

AWS Networking Simplified - A Comprehensive Tour of Key Features

Samuel Baruffi

Senior Solutions Architect @ AWS



Table of contents

Global infrastructure

Amazon Virtual Private Cloud (Amazon VPC)

Basics of Amazon VPC security

Peering, endpoints, gateways, and global connectivity

Simplify service-to-service connectivity (VPC Lattice)

Traffic visibility and monitoring

Global infrastructure



AWS Global Infrastructure

32 Launched Regions, 102 Availability Zones and 450+ Points of Presence



United States

GovCloud (U.S.):

U.S.-East (3), US-West (3)

U.S. West

Oregon (4), Northern California (3)

U.S. East

N. Virginia (6), Ohio (3)



Canada

Central (3)



Africa

Cape Town (3)



Middle East

Bahrain (3)

UAE (3)



Asia Pacific

*Beijing, operated by Sinnet (3)

*Ningxia, operated by NWCD (3)

Hong Kong (3)

Hyderabad (3)

Jakarta (3)

Mumbai (3)

Osaka (3)

Seoul (4)

Singapore (3)

Tokyo (4)

Israel (3)



South America

São Paulo (3)



Australia

Sydney (3)

Melbourne (3)

Latest Region & number of Availability Zones (AZs) can be found here [AWS global infrastructure page](#)

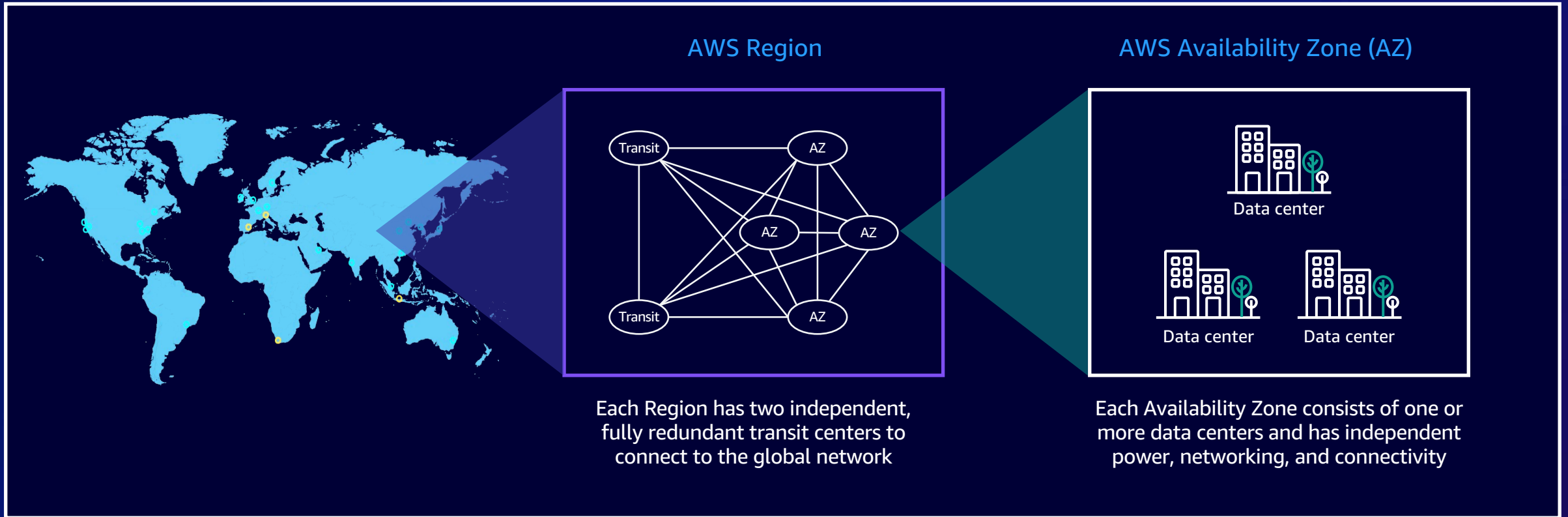
* To comply with China's legal and regulatory requirements, AWS has collaborated with Sinnet and NWCD, the local partners in China for delivering cloud services within AWS China (Beijing) Region and AWS China (Ningxia) Region respectively.

© 2023, Amazon Web Services, Inc. or its affiliates.



Fault tolerance in our physical infrastructure

AWS REGIONS ARE COMPRISED OF MULTIPLE AZS FOR HIGH AVAILABILITY AND SCALABILITY



AWS Region

AWS Availability Zone (AZ)

Each Region has two independent, fully redundant transit centers to connect to the global network

Each Availability Zone consists of one or more data centers and has independent power, networking, and connectivity

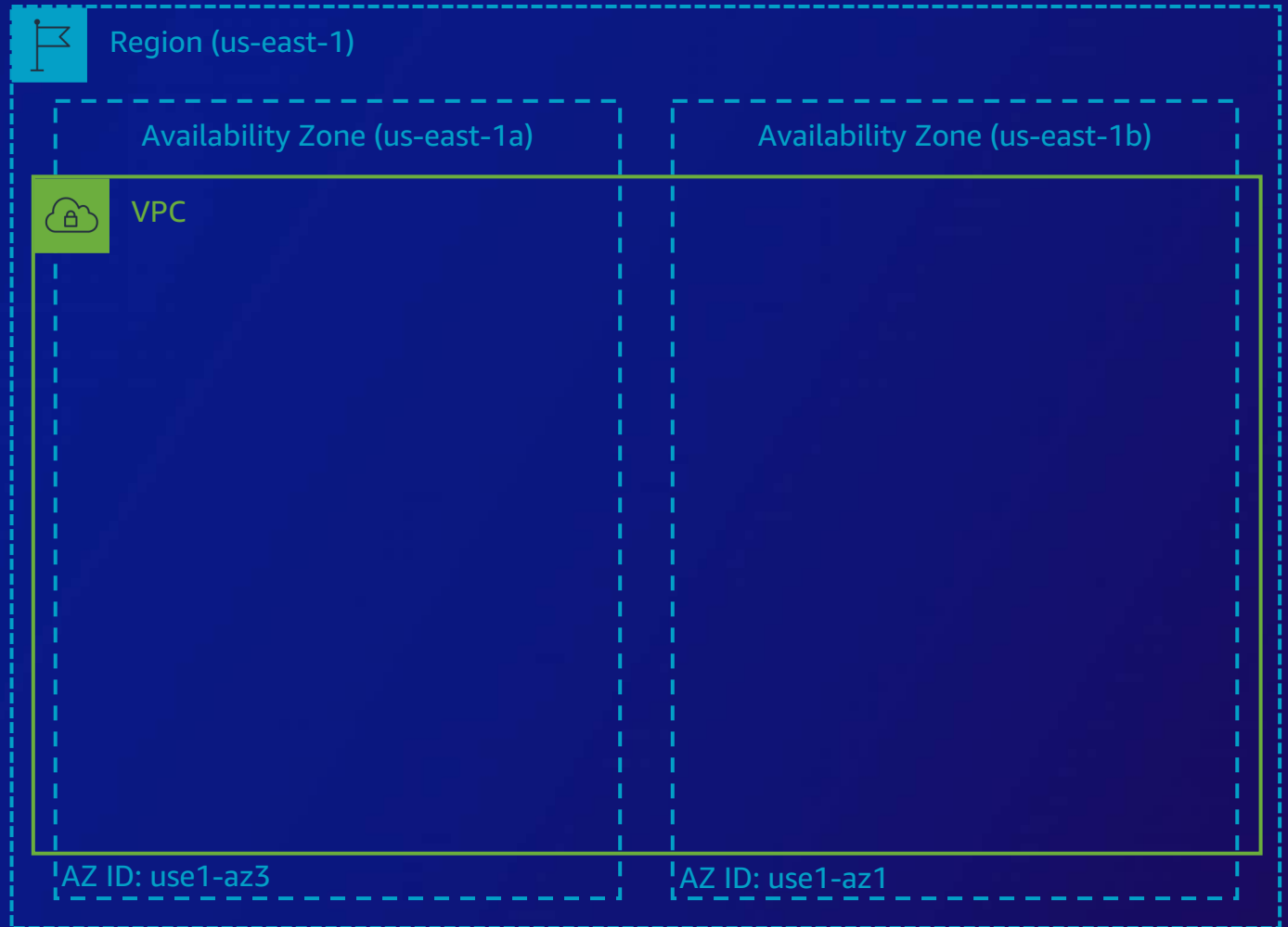
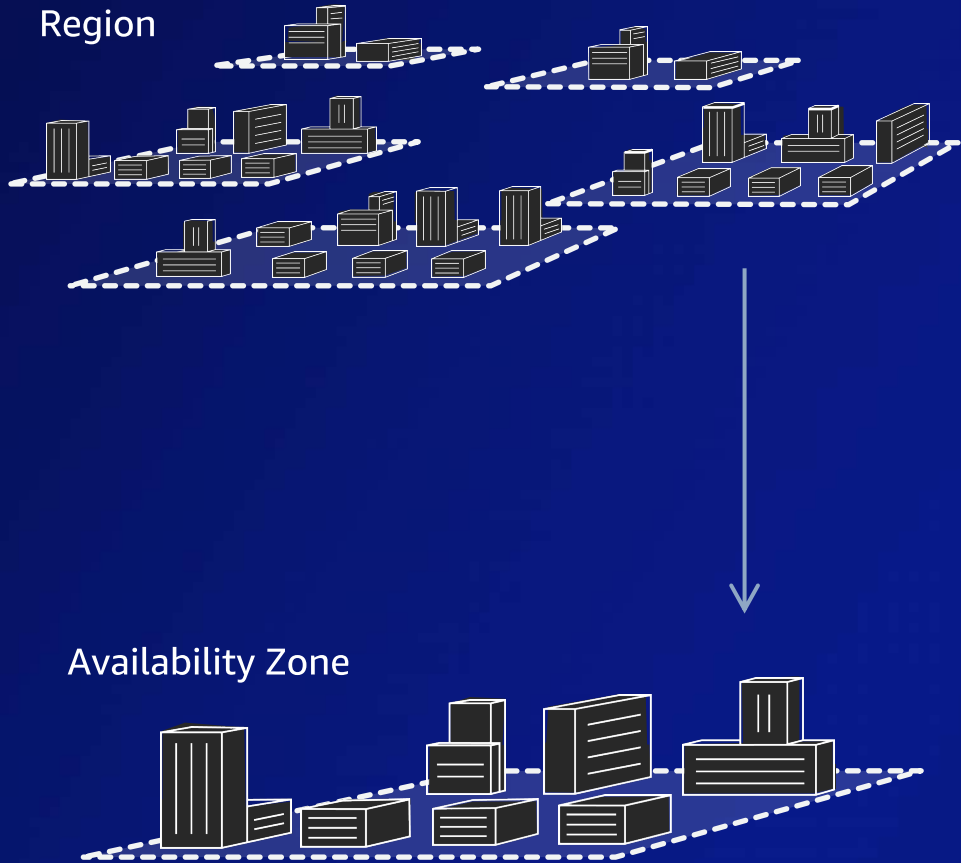
Amazon Virtual Private Cloud (Amazon VPC)



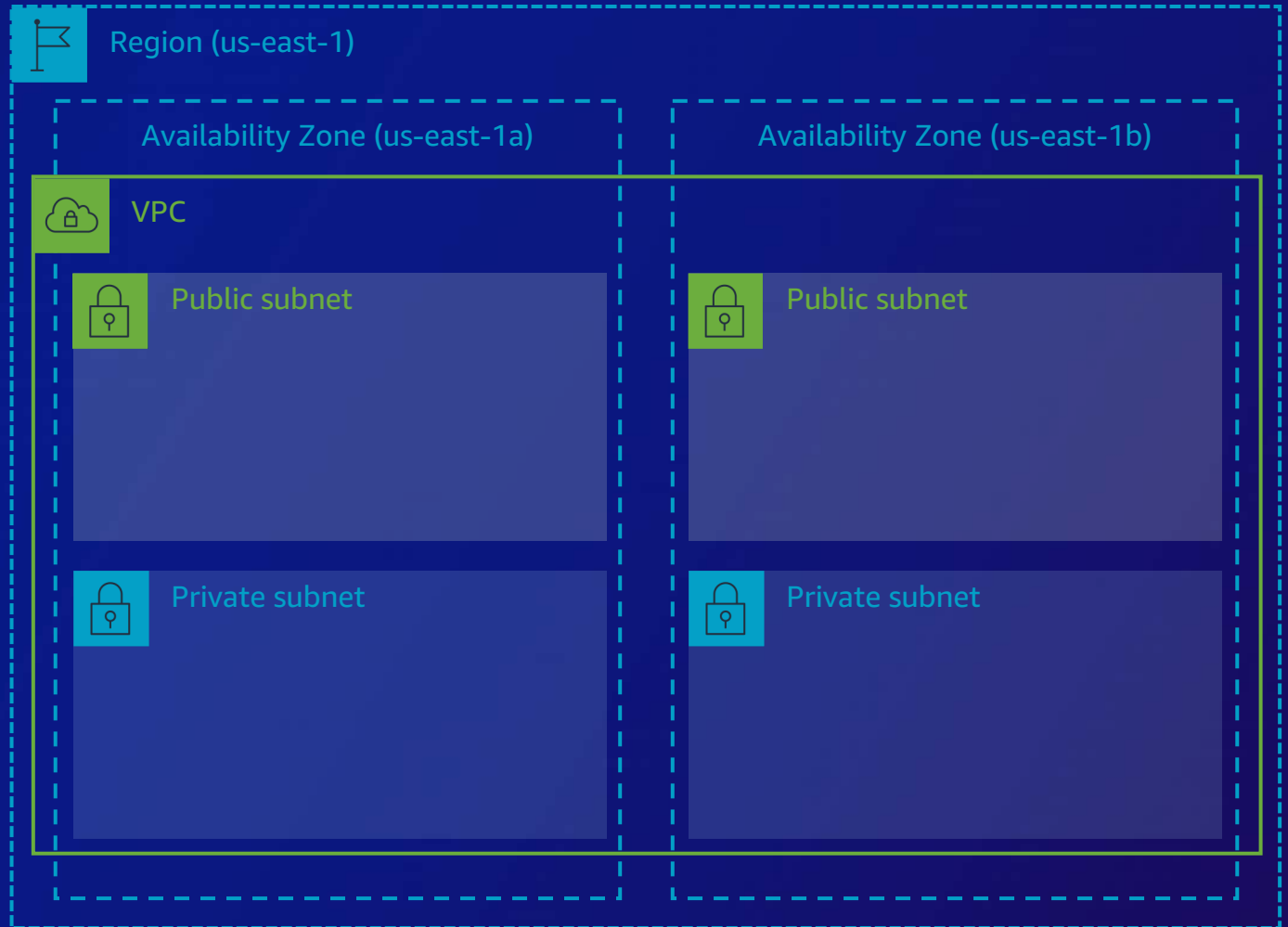
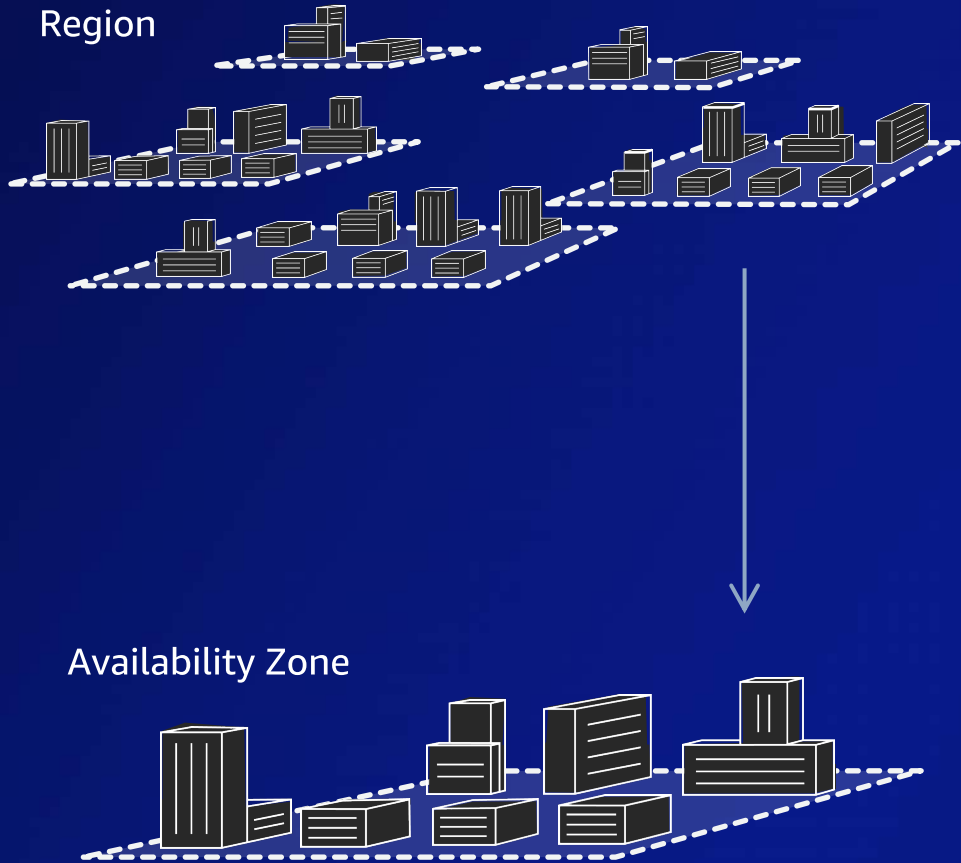
Building a VPC



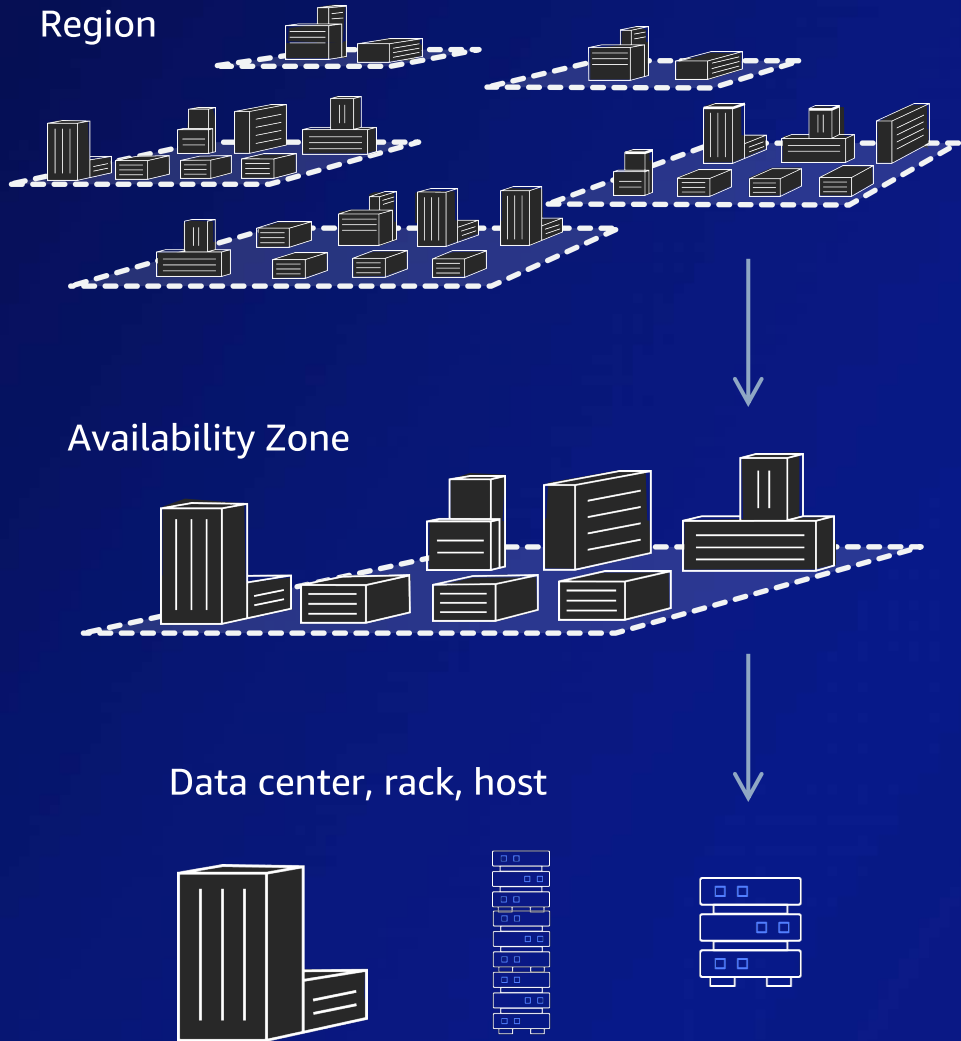
Building a VPC



Building a VPC



Building a VPC



IPv4 addressing

Reserved

10.0.0.0 – VPC Base

+ 2

10.0.0.2 – Route 53 Resolver

10.0.1.0 – Network Address

10.0.1.1 – VPC Router

10.0.1.2 – Reserved

10.0.1.3 – Reserved

10.0.1.255 – Network Broadcast

...

10.0.128.0 – Network Address

10.0.128.1 – VPC Router

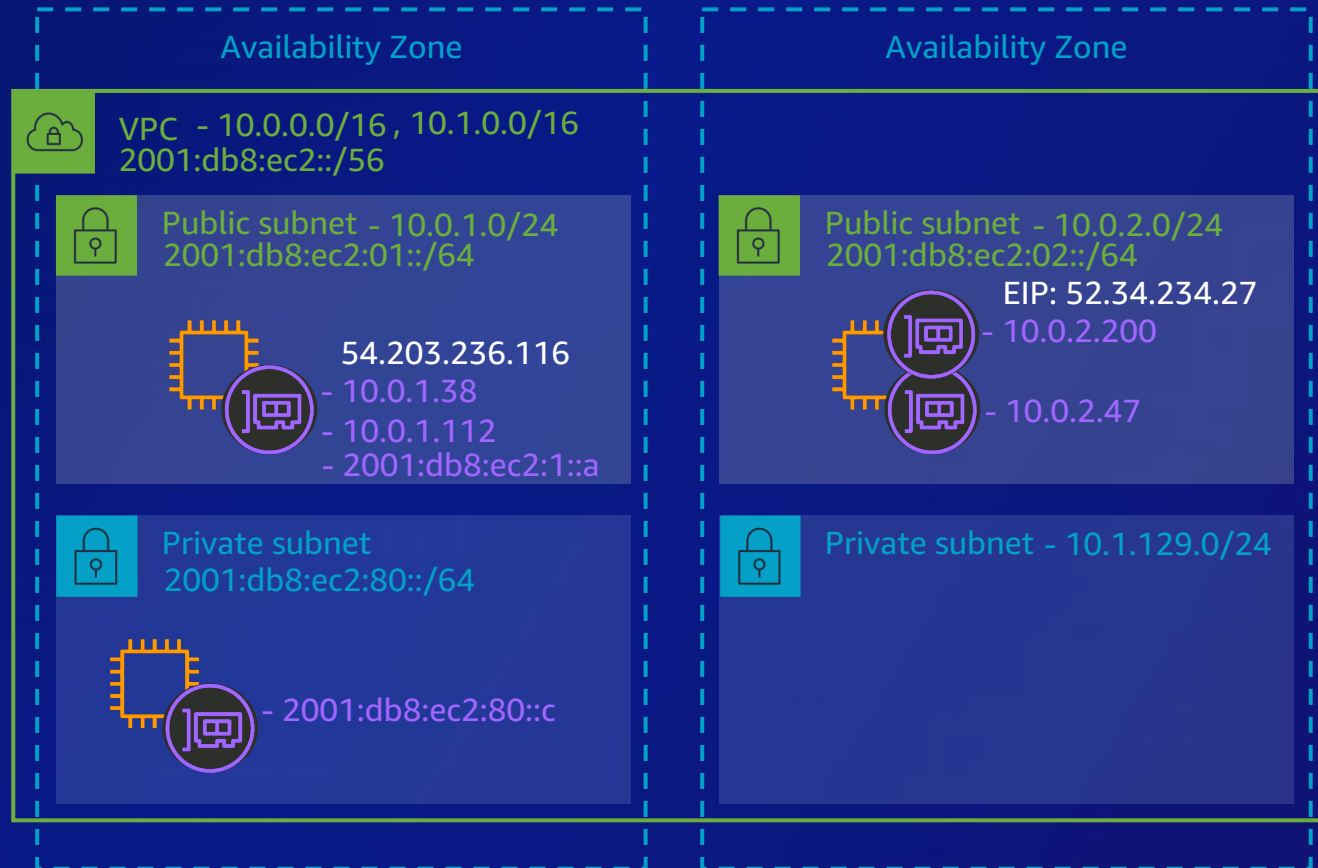
10.0.128.2 – Reserved

10.0.128.3 – Reserved

10.0.128.255 – Network Broadcast



IPv6 addressing



Reserved

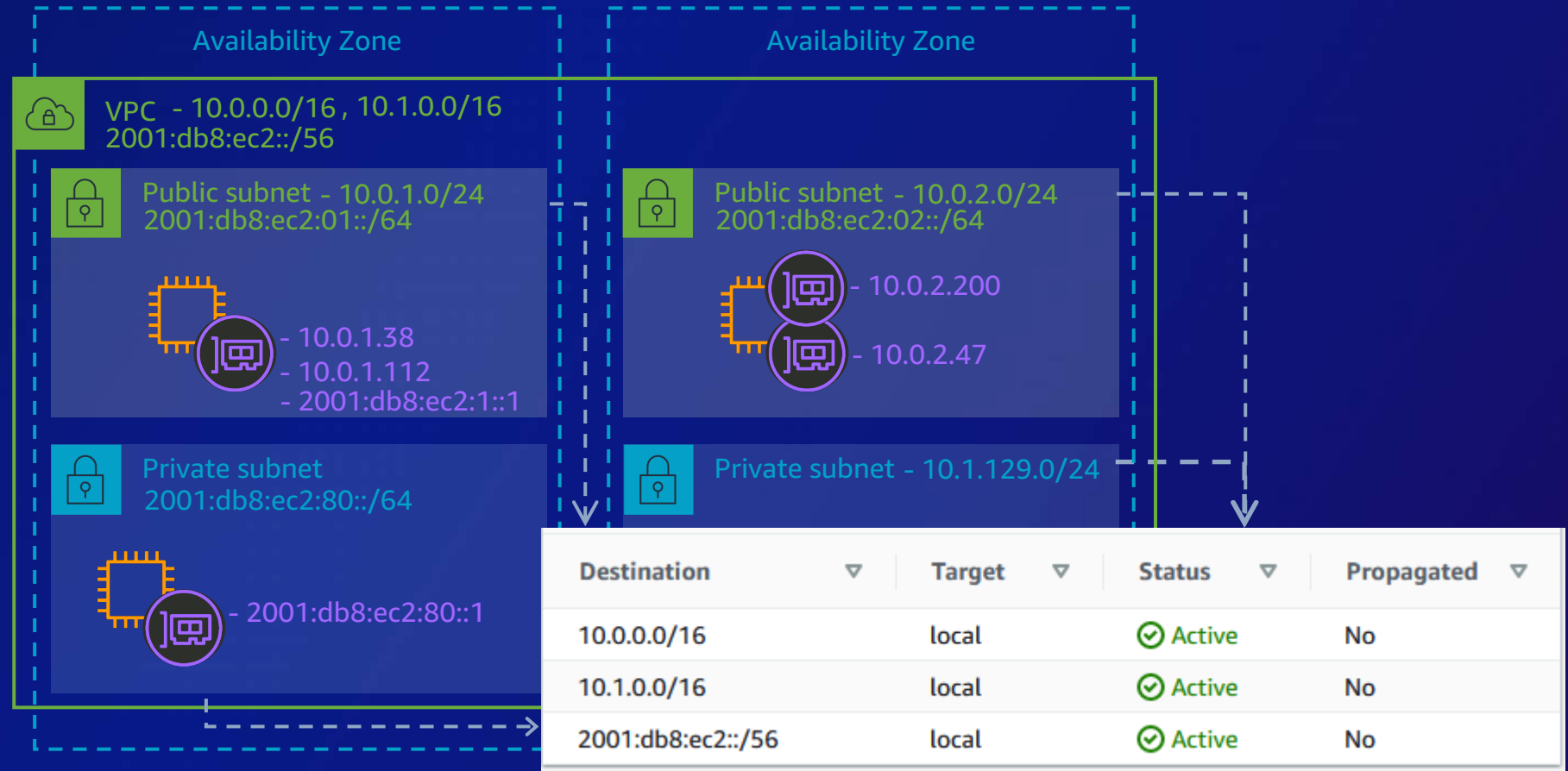
fd00:ec2::/32 - Reserved
fe80::X:Xff:feX:X/64 - VPC Router

2001:db8:ec2:01::0
2001:db8:ec2:01::1
2001:db8:ec2:01::2
2001:db8:ec2:01::3
2001:db8:ec2:01:ffff:ffff:ffff:ffff

...

2001:db8:ec2:80::0
2001:db8:ec2:80::1
2001:db8:ec2:80::2
2001:db8:ec2:80::3
2001:db8:ec2:80:ffff:ffff:ffff:ffff

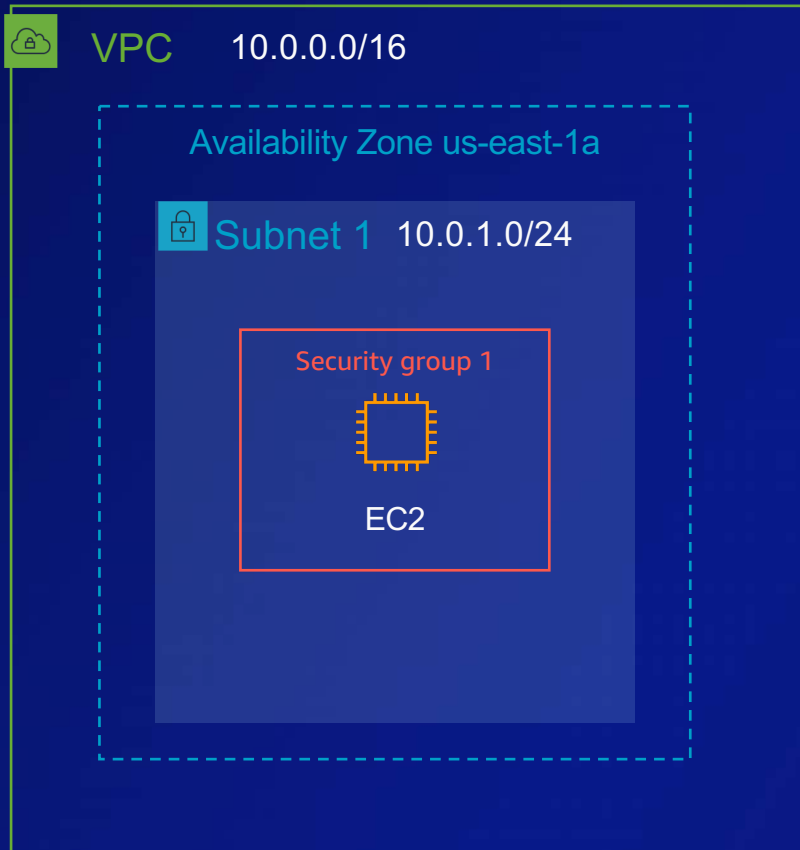
Intra-VPC routing



Basics of Amazon VPC security



Security Groups – Default Group Rules



Security Group 1

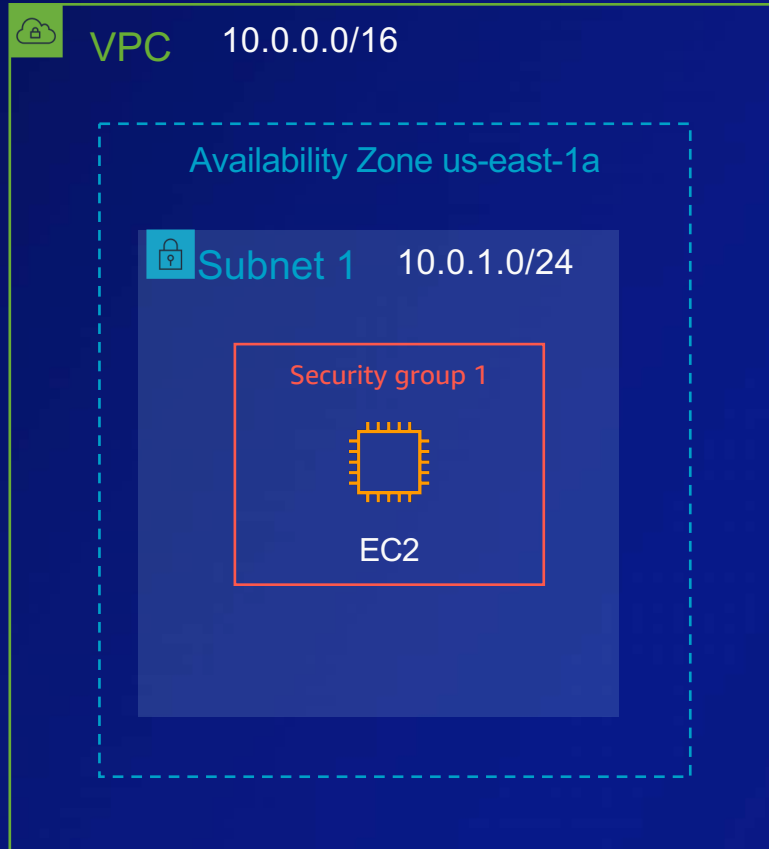
Inbound Rules

Protocol	Port	Source

Outbound Rules

Protocol	Port	Destination
All	All	0.0.0.0/0

Security Groups – Web Server Example



Security Group 1

Inbound Rules

Protocol	Port	Source
TCP	80	0.0.0.0/0

Outbound Rules

Protocol	Port	Destination
All	All	0.0.0.0/0

Security Groups – Reference other groups



Web server security group

Inbound Rules

Protocol	Port	Source
TCP	80	0.0.0.0/0

Outbound Rules

Protocol	Port	Destination
All	All	0.0.0.0/0

Database security group

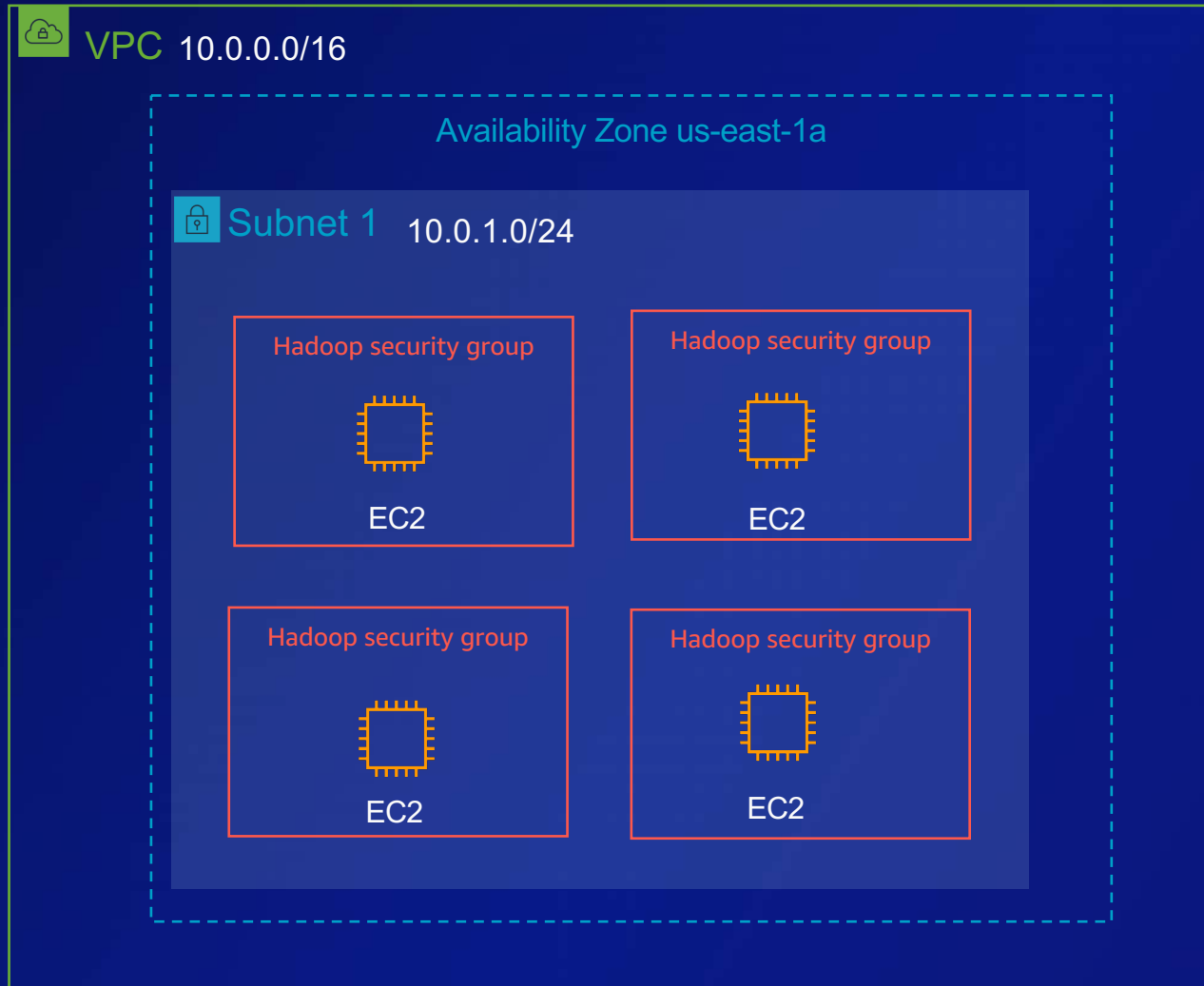
Inbound Rules

Protocol	Port	Source
TCP	3306	sg-webserver

Outbound Rules

Protocol	Port	Destination
All	All	0.0.0.0/0

Security Groups – Self-referencing rules



Hadoop Security Group

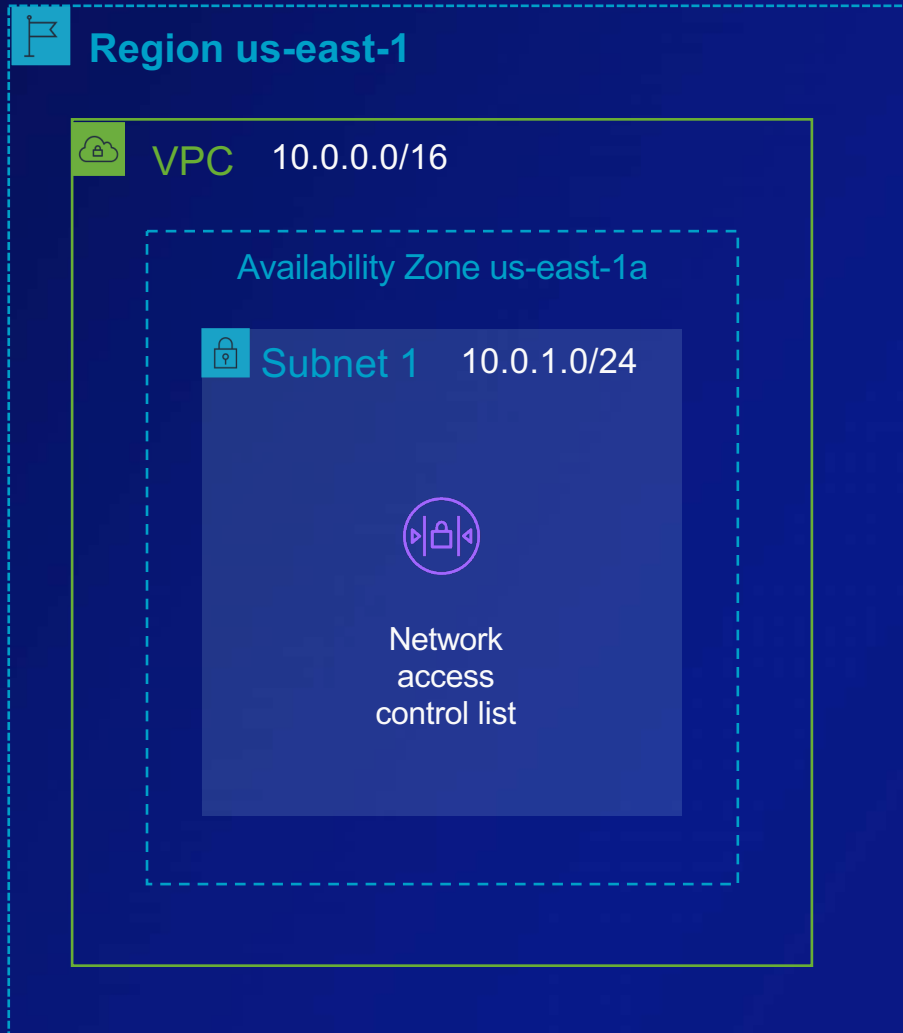
Inbound Rules

Protocol	Port	Source
TCP	80	<i>sg-hadoop</i>

Outbound Rules

Protocol	Port	Destination
All	All	0.0.0.0/0

Network Access Control Lists (NACLs)



NACL Configuration

Inbound Rules

Rule #	Protocol	Port	Source	Effect
1	All	All	0.0.0.0/0	Allow

Outbound Rules

Rule #	Protocol	Port	Source	Effect
1	All	All	0.0.0.0/0	Allow

Peering, endpoints, gateways, and global connectivity

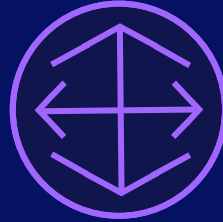
Peering, endpoints, gateways, and global connectivity



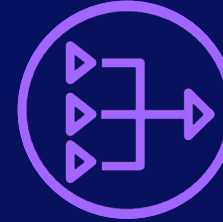
AWS Client
VPN



Virtual private
gateway



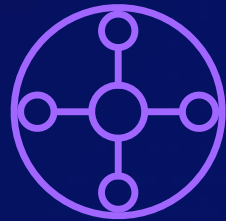
Direct Connect
gateway



NAT
gateway



Internet
gateway



AWS Transit
Gateway

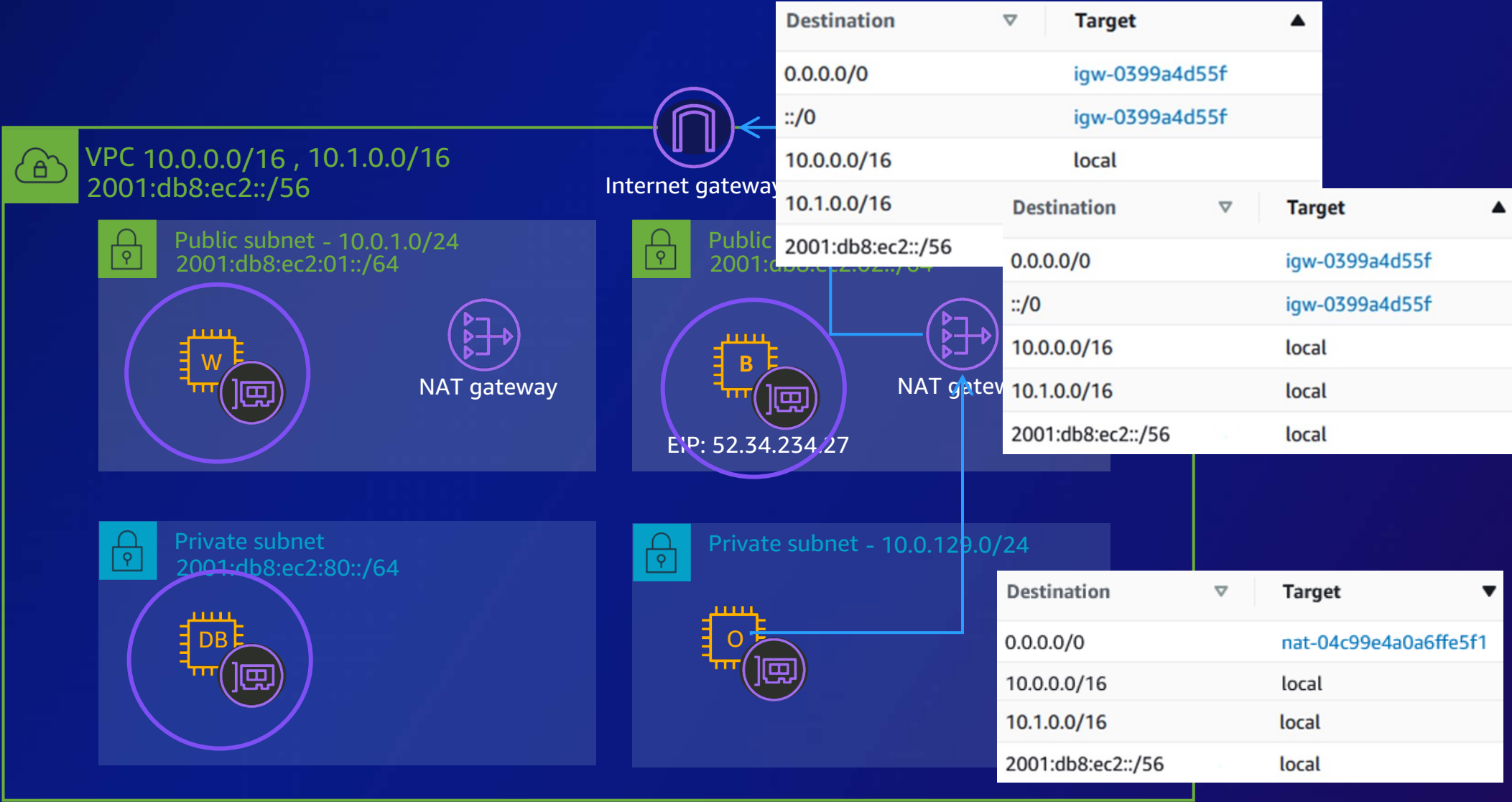


Endpoints

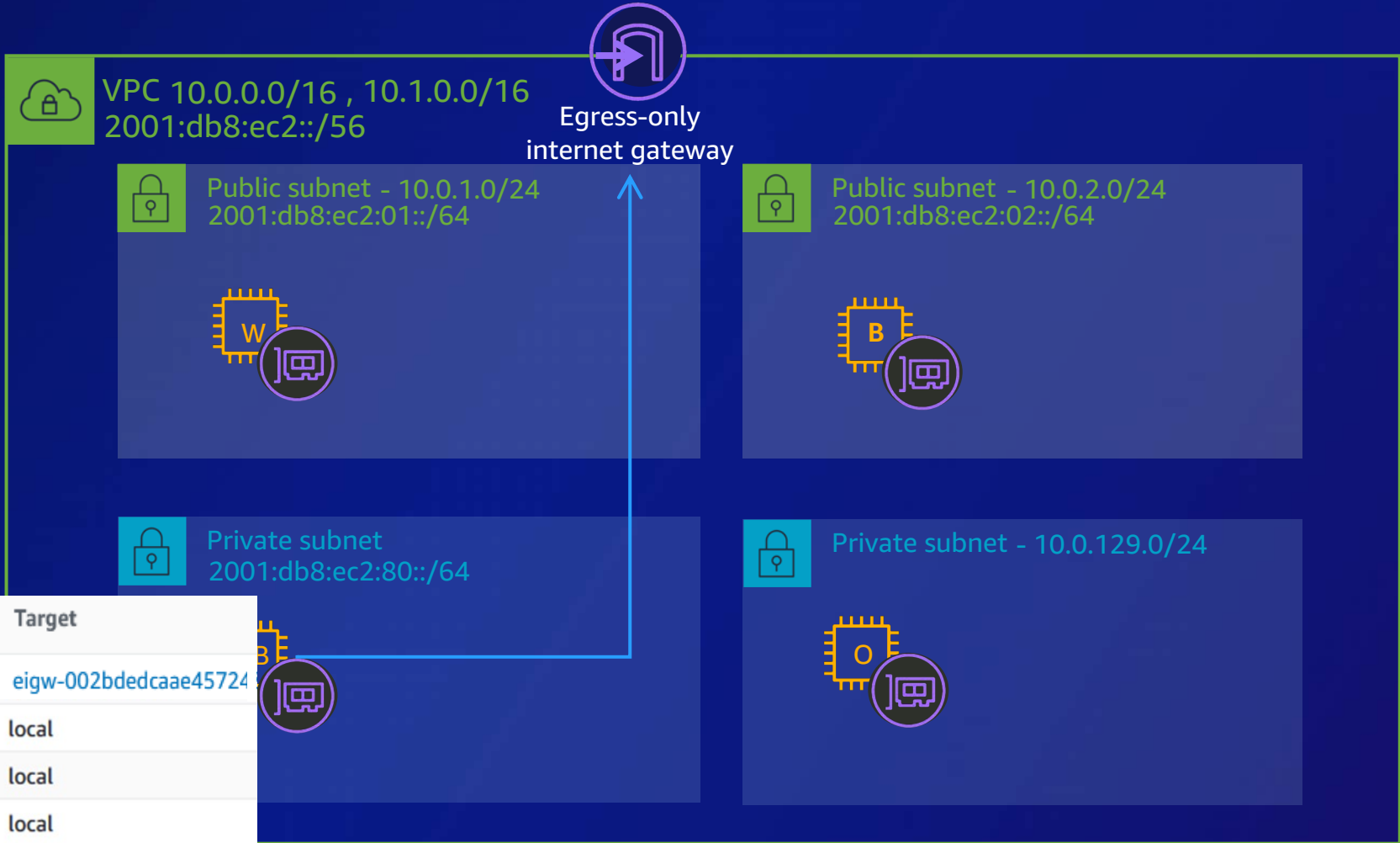


Peering
connection

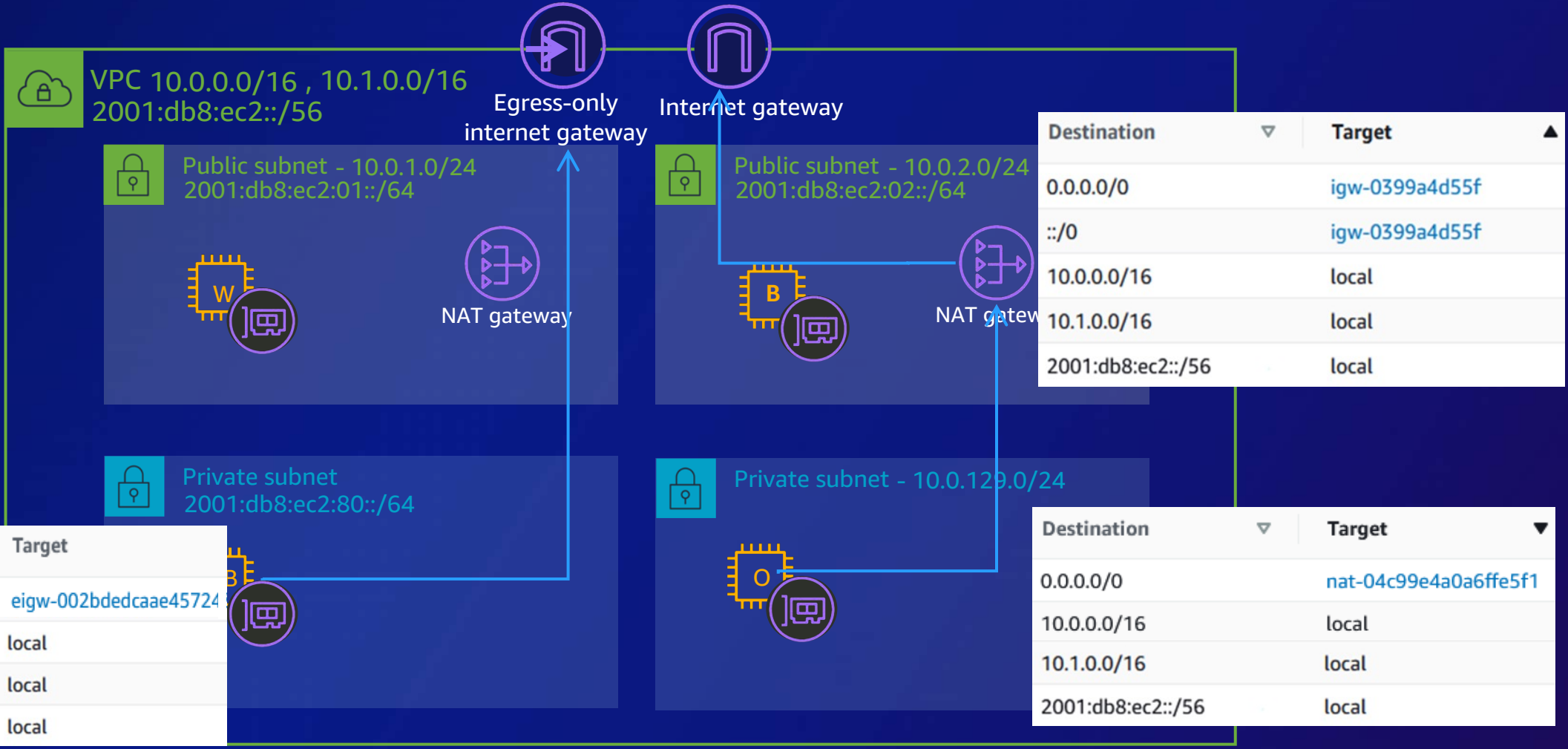
Connecting to the internet



Connecting to the internet



Connecting to the internet



Peering, endpoints, gateways, and global connectivity



AWS Client
VPN



Virtual private
gateway



NAT
gateway



Direct Connect
gateway



Internet
gateway



AWS Transit
Gateway

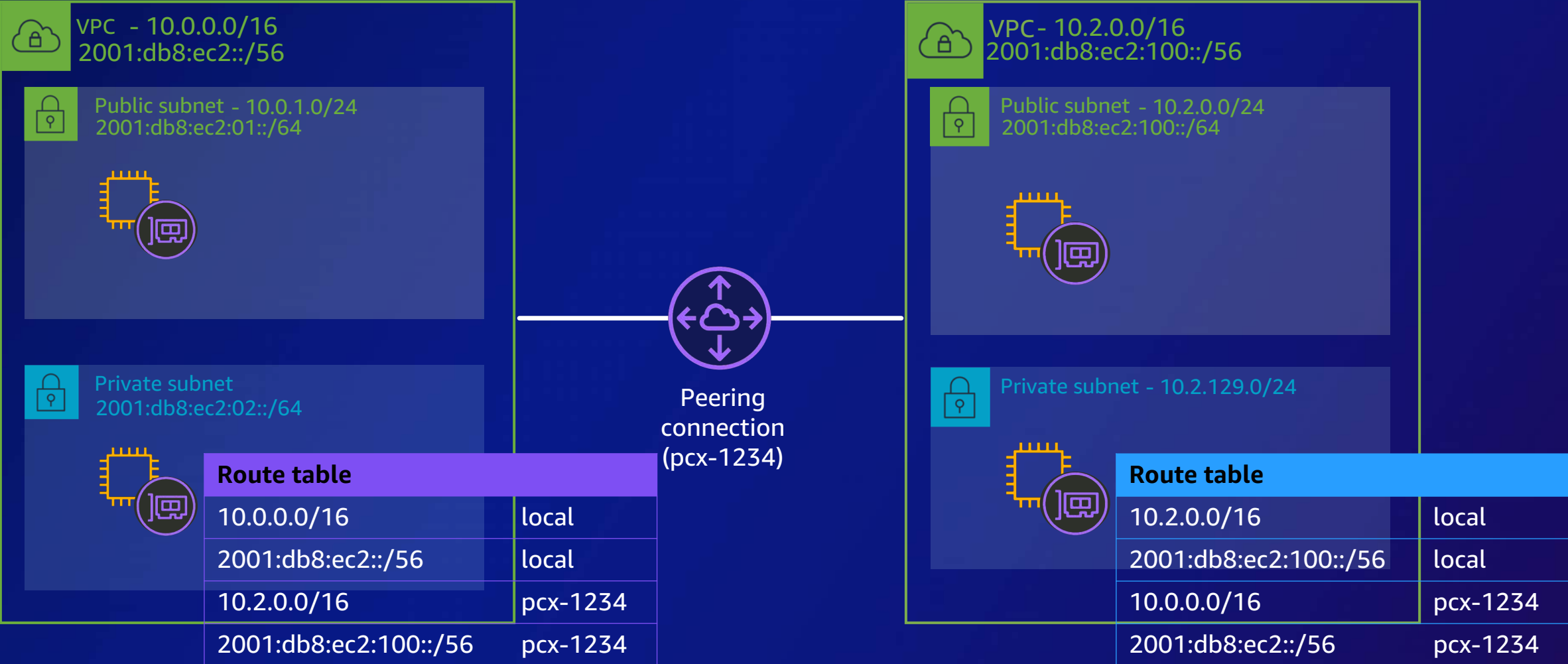


Endpoints

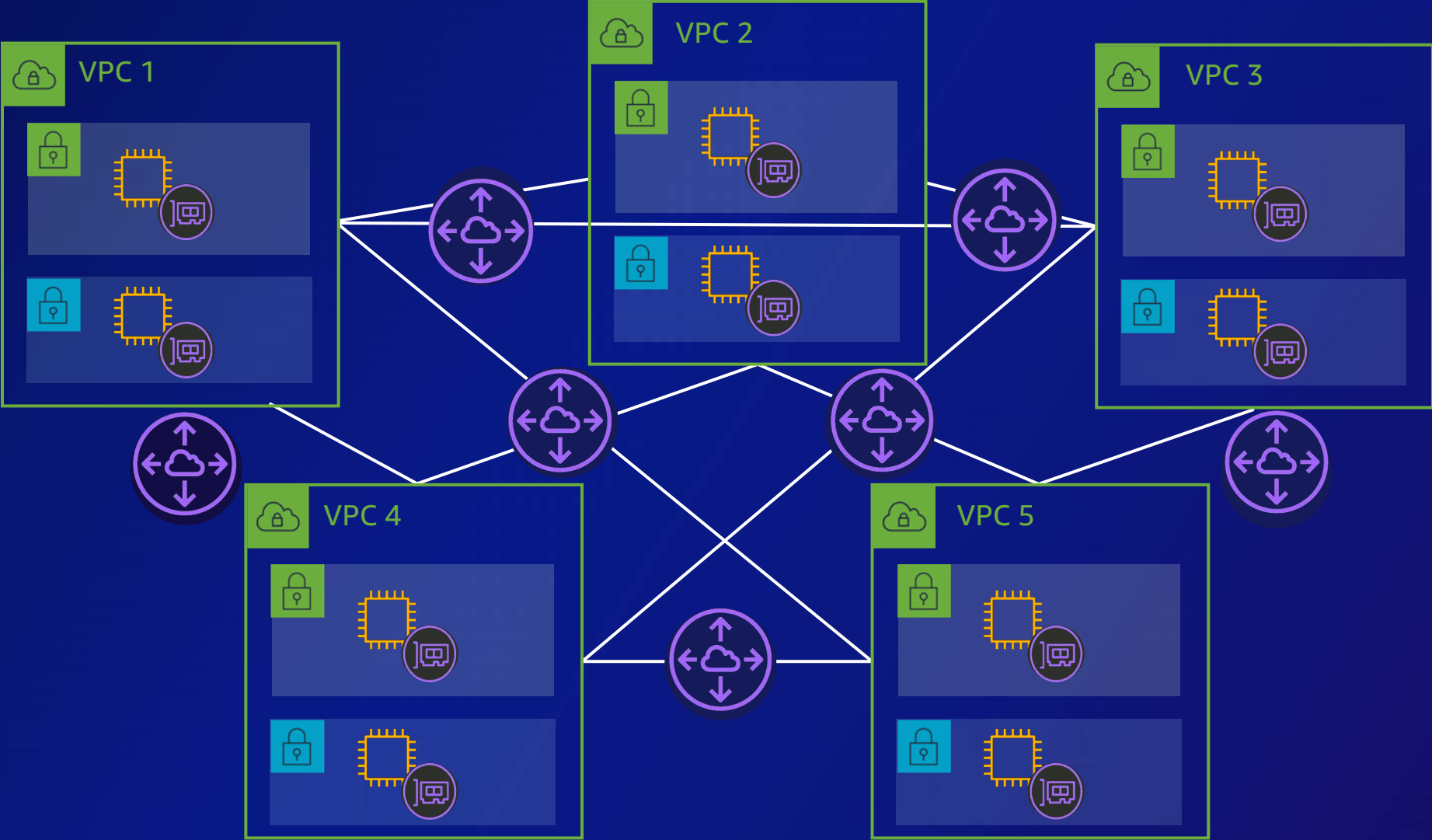


Peering
connection

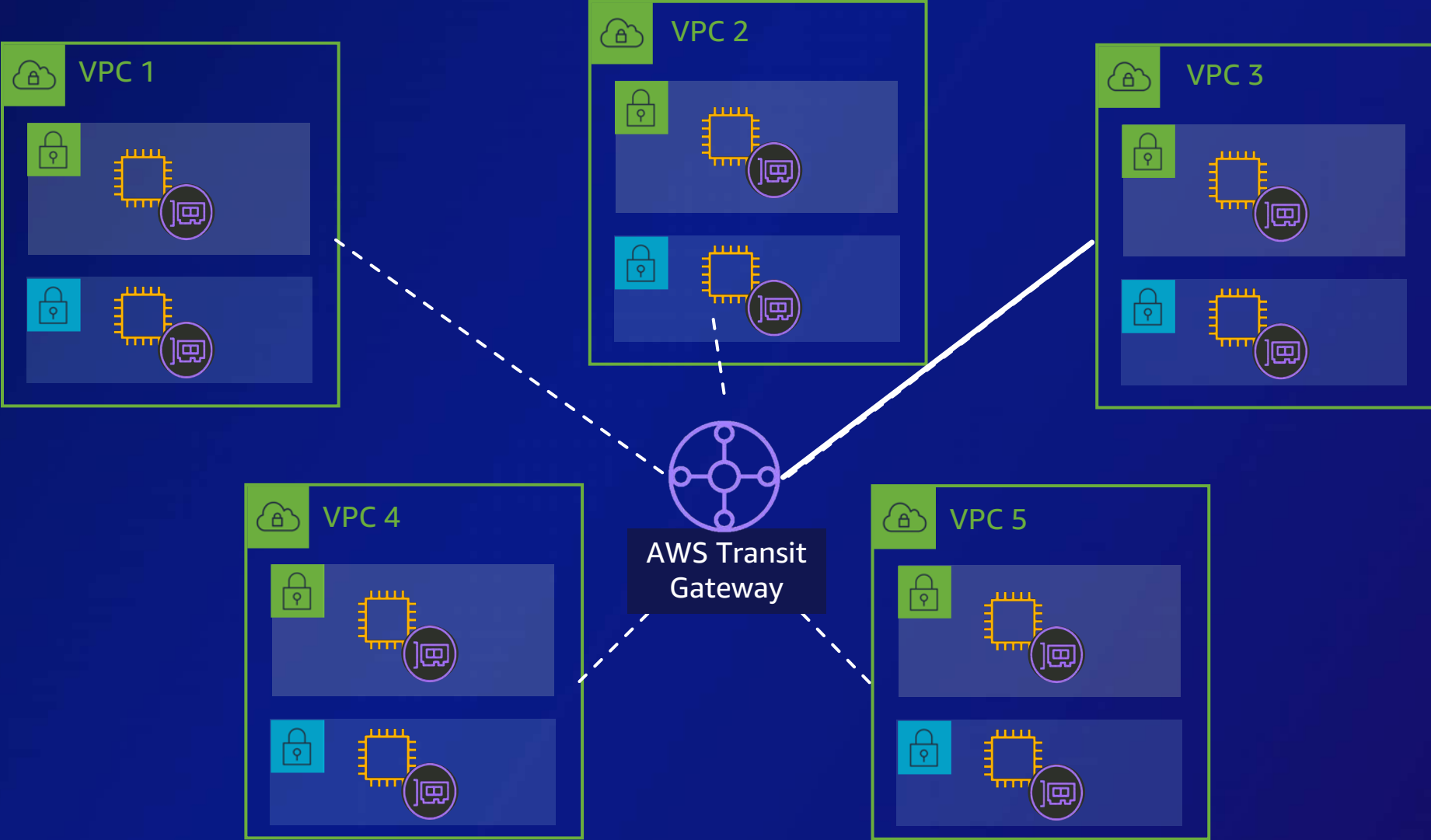
VPC peering



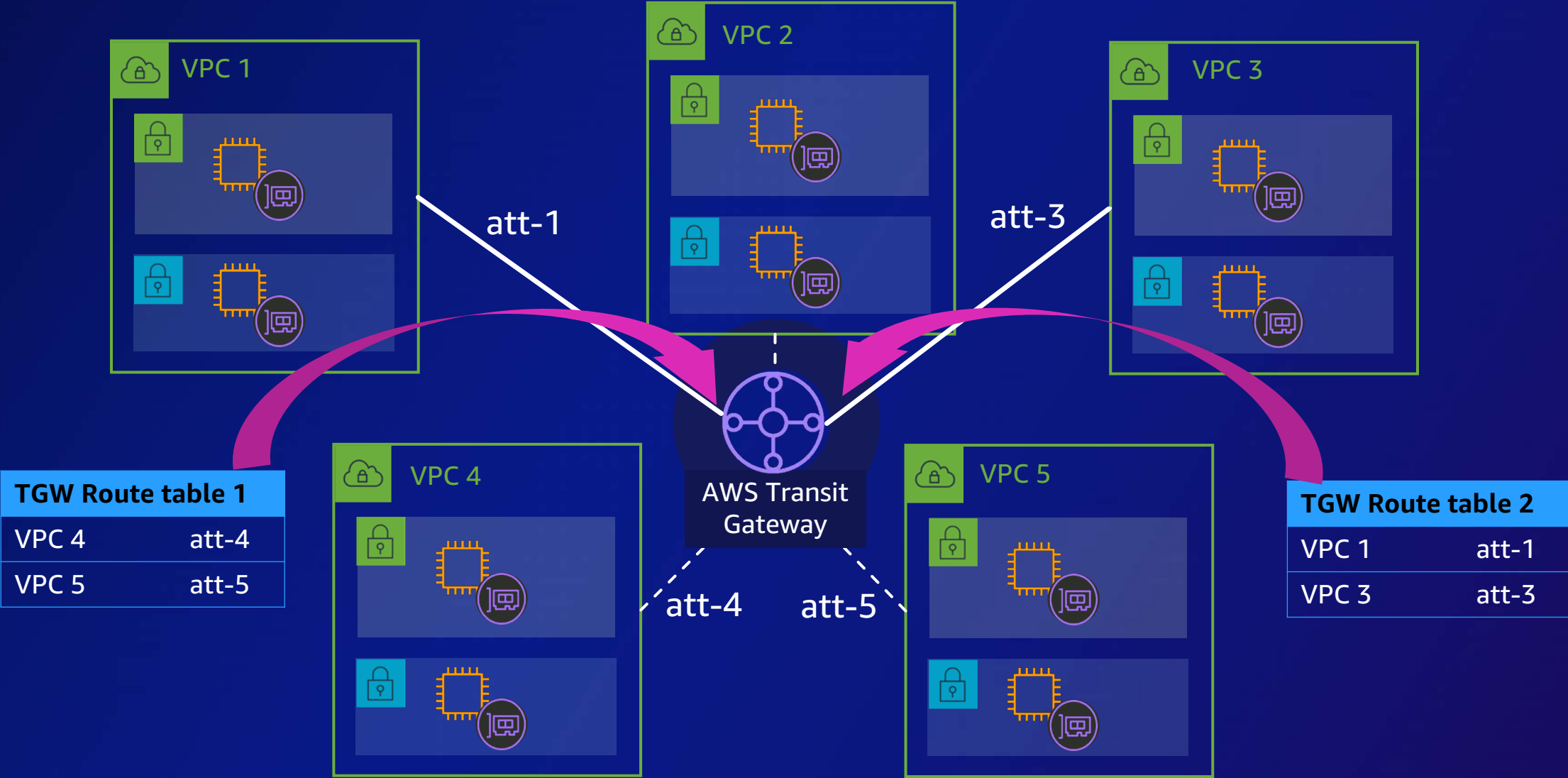
VPC peering



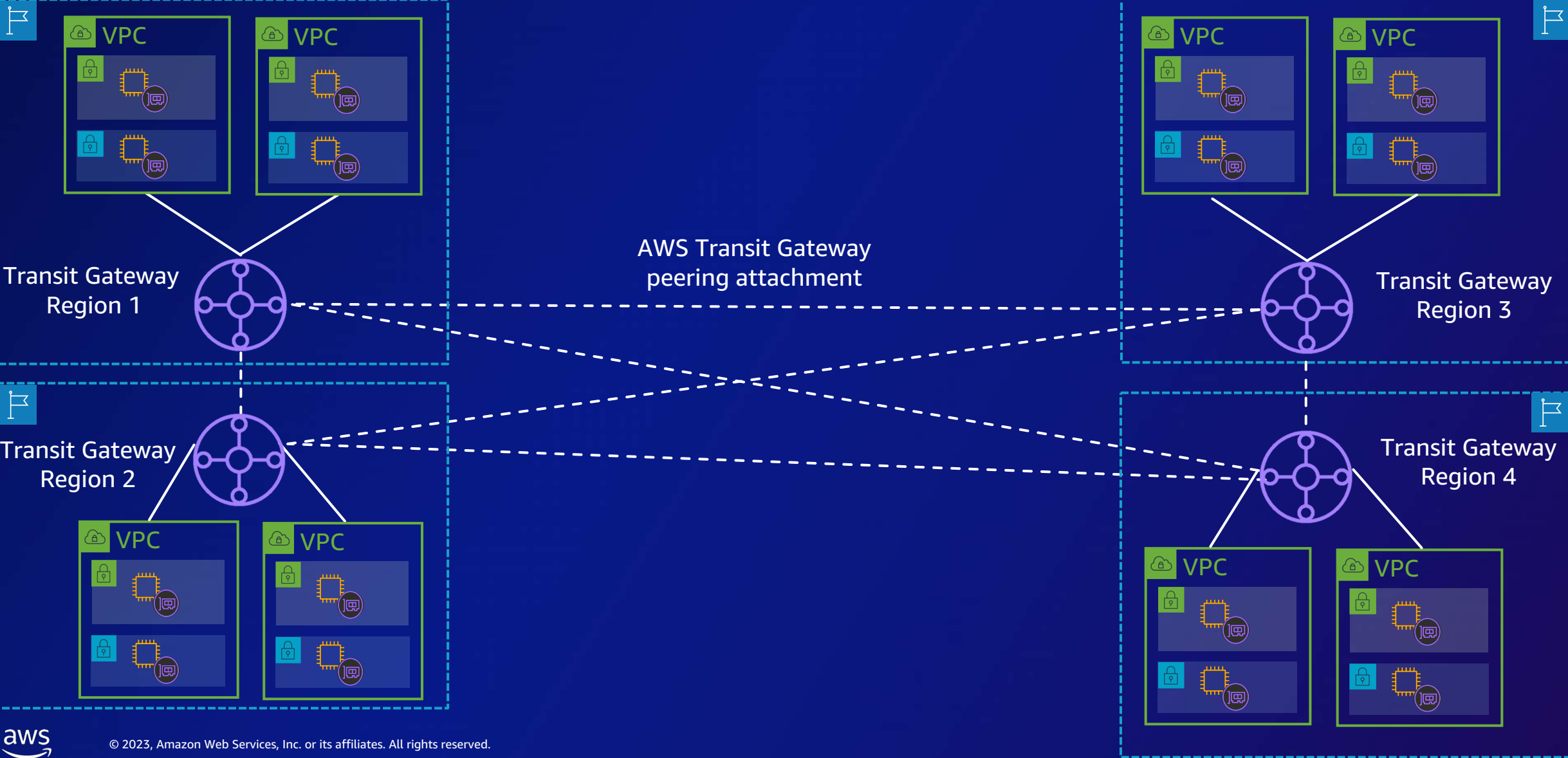
AWS Transit Gateway



AWS Transit Gateway (single Region)

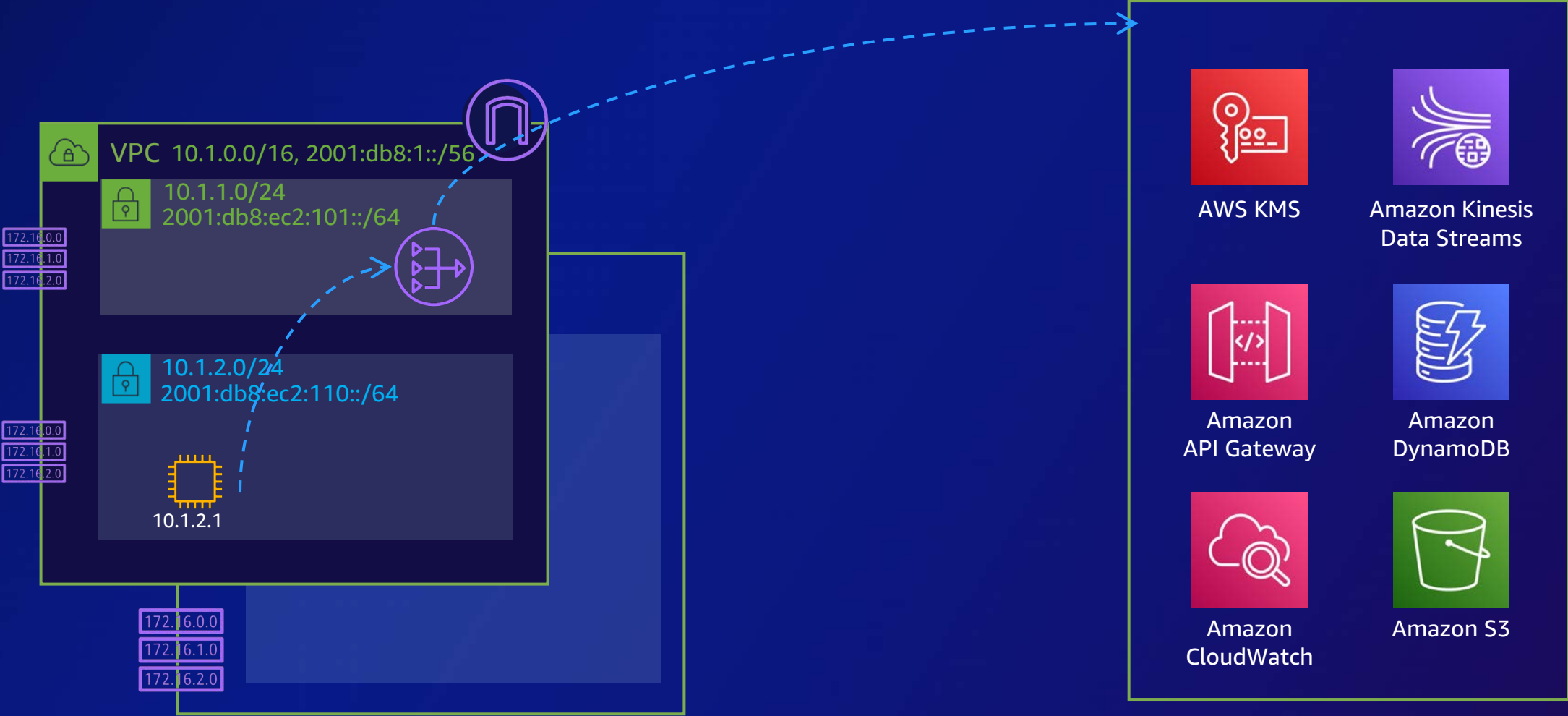


AWS Transit Gateway (multi-Region)



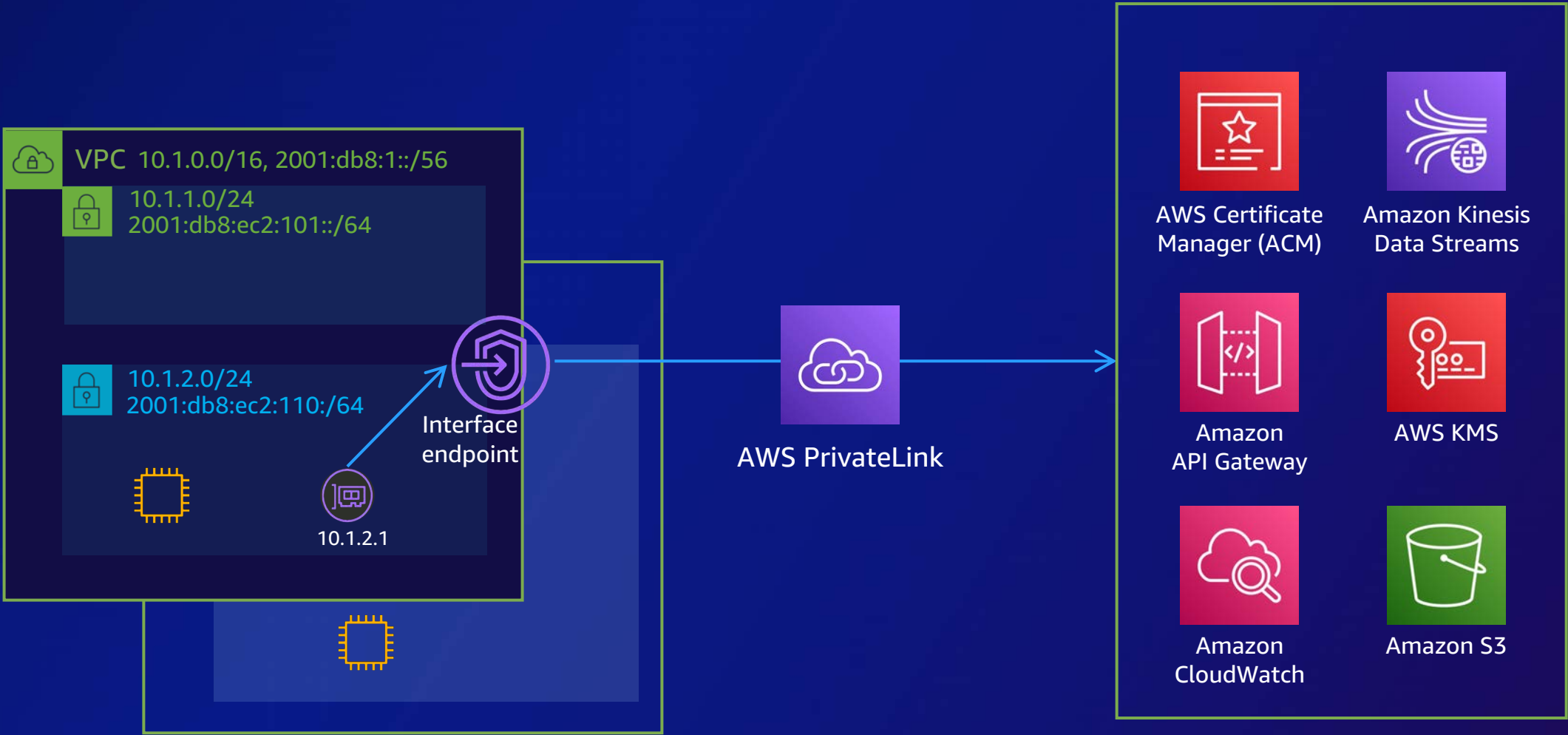
Accessing AWS services

WITHOUT VPC ENDPOINTS

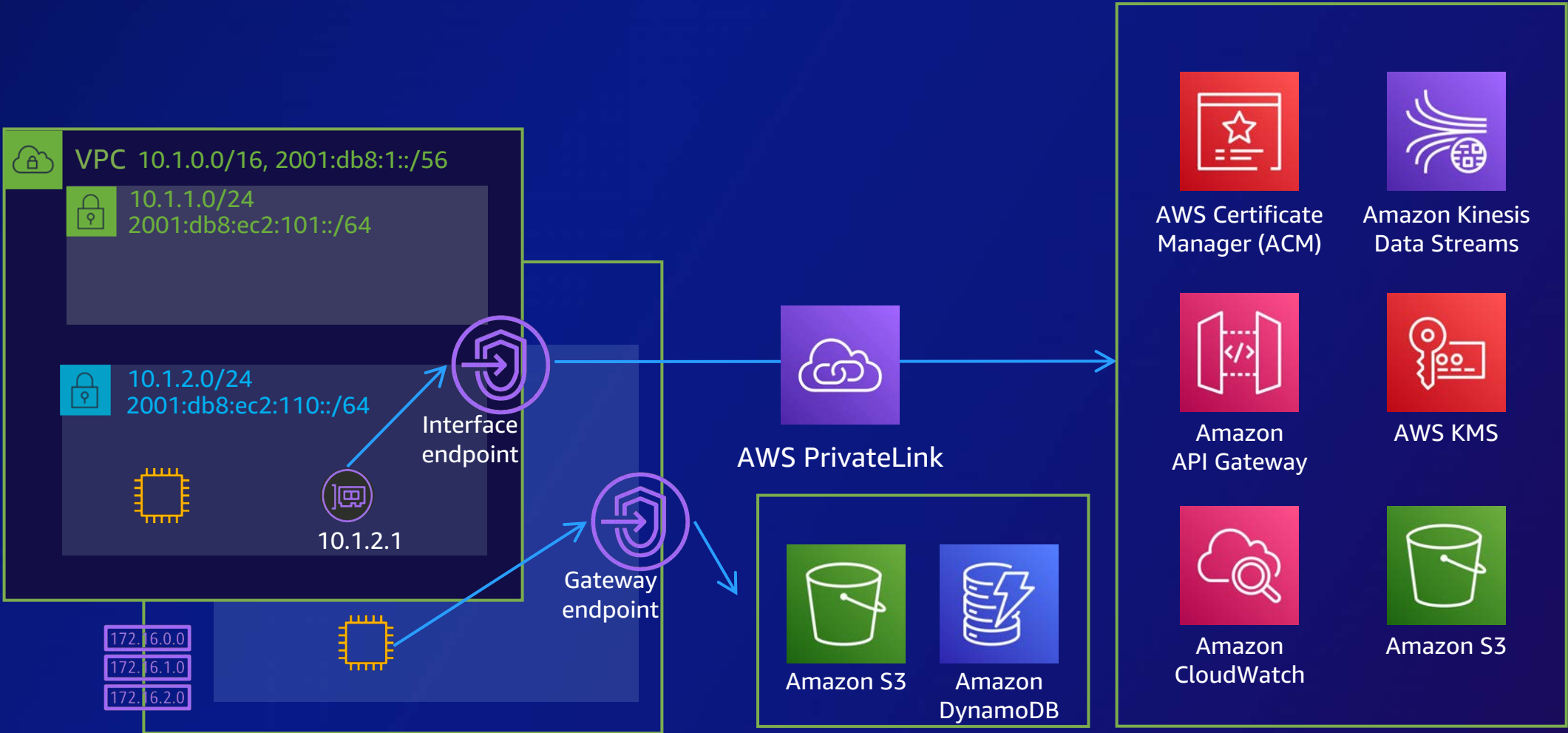


Accessing AWS services

WITH VPC ENDPOINTS



VPC gateway endpoints



VPC endpoint policies



```
{  
  "Sid": "Restrict-access-to-specific-IAM-role",  
  "Effect": "Allow",  
  "Principal": "*",  
  "Action": "*",  
  "Resource": "*",  
  "Condition": {  
    "ArnEquals": {  
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"  
    }  
  }  
}
```



AWS Certificate Manager (ACM)



Amazon Kinesis Data Streams



Amazon API Gateway



AWS KMS



Amazon CloudWatch



Amazon S3

172.16.0.0
172.16.1.0
172.16.2.0



endpoint

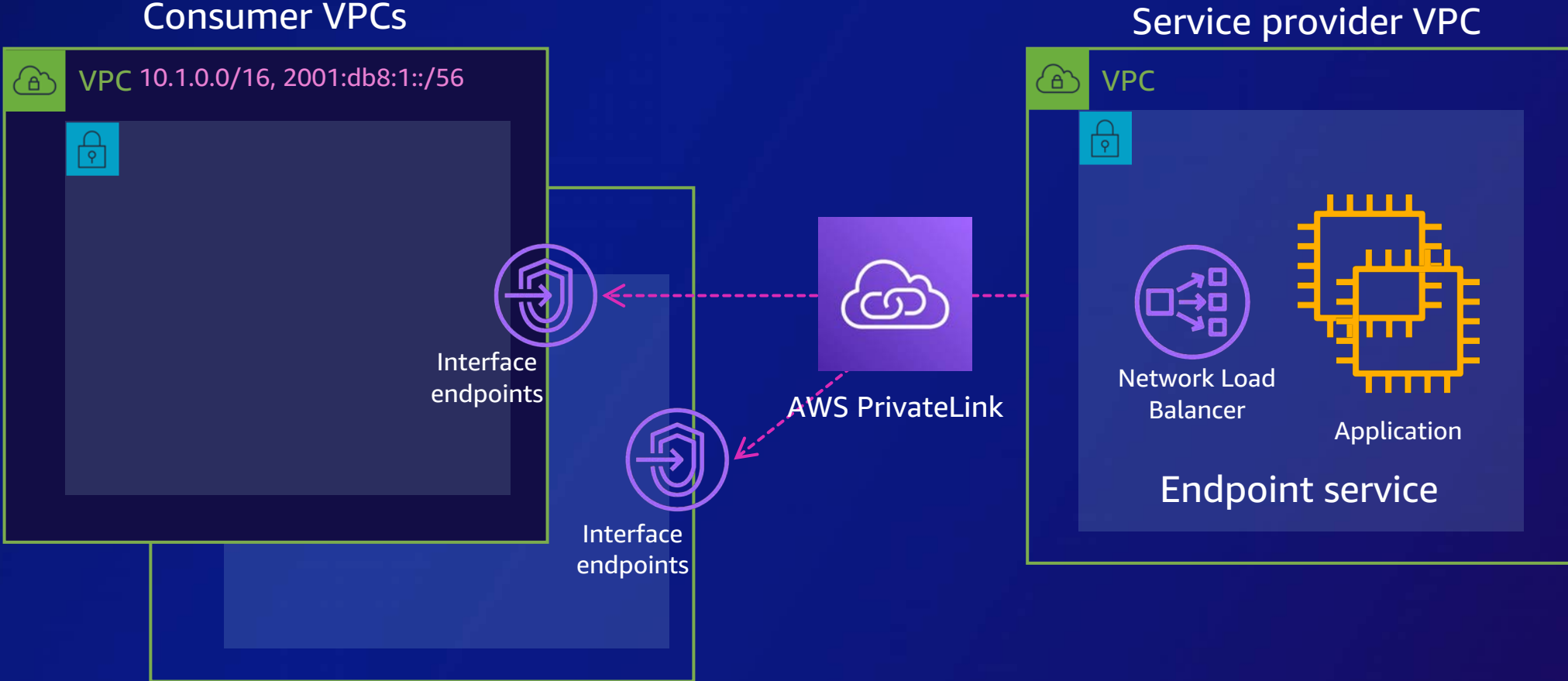


Amazon S3



Amazon DynamoDB

AWS PrivateLink



Peering, endpoints, gateways, and global connectivity



AWS Client
VPN



Virtual private
gateway

AWS Transit
Gateway



Direct Connect
gateway

Endpoints



NAT
gateway

Peering
connection

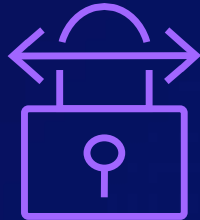


Internet
gateway

Hybrid connectivity and DNS



AWS Direct
Connect



AWS
Site-to-Site
VPN

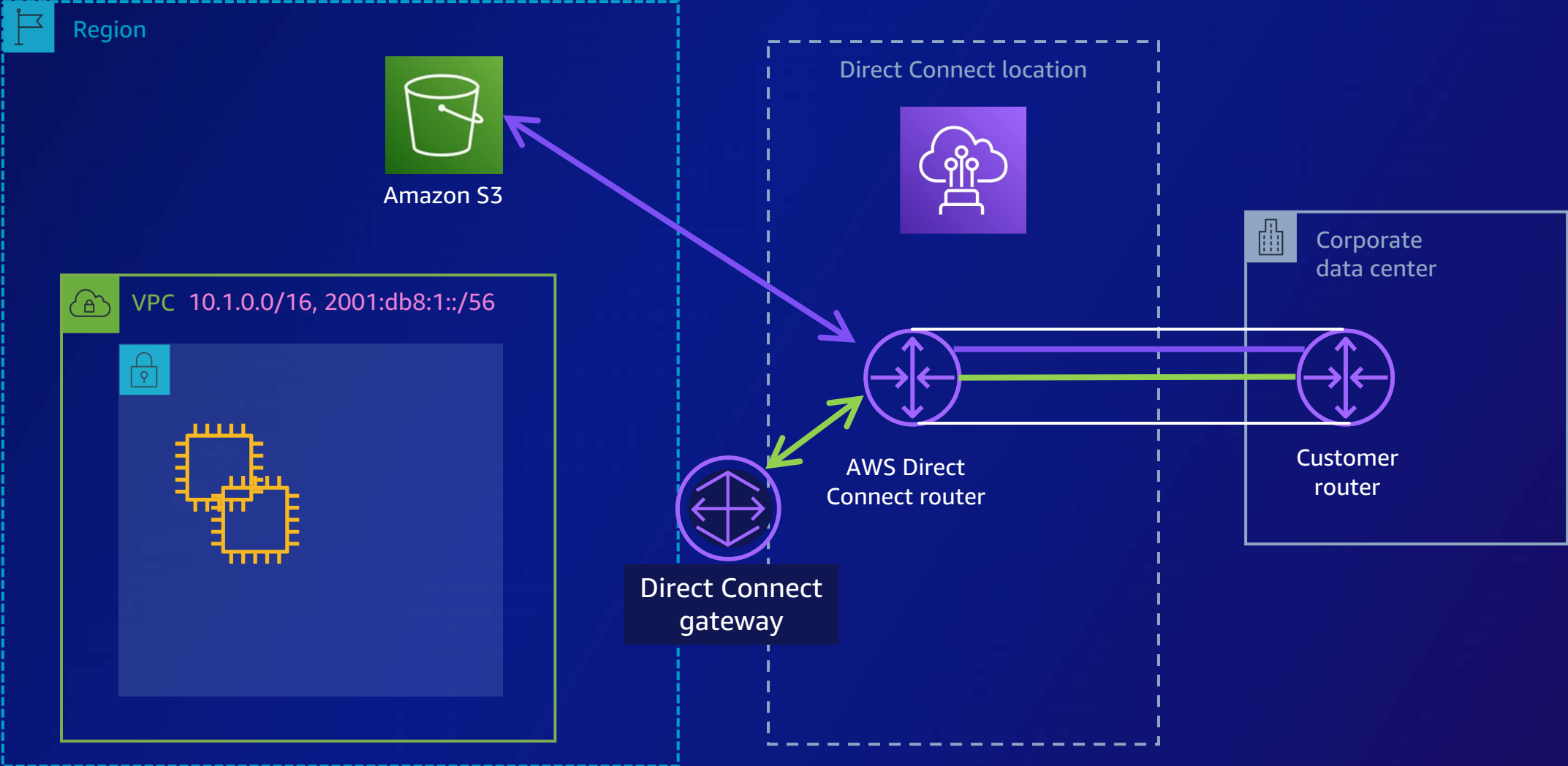


AWS Client VPN

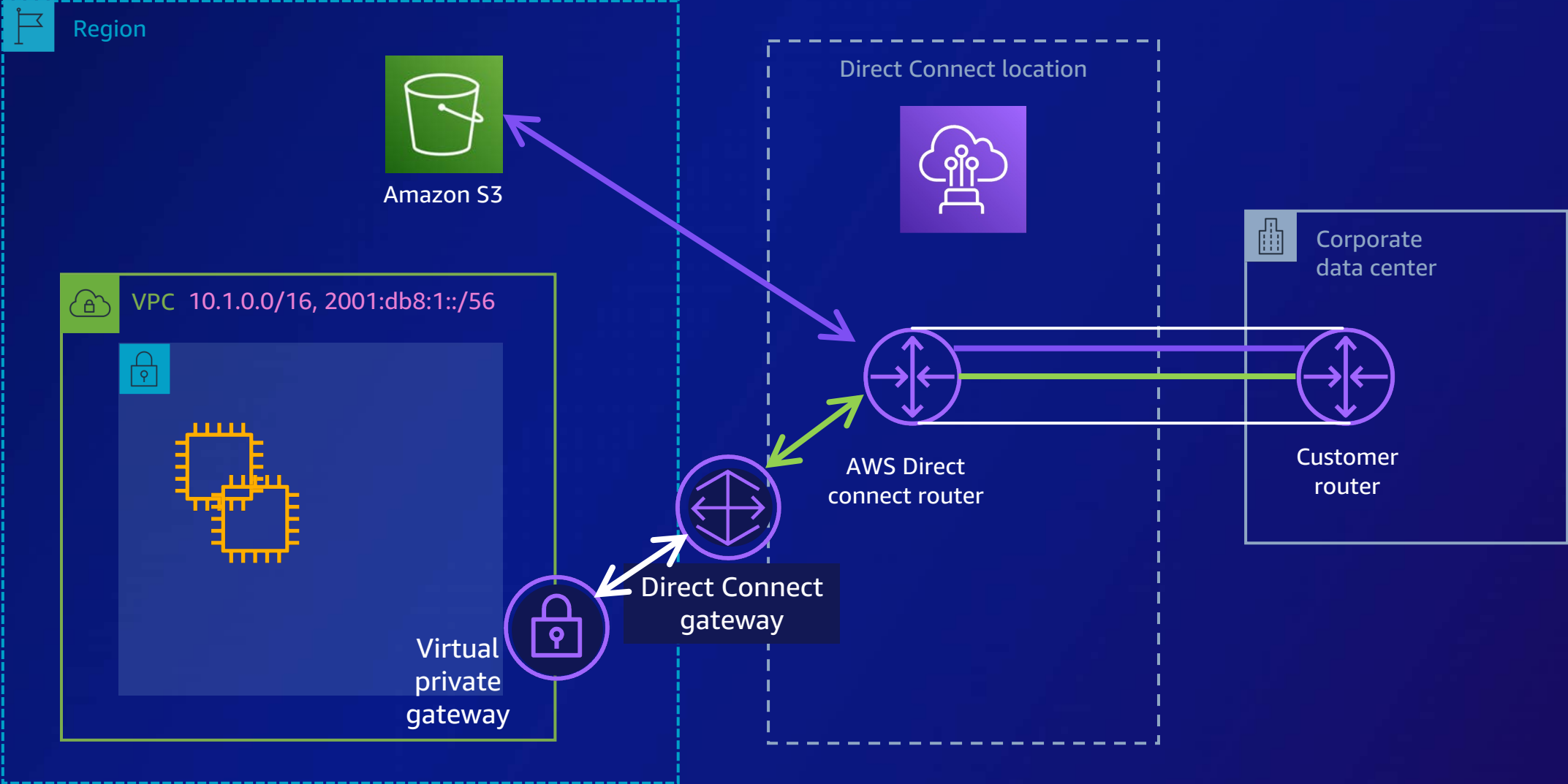


Amazon
Route 53

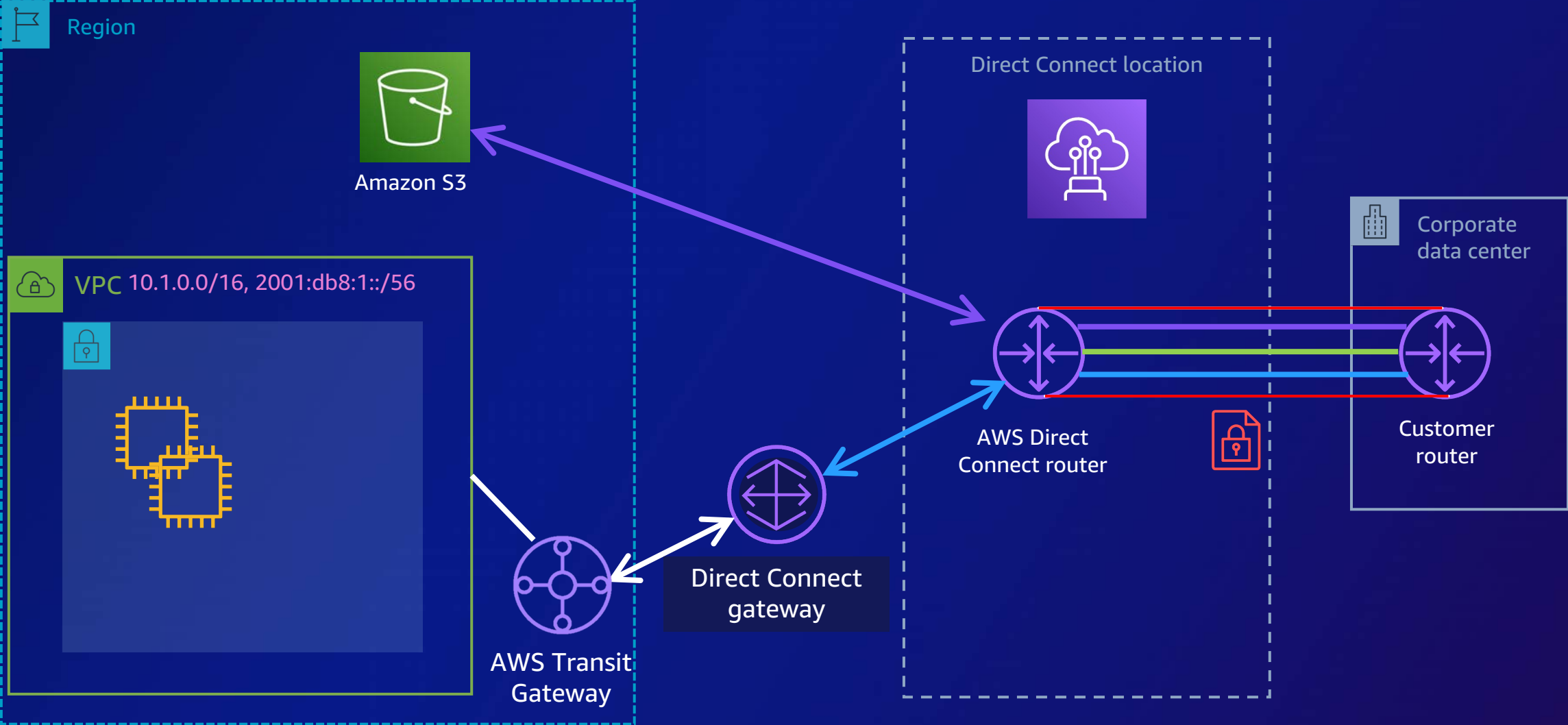
AWS Direct Connect



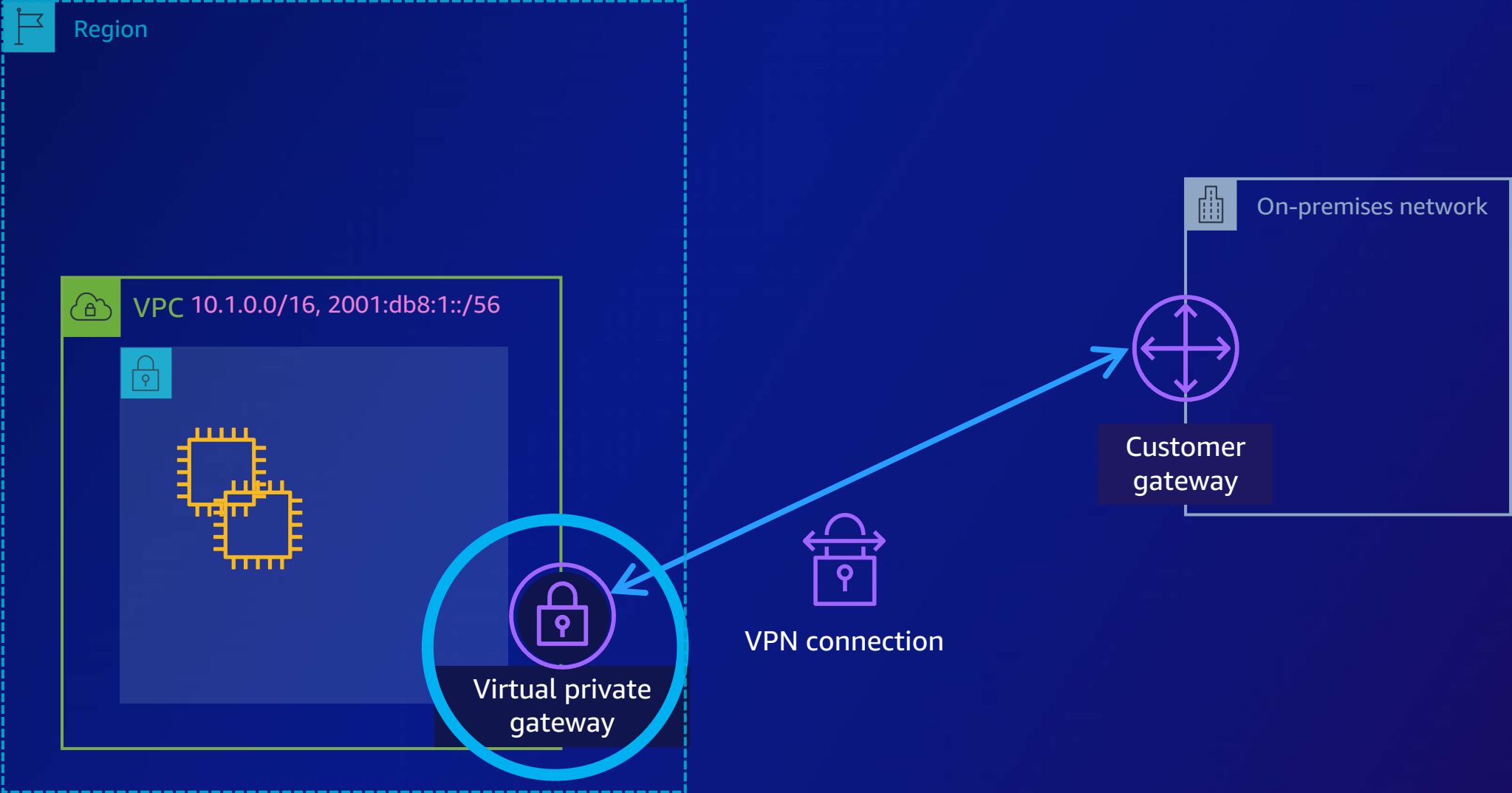
AWS Direct Connect



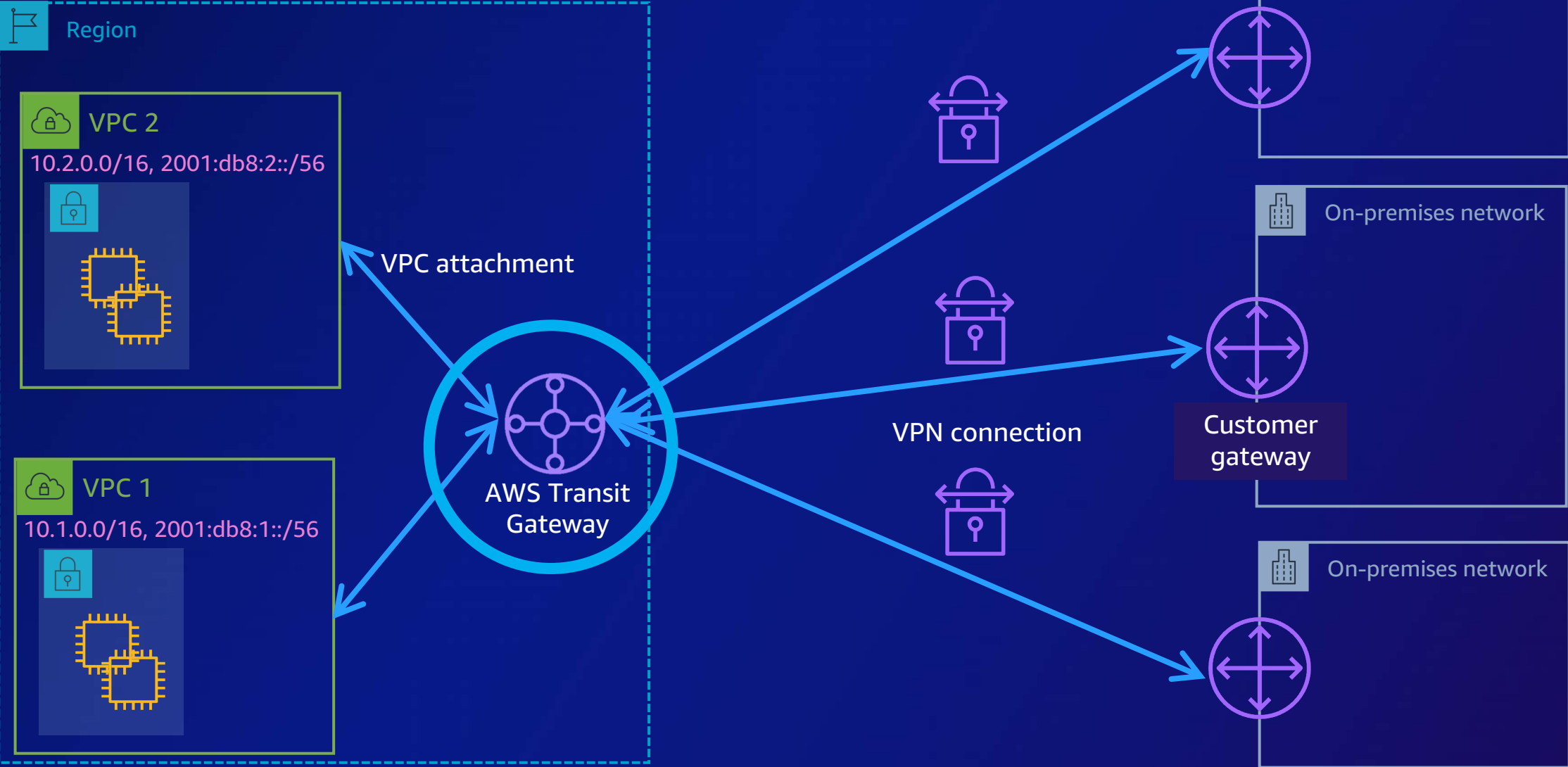
AWS Direct Connect



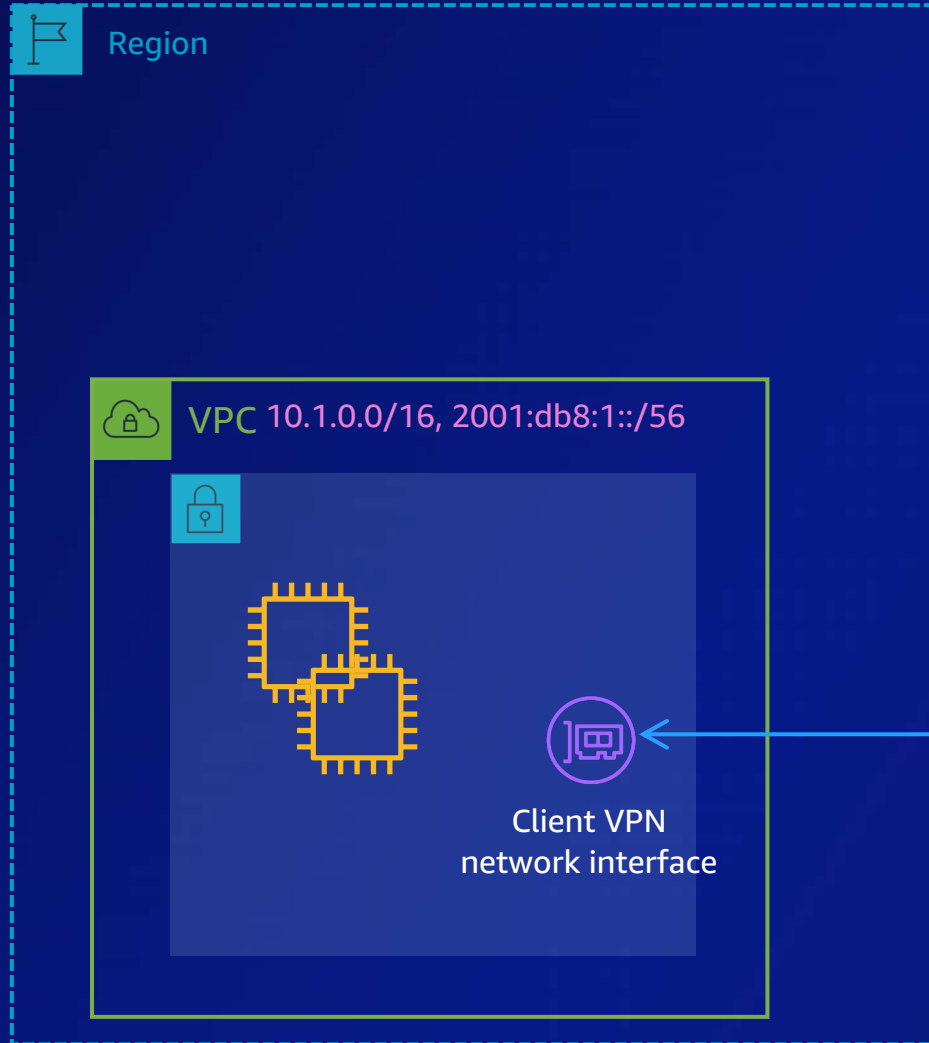
AWS Site-to-Site VPN



AWS Site-to-Site VPN



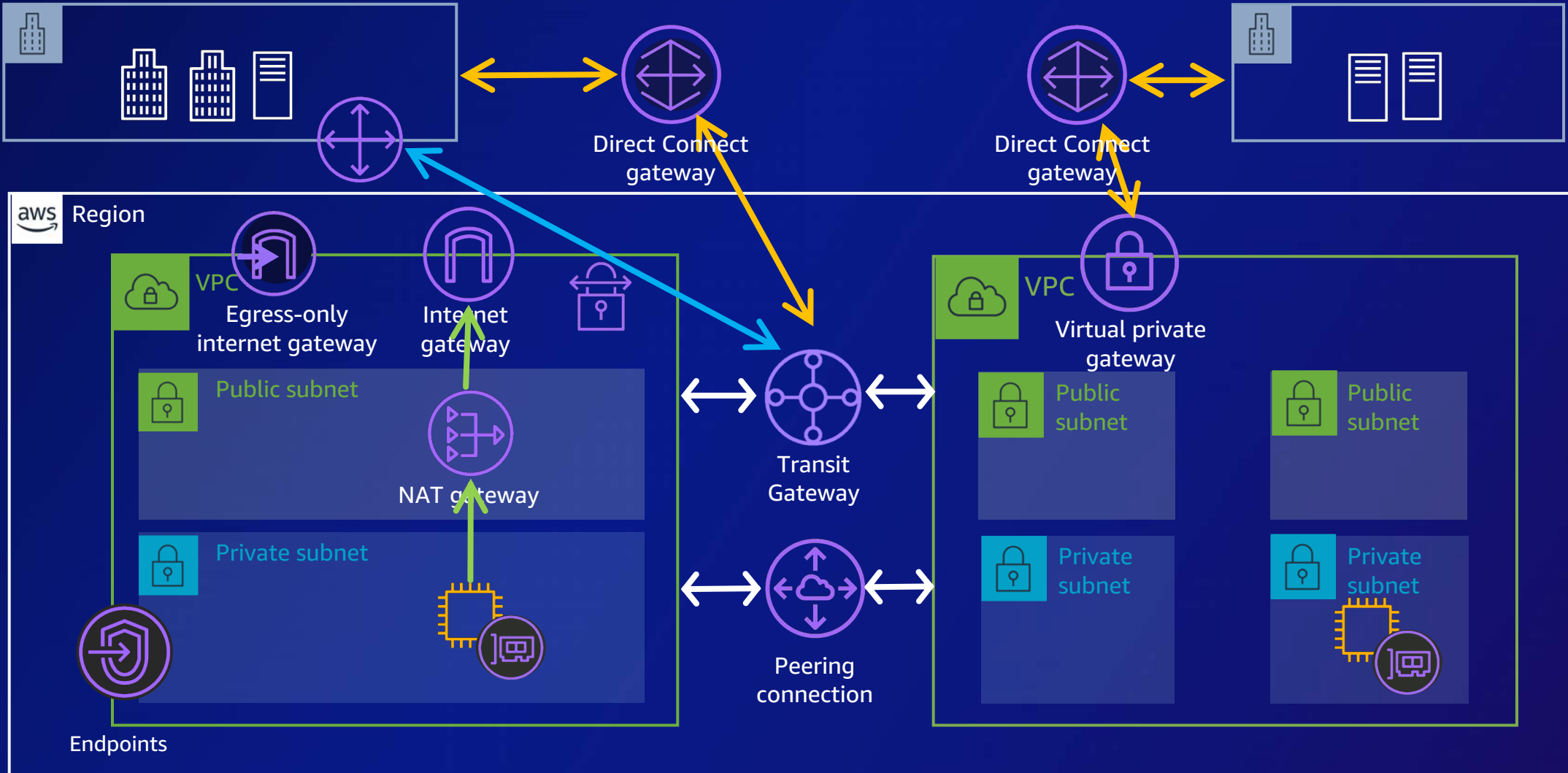
AWS Client VPN



- Fully managed, elastic, and secure TLS connections from any location using an OpenVPN-based client
- Supports split tunneling to provide secured access to resources on AWS and on-premises network
- Client authentication using Microsoft Active Directory, federated authentication, and certificate-based authentication
- Provides client-to-client connectivity




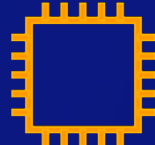
Bringing it all together



Amazon Route 53 Resolver 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
Route 53 Resolver

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

Simplify service-to-service connectivity



Amazon VPC Lattice

BUILT FOR DEVELOPERS, BUT WITH THE TOOLS AND CONTROLS ADMINS REQUIRE TO AUDIT AND ENFORCE



Simplifies the way developers connect, secure, and observe communication, with application layer networking between services

Connectivity

- Cross-account, cross-VPC connections to services
- Overlapping CIDRs across VPCs with IPv4 and v6 mix-and-match

Consistency across compute services

- Integration with Amazon Elastic Compute Cloud (EC2), Amazon Elastic Container Service (ECS), AWS Lambda, and Amazon Elastic Kubernetes Service (EKS) and Kubernetes

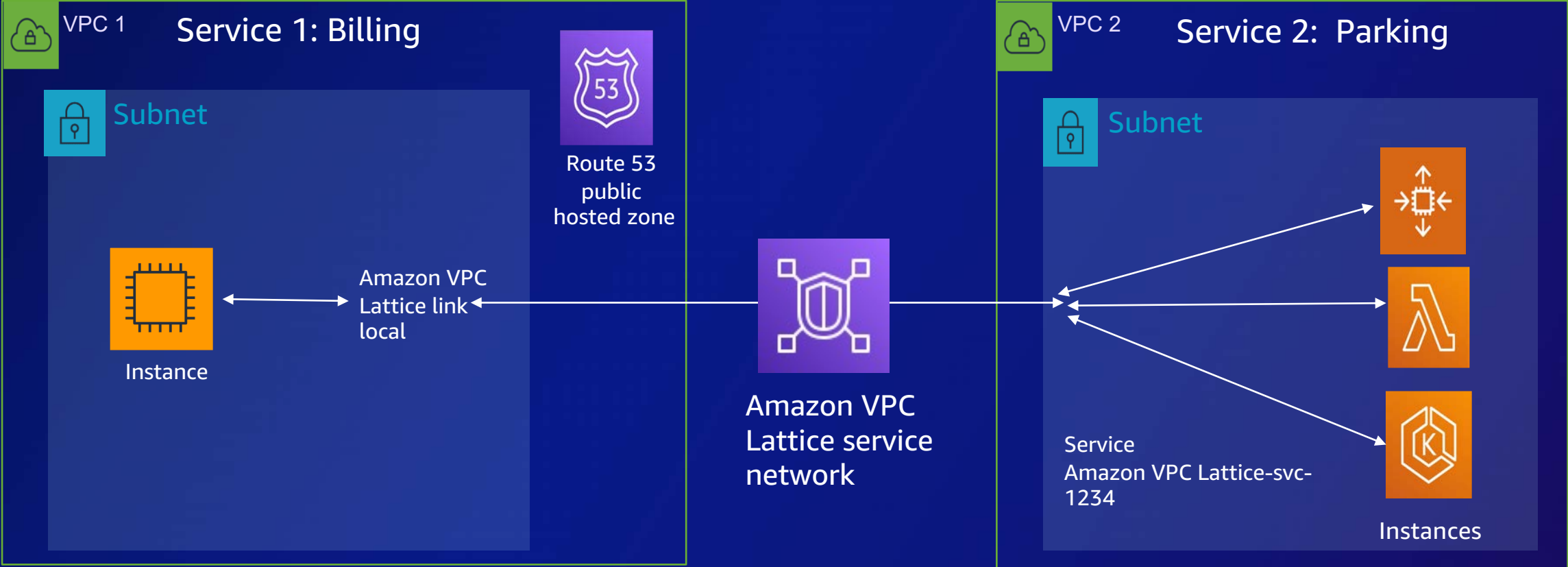
Observability and traffic control

- Logs or metrics export to Amazon Simple Storage Service (S3), Amazon CloudWatch, and Amazon Kinesis Data Firehose
- Advanced layer 7 routing, load balancing, and resiliency controls

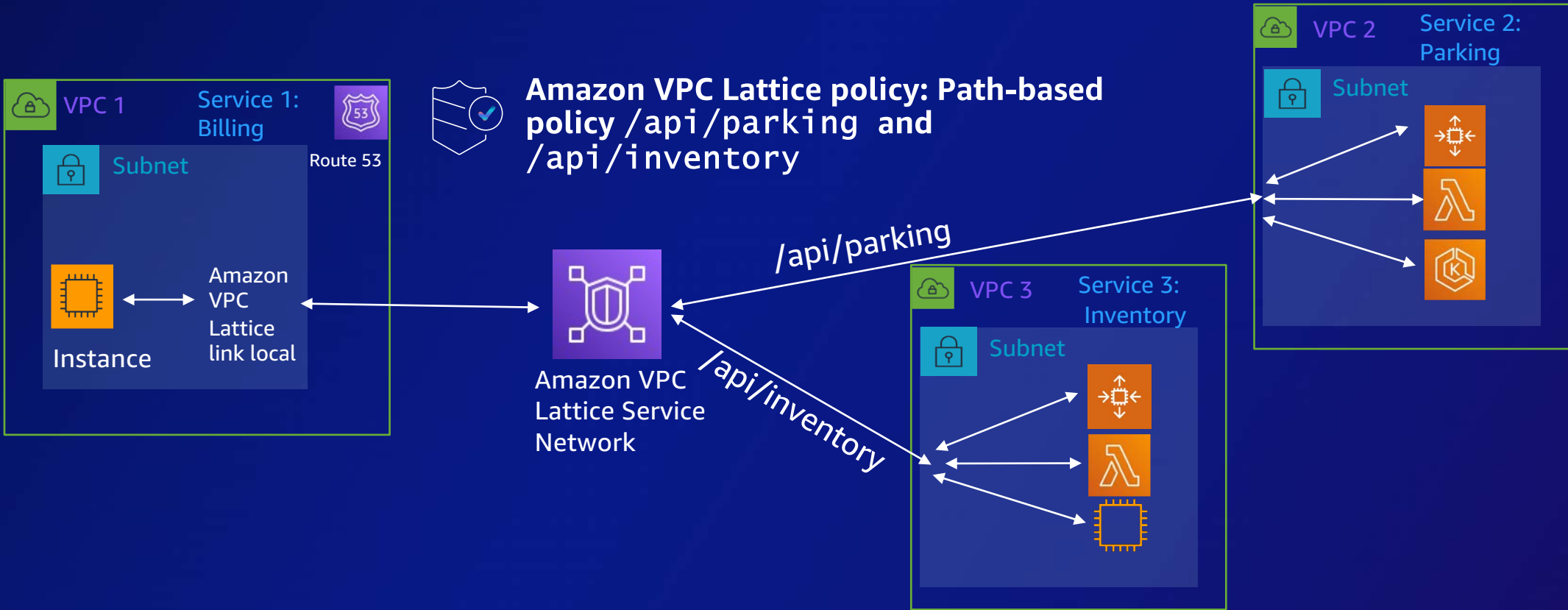
Security

- AWS Identity and Access Management (IAM) identity and access policies for Zero Trust architectures
- Centralized control of inbound and outbound traffic

Example: Secure and simple cross-VPC connectivity



Traffic management use case: Path-based routing



Amazon VPC Lattice policy: Path-based policy /api/parking and /api/inventory

Granular secure access to services for Zero Trust



Traffic visibility and monitoring



Amazon VPC Flow Logs

version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status vpc-id subnet-id instance-id tcp-flags type pkt-srcaddr pkt-dstaddr region az-id sublocation-type sublocation-id pkt-src-aws-service pkt-dst-aws-service flow-direction traffic-path

```
5 123456789097 eni-044feef0 52.218.241.56 10.0.1.38 443 58460 6 19 7710 1634606470 1634606481 ACCEPT OK vpc-0a19b648 subnet-094ee201 i-08bcbe49 19 IPv4 52.218.241.56 10.0.1.38 us-west-2 usw2-az2 - - S3 - ingress -
```

```
5 123456789097 eni-044feef0 2001:db2:1:f102::6 2001:db2:1:f101::f 0 0 58 10 1040 1634606496 1634606497 ACCEPT OK vpc-0a19b648 subnet-094ee201 i-08bcbe49 0 IPv6 2001:db2:1:f102::6 2001:db2:1:f101::f us-west-2 usw2-az2 - - EC2 EC2 ingress -
```

Select log group(s)

Clear flowLogs X

```
1 stats sum(bytes) as bytesTransferred by srcAddr, dstAddr
2 | sort bytesTransferred desc
3 | limit 10
```

Run query Save History

Queries are allowed to run for up to 15 minutes.

Logs Visualization

Export results Add to dashboard

Showing 10 of 845 records matched 876 records (238.7 kB) scanned in 3.9s @ 222 records/s (60.6 kB/s)

#	srcAddr	dstAddr	bytesTransferred
▶ 1	10.0.1.38	193.194.68.62	290499
▶ 2	10.0.1.38	35.86.195.128	152109
▶ 3	10.0.1.38	194.0.159.77	151468
▶ 4	194.0.159.77	10.0.1.38	127052
▶ 5	193.194.68.62	10.0.1.38	119652
▶ 6	35.86.195.128	10.0.1.38	83149
▶ 7	10.0.2.45	141.98.10.60	11941
▶ 8	141.98.10.60	10.0.2.45	8008
▶ 9	2600:1fa0:4040:9448:...	2600:1f14:dd8:f101...	8001
▶ 10	2600:1fa0:4040:808:3...	2600:1f14:dd8:f101...	7994

Amazon VPC Traffic Mirroring



Internet gateway

No traffic mirror sessions found

You do not have any traffic mirror sessions in this region.

Create traffic mirror session



- Build your own traffic analyzer
- Open-source traffic analysis
- AWS Traffic Mirroring partners



Thank you!

