Mimmit Koodaa - AWS

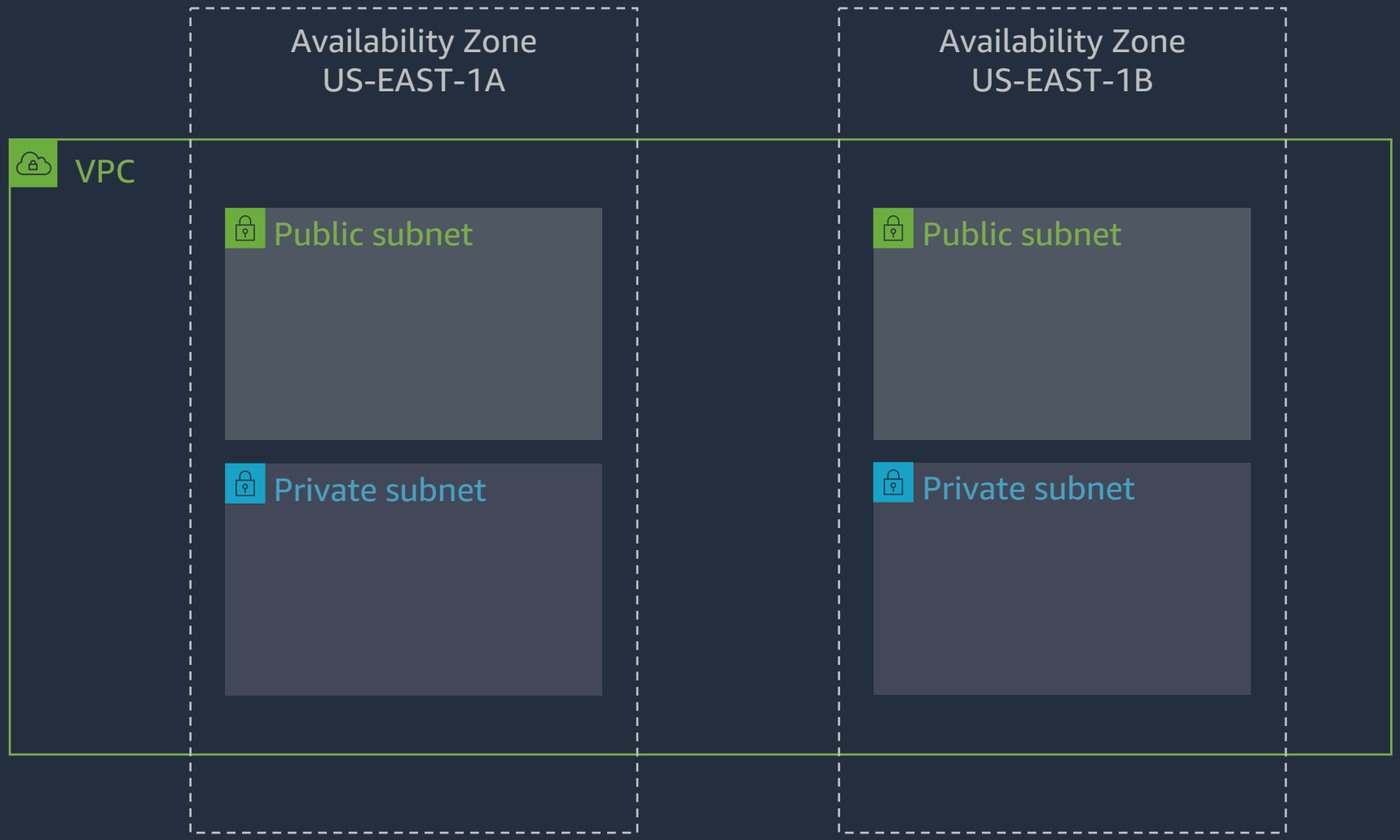
Networks and security

Jose Juhala

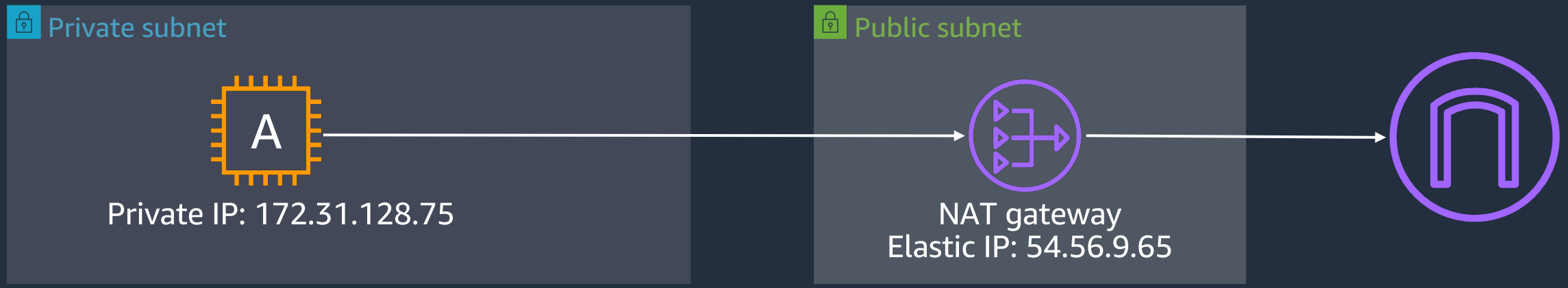
Senior Solutions Architect

Recap of VPC

Amazon Virtual Private Cloud



Private and Public subnets



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

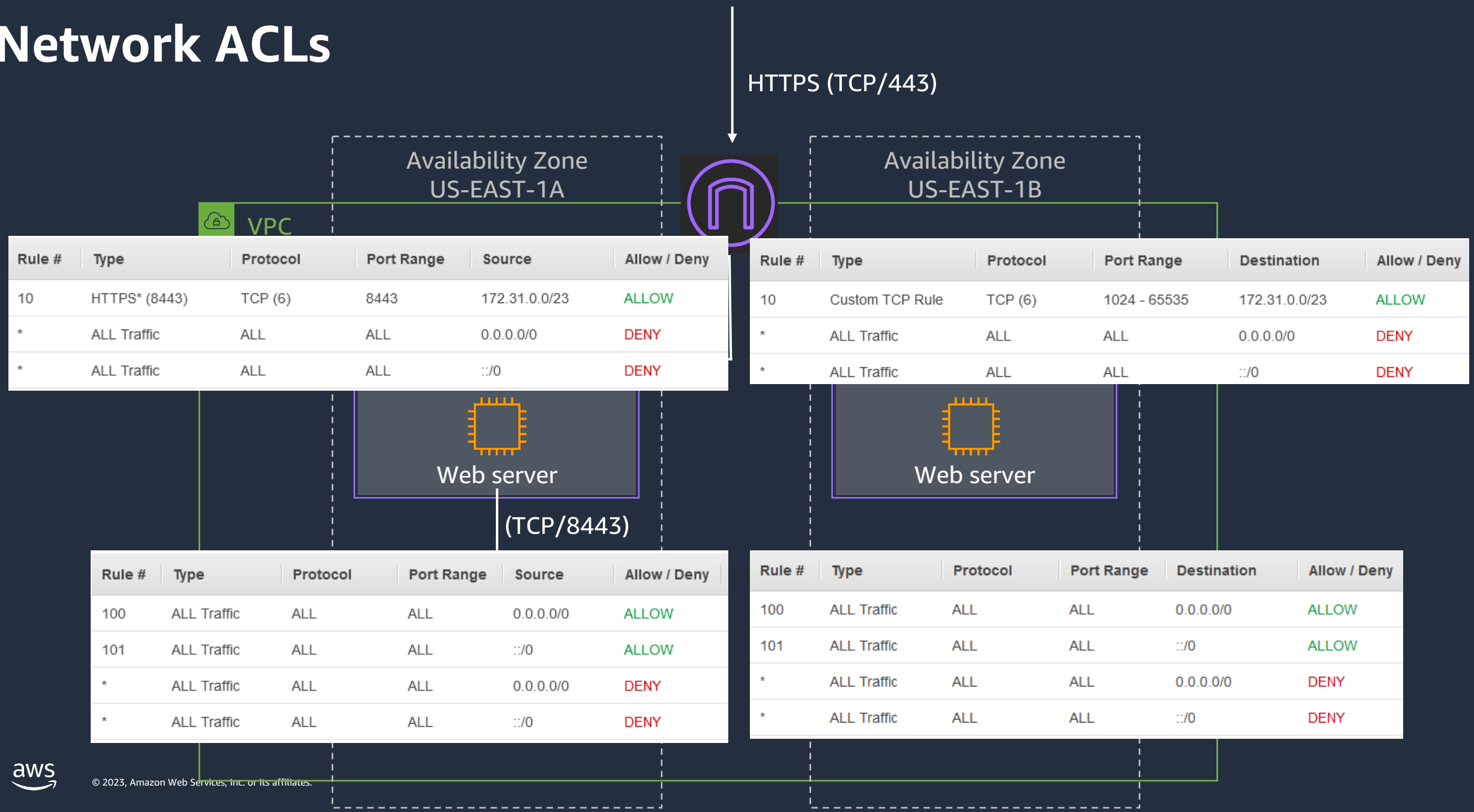
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
0.0.0.0/0	igw-09ef761d872bd7540	Active	No
::/0	igw-09ef761d872bd7540	Active	No

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 ACLs



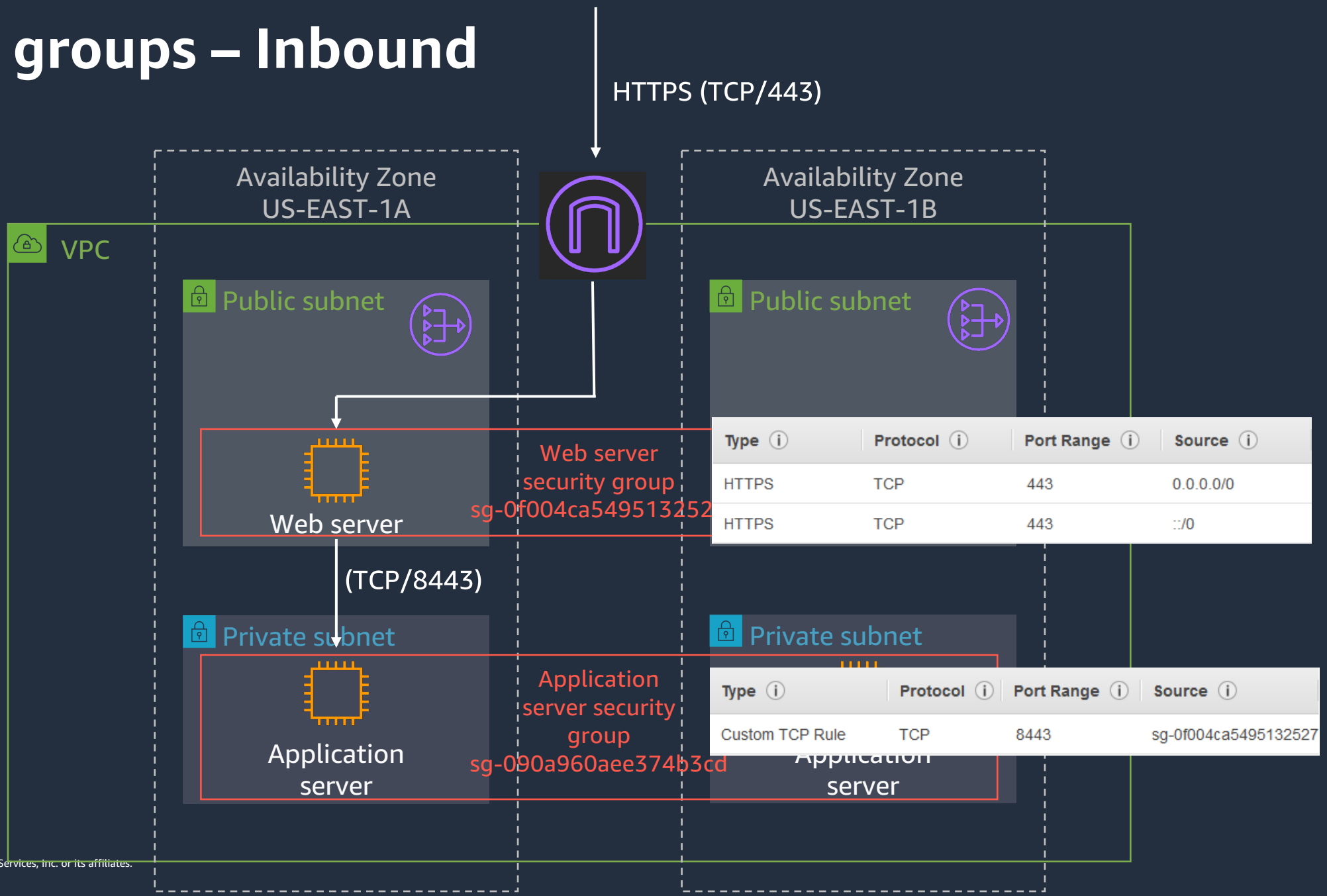
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
10	HTTPS* (8443)	TCP (6)	8443	172.31.0.0/23	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

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

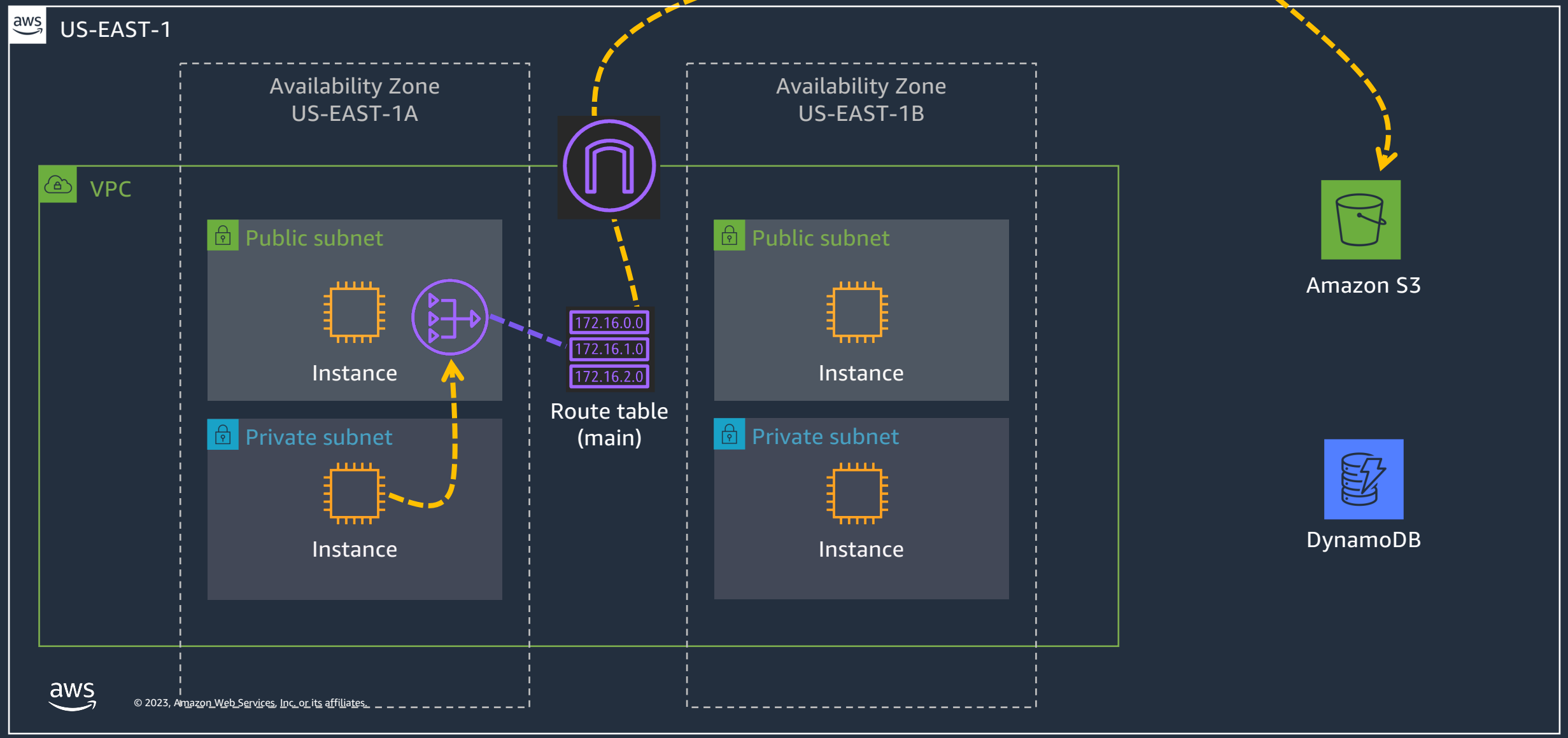


Type	Protocol	Port Range	Source
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	::/0

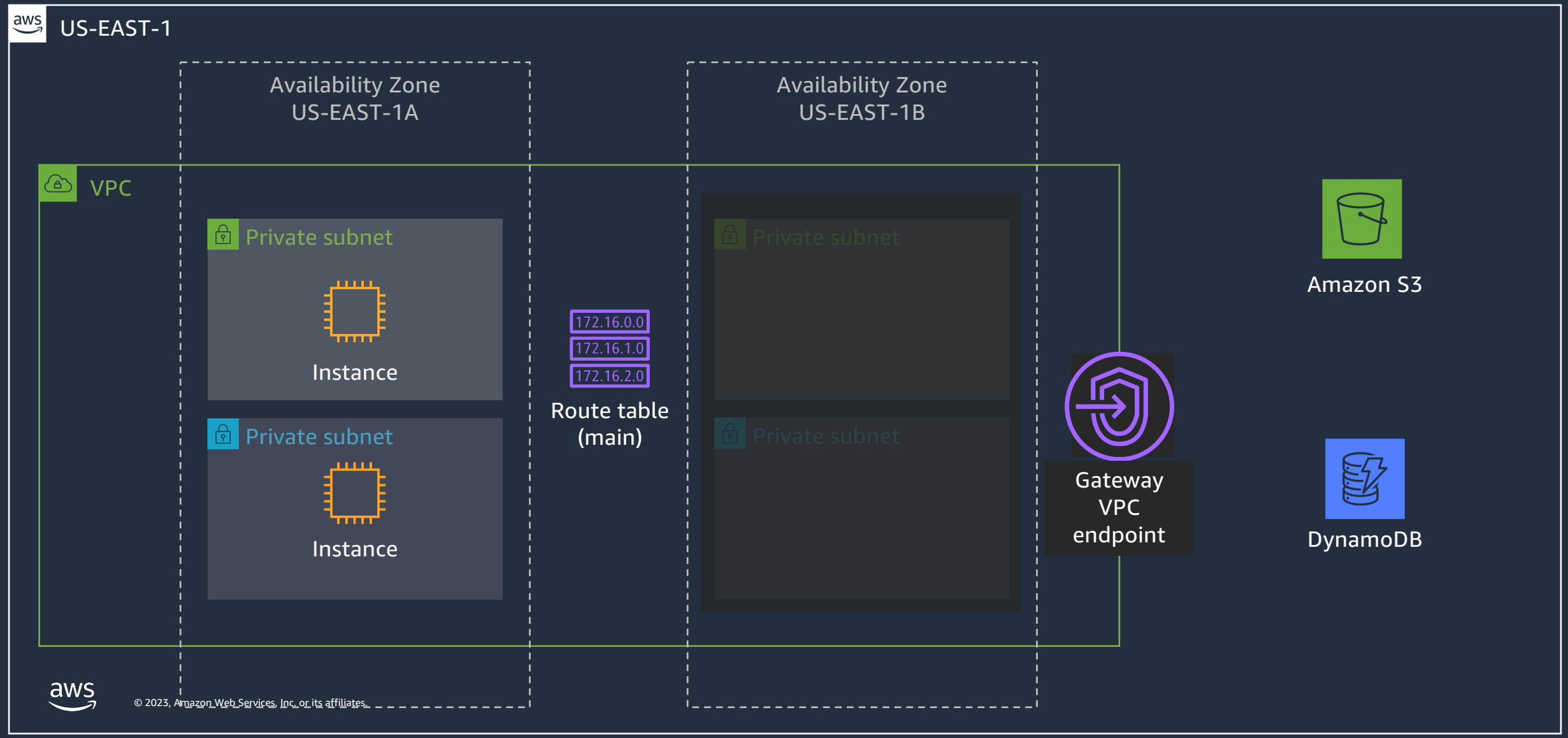
Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	8443	sg-0f004ca5495132527

VPC Endpoints

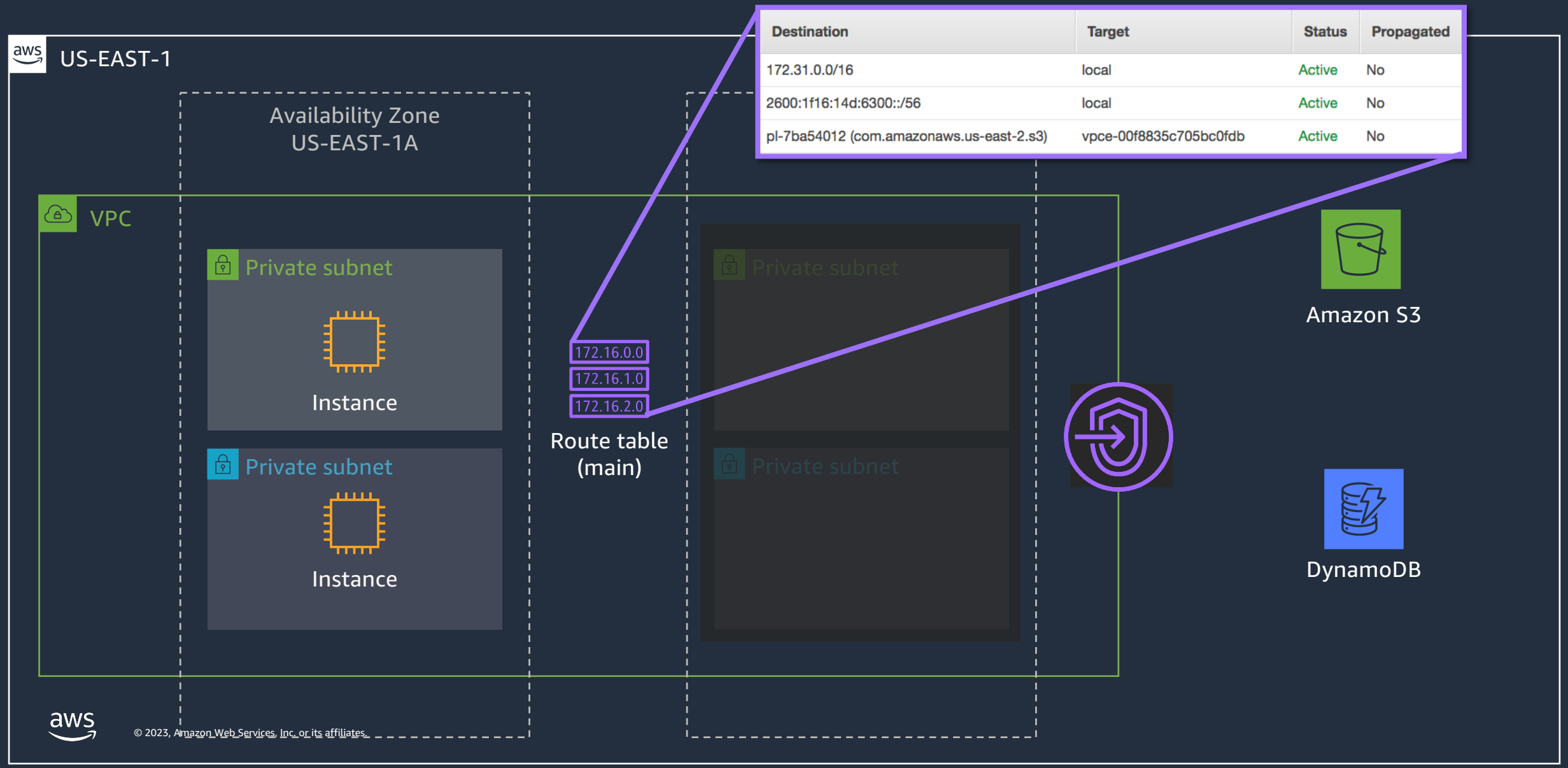
Gateway VPC endpoints



Gateway VPC endpoints

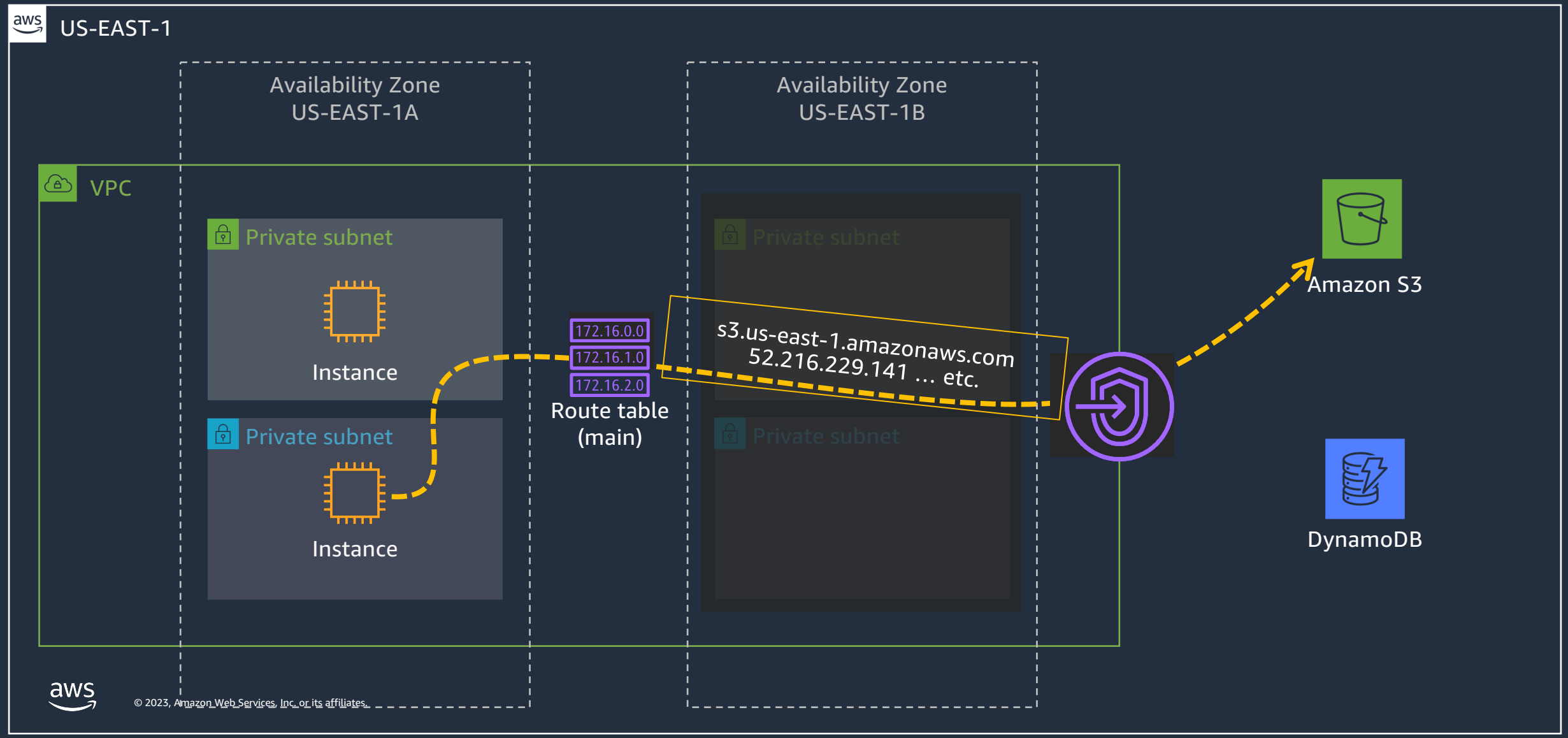


Gateway VPC endpoints

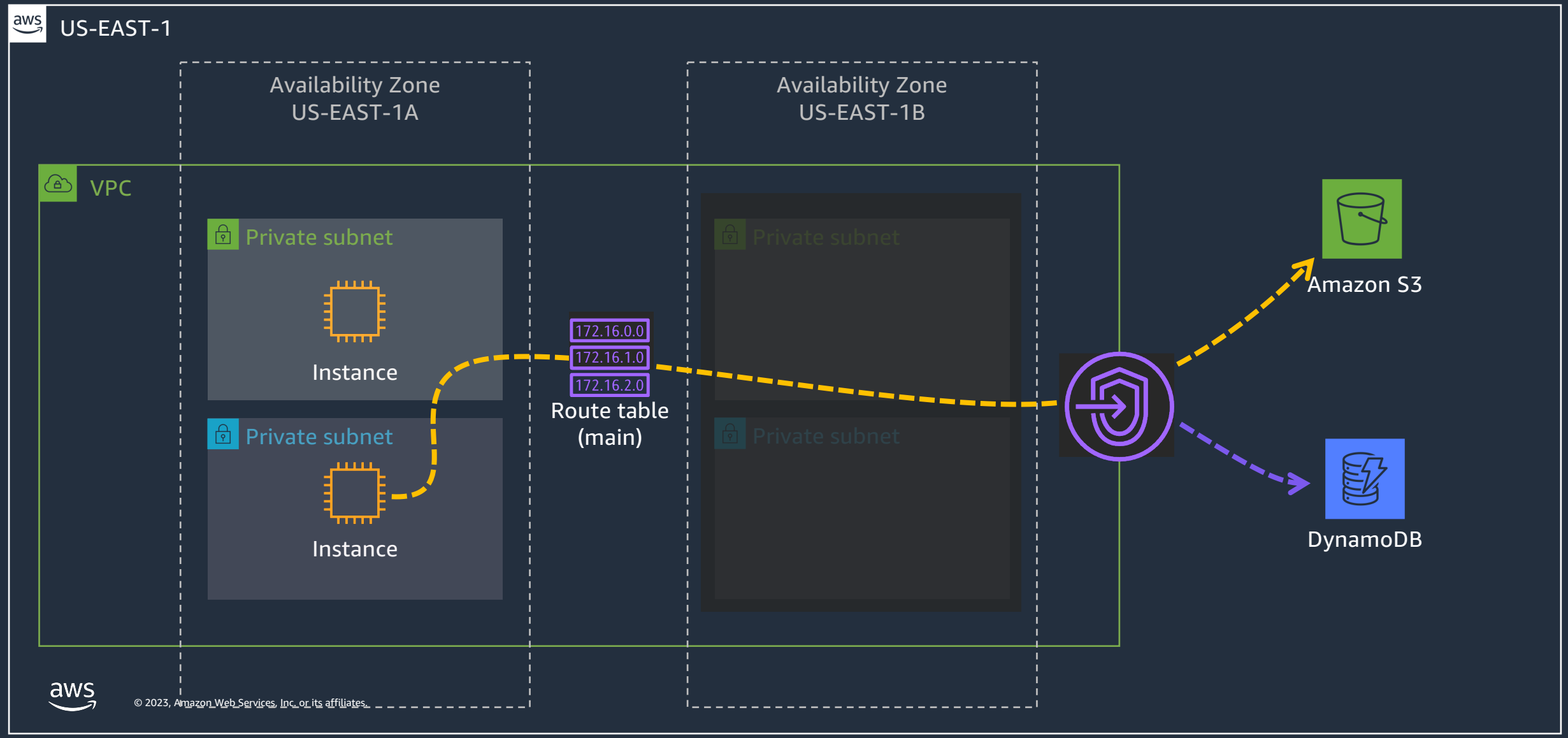


Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No
pl-7ba54012 (com.amazonaws.us-east-2.s3)	vpce-00f8835c705bc0fdb	Active	No

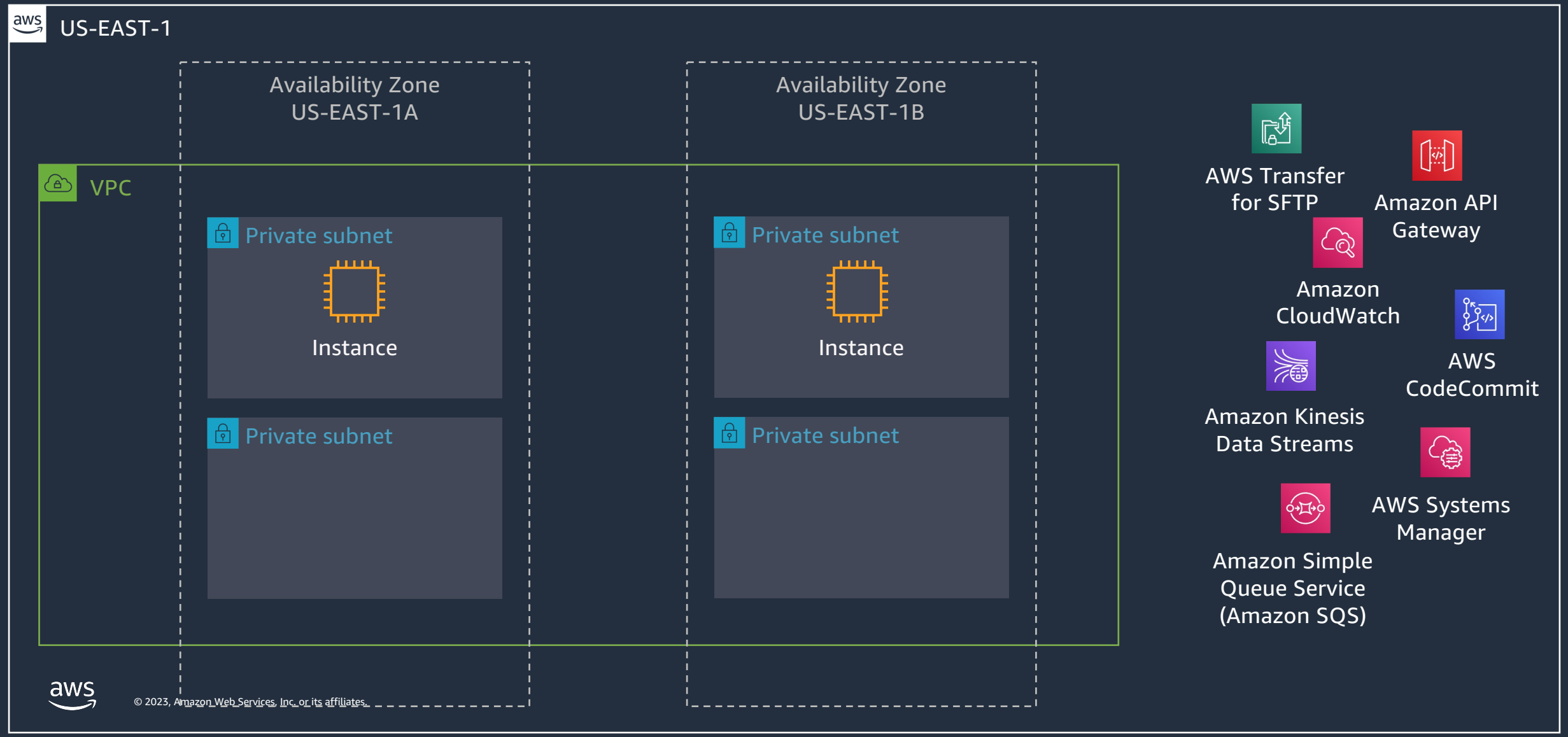
Gateway VPC endpoints



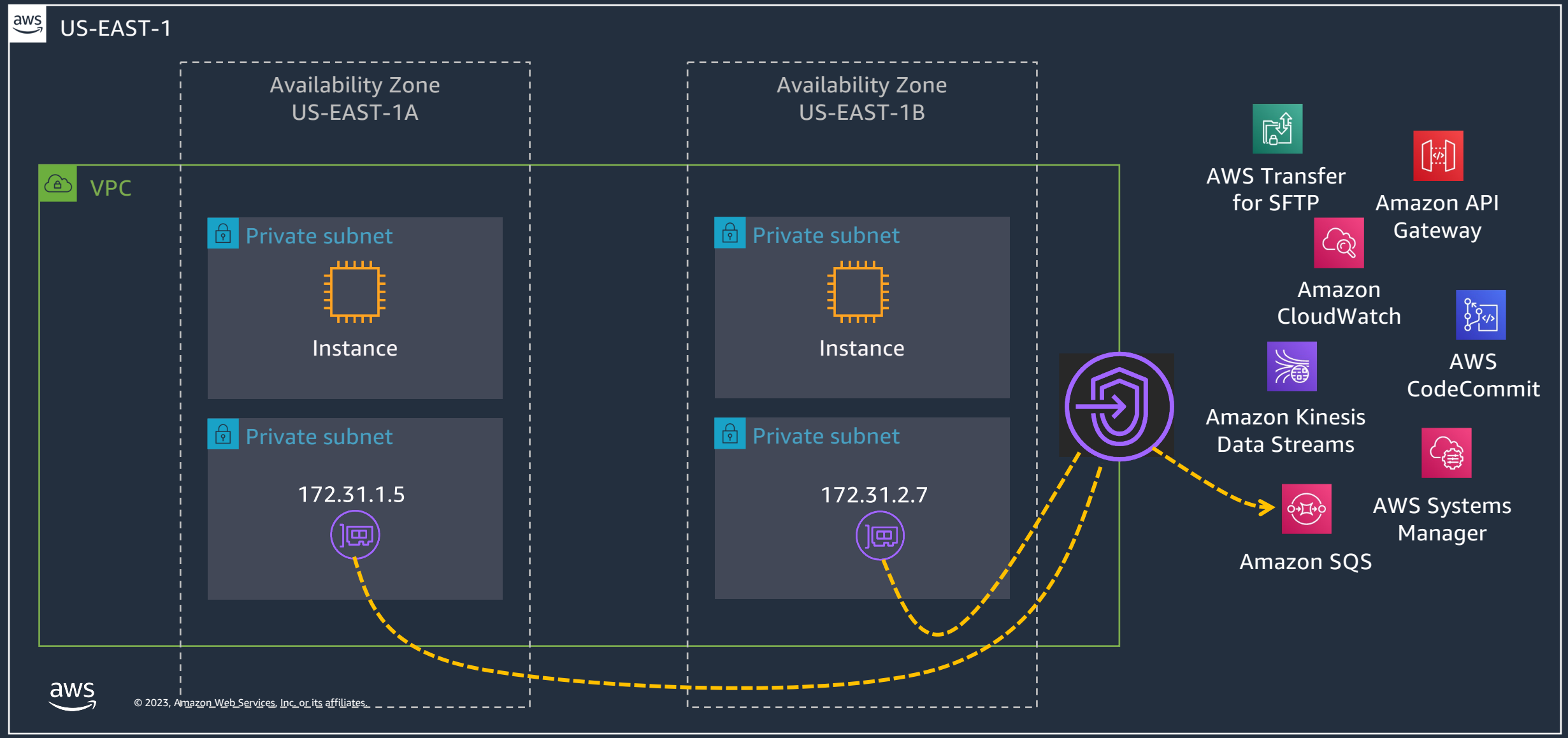
Gateway VPC endpoints



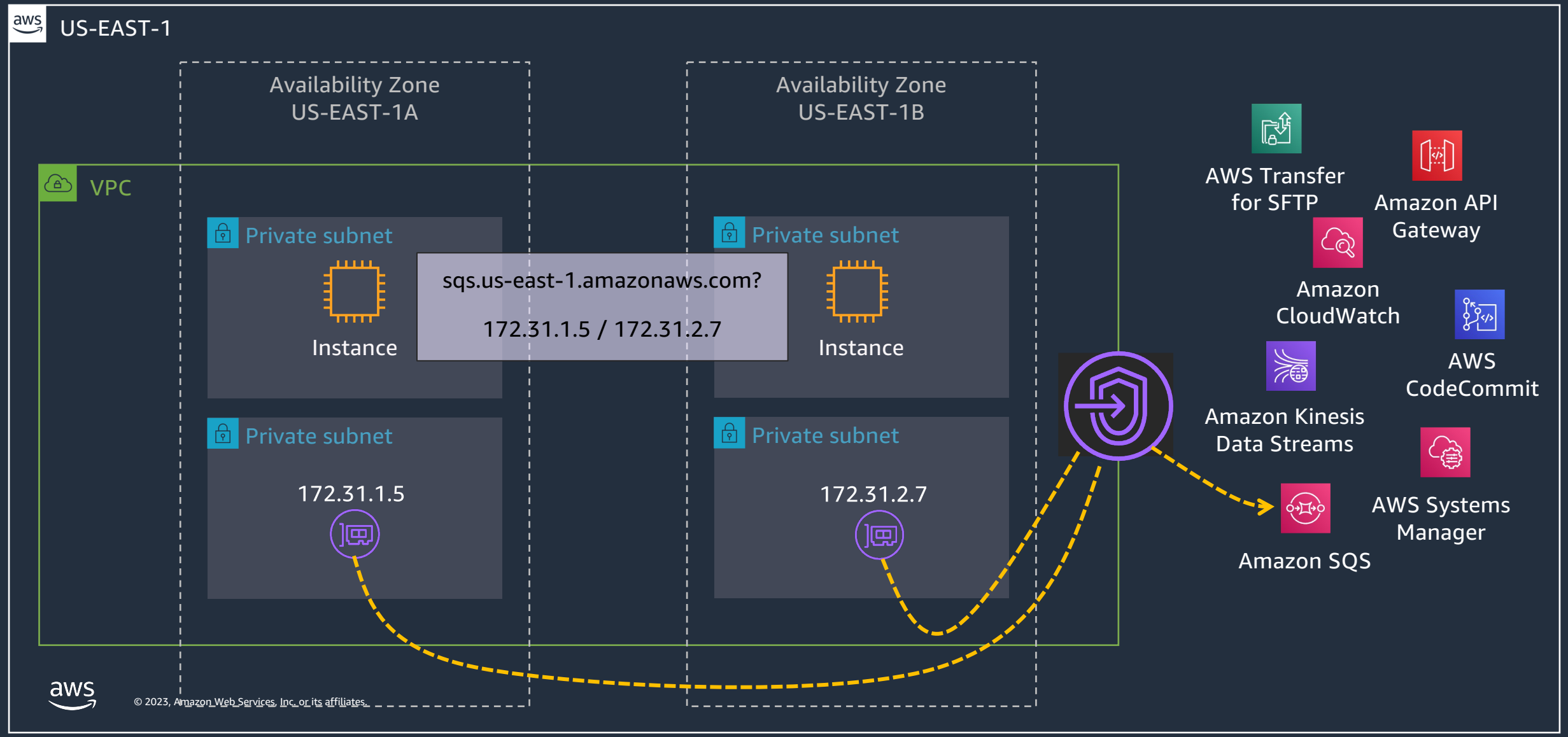
Interface VPC endpoints (AWS PrivateLink)



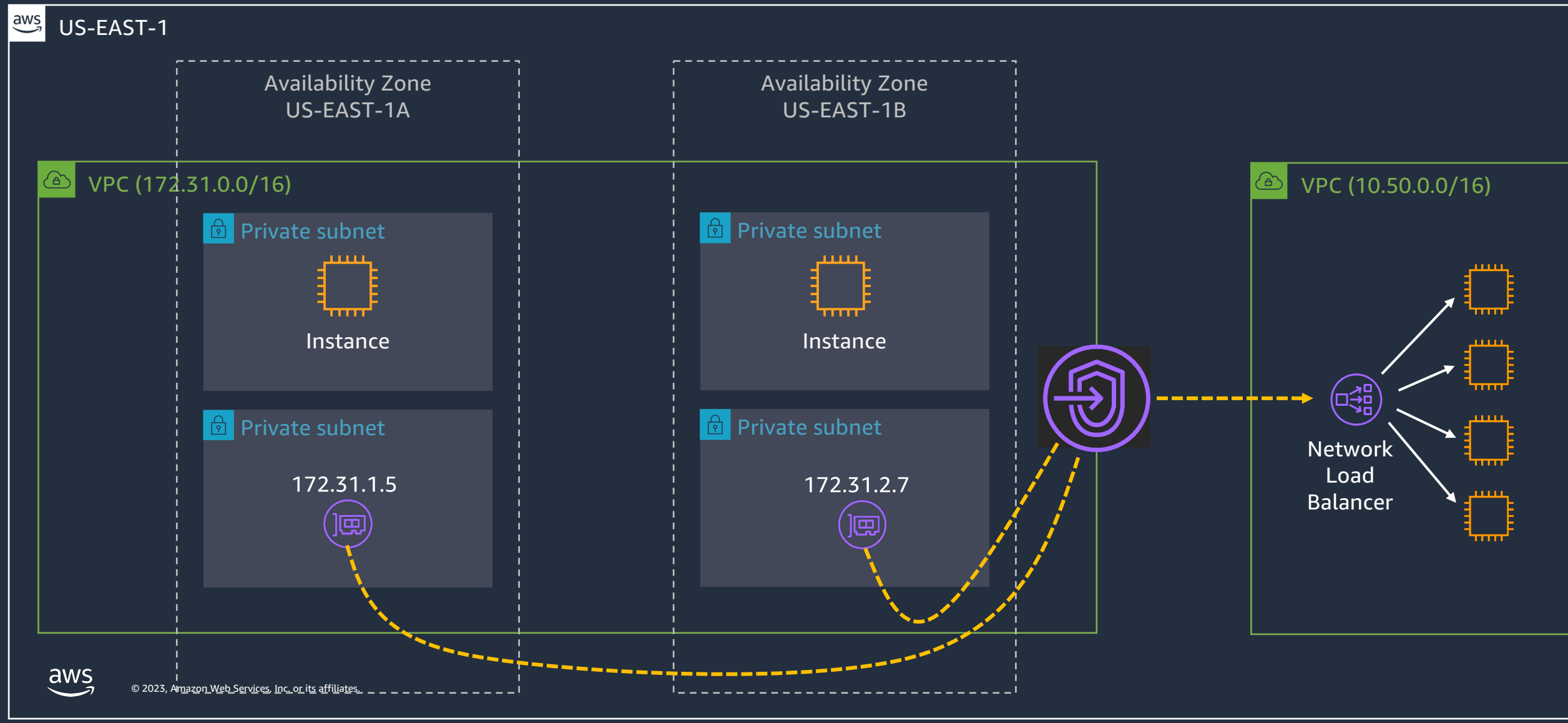
Interface VPC endpoints (AWS PrivateLink)



Interface VPC endpoints (AWS PrivateLink)

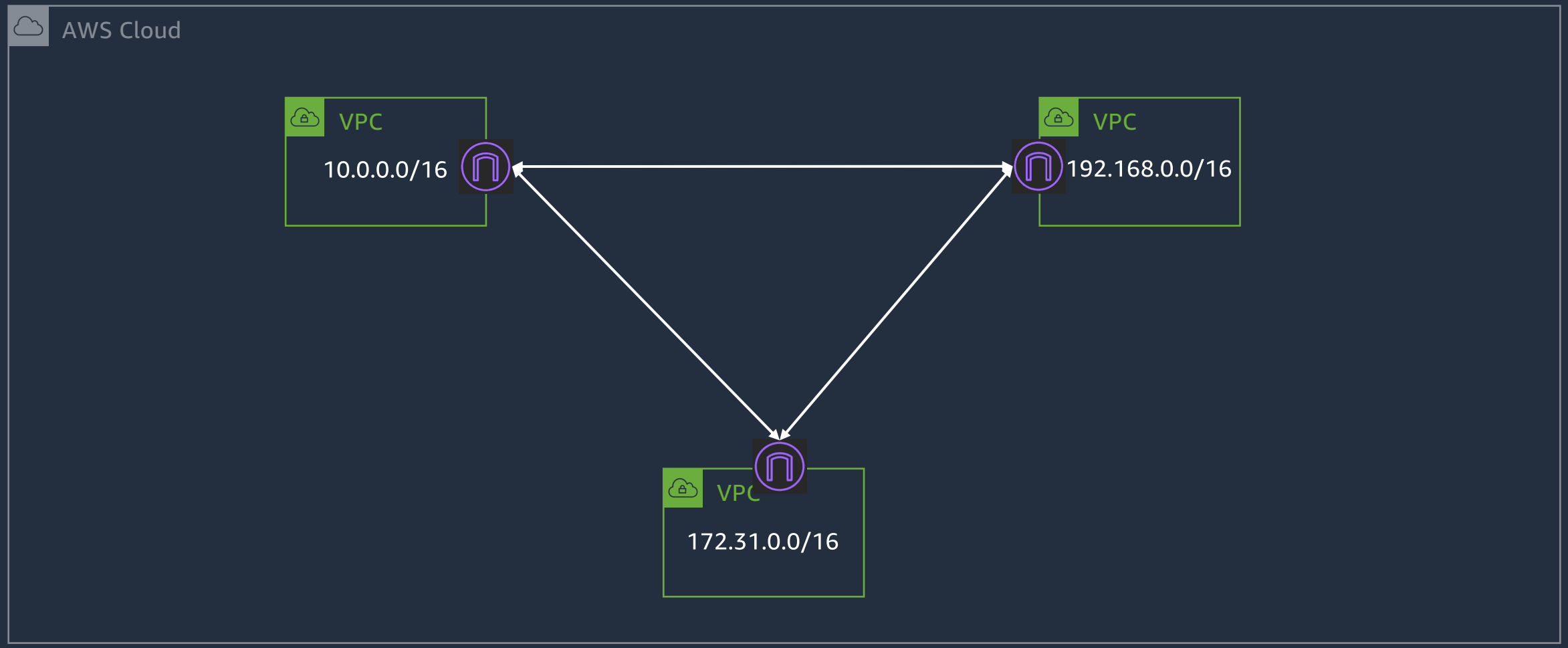


AWS PrivateLink – Your own services

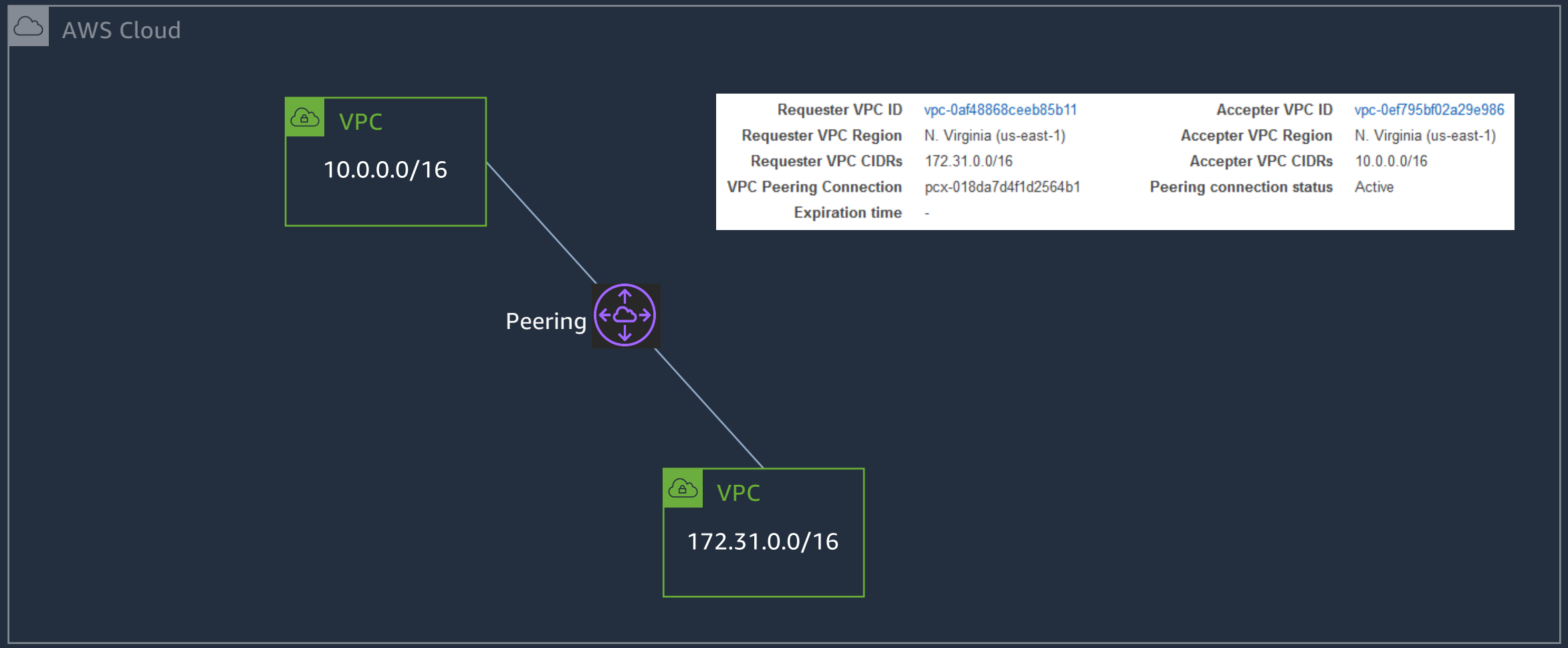


VPC Peering

Connecting between VPCs

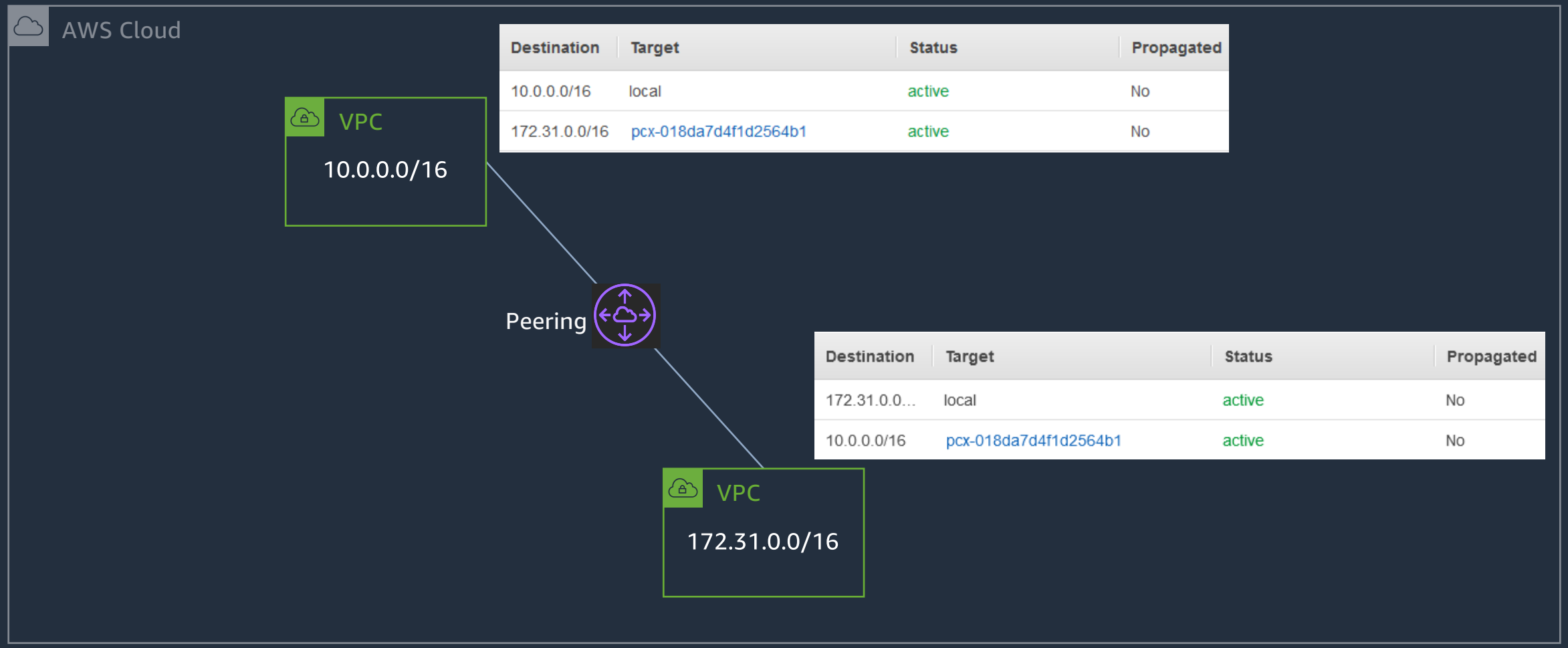


VPC peering



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	-		

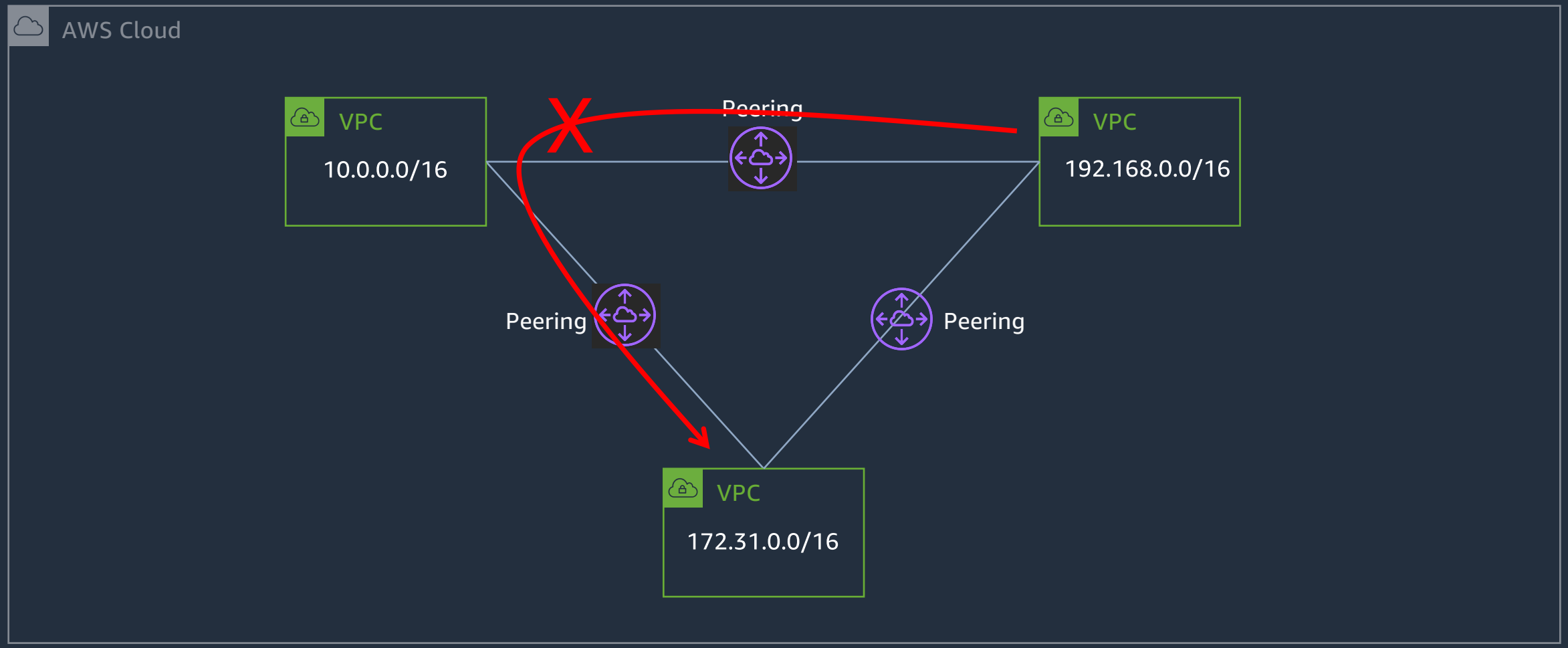
VPC peering



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

Can’t route through VPCs

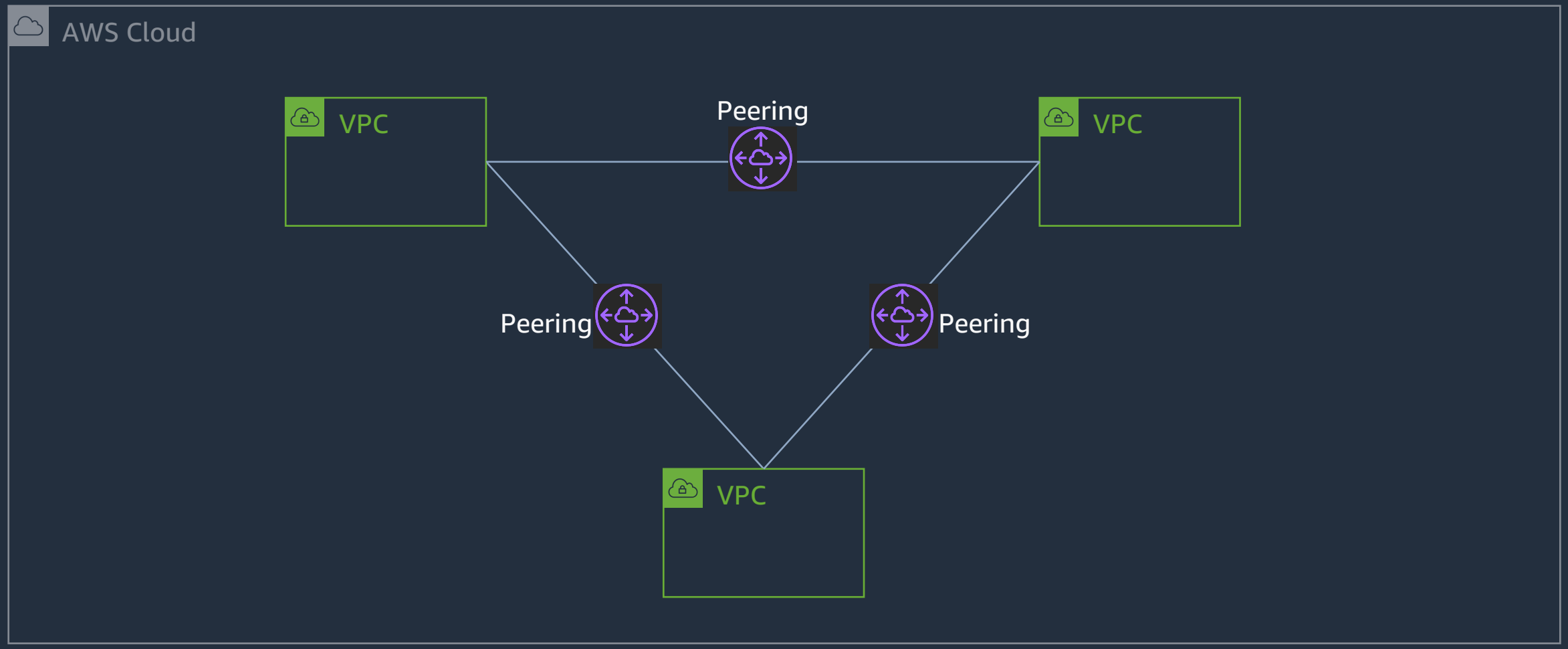


VPC peering – Things to know

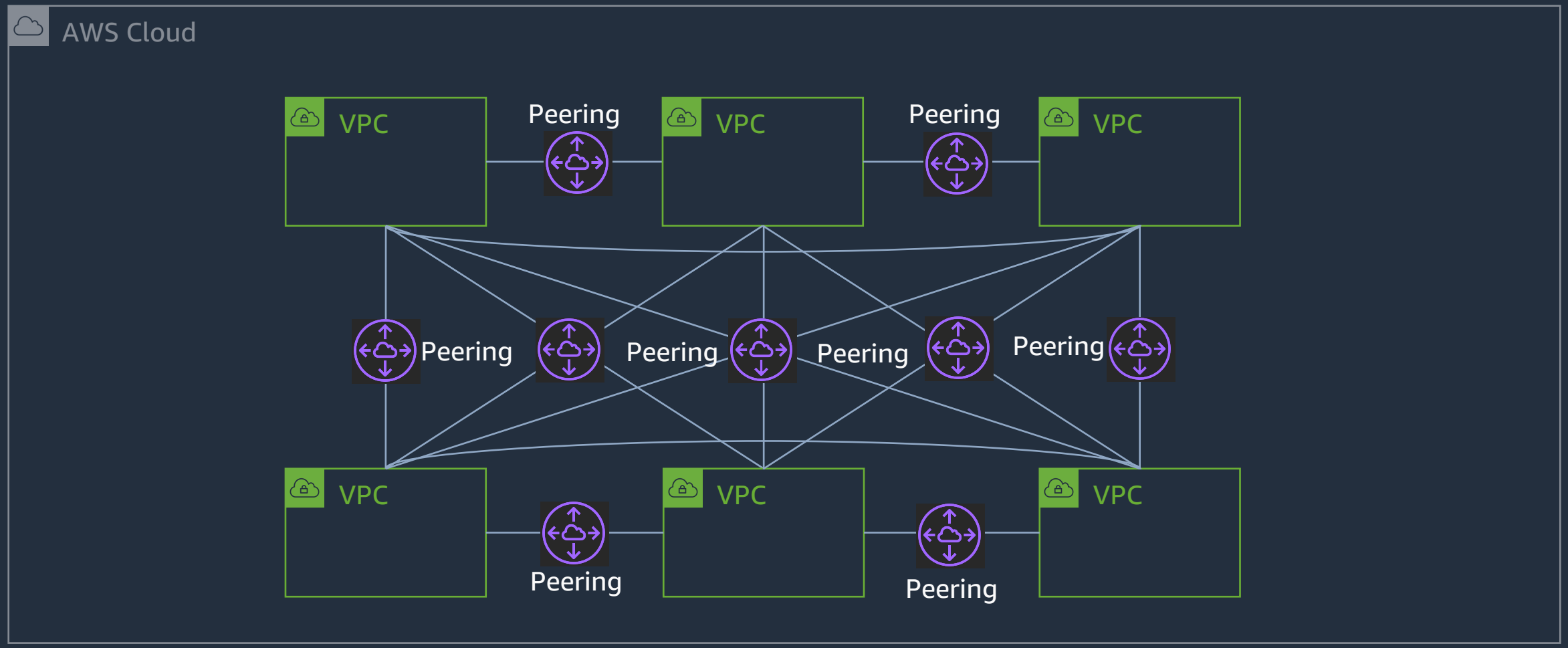
- Can reference security groups from the peer VPC in the same region
- Can enable DNS hostname resolution to return private IP addresses
- Can peer for both IPv4 and IPv6 addresses
- Cannot have overlapping IP addresses
- Cannot have multiple peers between the same pair of VPCs
- Cannot use jumbo frames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

AWS Transit Gateway

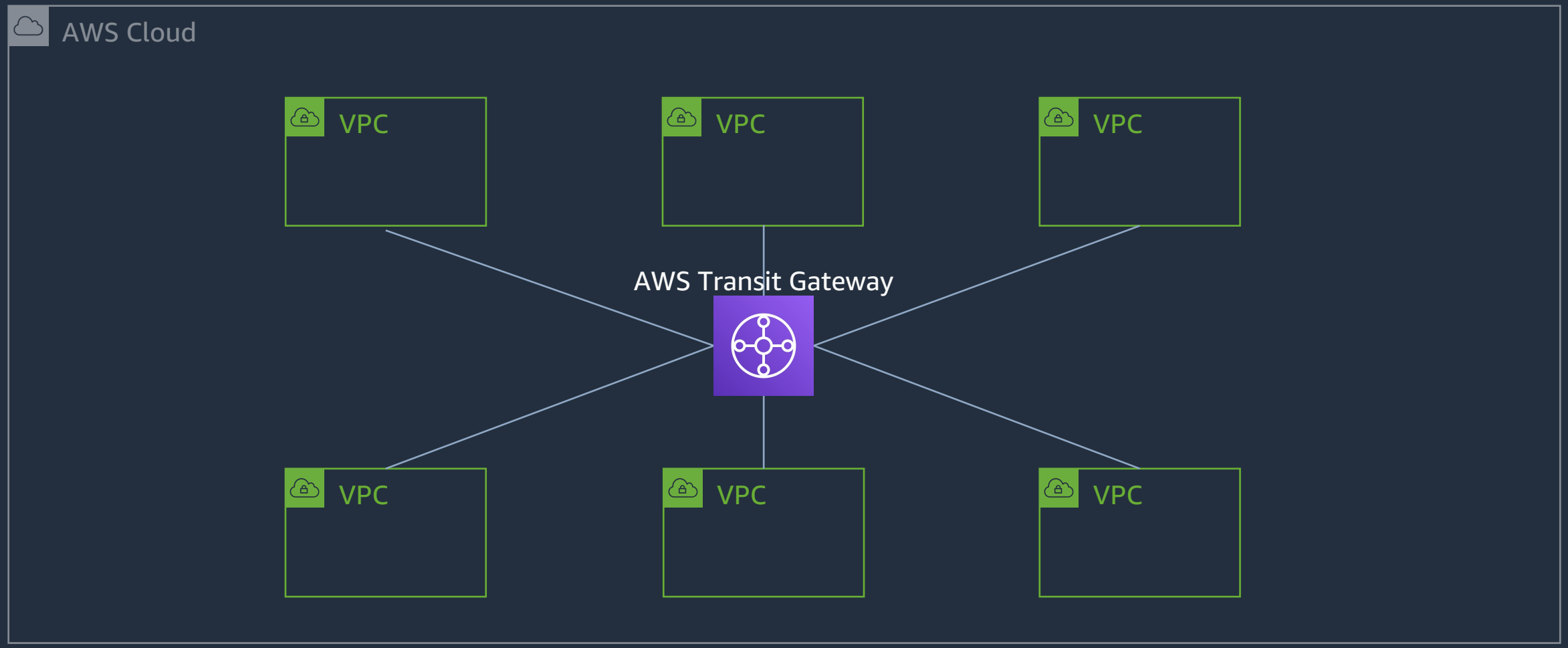
Interconnecting VPCs at scale – VPC peering



Interconnecting VPCs at scale – VPC peering

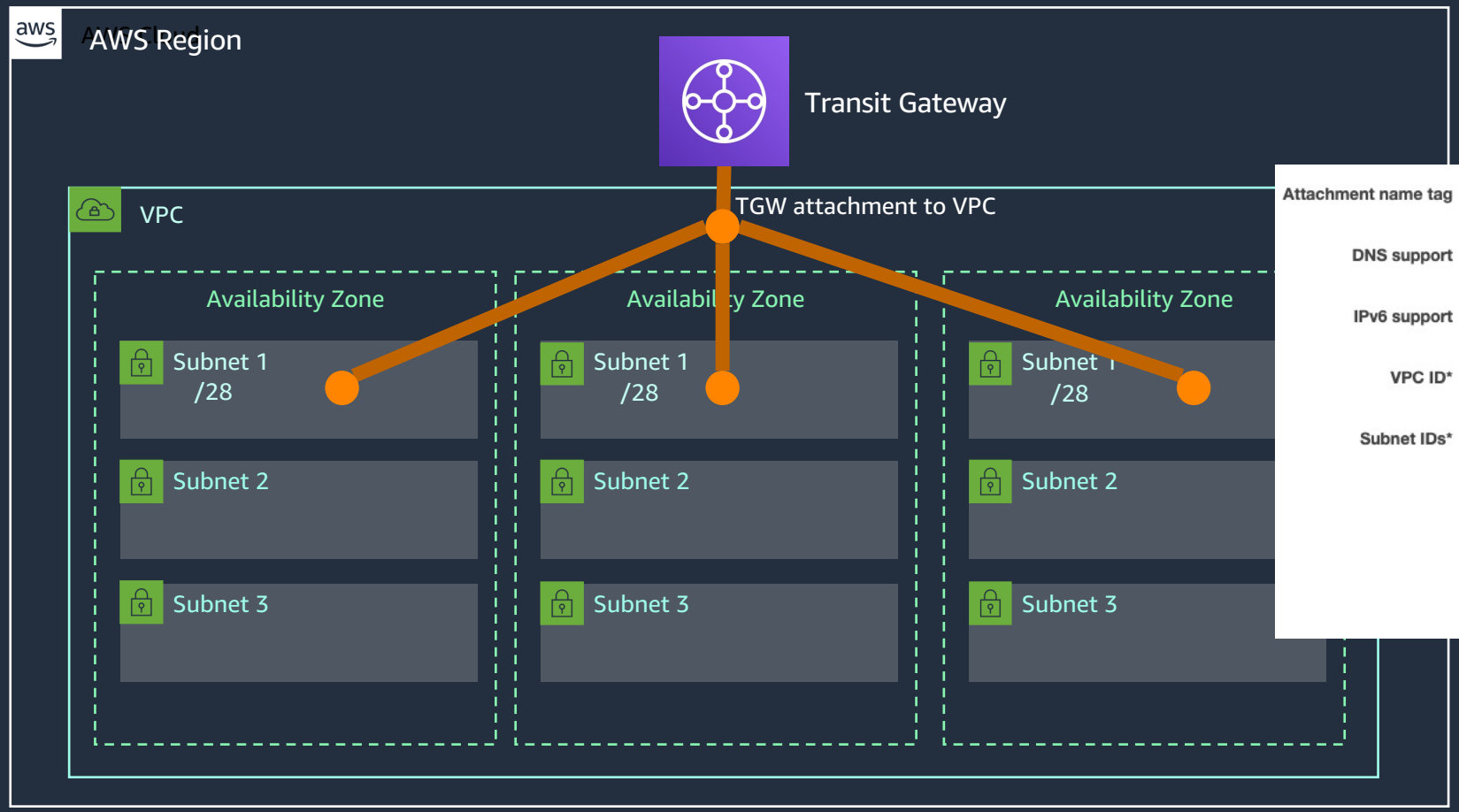


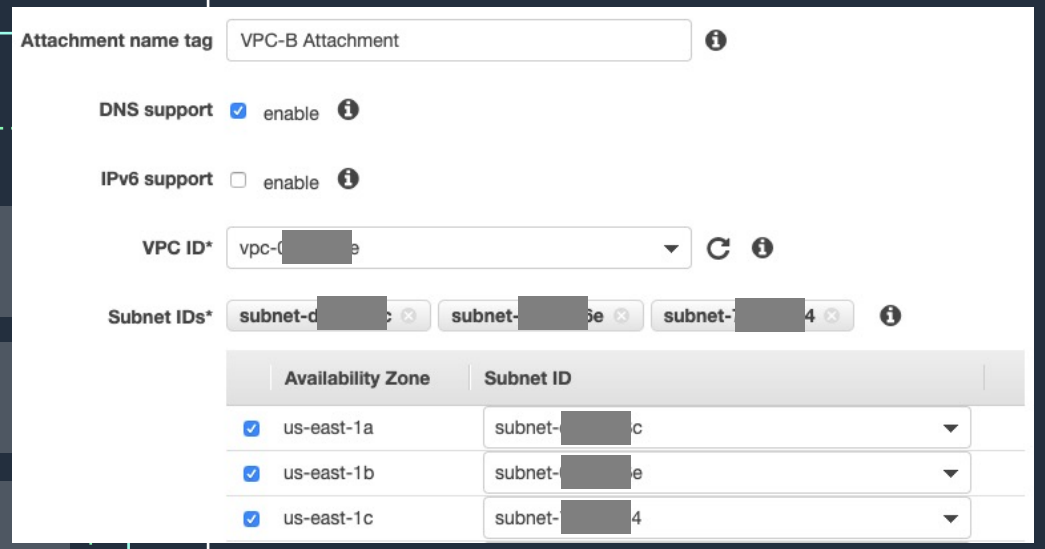
Multiple VPCs access models – AWS Transit Gateway



TGW attachment

A single TGW attachment can span multiple Availability Zones





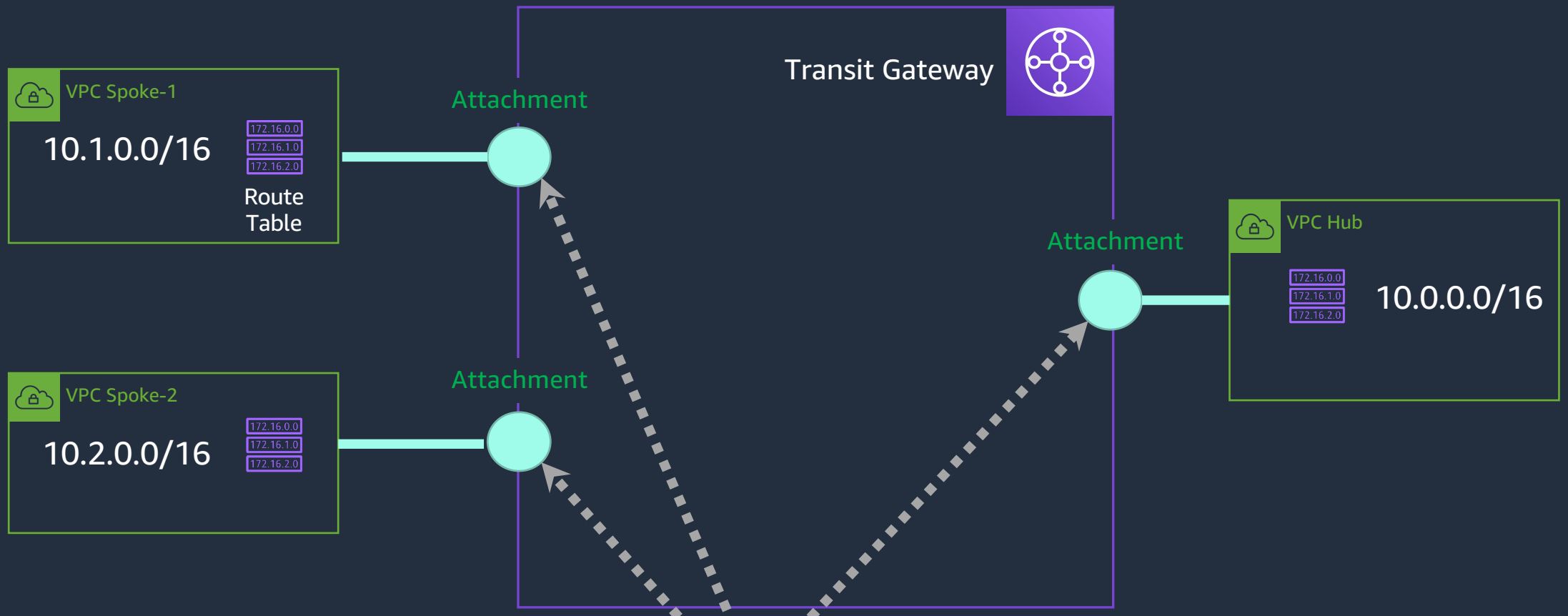
The best practice is to have an attachment in every AZ
Dedicate subnets for the VPC attachment (/28)

AWS Transit Gateway attachments

- You can attach the following resources to your transit gateway:
- One or more VPCs
- One or more VPN connections
- One or more AWS Direct Connect gateways
- One or more transit gateway peering connections
- Software-Defined Wide Area Network (SD-WAN) appliances

TGW Route Tables

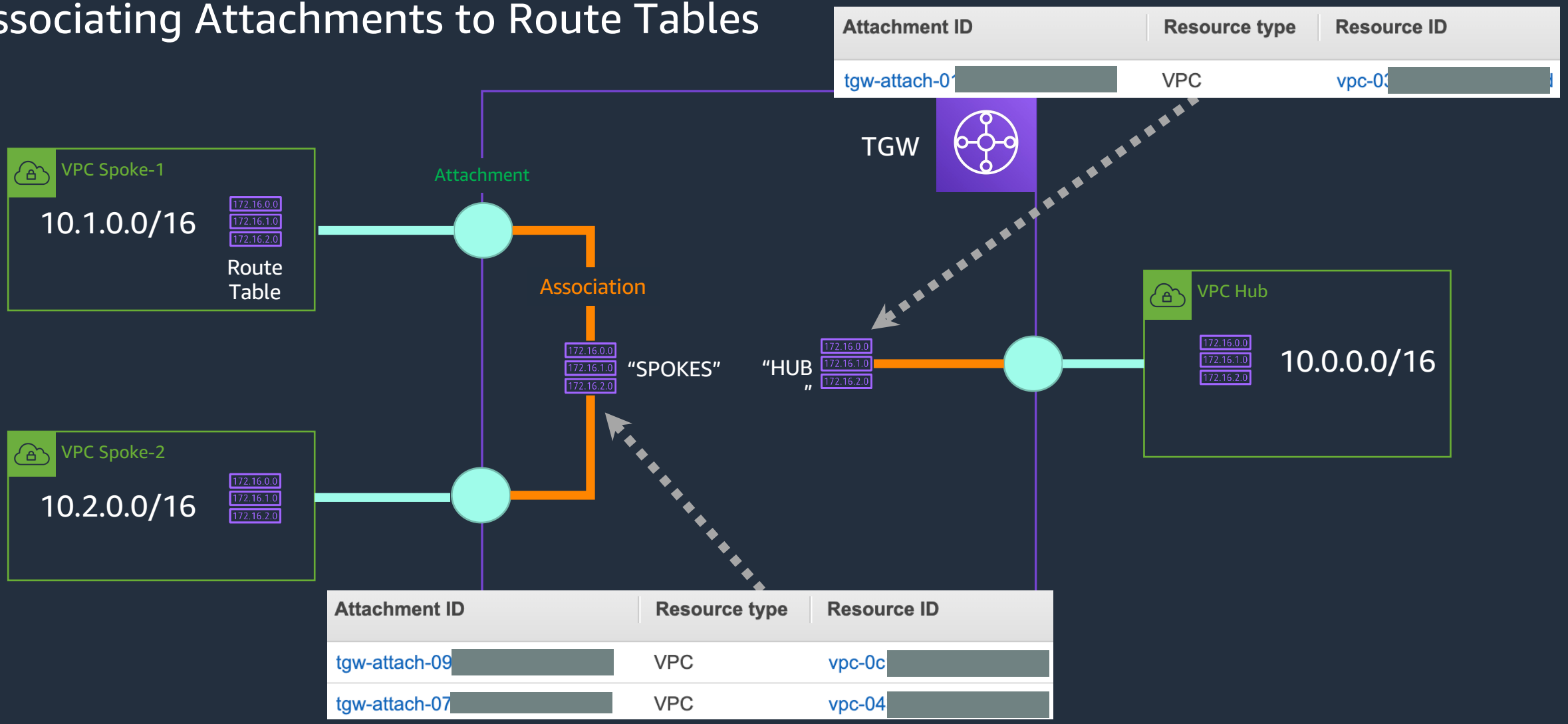
Attaching VPCs to AWS Transit Gateway



Name	Transit Gateway attachment ID	Transit Gateway ID	Resource typ	Resource ID
Hub	tgw-attach-011[redacted]	tgw-032[redacted]	VPC	vpc-036[redacted]
Spoke-1	tgw-attach-09b[redacted]	tgw-032[redacted]	VPC	vpc-0c1[redacted]
Spoke-2	tgw-attach-072[redacted]	tgw-032[redacted]	VPC	vpc-043[redacted]

TGW Route Tables

Associating Attachments to Route Tables



Connection to on-premises

AWS Site-to-Site VPN Components

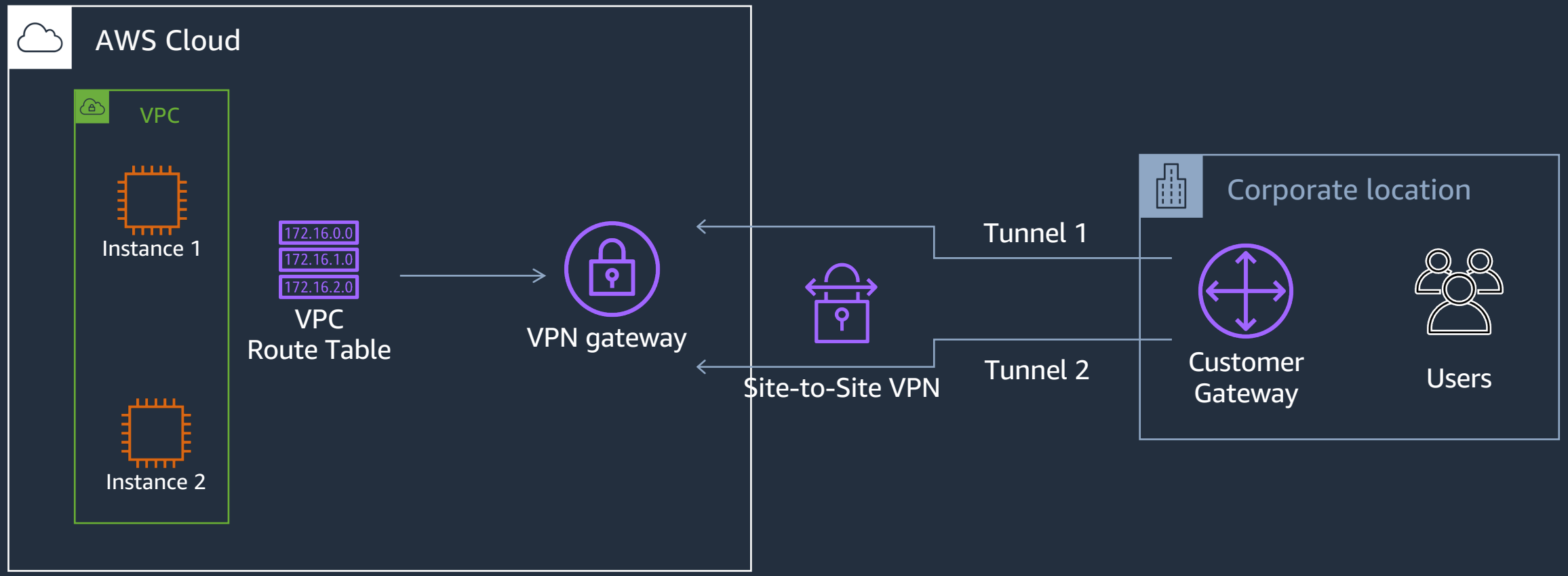
Customer Gateway

Virtual Private Gateway

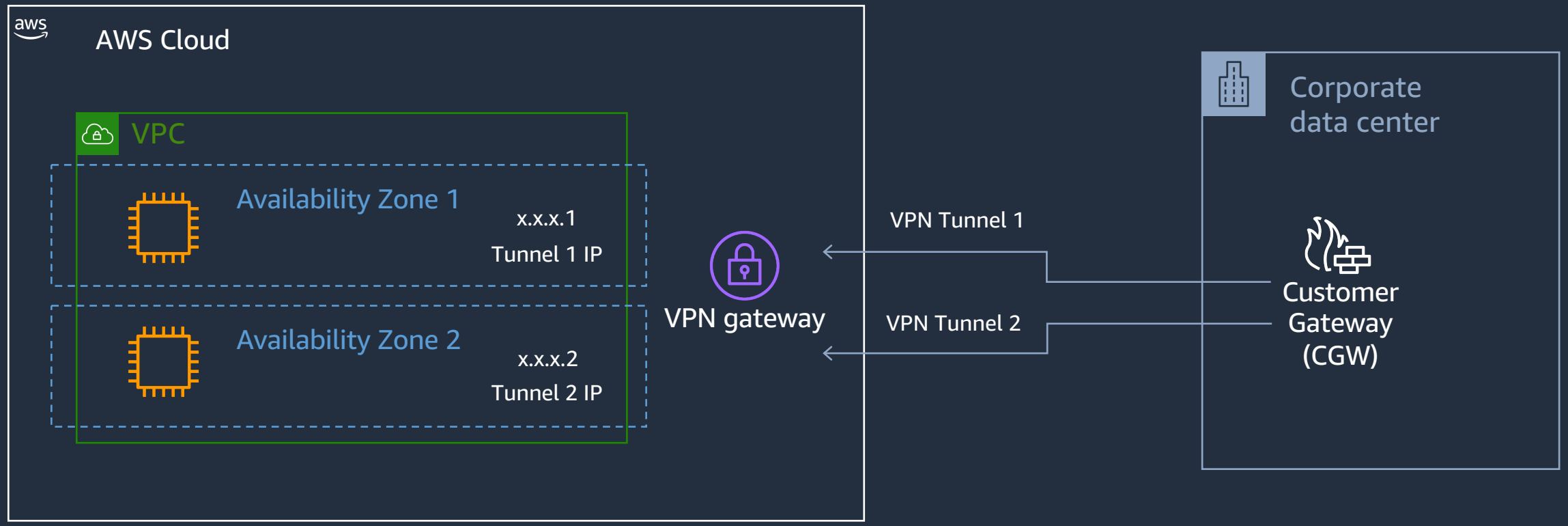
Transit Gateway

AWS Global Accelerator

Connecting corporate network to AWS VPC

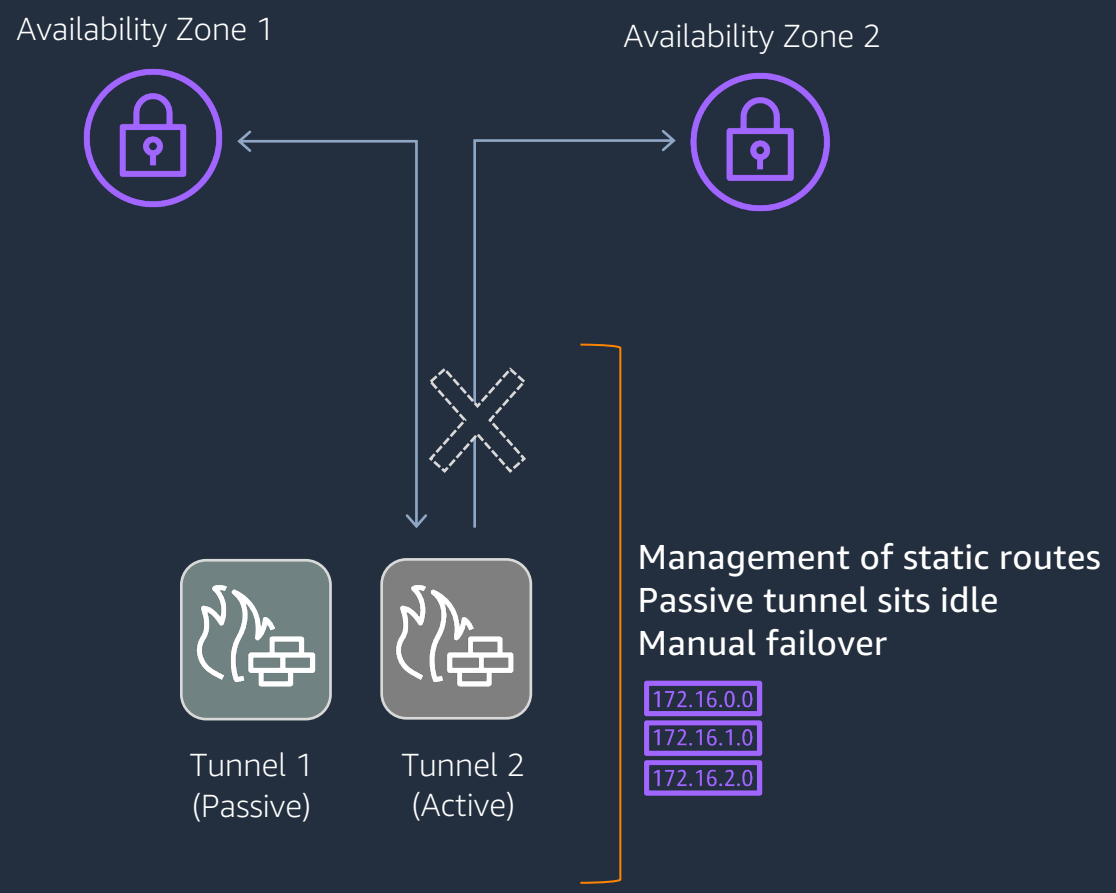


AWS Site-to-Site VPN Fault Tolerance: At-a-Glance

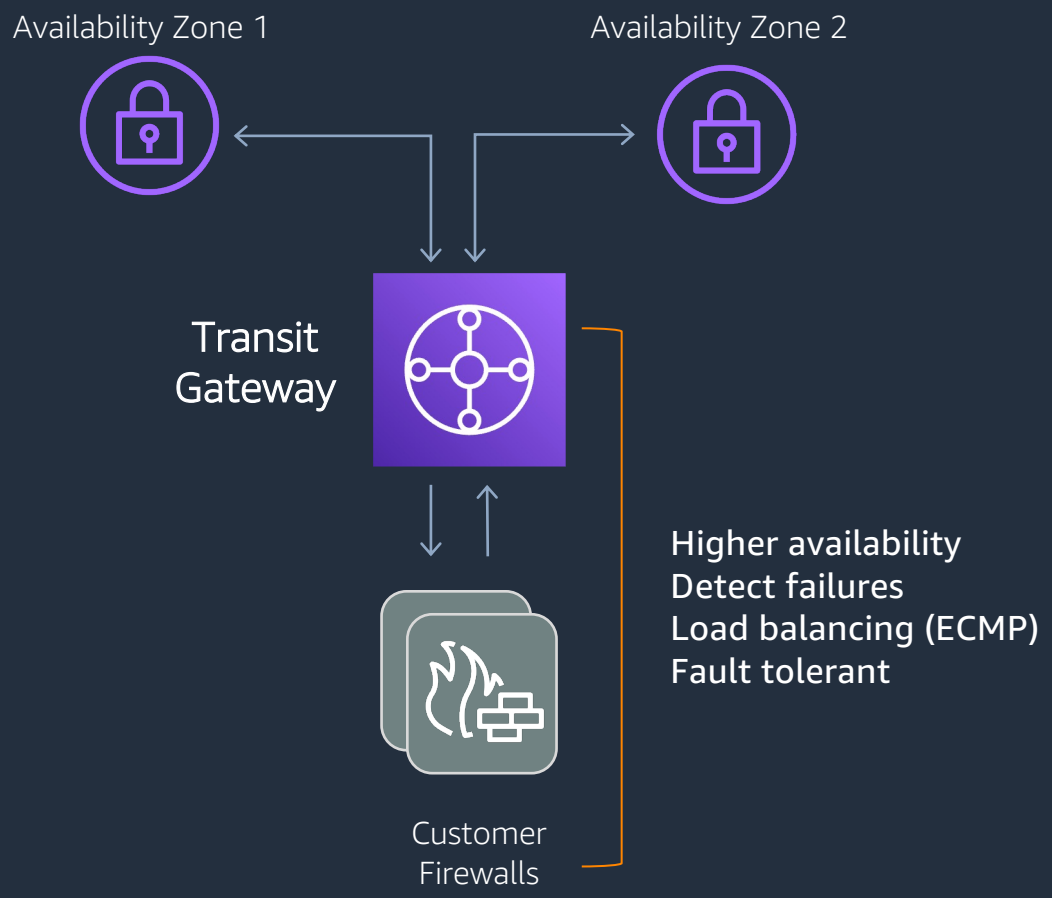


Routing With AWS Site-to-Site VPN

Static Routing



Dynamic Routing using BGP with AWS Transit Gateway



Accelerated Site-to-Site VPN

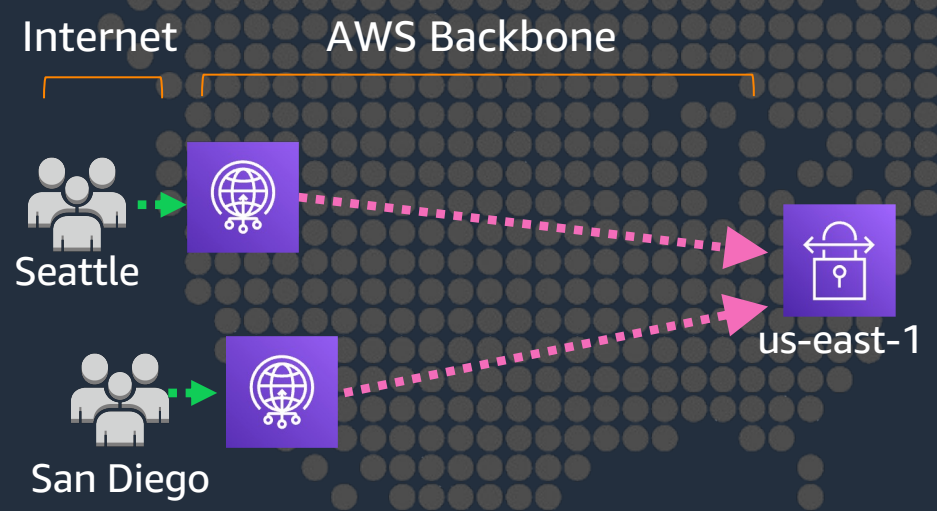
Uses AWS network

80+ global edge locations

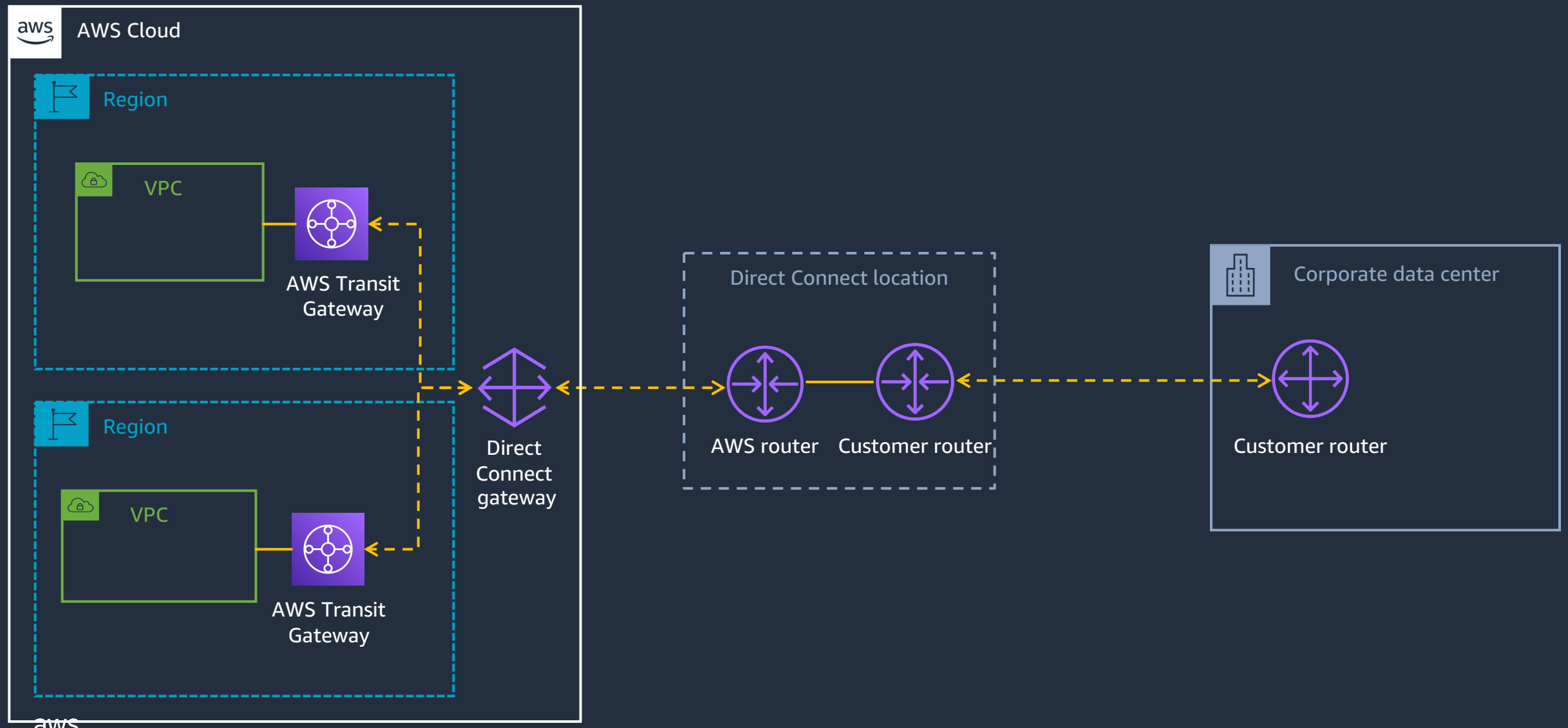
Reduce latency

Static anycast IP addresses

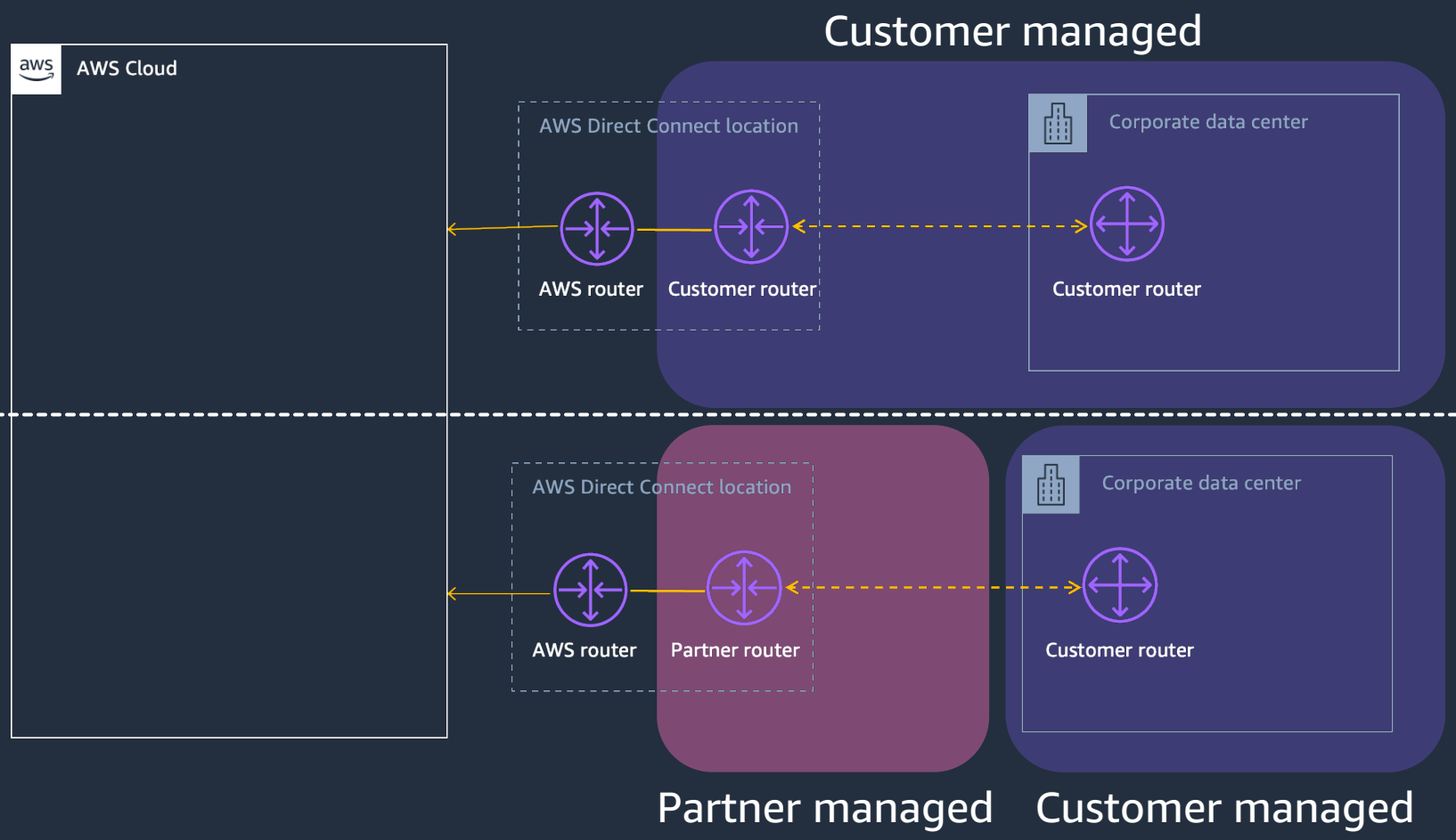
Increase traffic performance by up to 60%



Connectivity using AWS Direct Connect



Hosted vs. dedicated connections



Dedicated

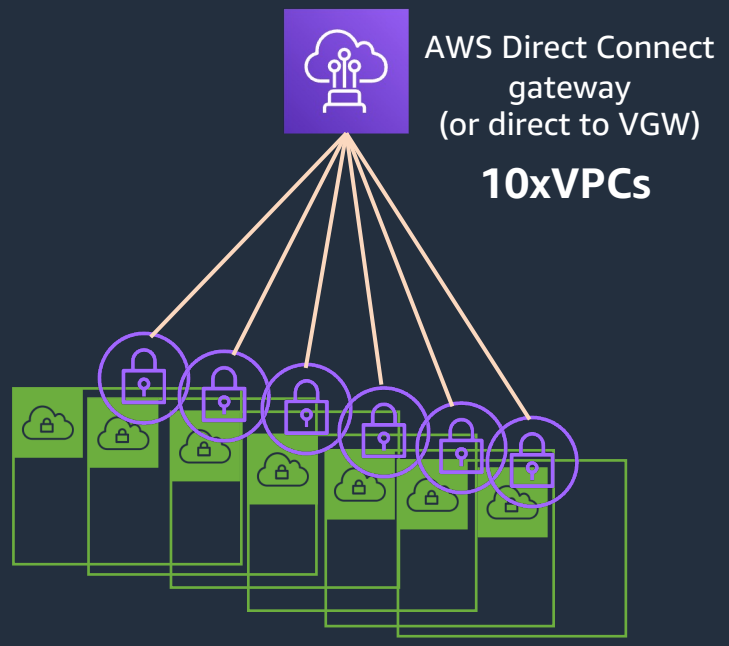
- 1 Gbps, 10 Gbps, 100 Gbps
- 51x virtual interfaces
  - 50x private or public VIF
  - 1x transit VIF

Hosted

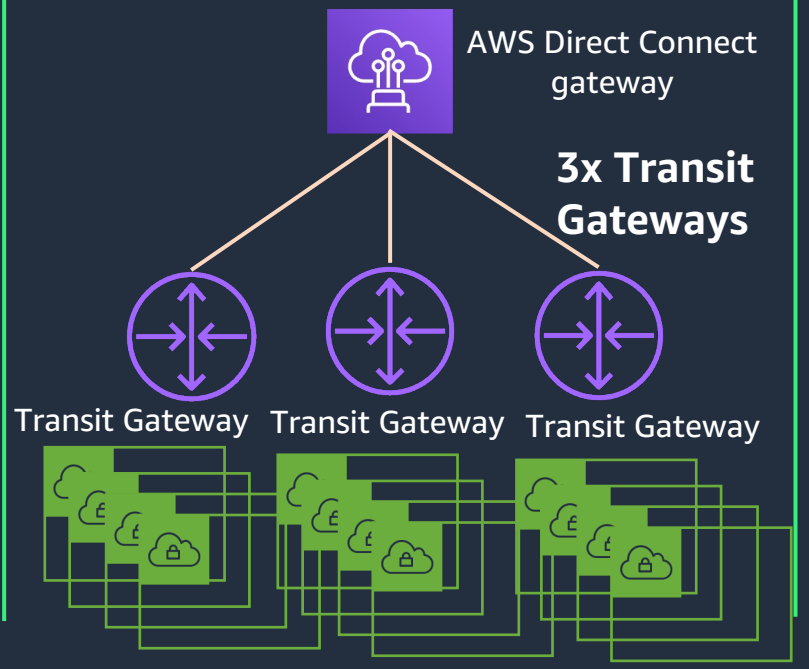
- 50 Mbps → 10 Gbps
- 1 x virtual interface
  - Private, Public or Transit

Direct Connect – Types of virtual interfaces

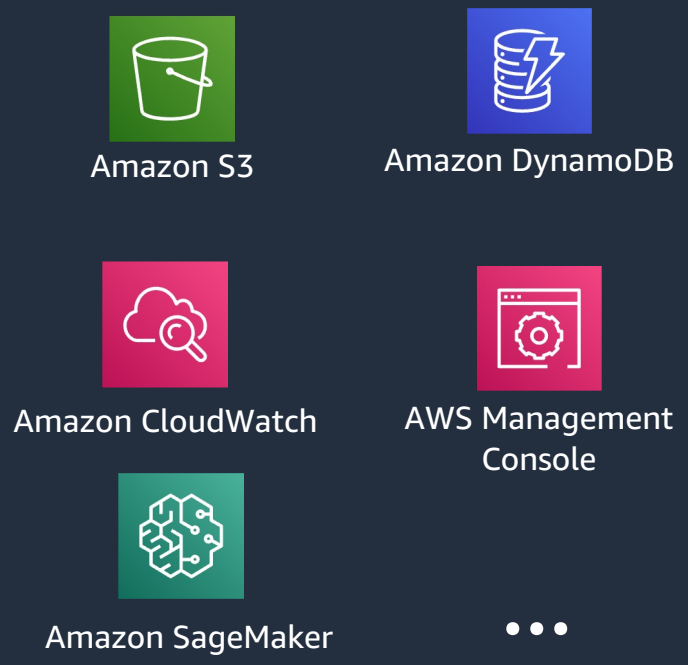
Private VIF



Transit VIF

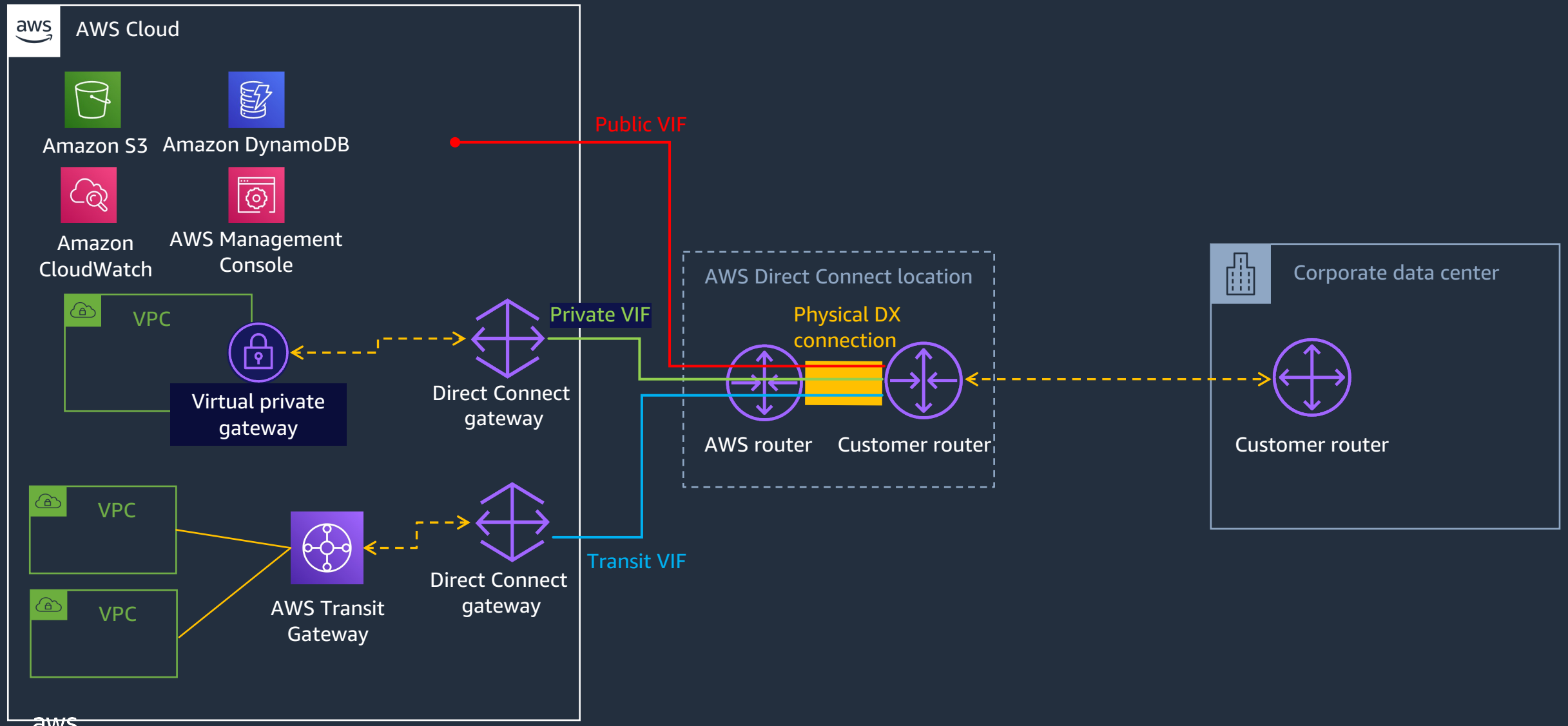


Public VIF

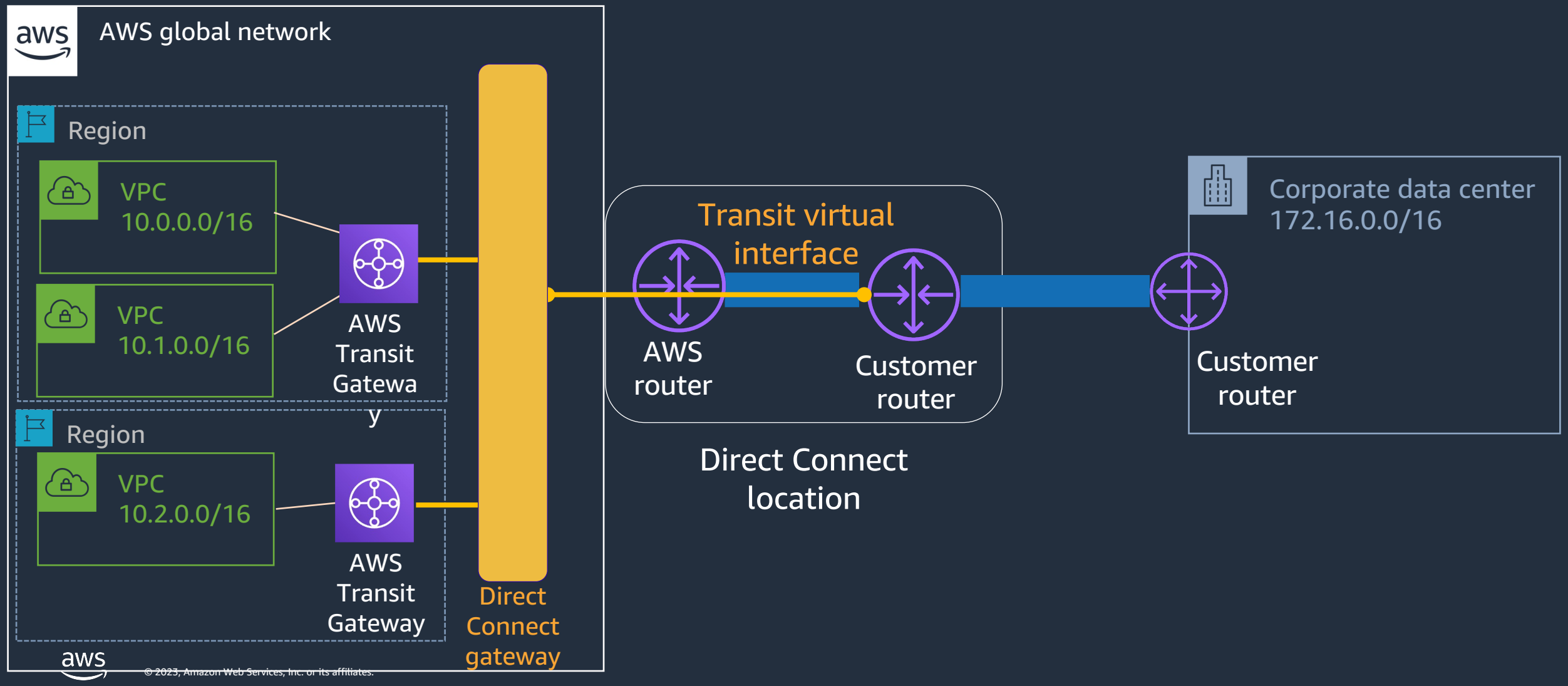


Virtual Interface = VLAN + eBGP session
IPv4 and IPv6 eBGP peering sessions supported on all the above virtual interface types

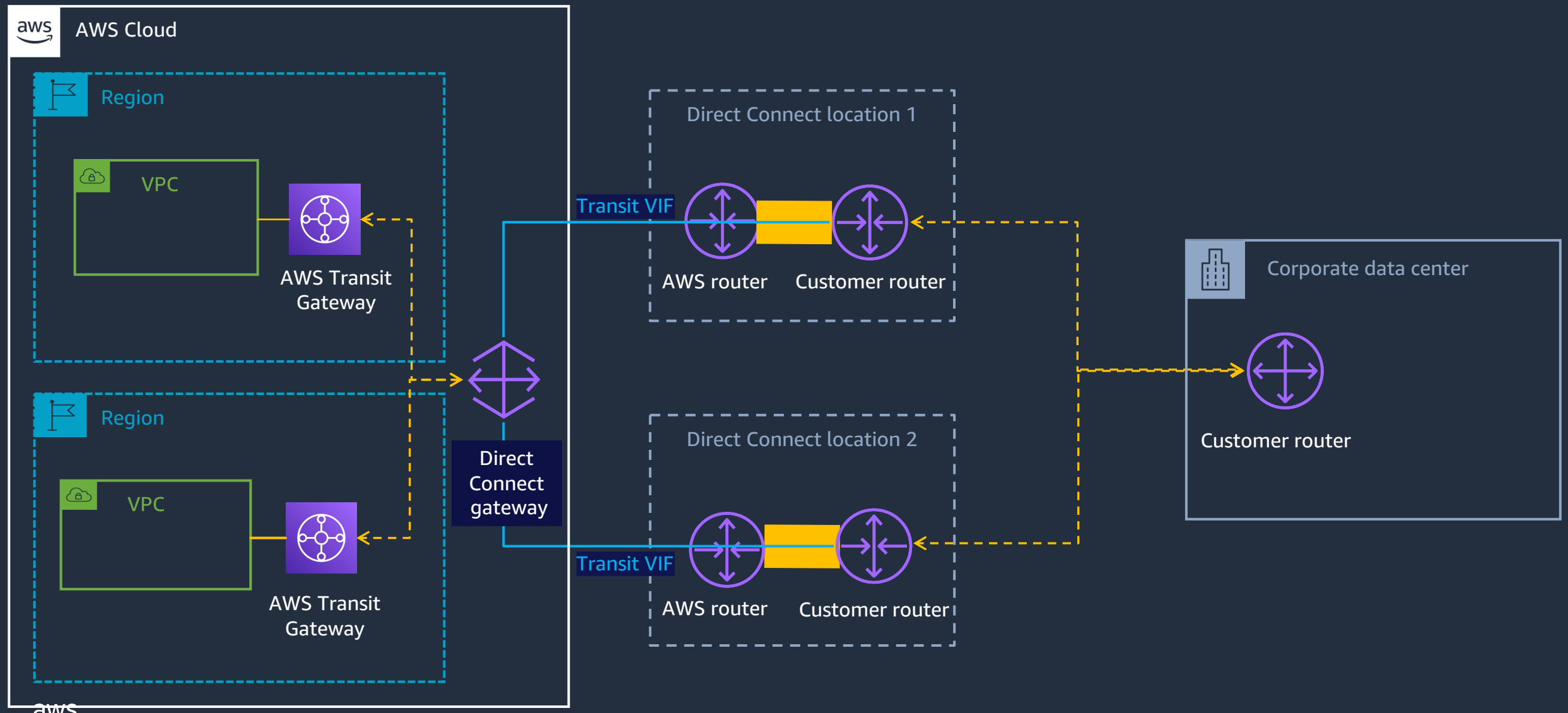
Direct Connect – VIFs



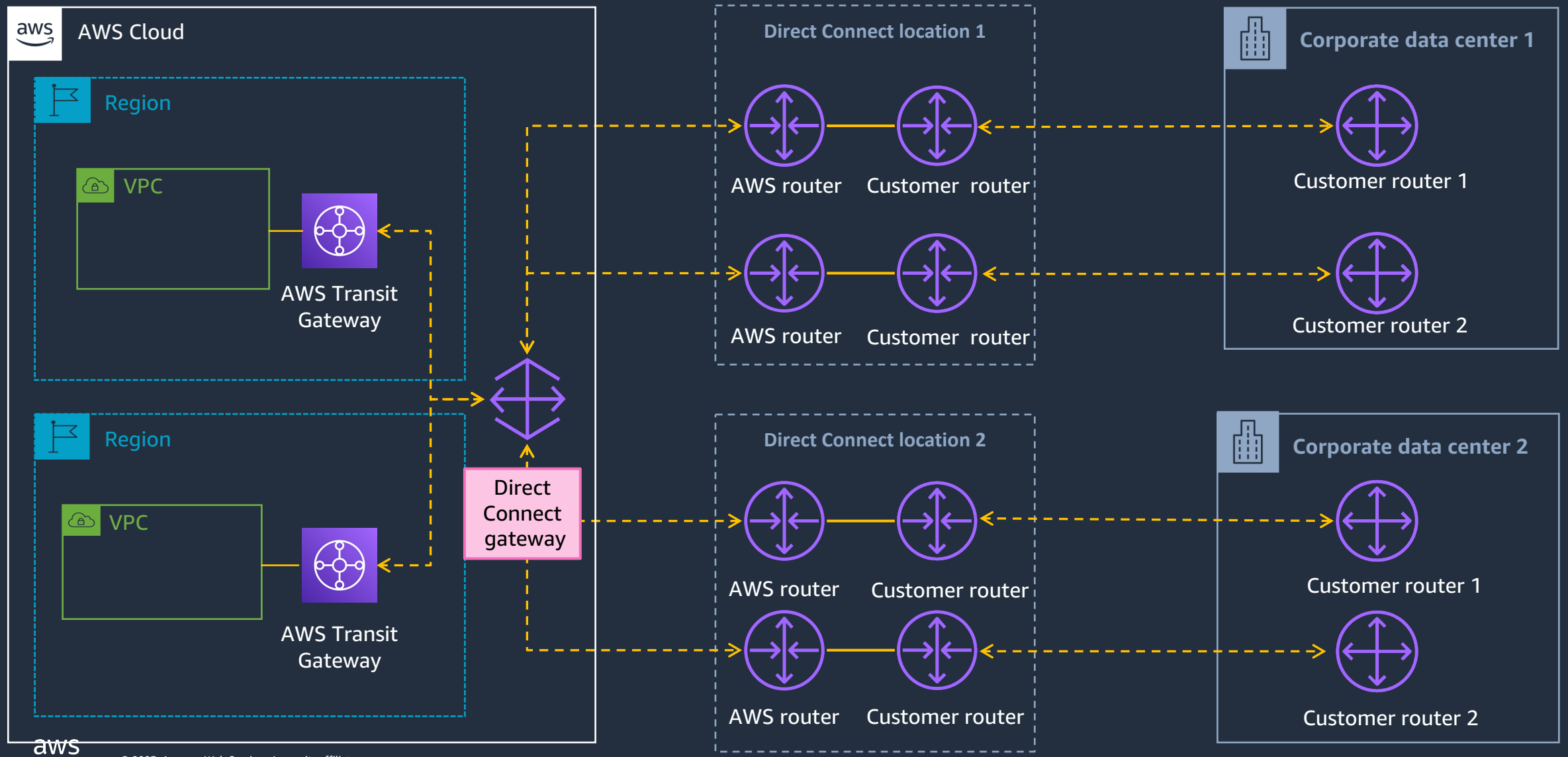
AWS Transit Gateway with Direct Connect gateway



Building high resiliency for Direct Connect

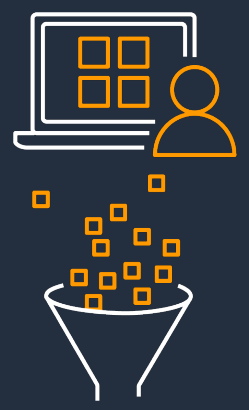


Direct Connect – Maximum Resiliency



AWS Network Firewall

Common use cases and architectures for AWS Network Firewall



Ingress Filtering

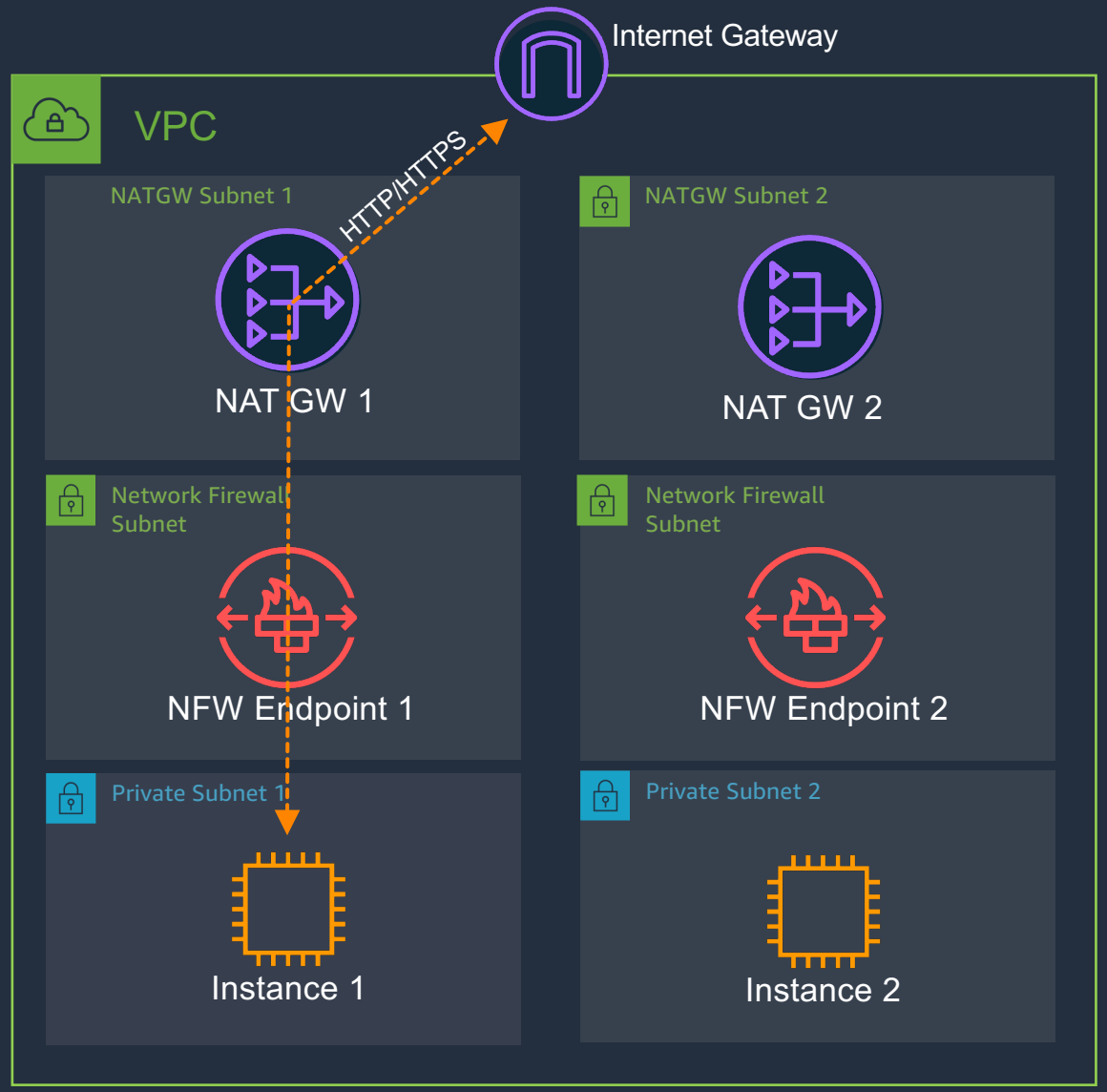
Egress Filtering

VPC-to-VPC Inspection

Use case: Ingress and egress filtering

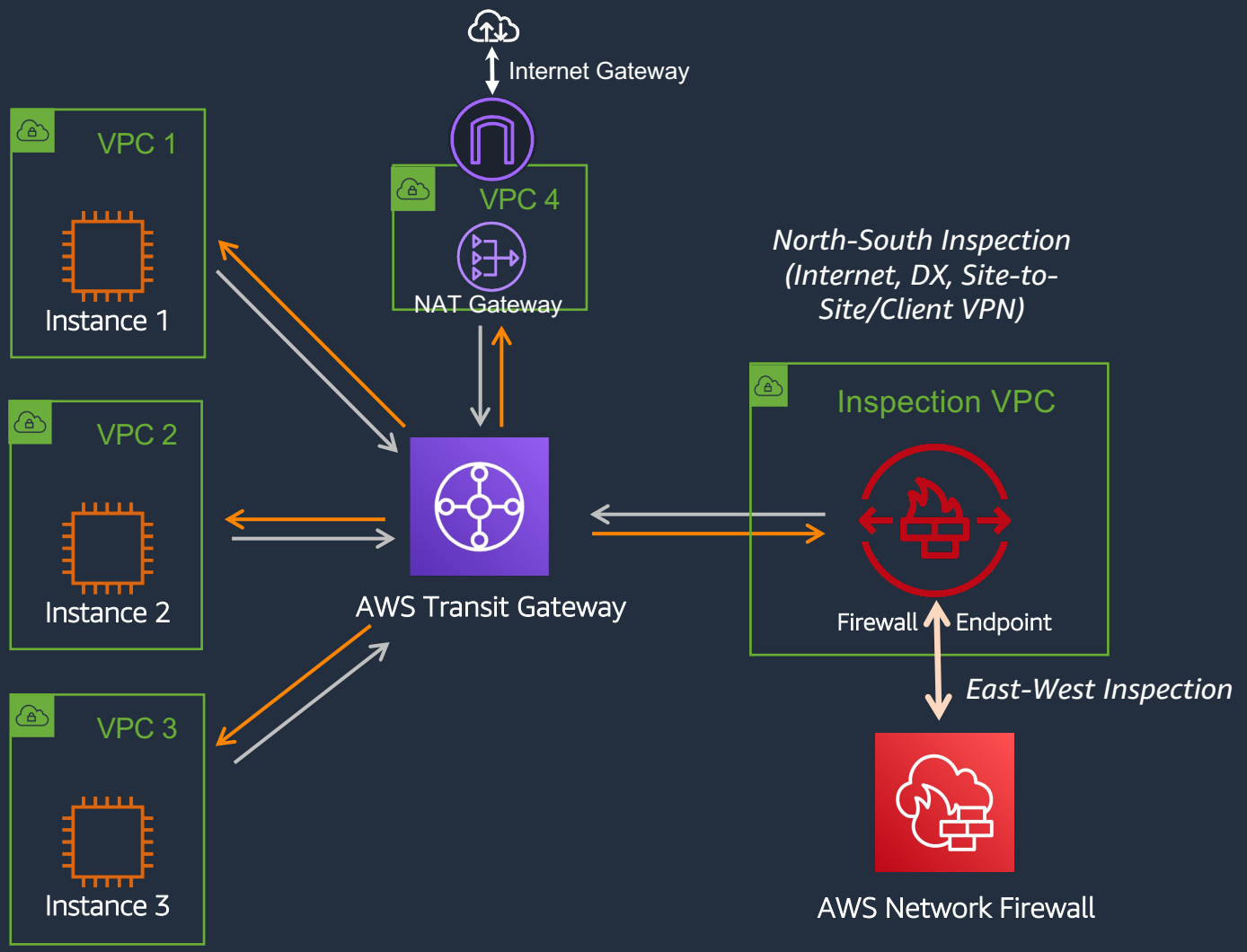
PREVENT INTRUSIONS, PROTECT AGAINST UNAUTHORIZED OUTBOUND TRAFFIC AND MALWARE

- Filter HTTP/HTTPS traffic based on domain name
- AWS managed domain lists and threat signatures across 16 categories including coin mining, phishing, botnets, scanners, web attacks, and emerging events
- Proactively block unused ports and protocols from exiting VPC
- Improve logging and threat detection of network traffic
- Use AWS Solutions to integrate with Amazon GuardDuty and update rules with data from latest findings



Inspection of VPC-to-VPC traffic

SAFEGUARD VPCs THROUGH LOGICAL SEPARATION FOR WORKLOADS



- Centralized inspection for east-west and north-south traffic flows
- 100 Gbps per endpoint throughput and reduce total firewall endpoint hours
- Optionally use AWS Transit Gateway to inspect traffic from other VPCs, AWS Regions, and on-premise data centers

AWS Web Application Firewall (AWS WAF)

AWS WAF (Web Application Firewall)

Protect your application against DDoS attacks, Web Attacks and Bot Attacks.

AWS WAF

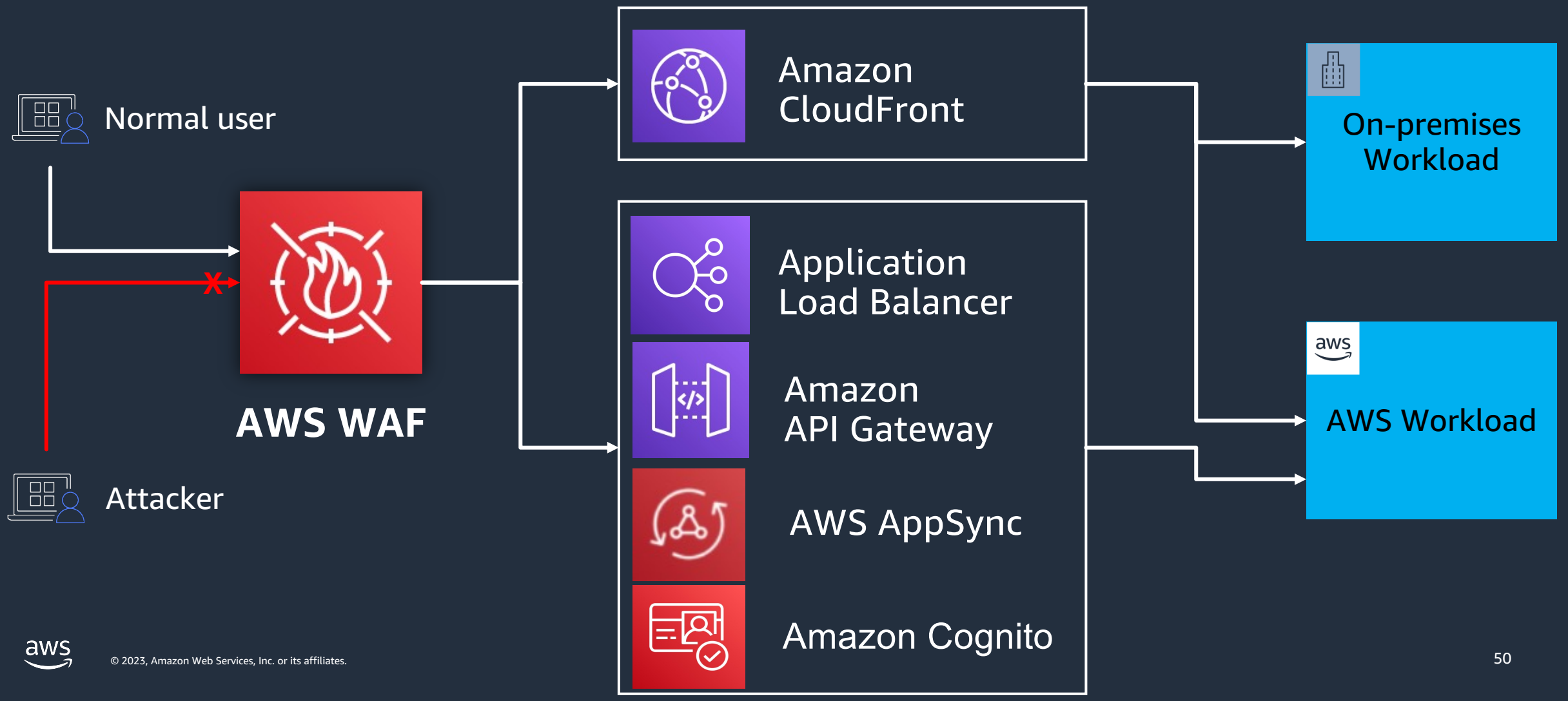
Multi layered security controls to protect against sophisticated attacks

Low operation overhead: Fully managed service with ready to use built-in rules

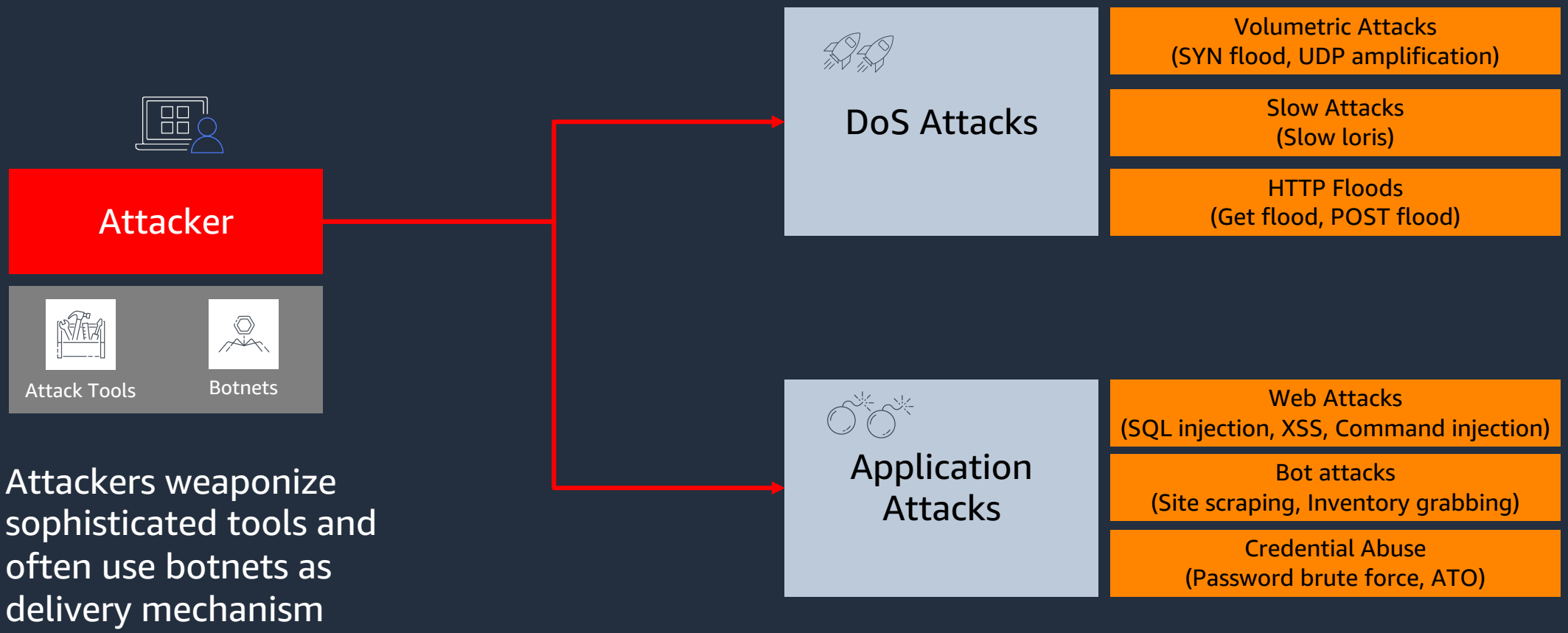
Customizable security: Customer customizable rules available

Frictionless set up: No application change required

Protect AWS and On-premises applications



Threat landscape



Attackers weaponize sophisticated tools and often use botnets as delivery mechanism

Rule Based Controls

Rule based controls provide protection against attacks that attempt to compromise servers and exfiltrate data. HTTP requests are inspected to check the presence of malicious payloads.

AWS Managed Rules

AWS provides built in rules for common attack vectors such as SQLi, XSS, Command injection etc.

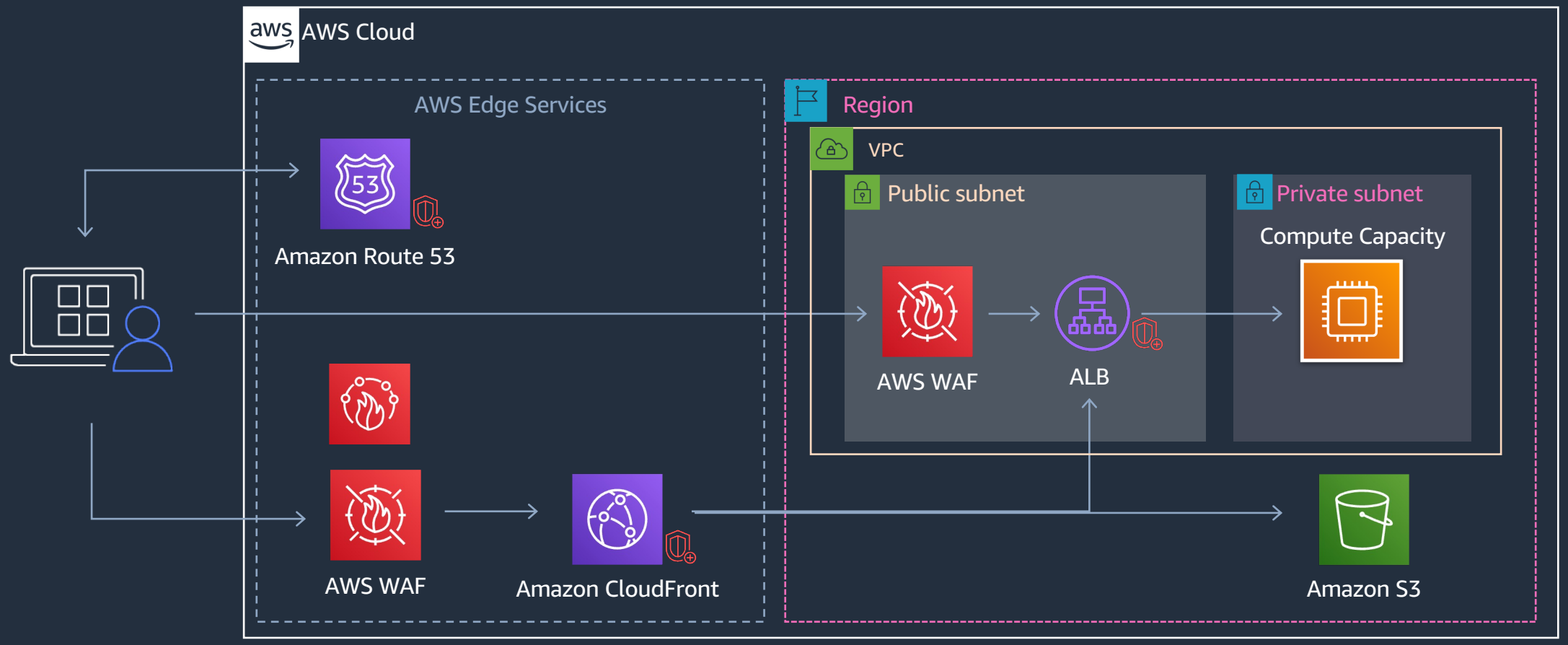
Customer Managed Rules

Customers can create their own rule to match their specific needs. Useful against new vulnerabilities and system specific defenses.

Third Party Rules

A list of third party rules available. Customers can easily deploy these rules to strenghten the defense posture.

Protecting web applications



Shield Advanced protected resource

Thank you!