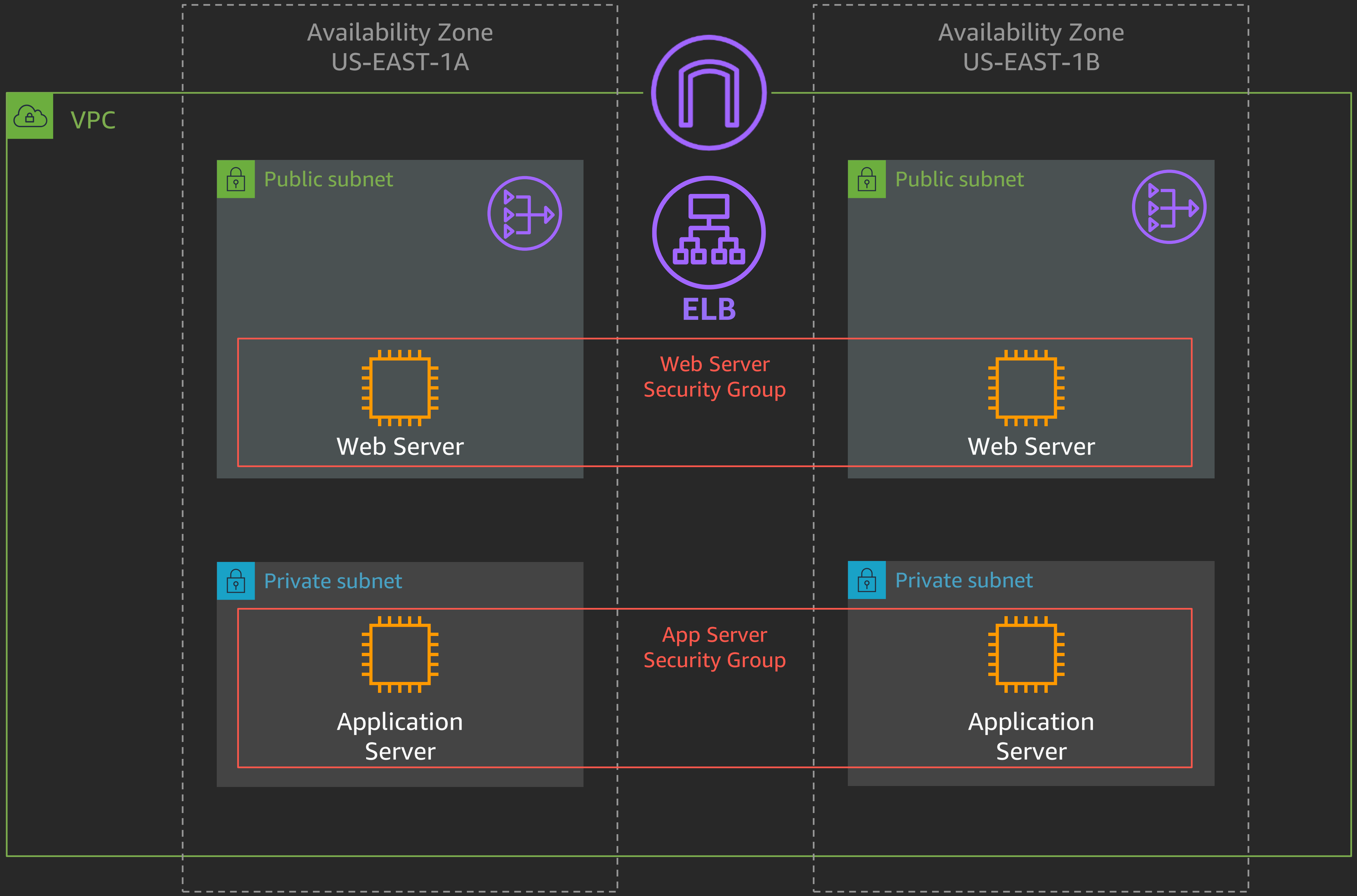
EC2 instances



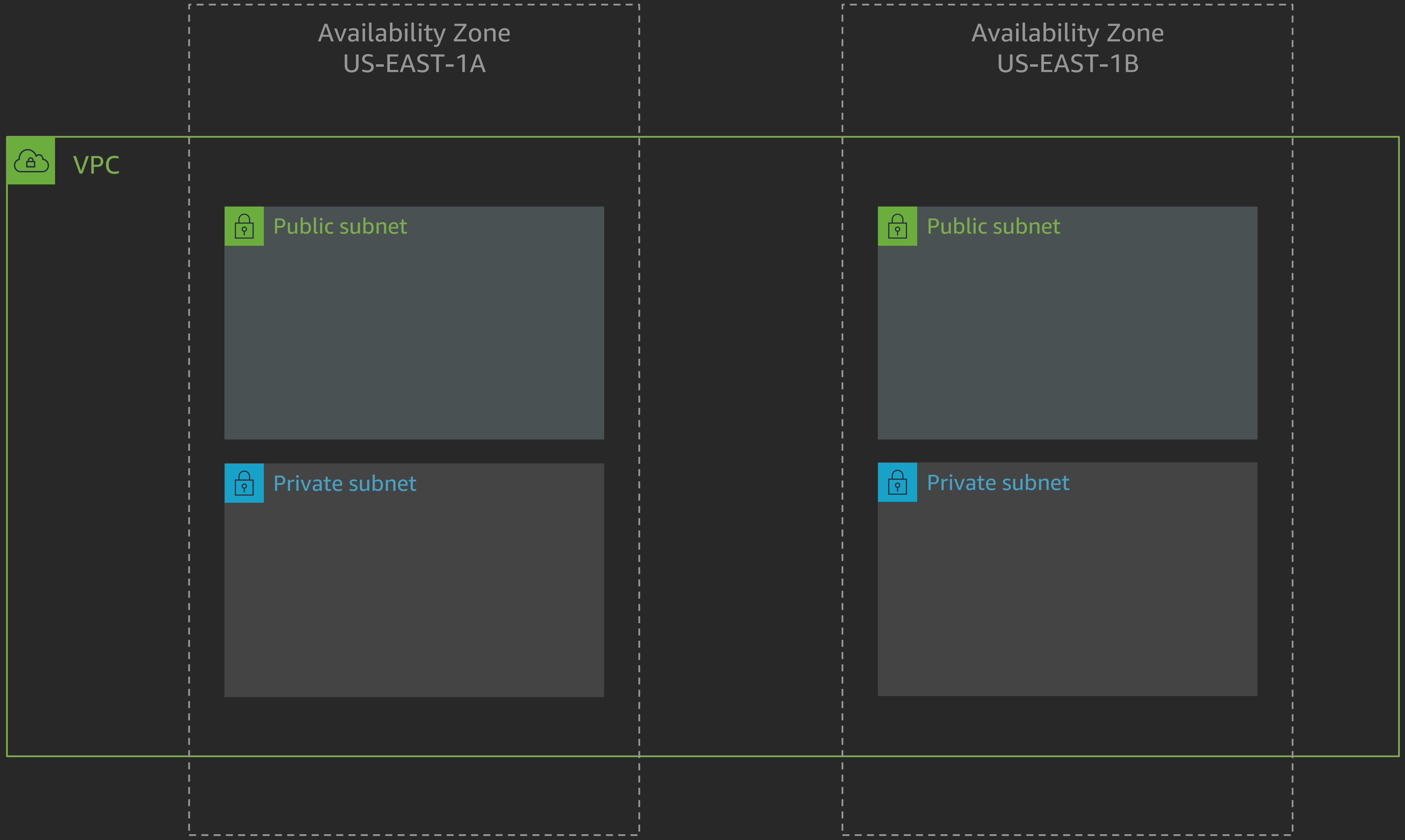
Gateways, endpoints & peering



Example web application



IP addressing

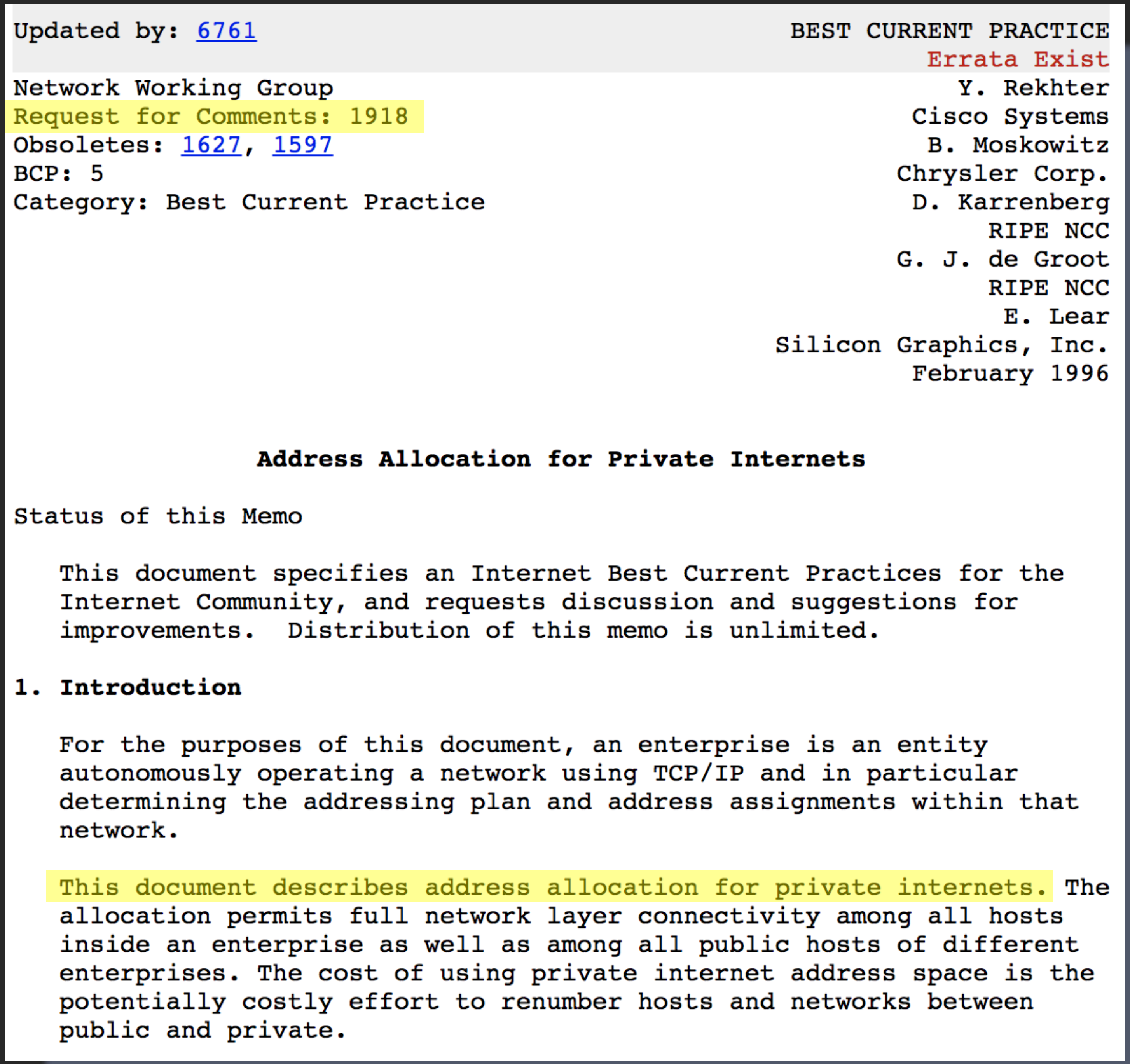


Private IP address range for your VPC – IPv4

- "CIDR" Range ?
  - Classless Inter-domain Routing
  - No more Class A, B, C

- RFC1918
  - 192.168.0.0 /16
  - 172.16.0.0 /12
  - 10.0.0.0 /8

- How much ?
  - /16
  - /28



Updated by: 6761 BEST CURRENT PRACTICE
Errata Exist

Network Working Group Y. Rekhter
Request for Comments: 1918 Cisco Systems
Obsoletes: 1627, 1597 B. Moskowitz
BCP: 5 Chrysler Corp.
Category: Best Current Practice D. Karrenberg
RIPE NCC
G. J. de Groot
RIPE NCC
E. Lear
Silicon Graphics, Inc.
February 1996

Address Allocation for Private Internets

Status of this Memo

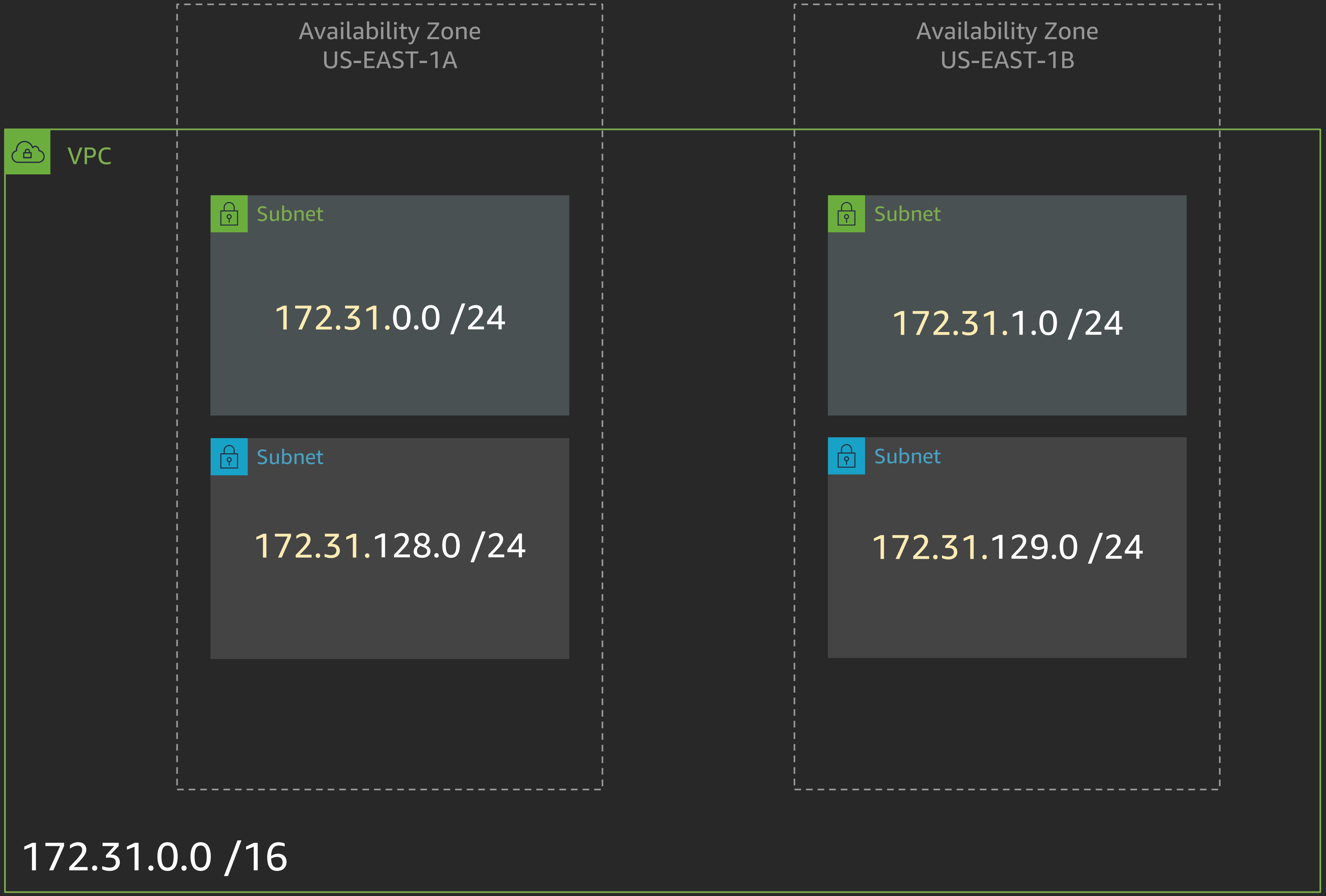
This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

1. Introduction

For the purposes of this document, an enterprise is an entity autonomously operating a network using TCP/IP and in particular determining the addressing plan and address assignments within that network.

This document describes address allocation for private internets. The allocation permits full network layer connectivity among all hosts inside an enterprise as well as among all public hosts of different enterprises. The cost of using private internet address space is the potentially costly effort to renumber hosts and networks between public and private.

Where to use IPv4 addresses ?



IPv6 basics

IPv6: Colon-Separated Hextet Notation + CIDR

2001:0db8:0ec2:0000:0000:0000:0000:0001/64	0000:0000:0000:0000:0000:0000:0000:0001/128
2001:db8:ec2:0:0:0:0:1/64	0:0:0:0:0:0:0:1/128
2001:db8:ec2::1/64	::1/128

Unicast Addresses

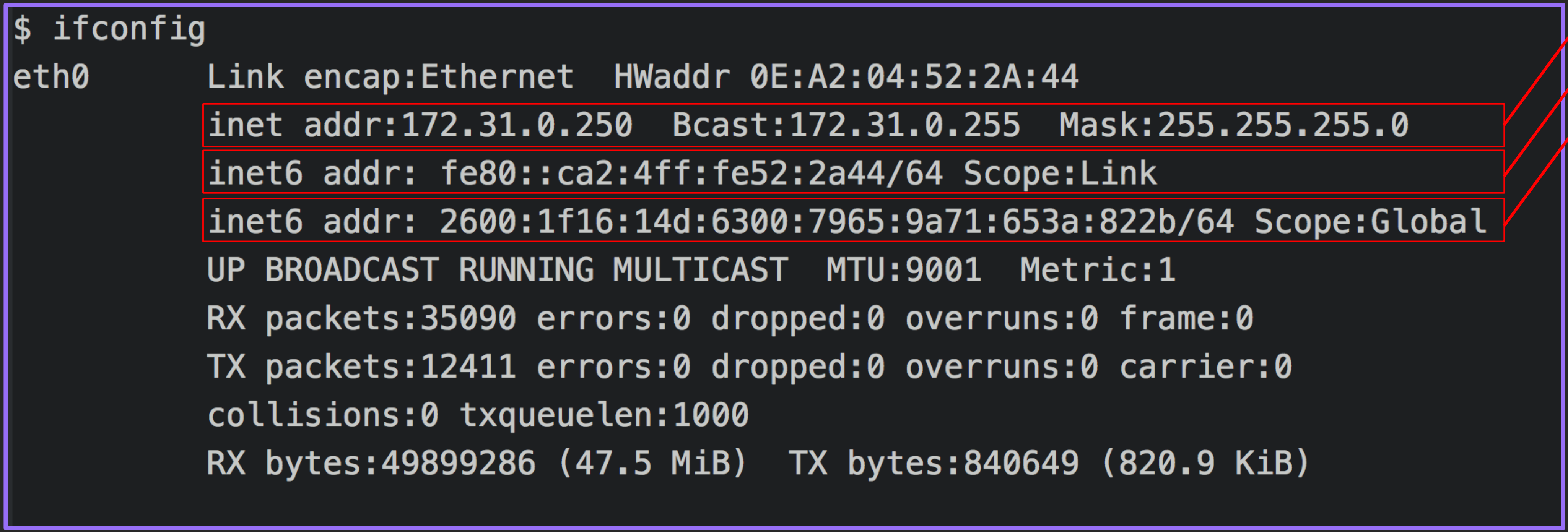
Loopback Address	::1
Link Local Address (LLA)	fe80::/10 (fe80::/64 in practice)
Global Unicast Address (GUA)	2600:1f16:14d:6300::/64

Multicast Addresses (ff00::/8)

All Nodes	ff02::1
All Routers	ff02::2
Solicited Node	ff02::1:ff00:0/104

IPv6 on AWS

- /56 VPC
- /64 Subnets
- Dualstack
- Link Local Address and Global Unicast Address required



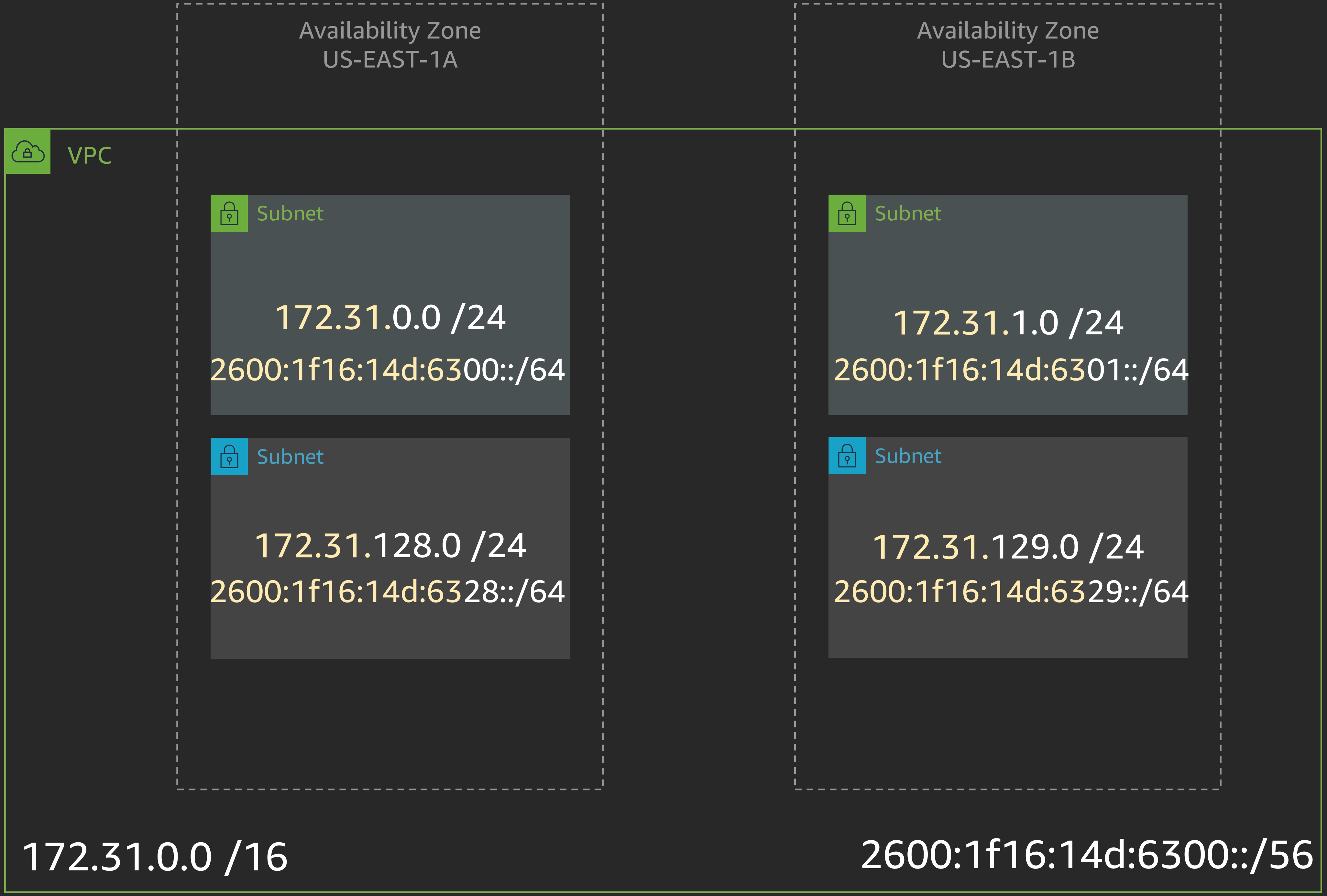
```
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0E:A2:04:52:2A:44
          inet addr:172.31.0.250  Bcast:172.31.0.255  Mask:255.255.255.0
          inet6 addr: fe80::ca2:4ff:fe52:2a44/64 Scope:Link
          inet6 addr: 2600:1f16:14d:6300:7965:9a71:653a:822b/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:35090 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12411 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:49899286 (47.5 MiB)  TX bytes:840649 (820.9 KiB)
```

IPv4 Private Address

IPv6 Link Local Address
(Private)

IPv6 Global Unicast Address
(Public)

Where to use IPv6 addresses ?



Availability Zone
US-EAST-1A

Availability Zone
US-EAST-1B

VPC

Subnet
172.31.0.0 /24
2600:1f16:14d:6300::/64

Subnet
172.31.1.0 /24
2600:1f16:14d:6301::/64

Subnet
172.31.128.0 /24
2600:1f16:14d:6328::/64

Subnet
172.31.129.0 /24
2600:1f16:14d:6329::/64

172.31.0.0 /16

2600:1f16:14d:6300::/56

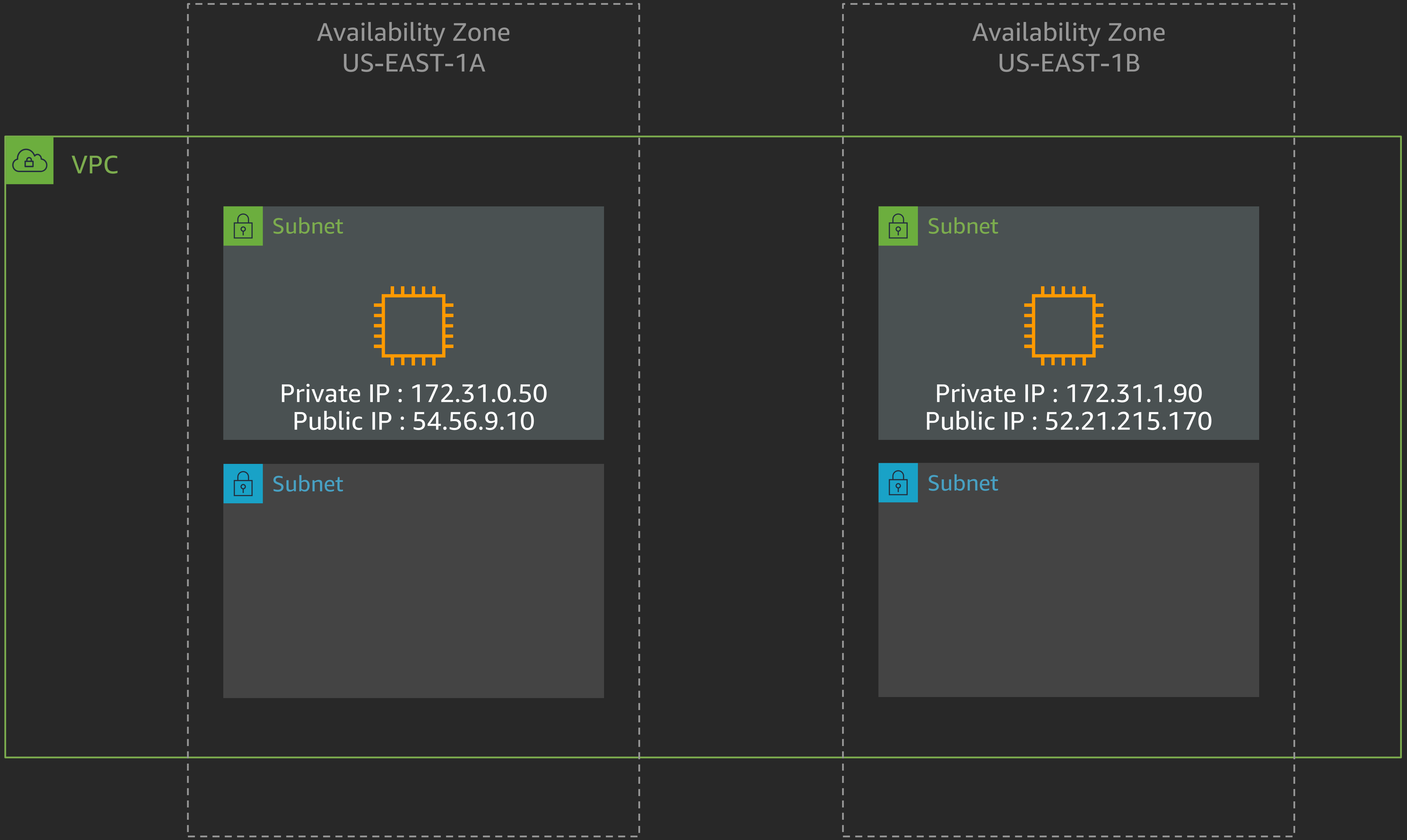
The “5 Things” required for Internet traffic

1. Public IP Address
2. Internet Gateway Attached to a VPC
3. Route to an Internet Gateway
4. NACL Allow Rule
5. Security Group Allow Rule

Public IP addresses for your instances

- Auto-assign public IP addresses
- Elastic IP Addresses (EIP)
  - Amazon EIP Pool
  - Bring Your Own IP (BYOIP) Pool

Public IP addresses



Gateways, endpoints & peering

Customer Gateway

VPN Gateway

NAT Gateway

Internet Gateway

AWS Transit Gateway

Endpoints

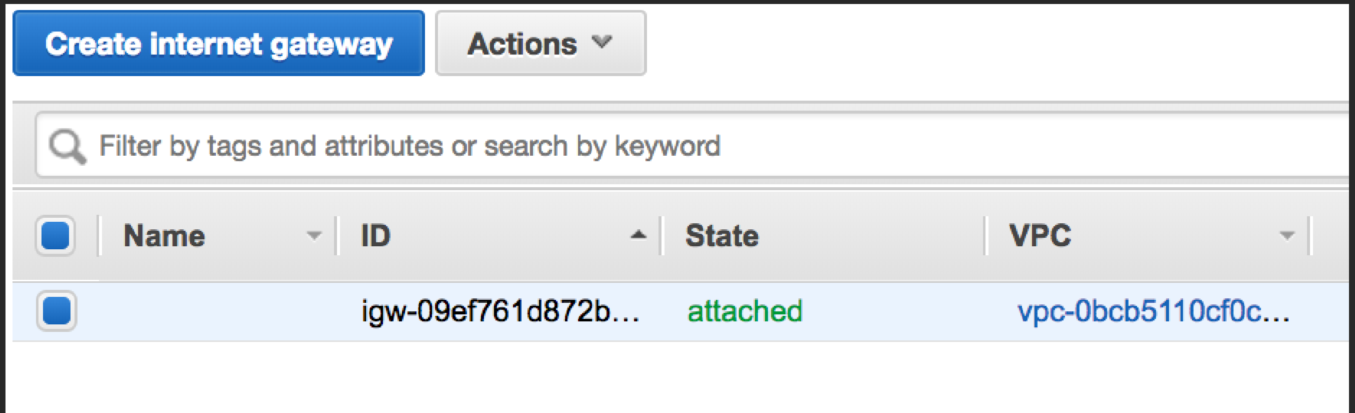
Peering connection

Internet access

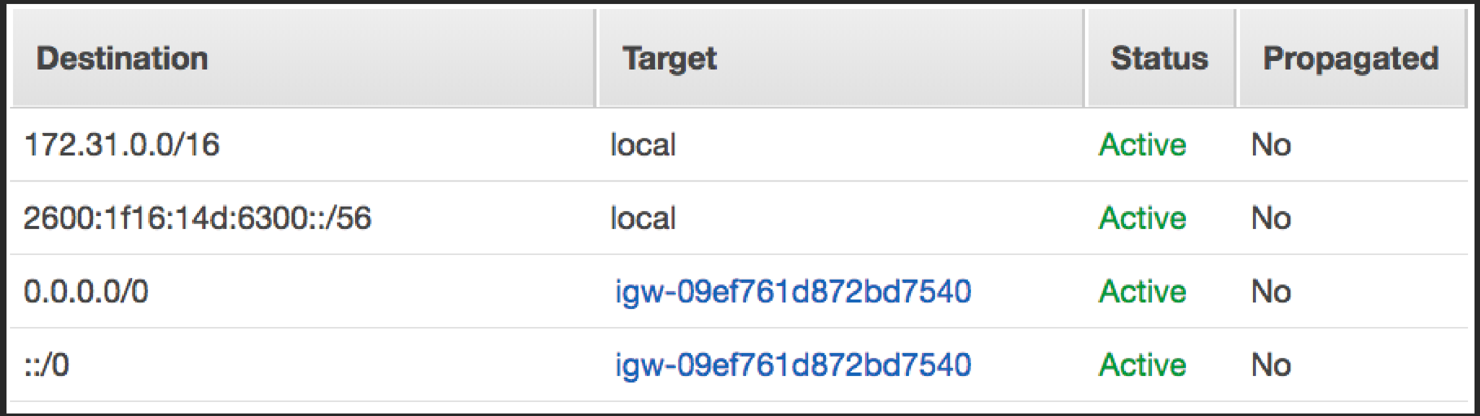
172.16.0.0

172.16.1.0

172.16.2.0



☐	Name	ID	State	VPC
☐		igw-09ef761d872b...	attached	vpc-0bcb5110cf0c...



Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09ef761d872bd7540	Active	No
::/0	igw-09ef761d872bd7540	Active	No

“To get to the IPv4 Internet (0.0.0.0/0) go via the Internet Gateway (IGW)”

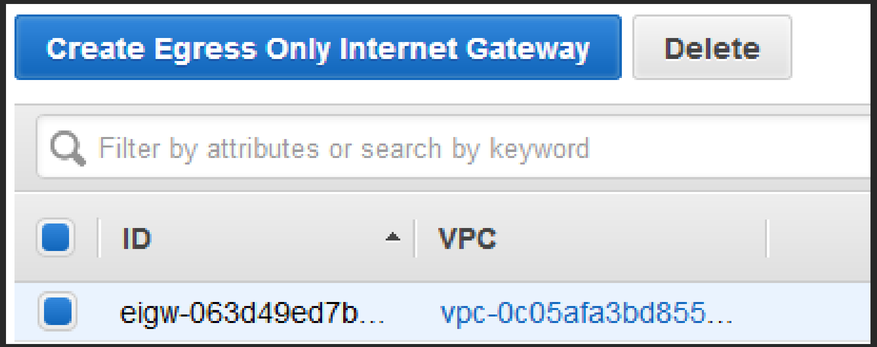
“To get to the IPv6 Internet (::/0) go via the Internet Gateway (IGW)”

Internet access

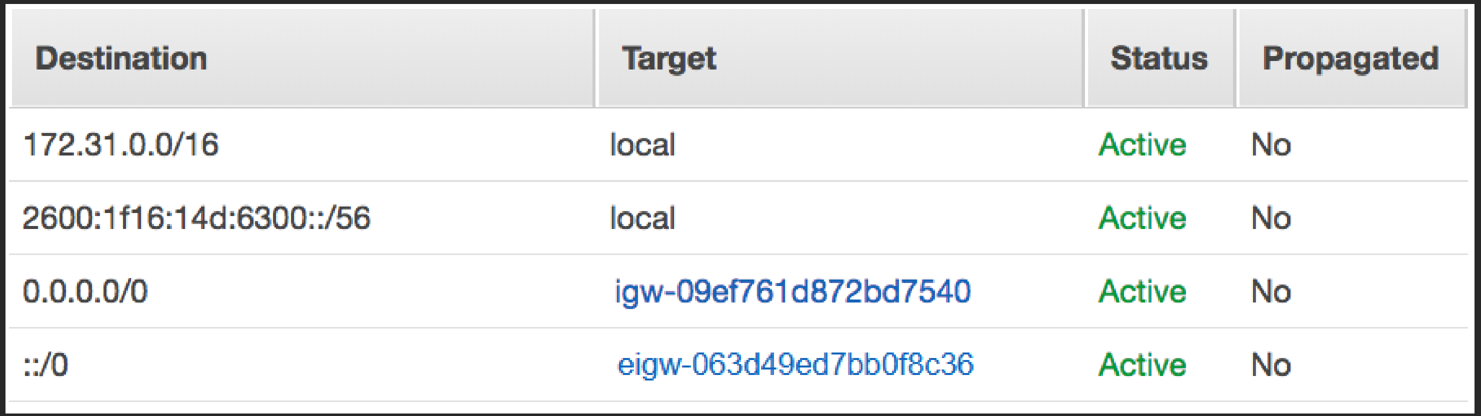
172.16.0.0

172.16.1.0

172.16.2.0


Create Egress Only Internet Gateway
Delete
Filter by attributes or search by keyword

☐	ID	VPC
☐	eigw-063d49ed7b...	vpc-0c05afa3bd855...



Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09ef761d872bd7540	Active	No
::/0	eigw-063d49ed7bb0f8c36	Active	No

“To get to the IPv6 Internet (::/0) go via the Egress Only Internet Gateway (EIGW)”

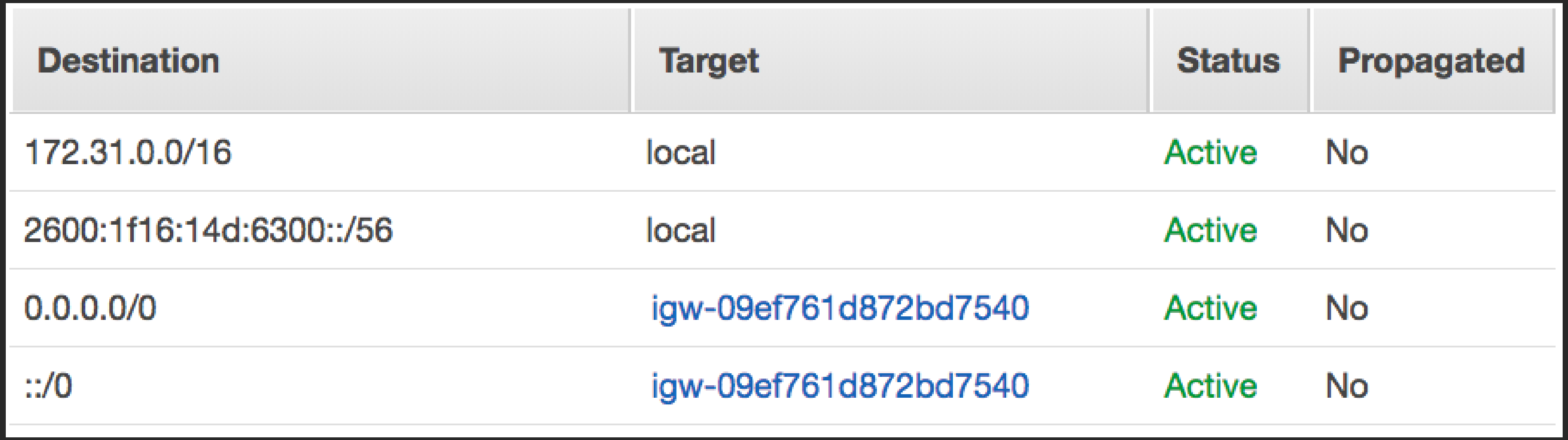
Different routes for different subnets

172.16.0.0

172.16.1.0

172.16.2.0

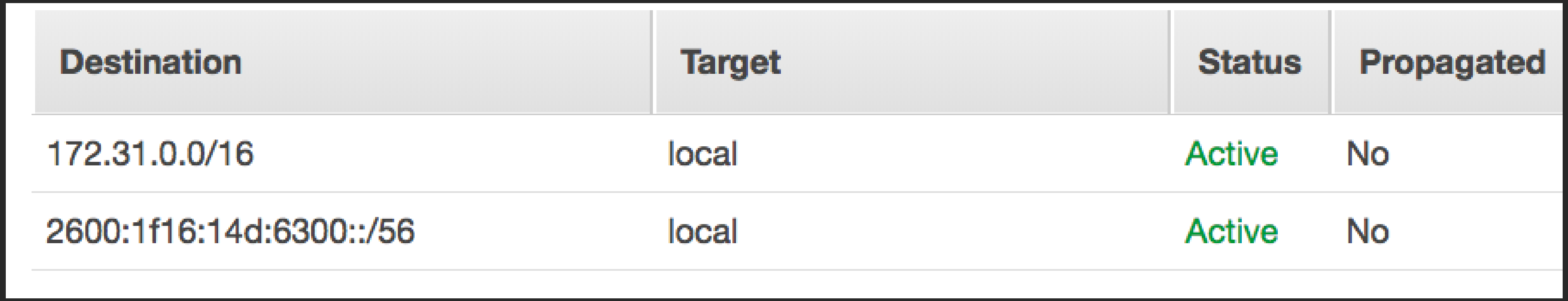
Public subnet



Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09ef761d872bd7540	Active	No
::/0	igw-09ef761d872bd7540	Active	No

"To get to the Internet go via the Internet Gateway (IGW)"

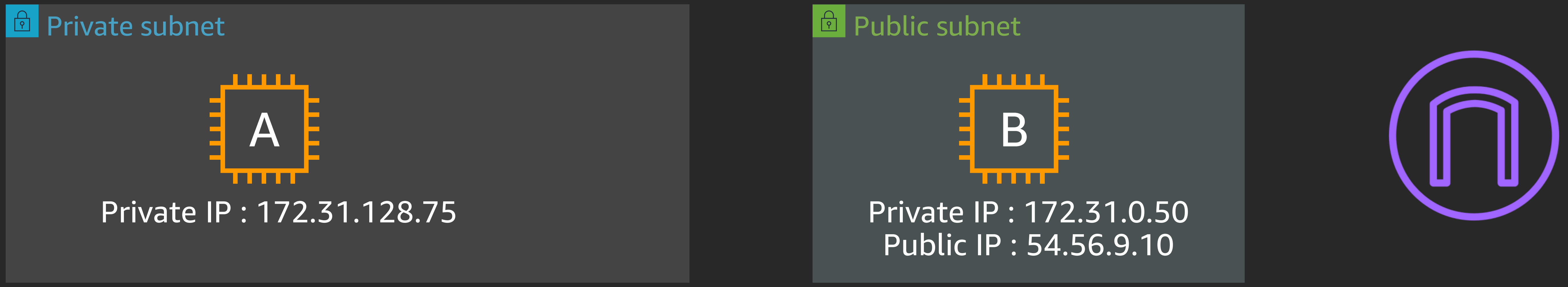
Private subnet

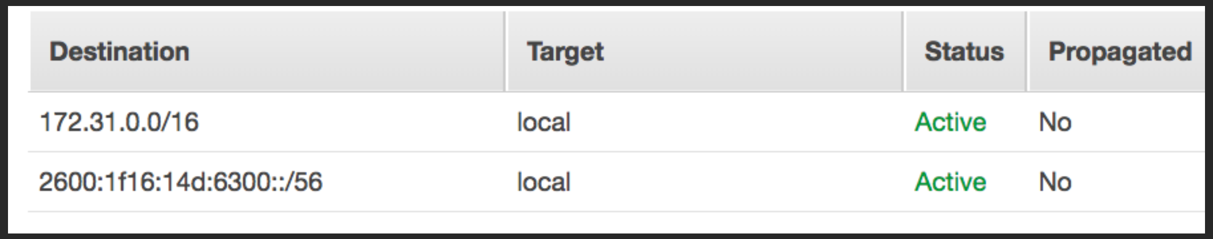


Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No

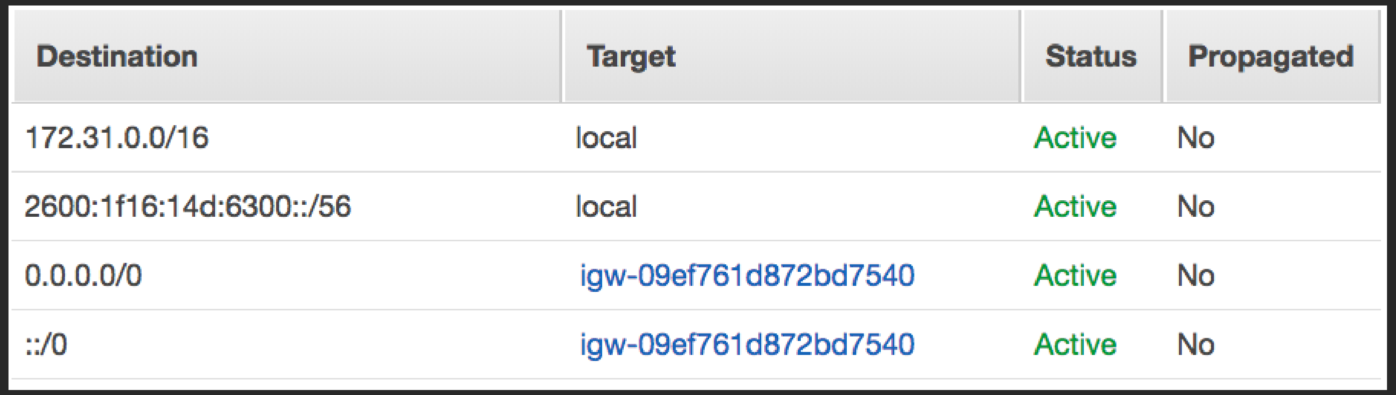
"To get to anything in the VPC – stay local. No route anywhere else."

Public & private subnets





Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No

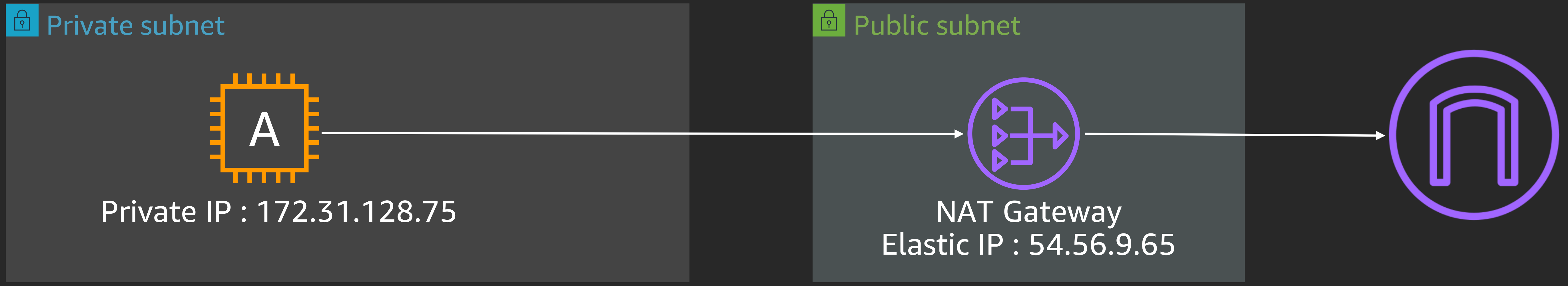


Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09ef761d872bd7540	Active	No
::/0	igw-09ef761d872bd7540	Active	No

“Instance A has a path to and from Instance B.”

”Instance B has a path to and from the Internet.”

Network Address Translation (NAT) Gateway

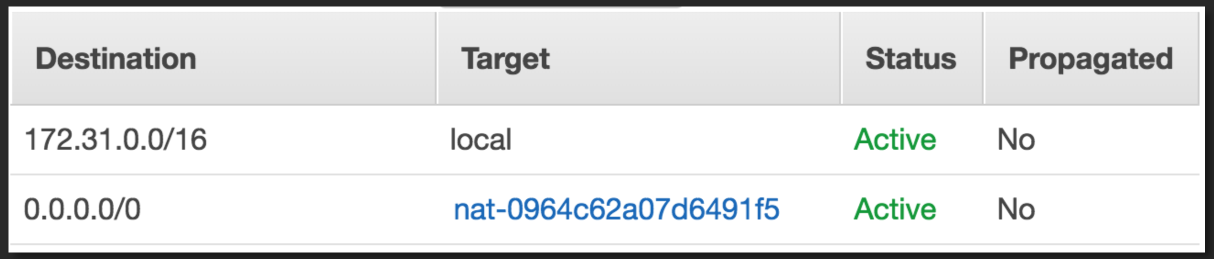


Private subnet

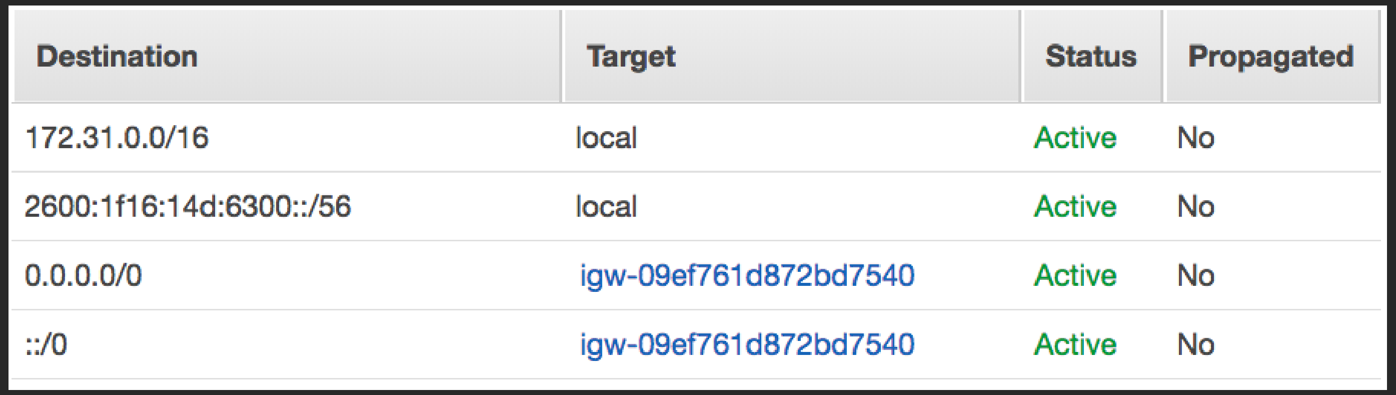
Private IP : 172.31.128.75

Public subnet

NAT Gateway
Elastic IP : 54.56.9.65



Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	nat-0964c62a07d6491f5	Active	No



Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09ef761d872bd7540	Active	No
::/0	igw-09ef761d872bd7540	Active	No

The Route Table for the Private Subnet says to send all IPv4 Internet Traffic to the NAT Gateway.

The NAT Gateway translates all traffic it receives such that it appears to come from itself.

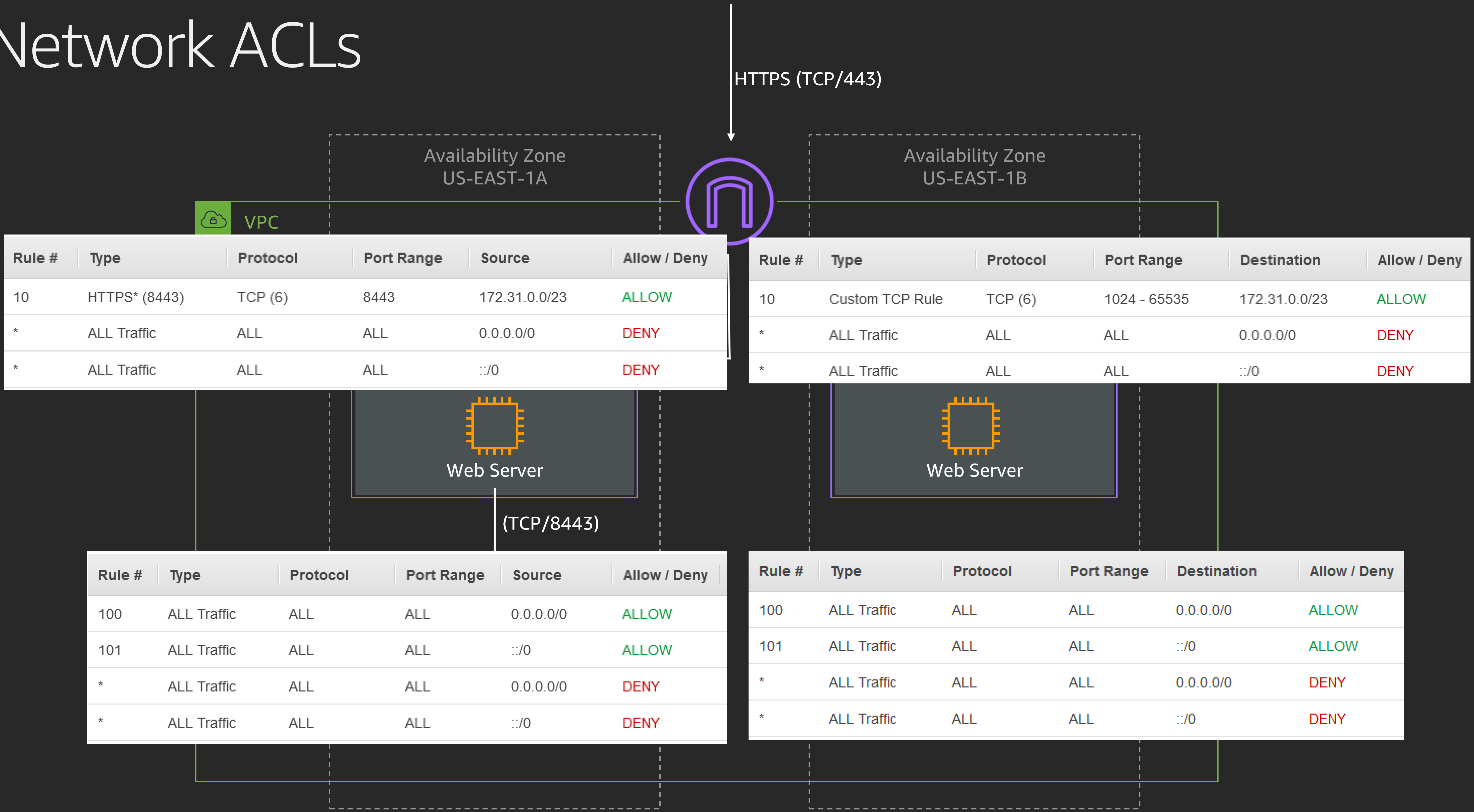
The Route Table for the Public Subnet says to send all Internet Traffic to the Internet Gateway.

Network security

Network security

- Network ACLs
- Security Groups
- VPC Flow Logs
- Amazon VPC Traffic Mirroring

Network ACLs



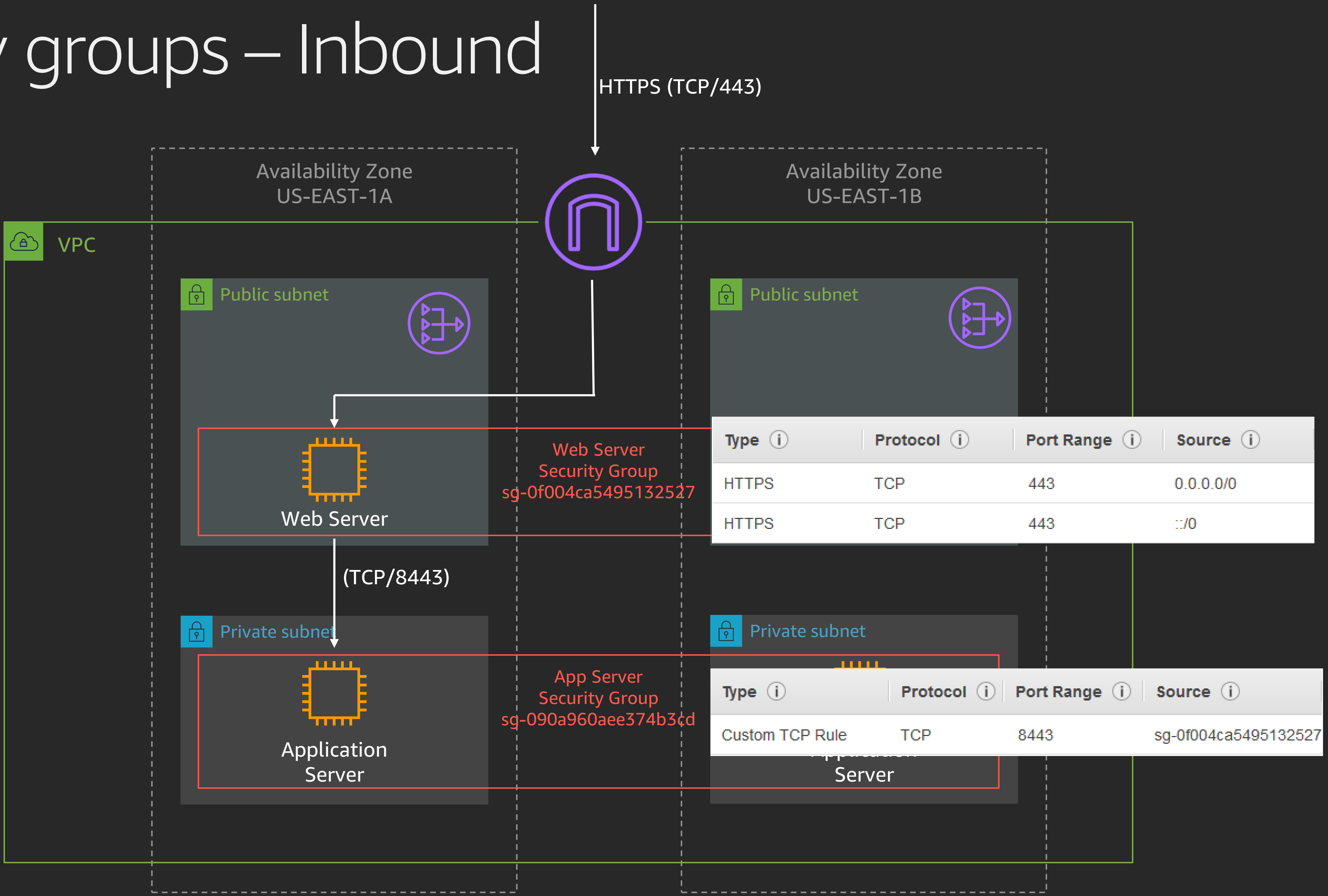
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
10	HTTPS* (8443)	TCP (6)	8443	172.31.0.0/23	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
10	Custom TCP Rule	TCP (6)	1024 - 65535	172.31.0.0/23	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

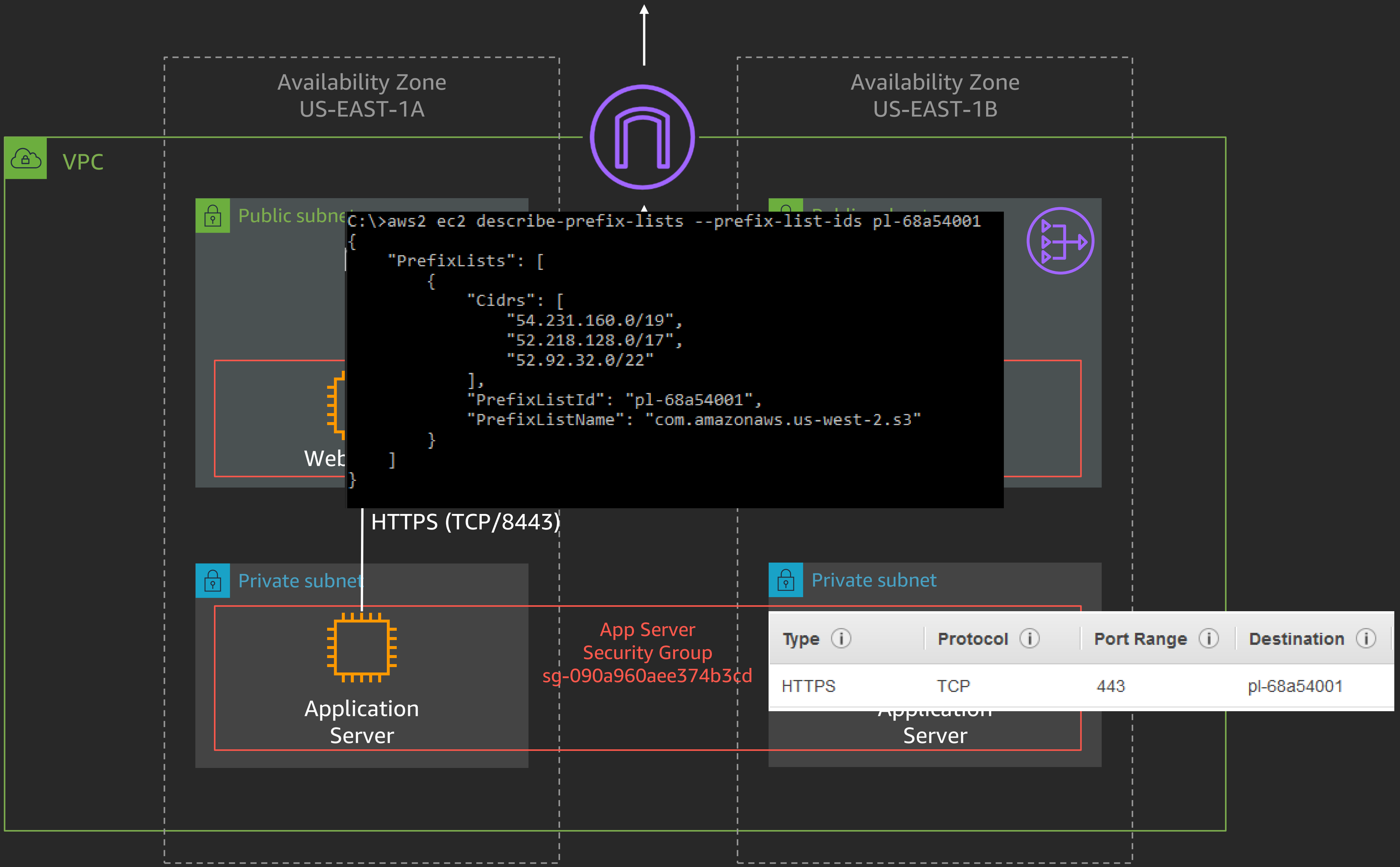
Security groups – Inbound



Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	::/0

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
Custom TCP Rule	TCP	8443	sg-0f004ca5495132527

Security groups – Outbound

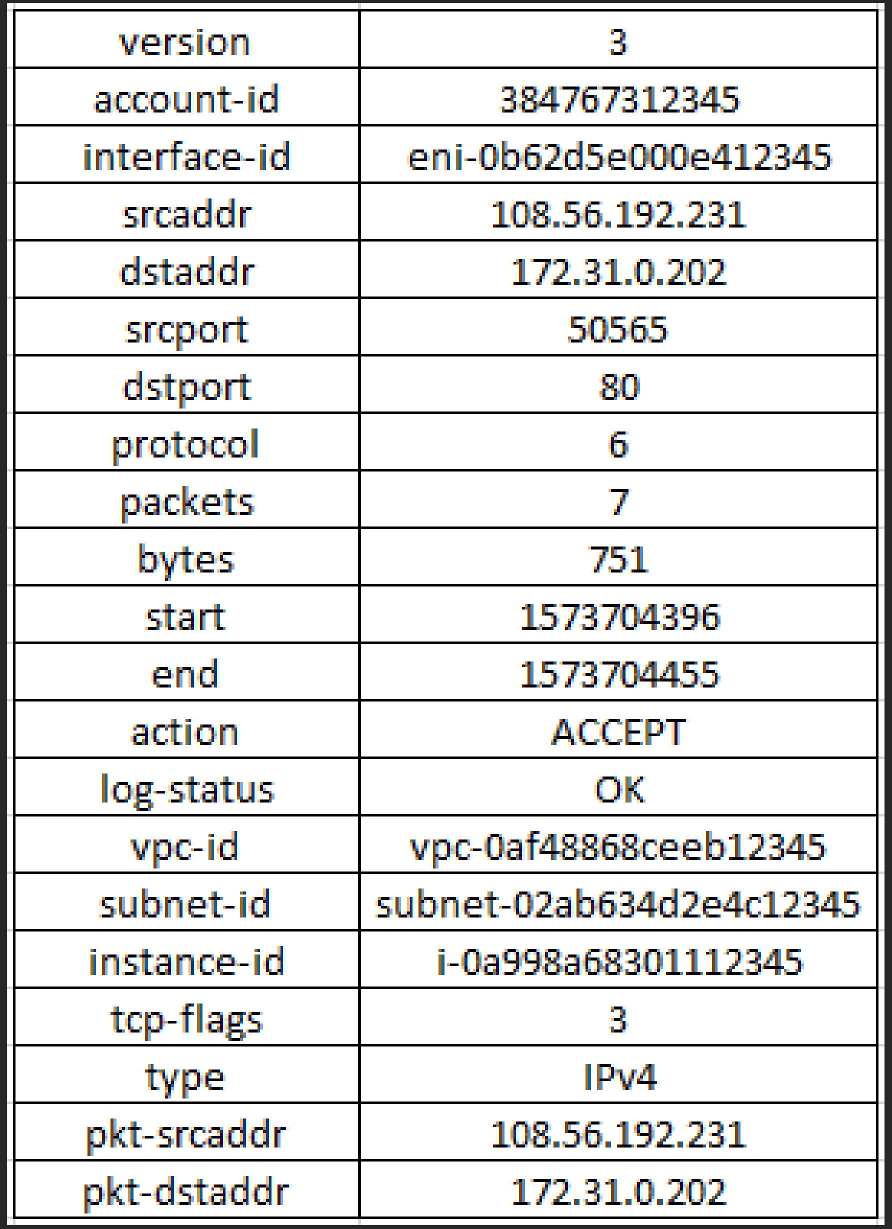


```
C:\>aws2 ec2 describe-prefix-lists --prefix-list-ids pl-68a54001
{
    "PrefixLists": [
        {
            "Cidrs": [
                "54.231.160.0/19",
                "52.218.128.0/17",
                "52.92.32.0/22"
            ],
            "PrefixListId": "pl-68a54001",
            "PrefixListName": "com.amazonaws.us-west-2.s3"
        }
    ]
}
```

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Destination ⓘ
HTTPS	TCP	443	pl-68a54001

VPC flow logs

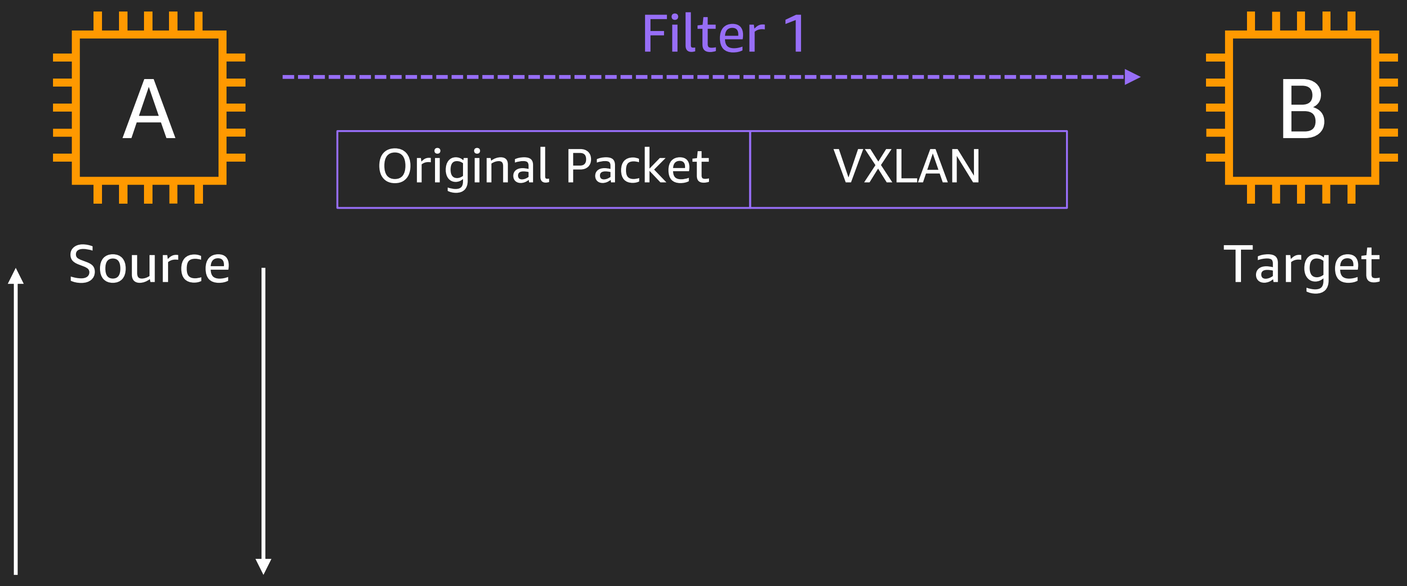
- Amazon CloudWatch Logs or Amazon S3
- Does not impact throughput or latency
- Apply to VPC, Subnet, or ENI
- Accepted, Rejected, or All traffic



version	3
account-id	384767312345
interface-id	eni-0b62d5e000e412345
srcaddr	108.56.192.231
dstaddr	172.31.0.202
srcport	50565
dstport	80
protocol	6
packets	7
bytes	751
start	1573704396
end	1573704455
action	ACCEPT
log-status	OK
vpc-id	vpc-0af48868ceeb12345
subnet-id	subnet-02ab634d2e4c12345
instance-id	i-0a998a68301112345
tcp-flags	3
type	IPv4
pkt-srcaddr	108.56.192.231
pkt-dstaddr	172.31.0.202

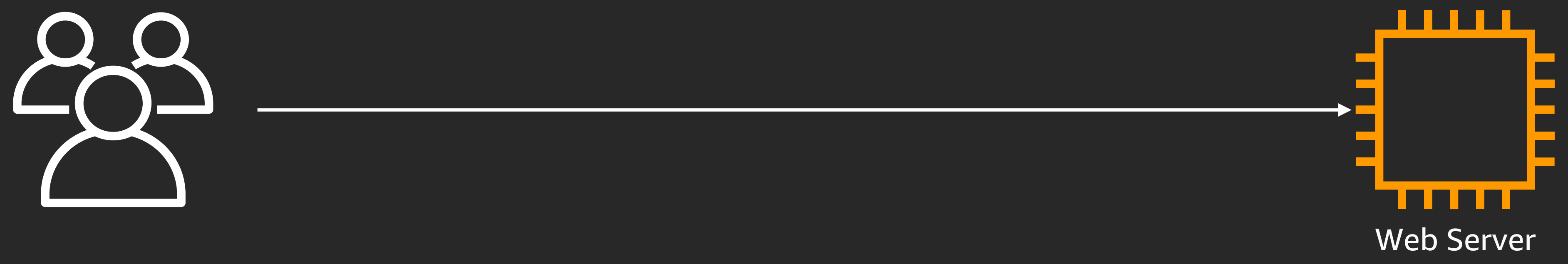
Amazon VPC traffic mirroring

- Mirror to another ENI or Network Load Balancer with UDP listener
- Packet copy. Shares interface bandwidth.
- Traffic mirror filters to define “interesting traffic”
- Traffic mirror session is the combination of source, target, and filter

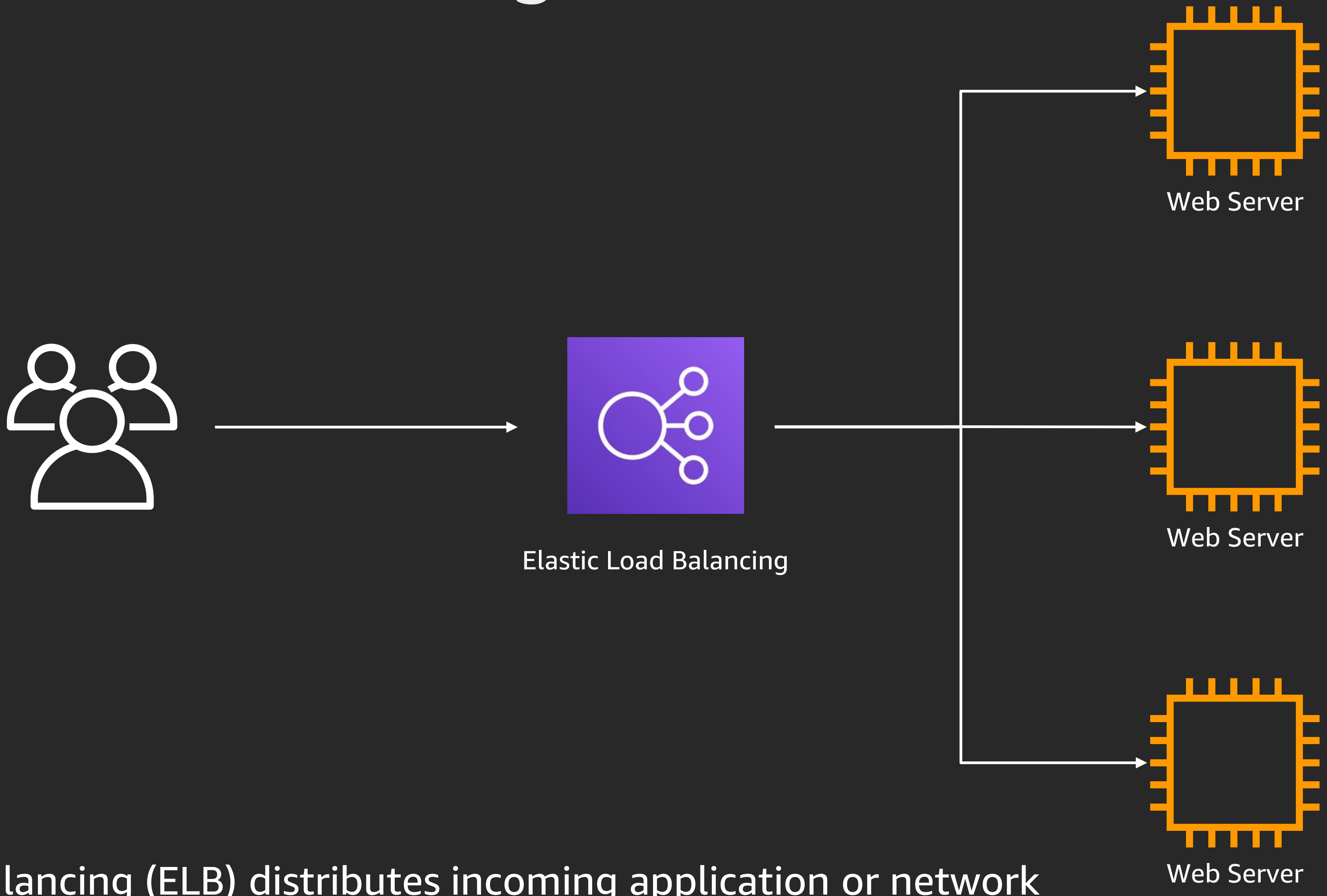


Elastic Load Balancing

High availability & scale



Elastic Load Balancing



Elastic Load Balancing (ELB) distributes incoming application or network traffic across multiple targets, such as Amazon EC2 instances, containers, Lambda functions, and IP addresses, in multiple Availability Zones.

ELB: Options

Application Load Balancer

- IPv4, Dualstack front-end
- Layer 7
- HTTP, HTTPS
- Host-, Path-based routing
- Integrated authentication
- Supported Targets
  - EC2 instances
  - Containers
  - AWS Lambda
  - Private IP addresses

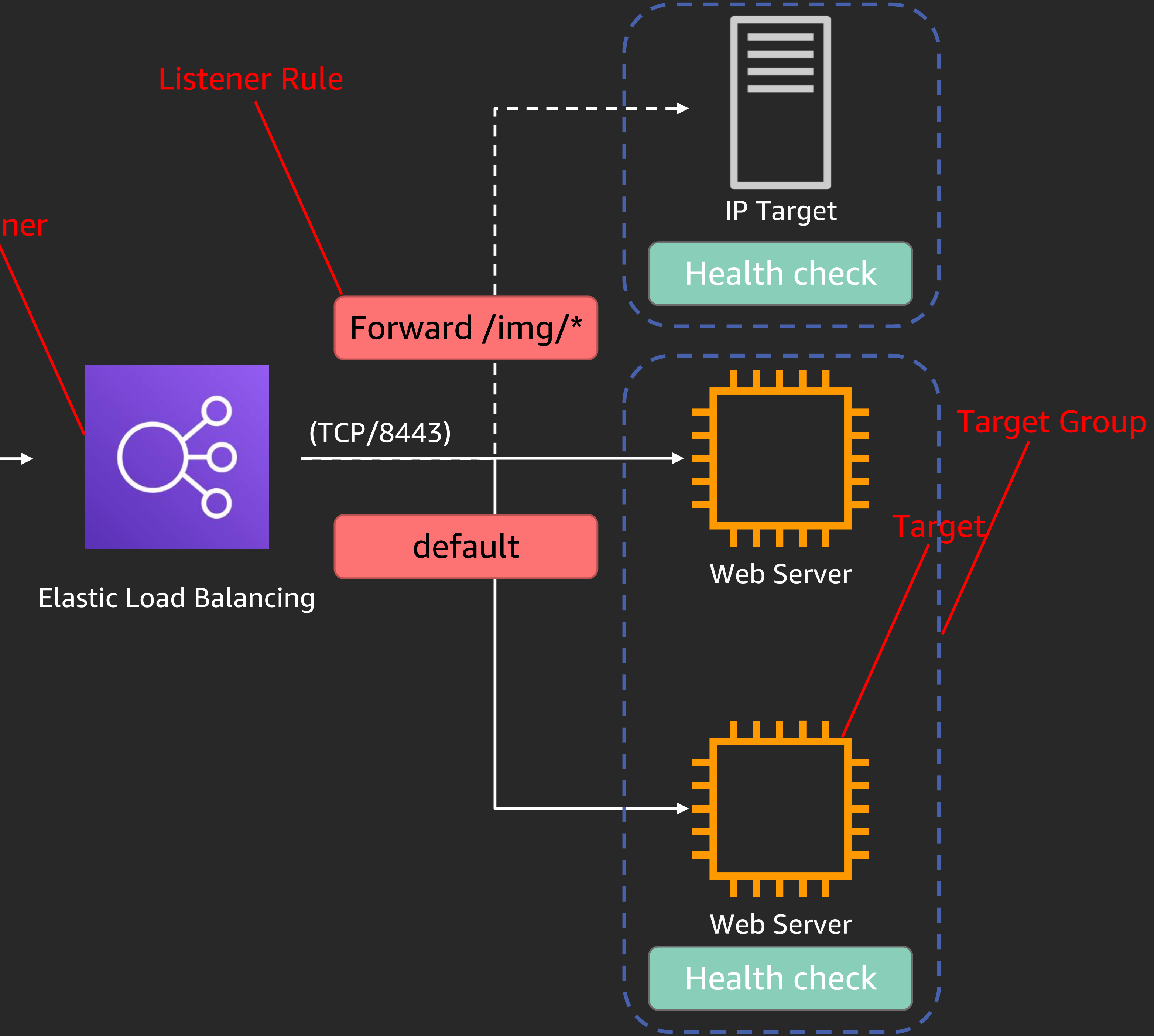
Network Load Balancer

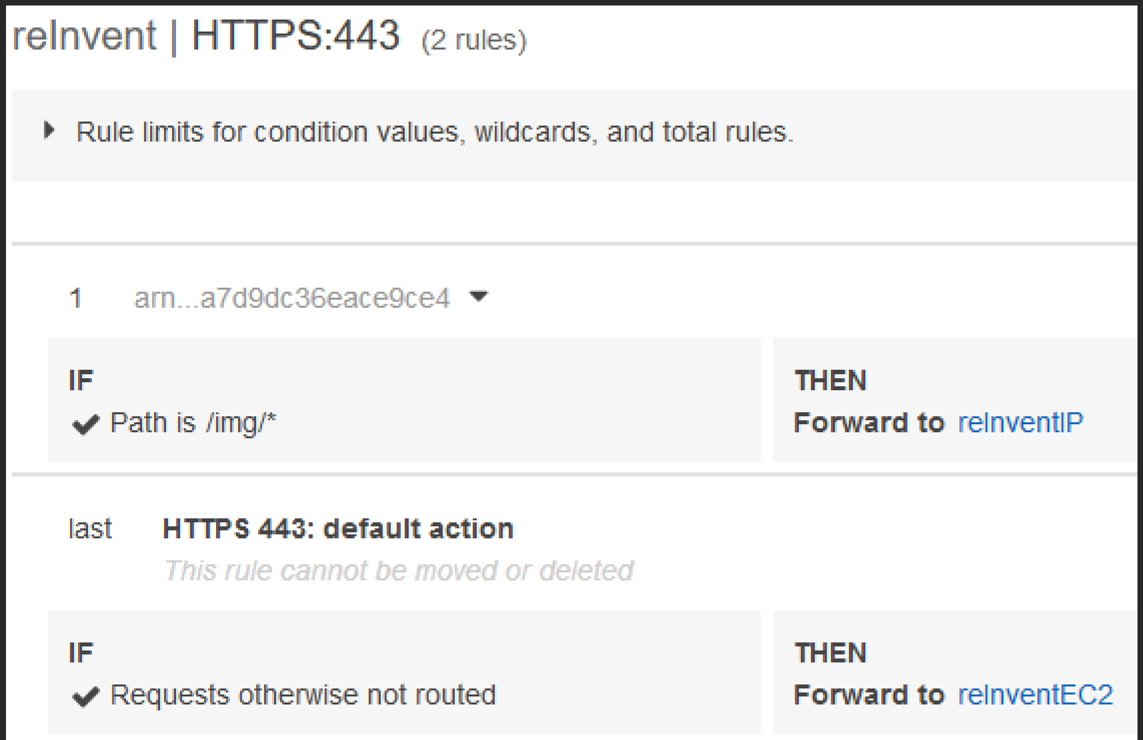
- IPv4
- Layer 4
- TCP, UDP, TLS
- Supported Targets
  - EC2 instances
  - Containers
  - Private IP addresses

Classic Load Balancer

- IPv4, Dualstack front-end
- Layer 4/7
- HTTP, HTTPS, TCP, TLS
- Supported Targets
  - EC2 Instances

ALB: Components





reInvent | HTTPS:443 (2 rules)

▸ Rule limits for condition values, wildcards, and total rules.

1 arn...a7d9dc36eace9ce4 ▾

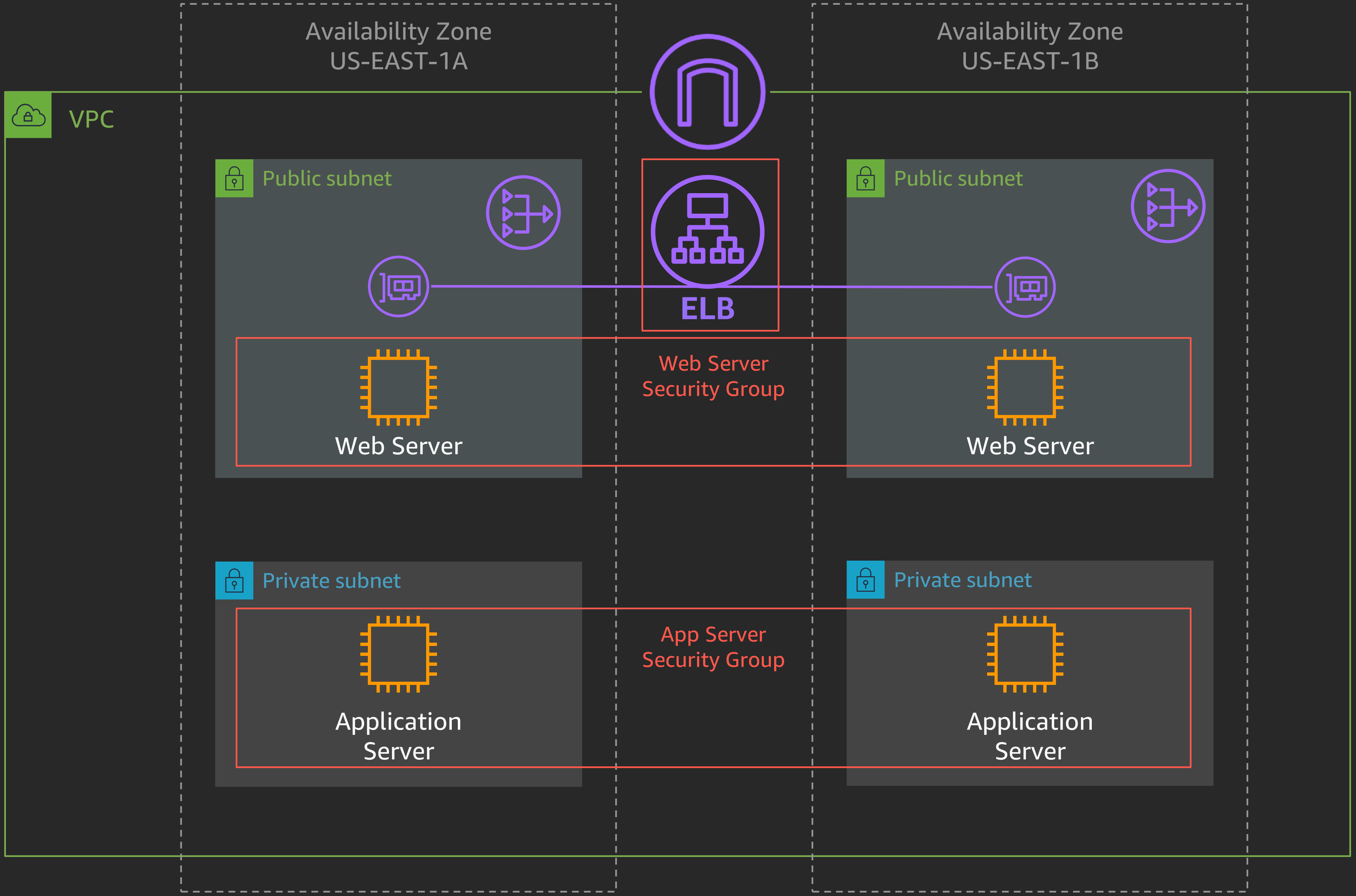
IF	THEN
✓ Path is /img/*	Forward to reInventIP

last **HTTPS 443: default action**

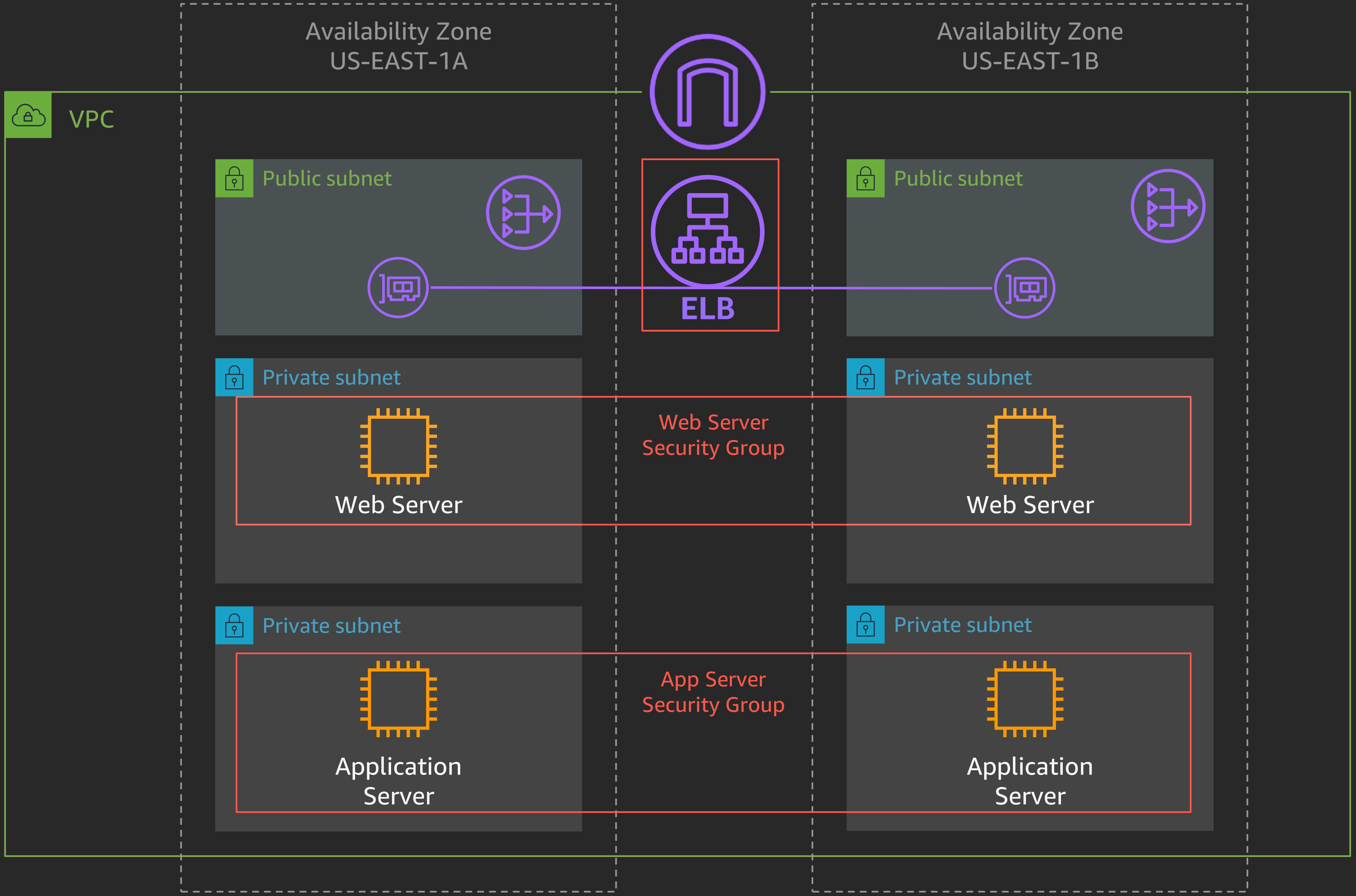
This rule cannot be moved or deleted

IF	THEN
✓ Requests otherwise not routed	Forward to reInventEC2

Example web application

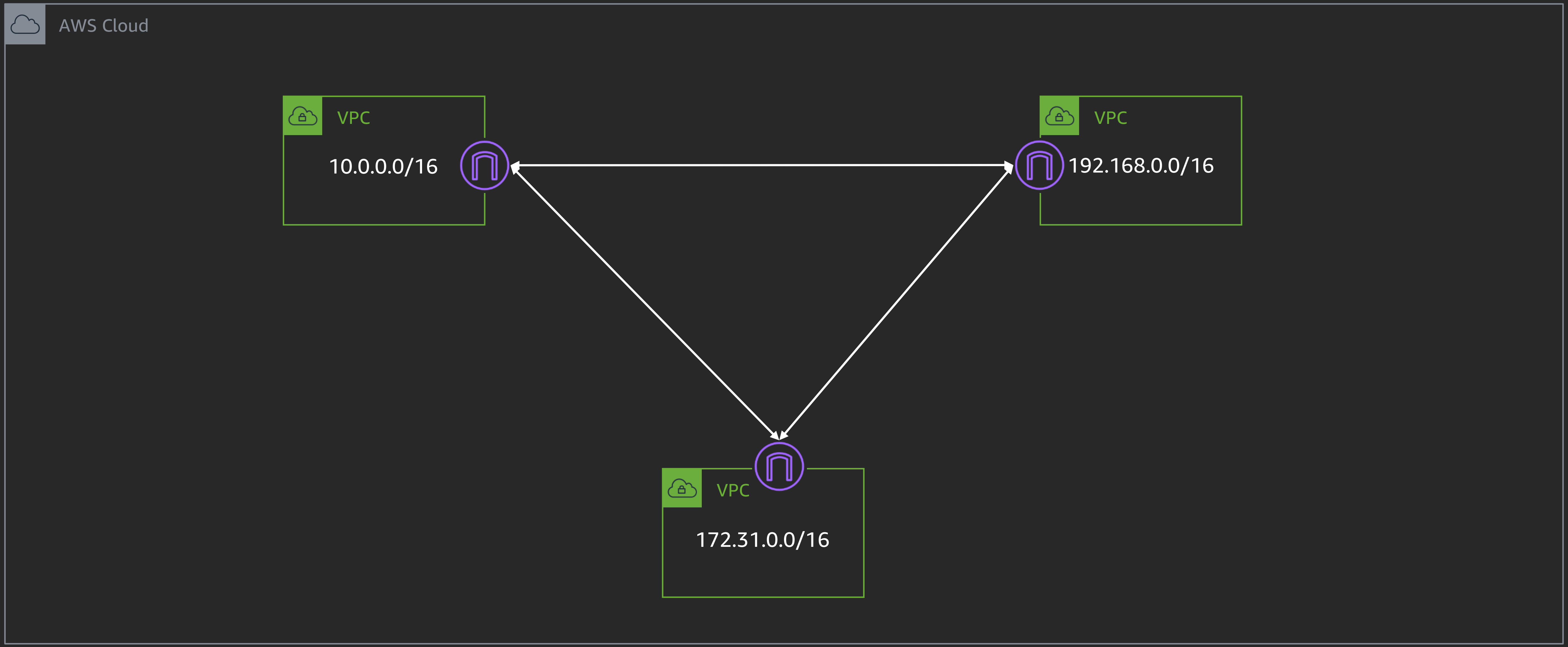


Example web application – Final

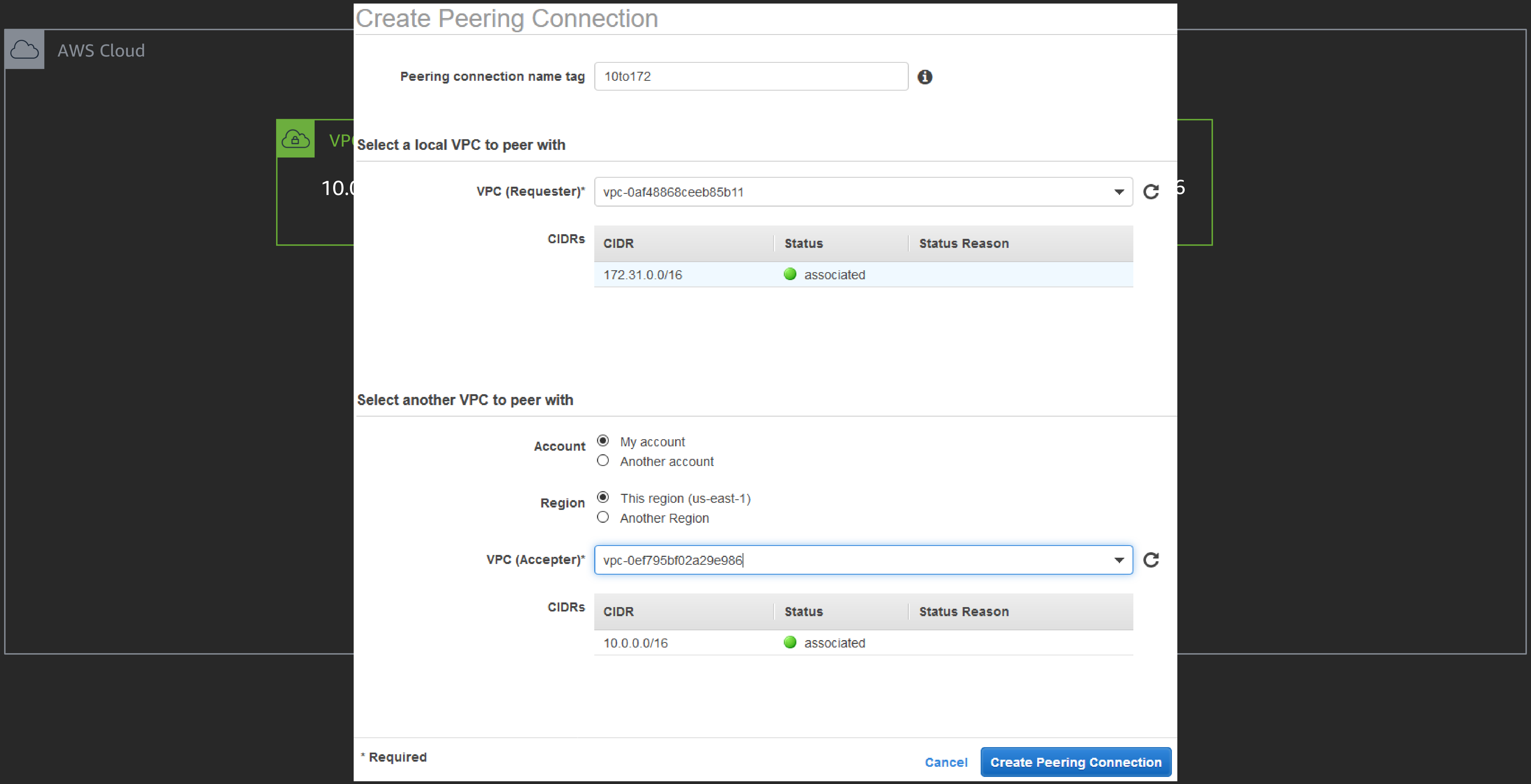


Connecting to other VPCs

Connecting between VPCs



VPC peering – same region



Create Peering Connection

Peering connection name tag: 10to172

Select a local VPC to peer with

VPC (Requester)*: vpc-0af48868ceeb85b11

CIDRs

CIDR	Status	Status Reason
172.31.0.0/16	● associated	

Select another VPC to peer with

Account: ● My account ○ Another account

Region: ● This region (us-east-1) ○ Another Region

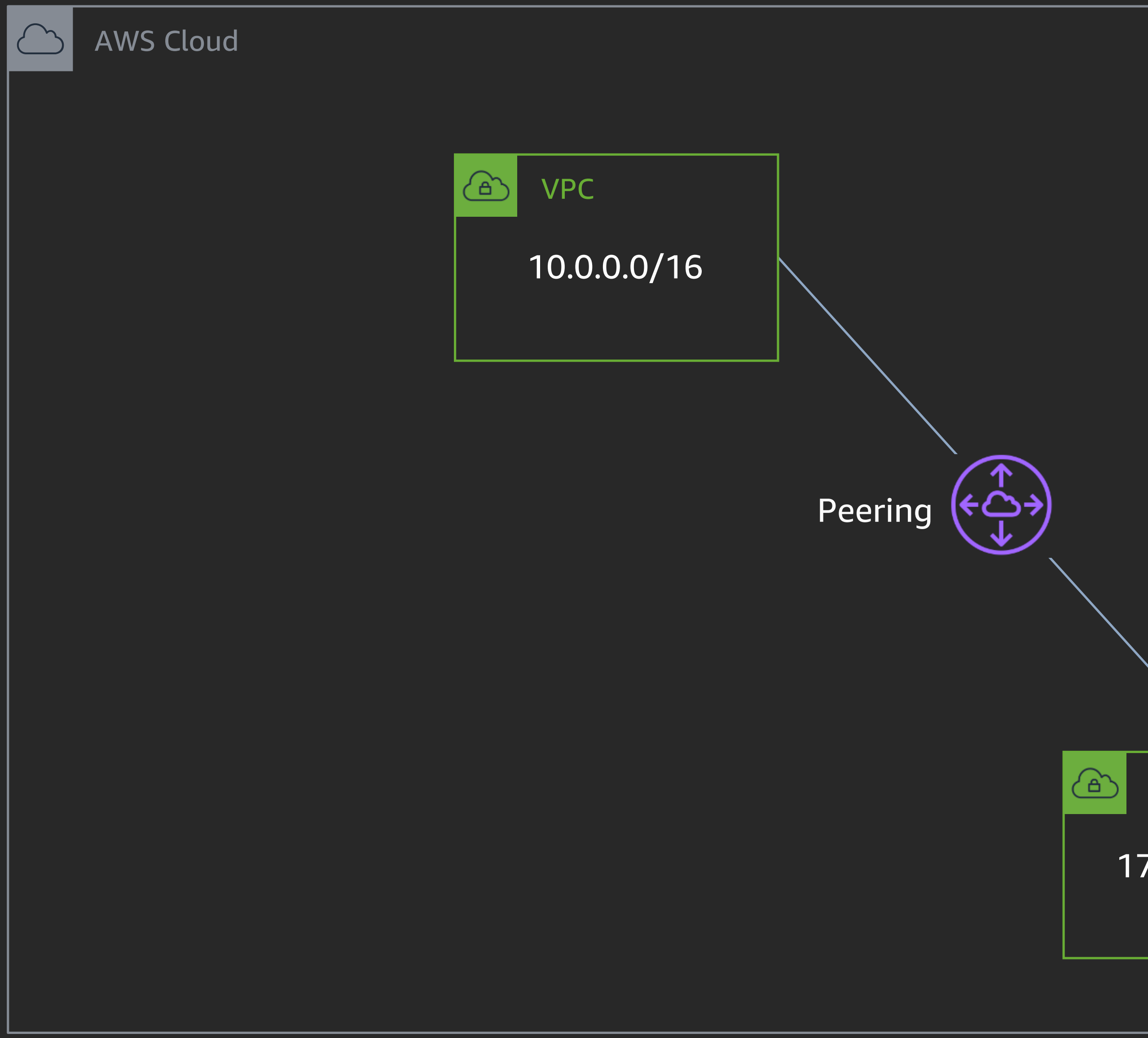
VPC (Accepter)*: vpc-0ef795bf02a29e986

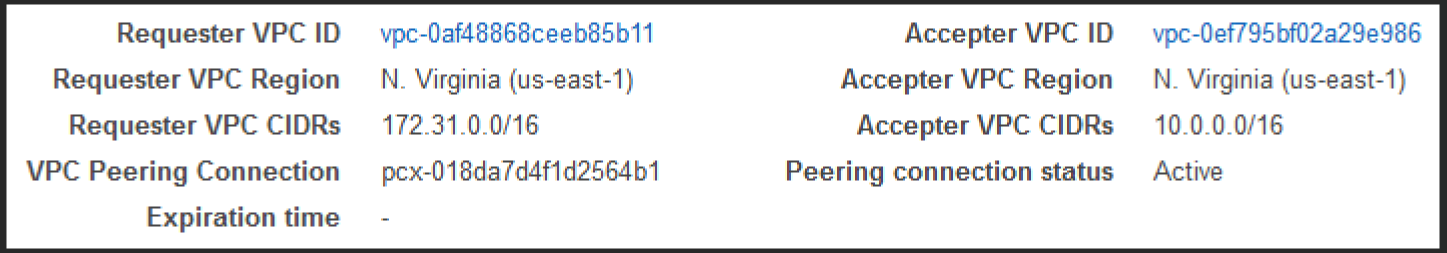
CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	● associated	

* Required

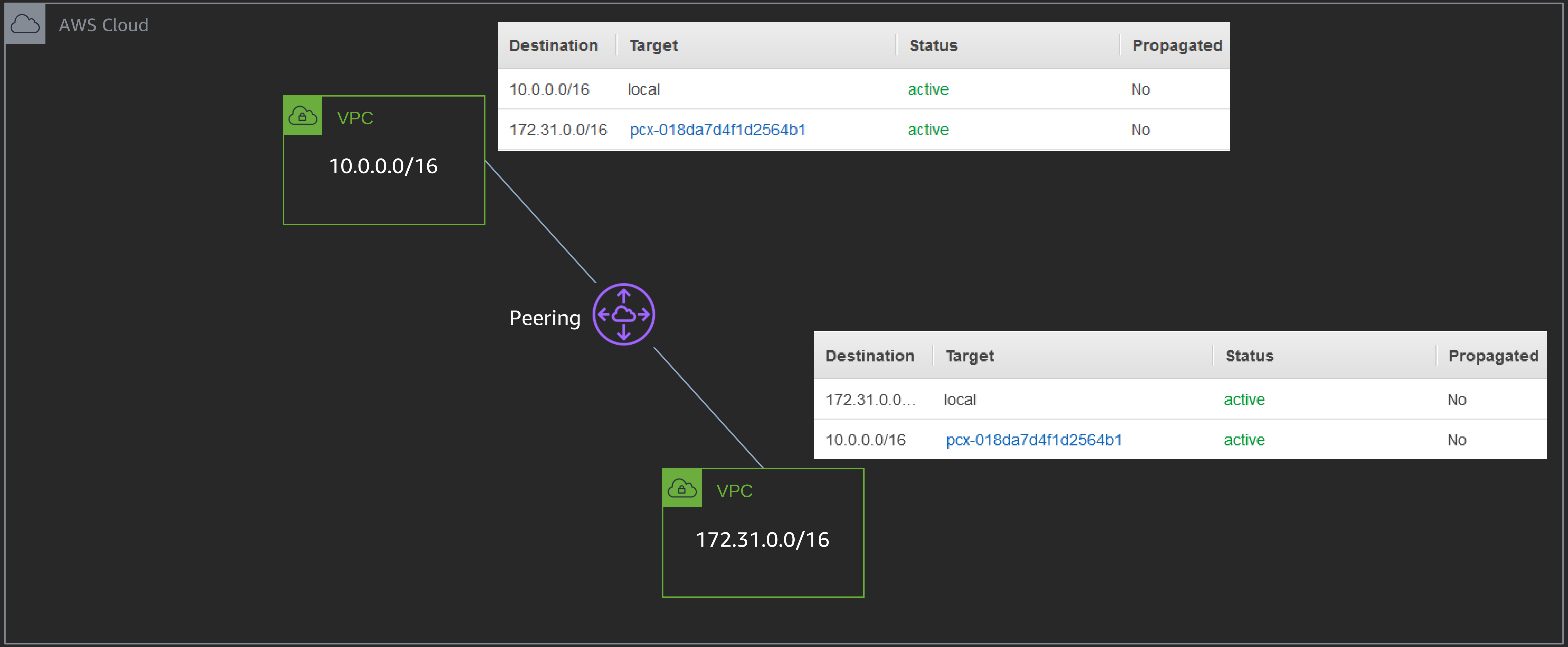
VPC peering – same region





Requester VPC ID	vpc-0af48868ceeb85b11	Accepter VPC ID	vpc-0ef795bf02a29e986
Requester VPC Region	N. Virginia (us-east-1)	Accepter VPC Region	N. Virginia (us-east-1)
Requester VPC CIDRs	172.31.0.0/16	Accepter VPC CIDRs	10.0.0.0/16
VPC Peering Connection	pcx-018da7d4f1d2564b1	Peering connection status	Active
Expiration time	-		

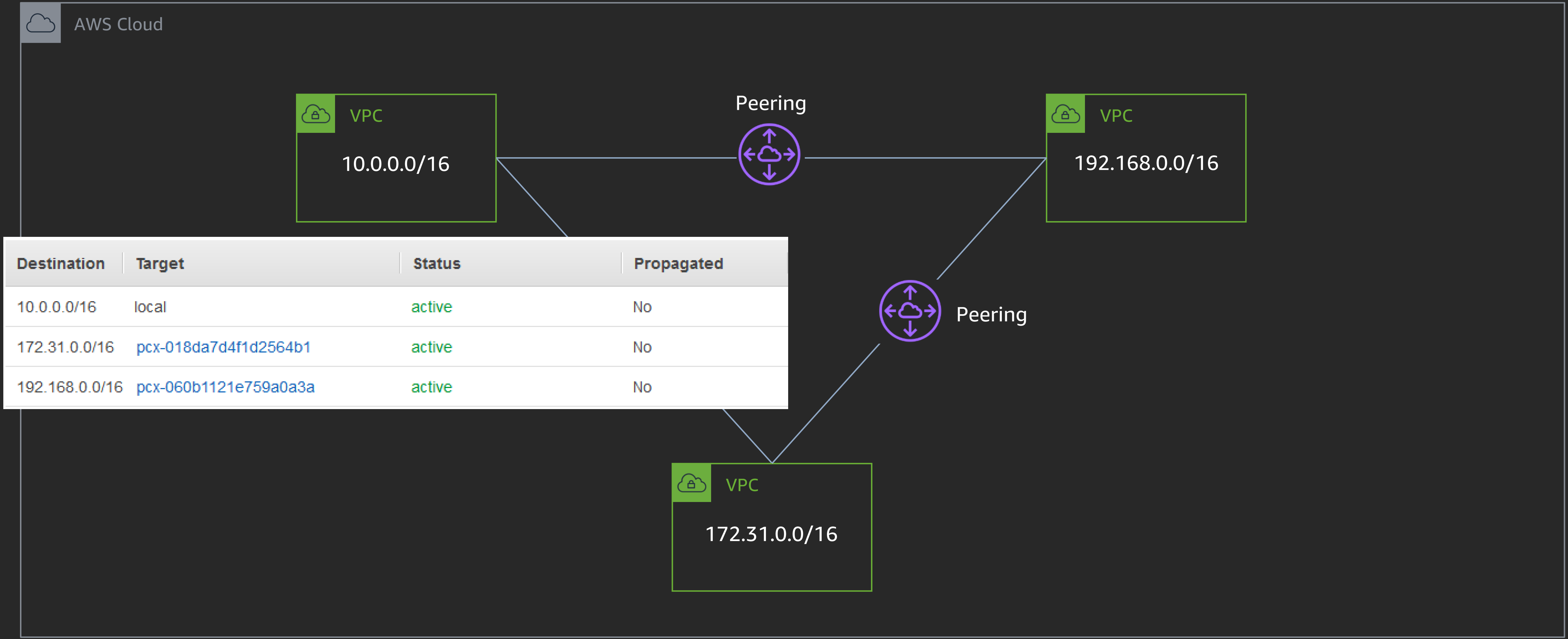
VPC peering – same region



Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
172.31.0.0/16	pcx-018da7d4f1d2564b1	active	No

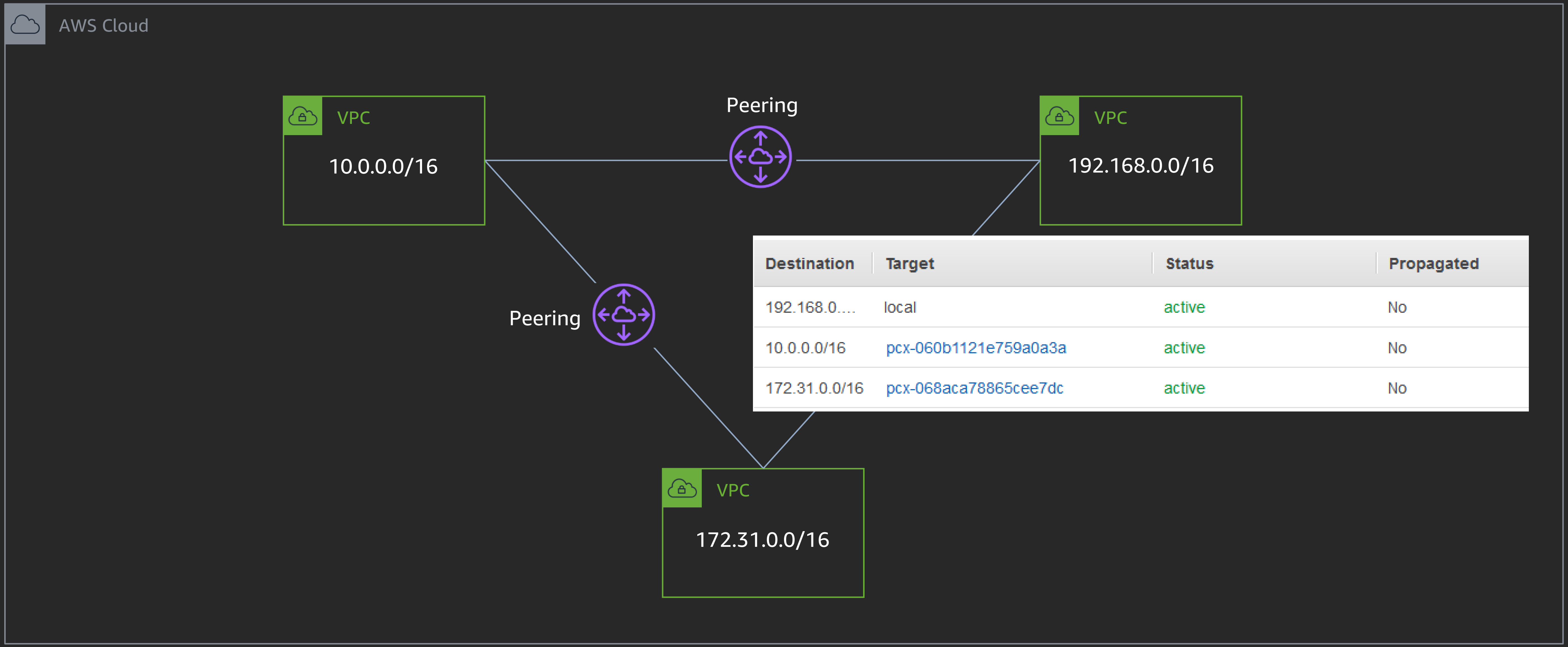
Destination	Target	Status	Propagated
172.31.0.0...	local	active	No
10.0.0.0/16	pcx-018da7d4f1d2564b1	active	No

VPC peering – same region



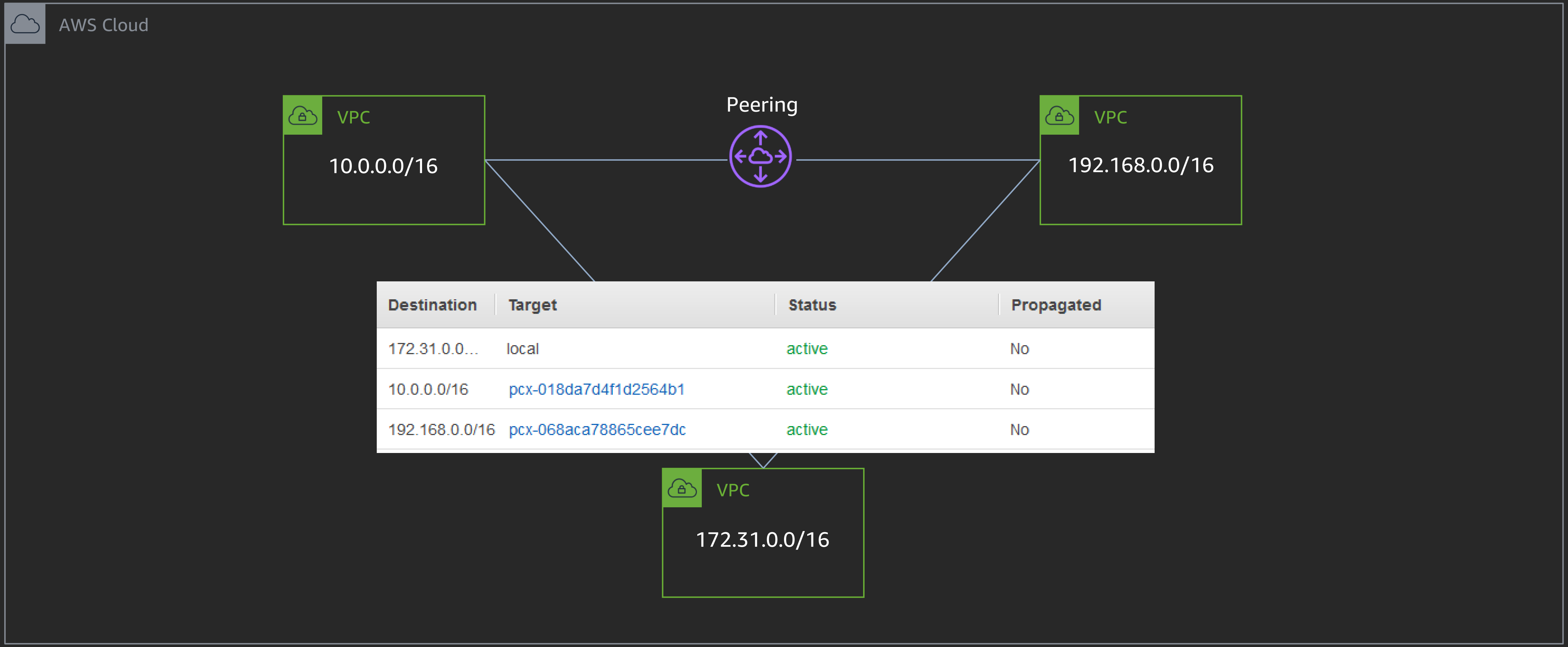
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
172.31.0.0/16	pcx-018da7d4f1d2564b1	active	No
192.168.0.0/16	pcx-060b1121e759a0a3a	active	No

VPC peering – same region



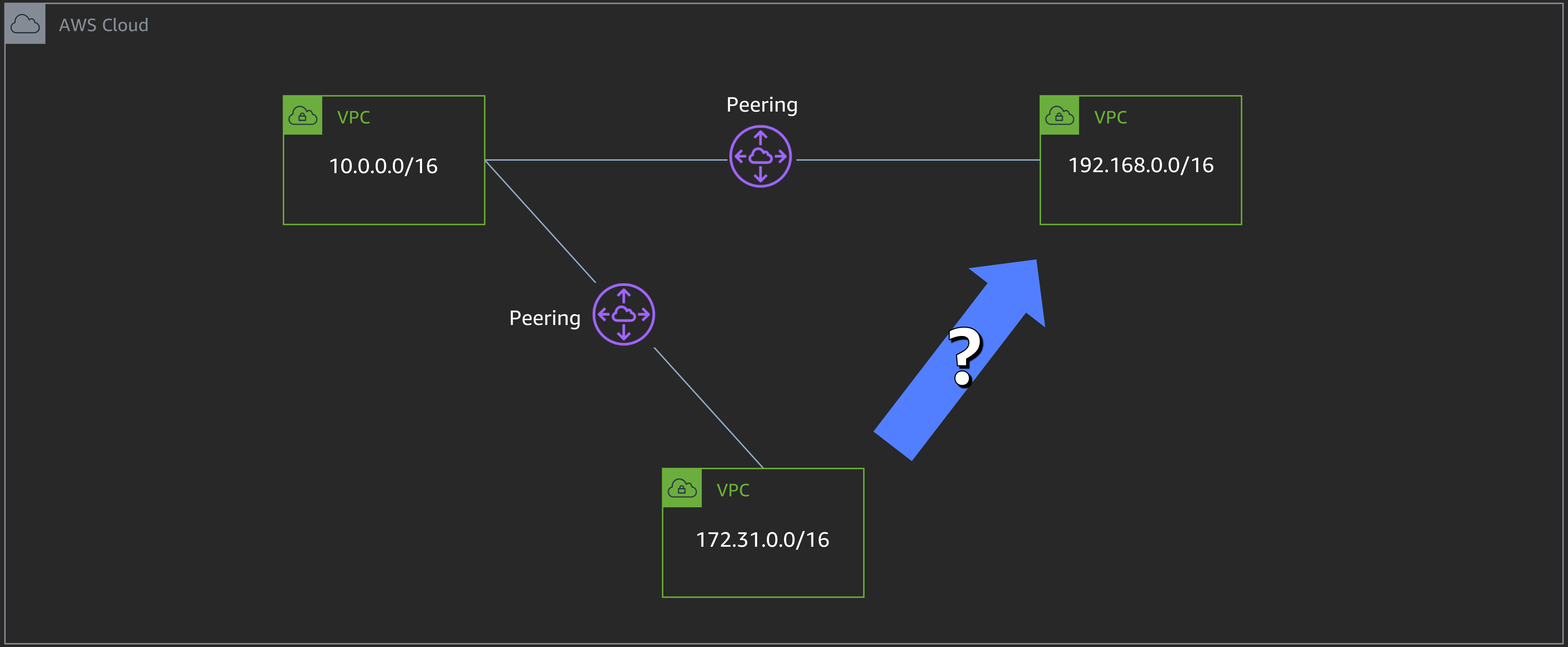
Destination	Target	Status	Propagated
192.168.0....	local	active	No
10.0.0.0/16	pcx-060b1121e759a0a3a	active	No
172.31.0.0/16	pcx-068aca78865cee7dc	active	No

VPC peering – same region

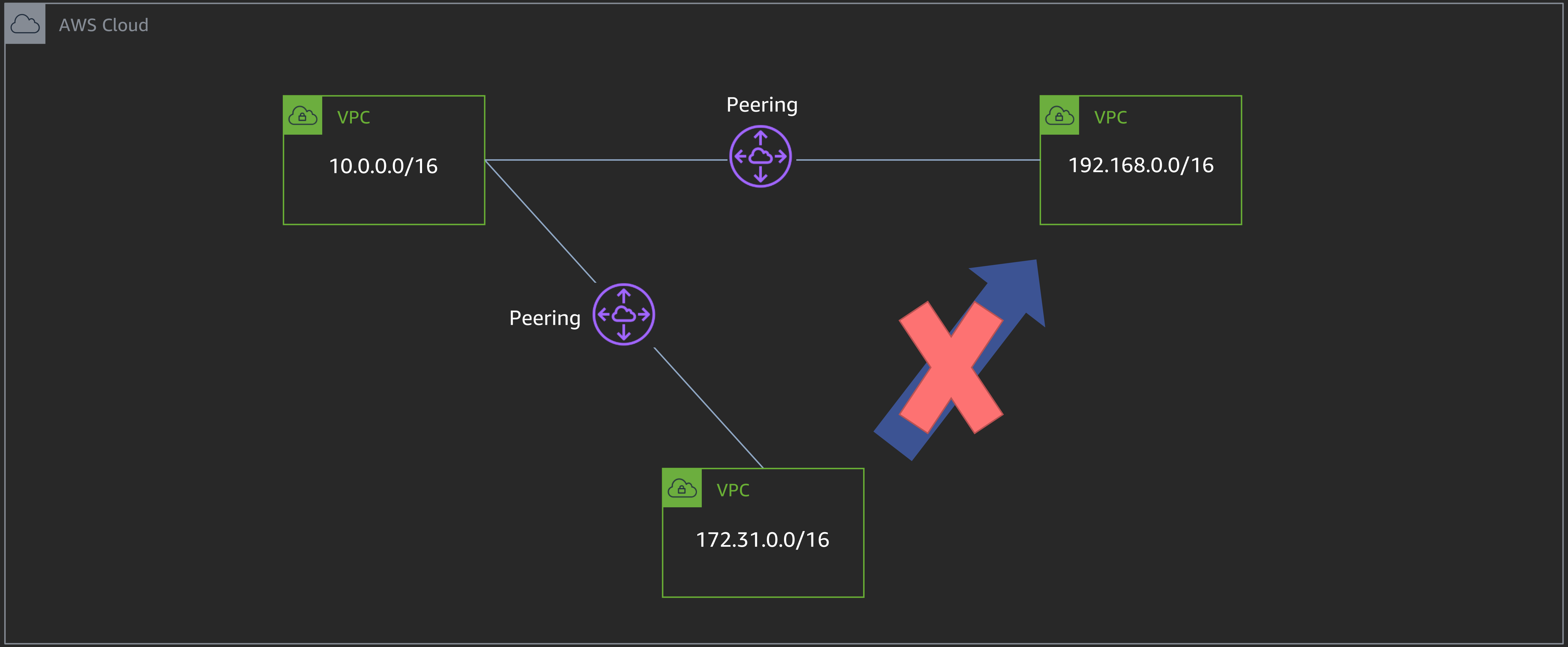


Destination	Target	Status	Propagated
172.31.0.0...	local	active	No
10.0.0.0/16	pcx-018da7d4f1d2564b1	active	No
192.168.0.0/16	pcx-068aca78865cee7dc	active	No

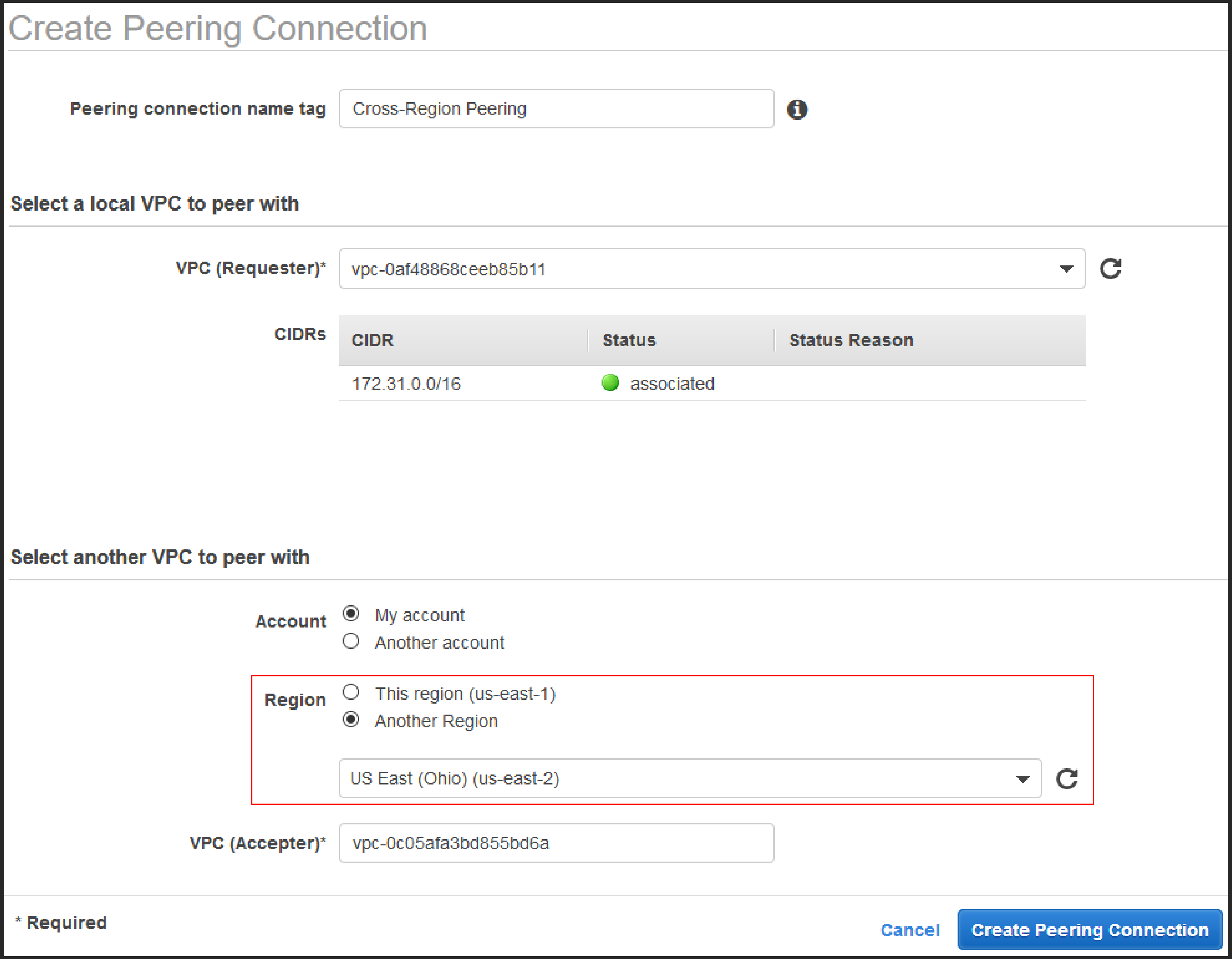
VPC peering – same region



VPC peering – same region



VPC peering – different region



Create Peering Connection

Peering connection name tag: Cross-Region Peering

Select a local VPC to peer with

VPC (Requester)*: vpc-0af48868ceeb85b11

CIDRs

CIDR	Status	Status Reason
172.31.0.0/16	● associated	

Select another VPC to peer with

Account: ● My account ○ Another account

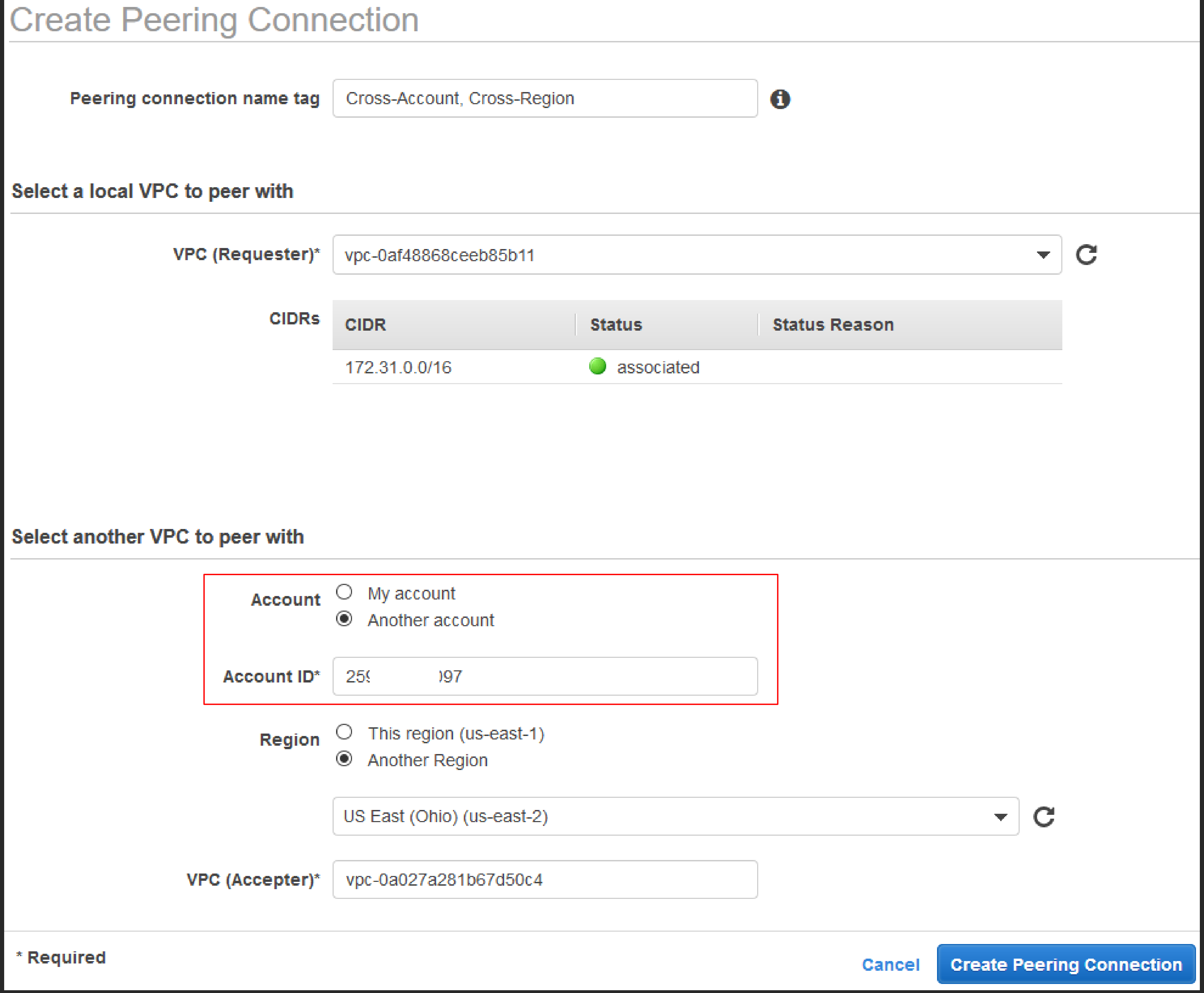
Region: ○ This region (us-east-1) ● Another Region

US East (Ohio) (us-east-2)

VPC (Accepter)*: vpc-0c05afa3bd855bd6a

* Required

VPC peering – different account



Create Peering Connection

Peering connection name tag: Cross-Account, Cross-Region

Select a local VPC to peer with

VPC (Requester)*: vpc-0af48868ceeb85b11

CIDRs

CIDR	Status	Status Reason
172.31.0.0/16	● associated	

Select another VPC to peer with

Account: ○ My account ● Another account

Account ID*: 25[redacted]97

Region: ○ This region (us-east-1) ● Another Region

US East (Ohio) (us-east-2)

VPC (Accepter)*: vpc-0a027a281b67d50c4

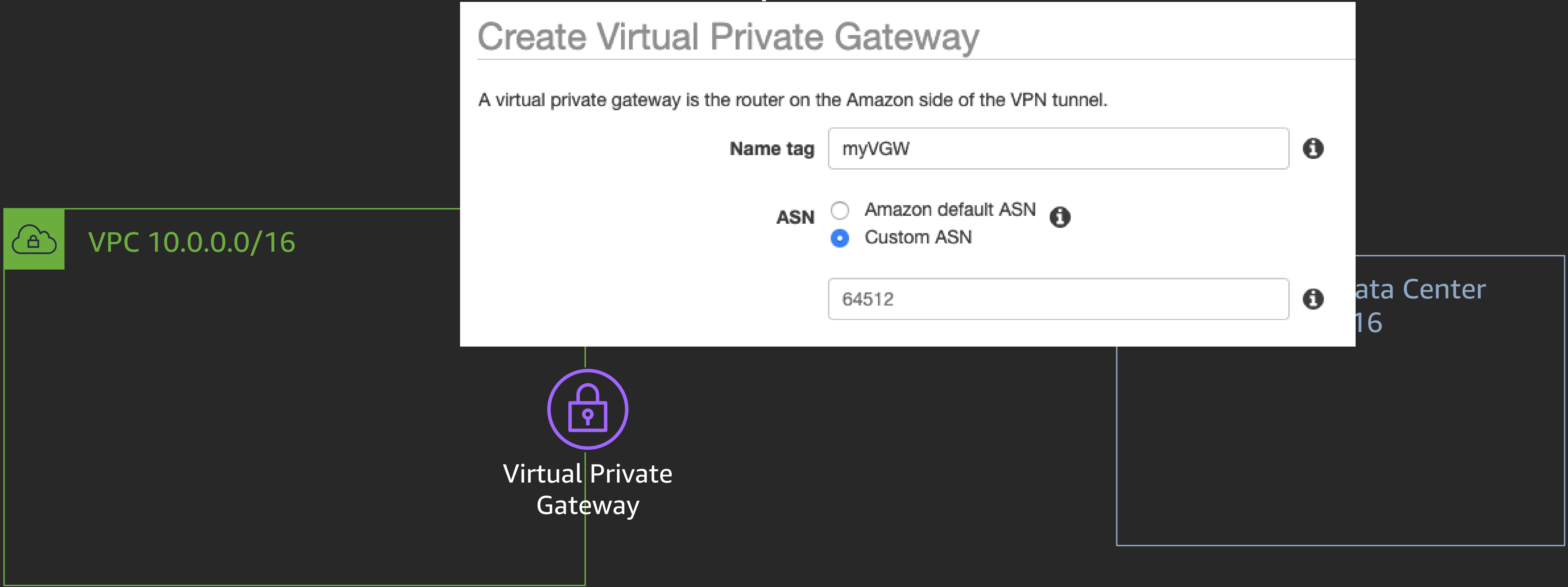
* Required

VPC peering – things to know

- Can reference security groups from the peer VPC in the same region
- Can enable DNS hostname resolution to return private IP addresses
- Can peer for both IPv4 & IPv6 addresses
- Cannot have overlapping IP addresses
- Cannot have multiple peers between the same pair of VPCs
- Cannot use jumbo frames across inter-region VPC peering

Connectivity to on-premises networks

AWS site-to-site VPN setup – VGW



Create Virtual Private Gateway

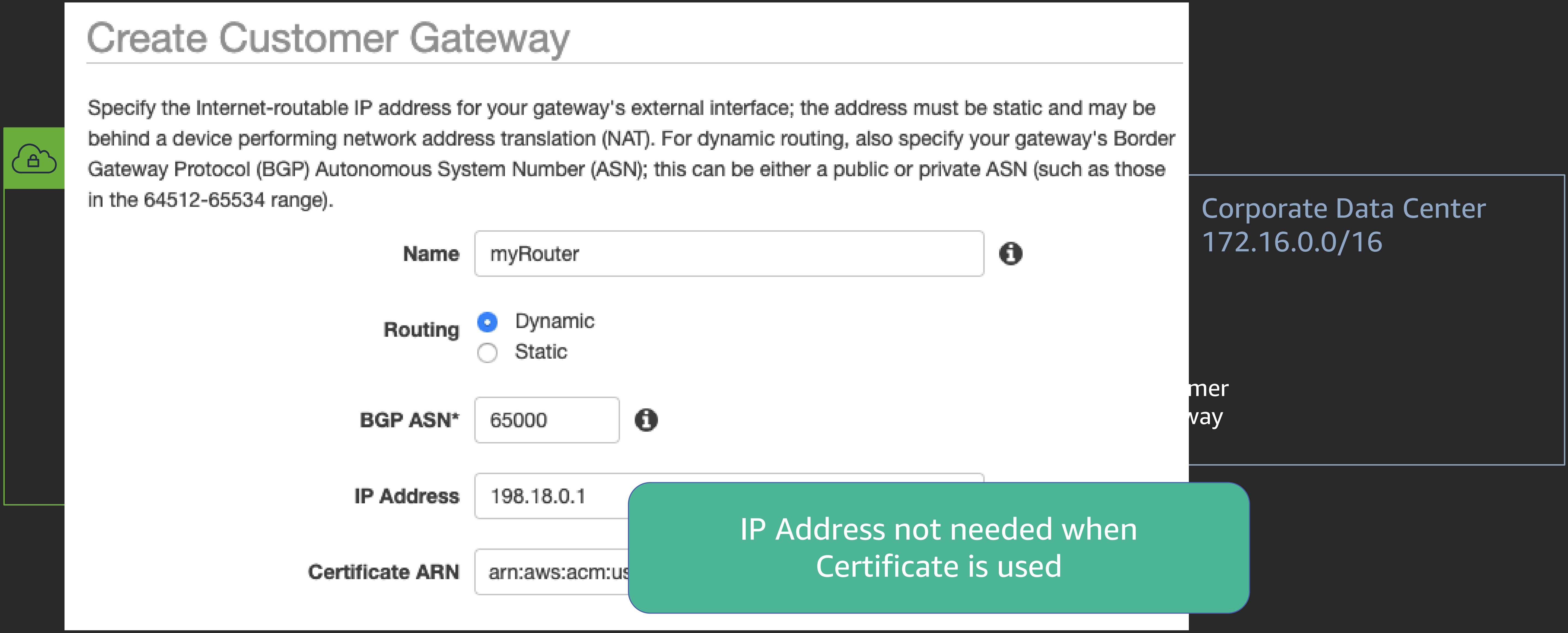
A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag myVGW

ASN ○ Amazon default ASN
● Custom ASN

64512

AWS site-to-site VPN – CGW



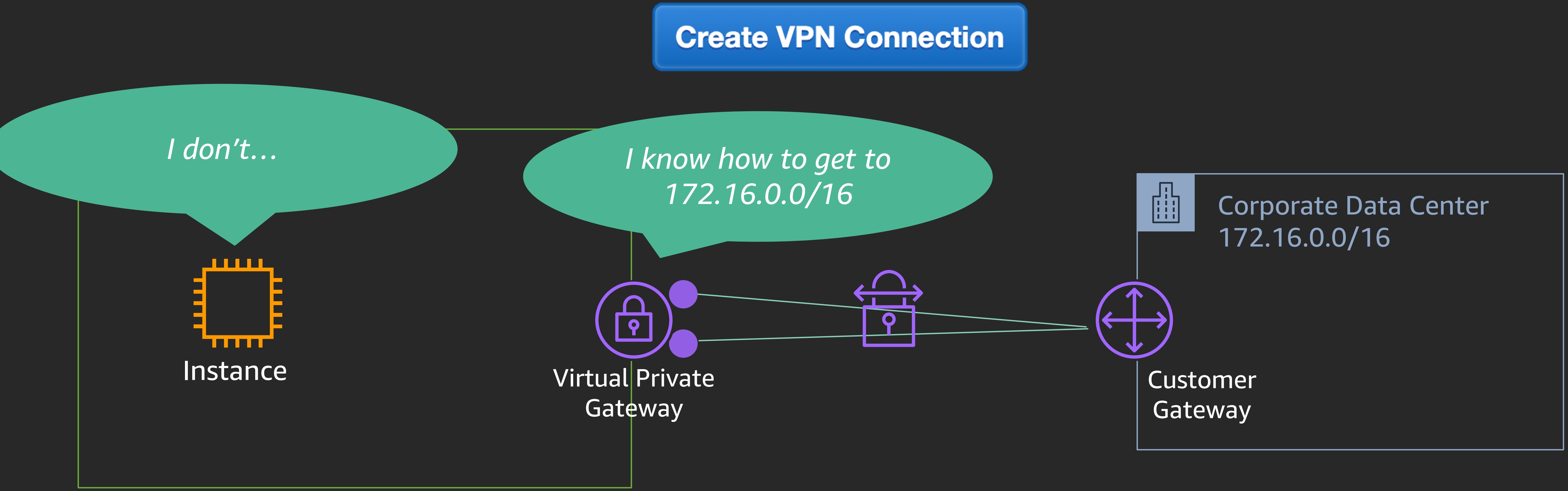
Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name	myRouter
Routing	● Dynamic ○ Static
BGP ASN*	65000
IP Address	198.18.0.1
Certificate ARN	arn:aws:acm:us

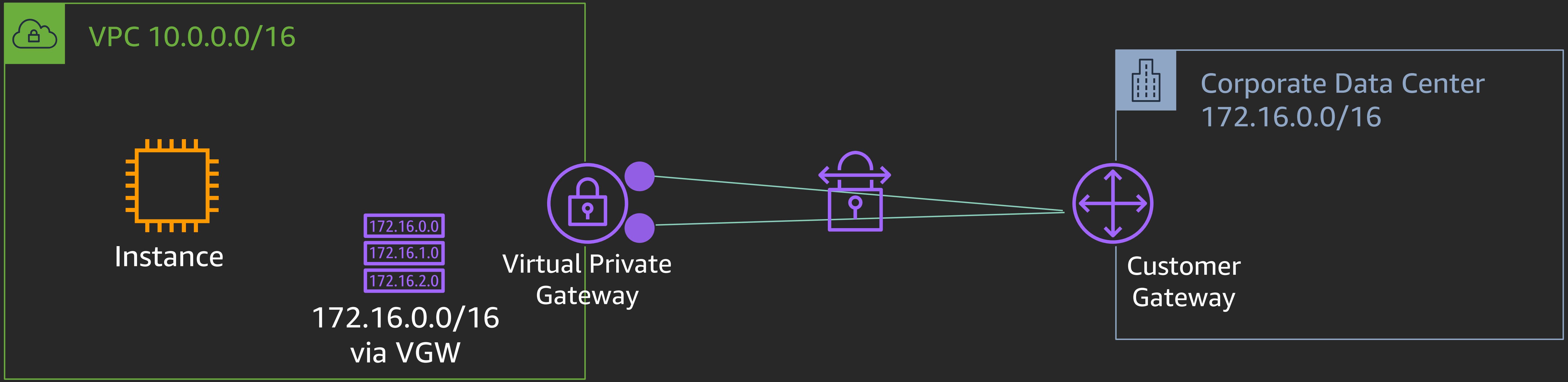
IP Address not needed when Certificate is used

AWS site-to-site VPN



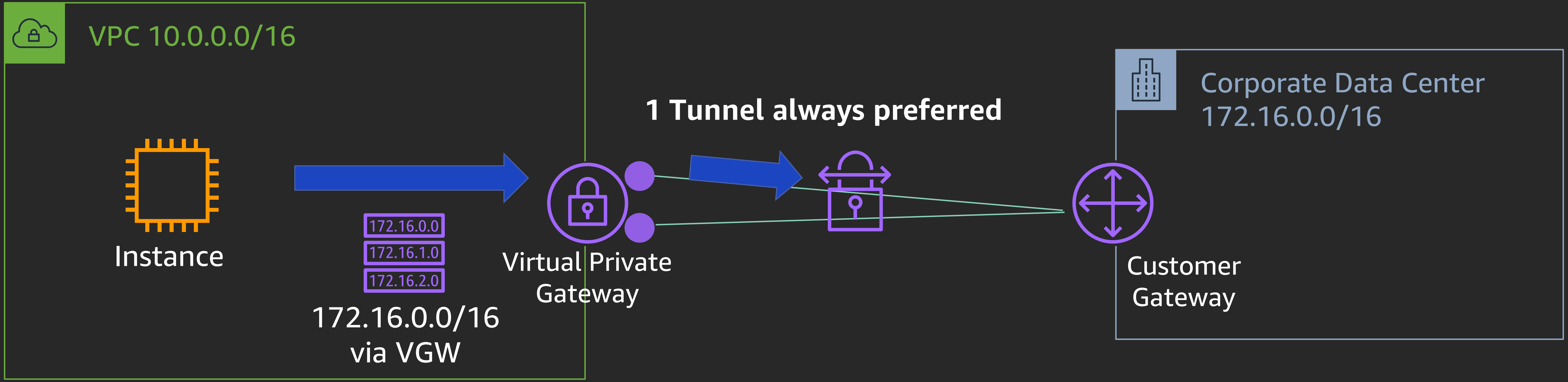
1x VPN Connection = 2x VPN Tunnels

AWS site-to-site VPN



1x VPN Connection = 2x VPN Tunnels

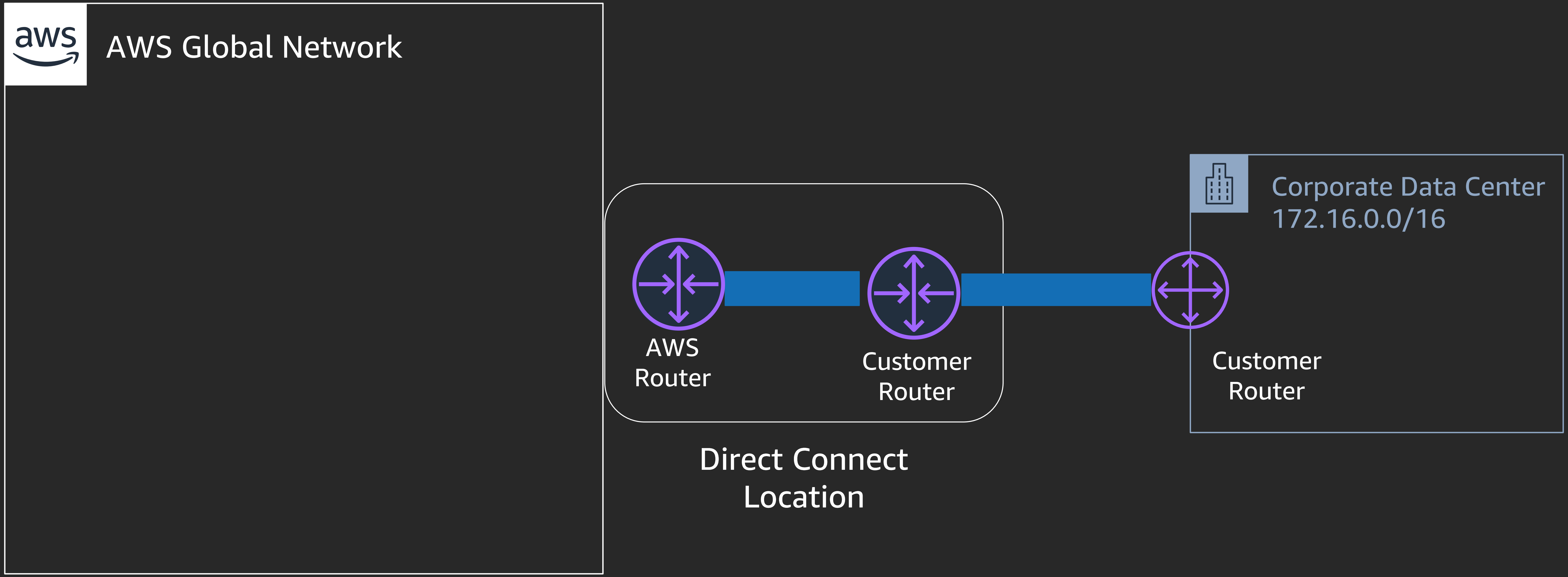
AWS site-to-site VPN



1x VPN Connection = 2x VPN Tunnels

1x VPN Tunnel = 1.25Gbps

AWS Direct Connect – physical connection

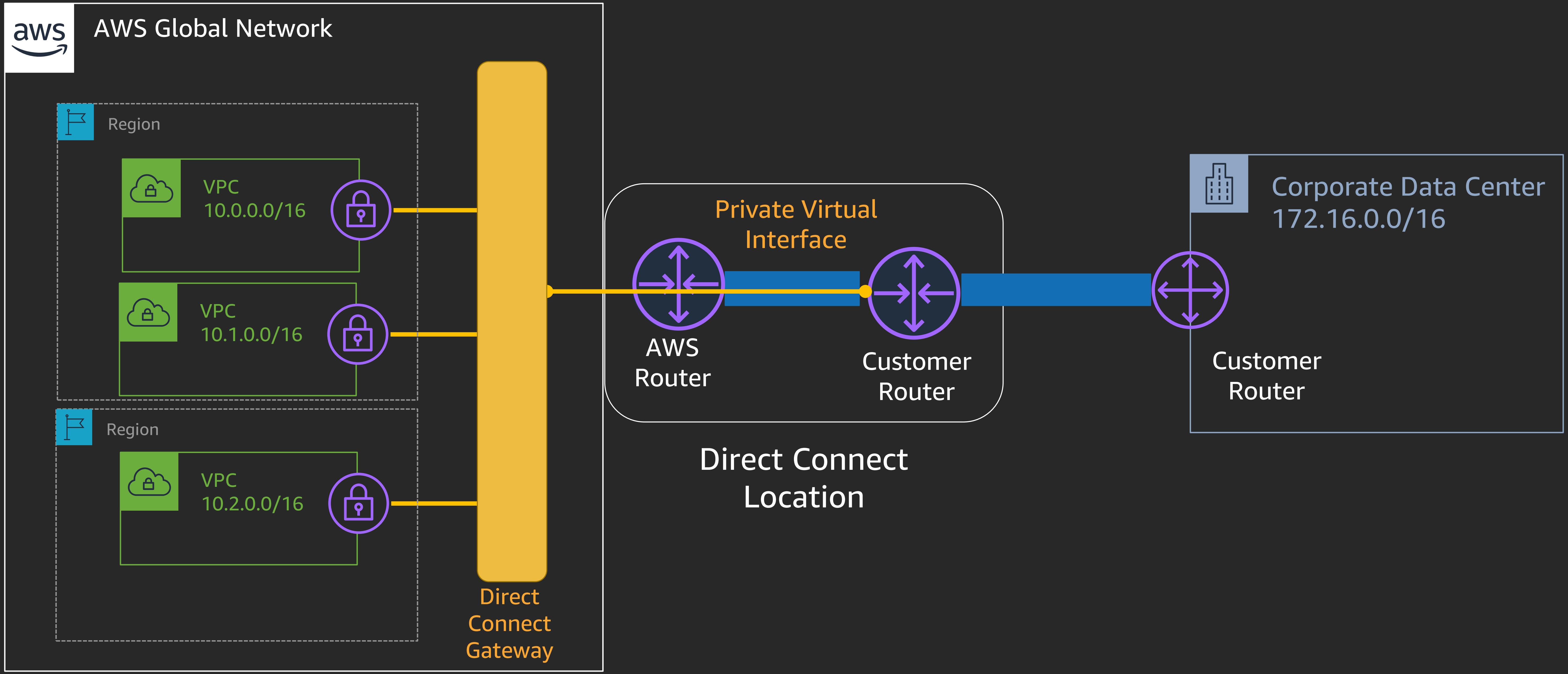


AWS Direct Connect – Interface types

- **Private VIF** – Used to connect to Amazon VPCs using private IP addresses; directly or via Direct Connect gateway
- **Transit VIF** – Used to connect to AWS Transit Gateways via Direct Connect gateway
- **Public VIF** – Used to access all AWS public services using public IP addresses

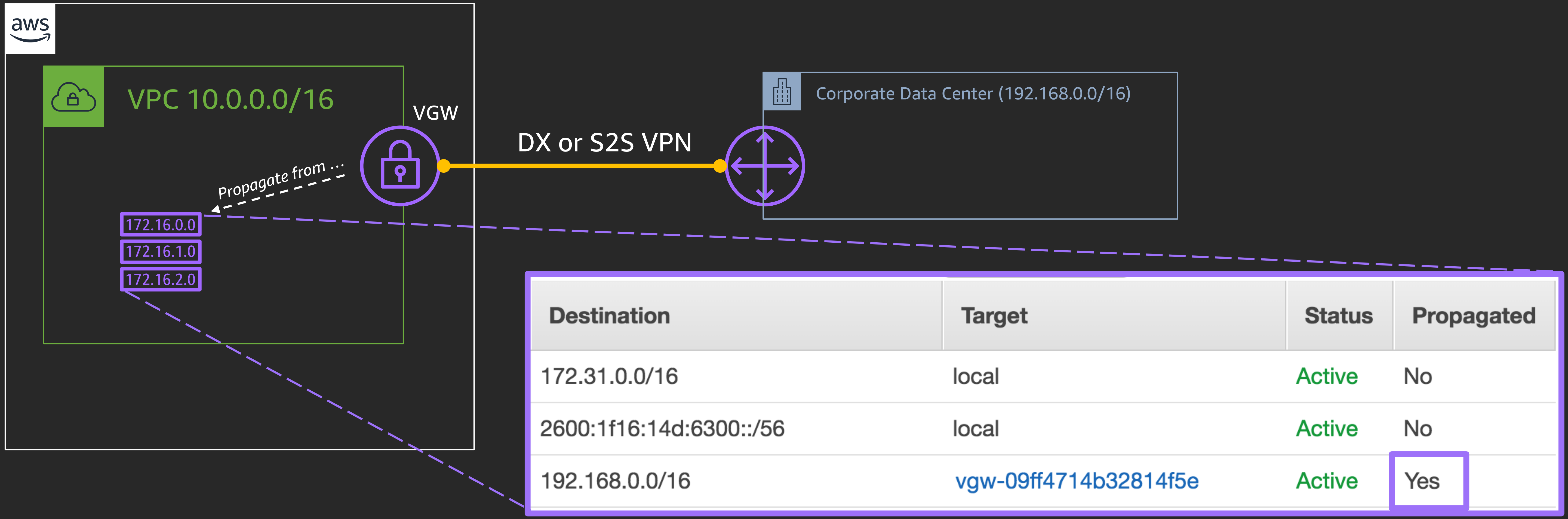
All Virtual Interfaces are 802.1Q VLANs with BGP peering

AWS Direct Connect gateway – Private VIF



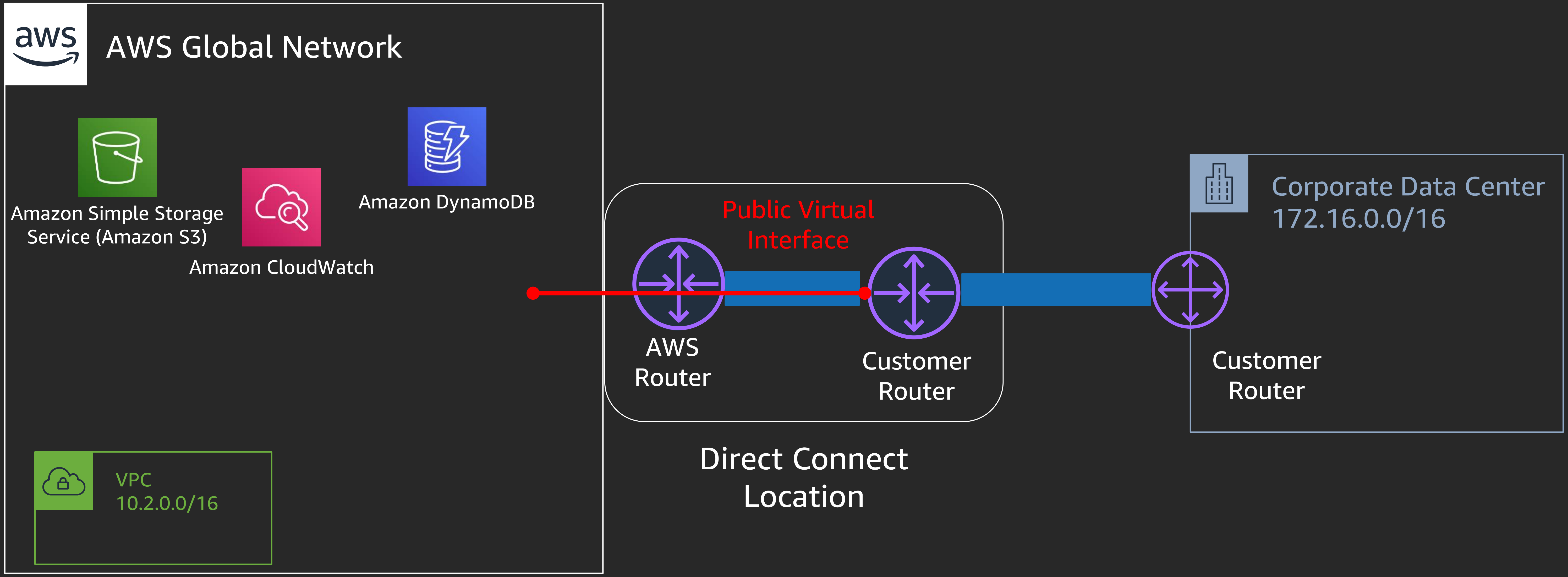
Route propagation

- Enable propagation on the Route Table
- Automatically populates with anything the VGW learns via BGP



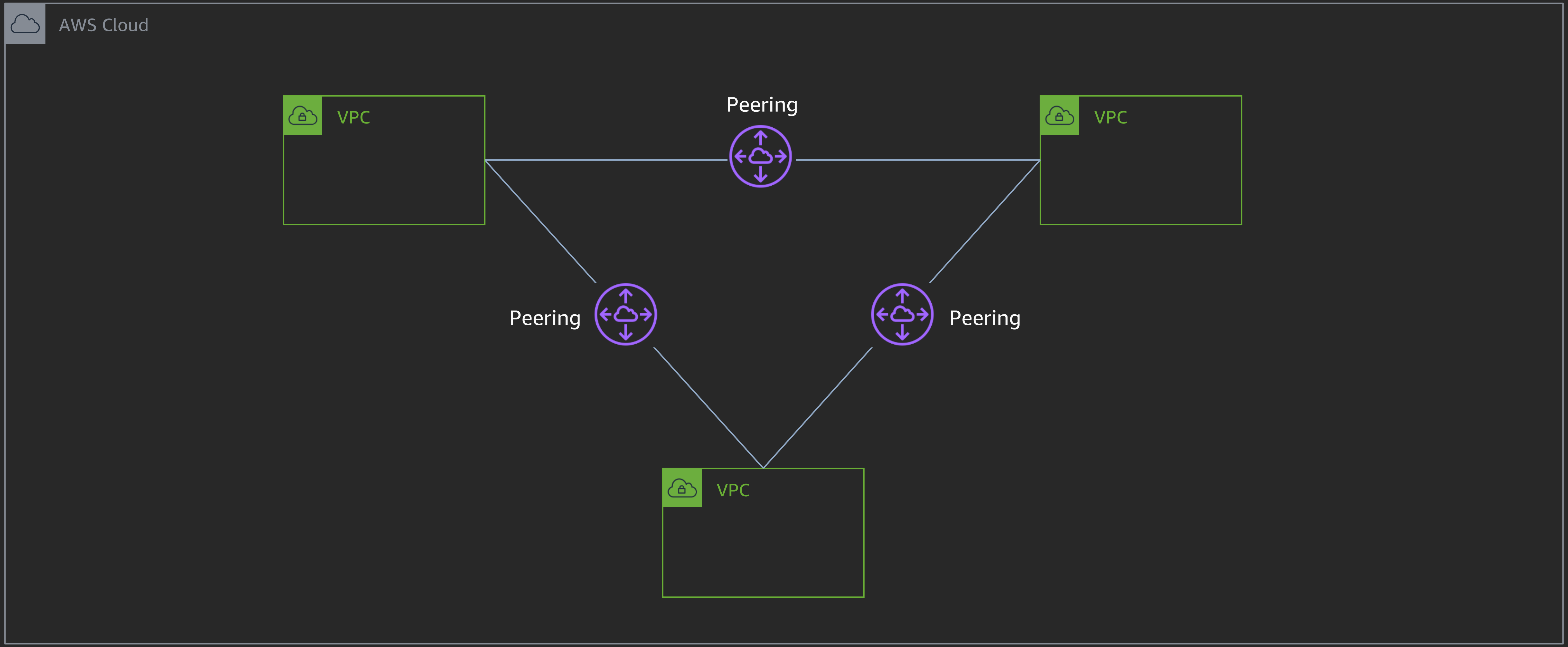
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
192.168.0.0/16	vgw-09ff4714b32814f5e	Active	Yes

AWS Direct Connect – Public VIF

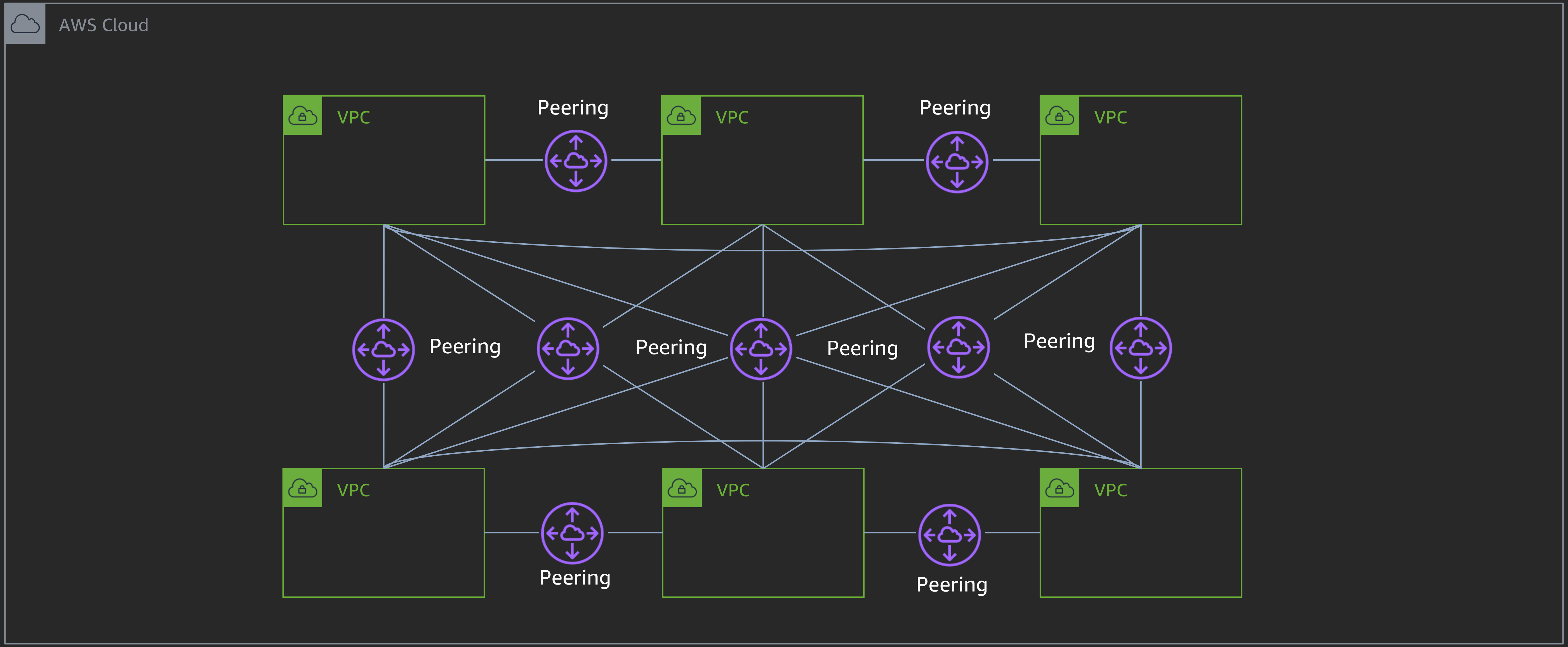


AWS Transit Gateway

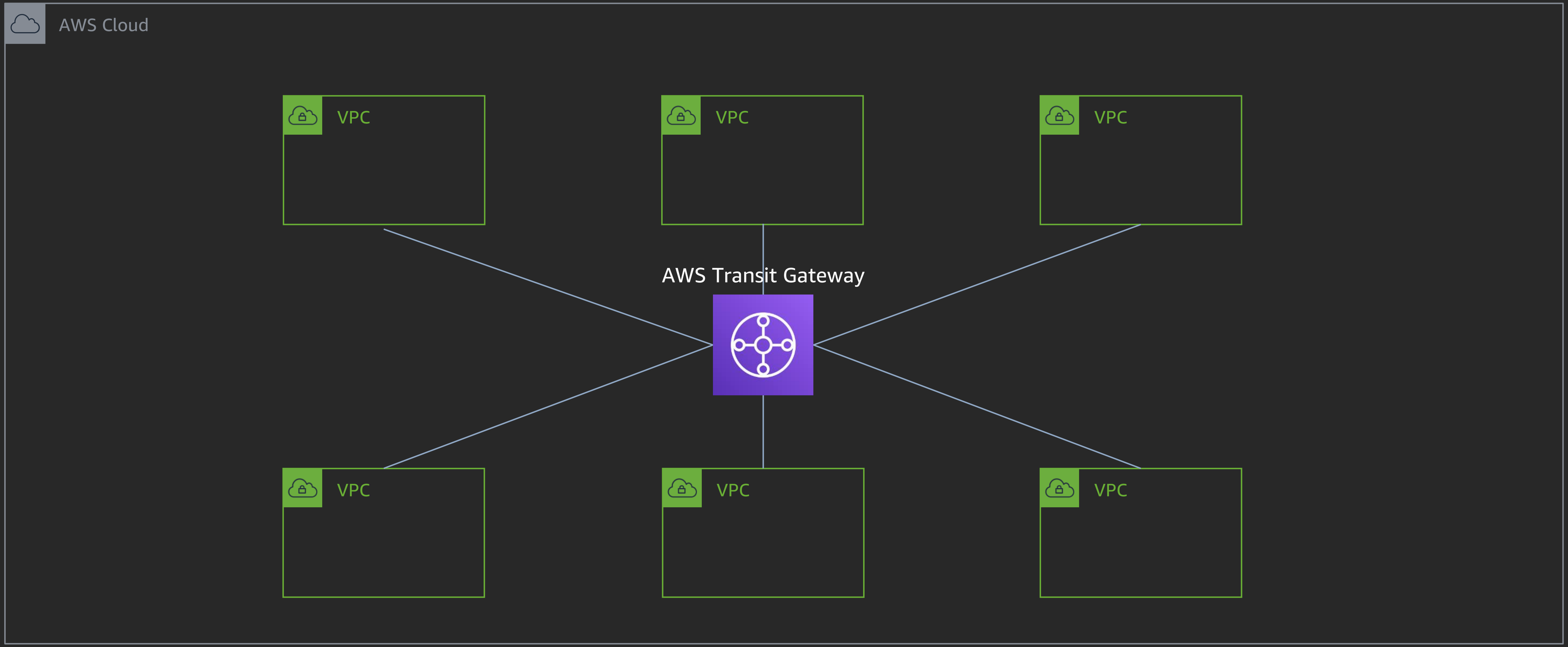
Interconnecting VPCs at scale – VPC peering



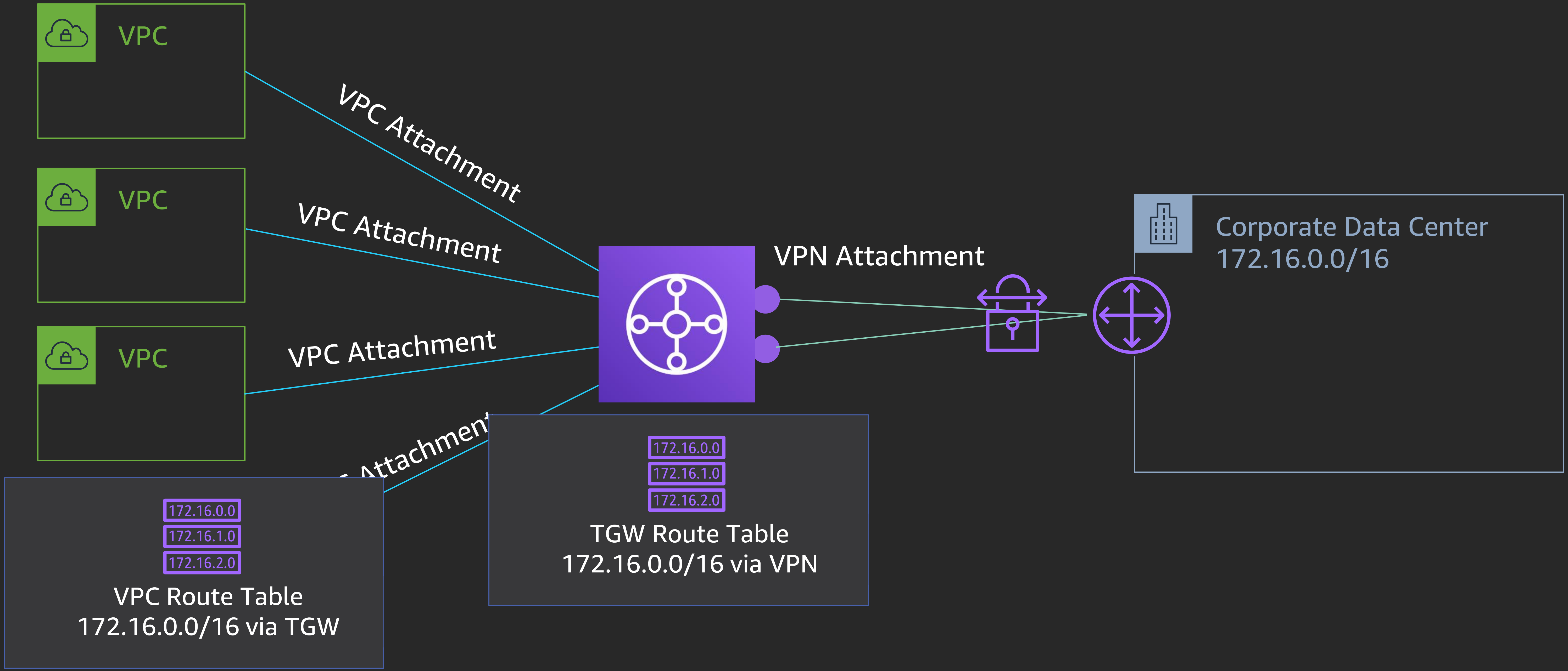
Interconnecting VPCs at scale – VPC peering



Multiple VPCs access models – AWS Transit Gateway



AWS Transit Gateway with AWS site-to-site VPN



VPC

VPC

VPC

VPC Attachment

VPC Attachment

VPC Attachment

Attachment

VPN Attachment

Corporate Data Center
172.16.0.0/16

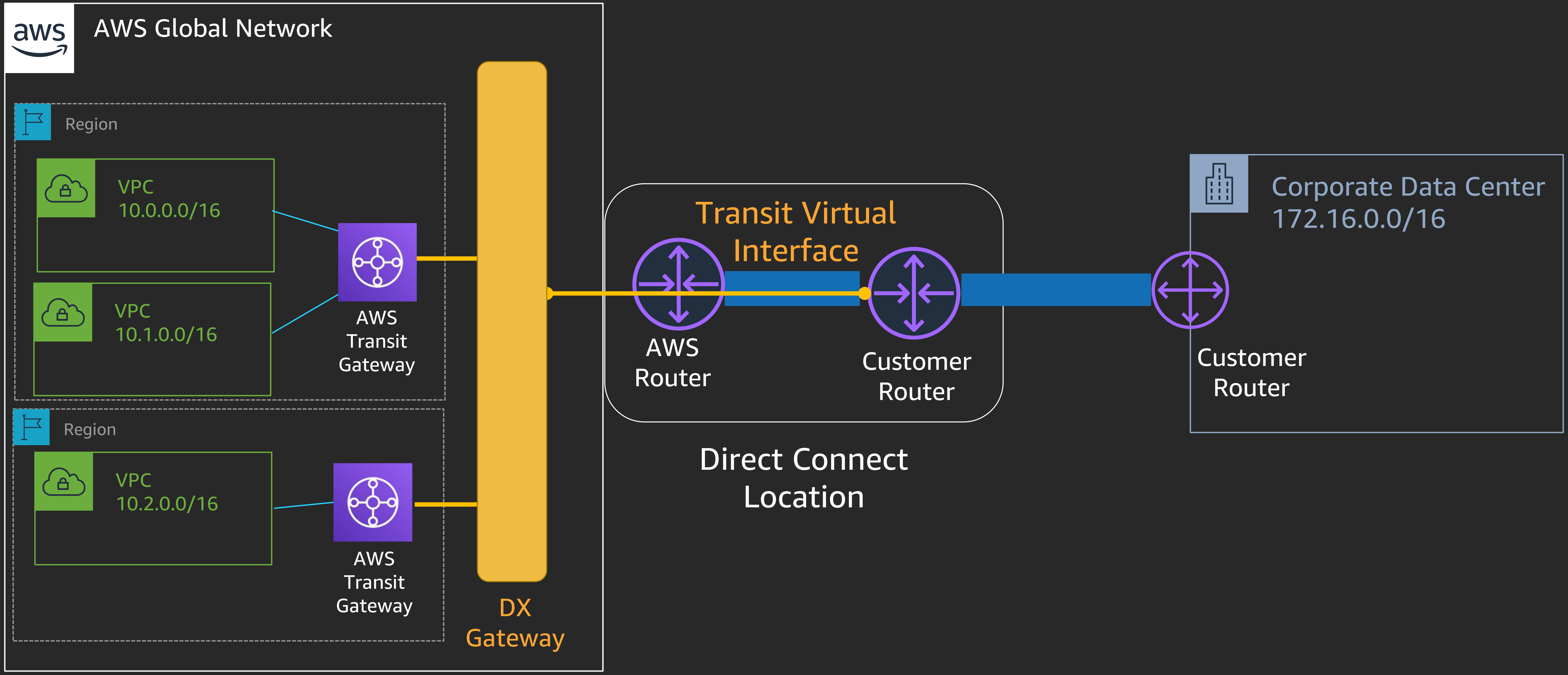
172.16.0.0
172.16.1.0
172.16.2.0

VPC Route Table
172.16.0.0/16 via TGW

172.16.0.0
172.16.1.0
172.16.2.0

TGW Route Table
172.16.0.0/16 via VPN

AWS Transit Gateway with DX gateway

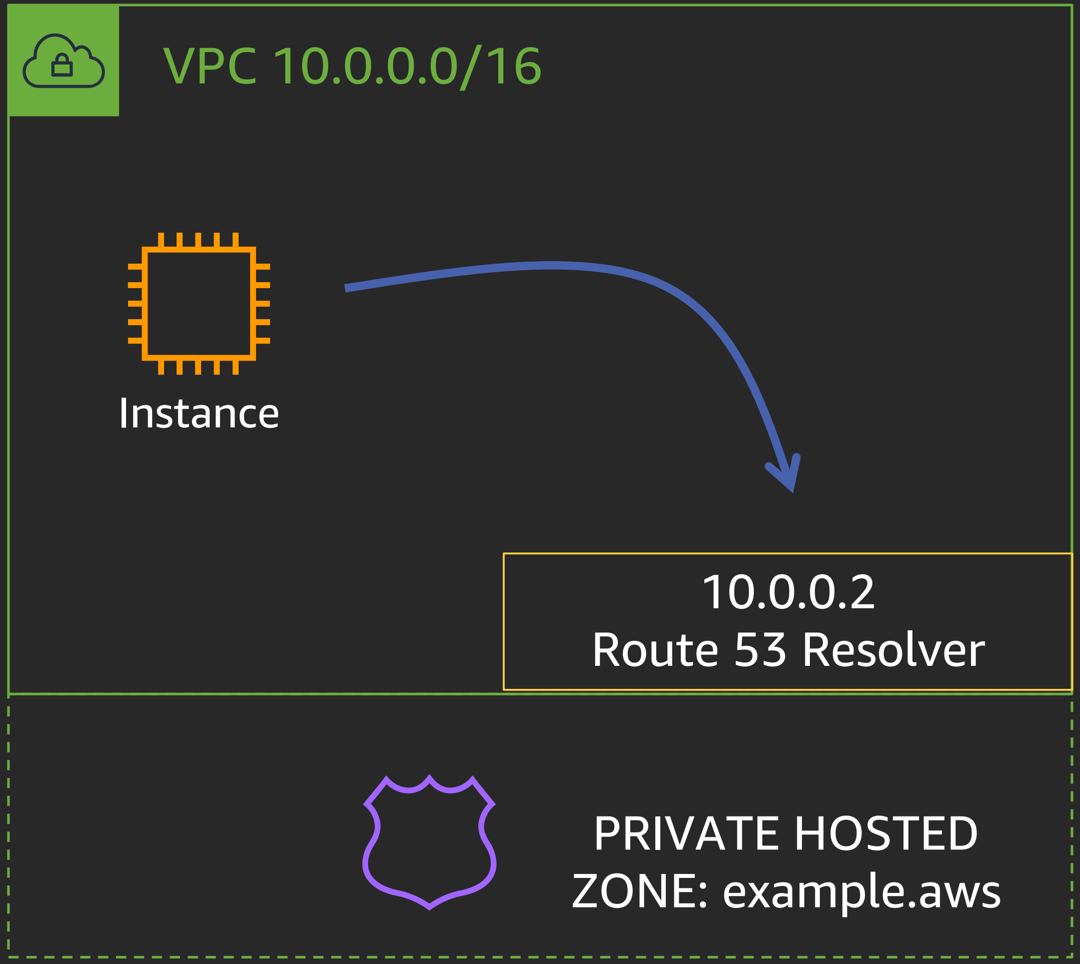


Name resolution (DNS)

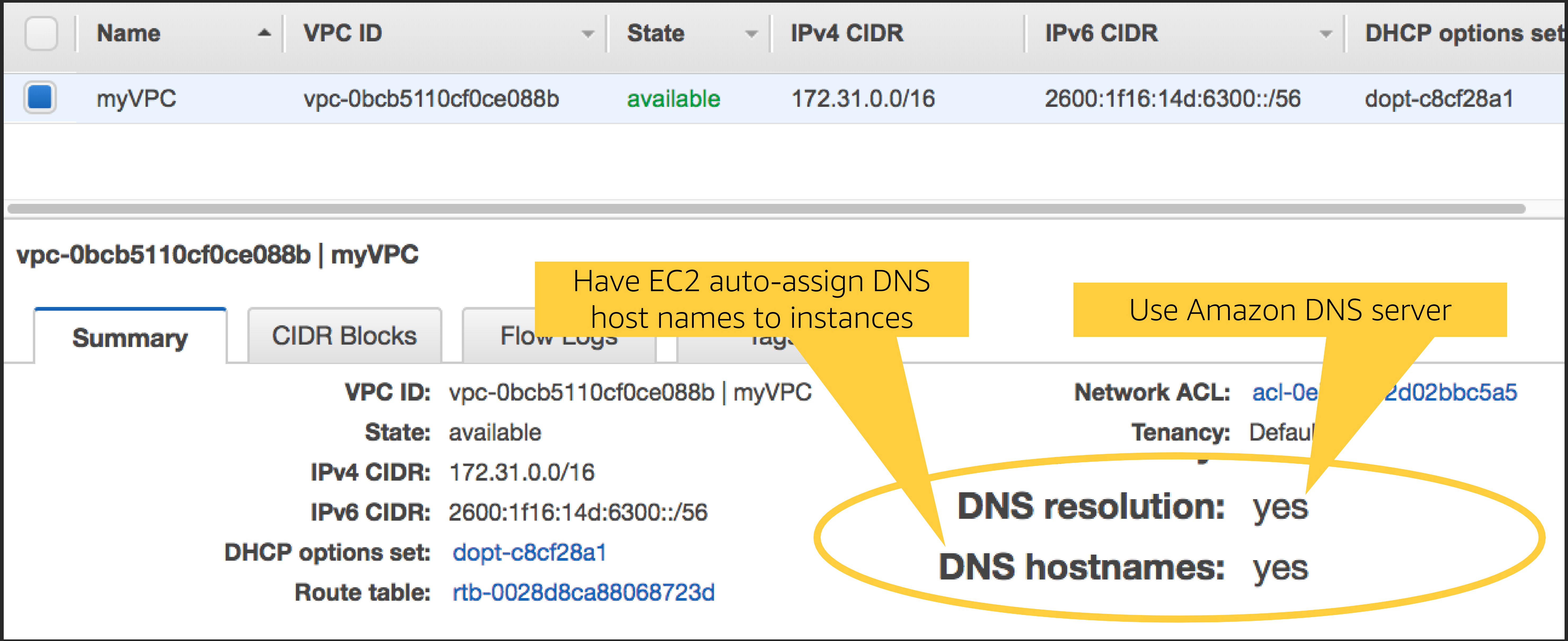
AWS re:Invent

Amazon Route 53 Resolver

- VPC+2 Resolver
- enableDnsHostnames
- enableDnsSupport
- Private Hosted Zones
- Inbound and Outbound Endpoints



VPC DNS options



□	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
■	myVPC	vpc-0bcb5110cf0ce088b	available	172.31.0.0/16	2600:1f16:14d:6300::/56	dopt-c8cf28a1

vpc-0bcb5110cf0ce088b | myVPC

VPC ID: vpc-0bcb5110cf0ce088b | myVPC
State: available
IPv4 CIDR: 172.31.0.0/16
IPv6 CIDR: 2600:1f16:14d:6300::/56
DHCP options set: dopt-c8cf28a1
Route table: rtb-0028d8ca88068723d

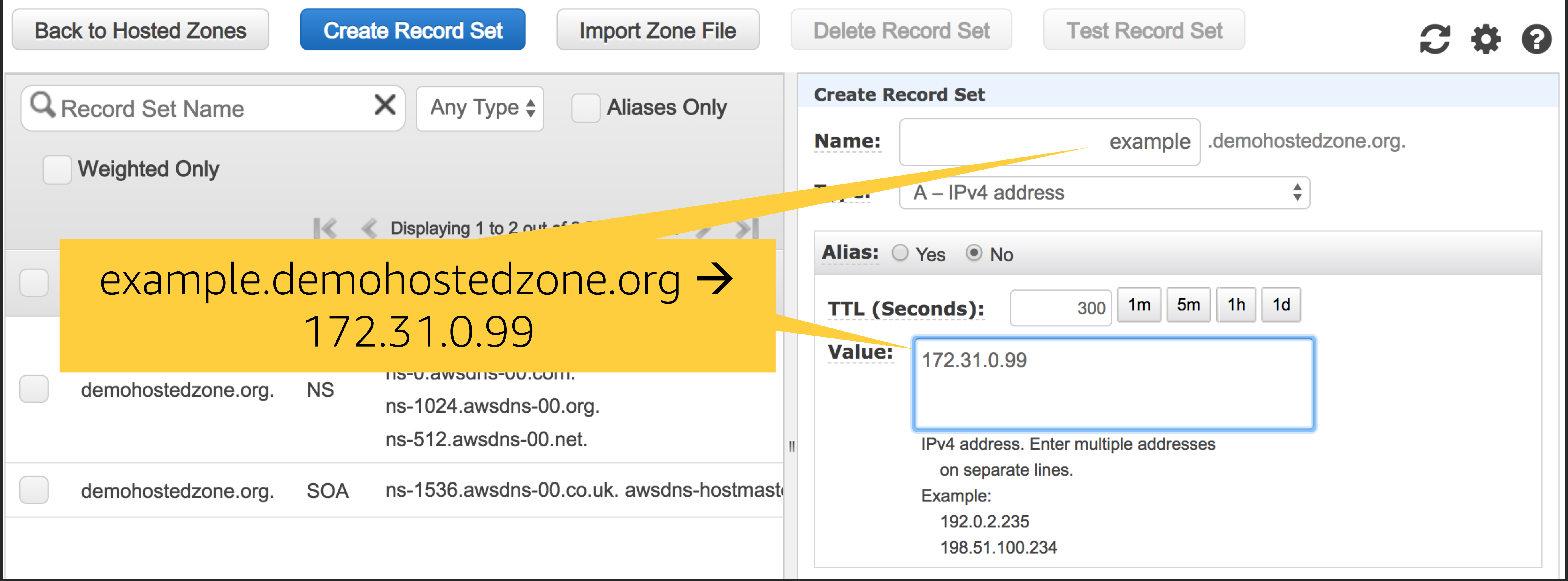
Network ACL: acl-0e 2d02bbc5a5
Tenancy: Defaul

DNS resolution: yes
DNS hostnames: yes

Have EC2 auto-assign DNS host names to instances

Use Amazon DNS server

Amazon Route 53 private hosted zones



□	demohostedzone.org.	NS	ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
□	demohostedzone.org.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmast

Create Record Set

Name: example .demohostedzone.org.

Type: A – IPv4 address

Alias: ○ Yes ● No

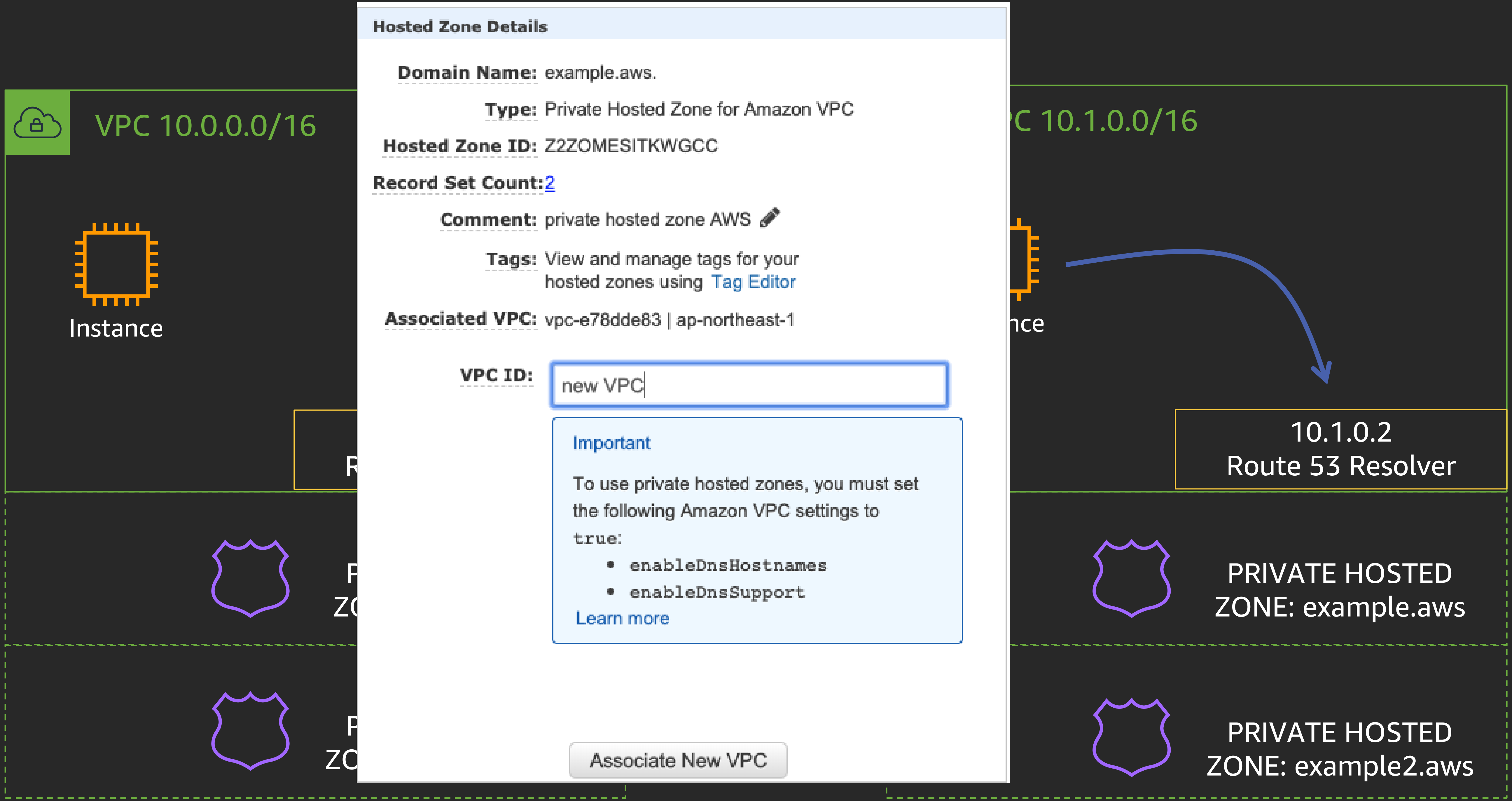
TTL (Seconds): 300 1m 5m 1h 1d

Value: 172.31.0.99

IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234

example.demohostedzone.org → 172.31.0.99

Associating private hosted zones to multiple VPCs



Hosted Zone Details

Domain Name: example.aws.

Type: Private Hosted Zone for Amazon VPC

Hosted Zone ID: Z2ZOMESITKWGCC

Record Set Count:2

Comment: private hosted zone AWS

Tags: View and manage tags for your hosted zones using Tag Editor

Associated VPC: vpc-e78dde83 | ap-northeast-1

VPC ID: new VPC

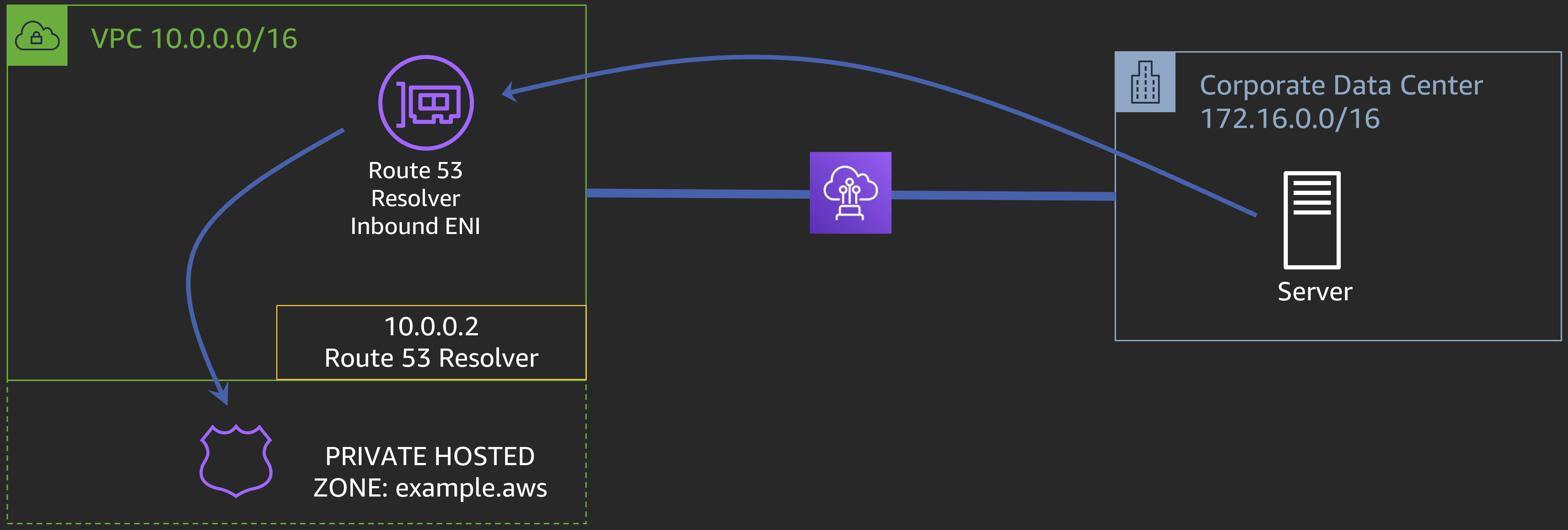
Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

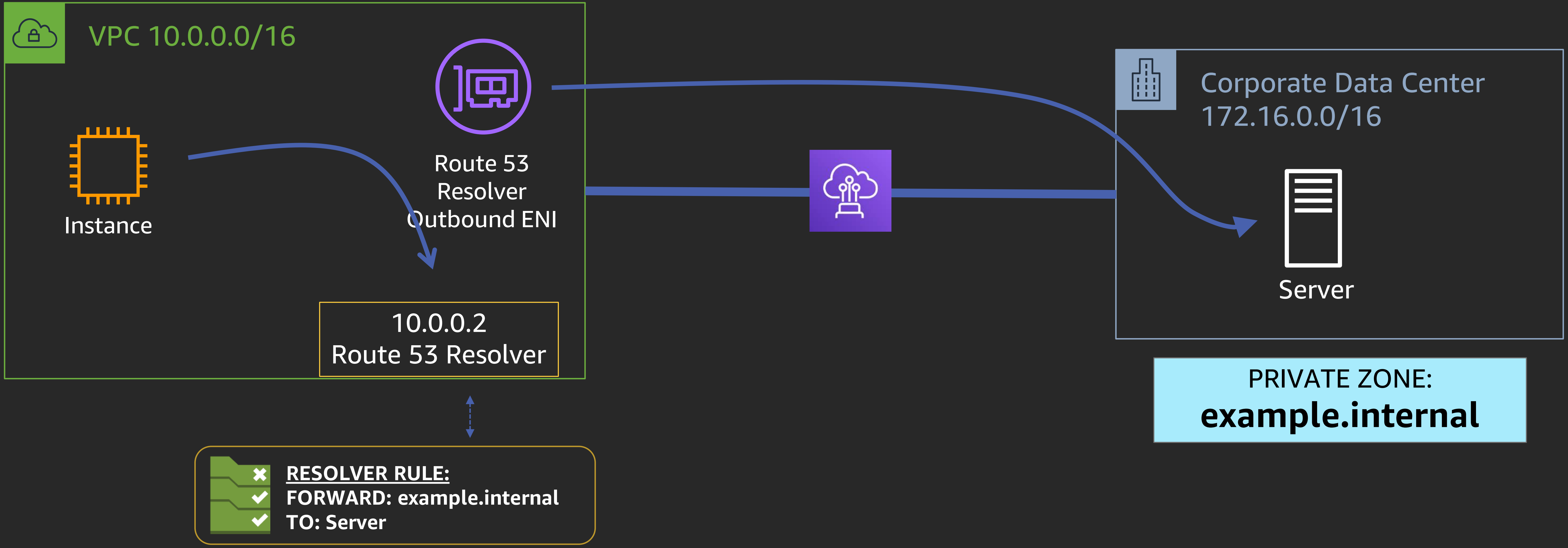
Learn more

Resolving AWS domains from on-premises – Route 53 Resolver



VPC 10.0.0.0/16
Route 53 Resolver Inbound ENI
10.0.0.2 Route 53 Resolver
PRIVATE HOSTED ZONE: example.aws
Corporate Data Center 172.16.0.0/16
Server

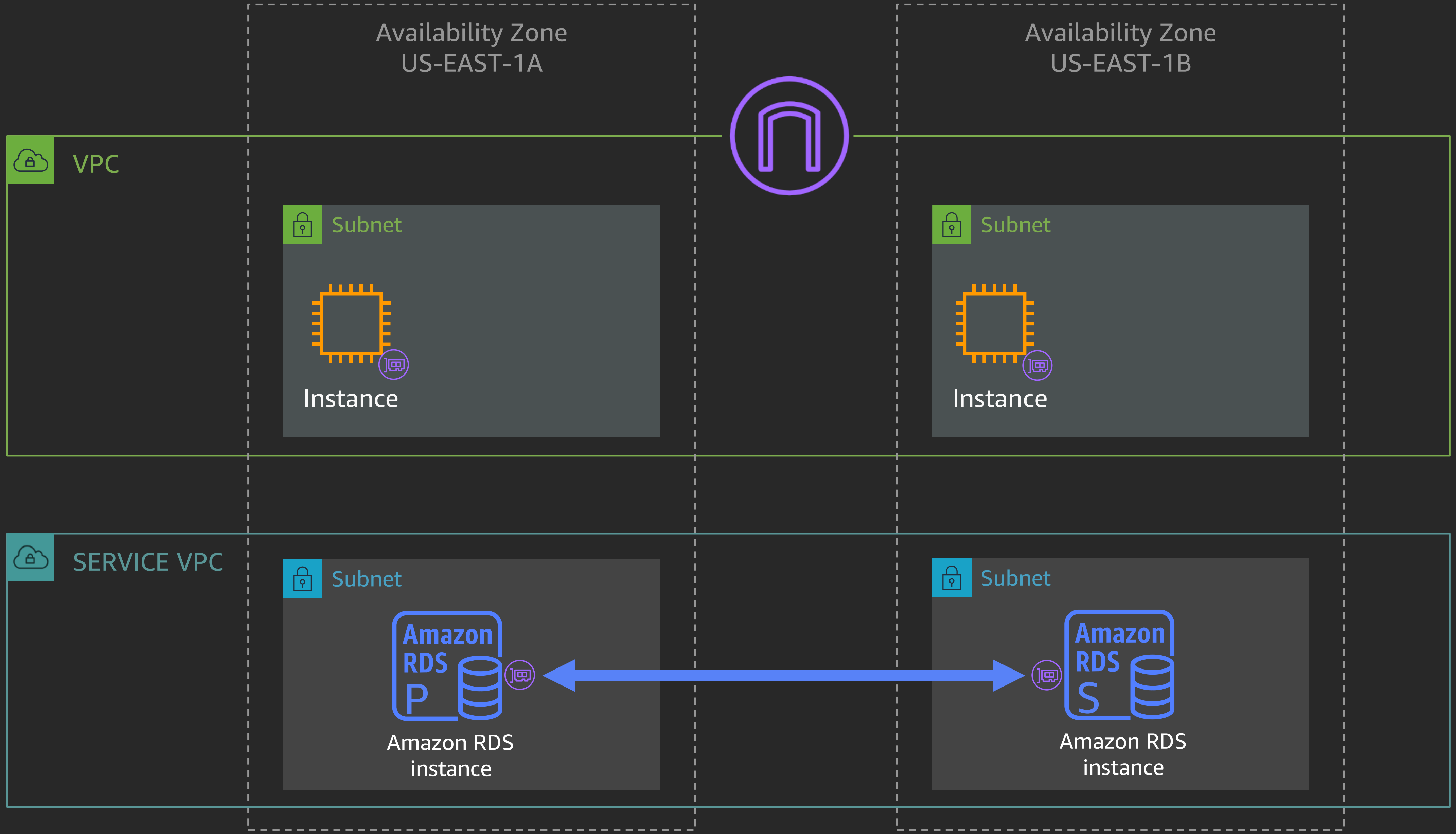
Resolving on-premise domains from AWS – Route 53 Resolver



Connecting to other AWS services

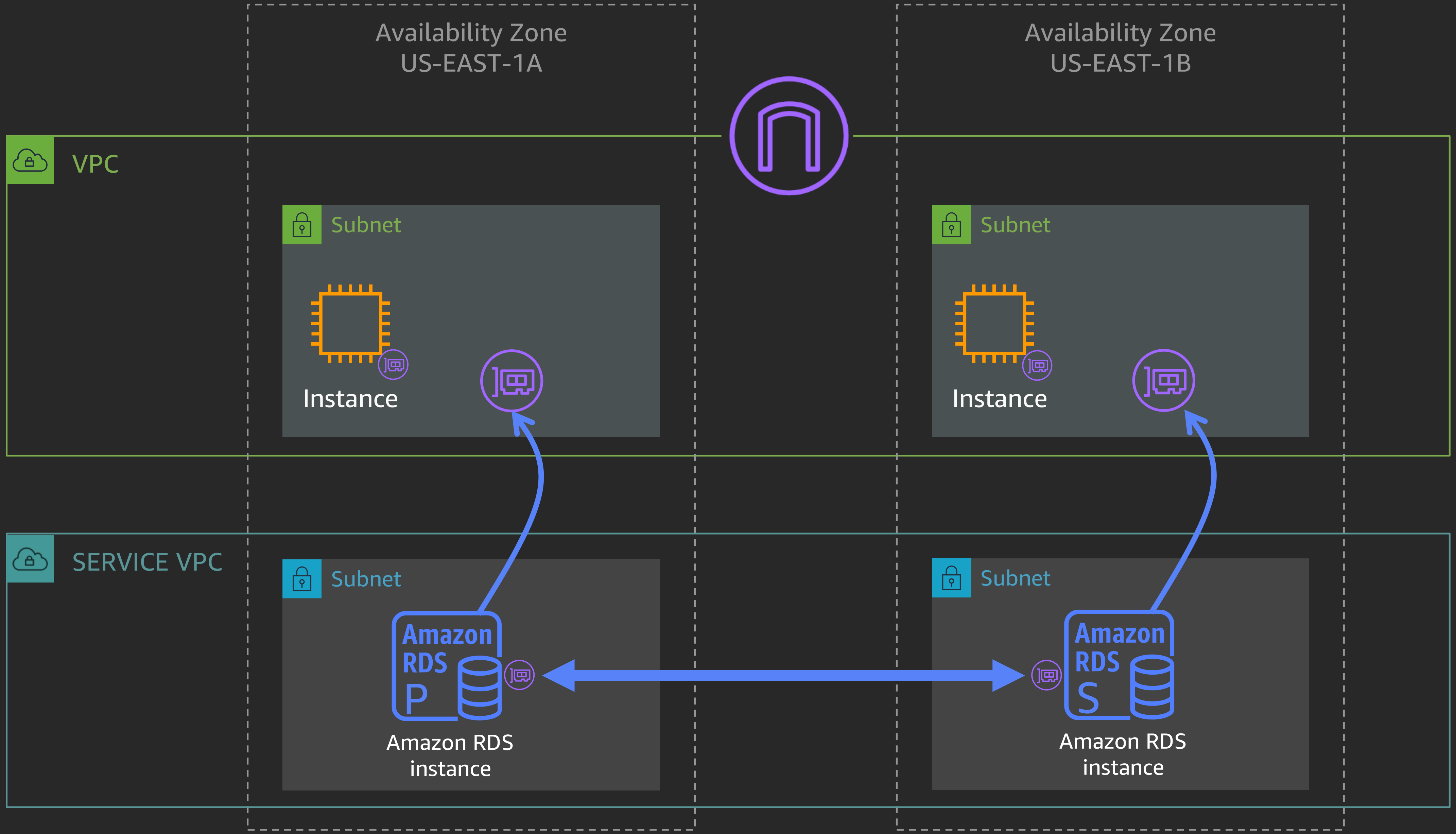
Other AWS services in your VPC

- Amazon Relational Database Service (Amazon RDS)



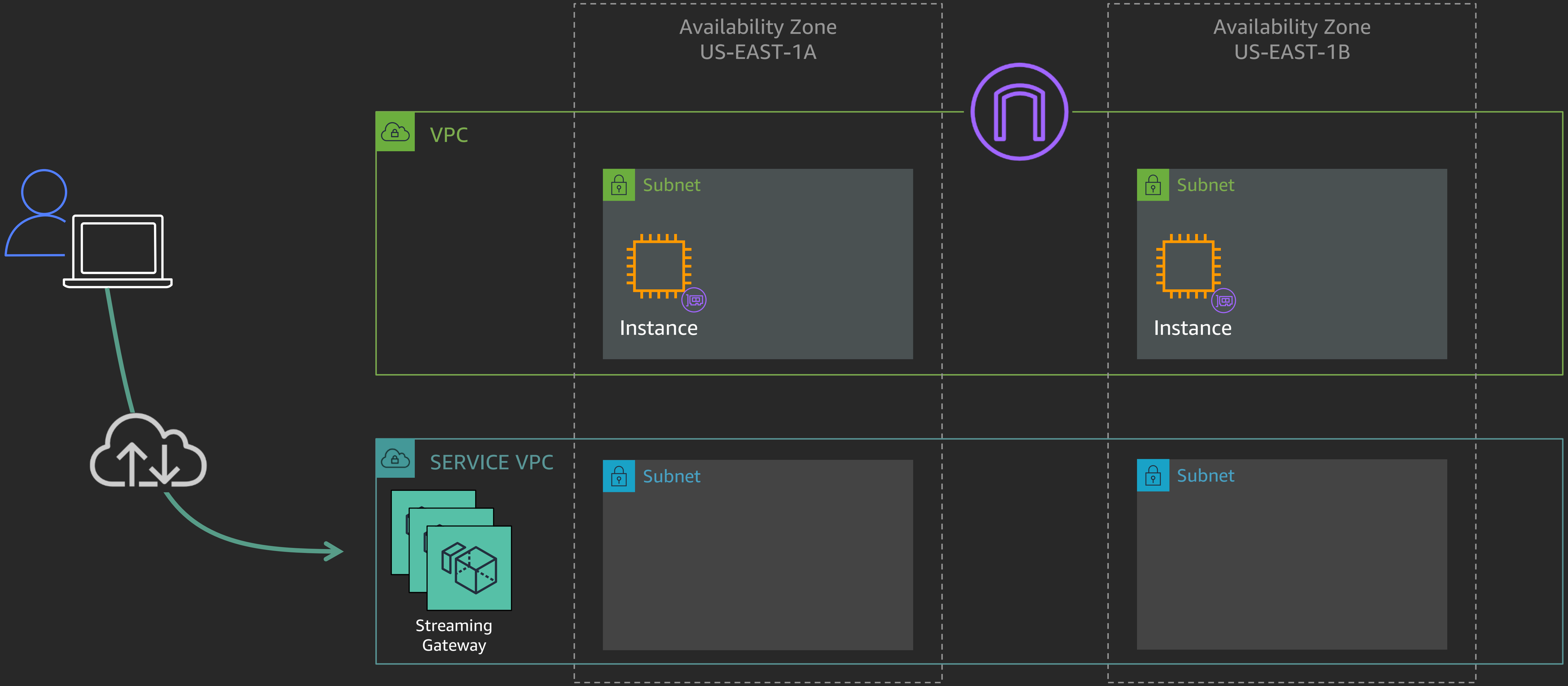
Other AWS services in your VPC

- Amazon Relational Database Service (Amazon RDS)



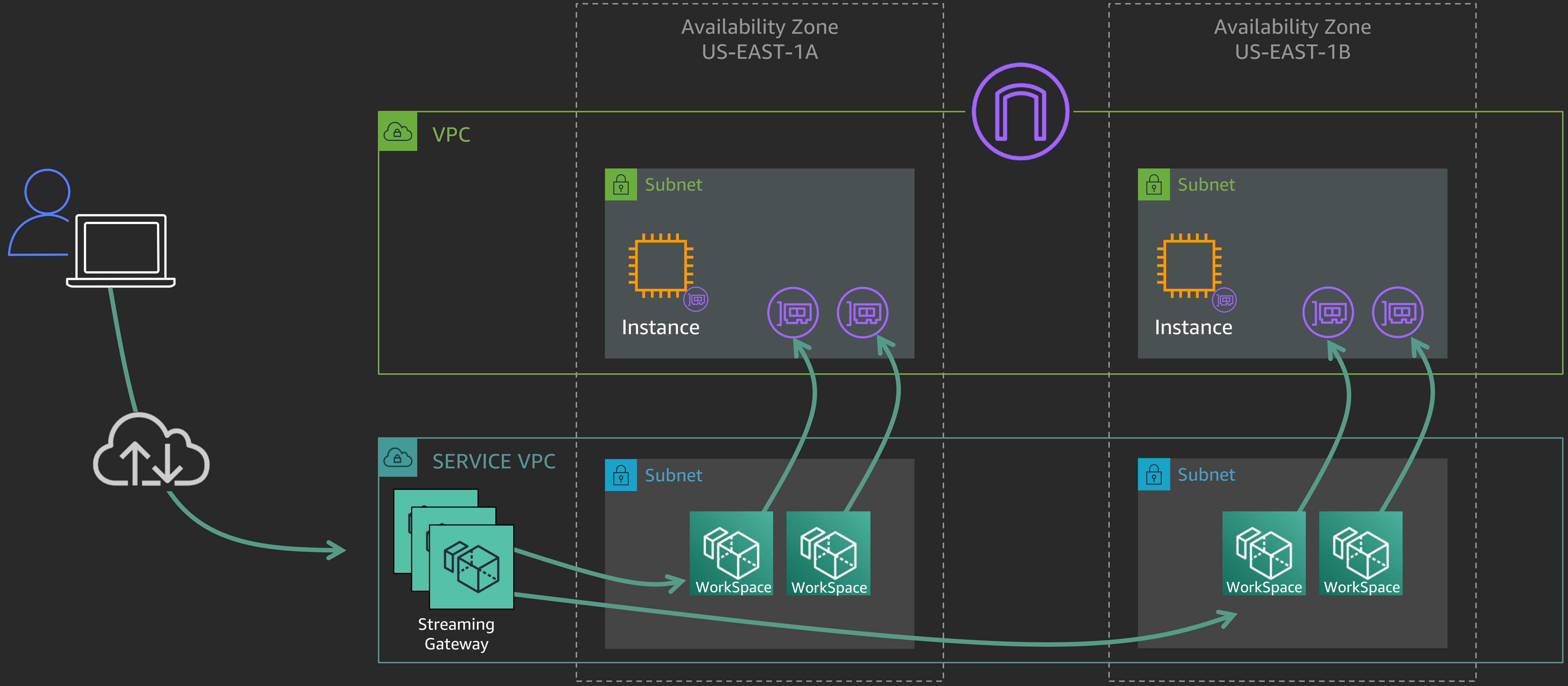
Other AWS services in your VPC

- Amazon WorkSpaces



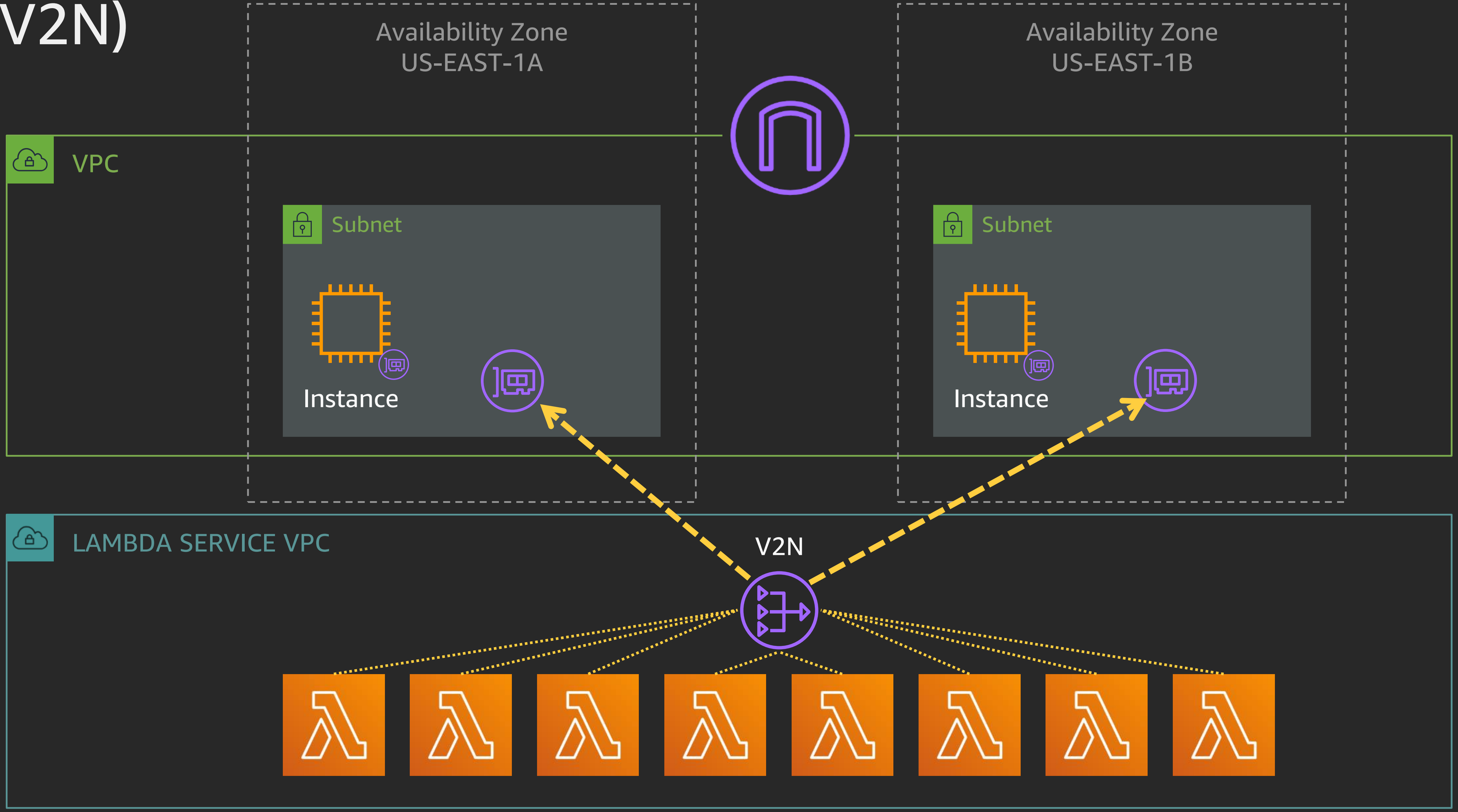
Other AWS services in your VPC

- Amazon WorkSpaces



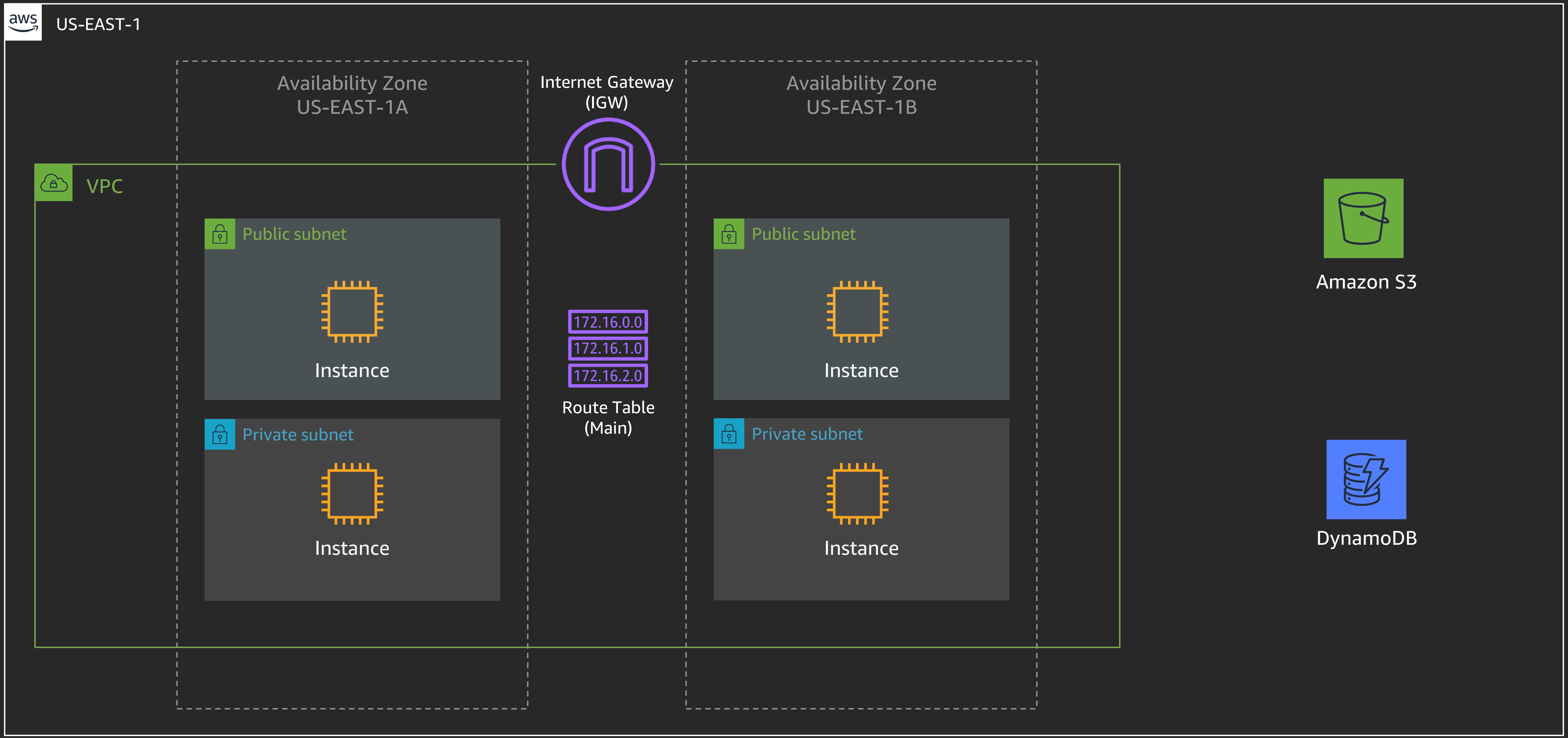
Other AWS services in your VPC

- AWS Lambda
- VPC-2-VPC NAT (V2N)



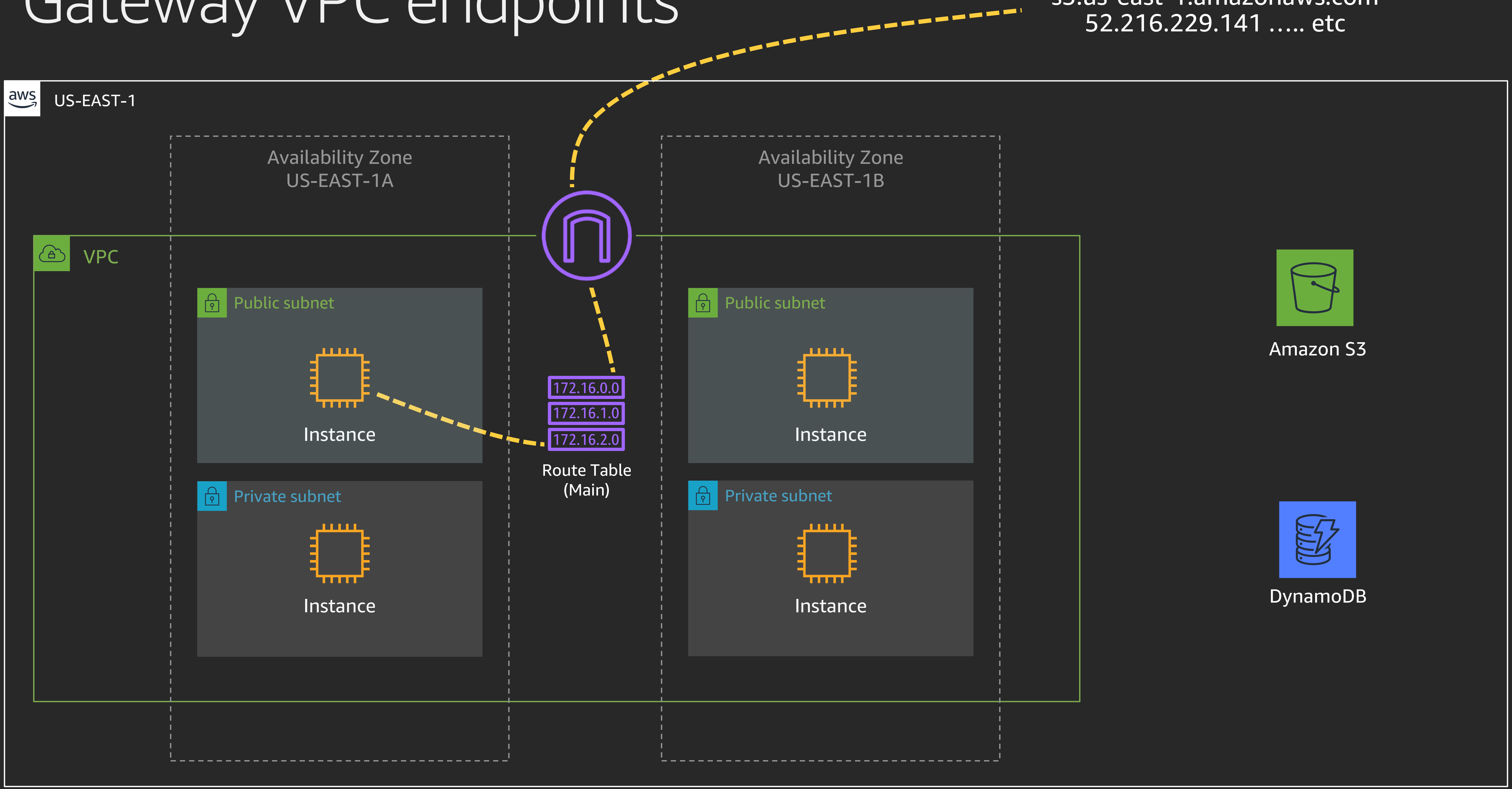
VPC endpoints

Gateway VPC endpoints

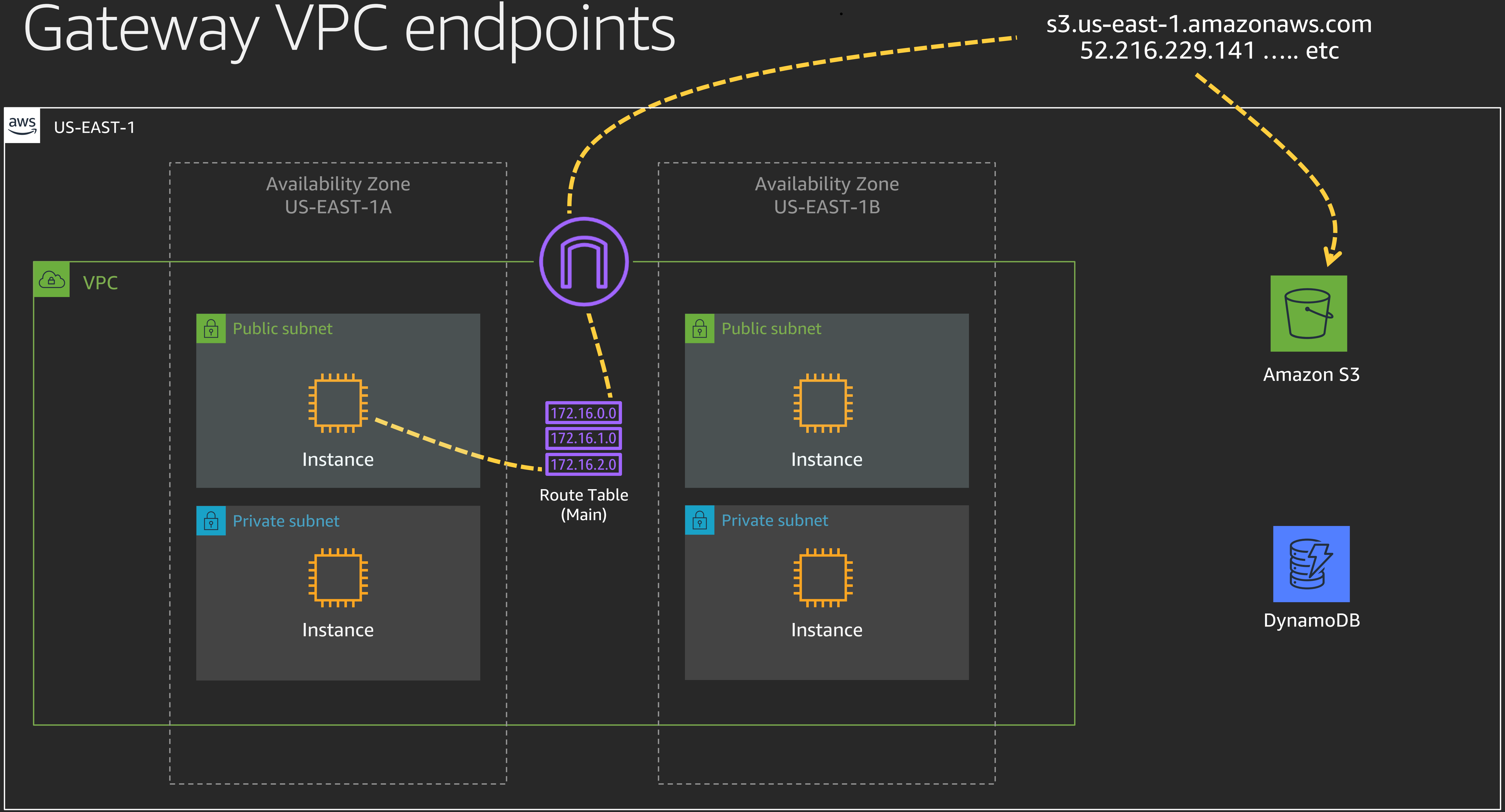


Gateway VPC endpoints

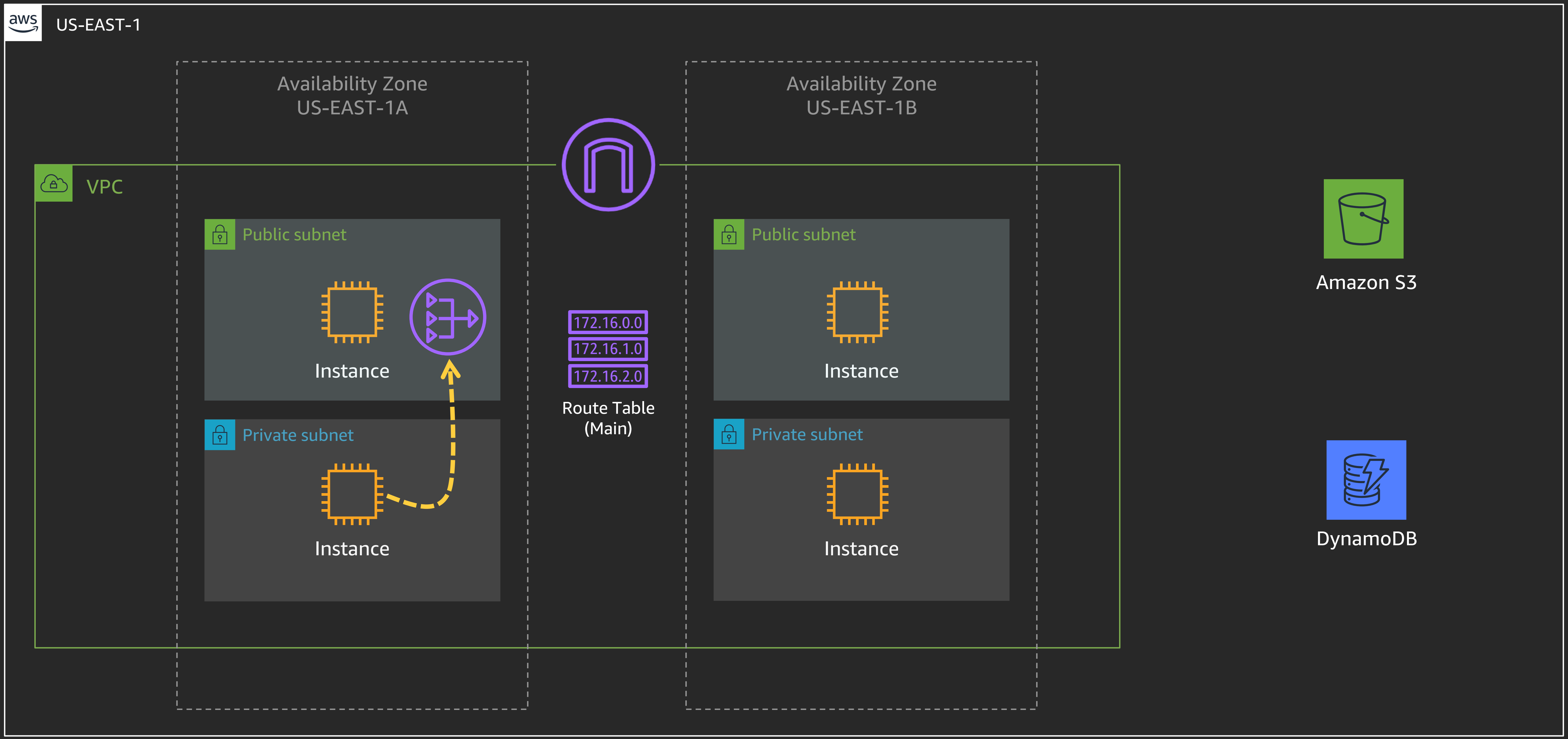
s3.us-east-1.amazonaws.com
52.216.229.141 ….. etc



Gateway VPC endpoints

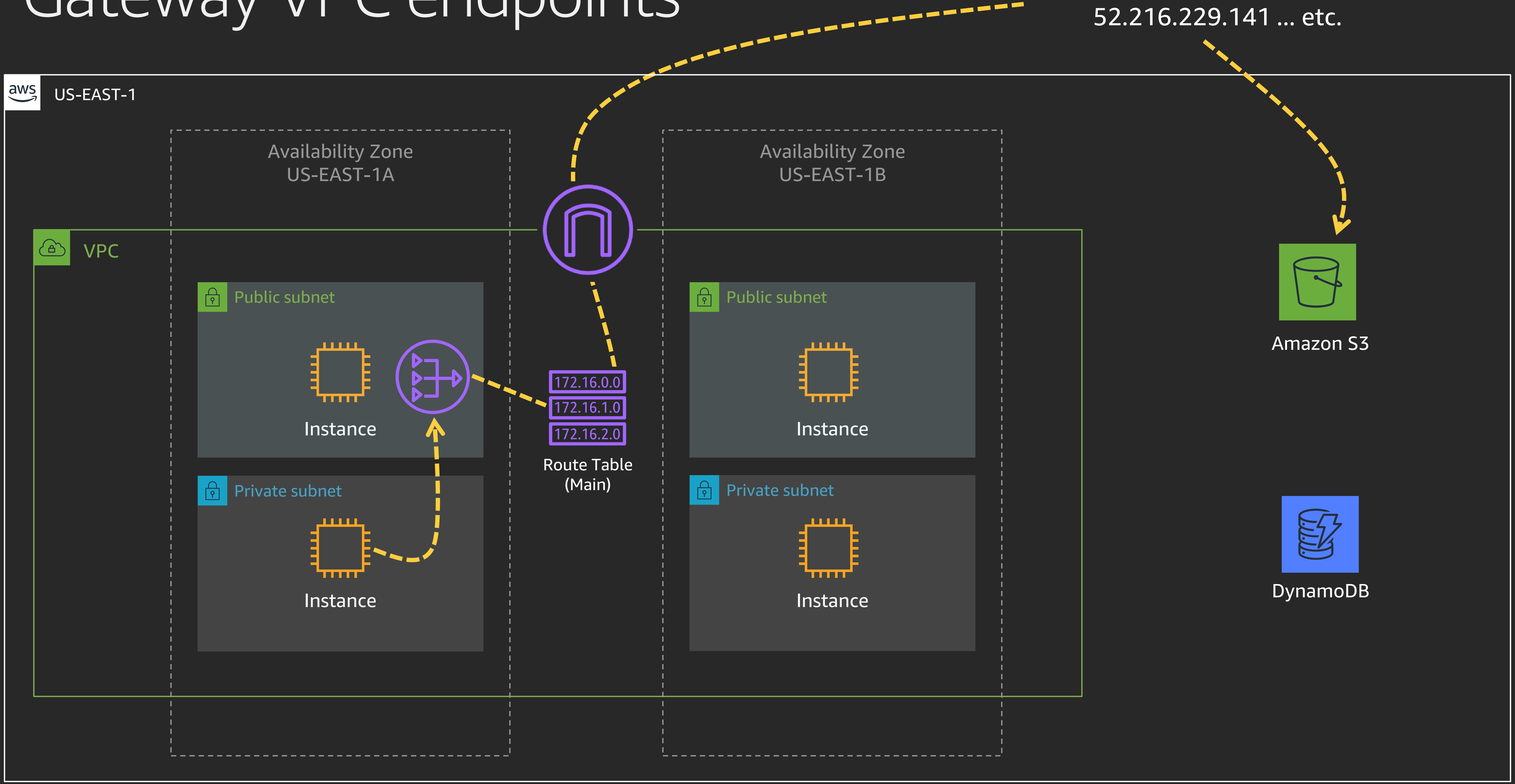


Gateway VPC endpoints

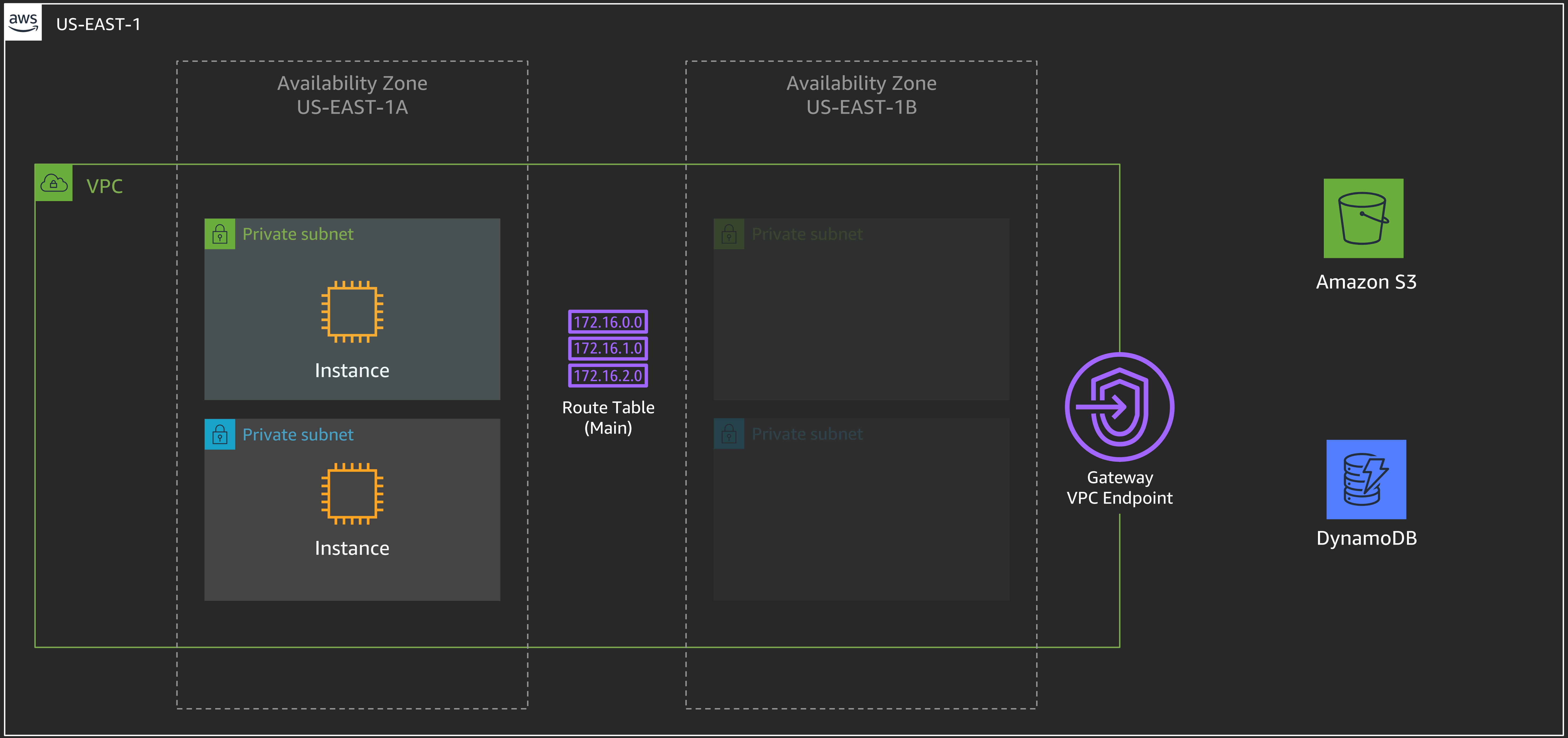


Gateway VPC endpoints

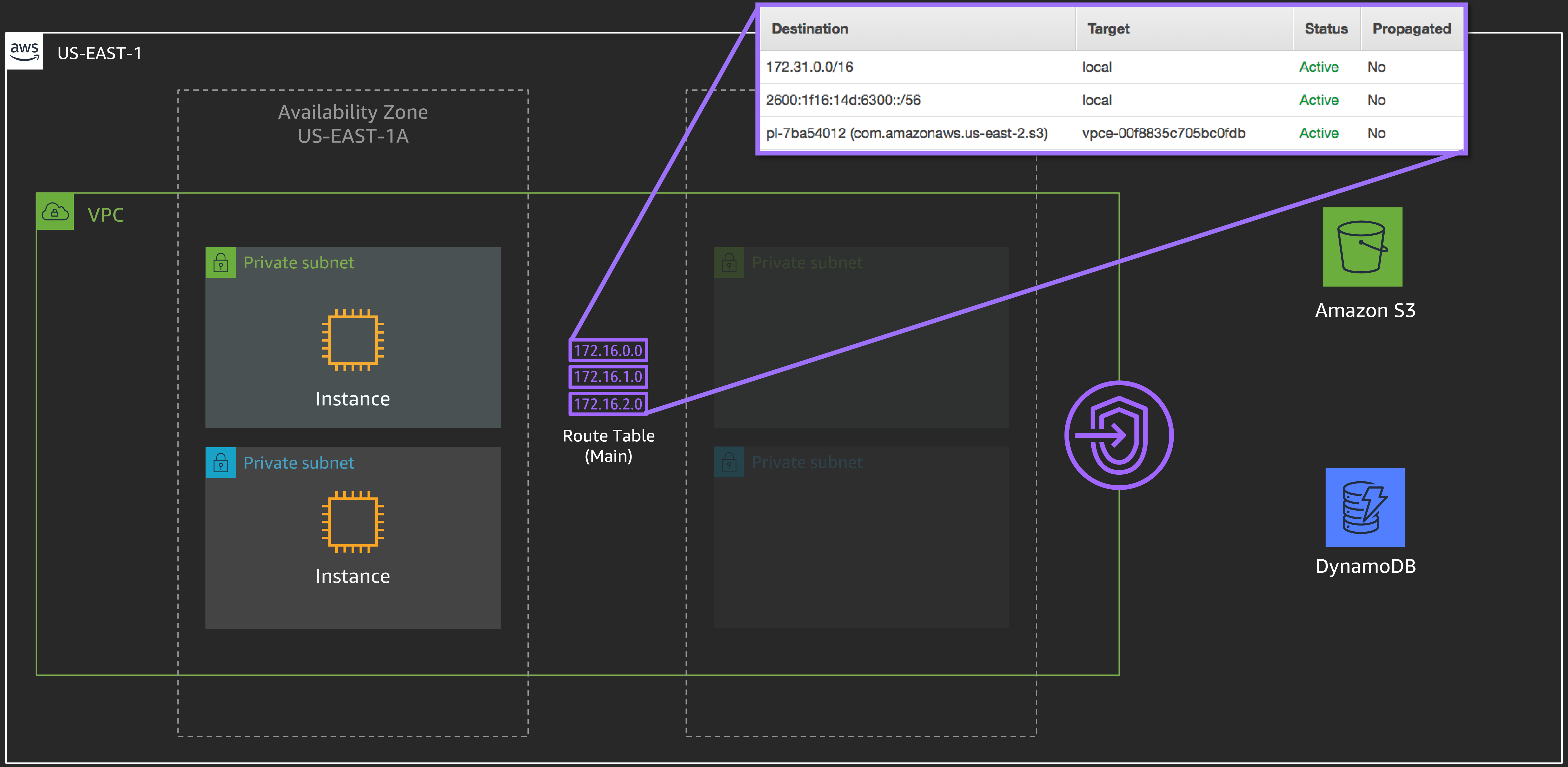
s3.us-east-1.amazonaws.com
52.216.229.141 ... etc.



Gateway VPC endpoints

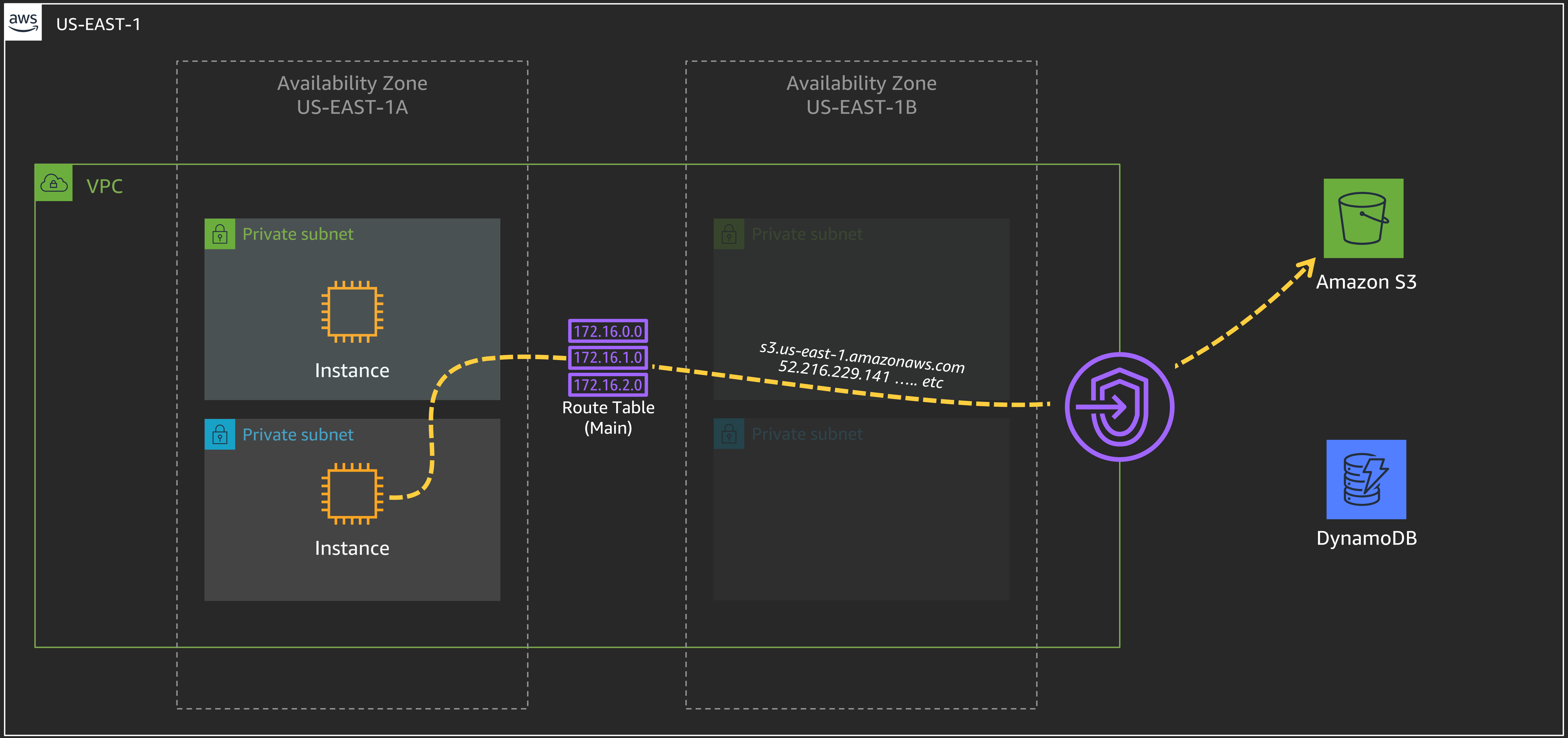


Gateway VPC endpoints

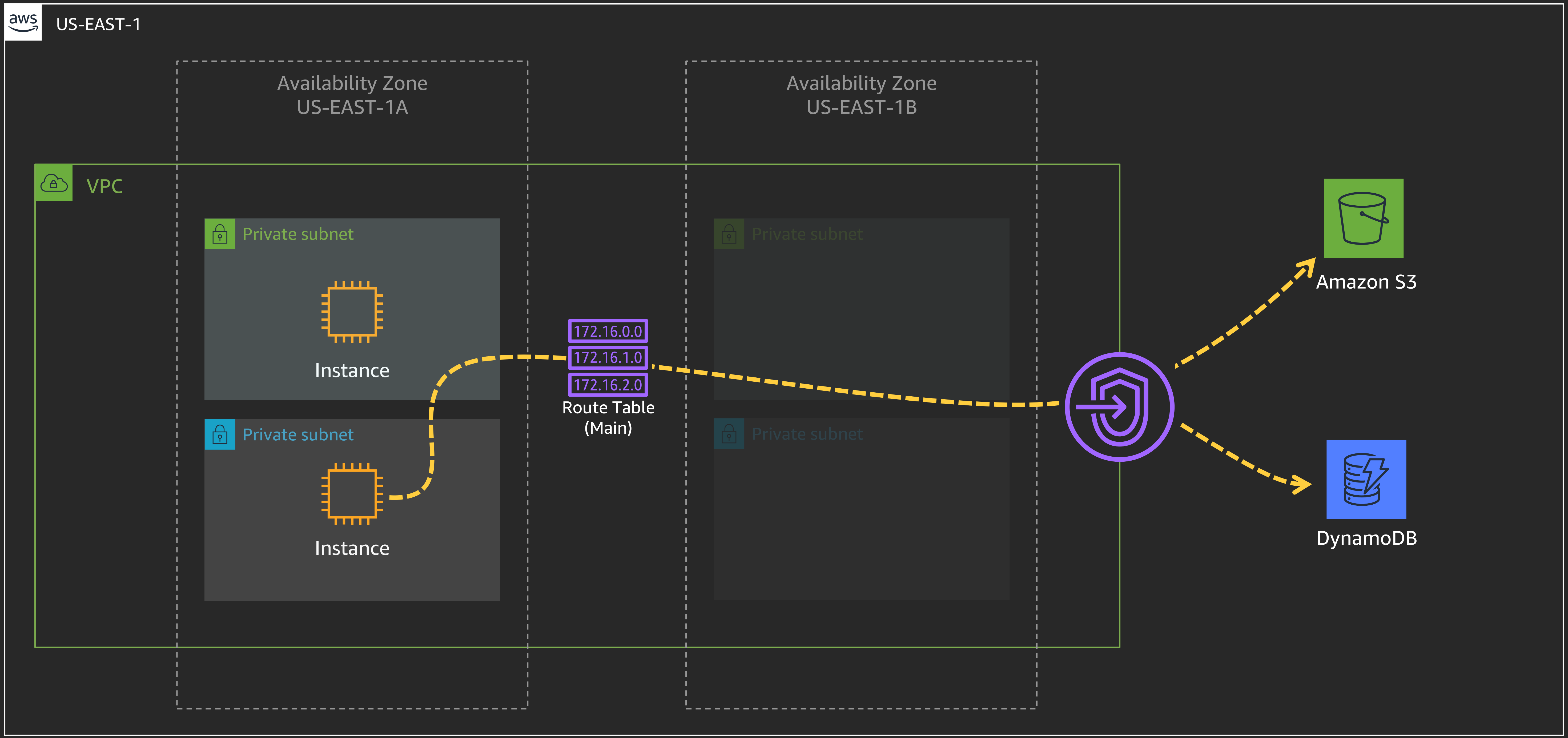


Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
pl-7ba54012 (com.amazonaws.us-east-2.s3)	vpce-00f8835c705bc0fdb	Active	No

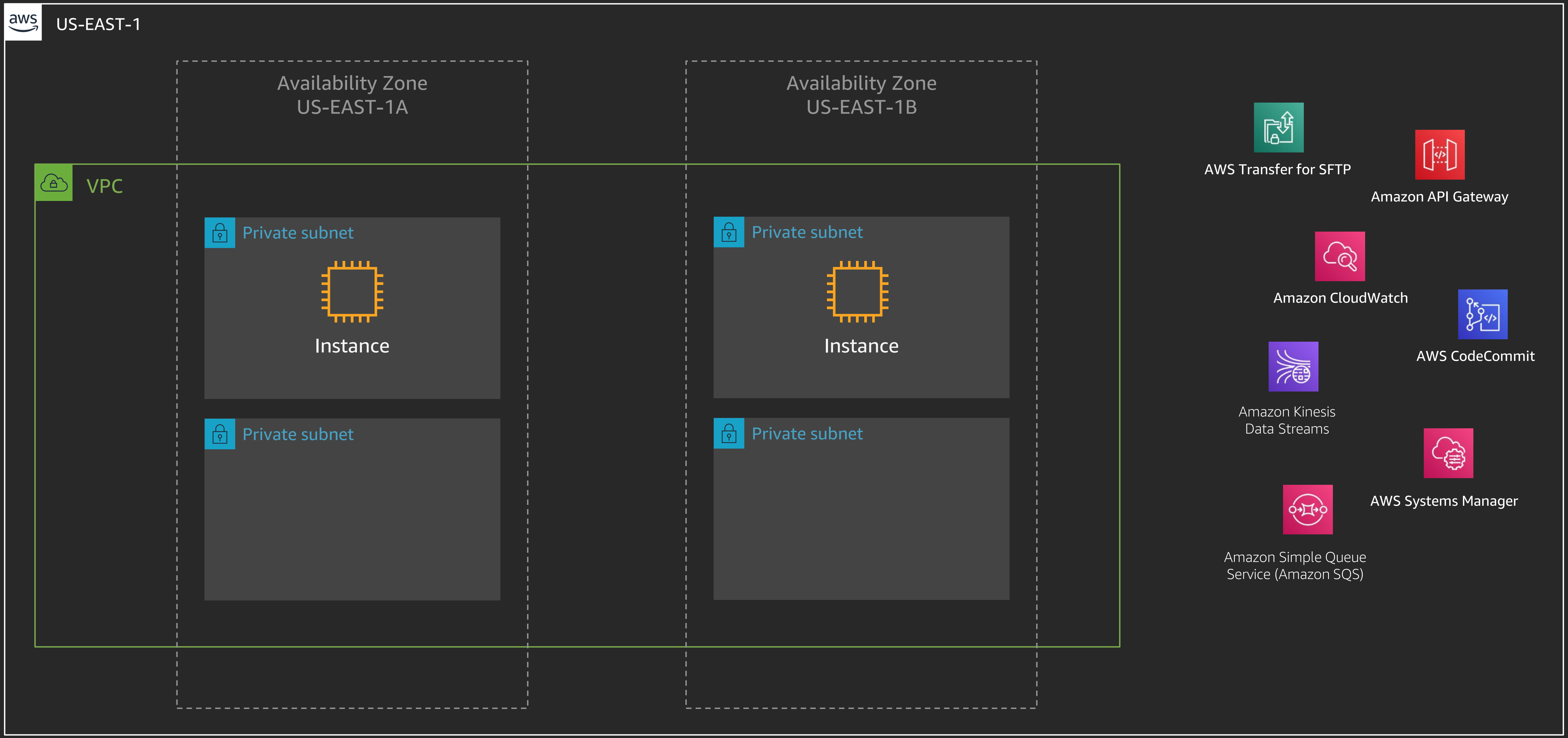
Gateway VPC endpoints



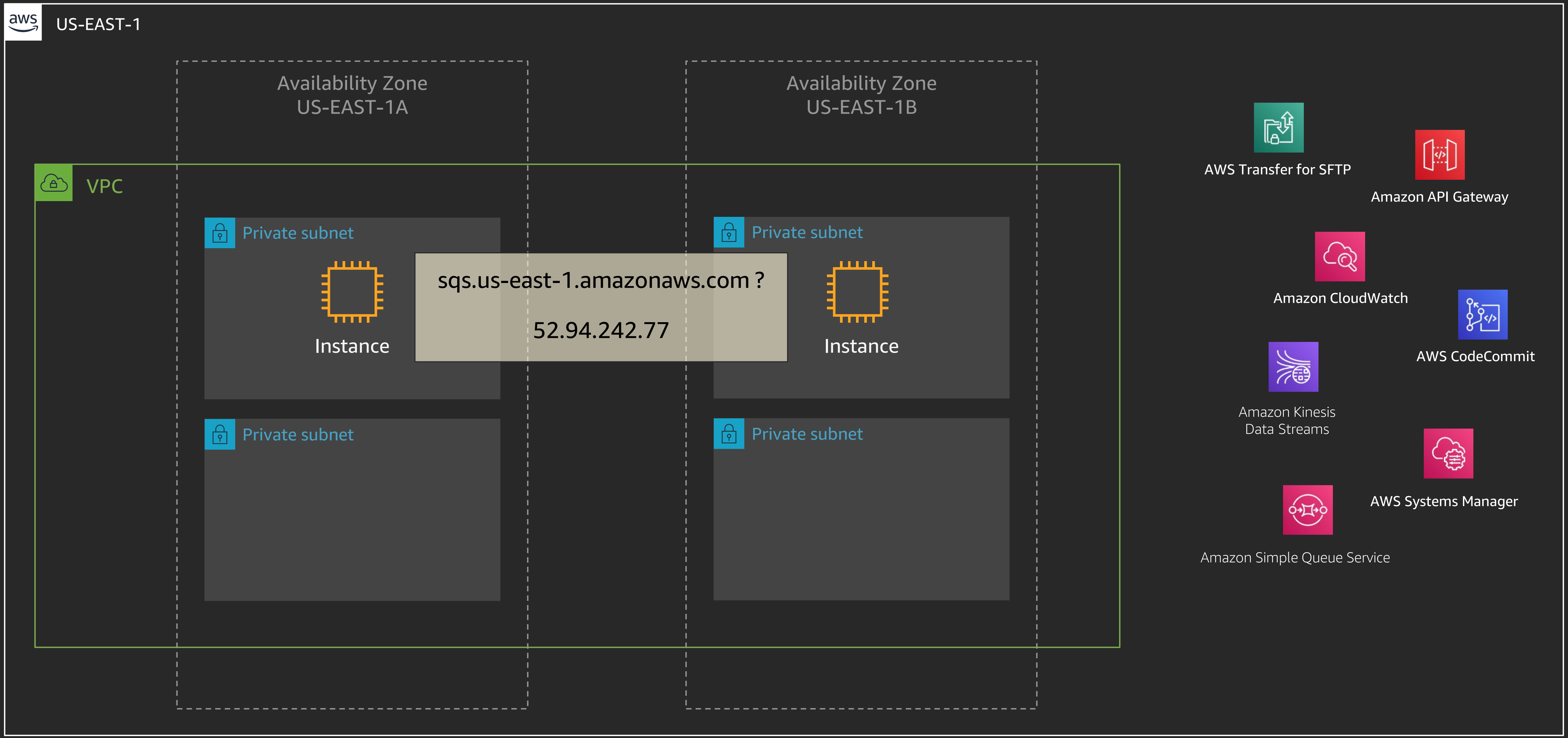
Gateway VPC endpoints



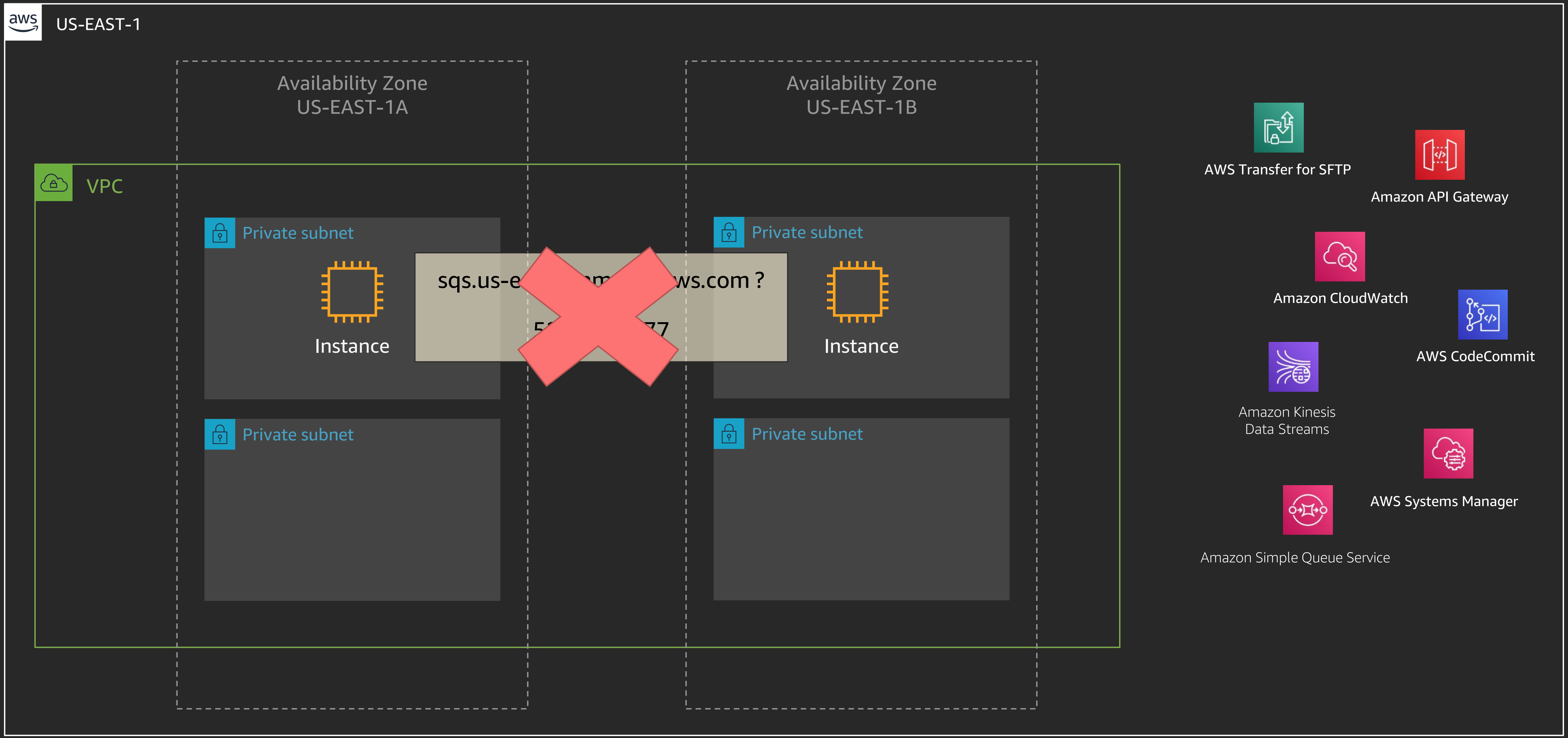
Interface VPC endpoints (AWS PrivateLink)



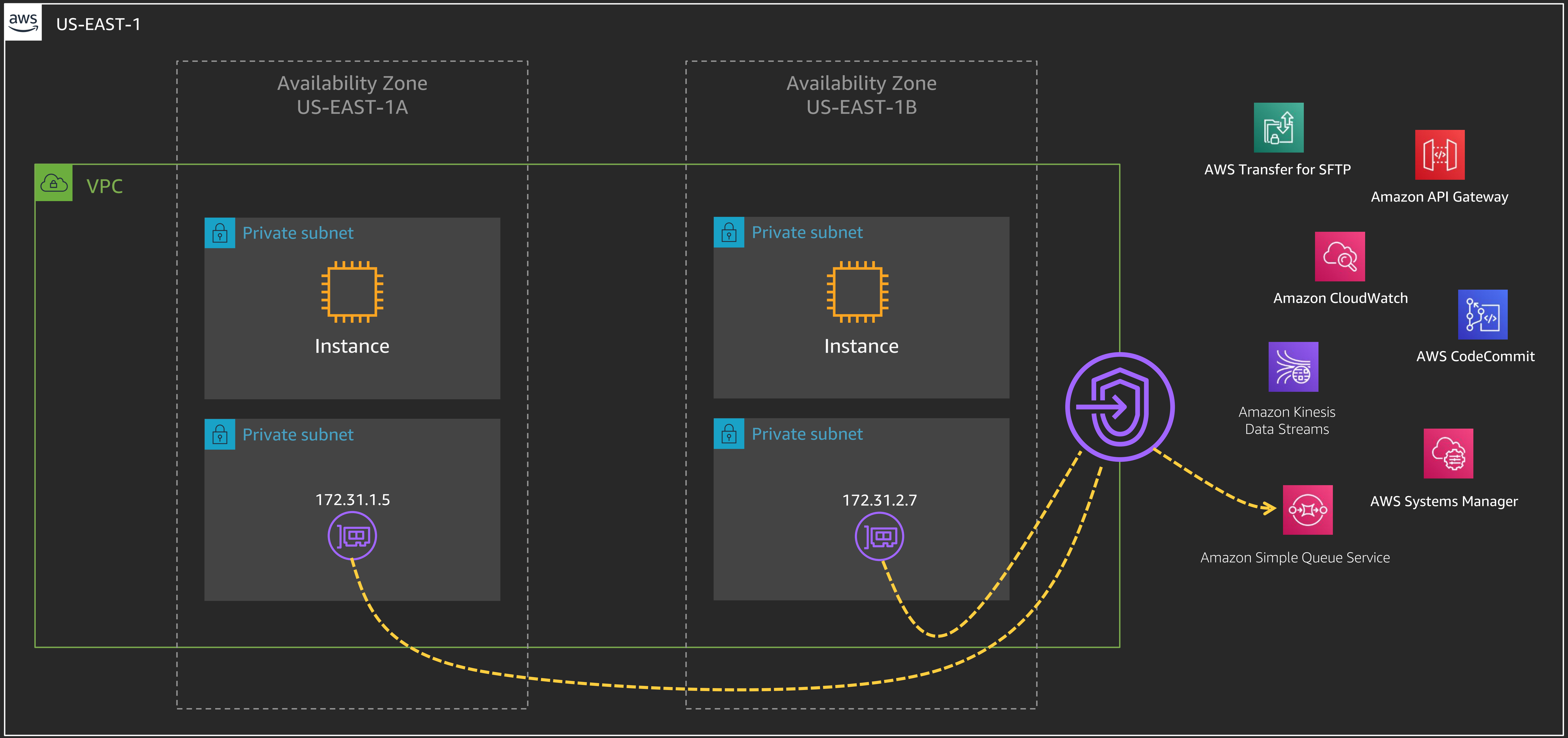
Interface VPC endpoints (AWS PrivateLink)



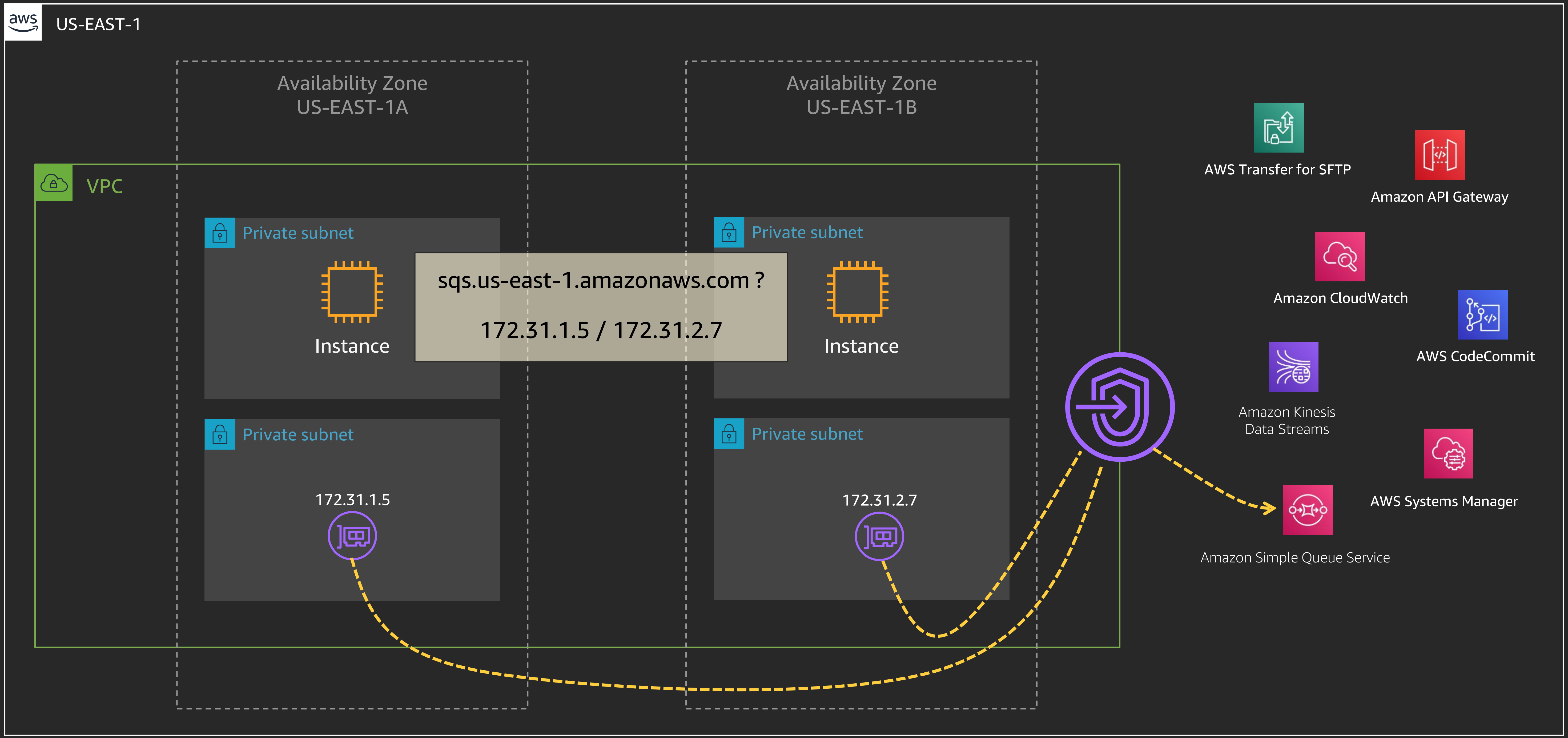
Interface VPC endpoints (AWS PrivateLink)



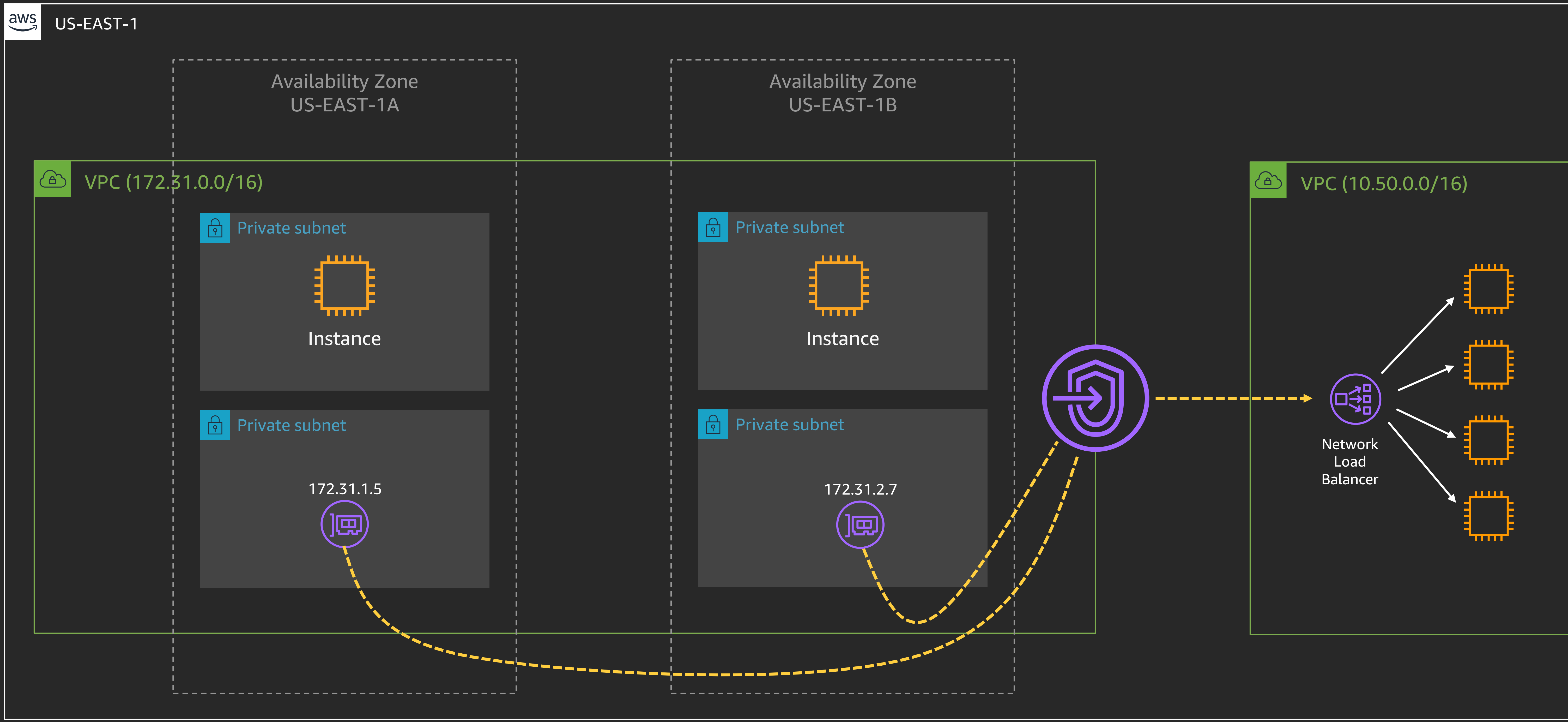
Interface VPC endpoints (AWS PrivateLink)



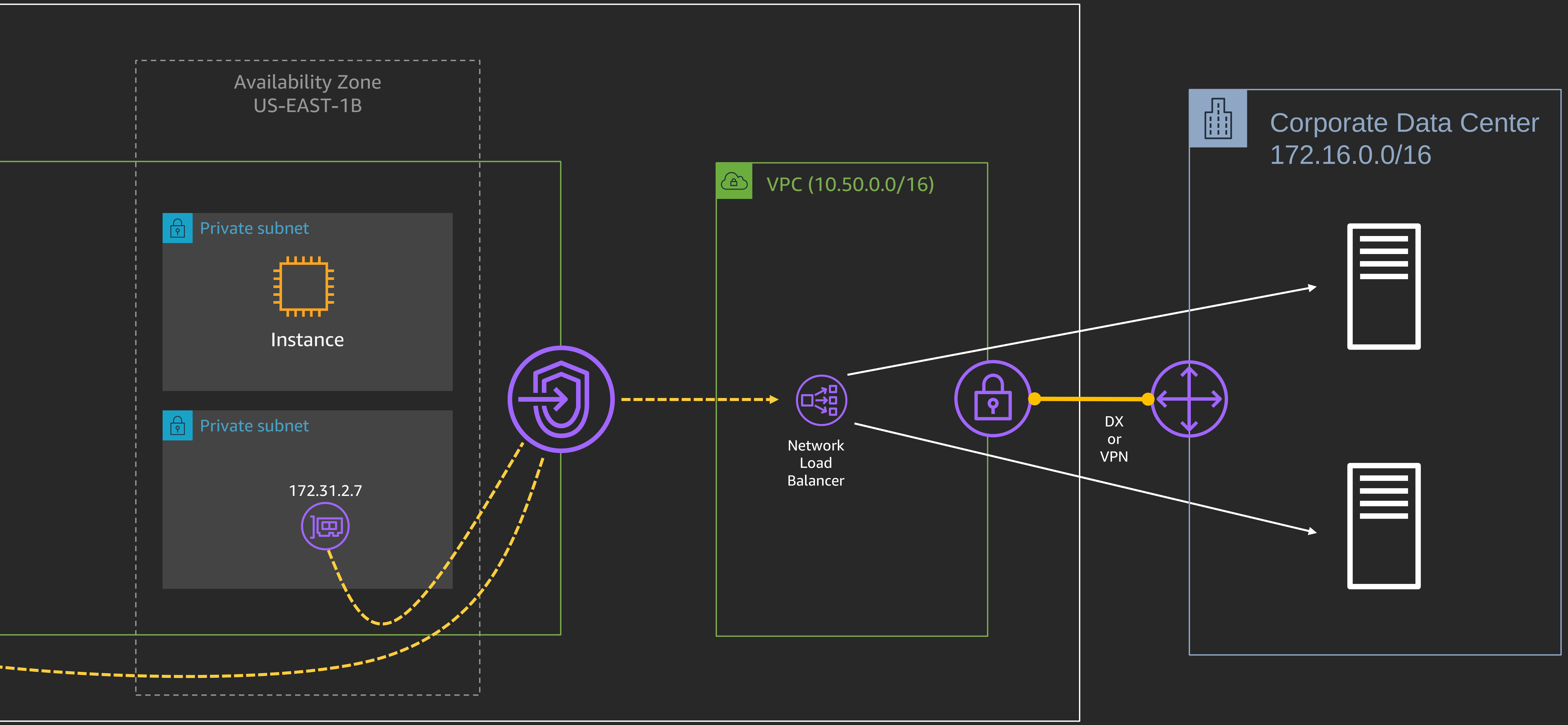
Interface VPC endpoints (AWS PrivateLink)



AWS PrivateLink – your own services



AWS PrivateLink – Your own services – On-prem



Endpoint policies

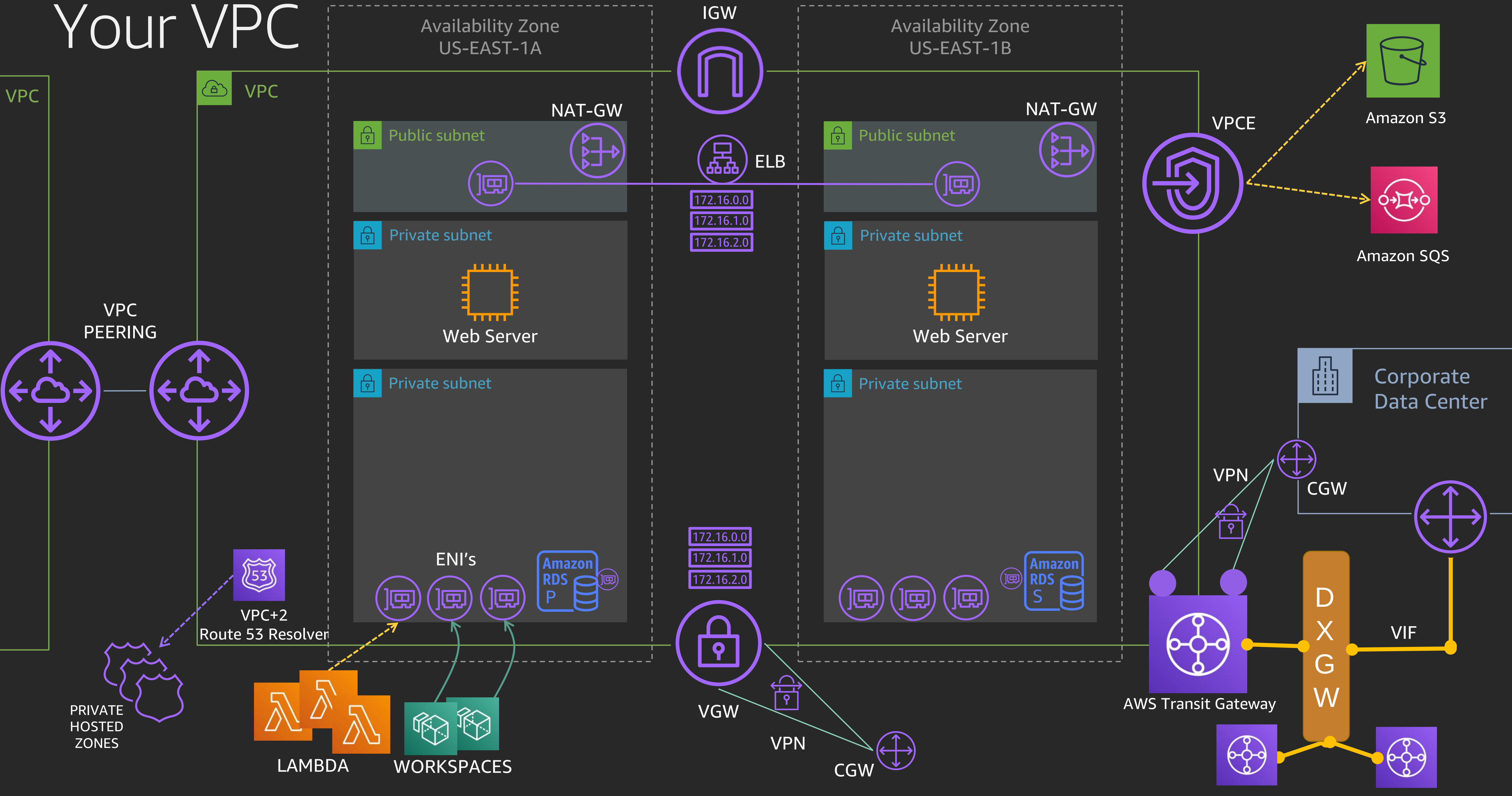
- A VPC endpoint policy is an AWS Identity and Access Management (IAM) resource policy that you attach to an endpoint
- An endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies)

Example for S3

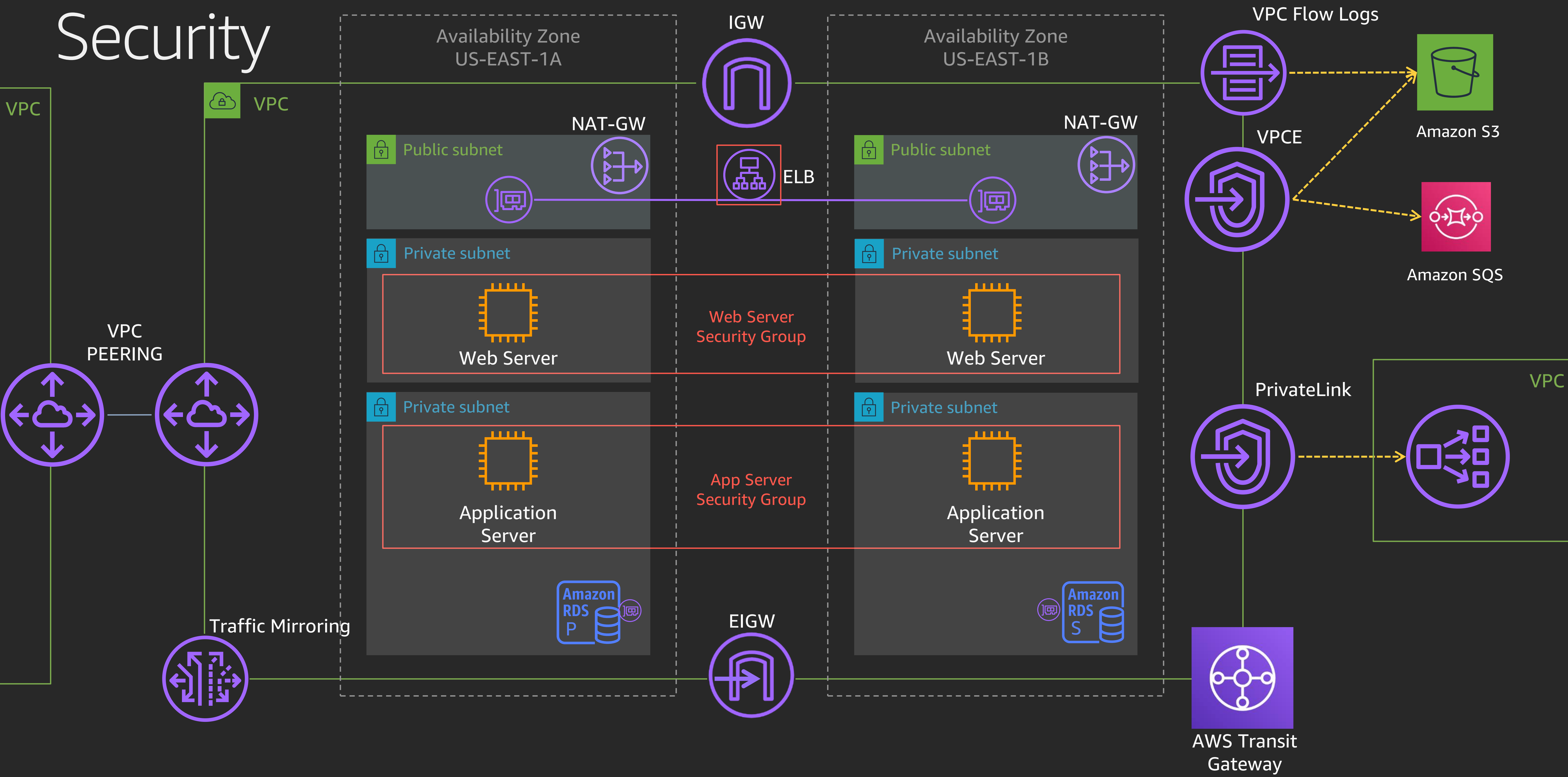
- IAM policy at VPC endpoint: You may only access the “Data” bucket
- IAM policy at S3 bucket: Access to this bucket is only allowed from VPCE-X

Bringing it all together

Your VPC


Availability Zone
US-EAST-1A
IGW
Availability Zone
US-EAST-1B
VPC
VPC
NAT-GW
Public subnet
ELB
NAT-GW
Public subnet
VPCE
Amazon S3
Amazon SQS
172.16.0.0
172.16.1.0
172.16.2.0
Private subnet
Web Server
Private subnet
Web Server
VPC
PEERING
Private subnet
Private subnet
Corporate
Data Center
VPN
CGW
ENI's
Amazon
RDS
P
172.16.0.0
172.16.1.0
172.16.2.0
Amazon
RDS
S
VPC+2
Route 53 Resolver
VIF
D
X
G
W
PRIVATE
HOSTED
ZONES
VGW
AWS Transit Gateway
VPN
LAMBDA
WORKSPACES
CGW

Security


VPC
VPC
Availability Zone
US-EAST-1A
IGW
Availability Zone
US-EAST-1B
VPC Flow Logs
Amazon S3
NAT-GW
NAT-GW
VPCE
Public subnet
ELB
Public subnet
Amazon SQS
Private subnet
Private subnet
Web Server
Web Server Security Group
Web Server
VPC PEERING
PrivateLink
VPC
Private subnet
Private subnet
Application Server
App Server Security Group
Application Server
Amazon RDS P
Amazon RDS S
Traffic Mirroring
EIGW
AWS Transit Gateway

Related sessions

Tuesday

- NET317-R Connectivity to AWS and hybrid AWS network architectures
- NET320-R1 The right AWS network architecture for the right reason

Wednesday

- NET305-R1 Advanced VPC design and new capabilities for Amazon VPC
- NET203-L Leadership session: Networking

Thursday

- NET339 Innovation and operation of the AWS global network infrastructure
- NET322-R1 Shared VPC: Simplify your AWS Cloud scale network with VPC sharing

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate networking skills

Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and Introduction to Amazon VPC

Validate expertise with the
AWS Certified Advanced Networking - specialty exam

Visit aws.amazon.com/training/paths-specialty

Thank you!

Alan Halachmi
Director, Public Sector
AWS Solutions Architecture
Amazon Web Services

Steve Seymour
WW Tech Leader, Networking
AWS Solutions Architecture
Amazon Web Services

Please complete the session survey in the mobile app.

AWS re:Invent

aws