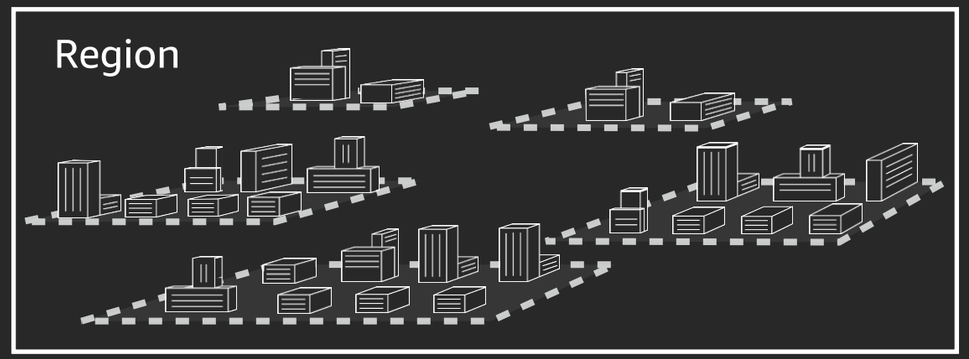
aws SUMMIT ONLINE

AWS networking fundamentals

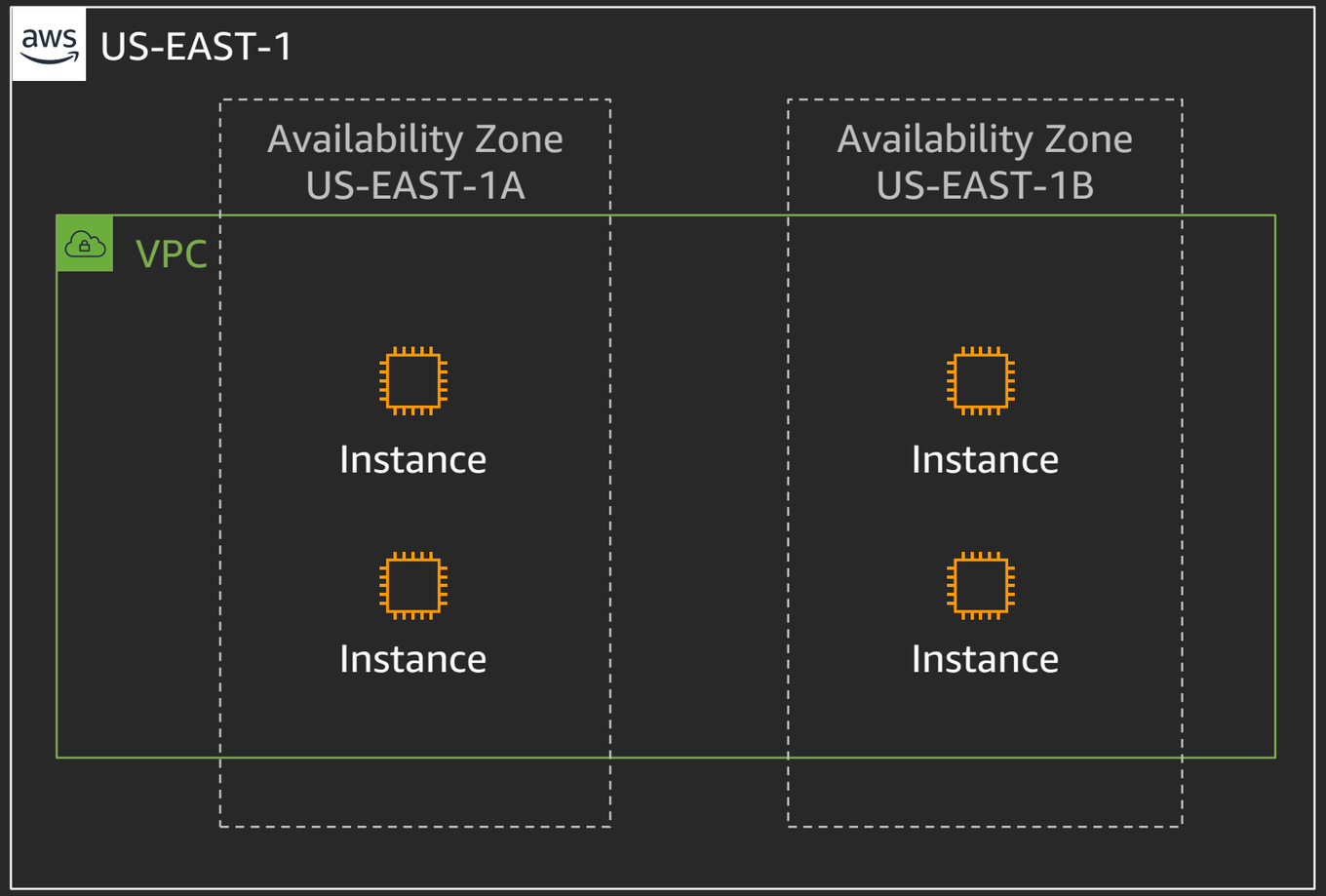
Aarthi Raju
Principal Solutions Architect
Amazon Web Services

aws SUMMIT ONLINE


Region

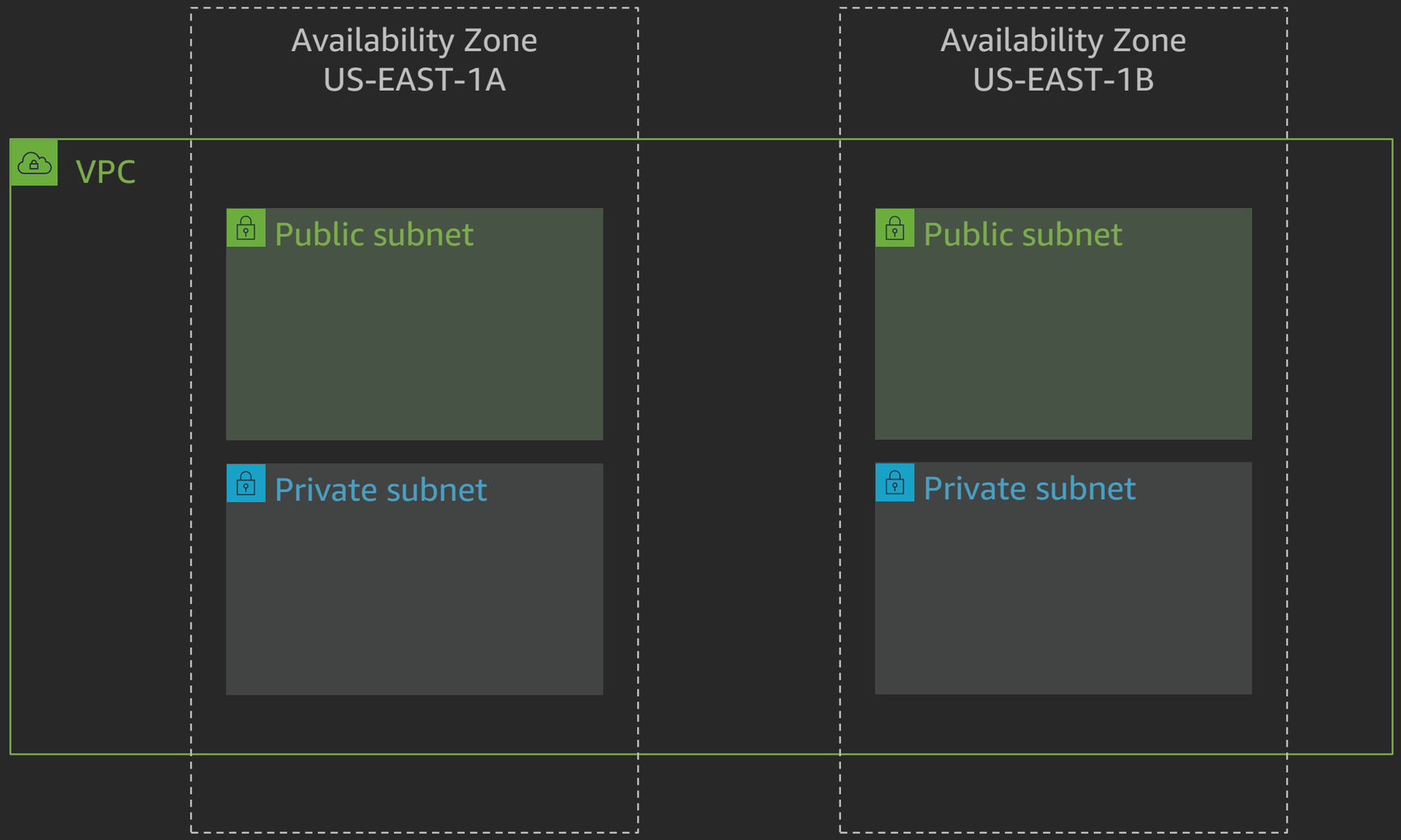

Availability Zone


Data center, rack, host

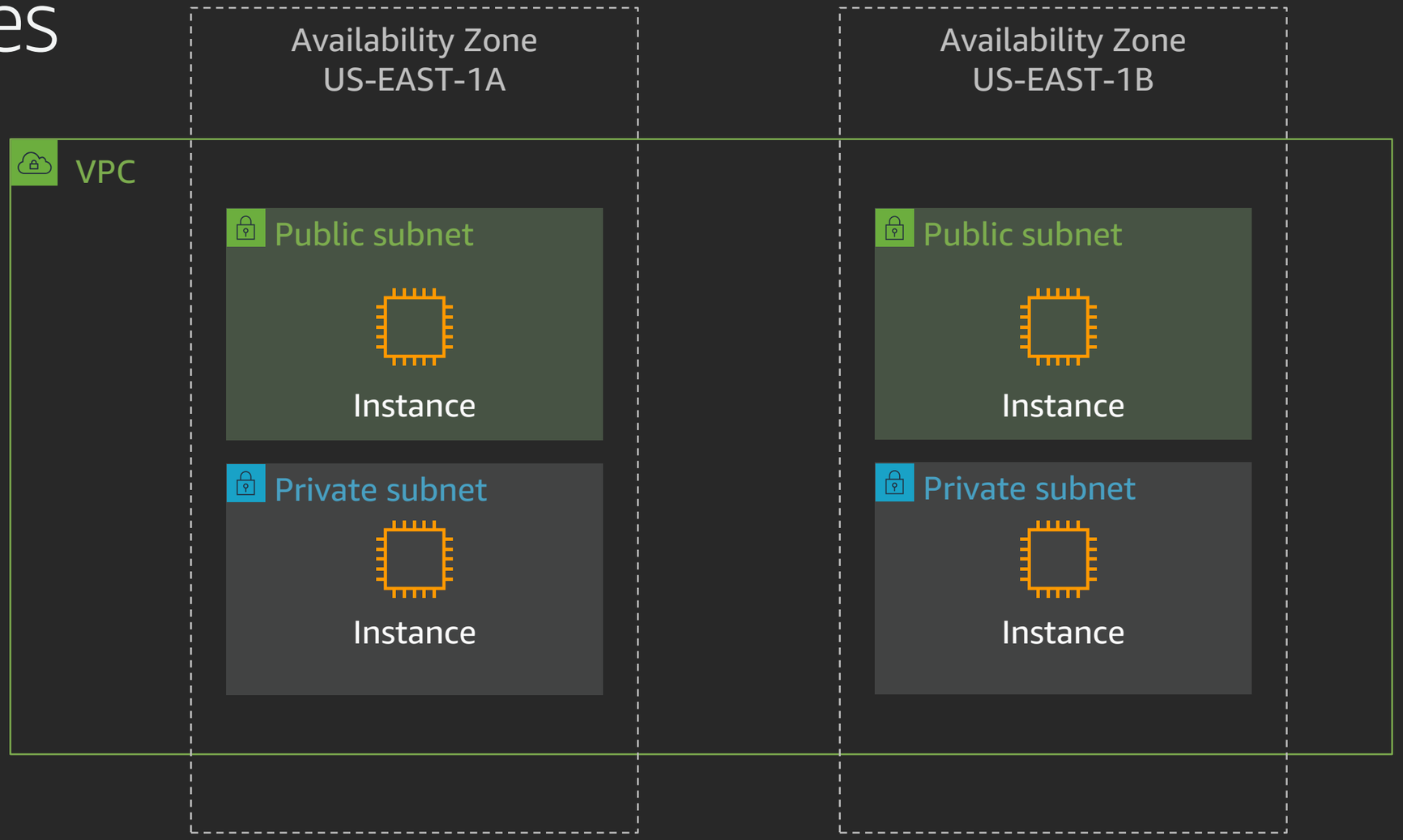

aws
US-EAST-1
Availability Zone
US-EAST-1A
Availability Zone
US-EAST-1B
VPC
Instance
Instance
Instance
Instance

Amazon Virtual Private Cloud (Amazon VPC)

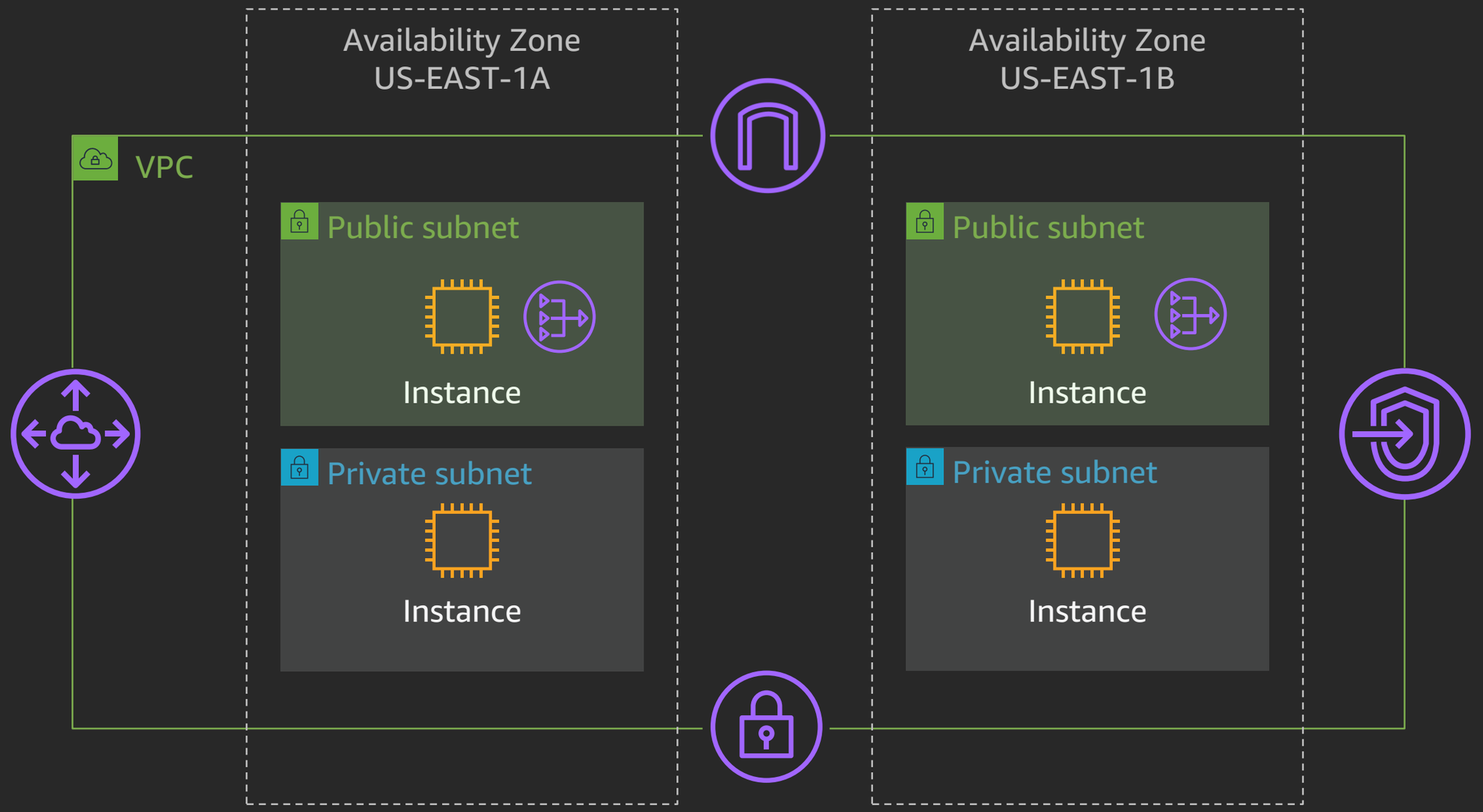
Subnets


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

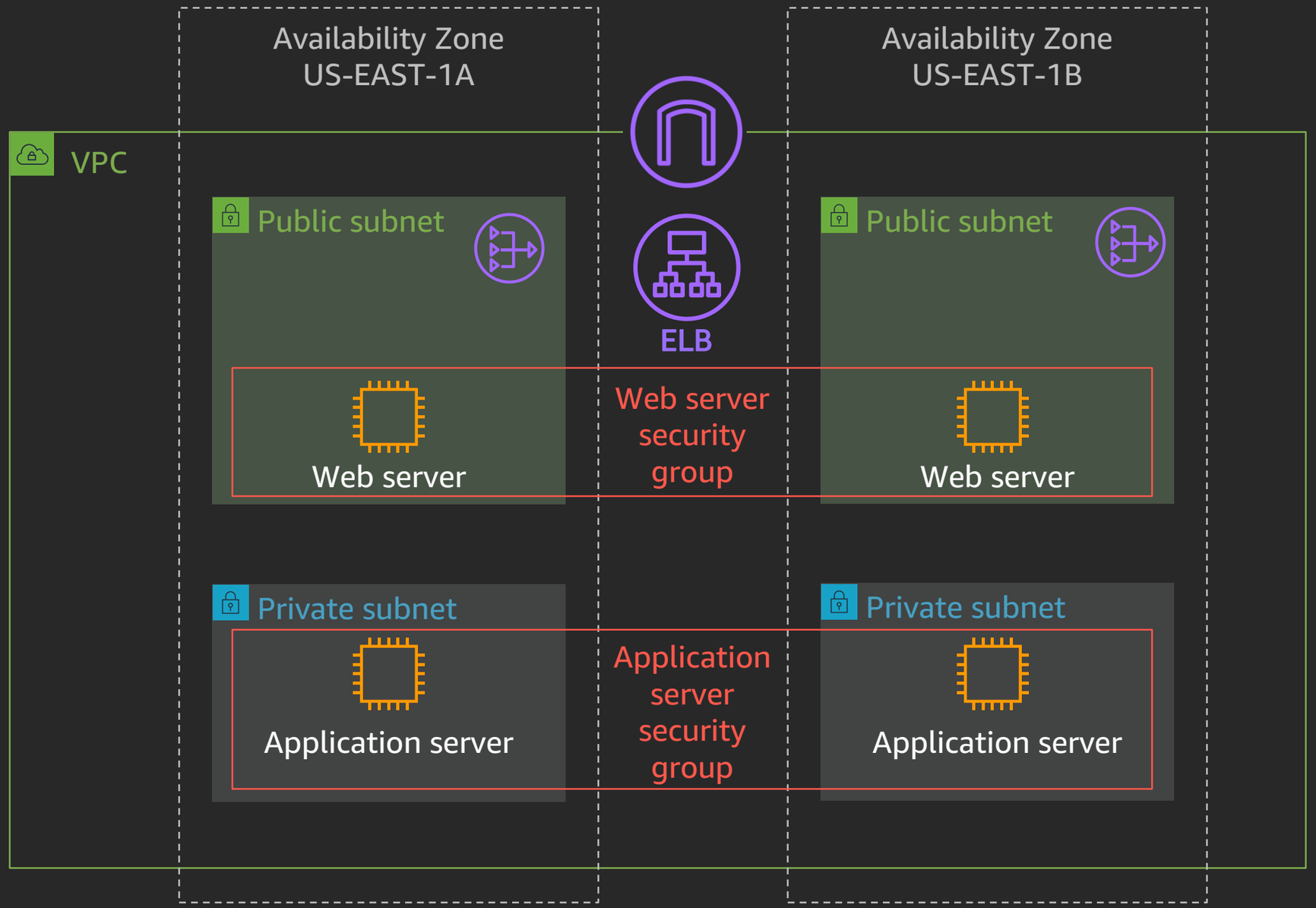
Amazon Elastic Compute Cloud (Amazon EC2) instances



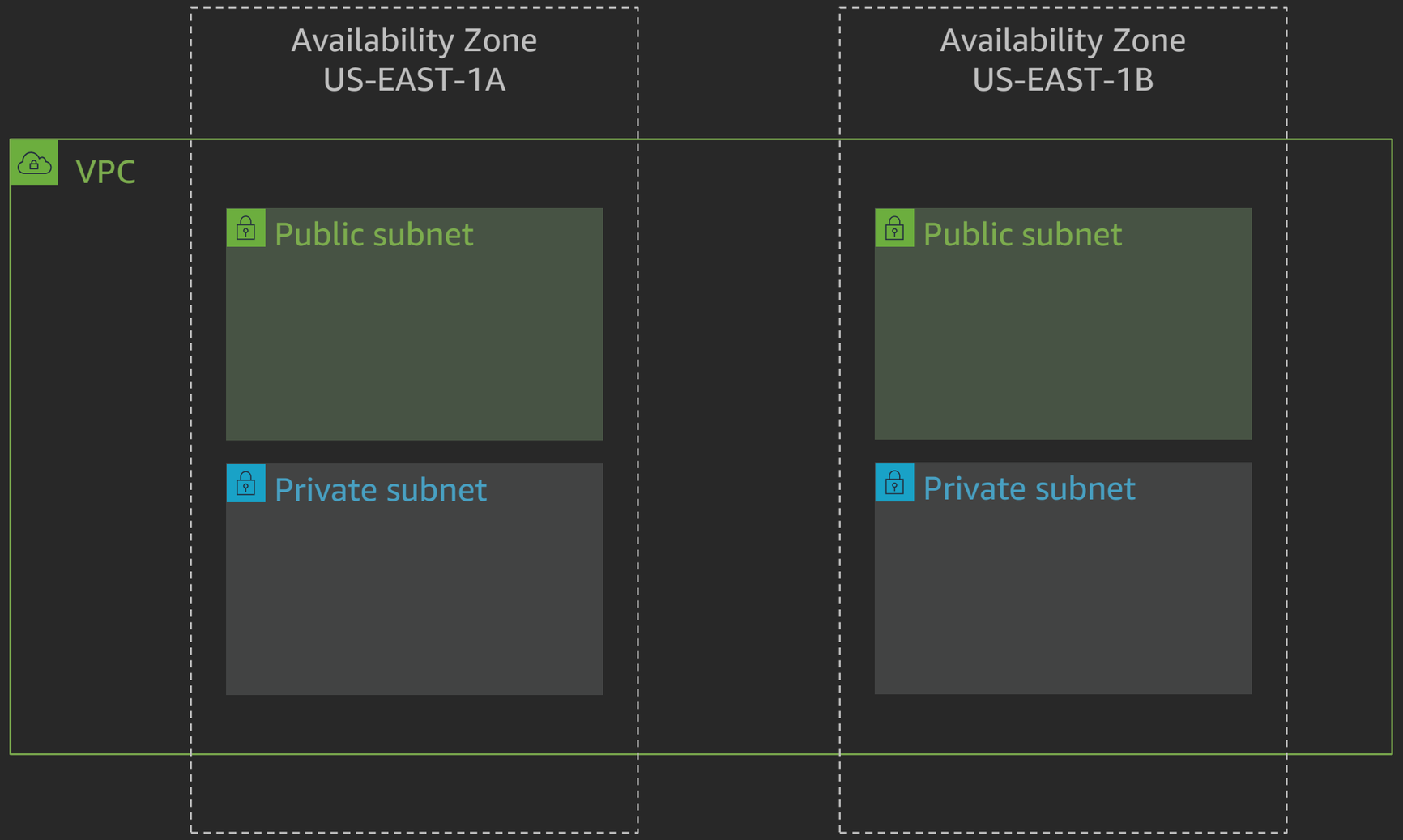
Gateways, endpoints, and peering



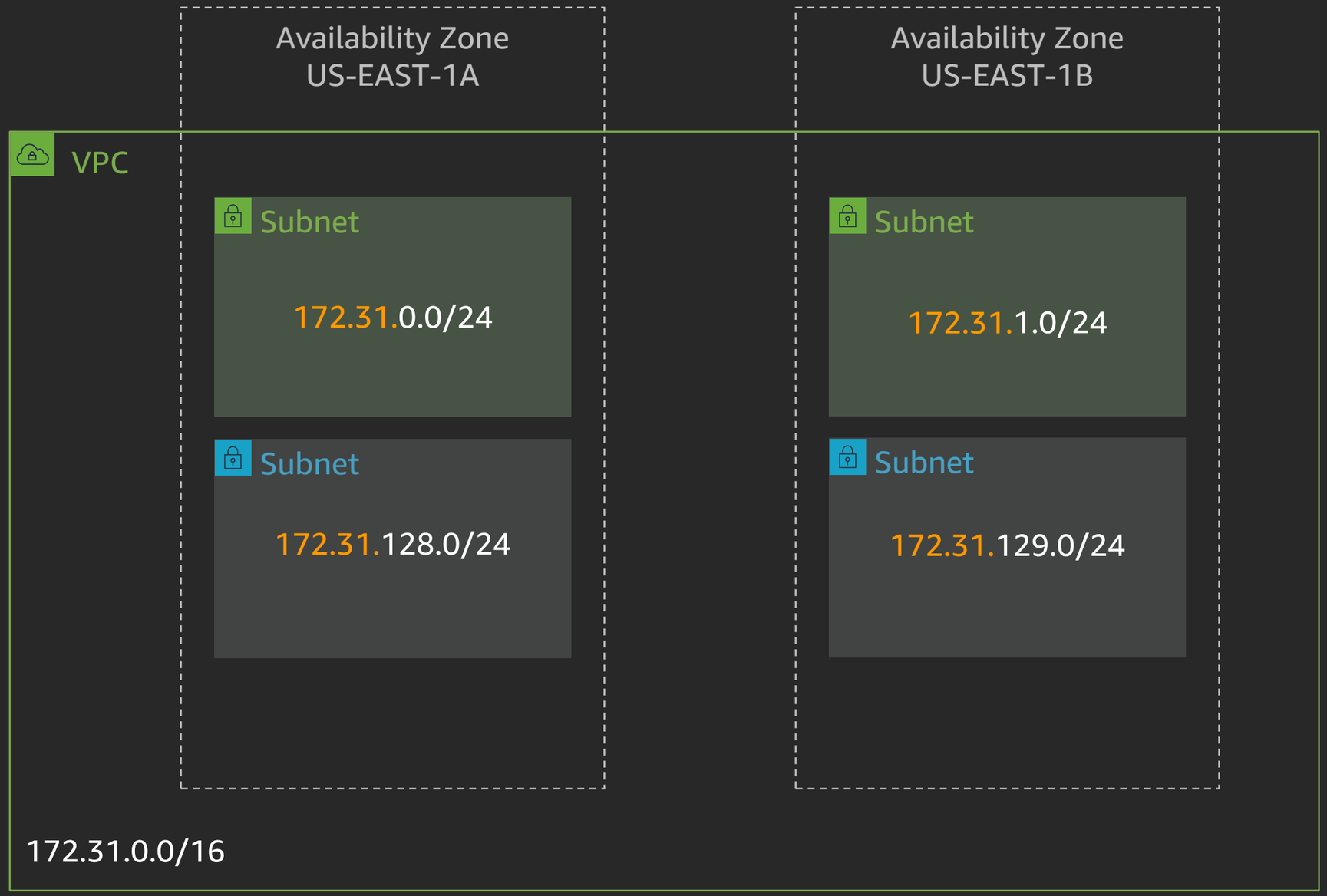
Example web application



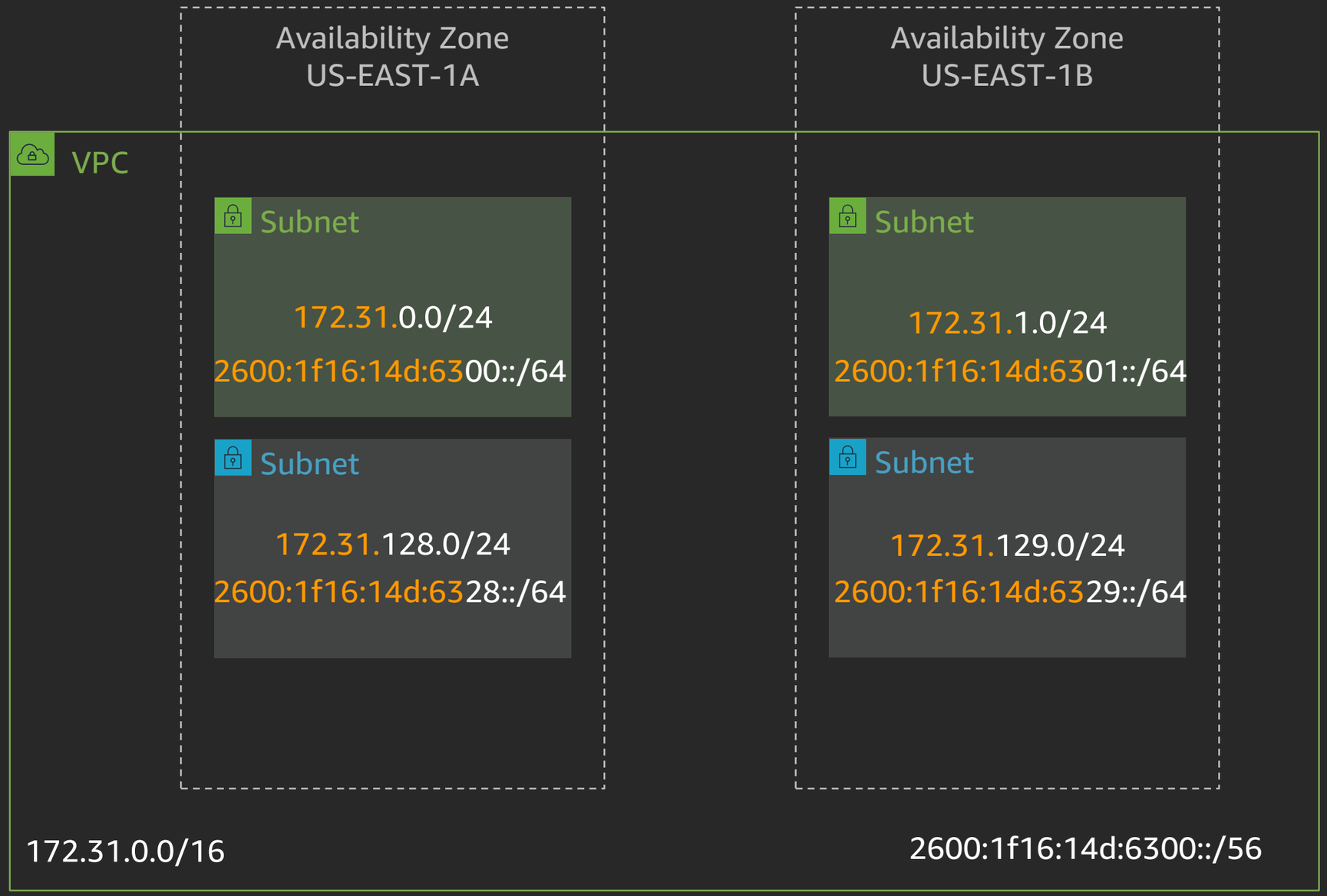
IP addressing



Where to use IPv4 addresses ?



Where to use IPv6 addresses ?

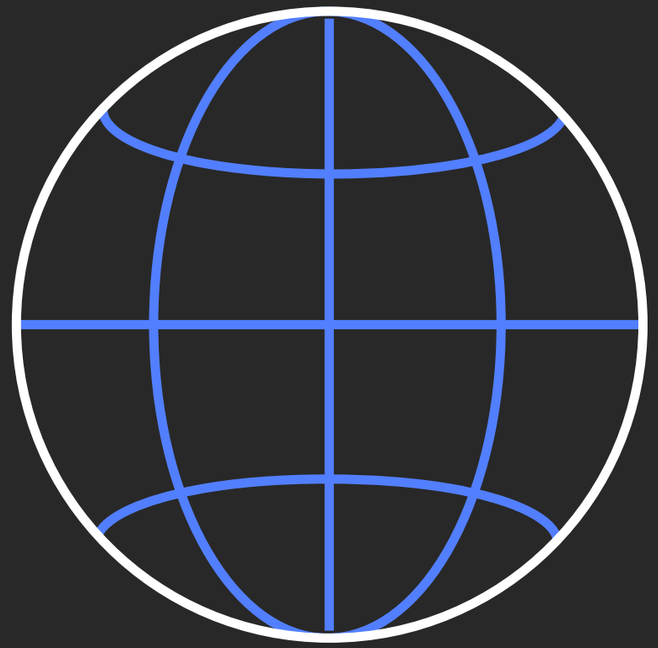


The 5 things required for internet traffic

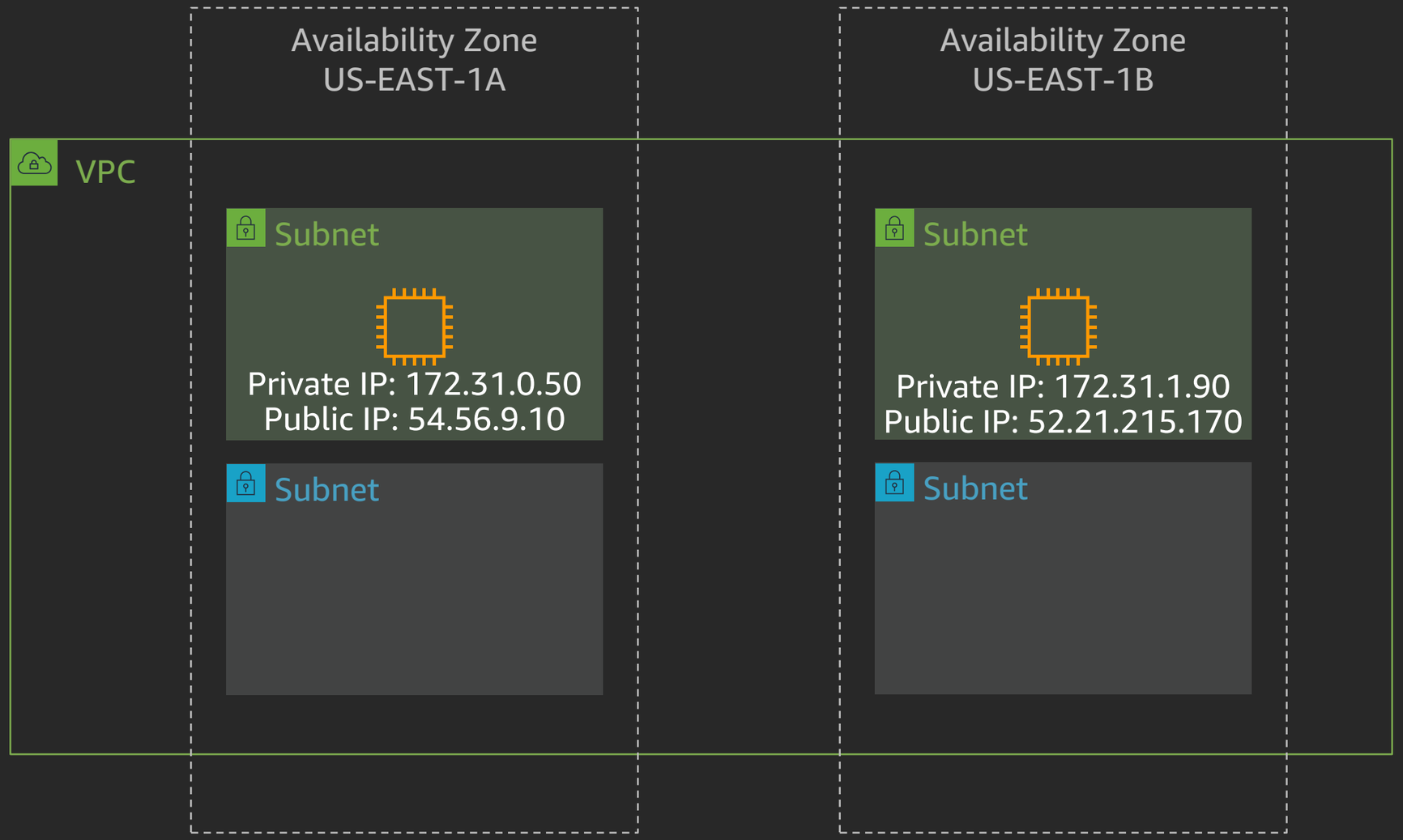
1. Public IP address
2. Internet gateway attached to a VPC
3. Route to an internet gateway
4. Network access control list (ACL) allow rule
5. Security group allow rule

Public IP addresses for your instances

- Auto-assign public IP addresses
- Elastic IP addresses
  - Amazon Elastic IP address pool
  - Bring Your Own IP (BYOIP) pool



Public IP addresses



Gateways, endpoints, and peering

Internet access

172.16.0.0
172.16.1.0
172.16.2.0

Create internet gateway | Actions

Filter by tags and attributes or search by keyword

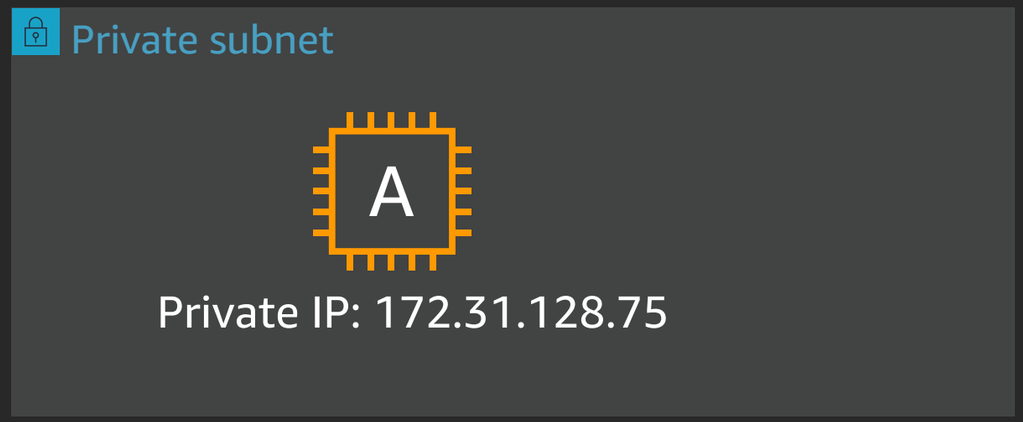
Name	ID	State	VPC
	igw-09ef761d872b…	attached	vpc-0bcb5110cf0c…

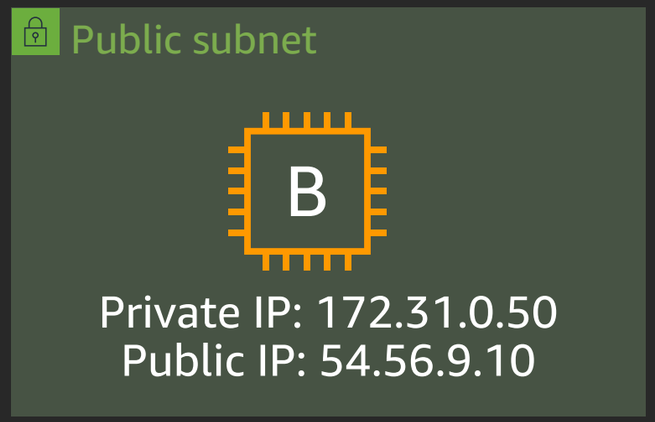
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09ef761d872bd7540	Active	No
::/0	igw-09ef761d872bd7540	Active	No

"To get to the IPv4 internet (0.0.0.0/0), go via the internet gateway"

"To get to the IPv6 internet (::/0), go via the internet gateway"

Public and private subnets





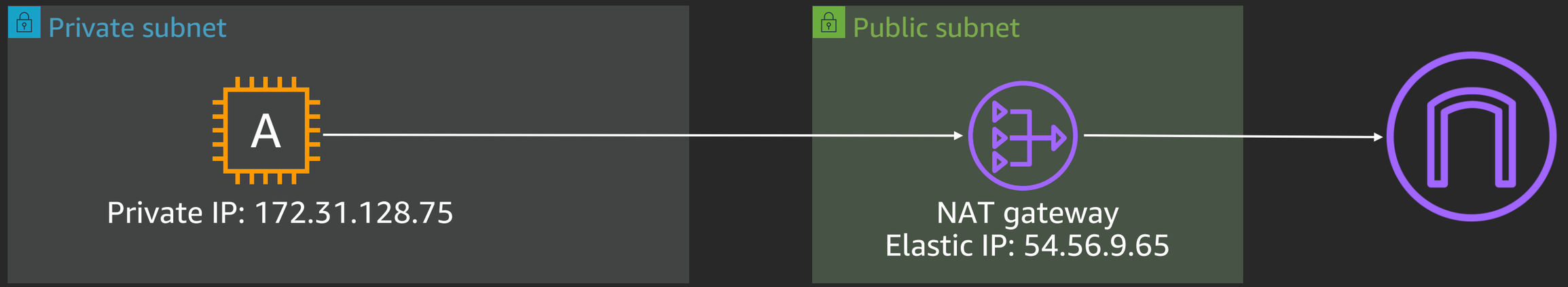
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No

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



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

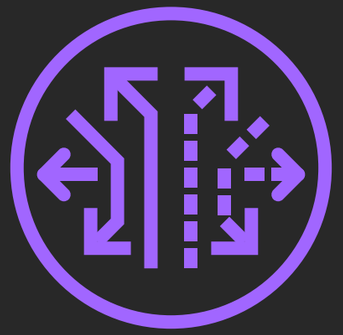
The route table for the public subnet says to send all internet traffic to the internet gateway

Network security

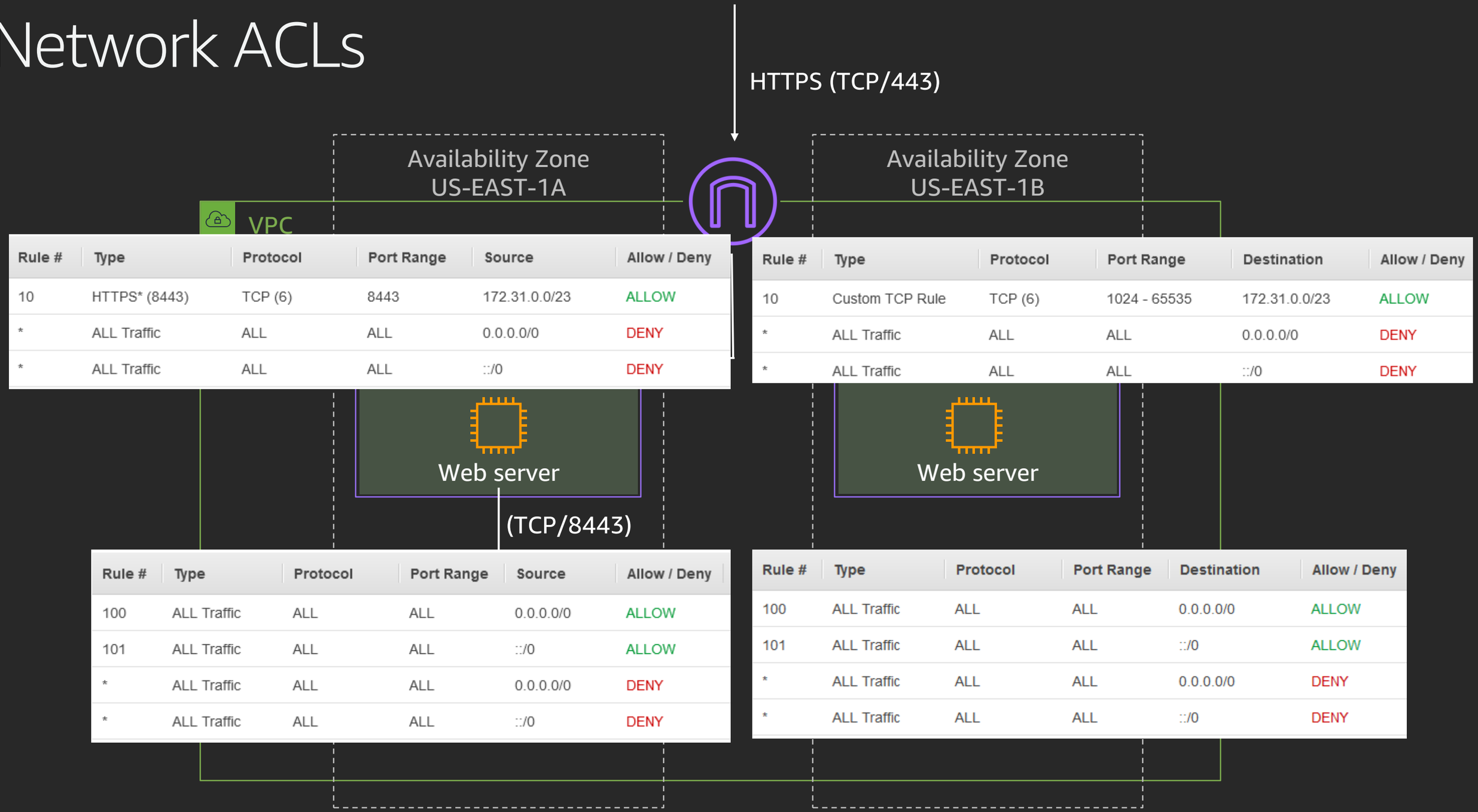
Network security

- Network ACLs
- Security groups
- VPC flow logs
- Amazon VPC Traffic Mirroring





Network ACLs



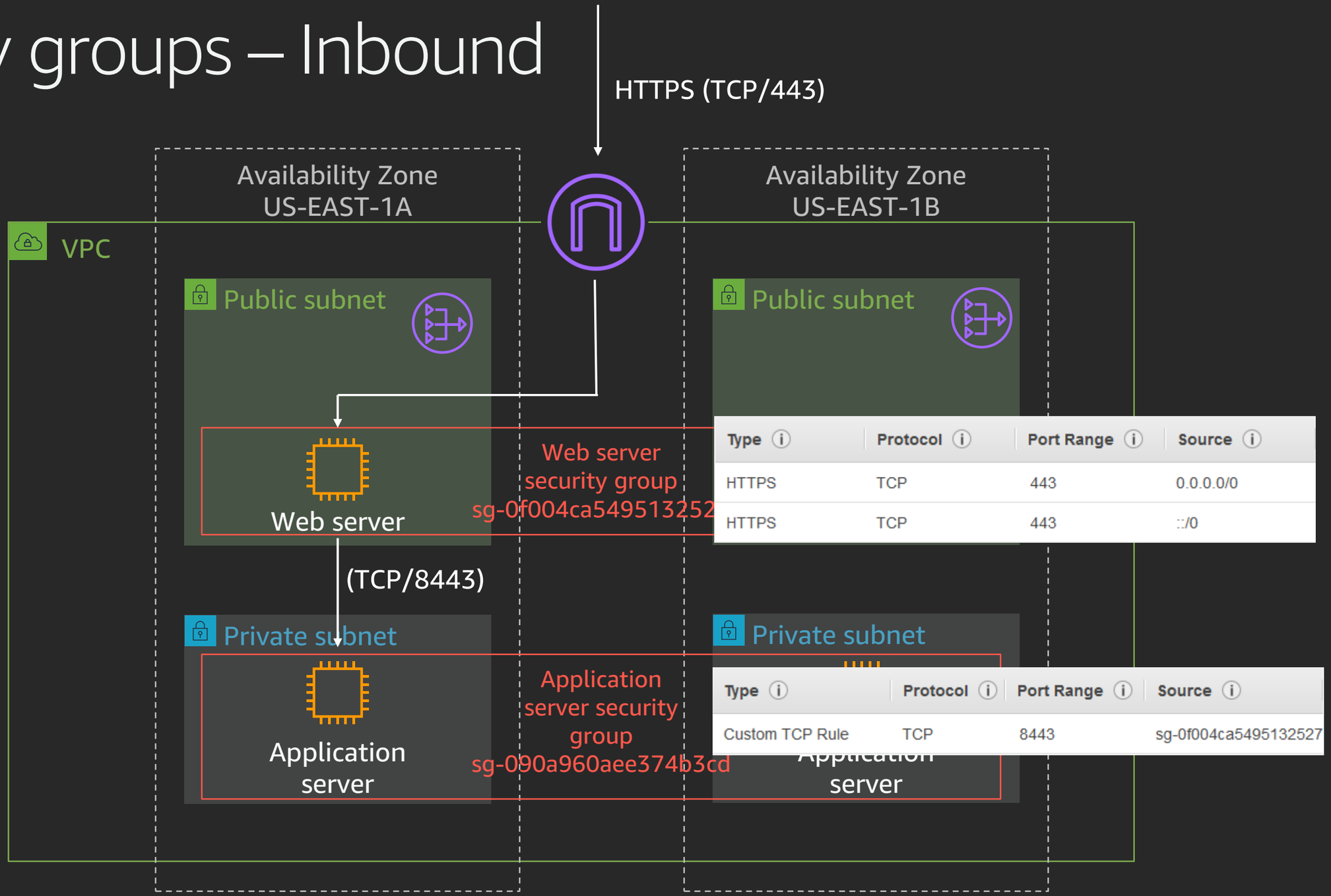
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
10	HTTPS* (8443)	TCP (6)	8443	172.31.0.0/23	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

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

VPC flow logs

- Amazon CloudWatch Logs or Amazon S3
- Does not impact throughput or latency
- Apply to VPC, subnet, or elastic network interface
- Accepted, rejected, or all traffic

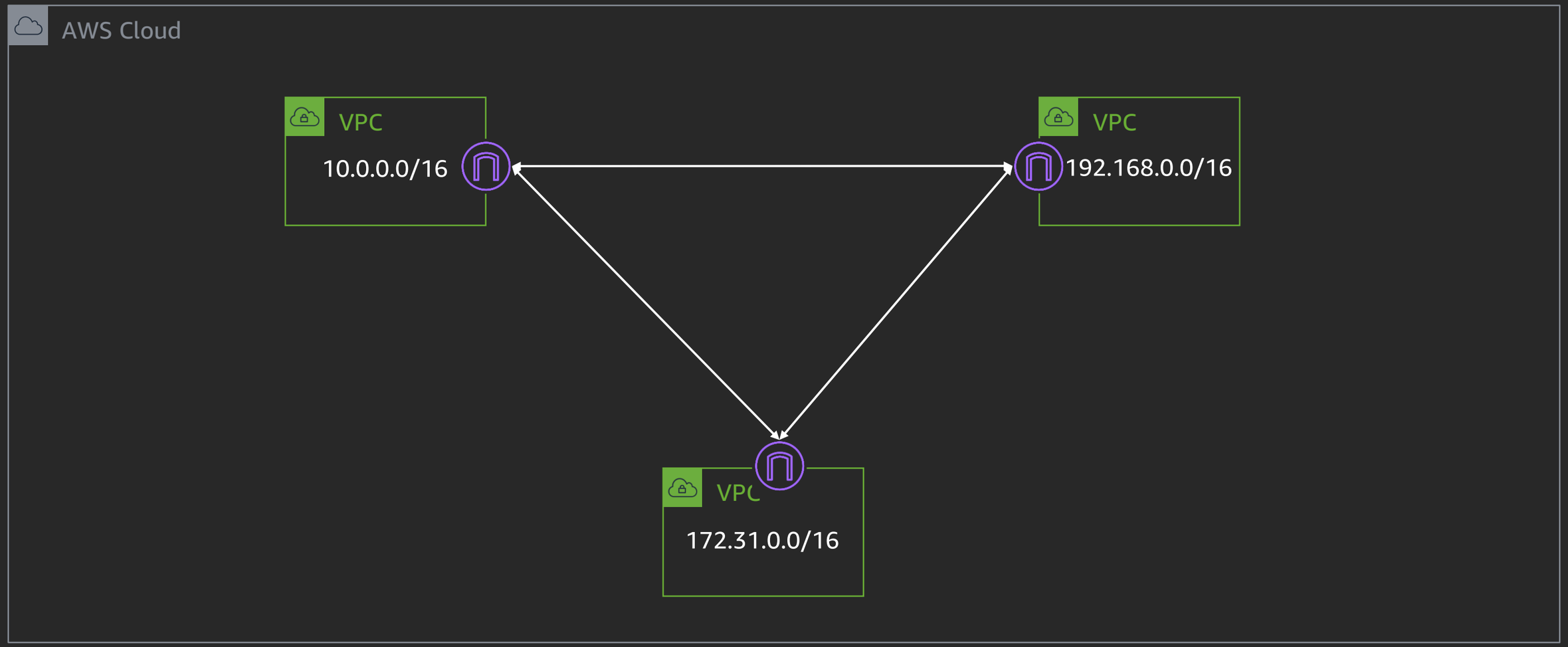
version	3
account-id	384767312345
interface-id	eni-0b62d5e000e412345
srcaddr	108.56.192.231
dstaddr	172.31.0.202
srcport	50565
dstport	80
protocol	6
packets	7
bytes	751
start	1573704396
end	1573704455
action	ACCEPT
log-status	OK
vpc-id	vpc-0af48868ceeb12345
subnet-id	subnet-02ab634d2e4c12345
instance-id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

Amazon VPC Traffic Mirroring

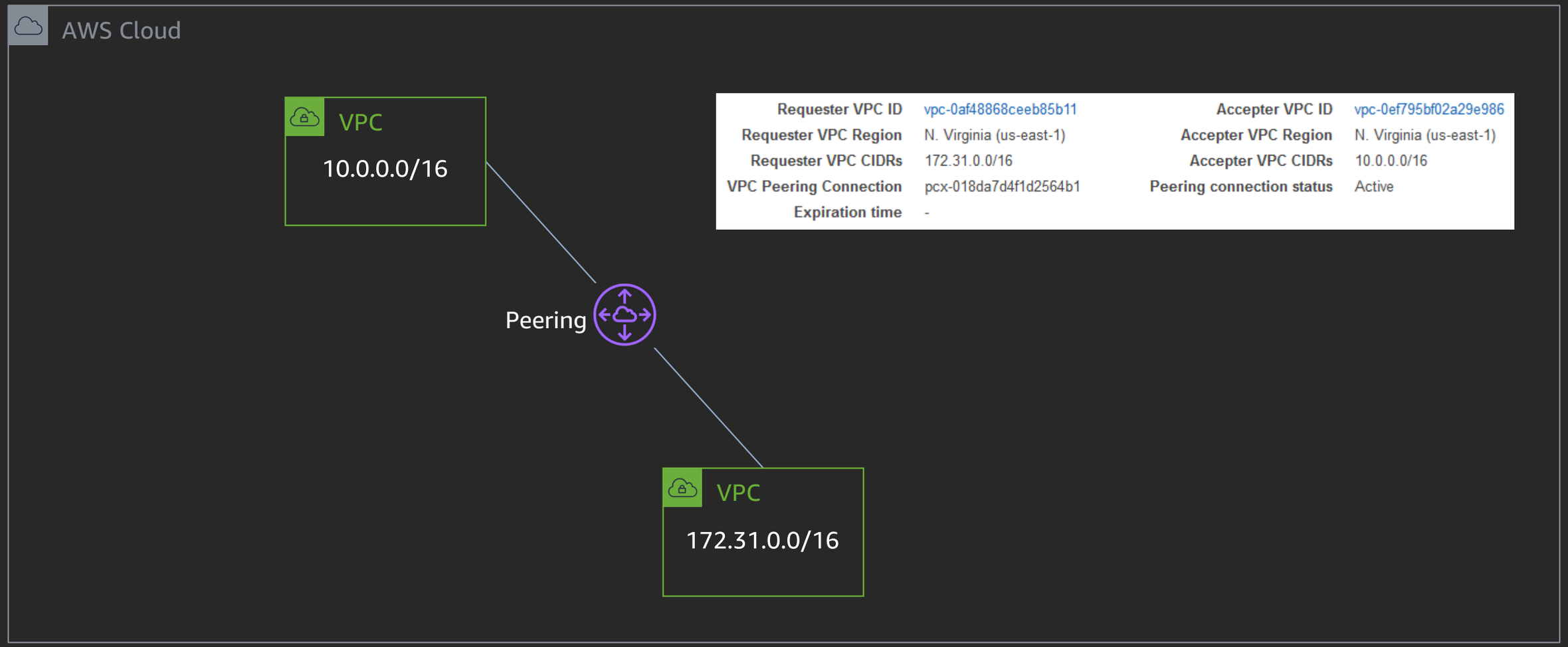
- Mirror to another elastic network interface or Network Load Balancer with UDP listener
- Packet copy – shares interface bandwidth
- Traffic mirror filters to define interesting traffic
- Traffic mirror session is the combination of source, target, and filter

Connecting to other VPCs

Connecting between VPCs

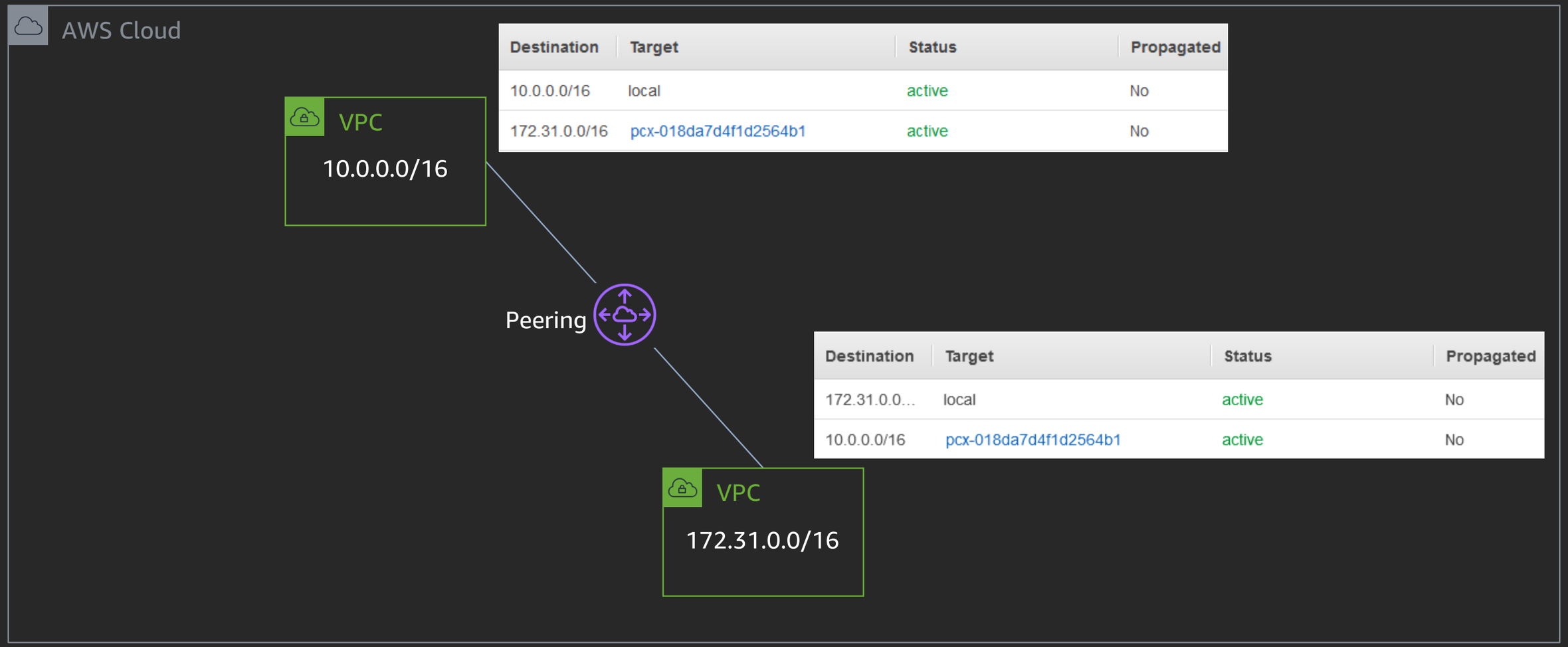


VPC peering



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	-		

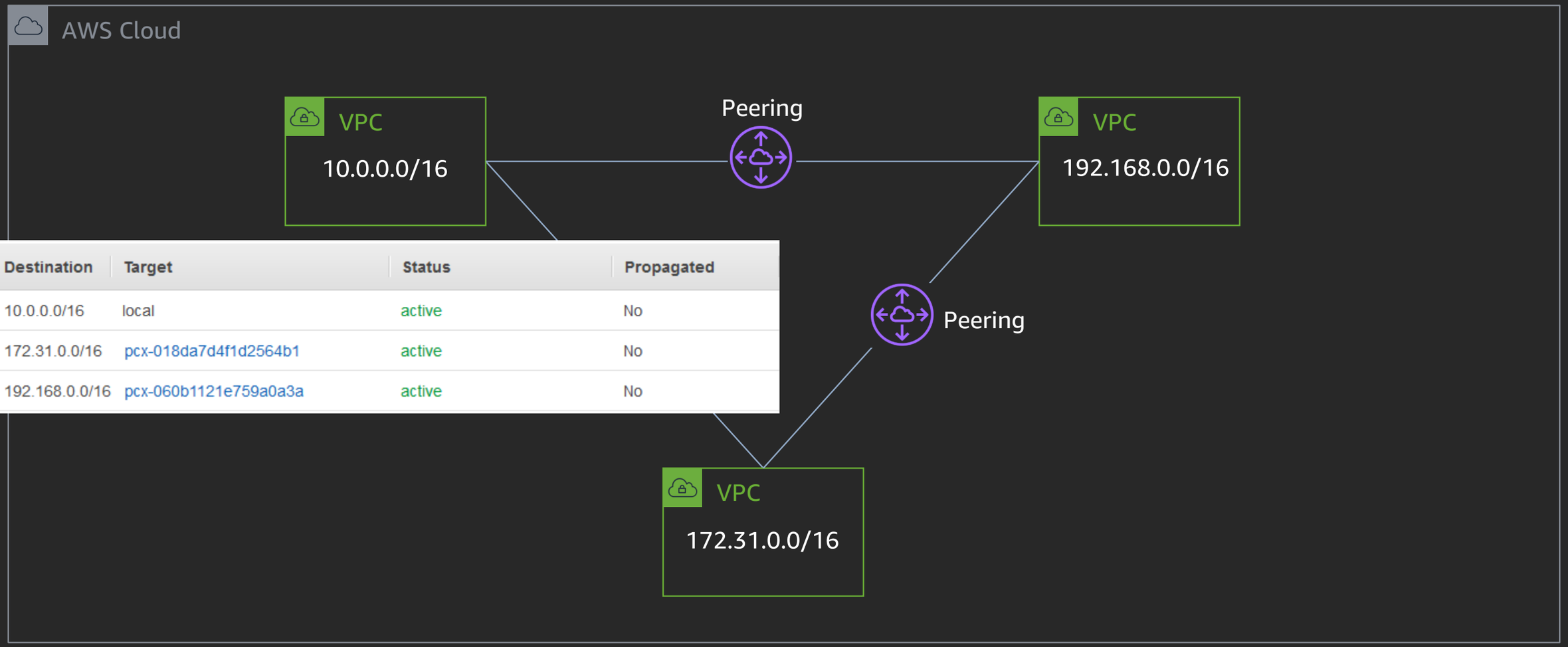
VPC peering



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

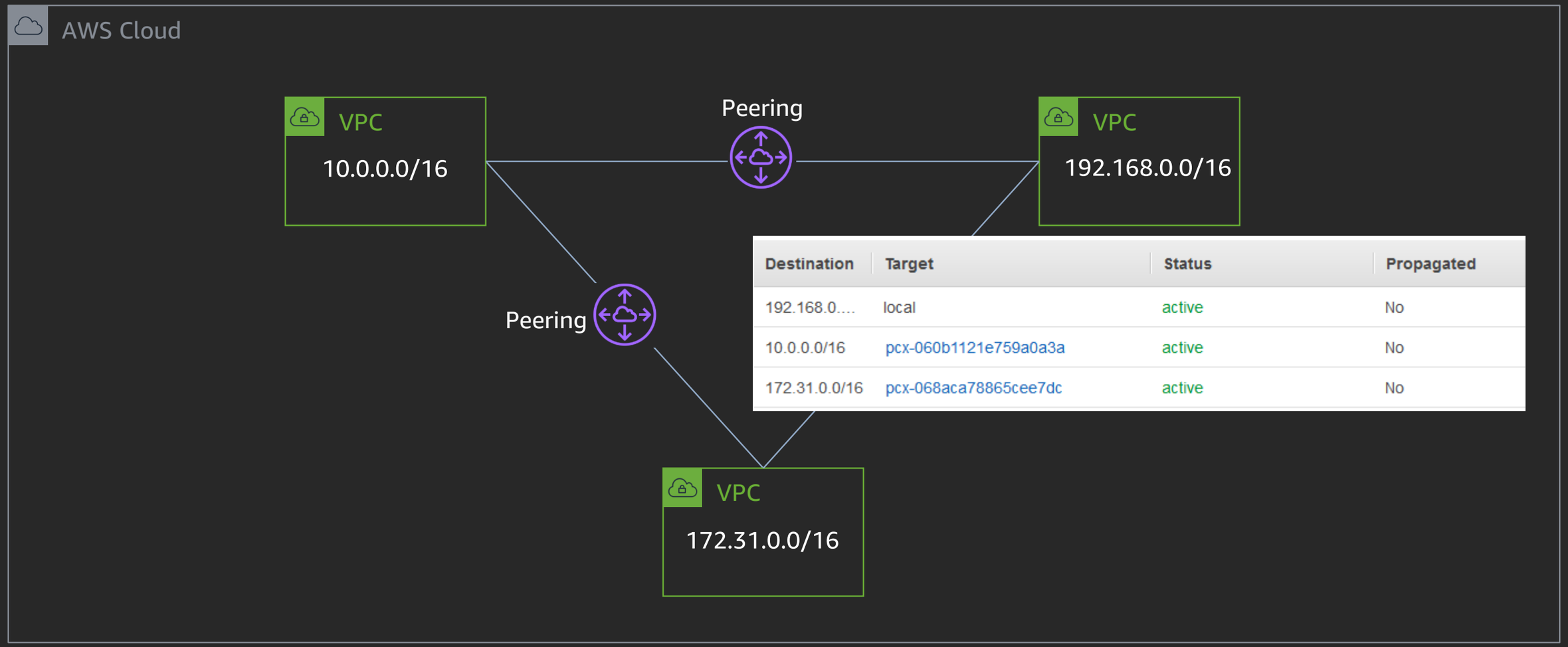
Destination	Target	Status	Propagated
172.31.0.0...	local	active	No
10.0.0.0/16	pcx-018da7d4f1d2564b1	active	No

VPC peering



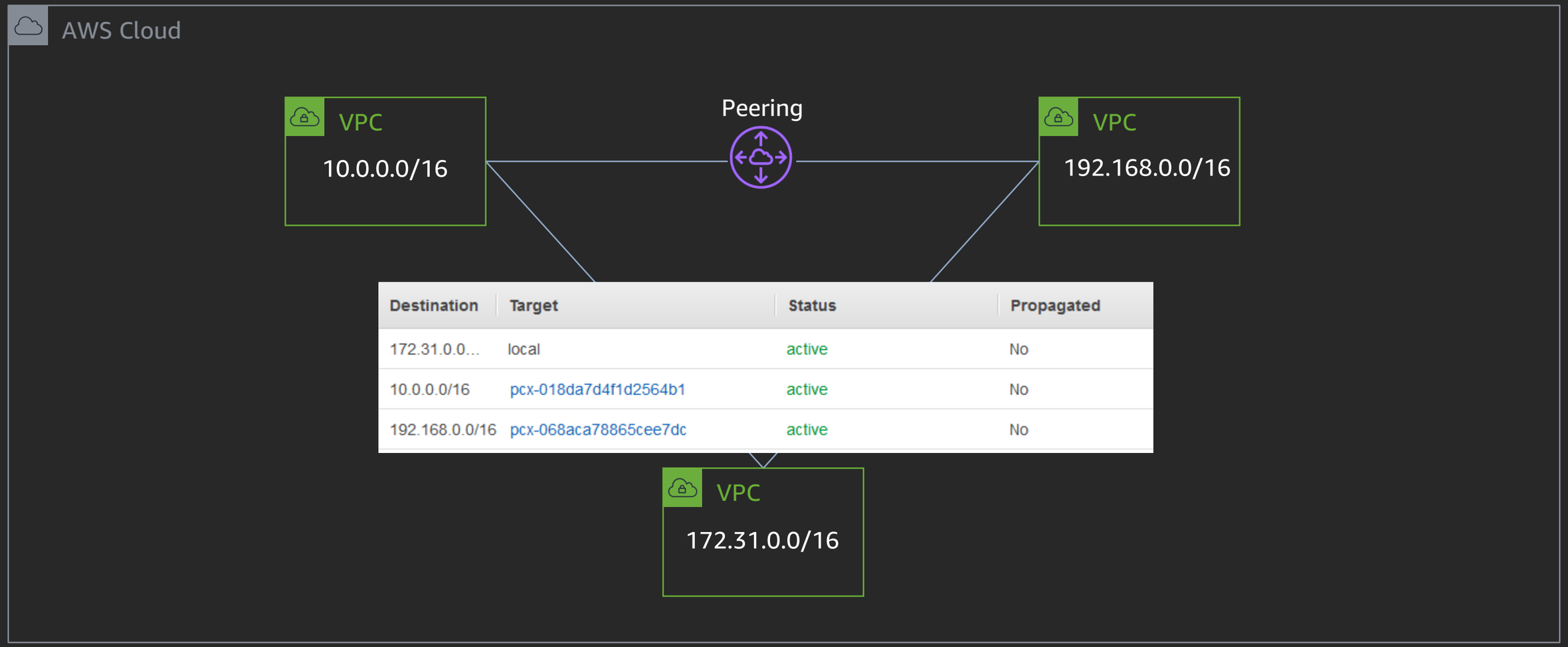
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
172.31.0.0/16	pcx-018da7d4f1d2564b1	active	No
192.168.0.0/16	pcx-060b1121e759a0a3a	active	No

VPC peering



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



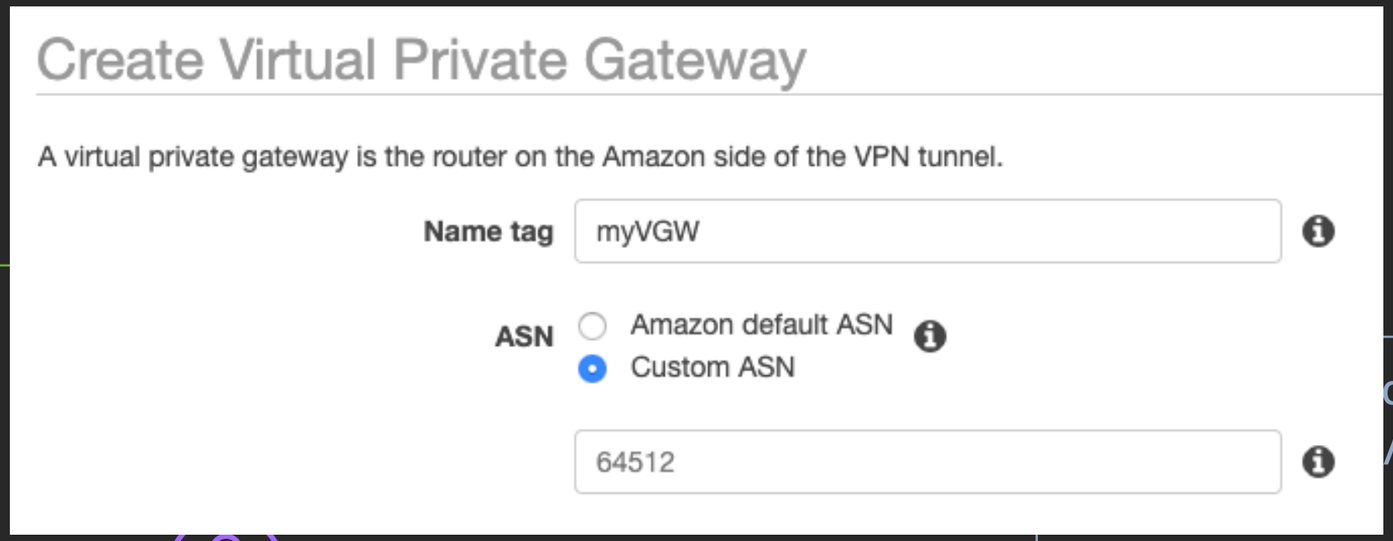
Destination	Target	Status	Propagated
172.31.0.0...	local	active	No
10.0.0.0/16	pcx-018da7d4f1d2564b1	active	No
192.168.0.0/16	pcx-068aca78865cee7dc	active	No

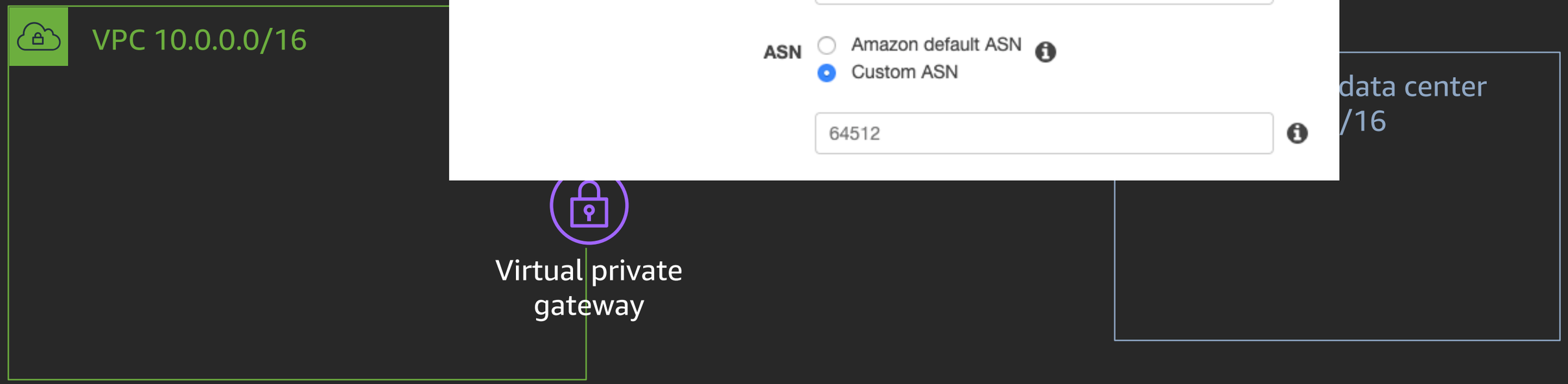
VPC peering – Things to know

- 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 and 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





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

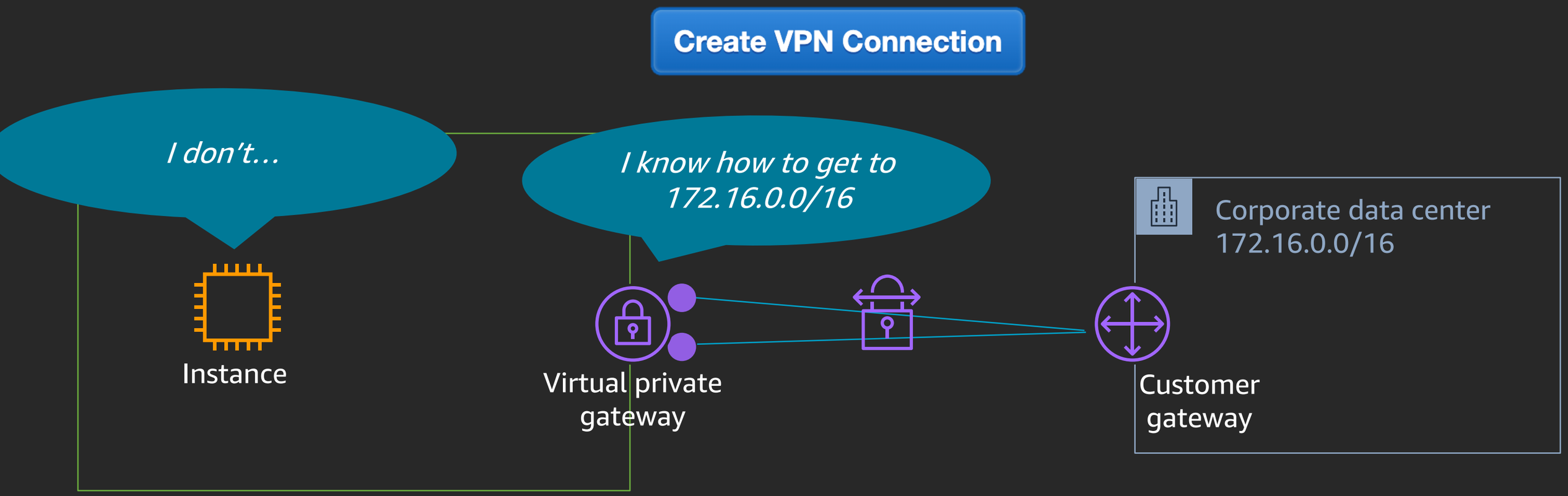
Certificate ARN arn:aws:acm:us

IP address not needed when certificate is used

Corporate data center
172.16.0.0/16

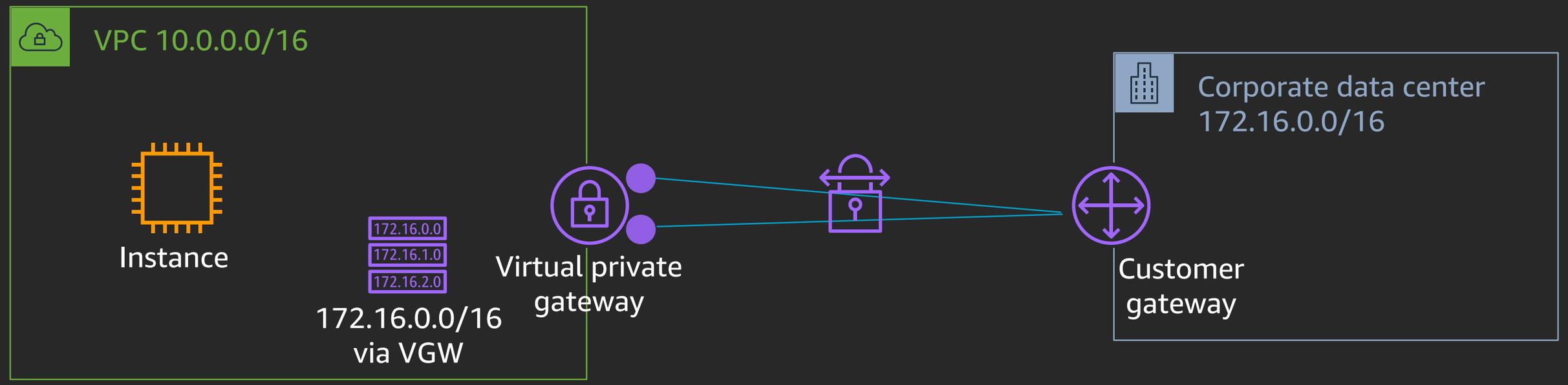
mer
way

AWS Site-to-Site VPN



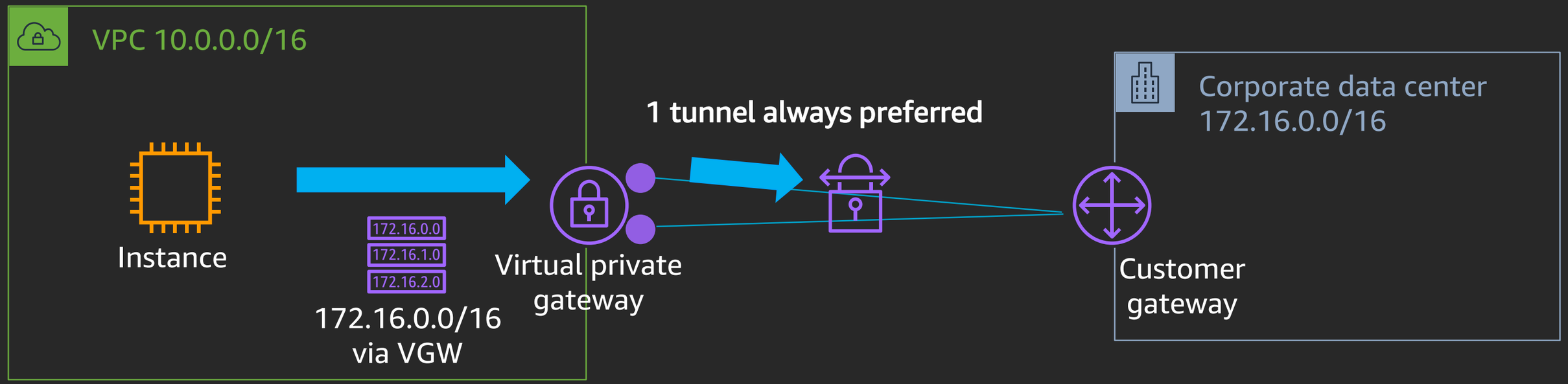
1x VPN connection = 2x VPN tunnels

AWS Site-to-Site VPN



1x VPN connection = 2x VPN tunnels

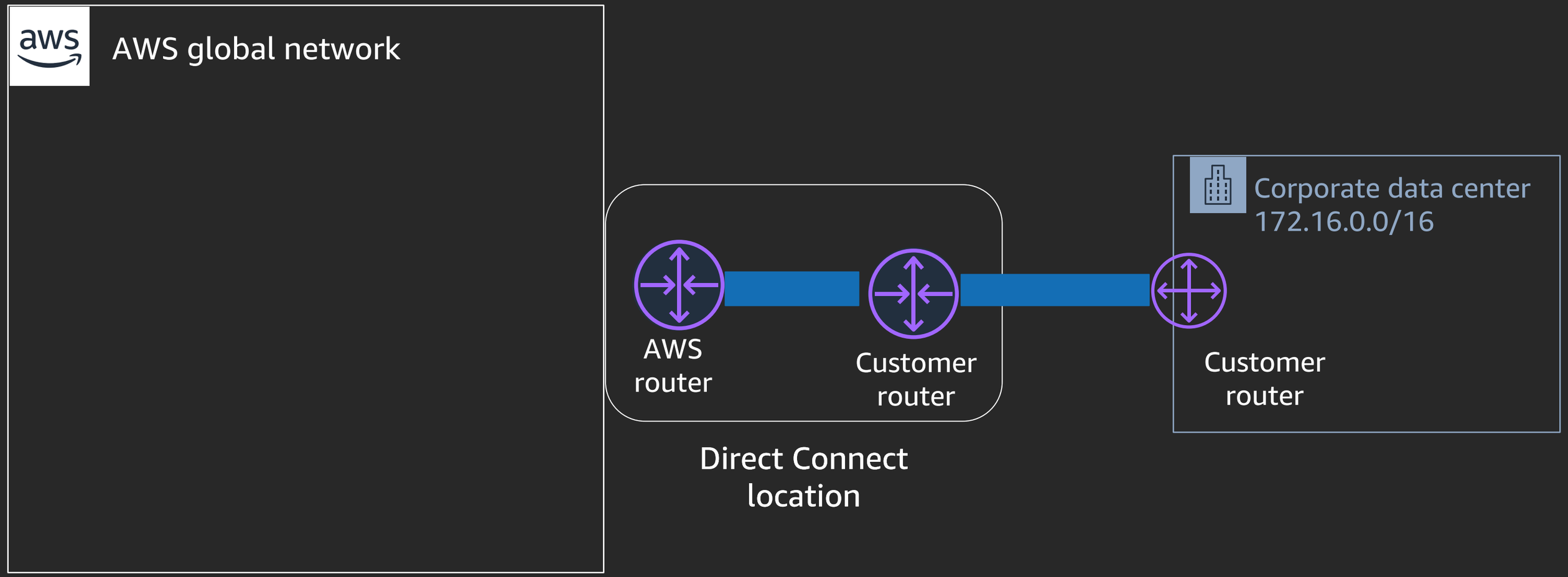
AWS Site-to-Site VPN



1x VPN connection = 2x VPN tunnels

1x VPN tunnel = 1.25 Gbps

AWS Direct Connect – Physical connection

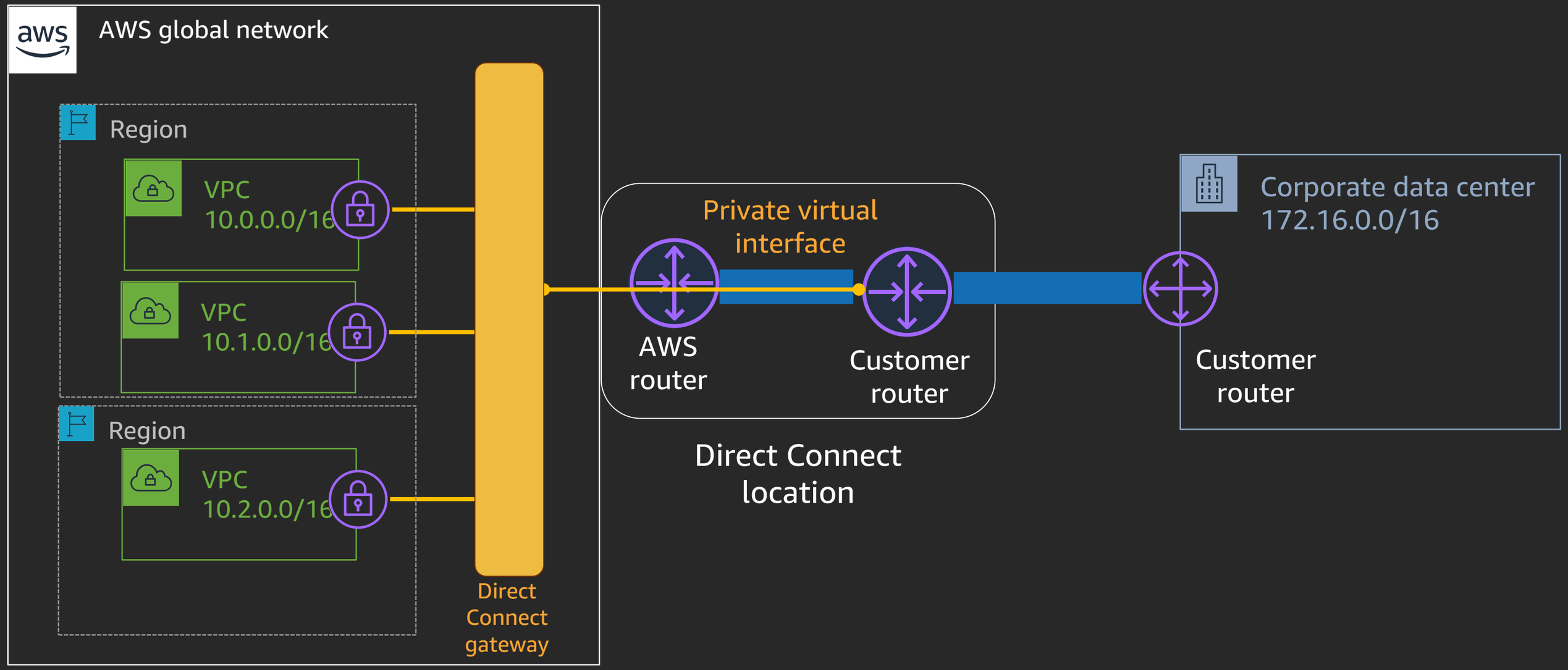


AWS Direct Connect – Interface types

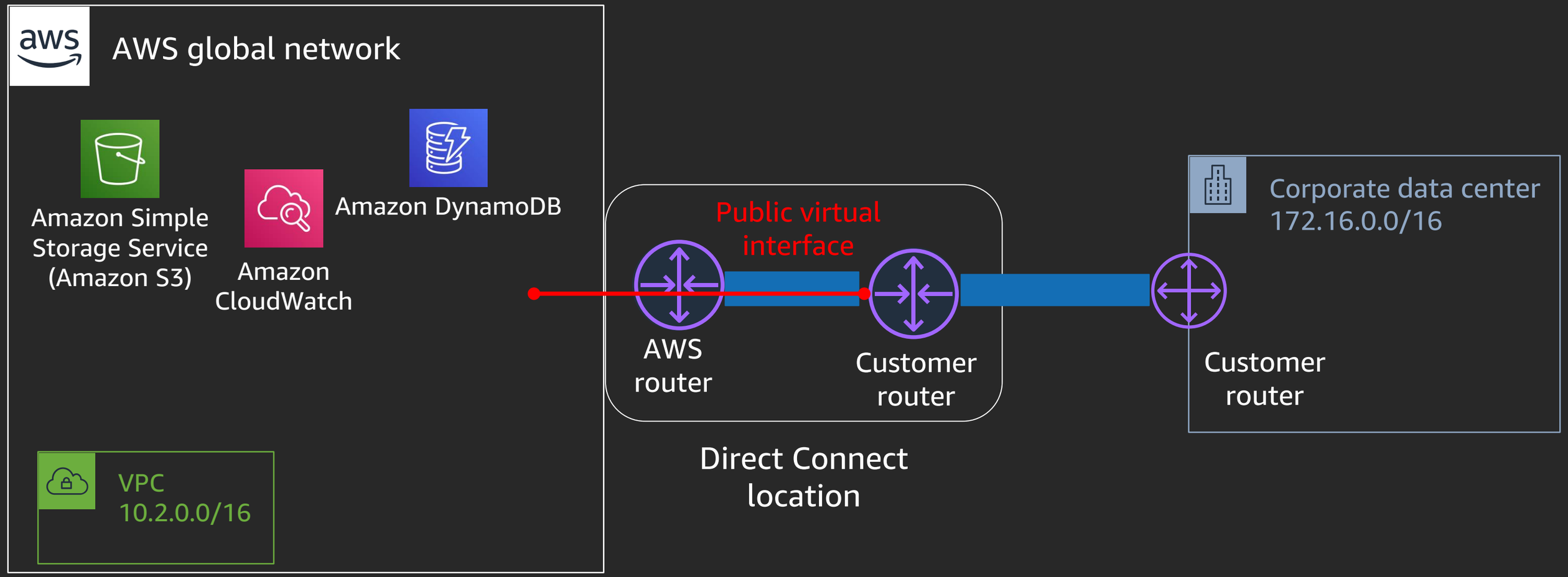
- **Private VIF** – used to connect to Amazon VPCs using private IP addresses; directly or via Direct Connect gateway
- **Transit VIF** – used to connect to AWS transit gateways via Direct Connect gateway
- **Public VIF** – used to access all AWS public services using public IP addresses

All virtual interfaces are 802.1Q VLANs with BGP peering

AWS Direct Connect gateway – Private VIF

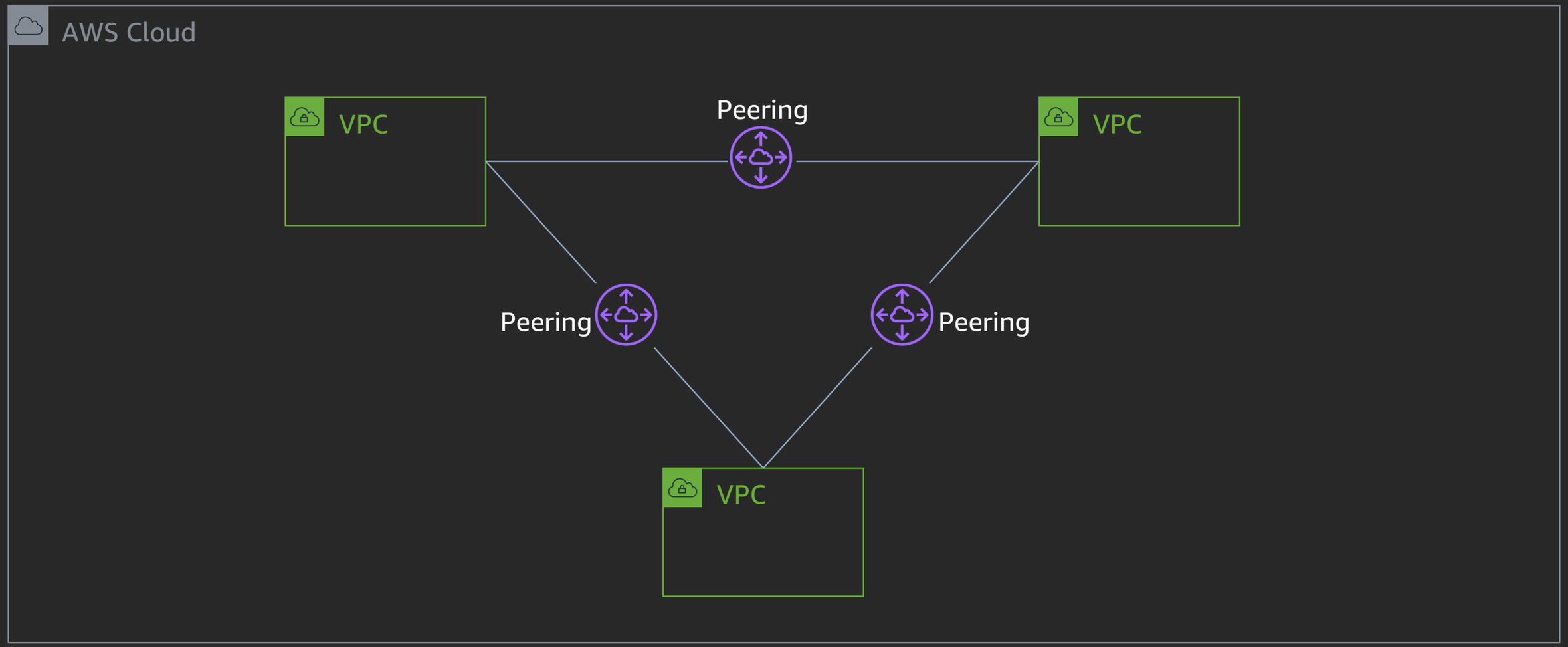


AWS Direct Connect – Public VIF

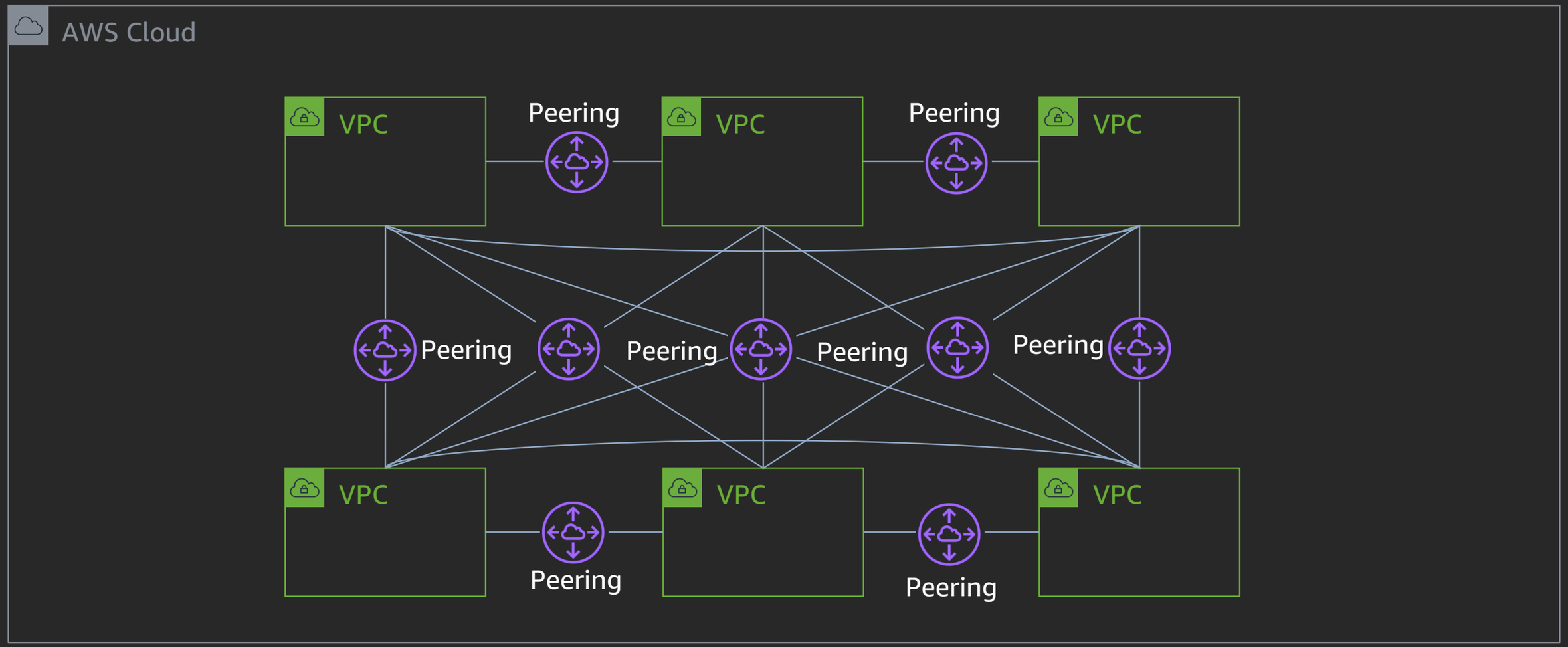


AWS Transit Gateway

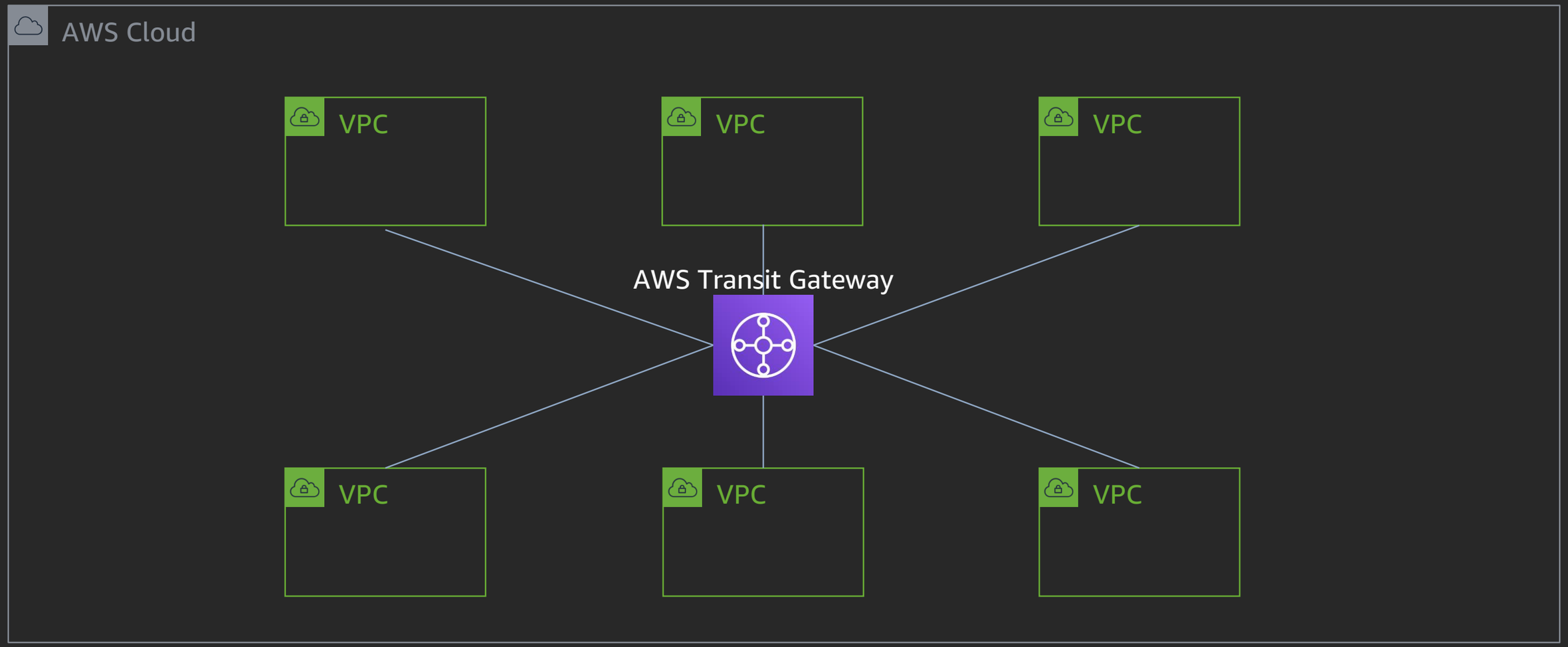
Interconnecting VPCs at scale – VPC peering



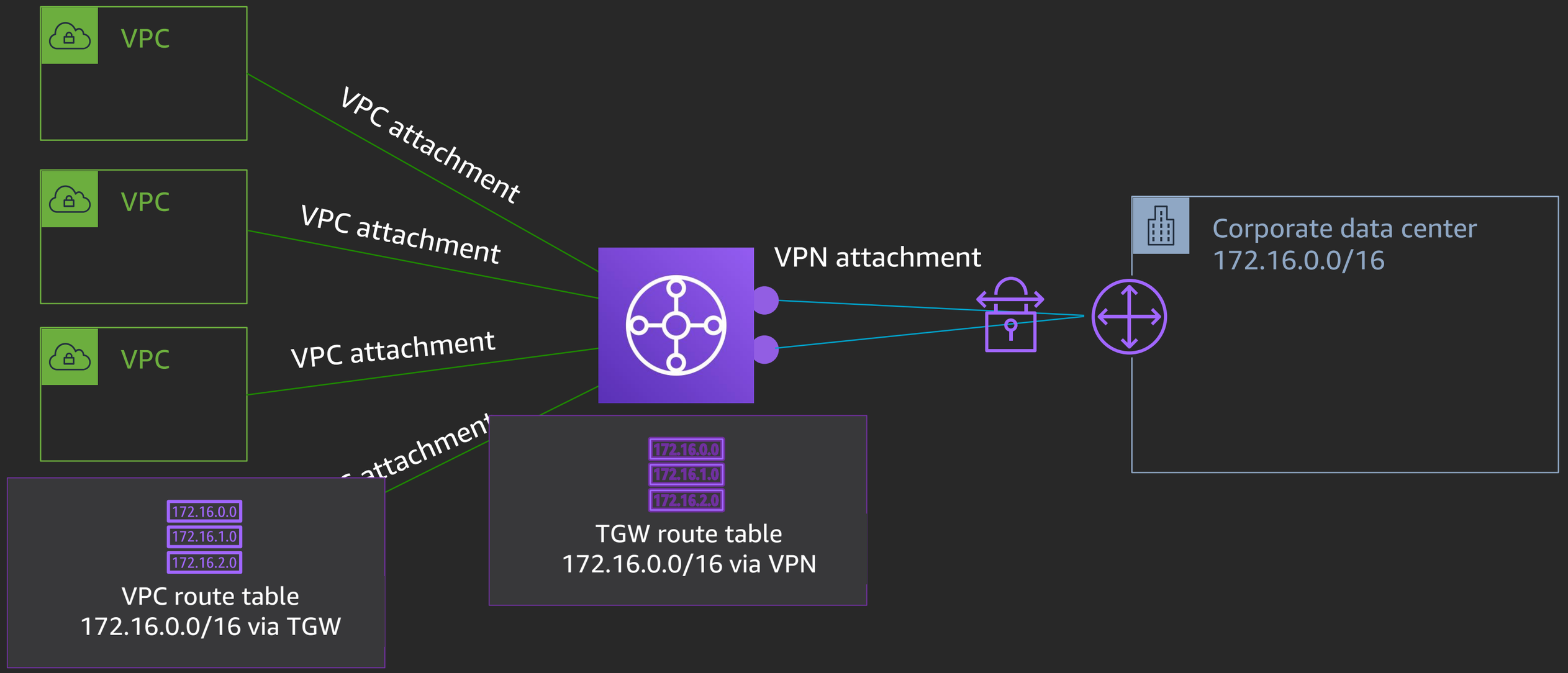
Interconnecting VPCs at scale – VPC peering



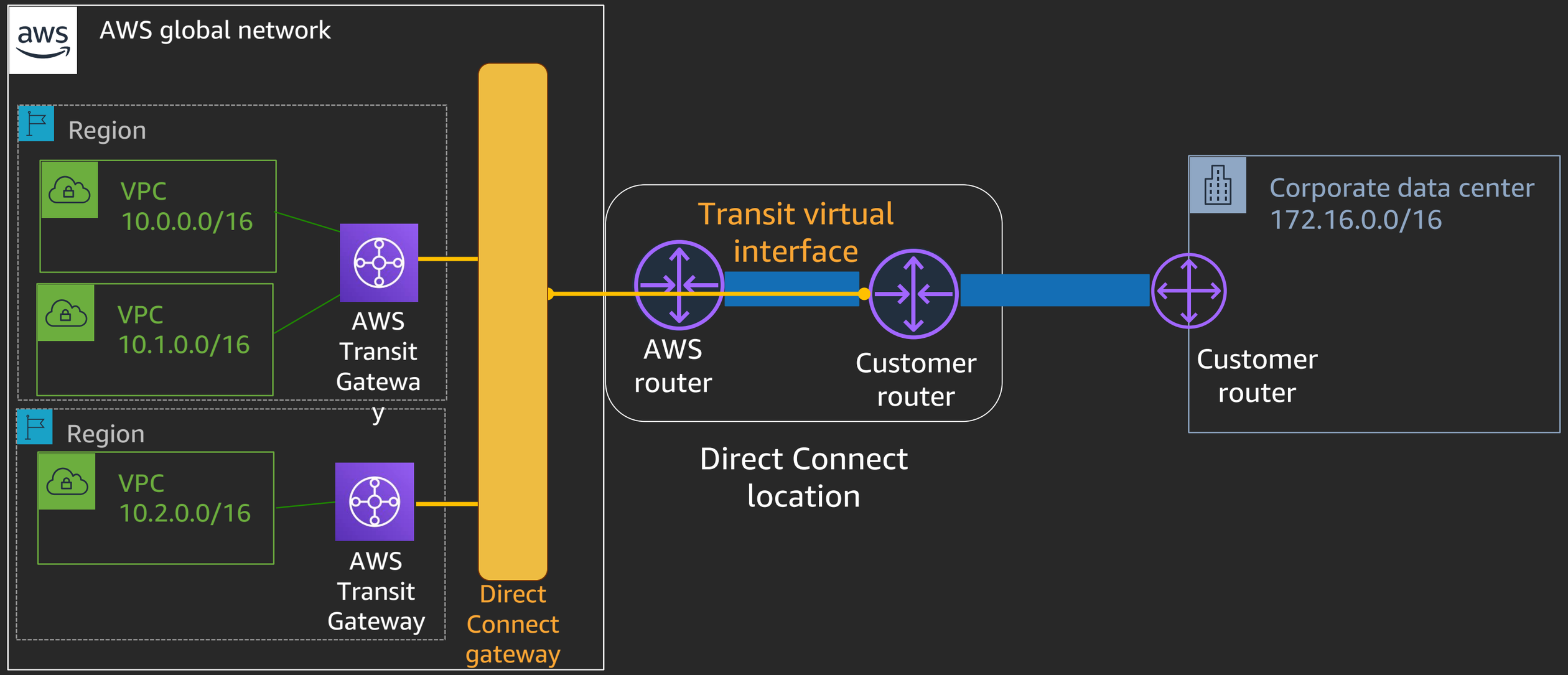
Multiple VPCs access models – AWS Transit Gateway



AWS Transit Gateway with AWS Site-to-Site VPN

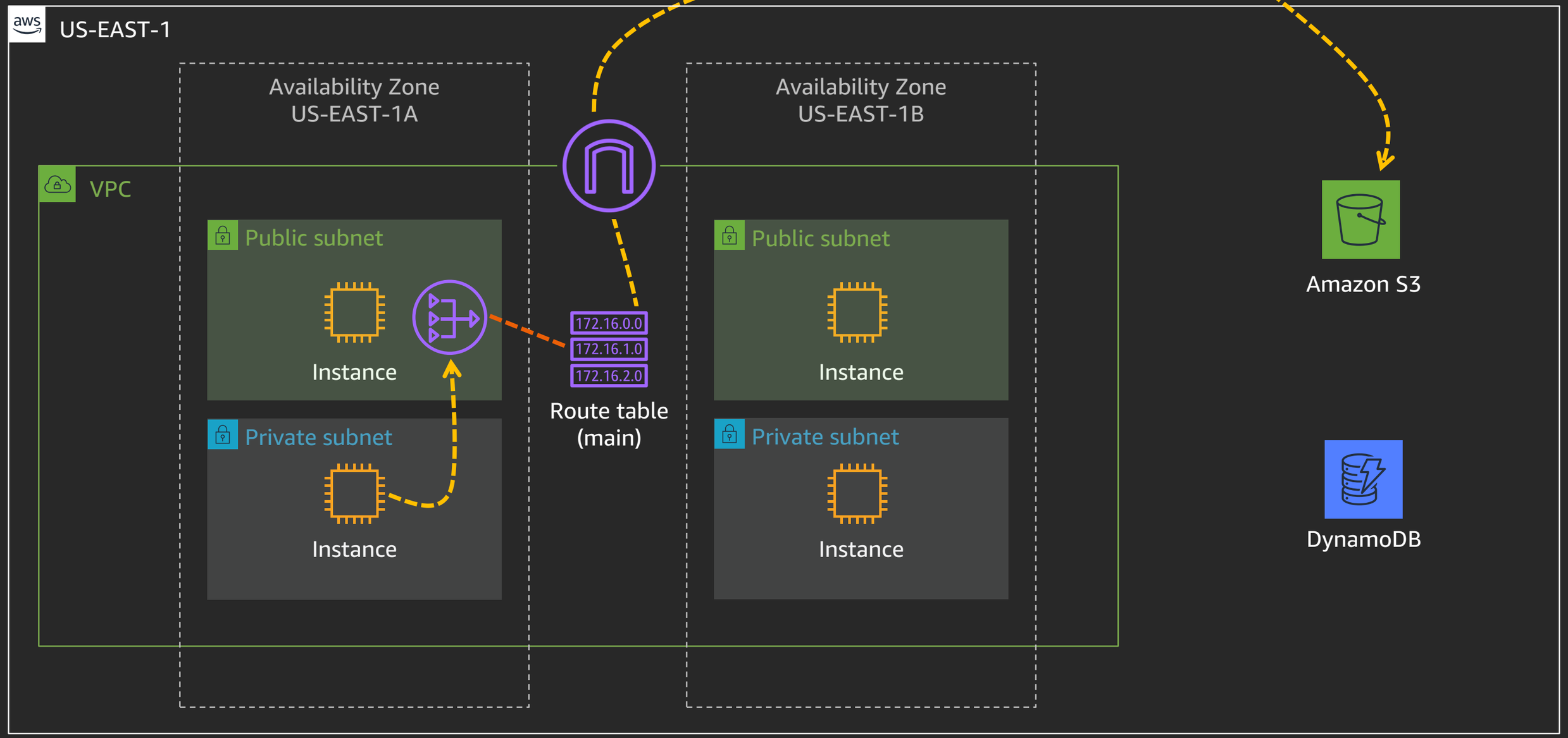


AWS Transit Gateway with Direct Connect gateway

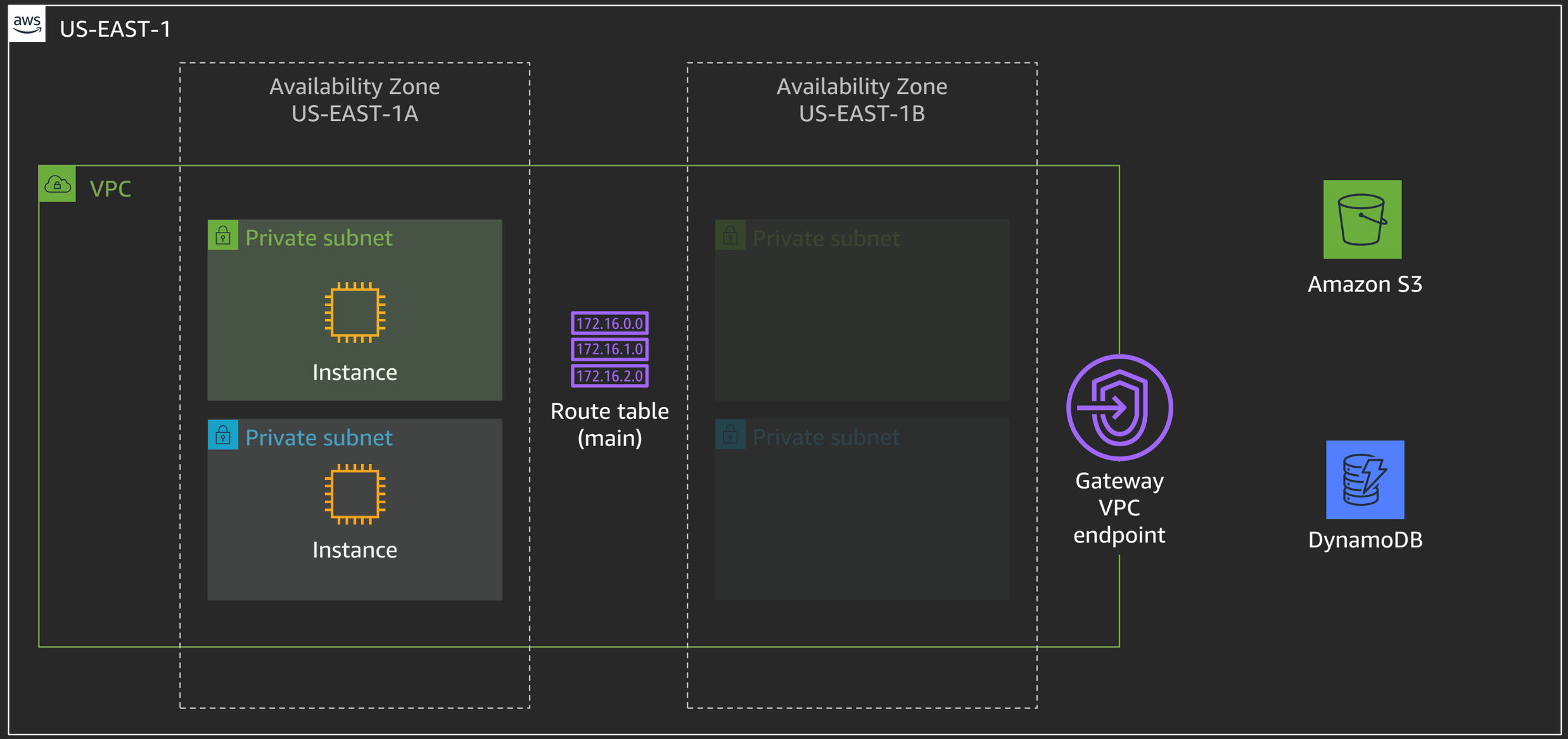


VPC endpoints

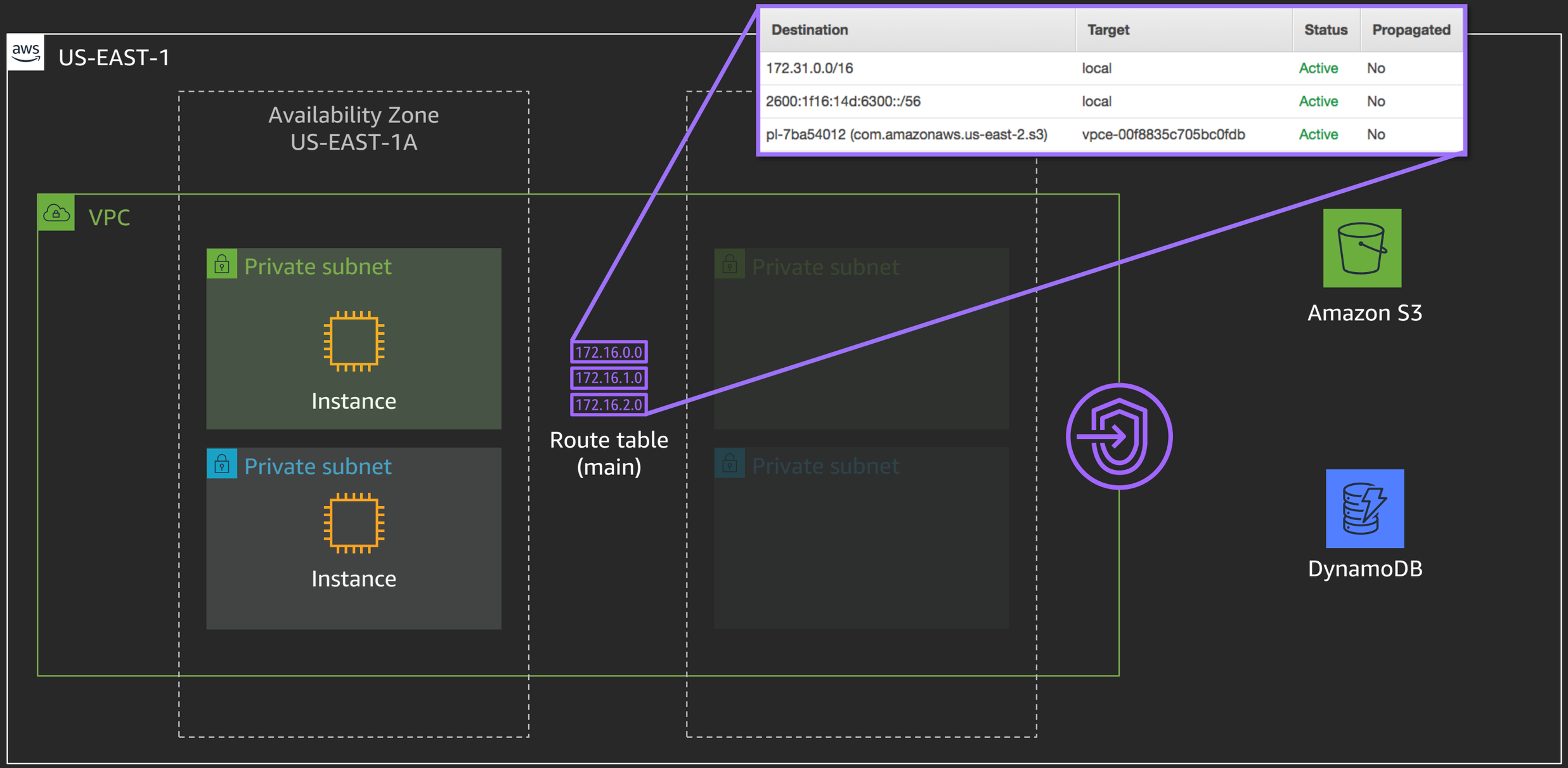
Gateway VPC endpoints



Gateway VPC endpoints

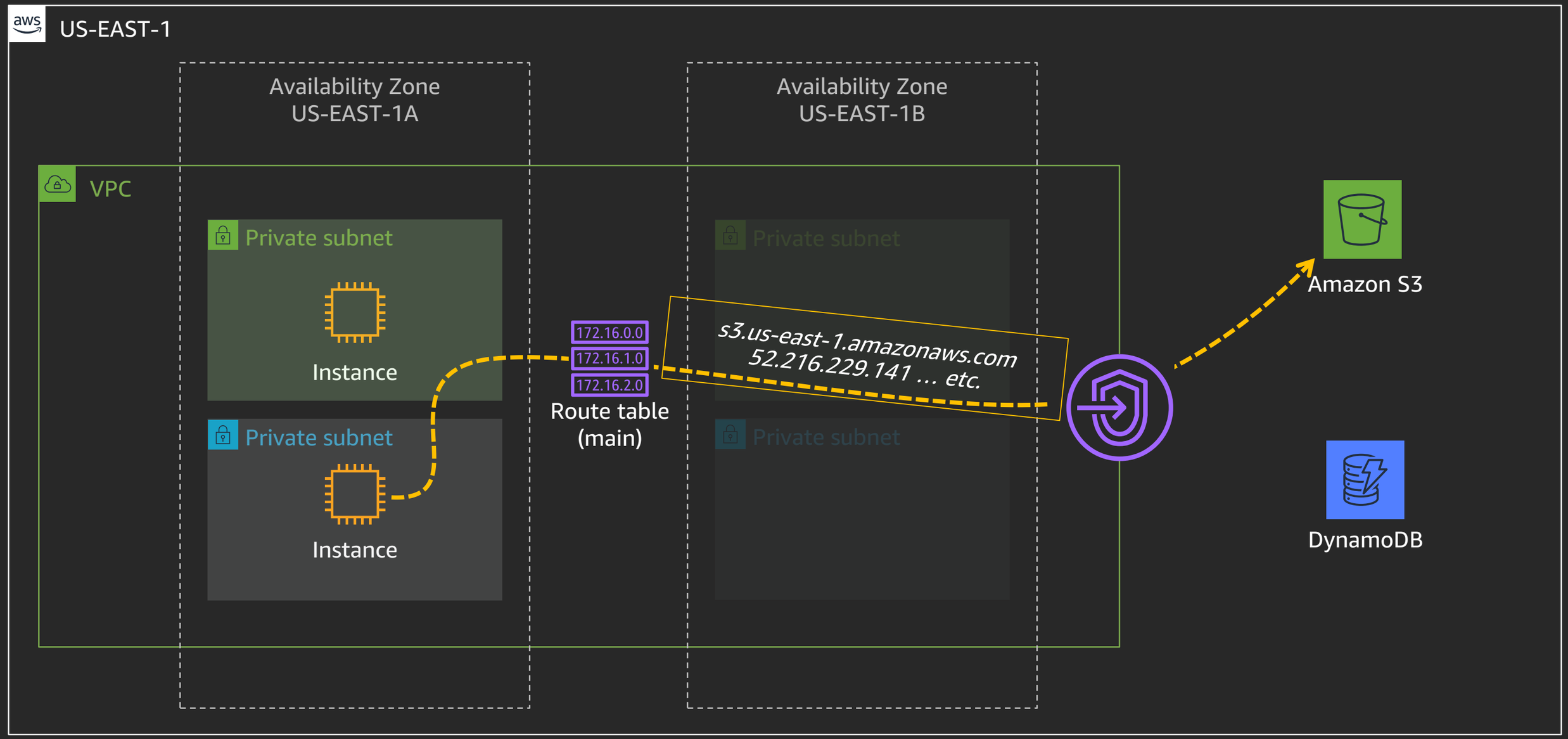


Gateway VPC endpoints

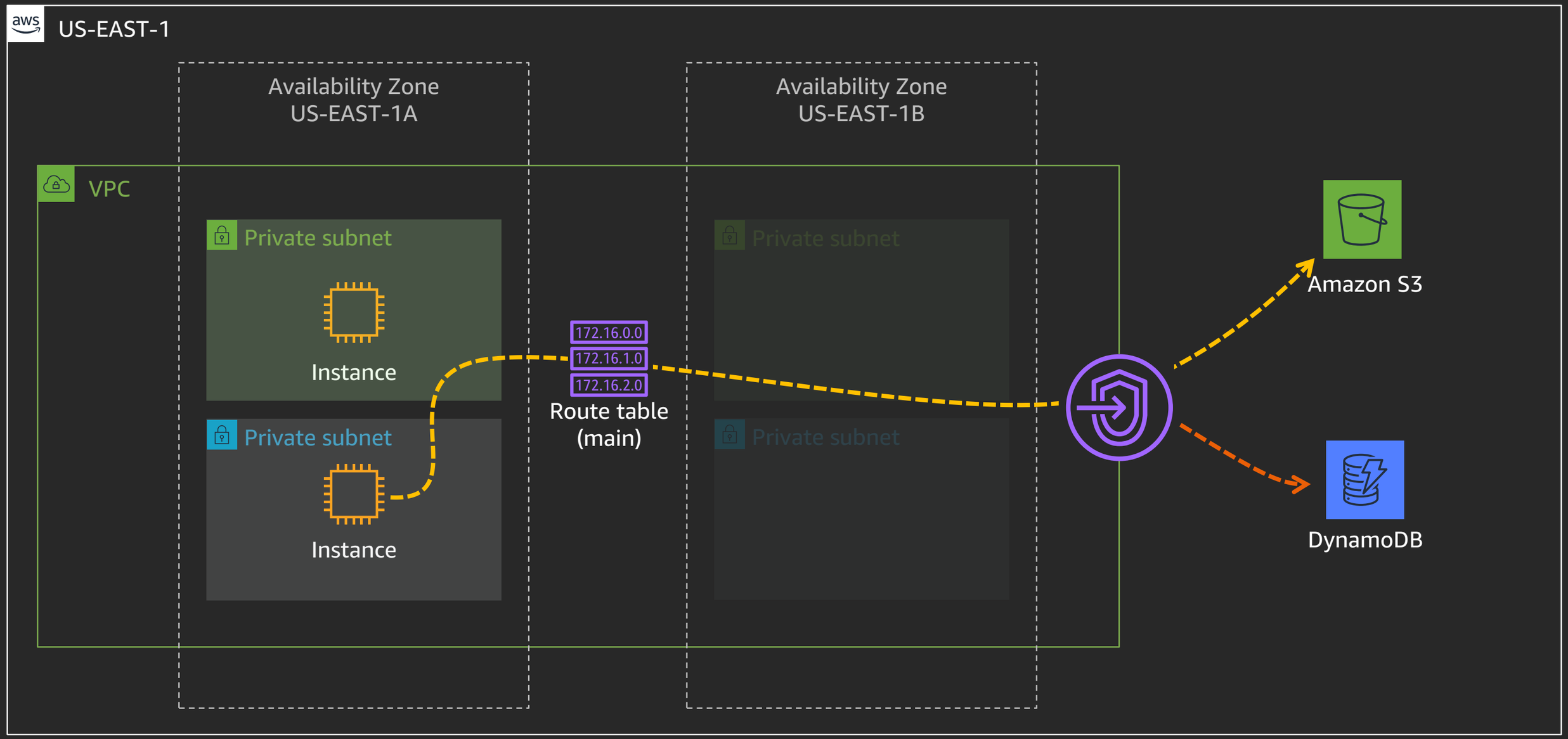


Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
pl-7ba54012 (com.amazonaws.us-east-2.s3)	vpce-00f8835c705bc0fdb	Active	No

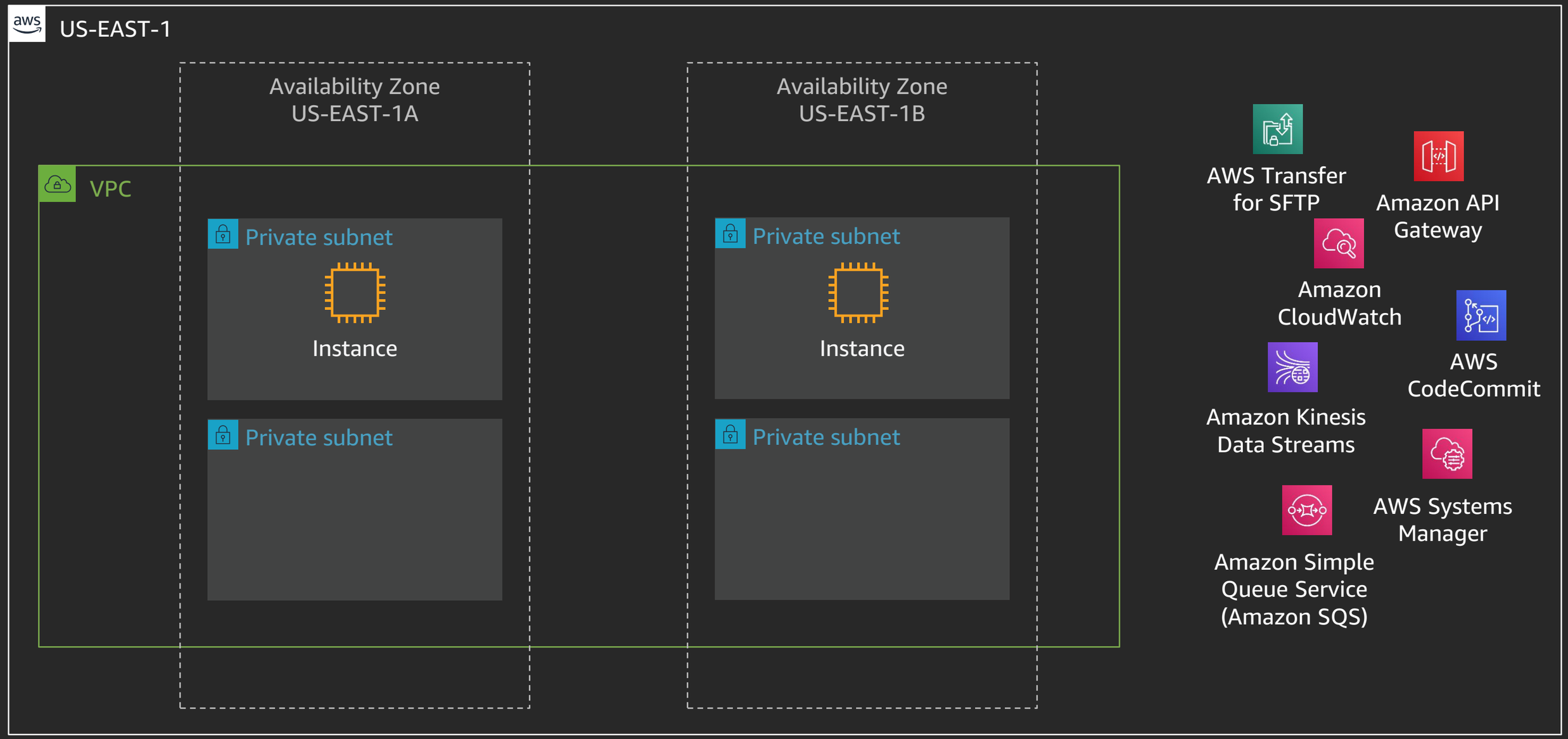
Gateway VPC endpoints



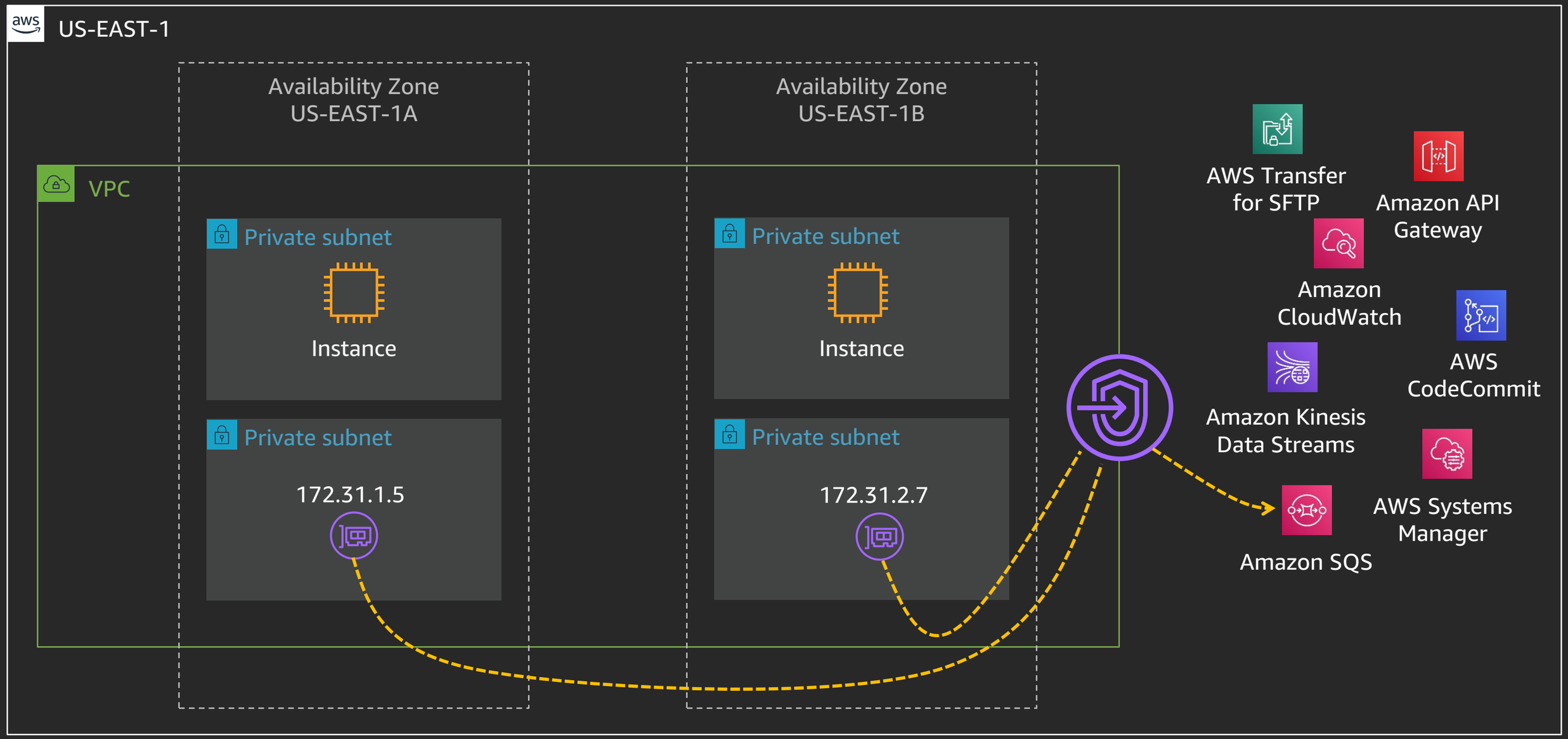
Gateway VPC endpoints



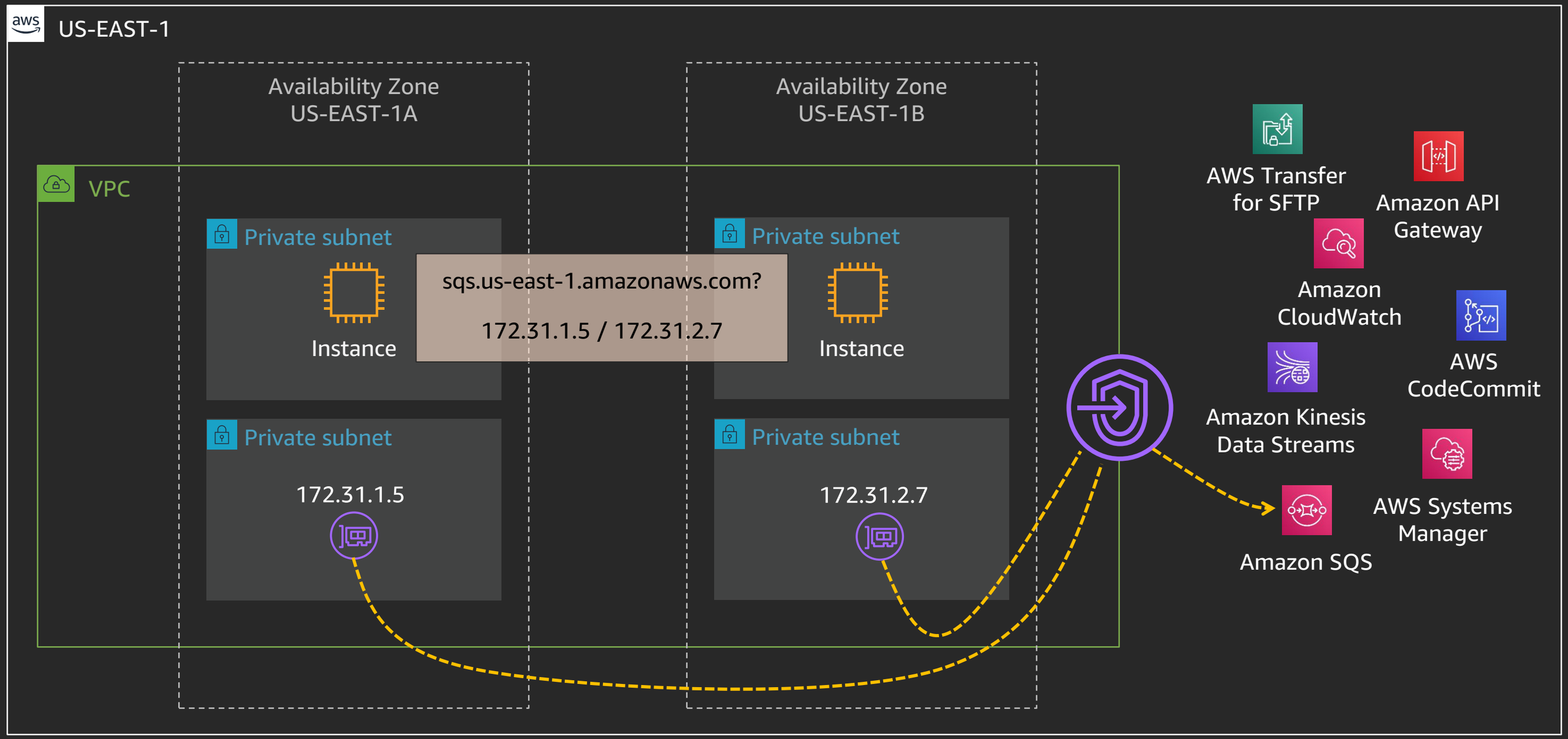
Interface VPC endpoints (AWS PrivateLink)



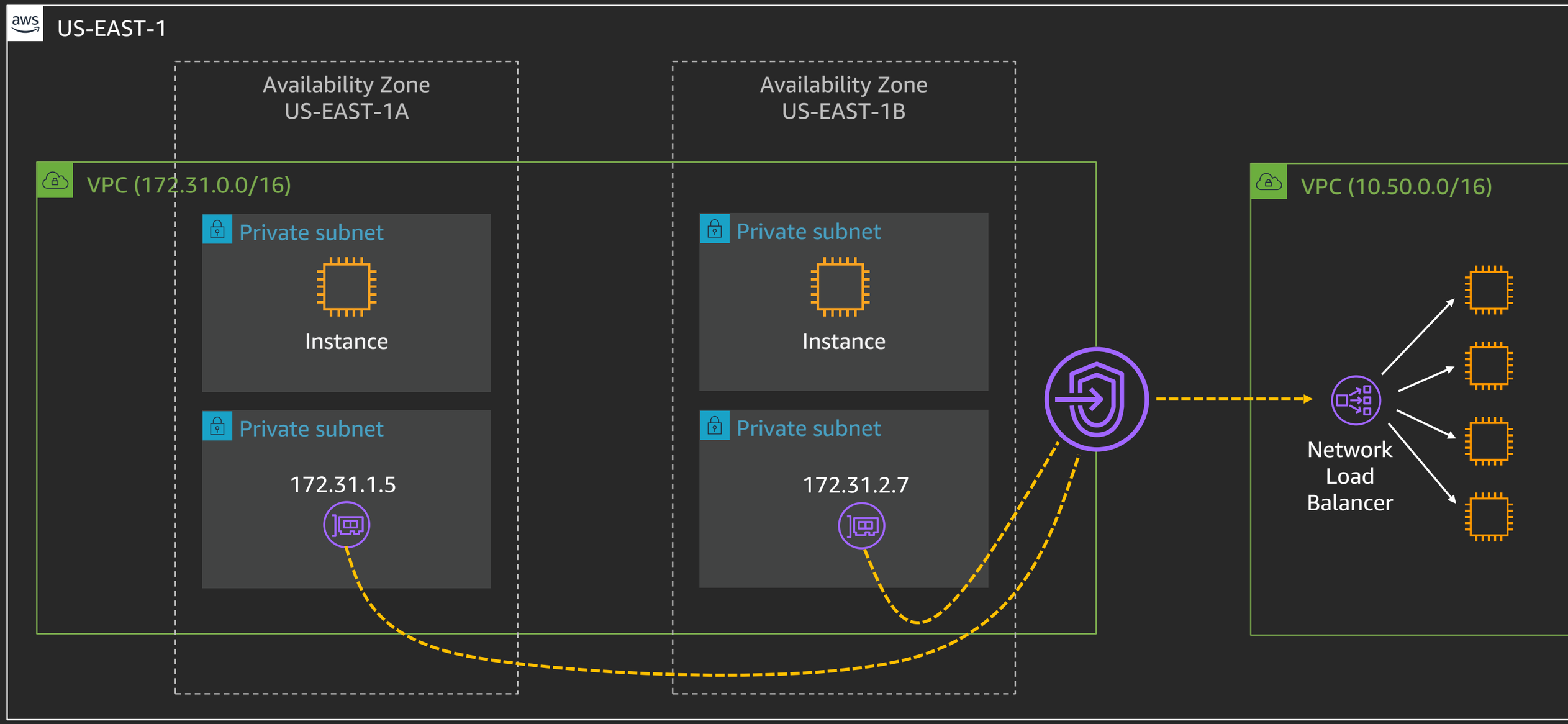
Interface VPC endpoints (AWS PrivateLink)



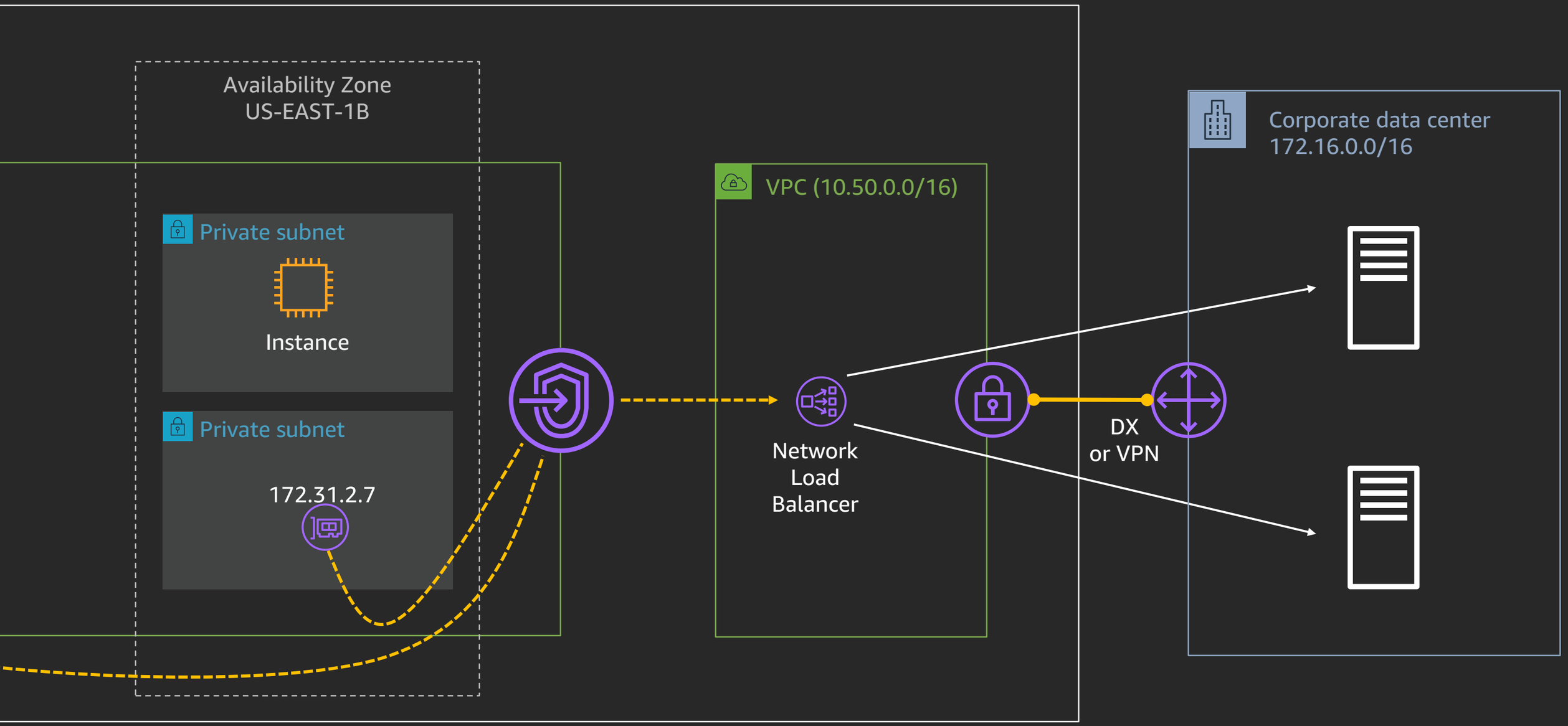
Interface VPC endpoints (AWS PrivateLink)



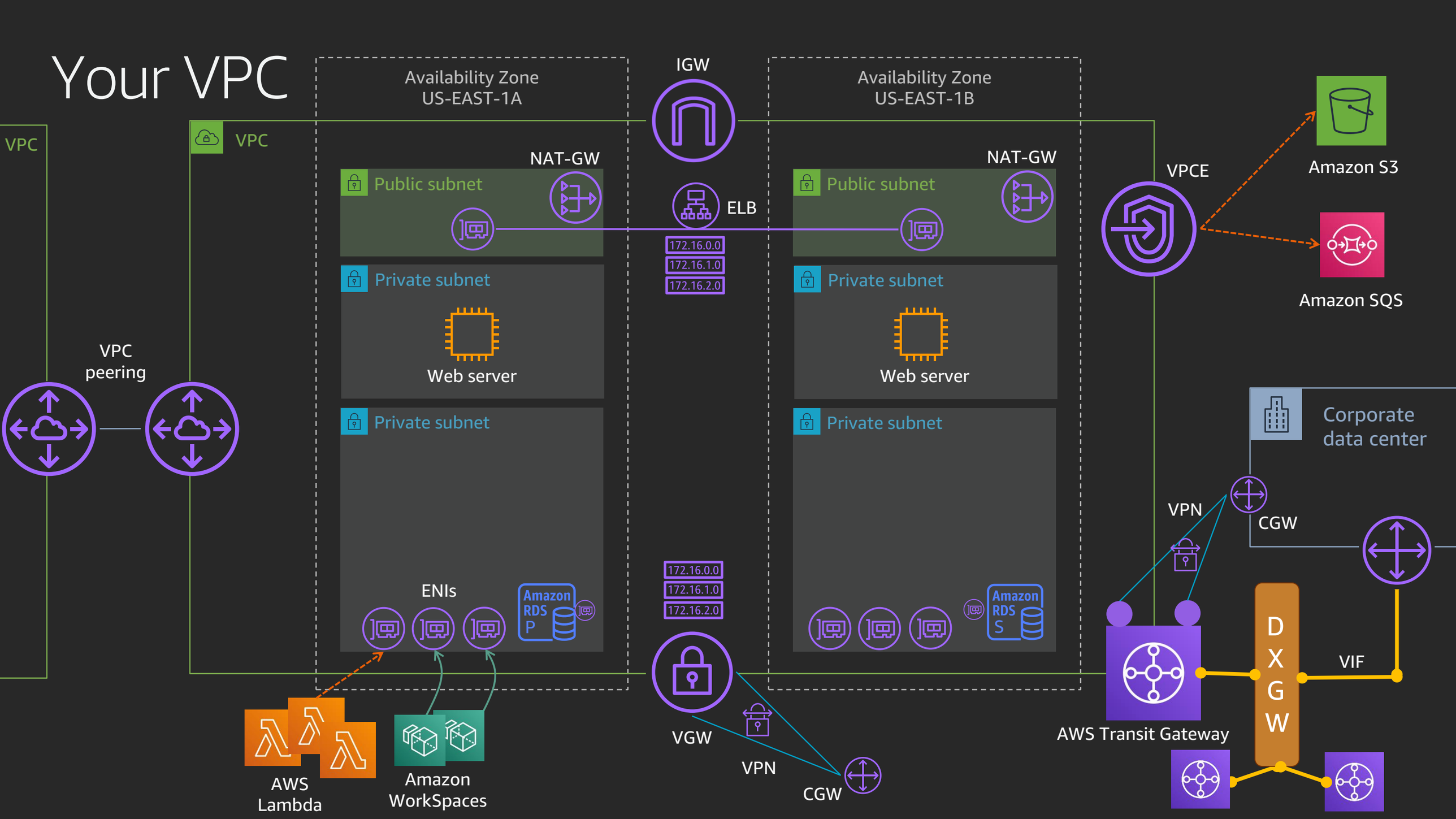
AWS PrivateLink – Your own services



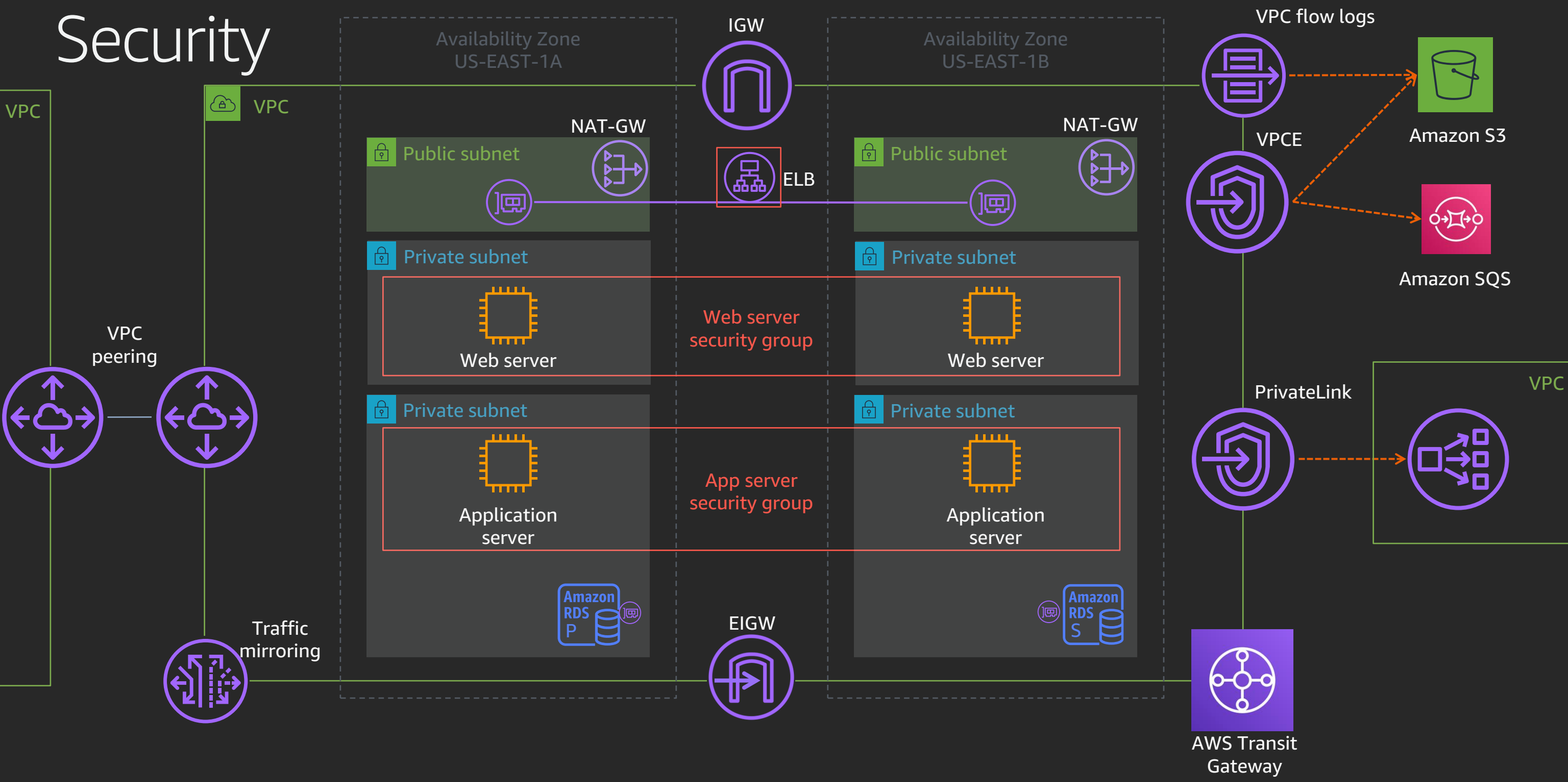
AWS PrivateLink – Your own services, on-premises



Bringing it all together


Your VPC
VPC
VPC
VPC peering
Availability Zone US-EAST-1A
Availability Zone US-EAST-1B
IGW
NAT-GW
Public subnet
Private subnet
Web server
Private subnet
ENIs
Amazon RDS P
ELB
172.16.0.0
172.16.1.0
172.16.2.0
Amazon RDS S
VGW
VPN
CGW
AWS Lambda
Amazon WorkSpaces
VPCE
Amazon S3
Amazon SQS
Corporate data center
AWS Transit Gateway
DXGW
VIF

Security


VPC
VPC
VPC peering
Traffic mirroring
Availability Zone US-EAST-1A
Availability Zone US-EAST-1B
IGW
EIGW
NAT-GW
NAT-GW
ELB
Public subnet
Public subnet
Private subnet
Private subnet
Private subnet
Private subnet
Web server
Web server
Web server security group
Application server
Application server
App server security group
Amazon RDS P
Amazon RDS S
VPC flow logs
Amazon S3
VPCE
Amazon SQS
PrivateLink
VPC
AWS Transit Gateway

What's new since re:Invent 2019?

- Amazon VPC Ingress Routing – AWS CloudFormation support
- AWS Transit Gateway
  - Inter-region peering
  - Multicast support
  - Additional regions
- Amazon VPC Flow Logs now supports 1-minute aggregation intervals

Thank you!

aws SUMMIT ONLINE