aws SUMMIT

LONDON | APRIL 29, 2022

NT-01

AWS Networking Fundamentals

Laura Verghote (she/her)
Associate Technical Trainer
Amazon Web Services

Agenda

Global infrastructure

Amazon Virtual Private Cloud (Amazon VPC)

Basics of VPC security

Peering, endpoints, and gateways

Global infrastructure

AWS global infrastructure

○ Region & number of Availability Zones (AZs)

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)

South America
São Paulo (3)

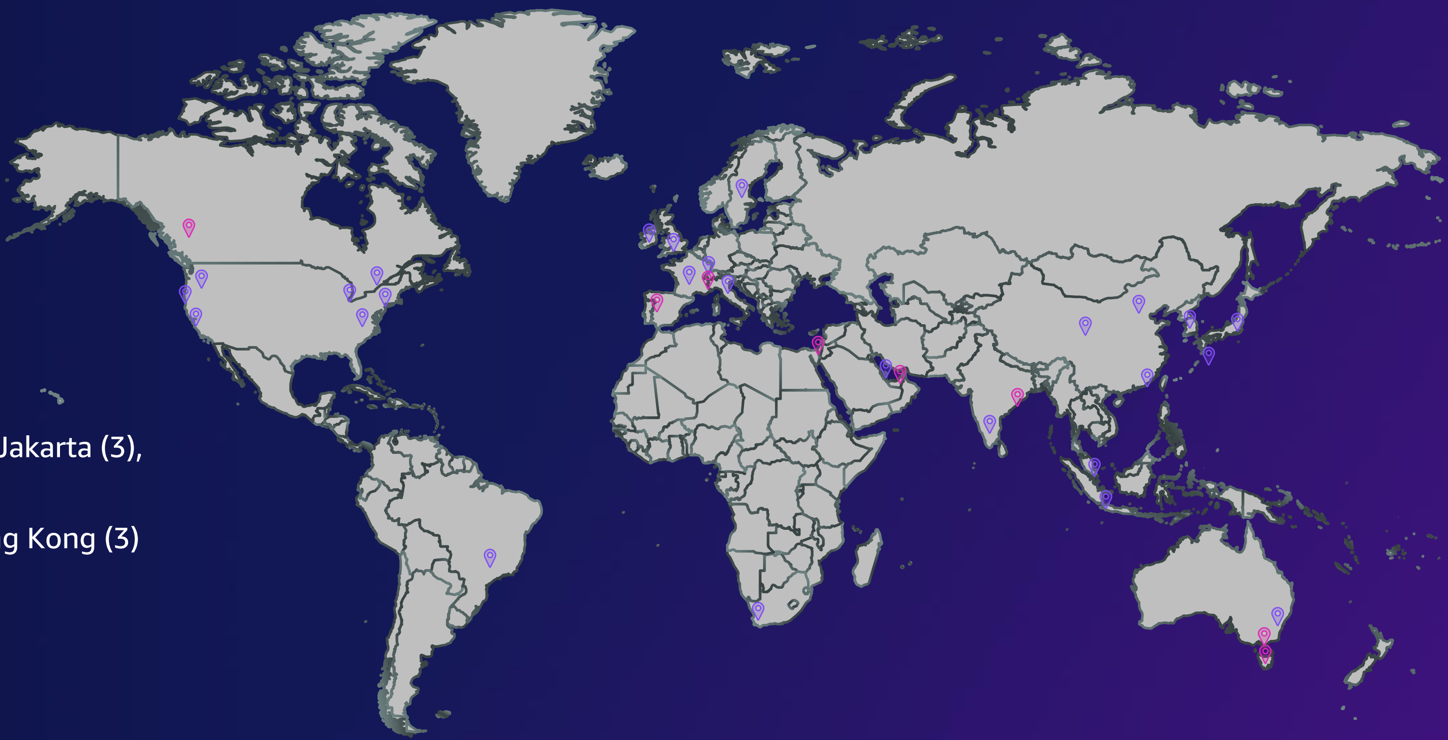
Africa
Cape Town (3)

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

Middle East
Bahrain (3)

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

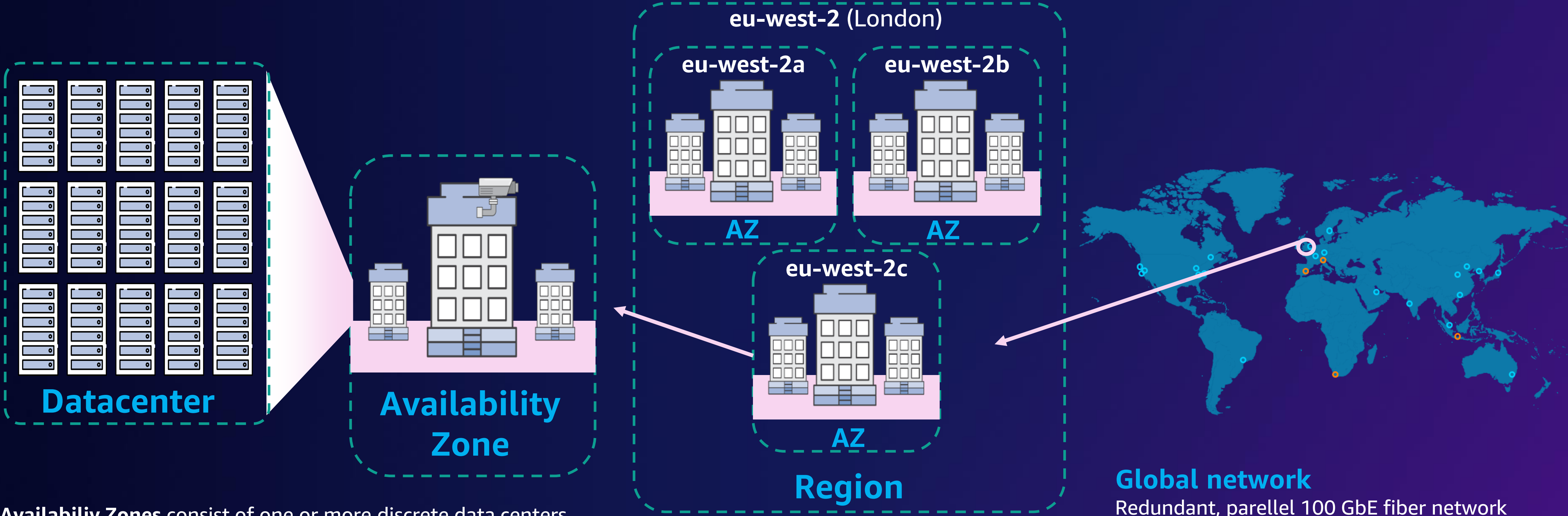
China
Beijing (3), Ningxia (3)



○ Announced Regions

8 Regions in Australia, Canada, India, Indonesia, Israel, Australia, Switzerland, Spain, and United Arab Emirates (UAE)

AWS global network components

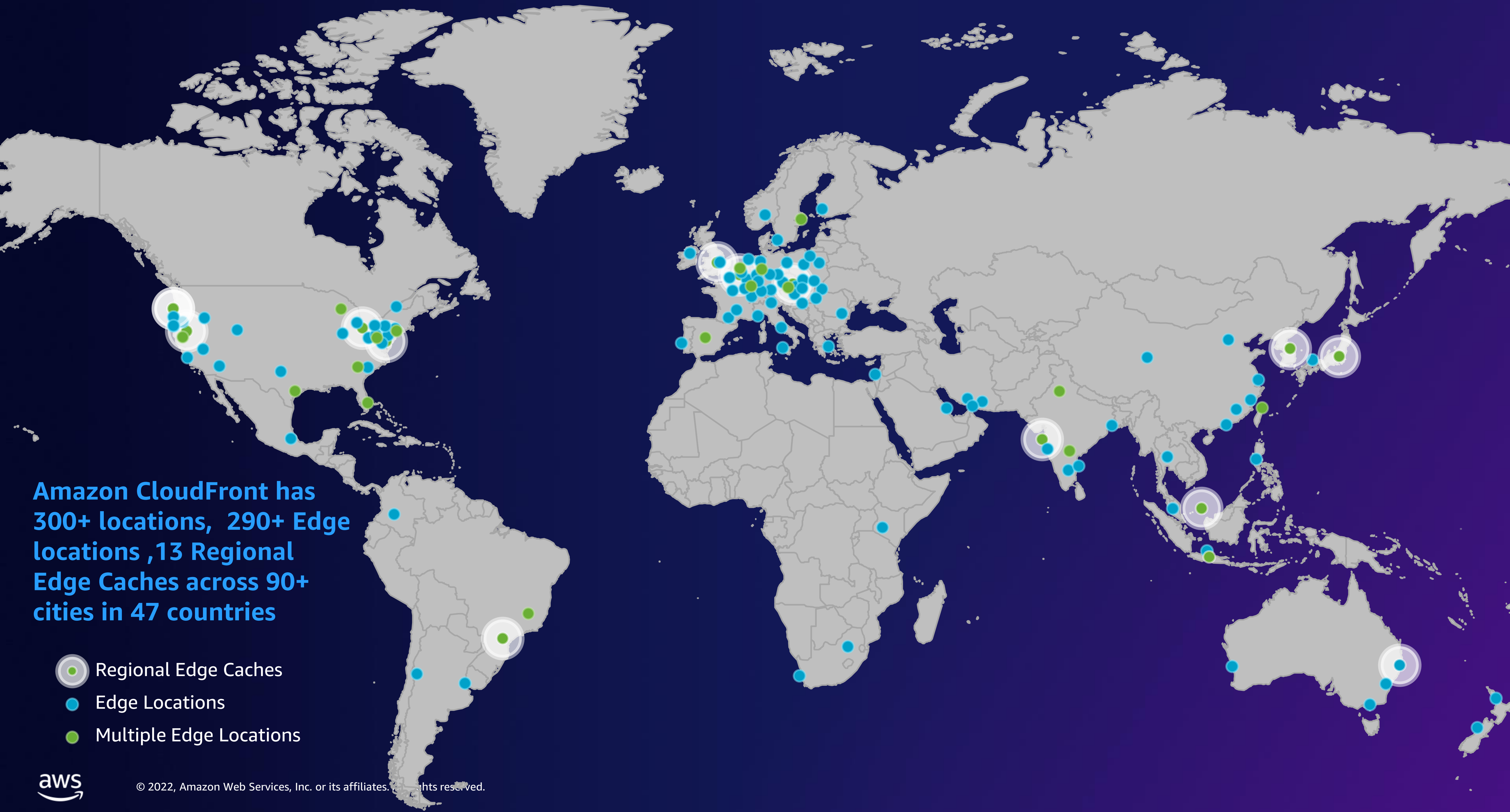


Availabiliy Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity in an AWS Region.

A Region is a physical location in the world where we have multiple **Availability Zones.**

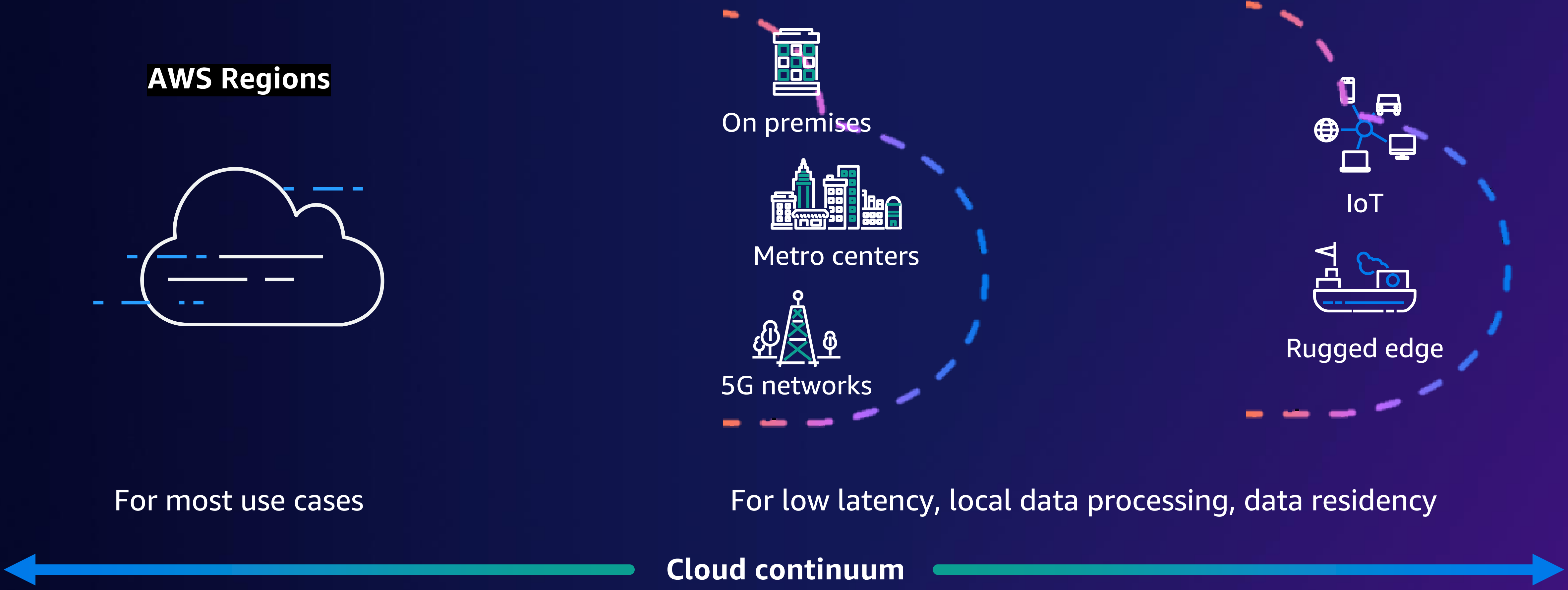
Global network

Redundant, parellel 100 GbE fiber network and low-latency private capacity between all regions except China. Includes trans-ocean cables.



Amazon CloudFront has 300+ locations, 290+ Edge locations ,13 Regional Edge Caches across 90+ cities in 47 countries

Cloud continuum



AWS Regions

On premises

Metro centers

5G networks

IoT

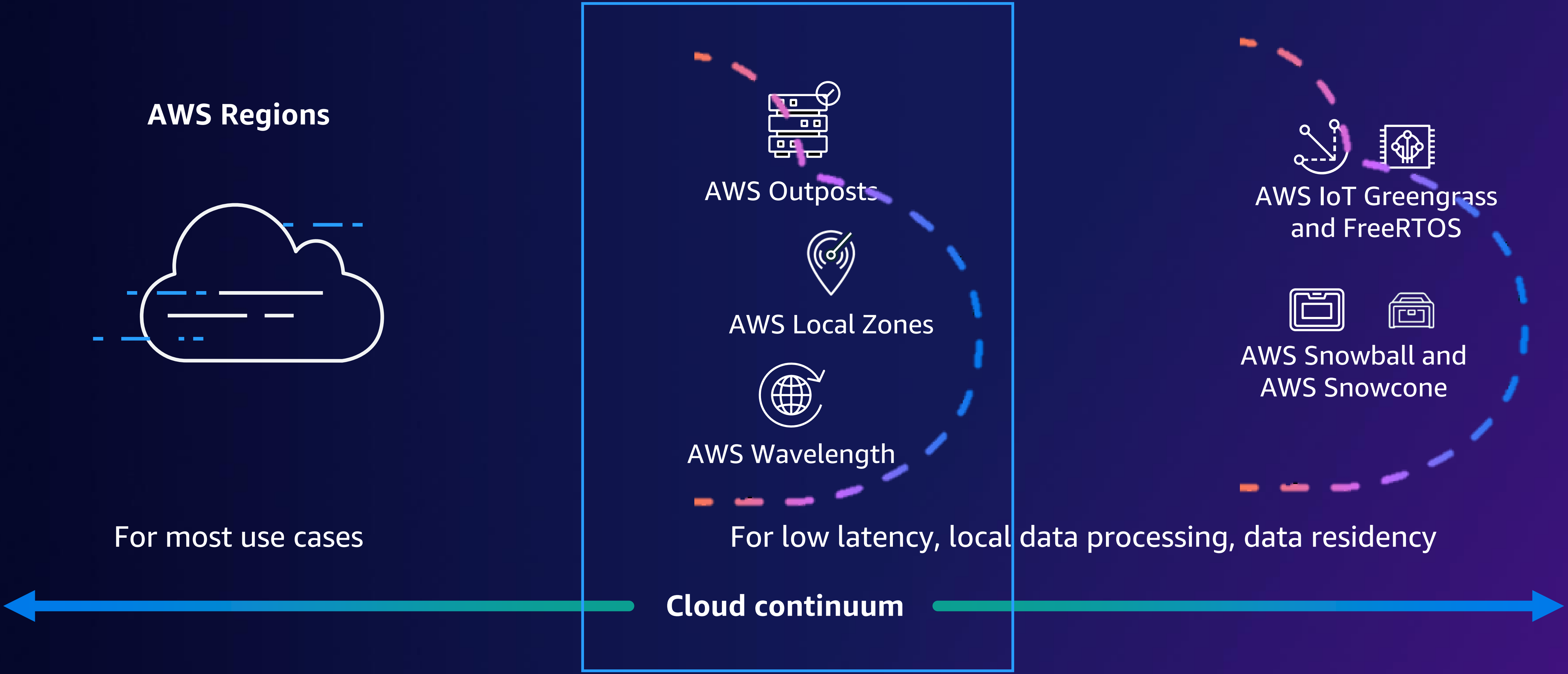
Rugged edge

For most use cases

For low latency, local data processing, data residency

Cloud continuum

Bringing the cloud to where you need it



AWS Regions

AWS Outposts

AWS Local Zones

AWS Wavelength

AWS IoT Greengrass and FreeRTOS

AWS Snowball and AWS Snowcone

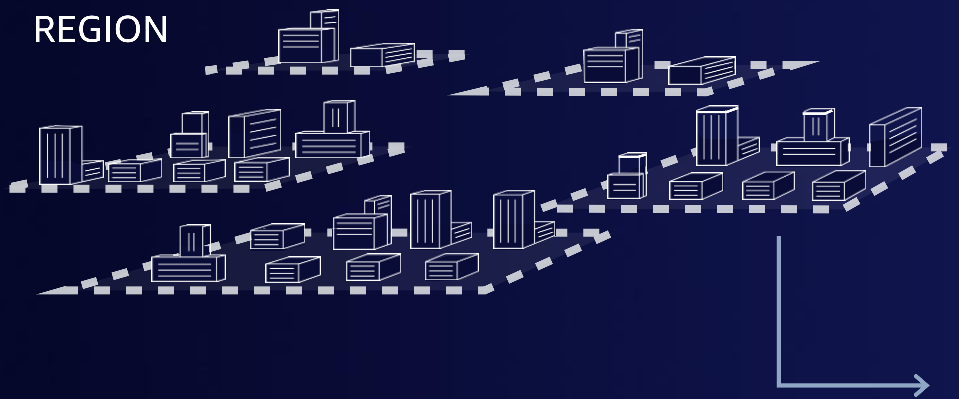
For most use cases

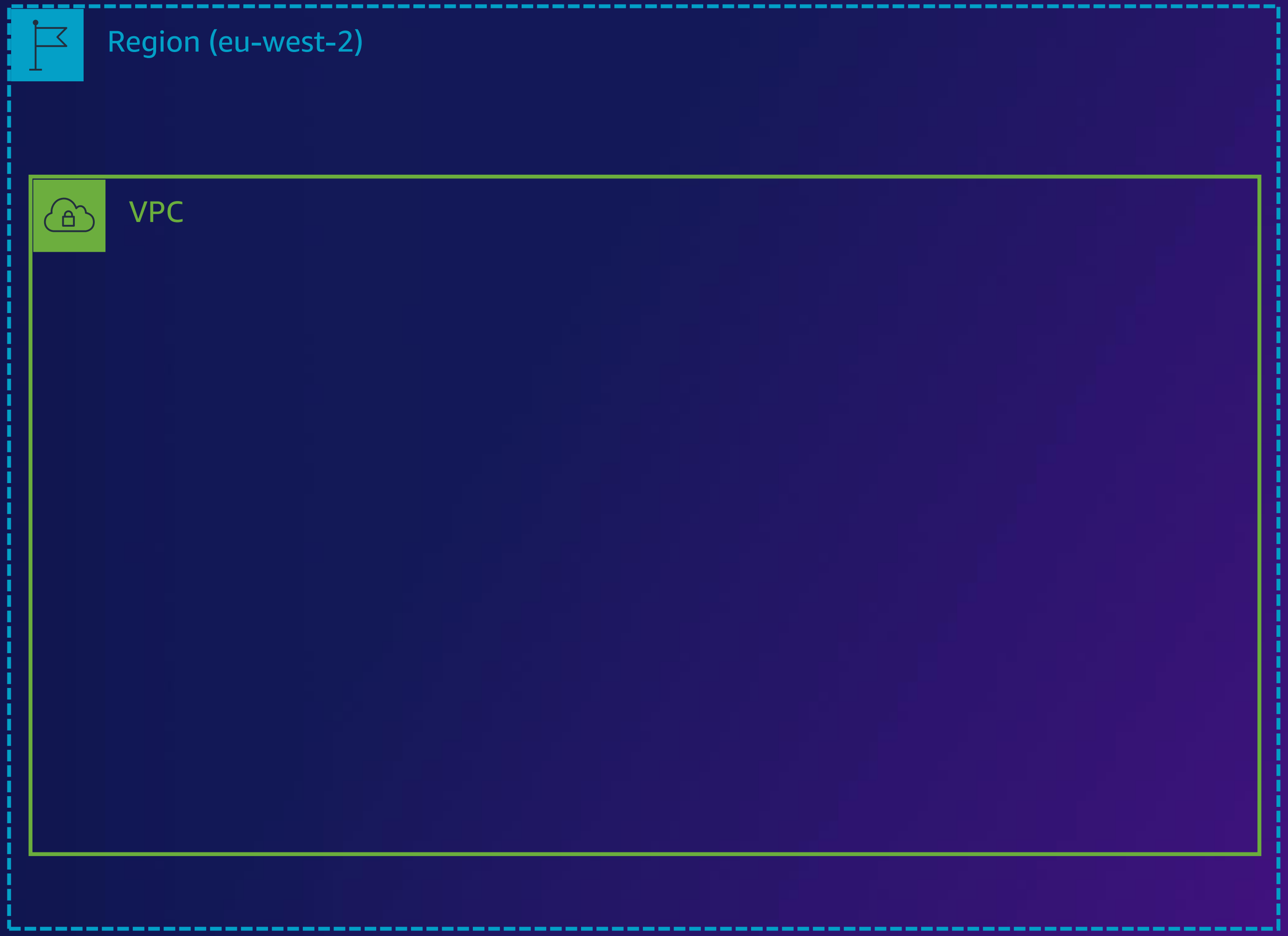
For low latency, local data processing, data residency

Cloud continuum

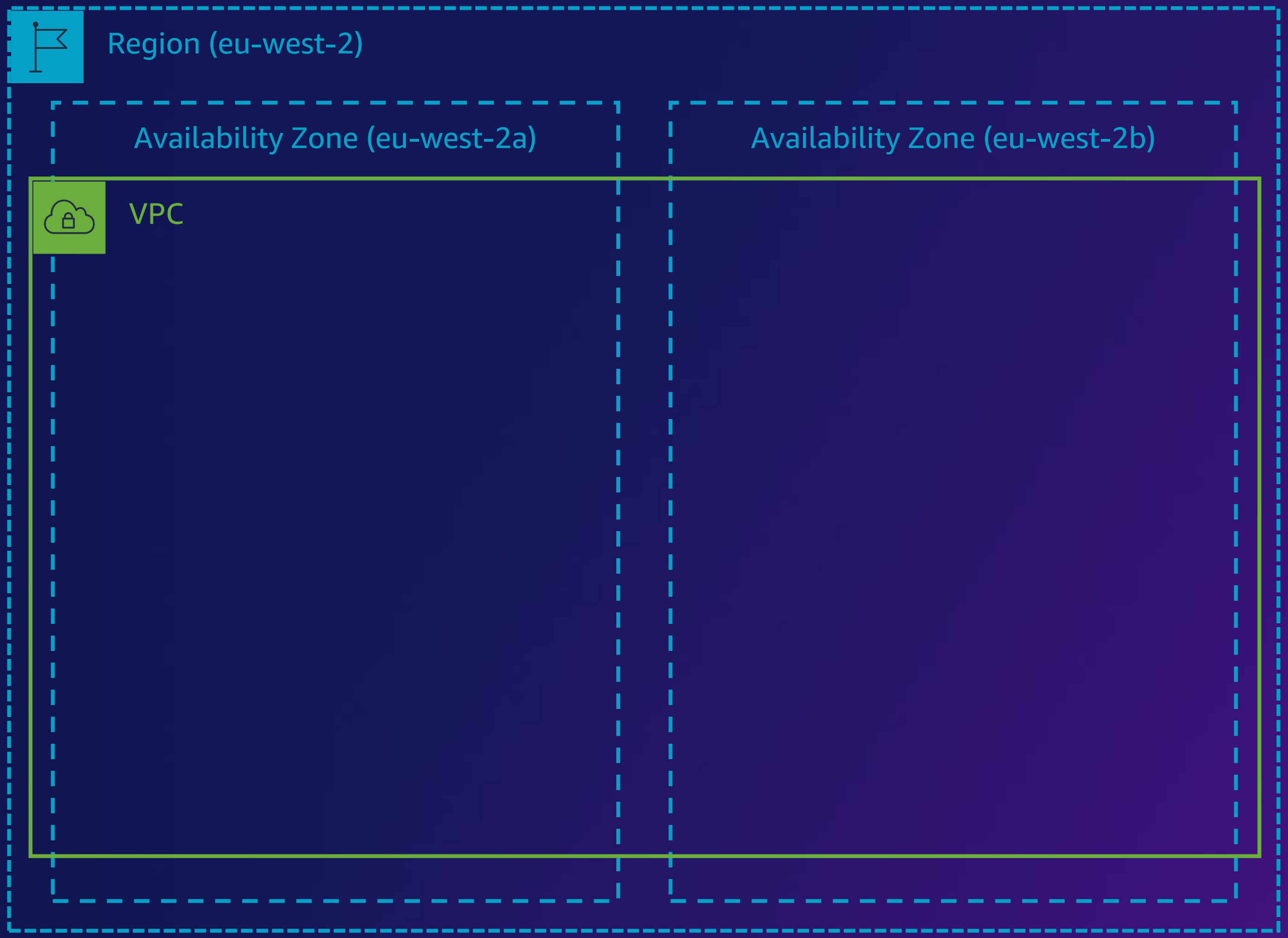
Amazon Virtual Private Cloud

Building a VPC

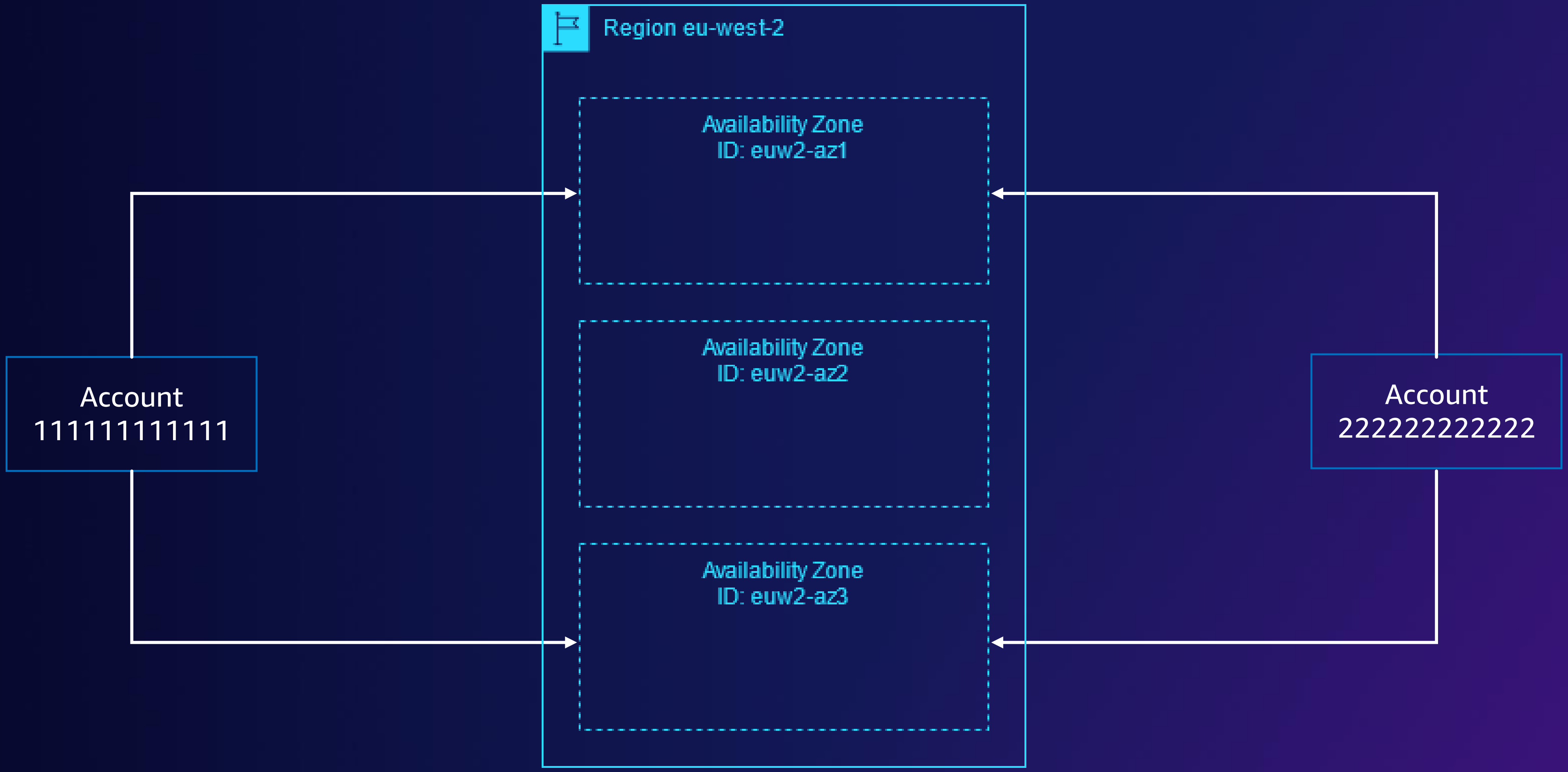




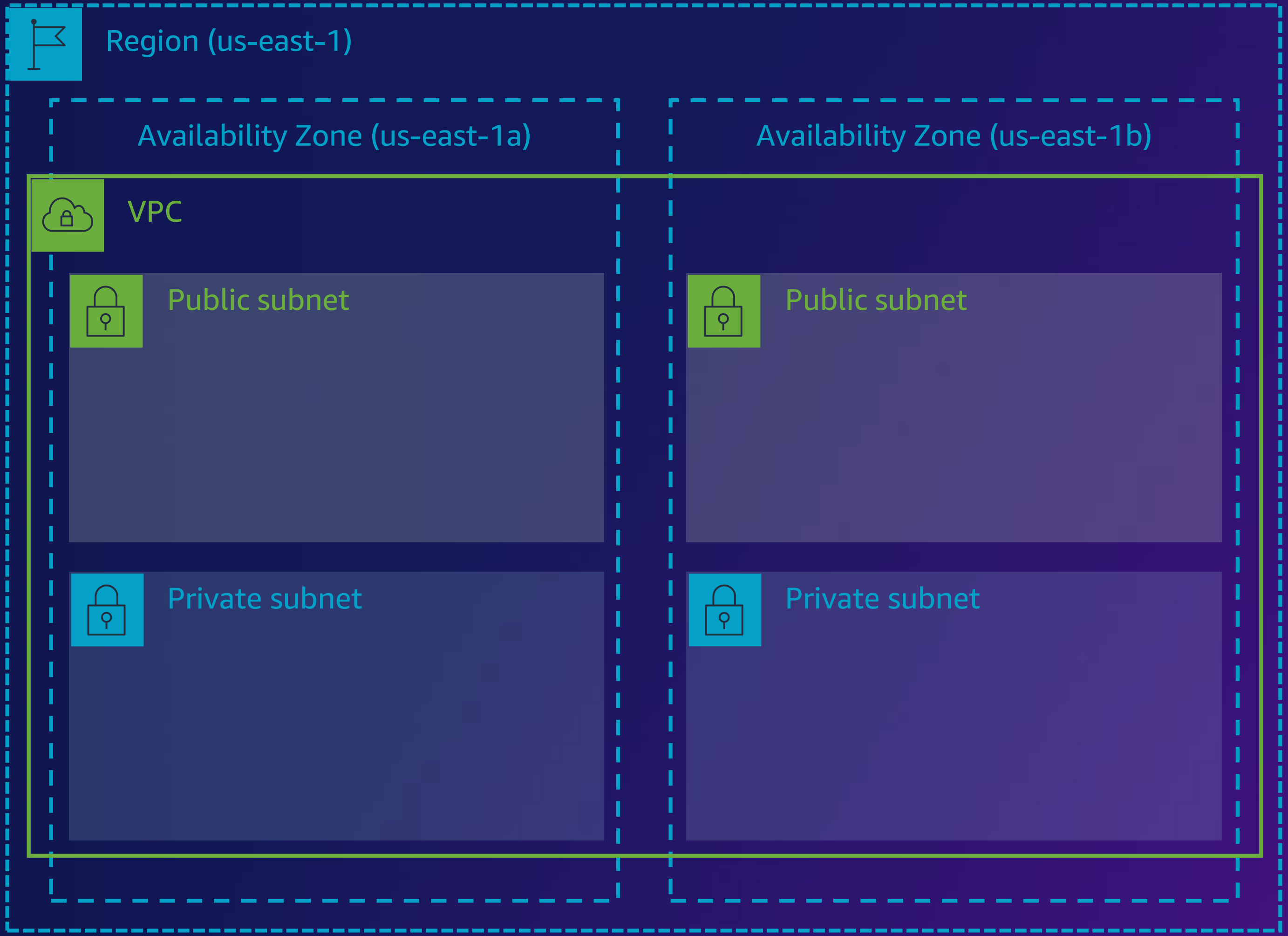
Building a VPC


Region (eu-west-2)
Availability Zone (eu-west-2a)
Availability Zone (eu-west-2b)
VPC

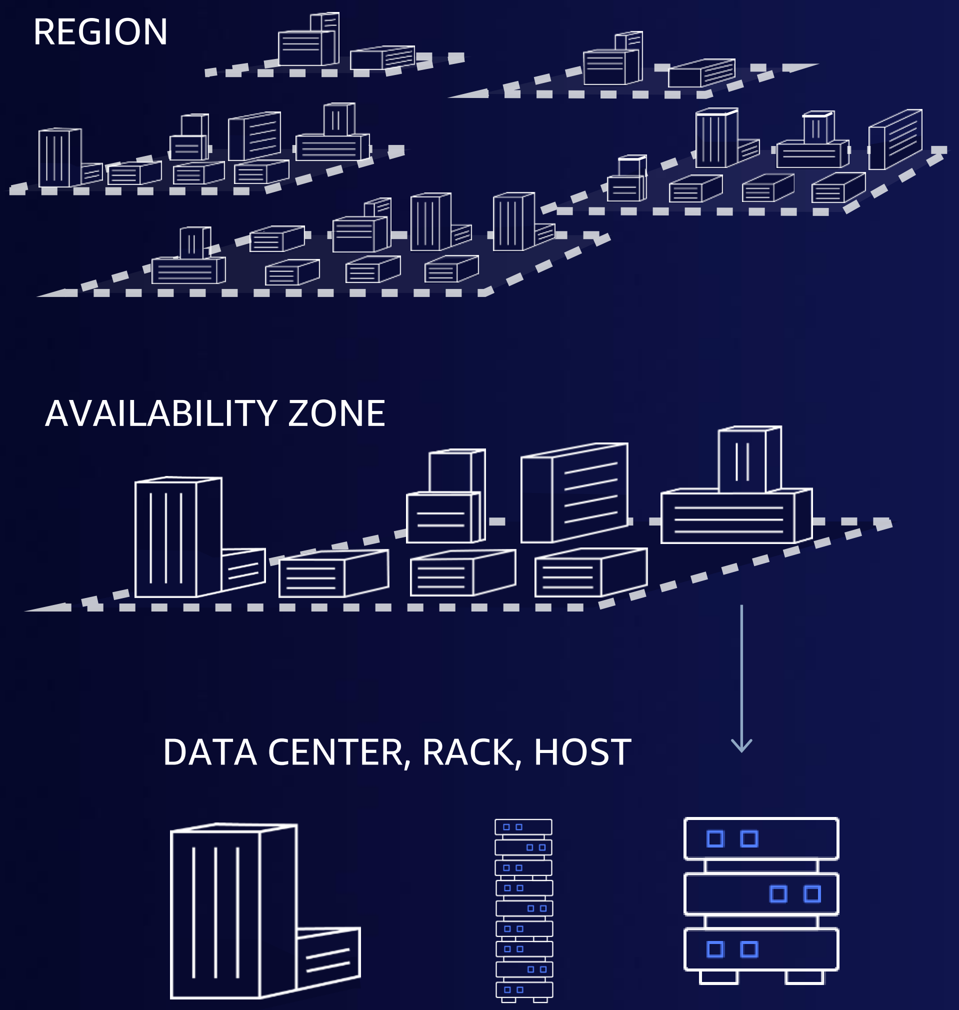
Availability Zone IDs for your AWS resources



Building a VPC



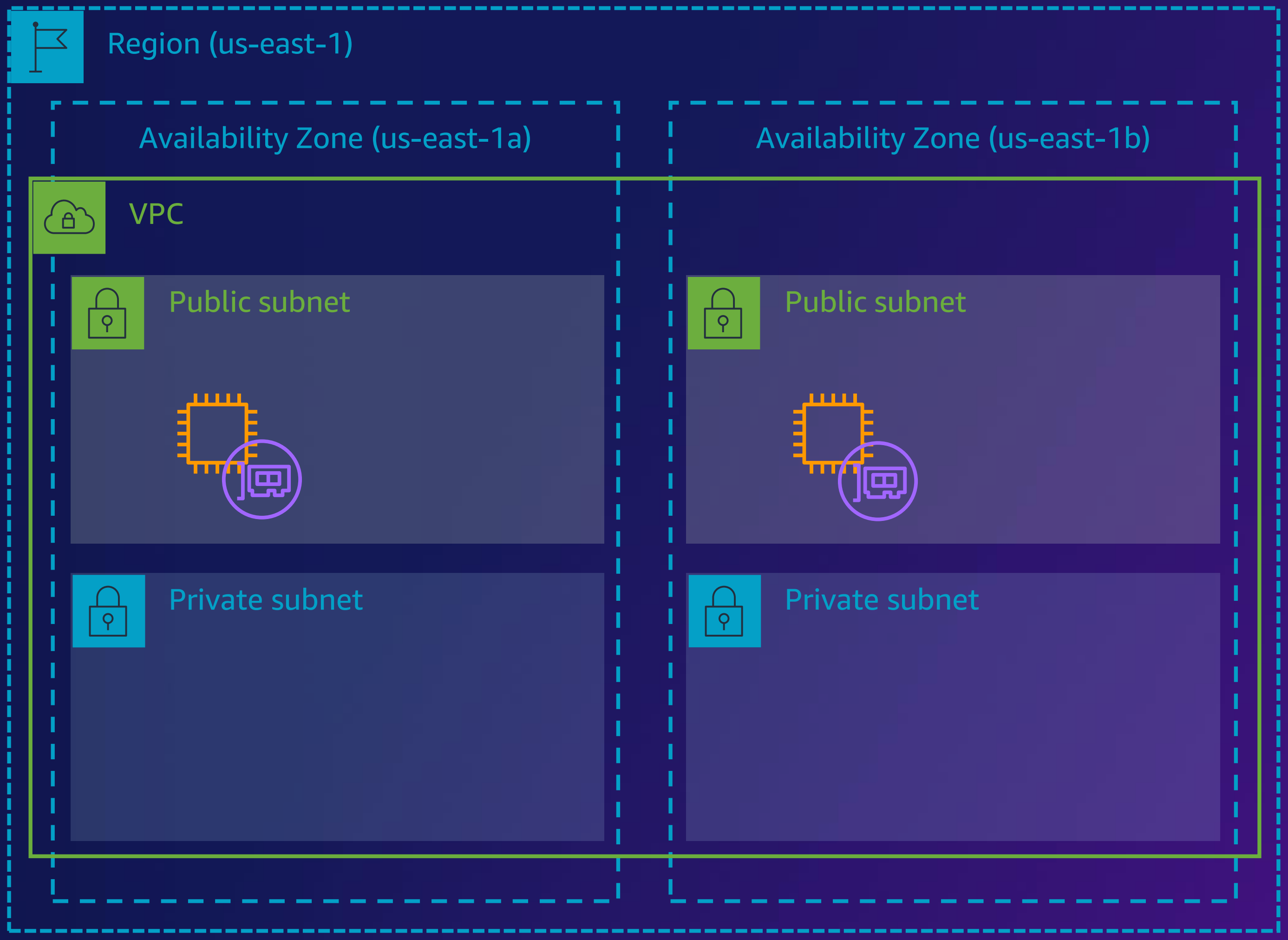
Building a VPC



REGION

AVAILABILITY ZONE

DATA CENTER, RACK, HOST



Region (us-east-1)

Availability Zone (us-east-1a)

Availability Zone (us-east-1b)

VPC

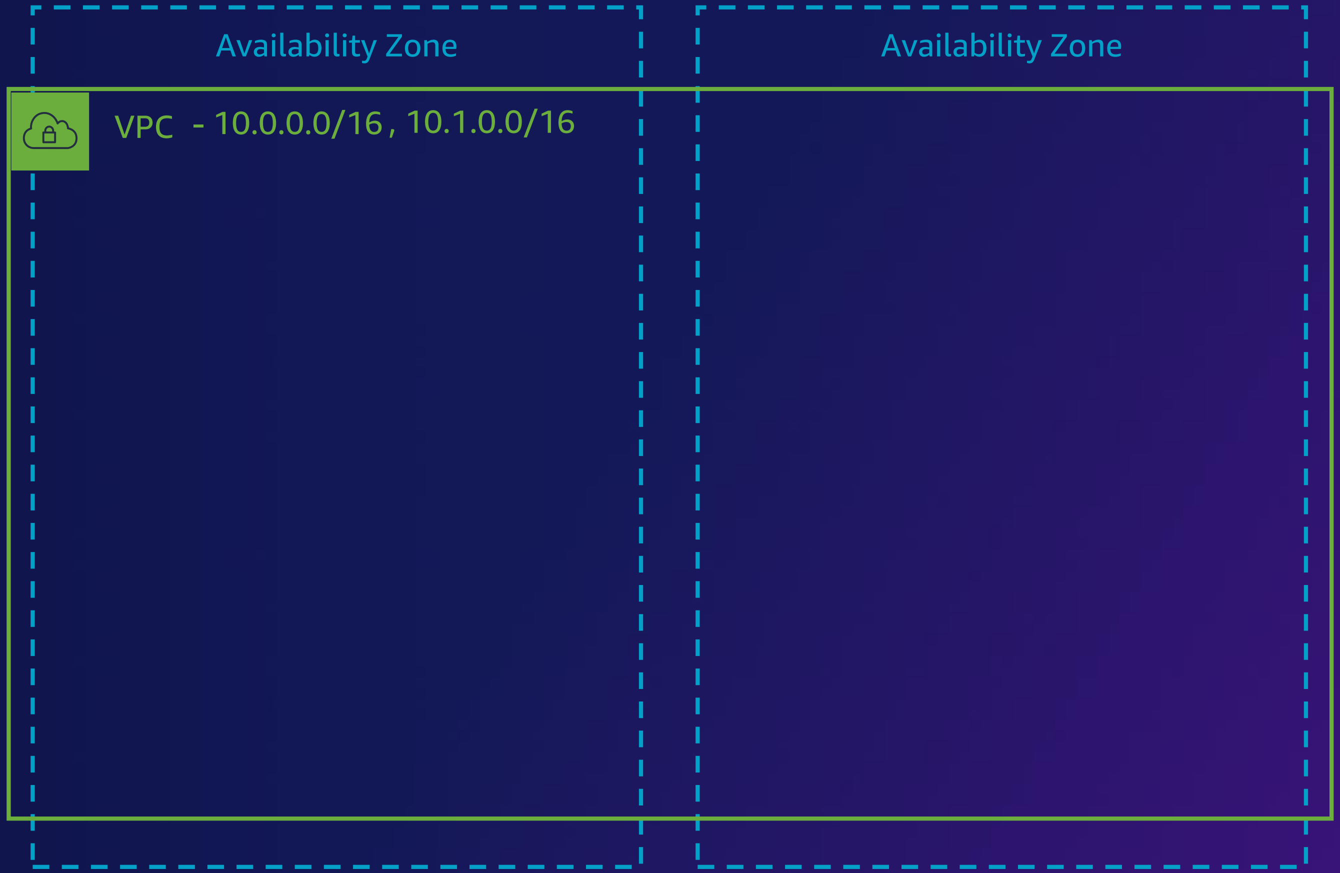
Public subnet

Public subnet

Private subnet

Private subnet

IPv4 addressing



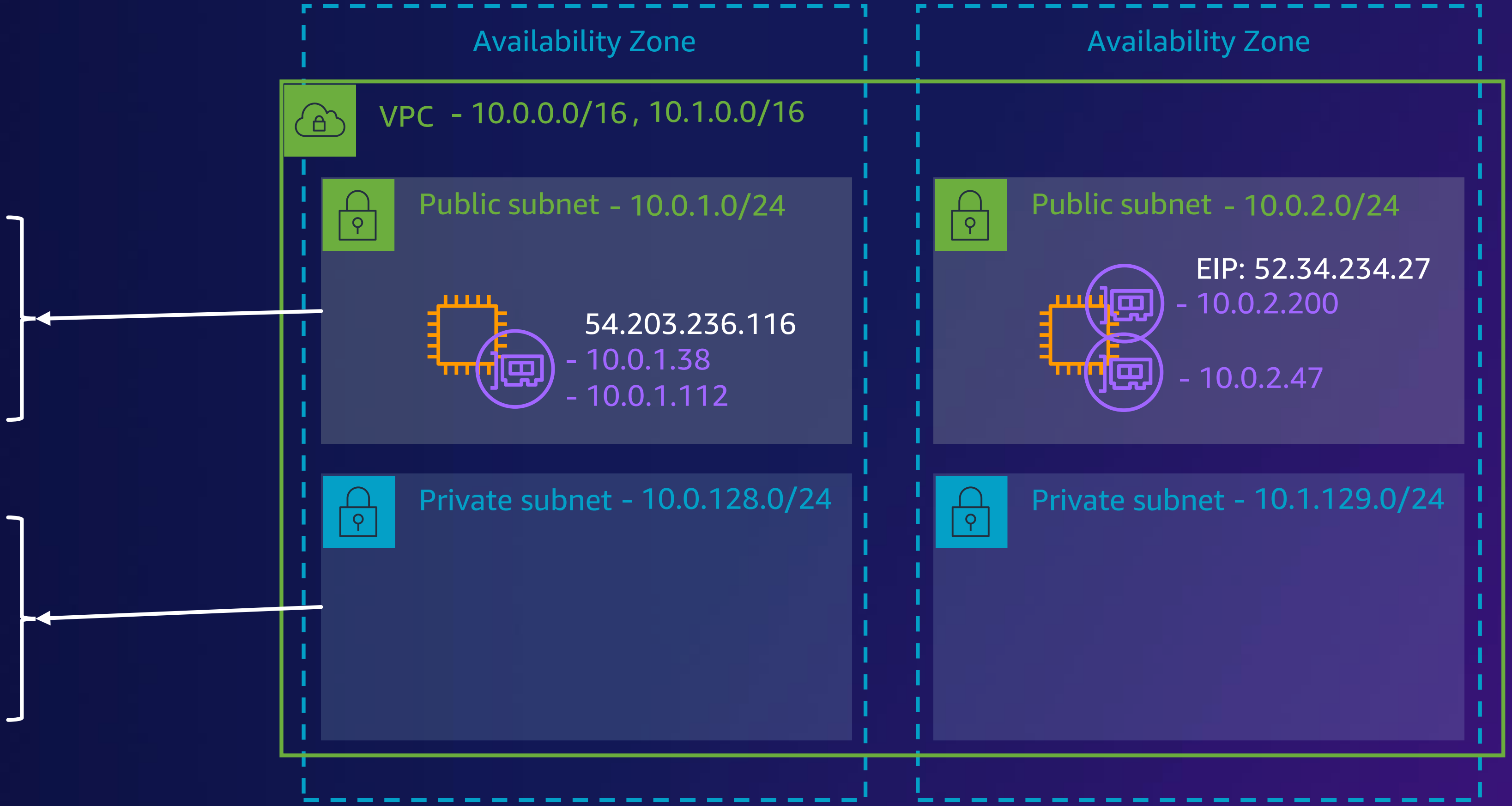
IPv4 addressing

Reserved

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

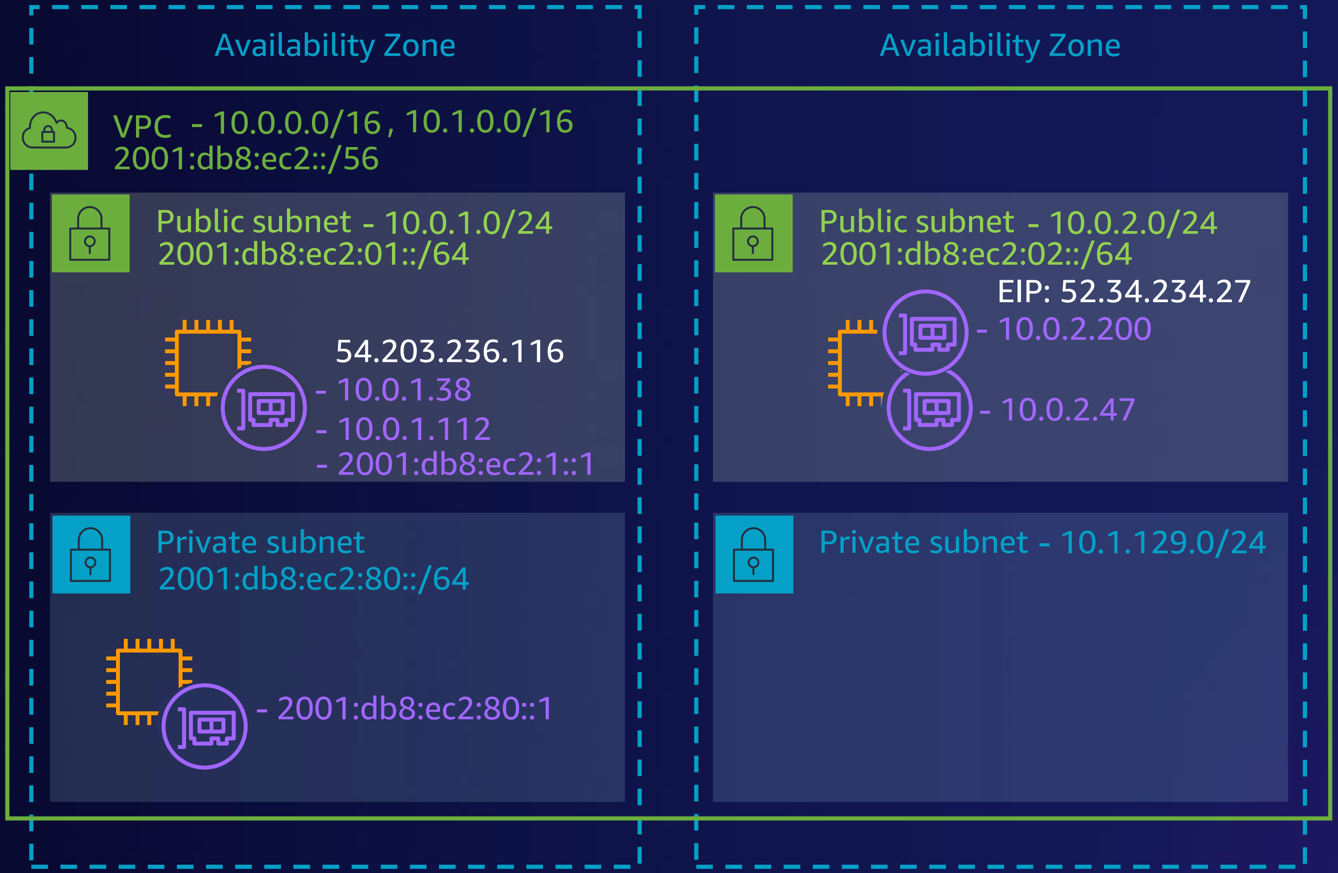
. . .

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



Availability Zone
Availability Zone
VPC - 10.0.0.0/16 , 10.1.0.0/16
Public subnet - 10.0.1.0/24
54.203.236.116
- 10.0.1.38
- 10.0.1.112
Public subnet - 10.0.2.0/24
EIP: 52.34.234.27
- 10.0.2.200
- 10.0.2.47
Private subnet - 10.0.128.0/24
Private subnet - 10.1.129.0/24

IPv6 addressing

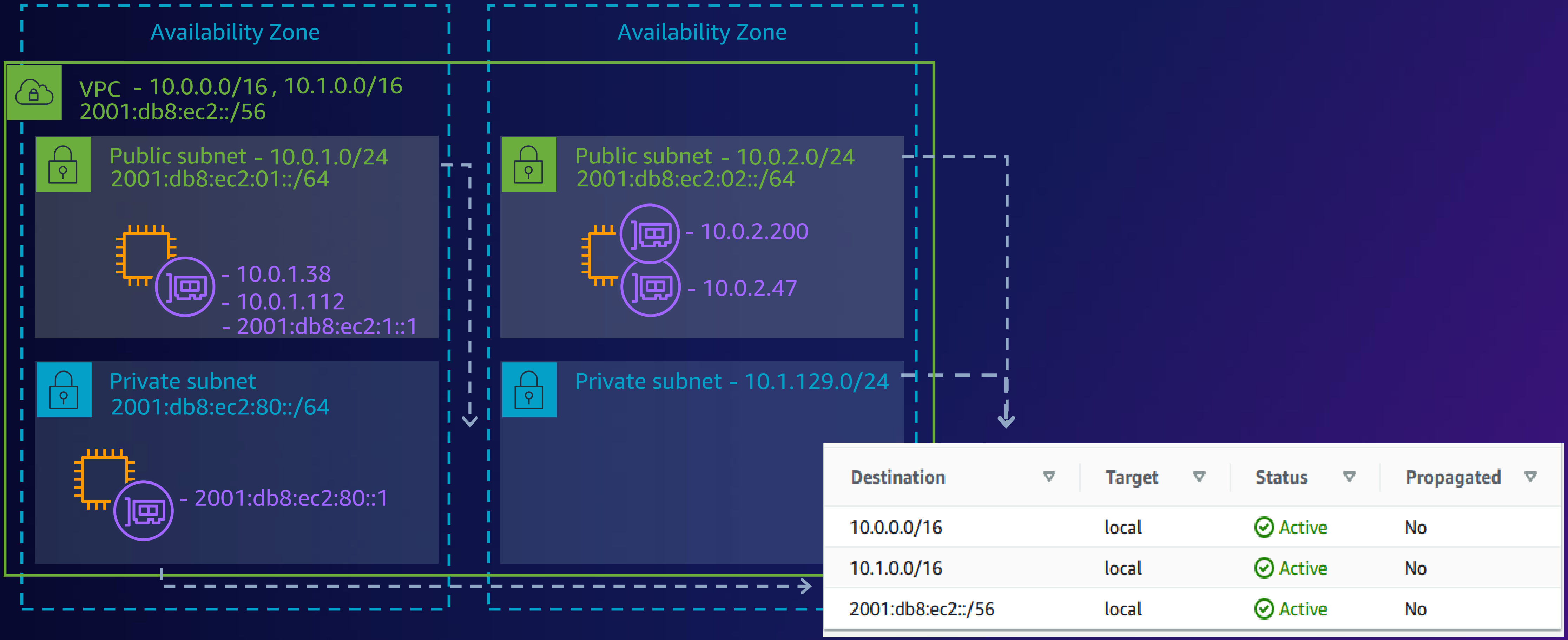


Reserved
fd00:ec2::/32 - Reserved
fe80::X:Xff:feX:X/64 – VPC Router

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
. . .

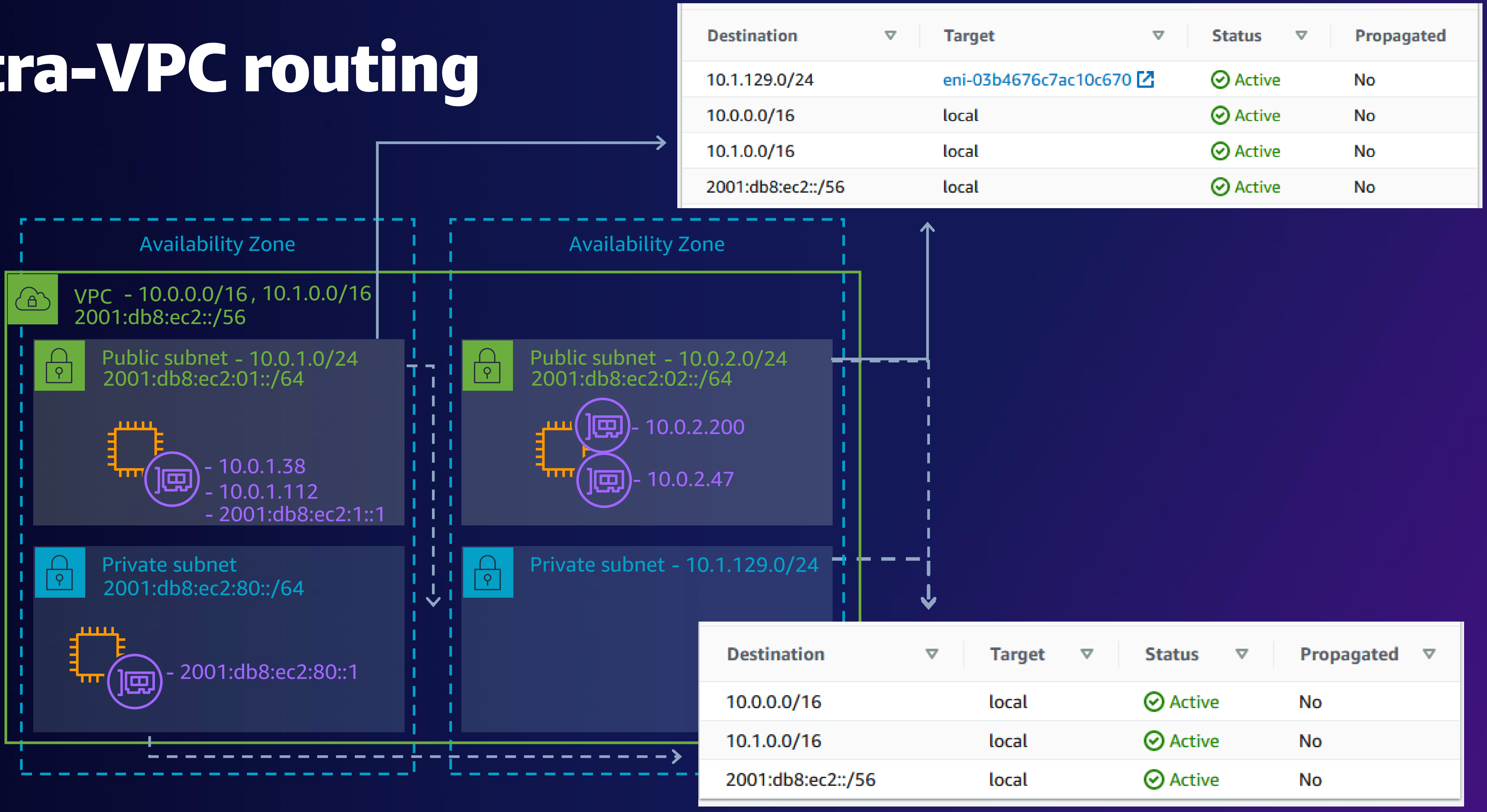
2001:db8:ec2:80::0
2001:db8:ec2:80::1
2001:db8:ec2:80::2
2001:db8:ec2:80::3
2001:db8:ec2:80:ffff:ffff:ffff:ffff

Intra-VPC routing



Destination ▽	Target ▽	Status ▽	Propagated ▽
10.0.0.0/16	local	✓ Active	No
10.1.0.0/16	local	✓ Active	No
2001:db8:ec2::/56	local	✓ Active	No

Intra-VPC routing



Destination	Target	Status	Propagated
10.1.129.0/24	eni-03b4676c7ac10c670	✓ Active	No
10.0.0.0/16	local	✓ Active	No
10.1.0.0/16	local	✓ Active	No
2001:db8:ec2::/56	local	✓ Active	No

Availability Zone

Availability Zone

VPC - 10.0.0.0/16, 10.1.0.0/16
2001:db8:ec2::/56

Public subnet - 10.0.1.0/24
2001:db8:ec2:01::/64

- 10.0.1.38
- 10.0.1.112
- 2001:db8:ec2:1::1

Public subnet - 10.0.2.0/24
2001:db8:ec2:02::/64

- 10.0.2.200
- 10.0.2.47

Private subnet
2001:db8:ec2:80::/64

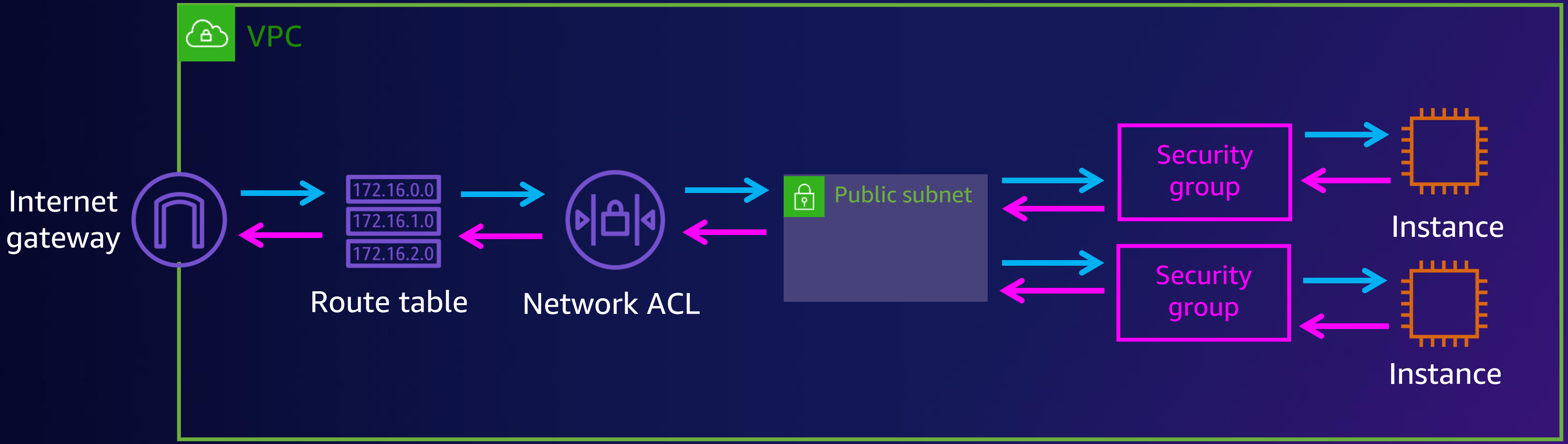
- 2001:db8:ec2:80::1

Private subnet - 10.1.129.0/24

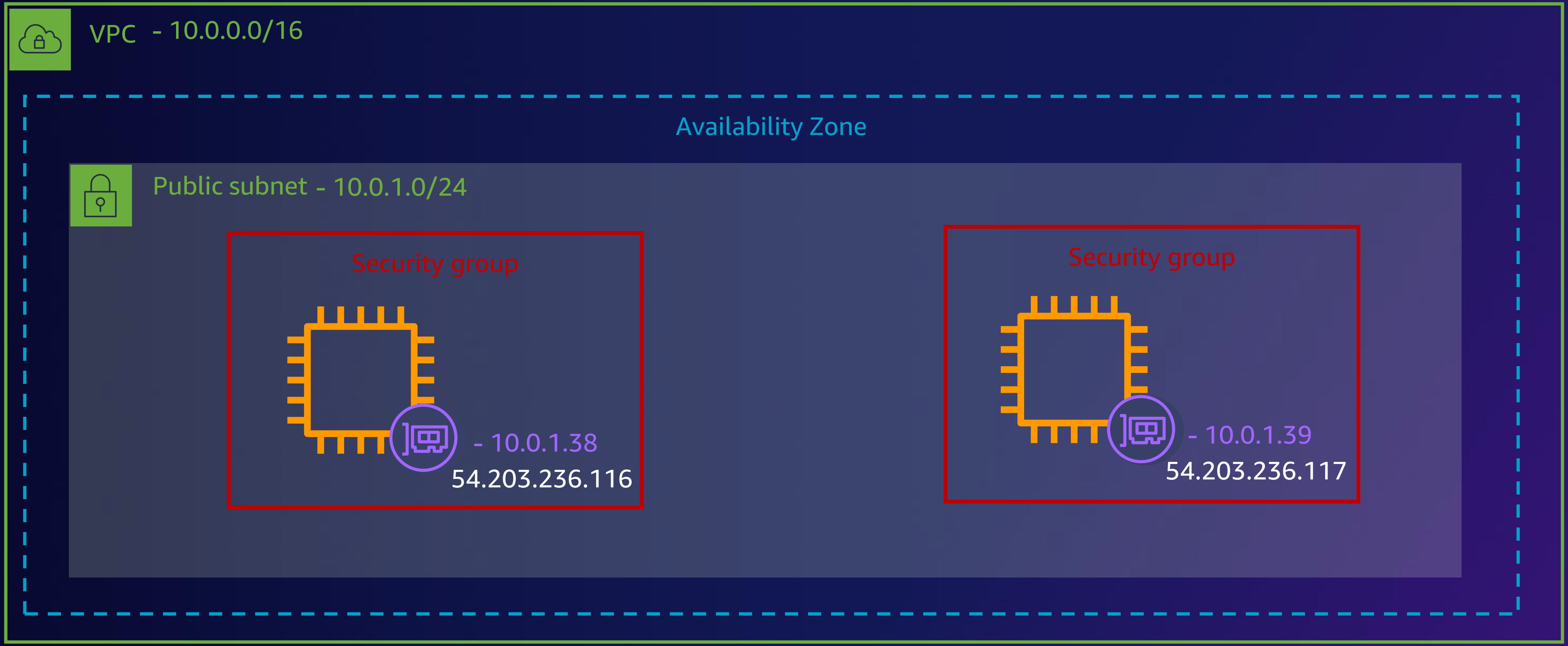
Destination	Target	Status	Propagated
10.0.0.0/16	local	✓ Active	No
10.1.0.0/16	local	✓ Active	No
2001:db8:ec2::/56	local	✓ Active	No

Basics of VPC security

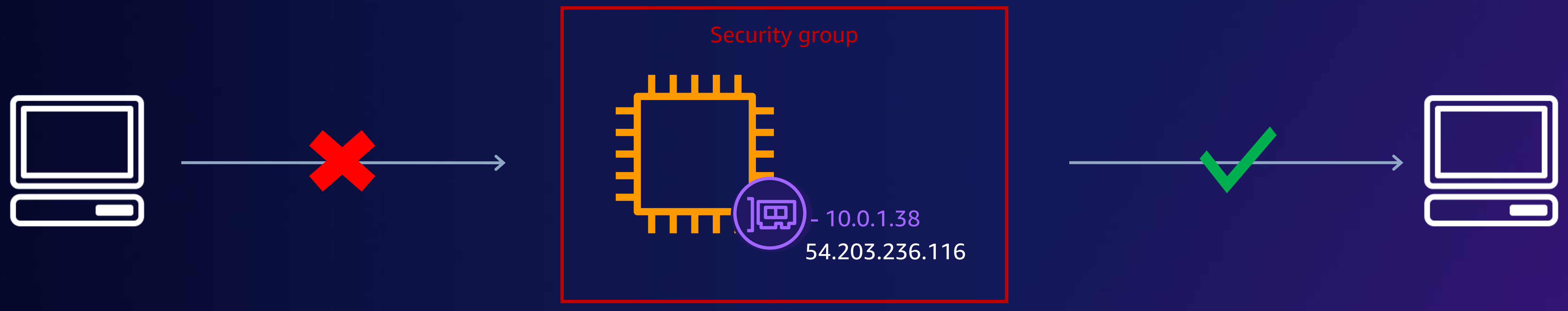
VPC defense in depth

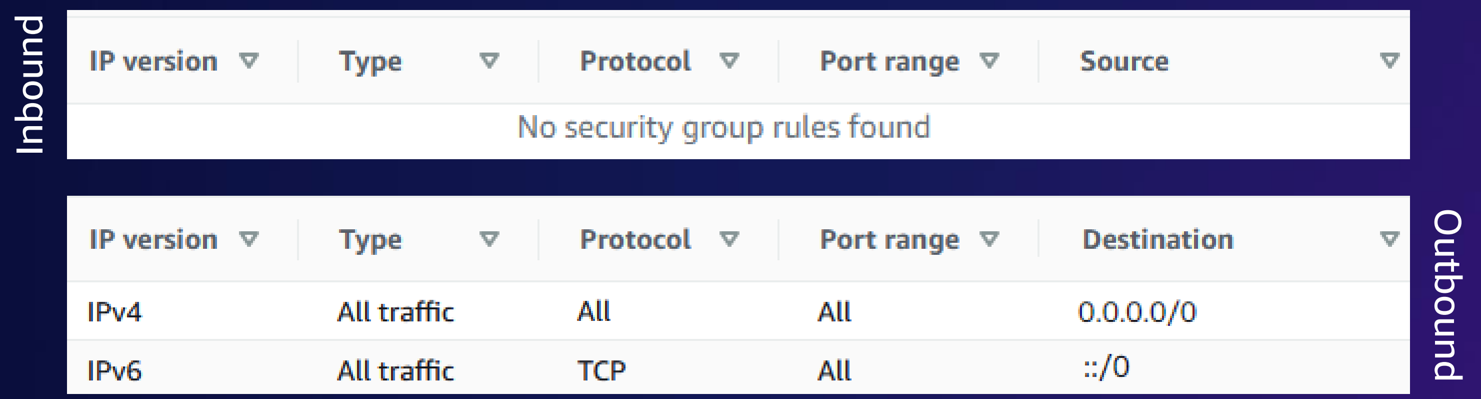


Security groups



Security groups – default behavior





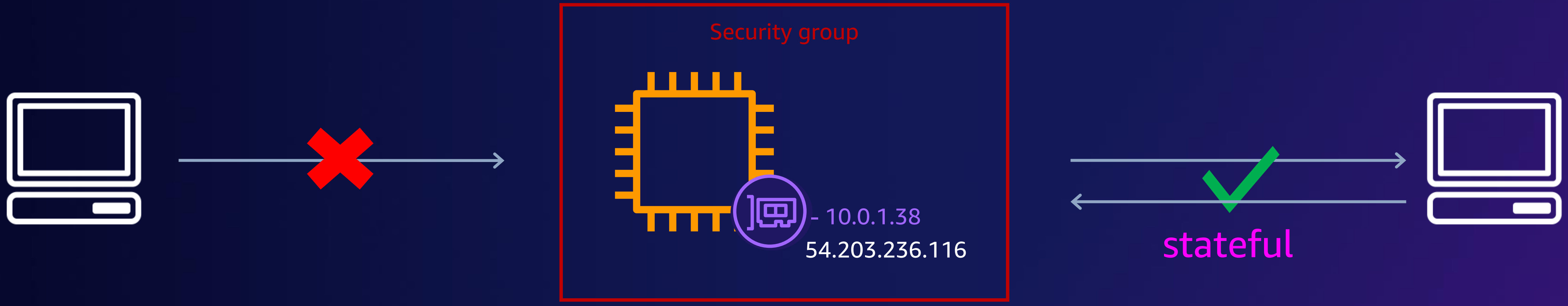
Inbound

IP version	Type	Protocol	Port range	Source
No security group rules found				

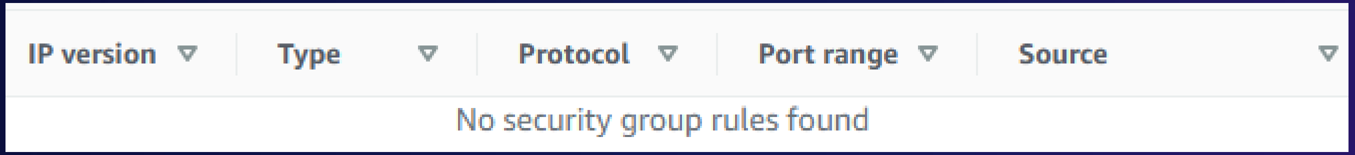
Outbound

IP version	Type	Protocol	Port range	Destination
IPv4	All traffic	All	All	0.0.0.0/0
IPv6	All traffic	TCP	All	::/0

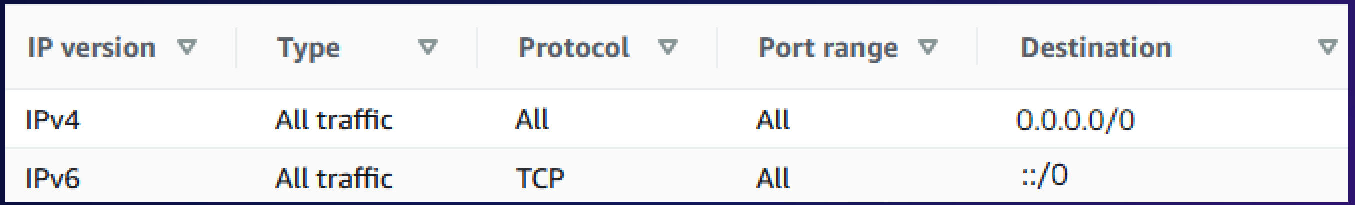
Security groups – default behavior



Inbound



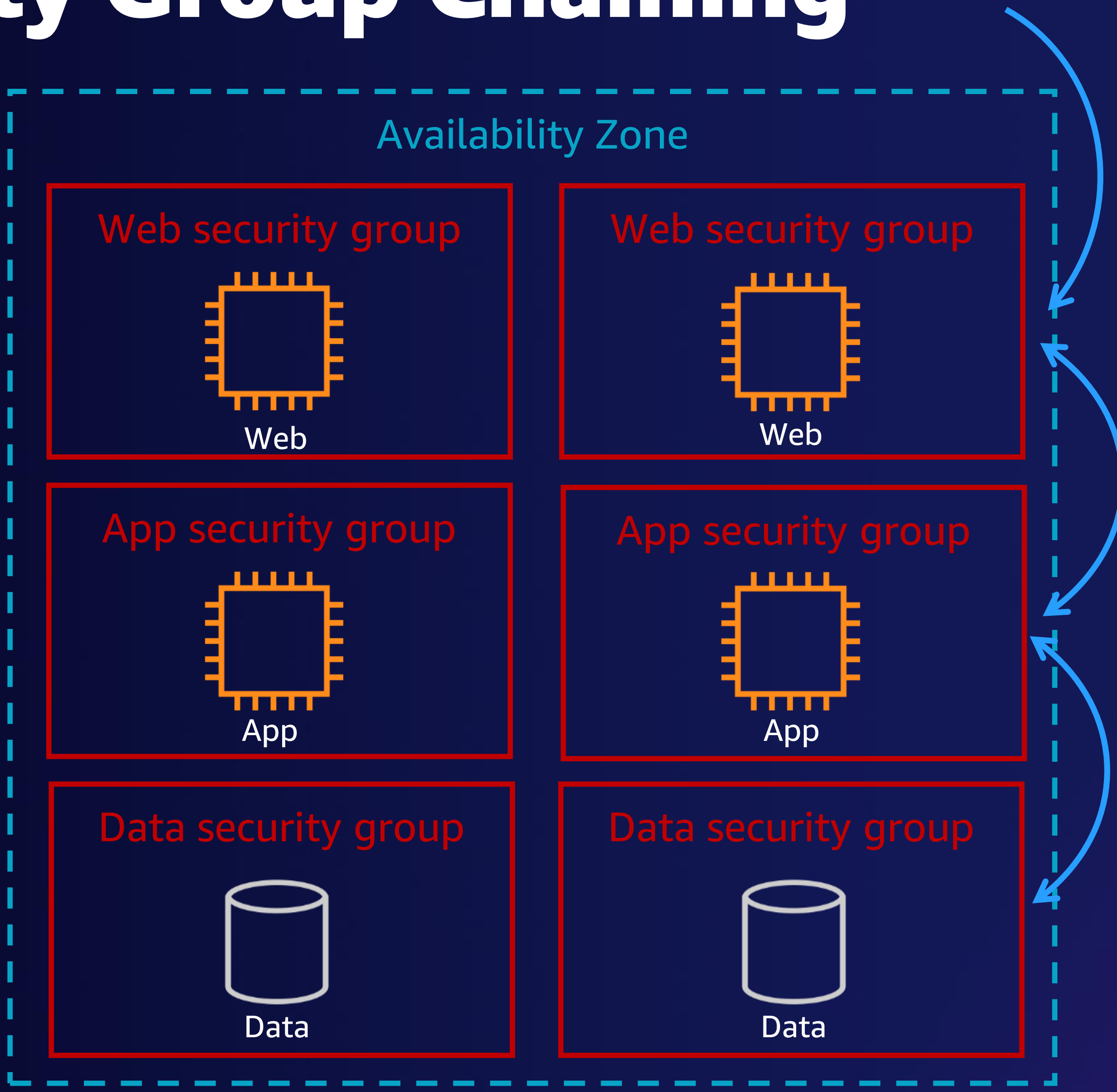
IP version	Type	Protocol	Port range	Source
No security group rules found				



IP version	Type	Protocol	Port range	Destination
IPv4	All traffic	All	All	0.0.0.0/0
IPv6	All traffic	TCP	All	::/0

Outbound

Security Group Chaining

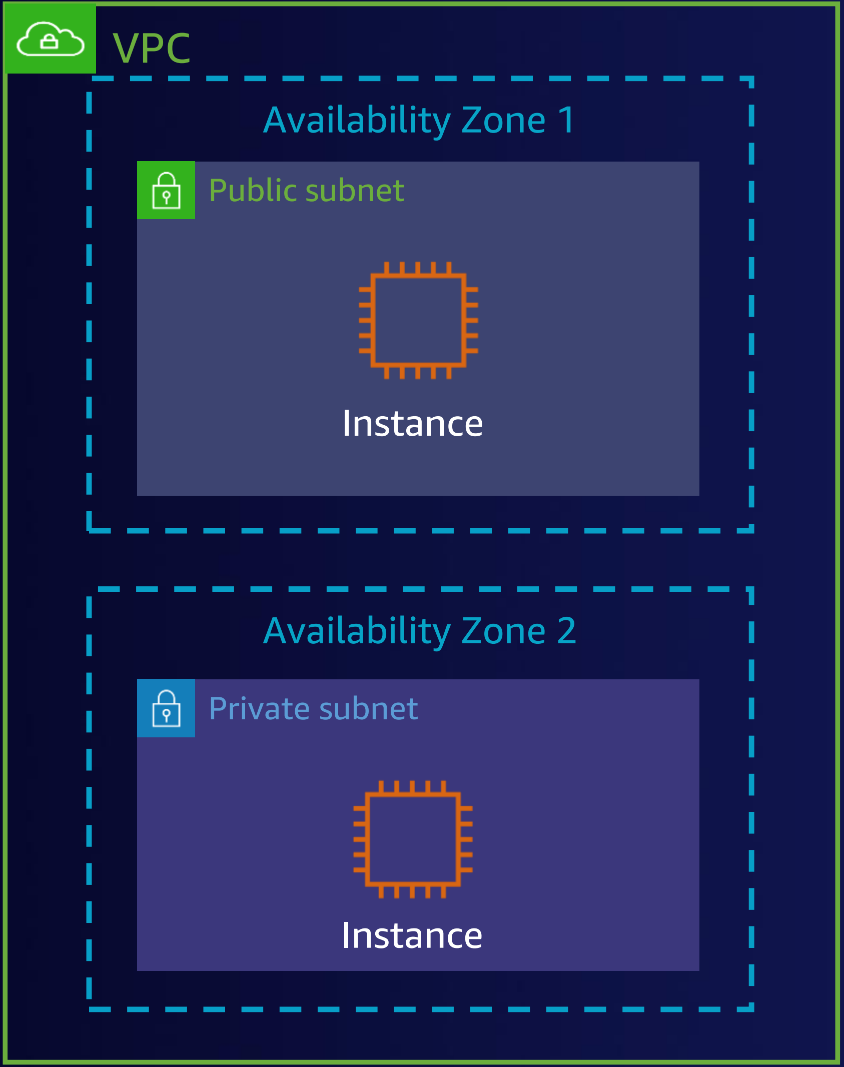


Inbound rule
Allow HTTPS port 443
Source: 0.0.0.0/0 (any)

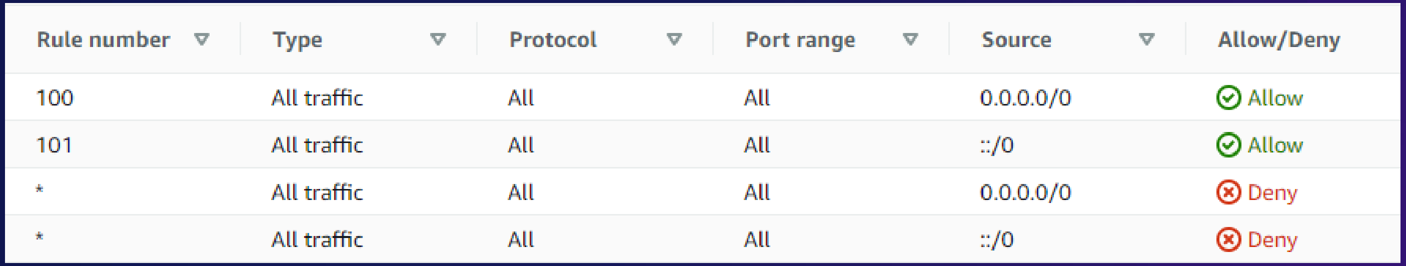
Inbound rule
Allow HTTP port 80
Source: Web tier

Inbound rule
Allow TCP port 3306
Source: App tier

Network access control lists (NACLs)

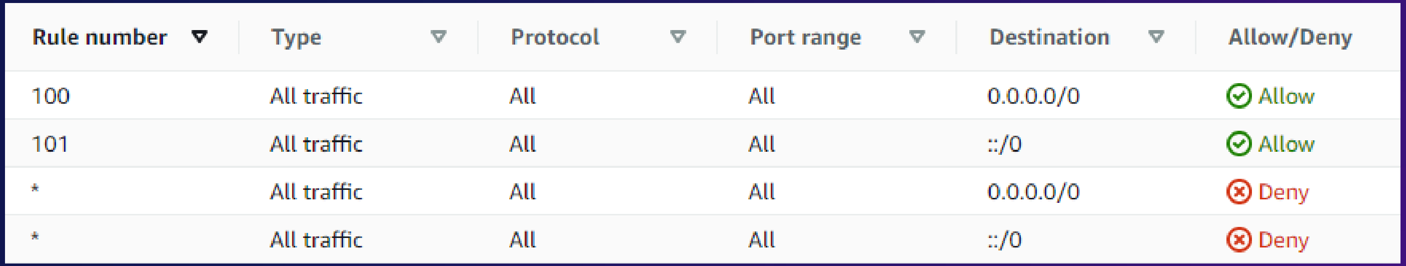


Inbound rules - default



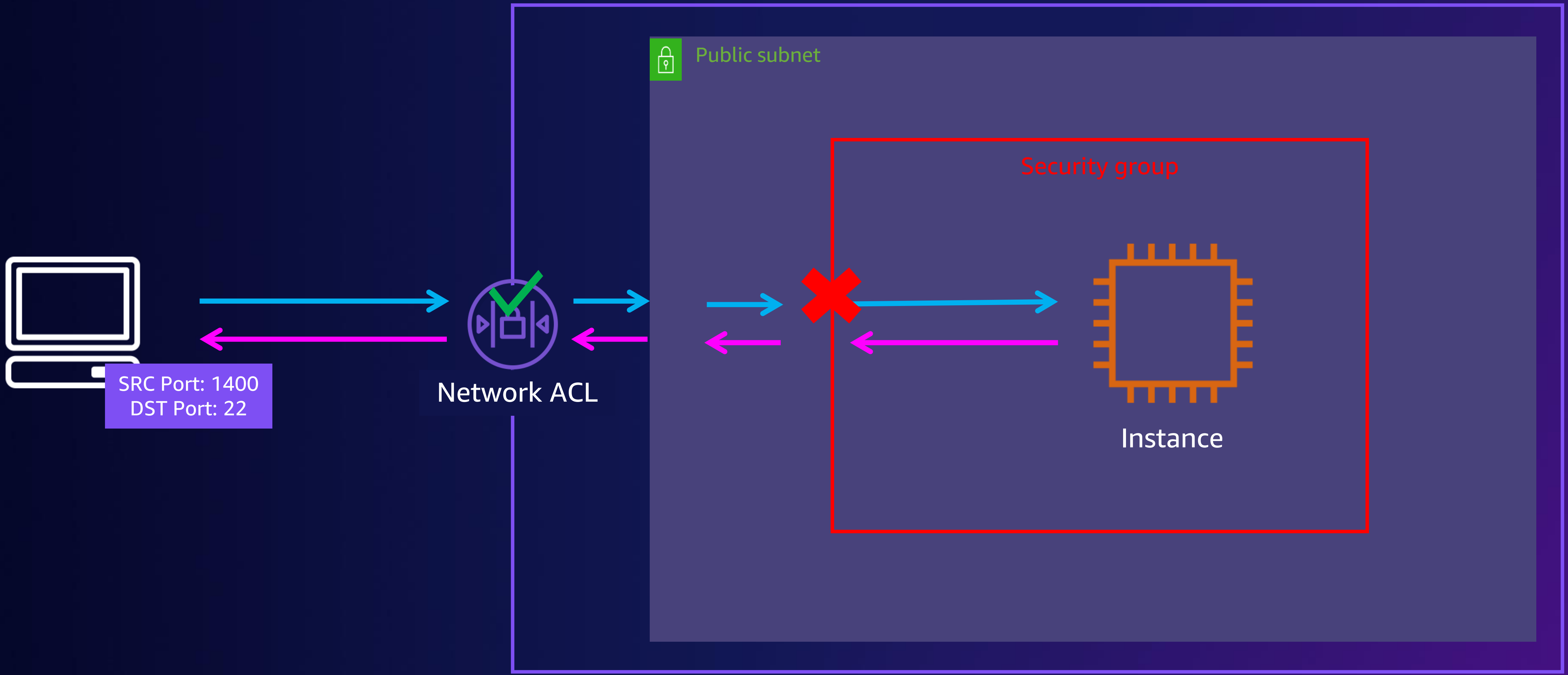
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
101	All traffic	All	All	::/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny
*	All traffic	All	All	::/0	⊗ Deny

Outbound rules - default



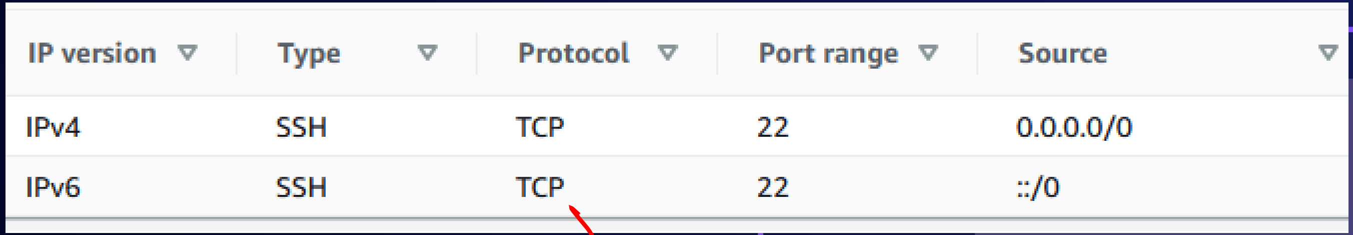
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
101	All traffic	All	All	::/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny
*	All traffic	All	All	::/0	⊗ Deny

Additional configurations for inbound traffic

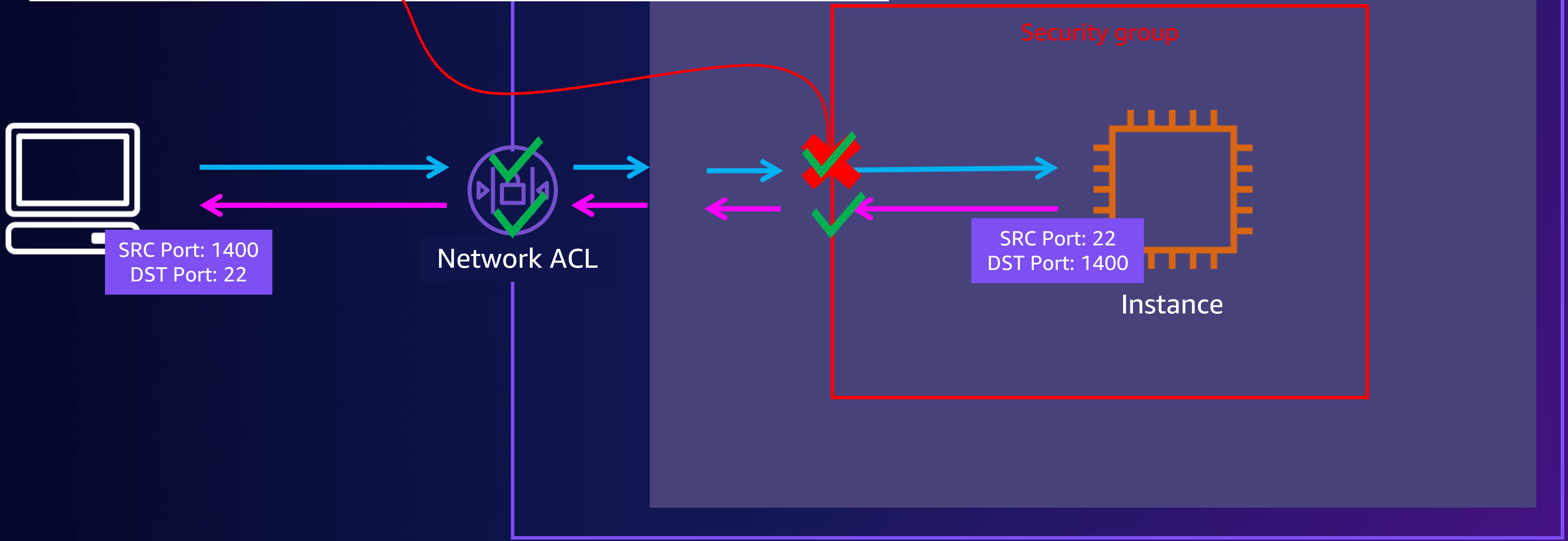


Additional configurations for inbound traffic

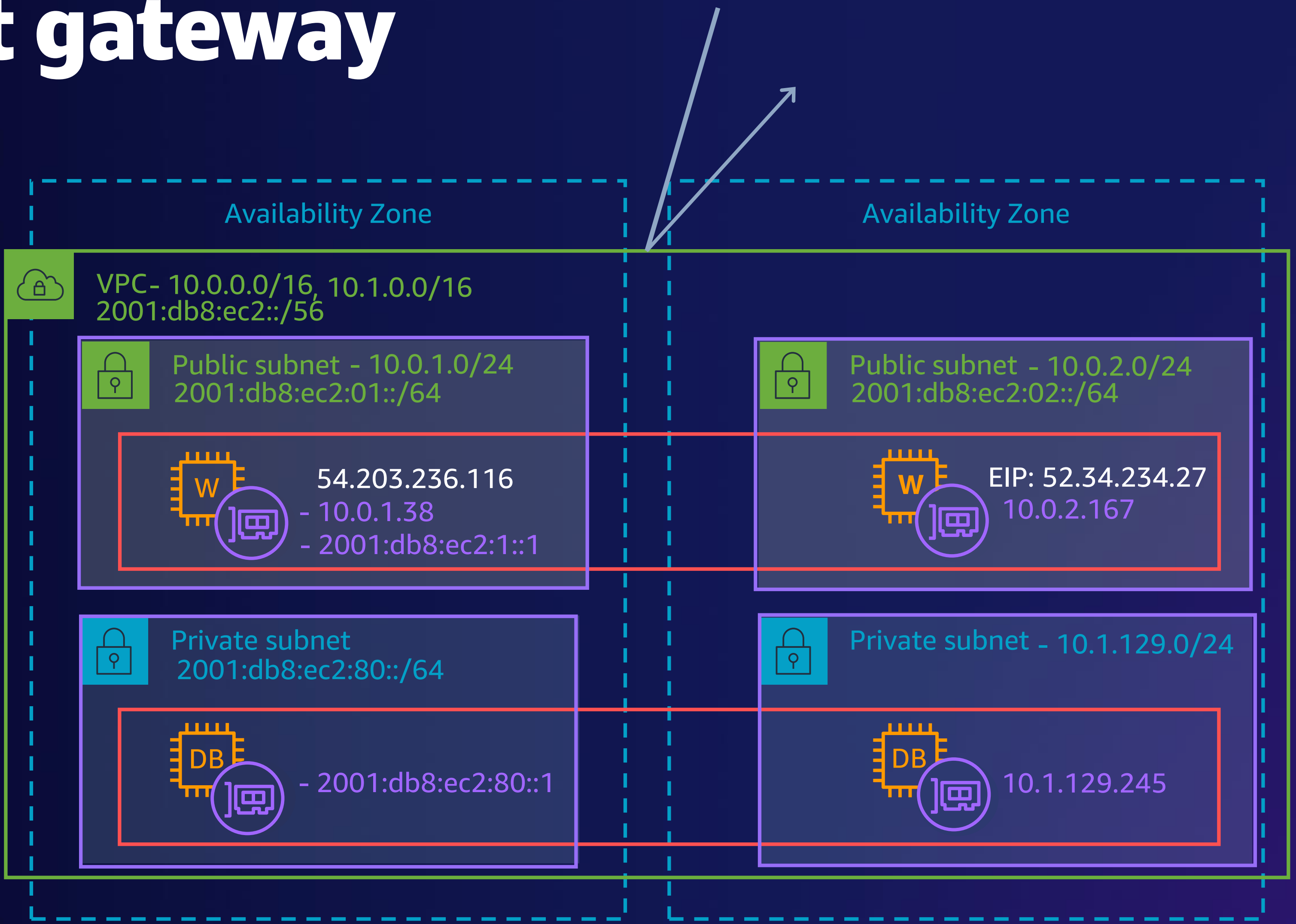
Inbound



IP version	Type	Protocol	Port range	Source
IPv4	SSH	TCP	22	0.0.0.0/0
IPv6	SSH	TCP	22	::/0



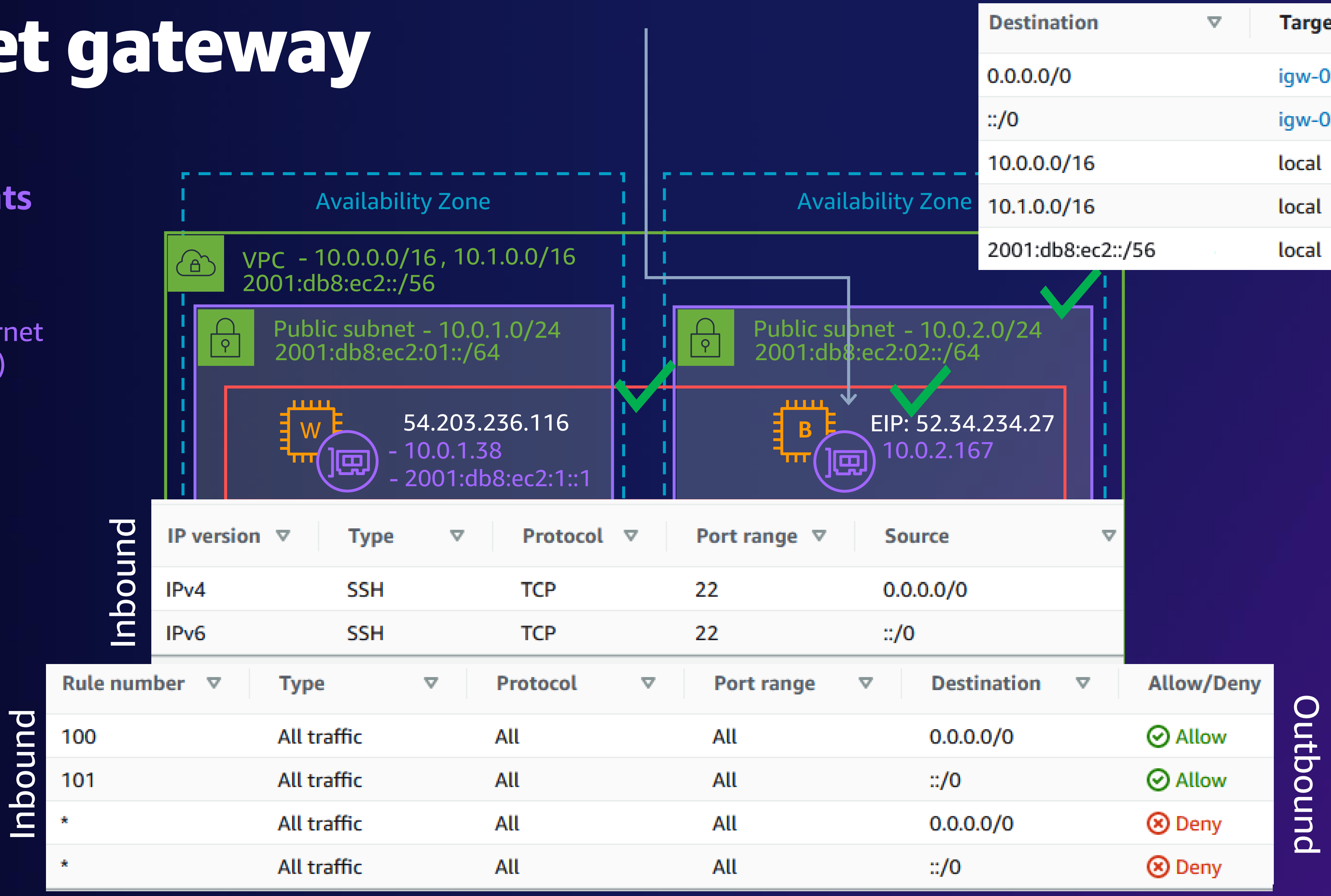
Internet gateway



Internet gateway

5 Requirements

1) Public IP
2) SGs allow
3) NACLs allow
4) Attached internet gateway (IGW)
5) Route to IGW



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

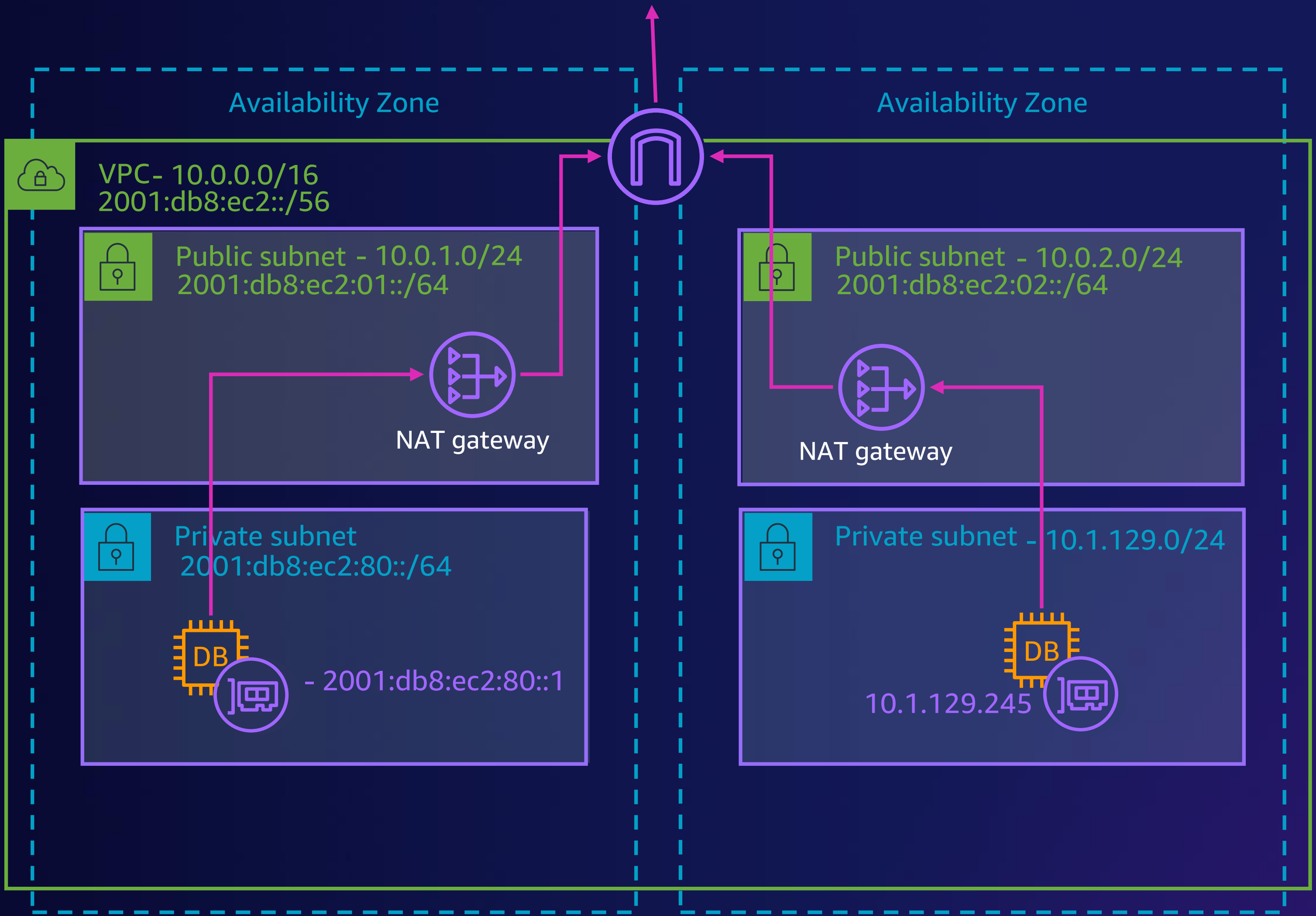
Inbound

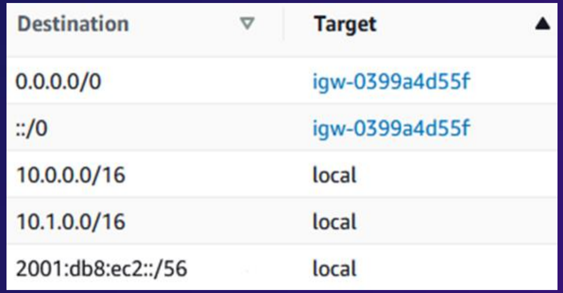
IP version	Type	Protocol	Port range	Source
IPv4	SSH	TCP	22	0.0.0.0/0
IPv6	SSH	TCP	22	::/0

Inbound / Outbound

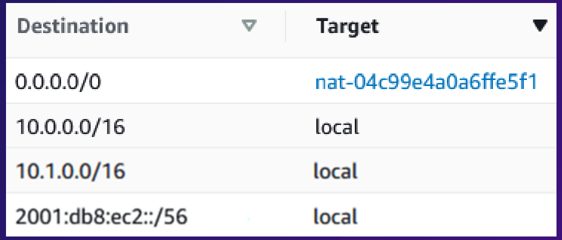
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
101	All traffic	All	All	::/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	☒ Deny
*	All traffic	All	All	::/0	☒ Deny

Connecting to the internet from private subnet



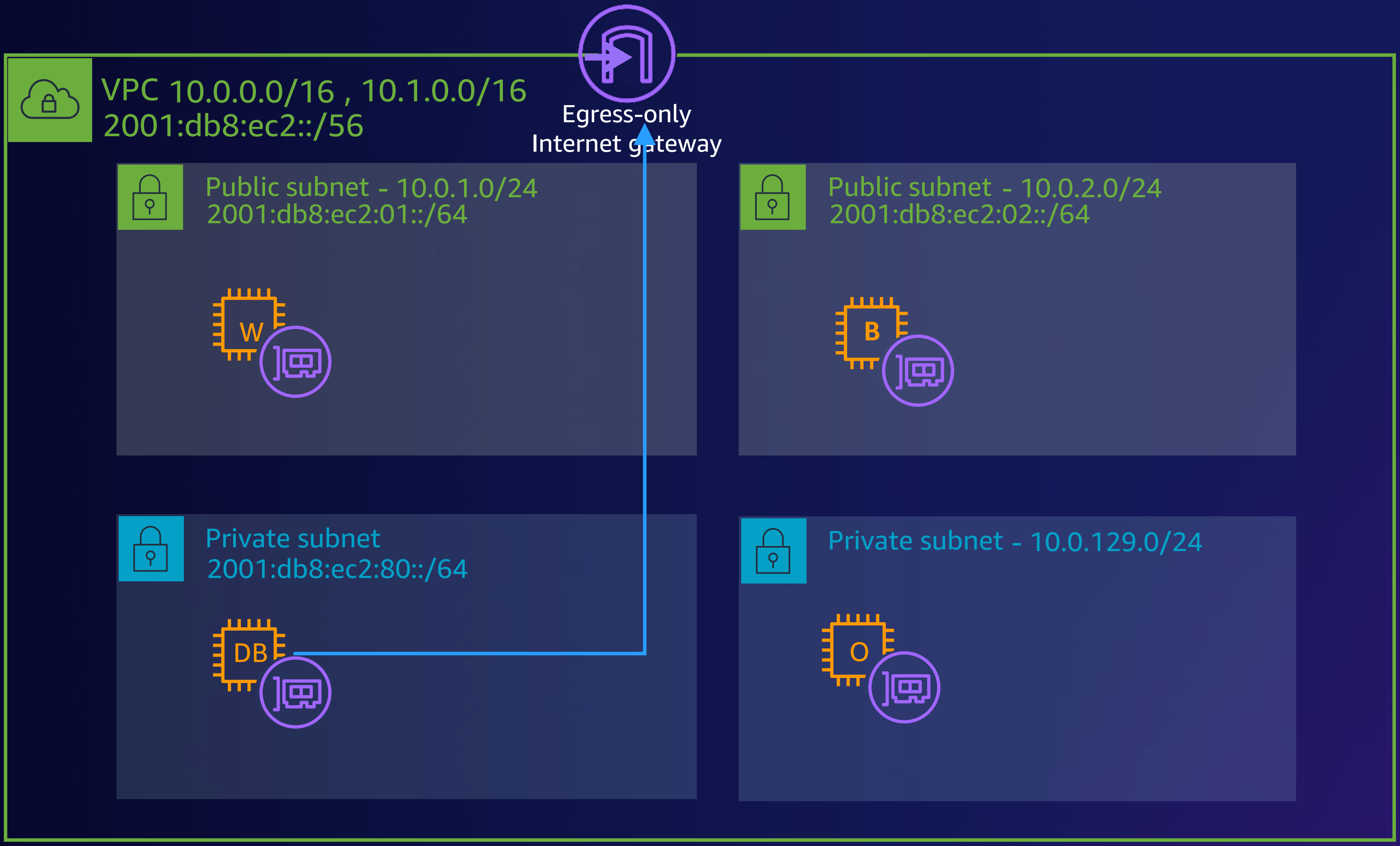


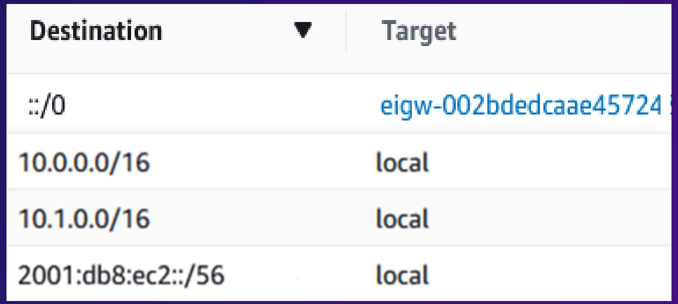
Destination	Target
0.0.0.0/0	igw-0399a4d55f
::/0	igw-0399a4d55f
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local



Destination	Target
0.0.0.0/0	nat-04c99e4a0a6ffe5f1
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local

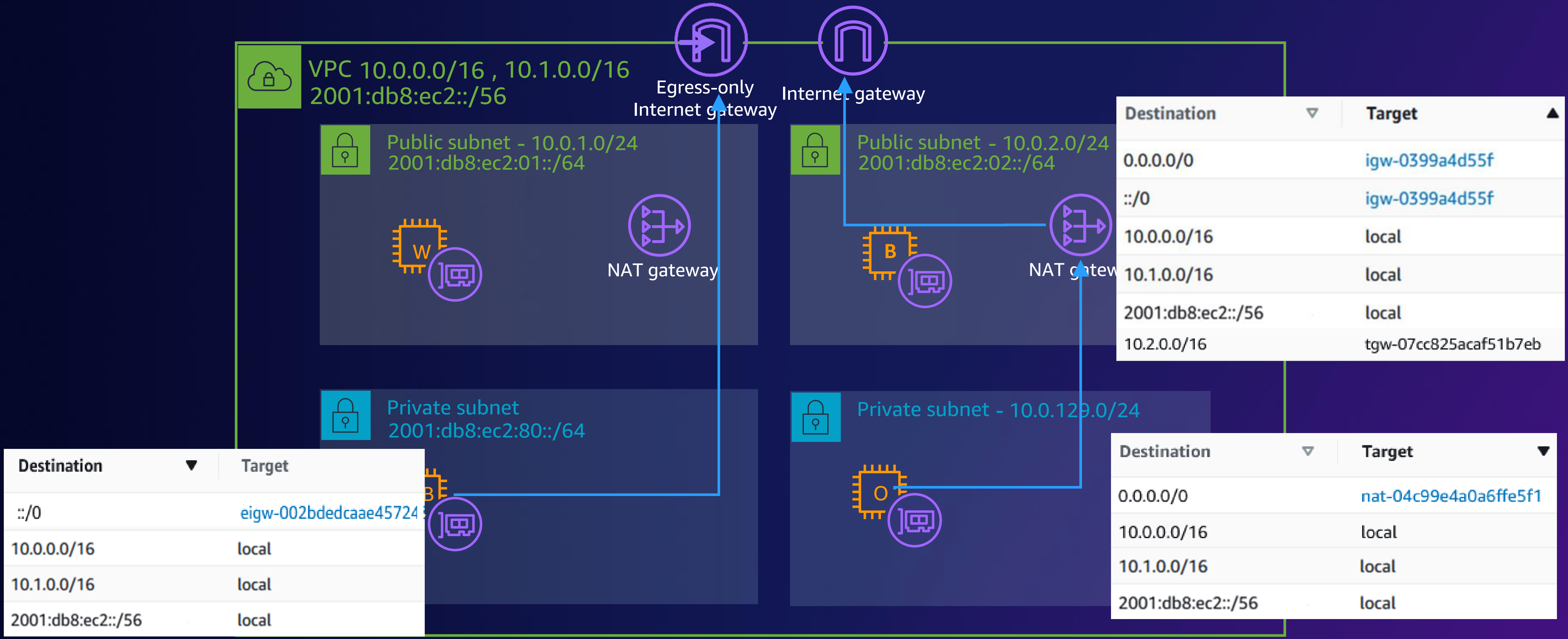
Connecting to the internet: IPv6





Destination ▼	Target
::/0	eigw-002bdedcaae45724
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local

Connecting to the internet

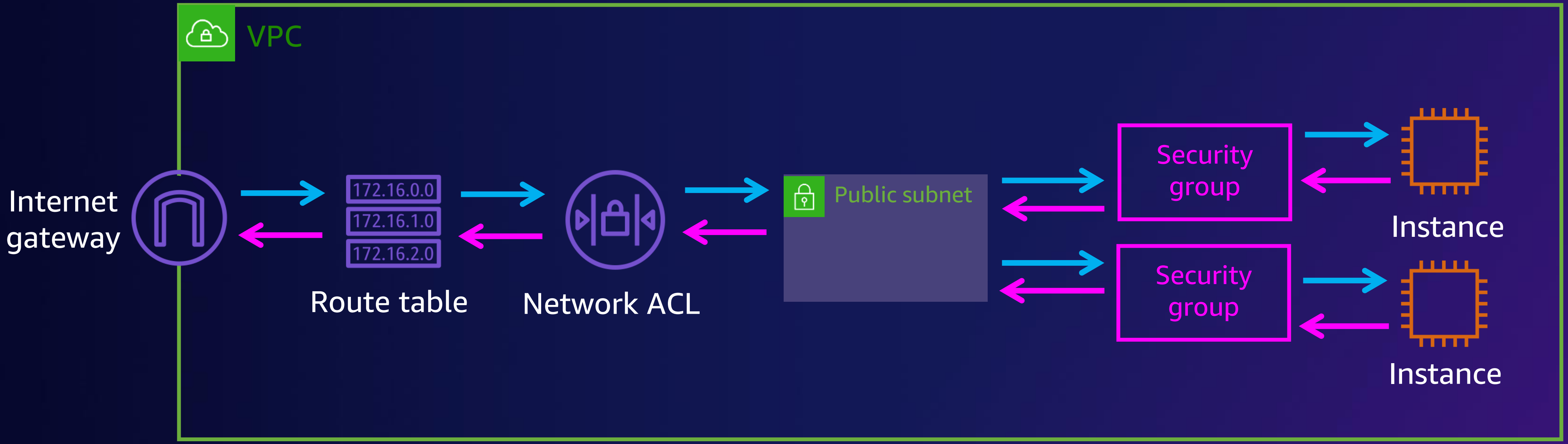


Destination	Target
0.0.0.0/0	igw-0399a4d55f
::/0	igw-0399a4d55f
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local
10.2.0.0/16	tgw-07cc825acaf51b7eb

Destination	Target
::/0	eigw-002bdedcaae45724
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local

Destination	Target
0.0.0.0/0	nat-04c99e4a0a6ffe5f1
10.0.0.0/16	local
10.1.0.0/16	local
2001:db8:ec2::/56	local

VPC defense in depth



Peering, endpoints, and gateways

Peering, endpoints, and gateways

AWS Client VPN endpoint

Virtual private gateway

Direct Connect gateway

NAT gateway

Internet gateway

AWS Transit Gateway

Endpoints

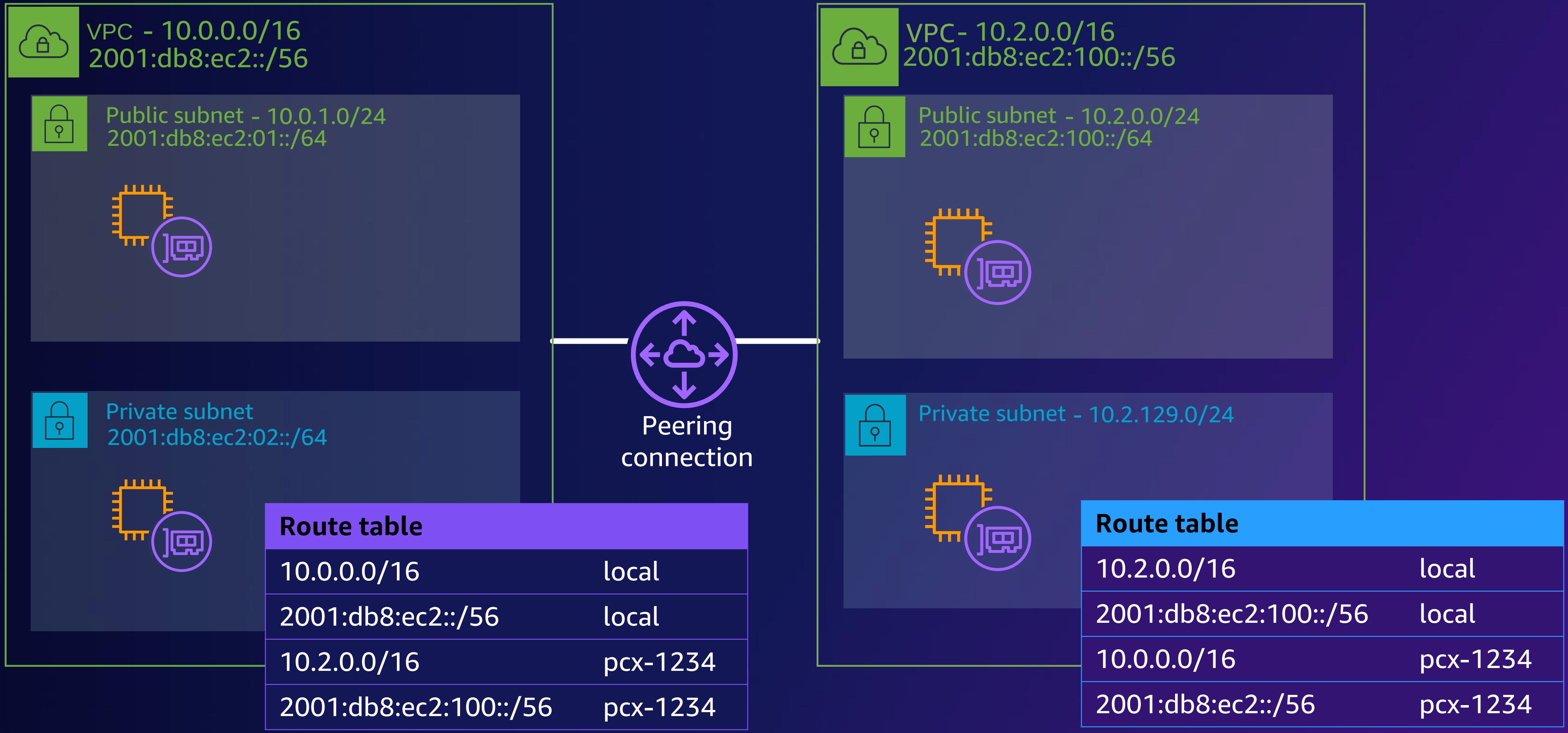
Peering connection

Connecting multiple VPC

VPC Peering

Transit Gateway

VPC Peering



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

Public subnet - 10.0.1.0/24
2001:db8:ec2:01::/64

Private subnet
2001:db8:ec2:02::/64

Peering connection

VPC- 10.2.0.0/16
2001:db8:ec2:100::/56

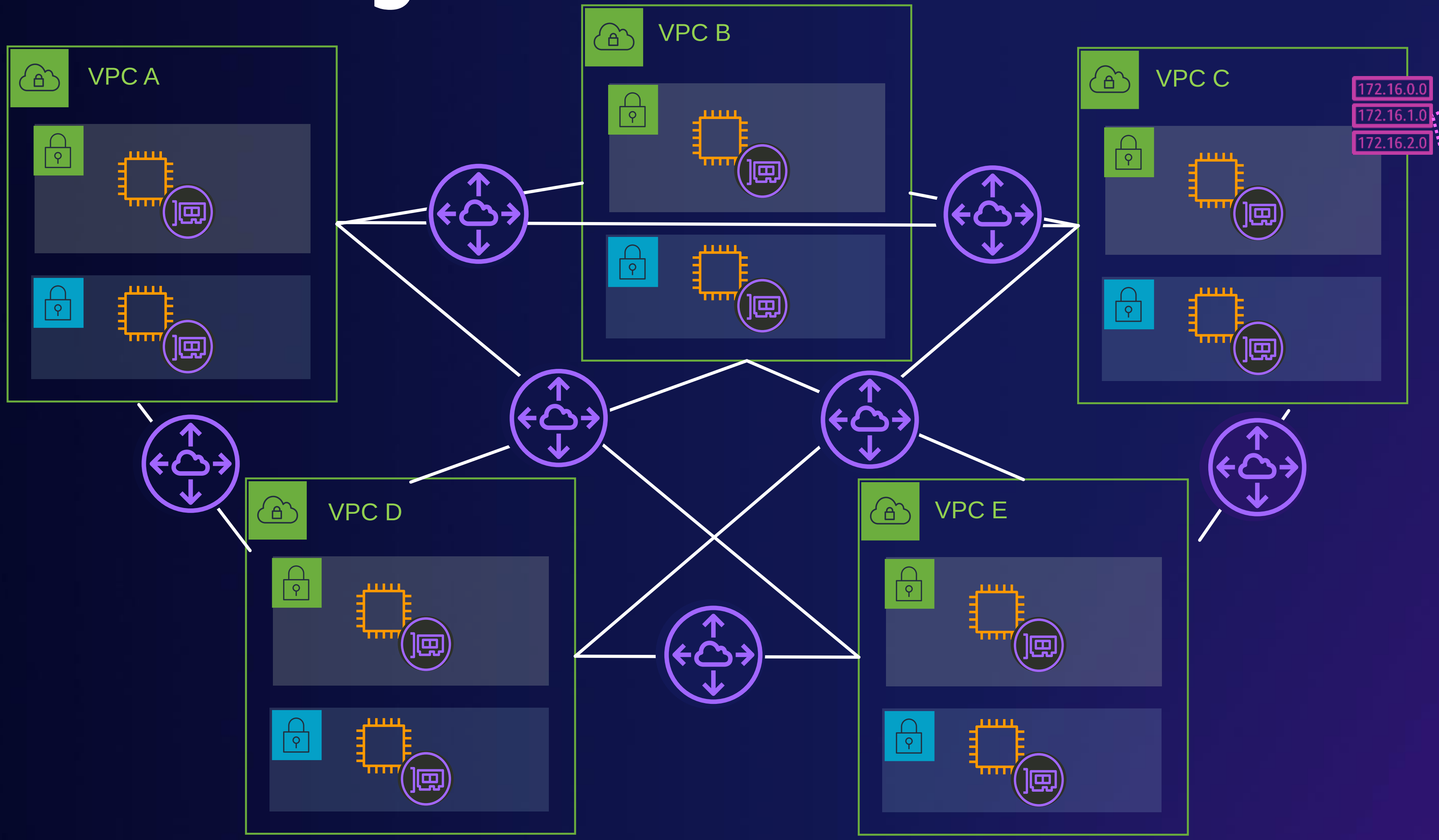
Public subnet - 10.2.0.0/24
2001:db8:ec2:100::/64

Private subnet - 10.2.129.0/24

Route table	
10.0.0.0/16	local
2001:db8:ec2::/56	local
10.2.0.0/16	pcx-1234
2001:db8:ec2:100::/56	pcx-1234

Route table	
10.2.0.0/16	local
2001:db8:ec2:100::/56	local
10.0.0.0/16	pcx-1234
2001:db8:ec2::/56	pcx-1234

VPC Peering



Destination	Target
C	Local
A	PCX-1
B	PCX-2
D	PCX-3
E	PCX-4

Number of peering connections for a full mesh:

$$\frac{n(n-1)}{2}$$

What is the problem?

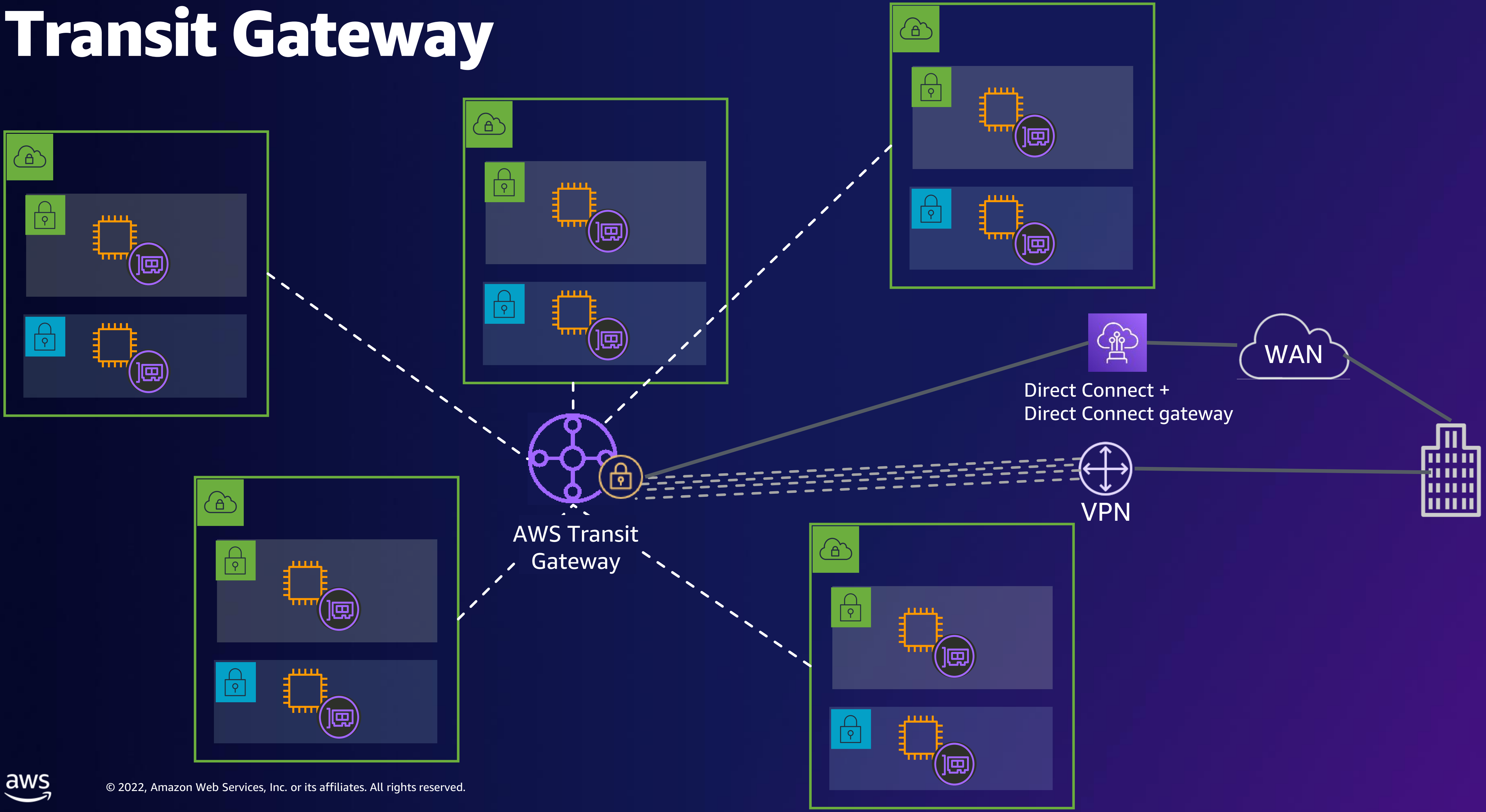
Complexity:

$$\frac{100\ (100 - 1)}{2} = 4{,}950$$

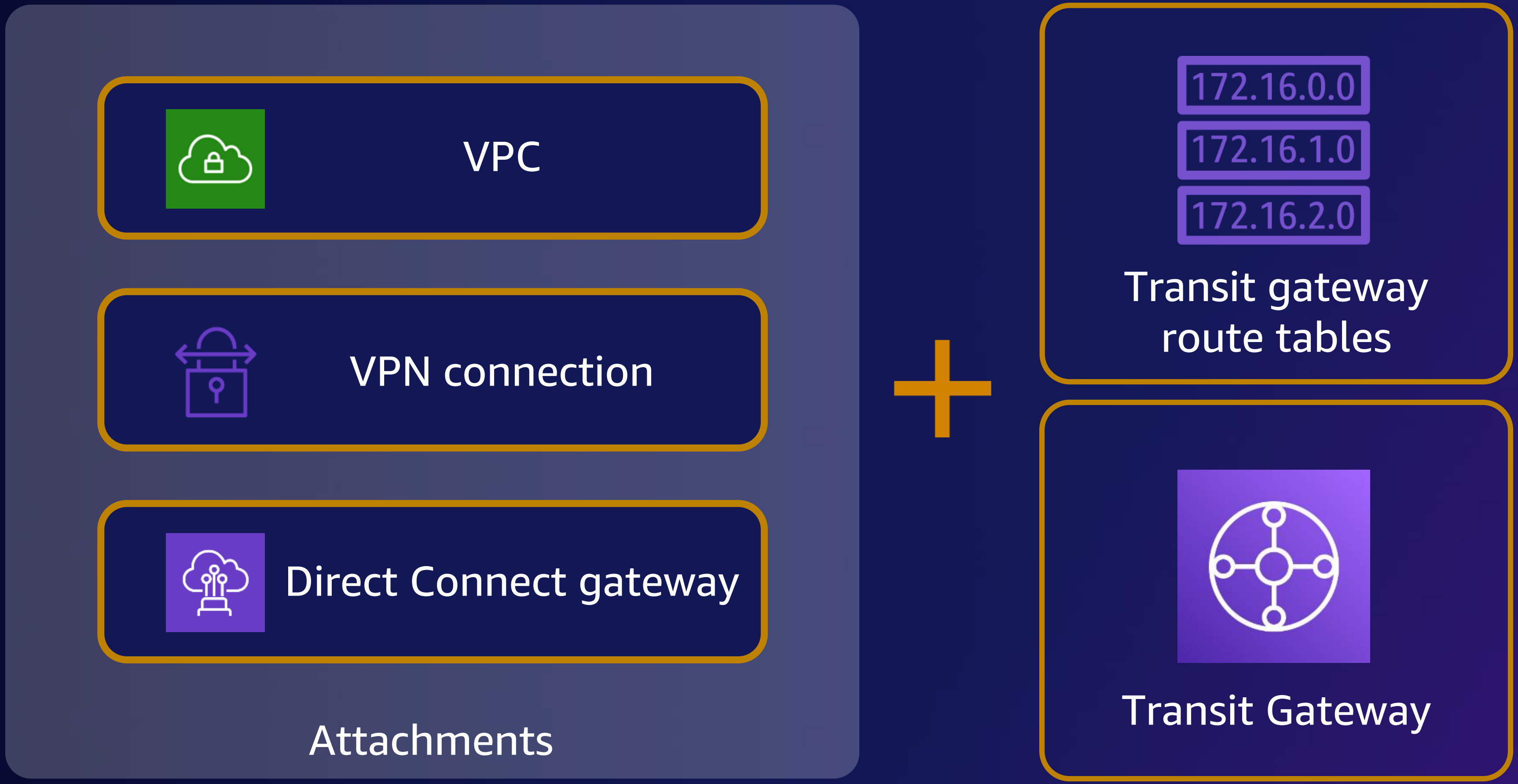
Service Limit:

Amazon VPC peering connections per Amazon VPC = 125

Transit Gateway



Transit Gateway component



VPC

VPN connection

Direct Connect gateway

Attachments

+

172.16.0.0

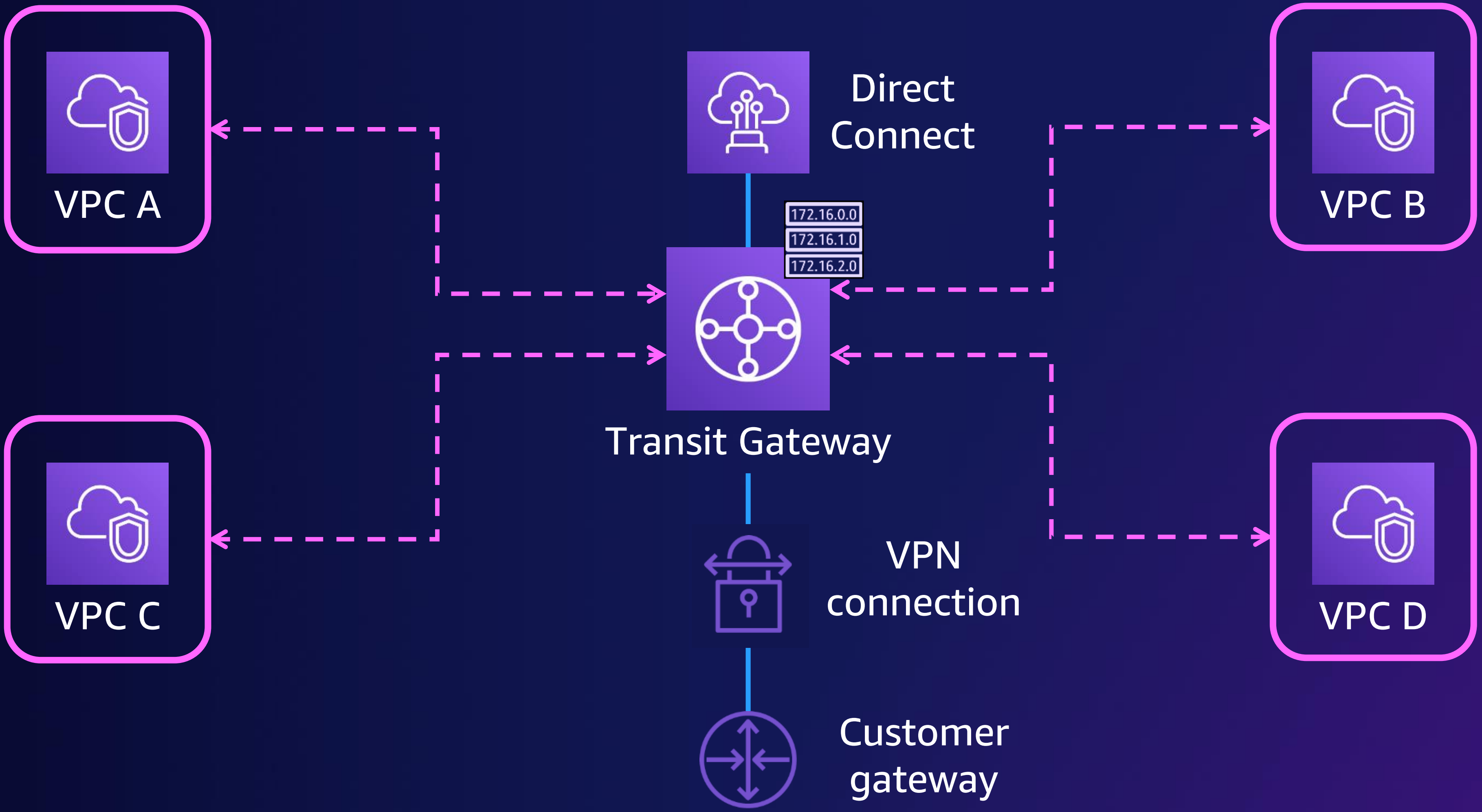
172.16.1.0

172.16.2.0

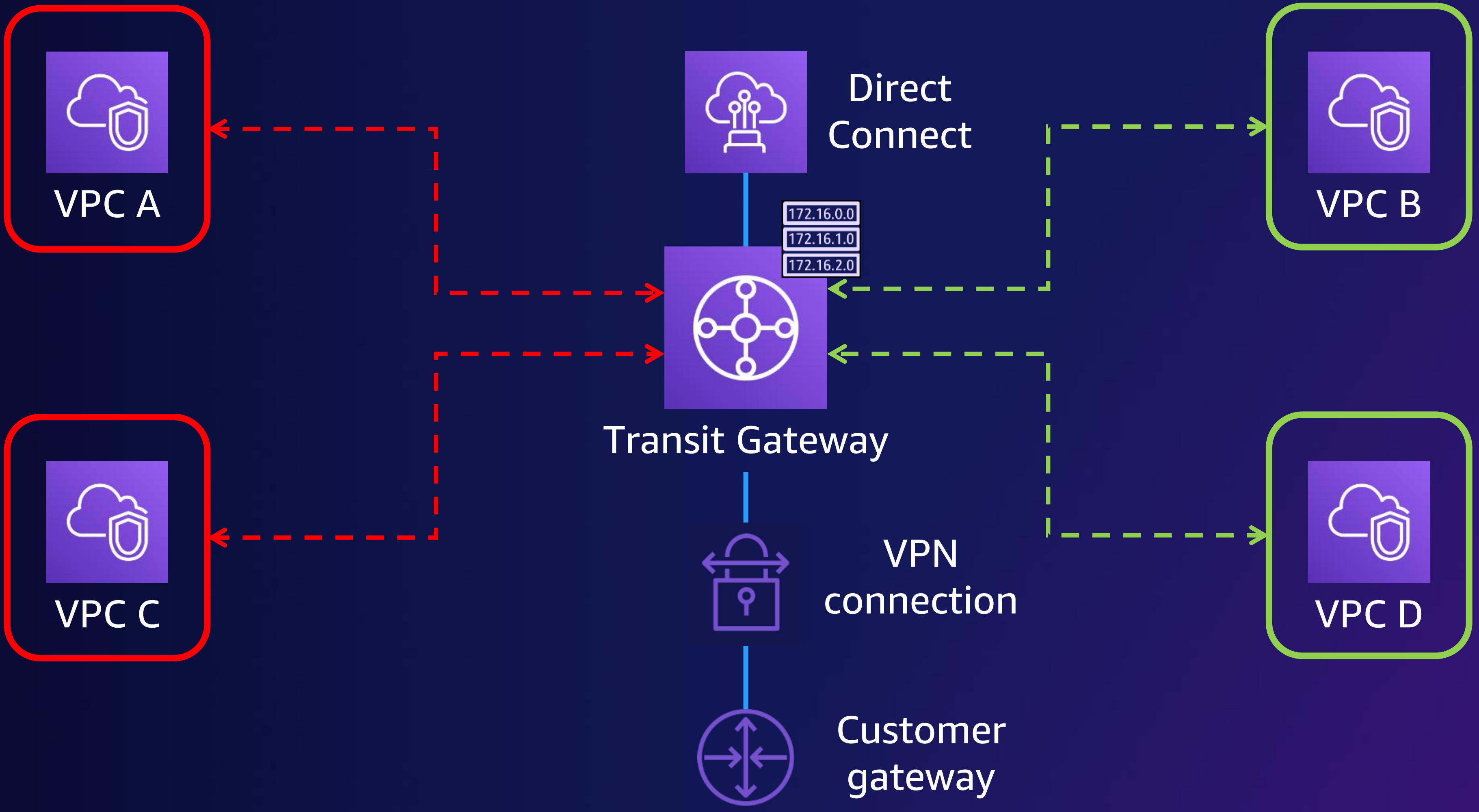
Transit gateway route tables

Transit Gateway

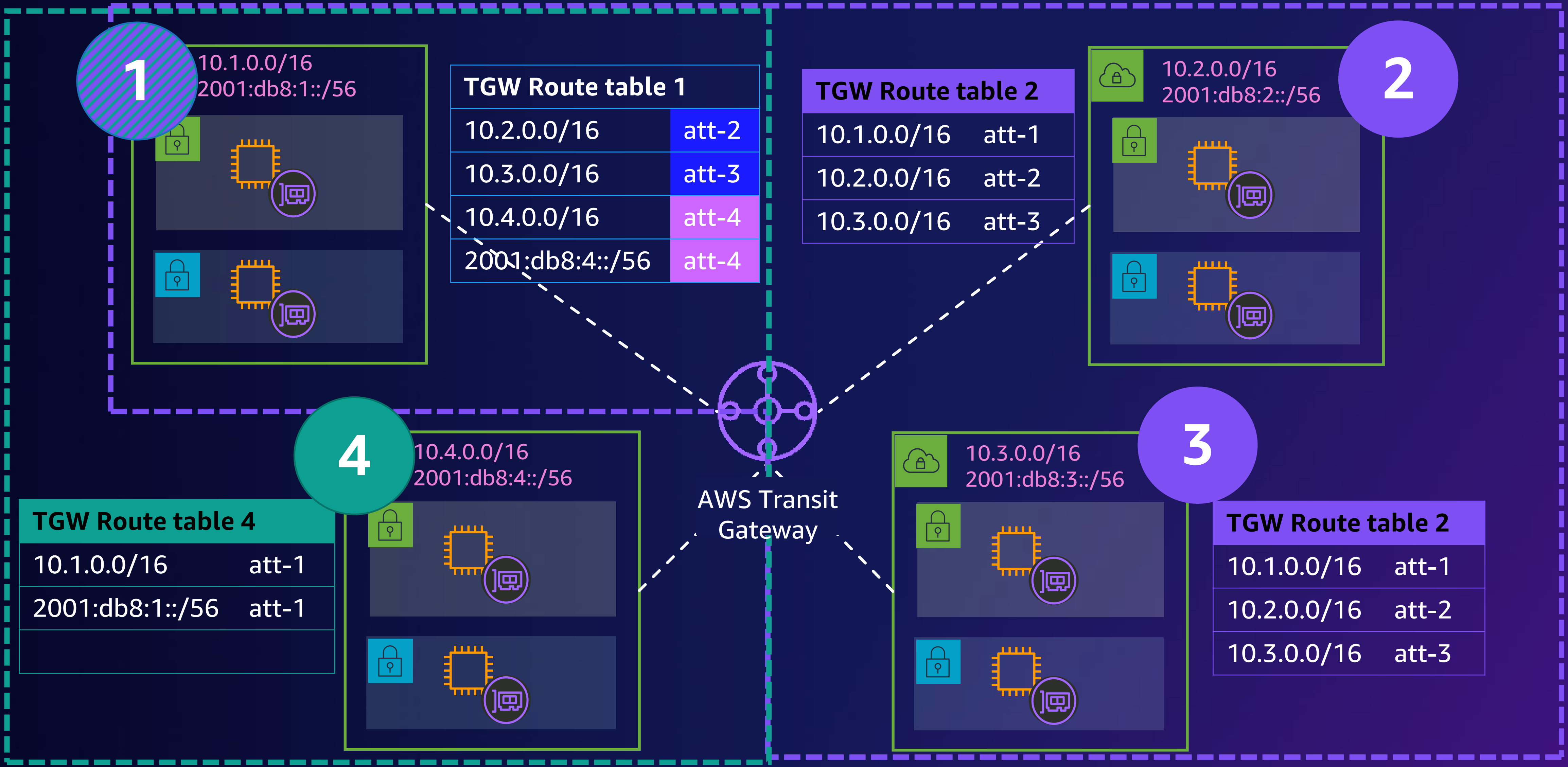
Full Connectivity



Partial connectivity



Transit Gateway route tables and domains



1

10.1.0.0/16
2001:db8:1::/56

TGW Route table 1	
10.2.0.0/16	att-2
10.3.0.0/16	att-3
10.4.0.0/16	att-4
2001:db8:4::/56	att-4

TGW Route table 2	
10.1.0.0/16	att-1
10.2.0.0/16	att-2
10.3.0.0/16	att-3

2

10.2.0.0/16
2001:db8:2::/56

AWS Transit Gateway

4

10.4.0.0/16
2001:db8:4::/56

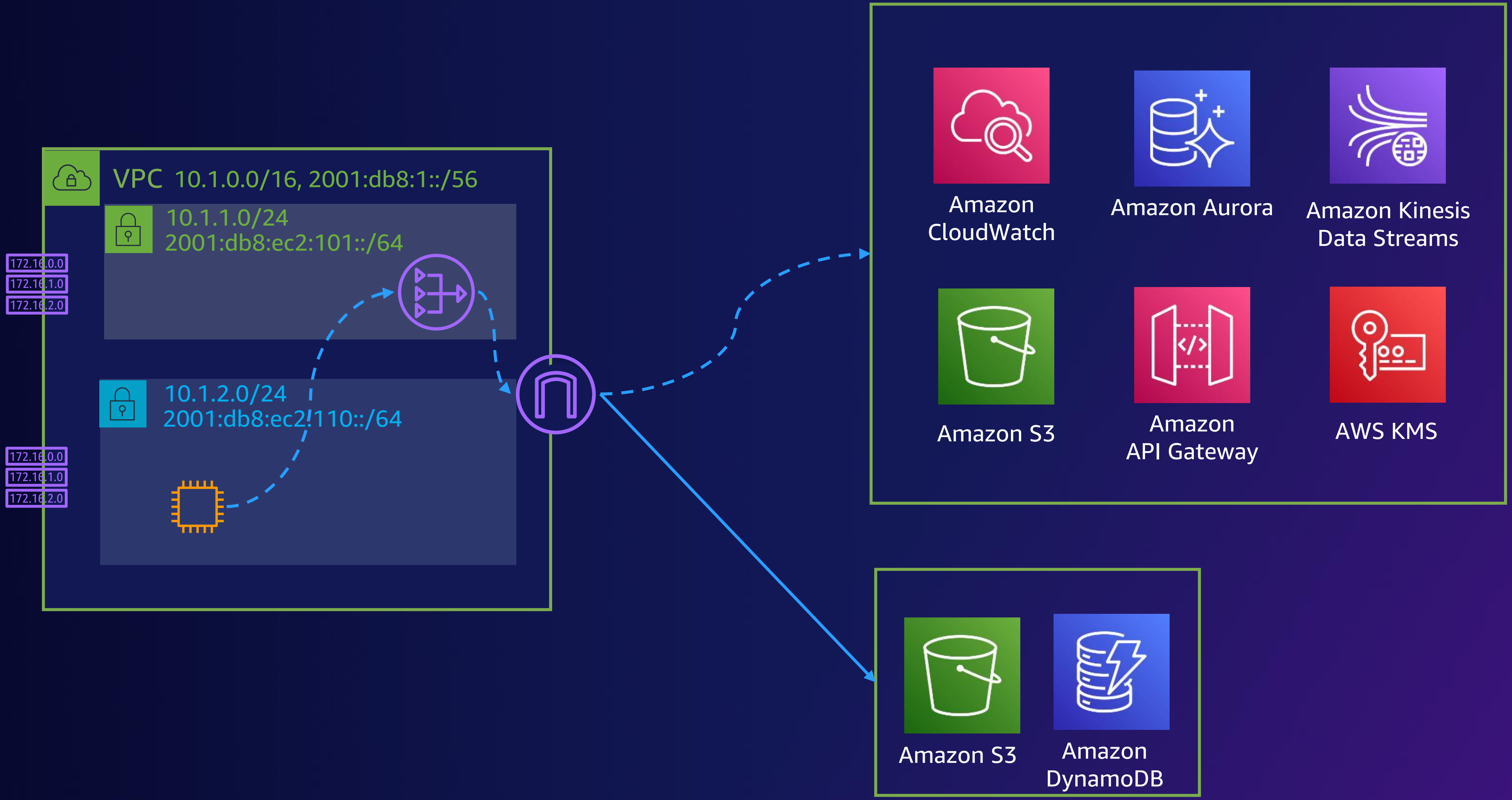
TGW Route table 4	
10.1.0.0/16	att-1
2001:db8:1::/56	att-1

3

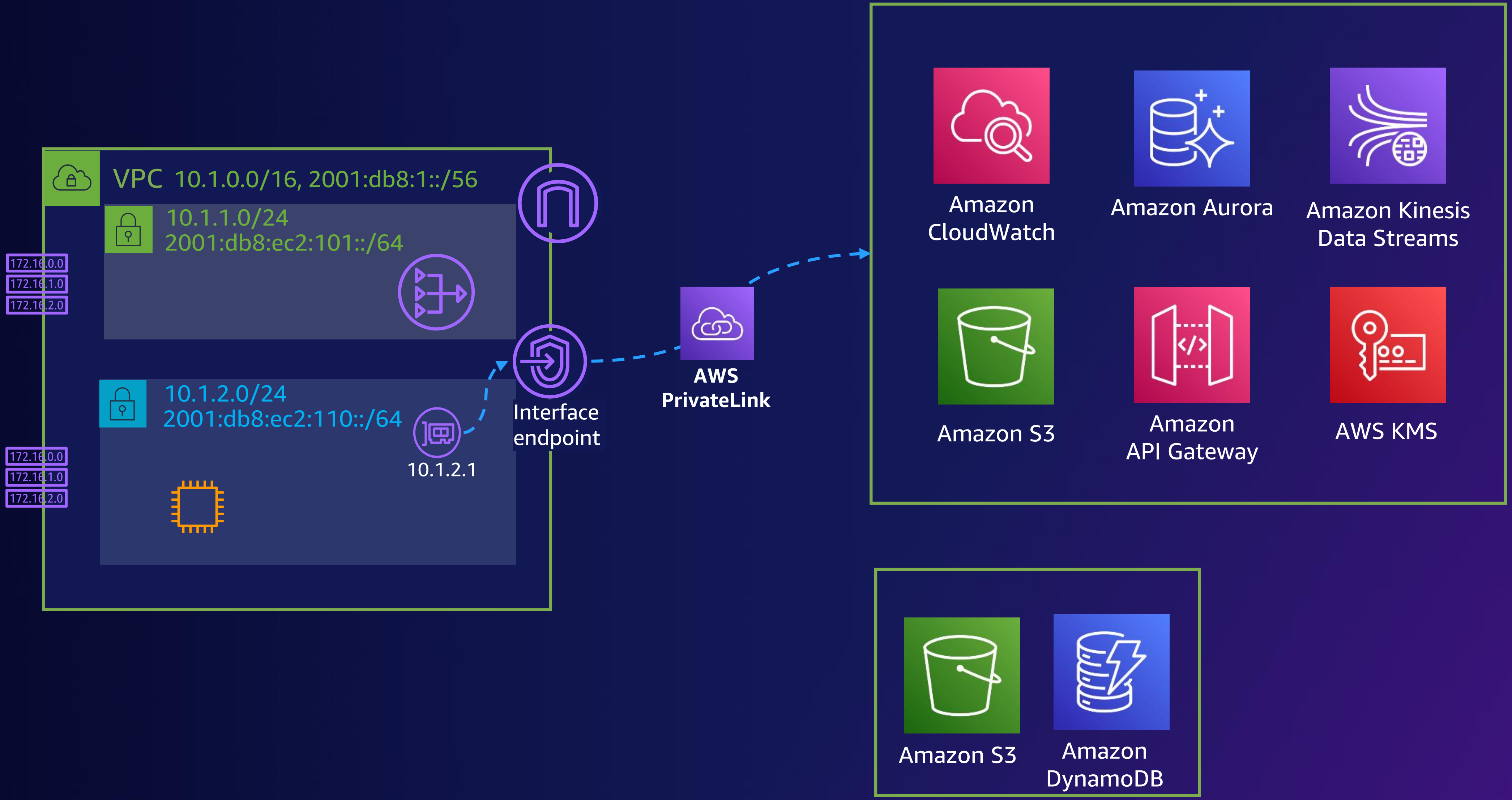
10.3.0.0/16
2001:db8:3::/56

TGW Route table 2	
10.1.0.0/16	att-1
10.2.0.0/16	att-2
10.3.0.0/16	att-3

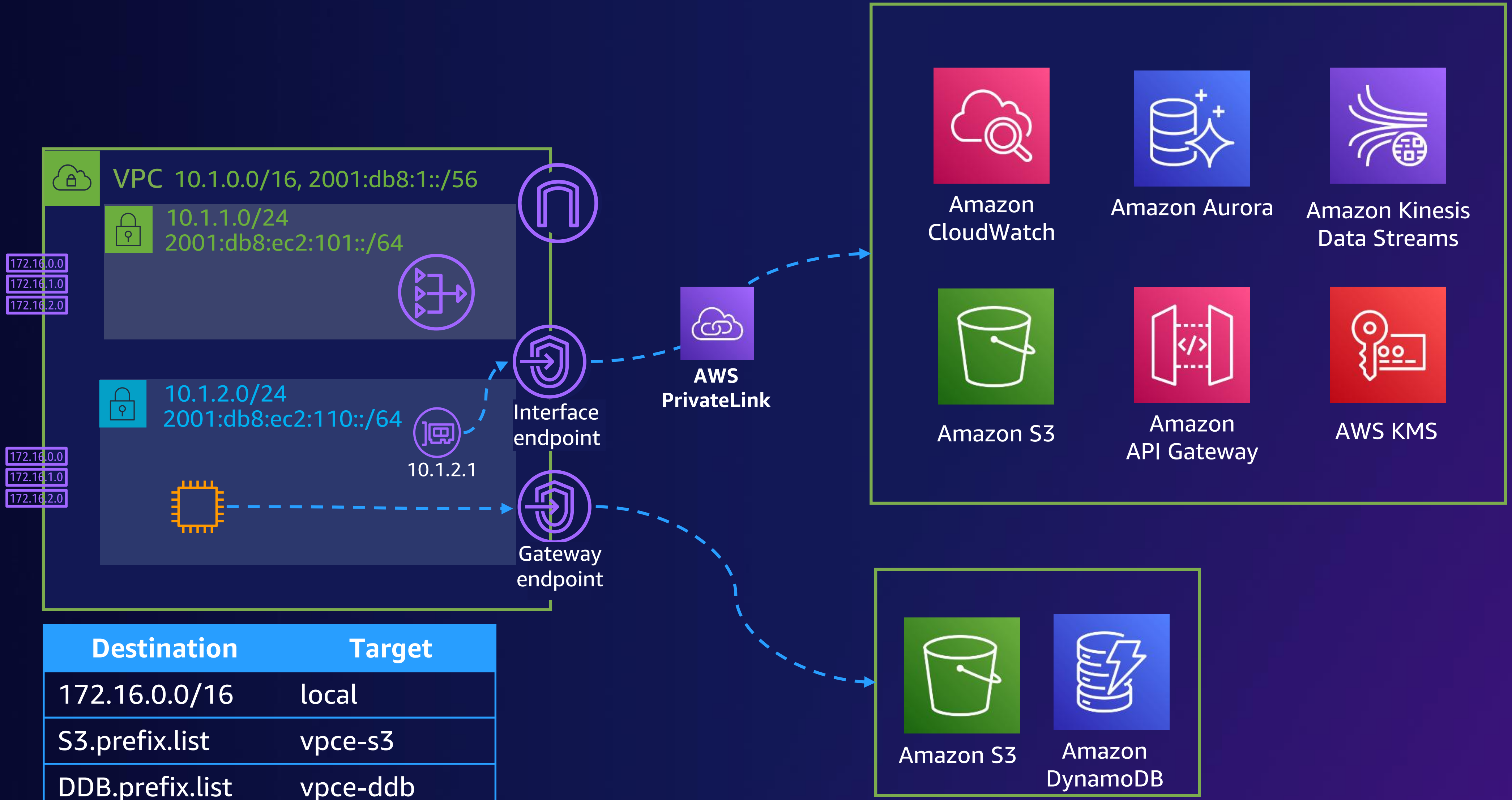
Without VPC endpoints



With VPC endpoints: Interface endpoints

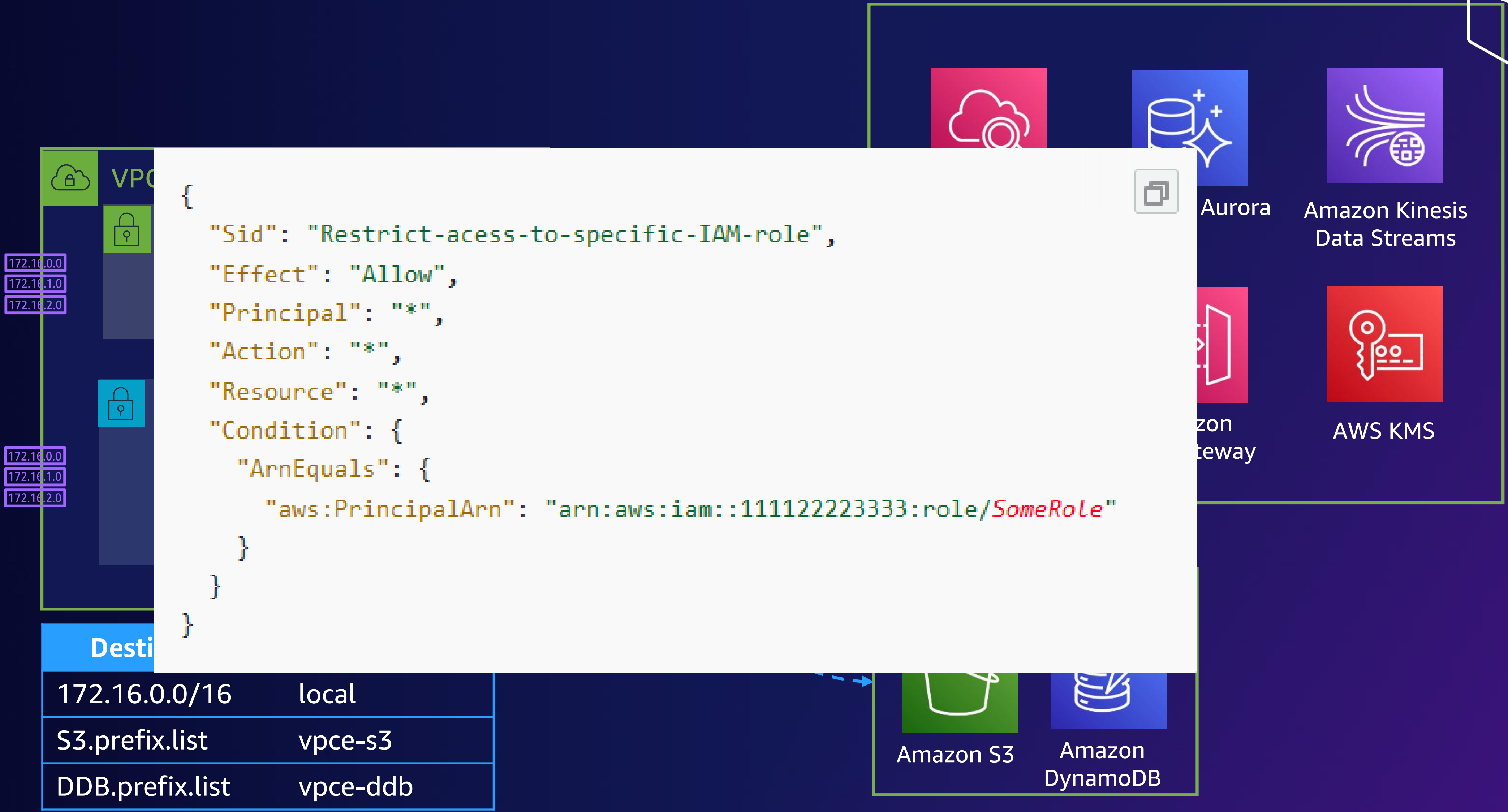


With VPC endpoints: Gateway endpoints



Destination	Target
172.16.0.0/16	local
S3.prefix.list	vpce-s3
DDB.prefix.list	vpce-ddb

With VPC endpoints: gateway endpoints



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

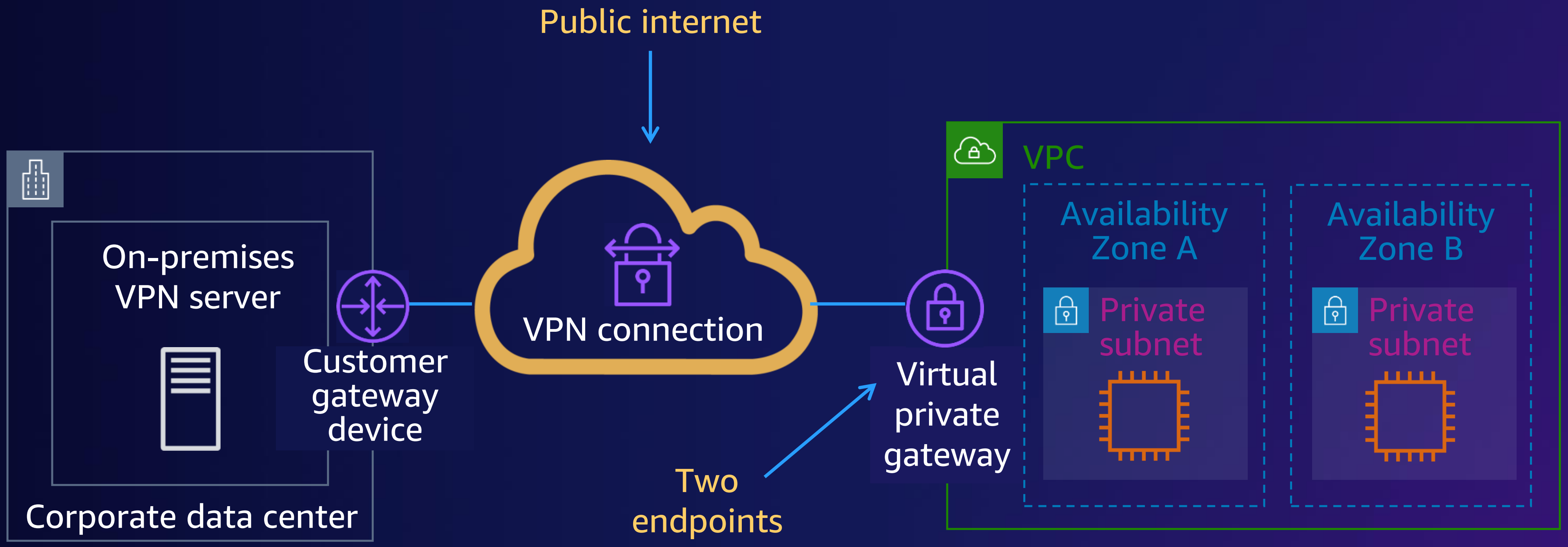
Desti	
172.16.0.0/16	local
S3.prefix.list	vpce-s3
DDB.prefix.list	vpce-ddb

Hybrid connectivity and gateways

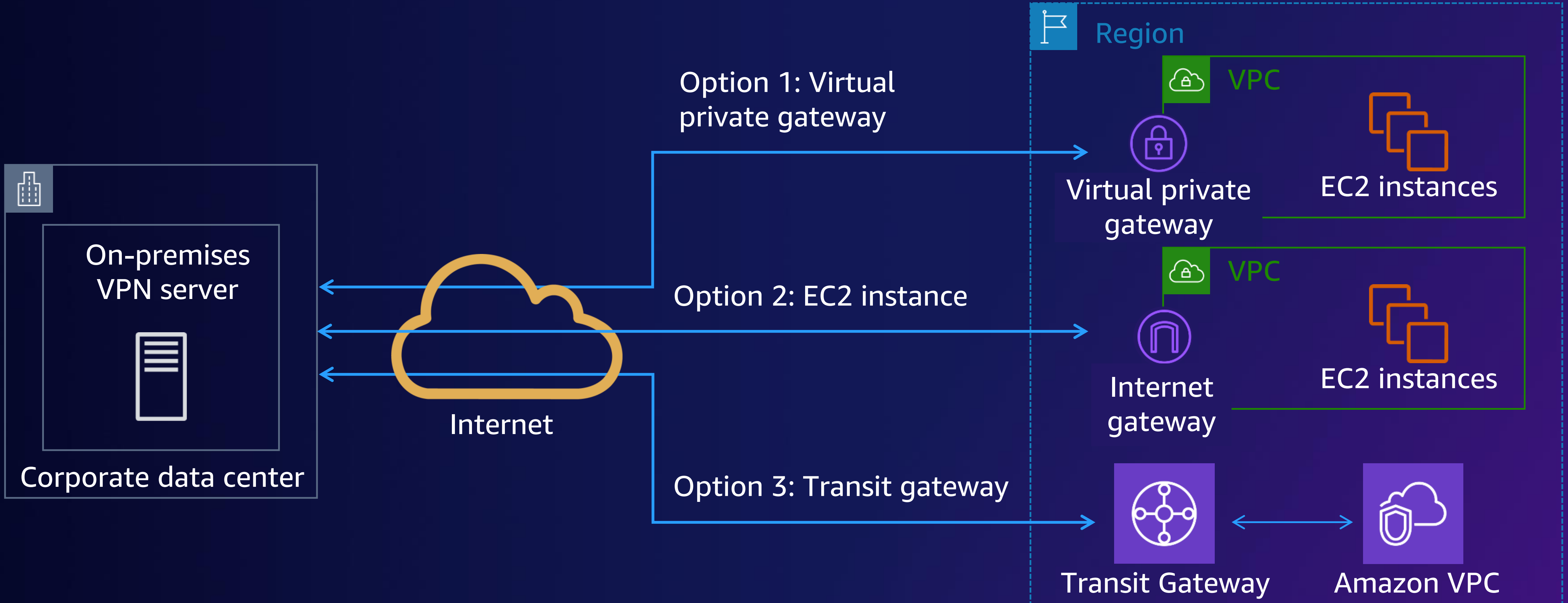
AWS Site-to-Site VPN

AWS Direct Connect

AWS Site-to-Site VPN



AWS Site-to-Site VPN

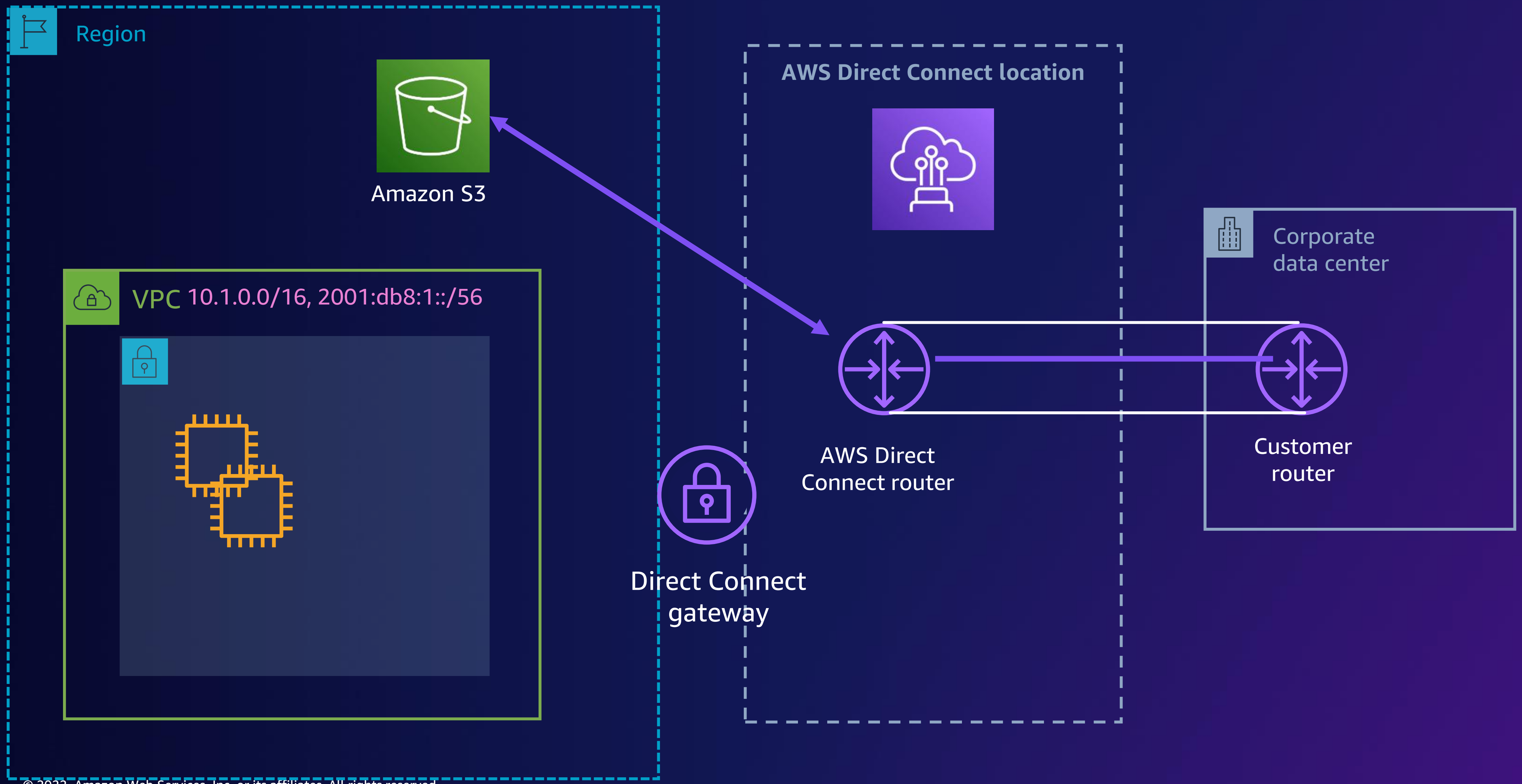


Option 1: Virtual private gateway

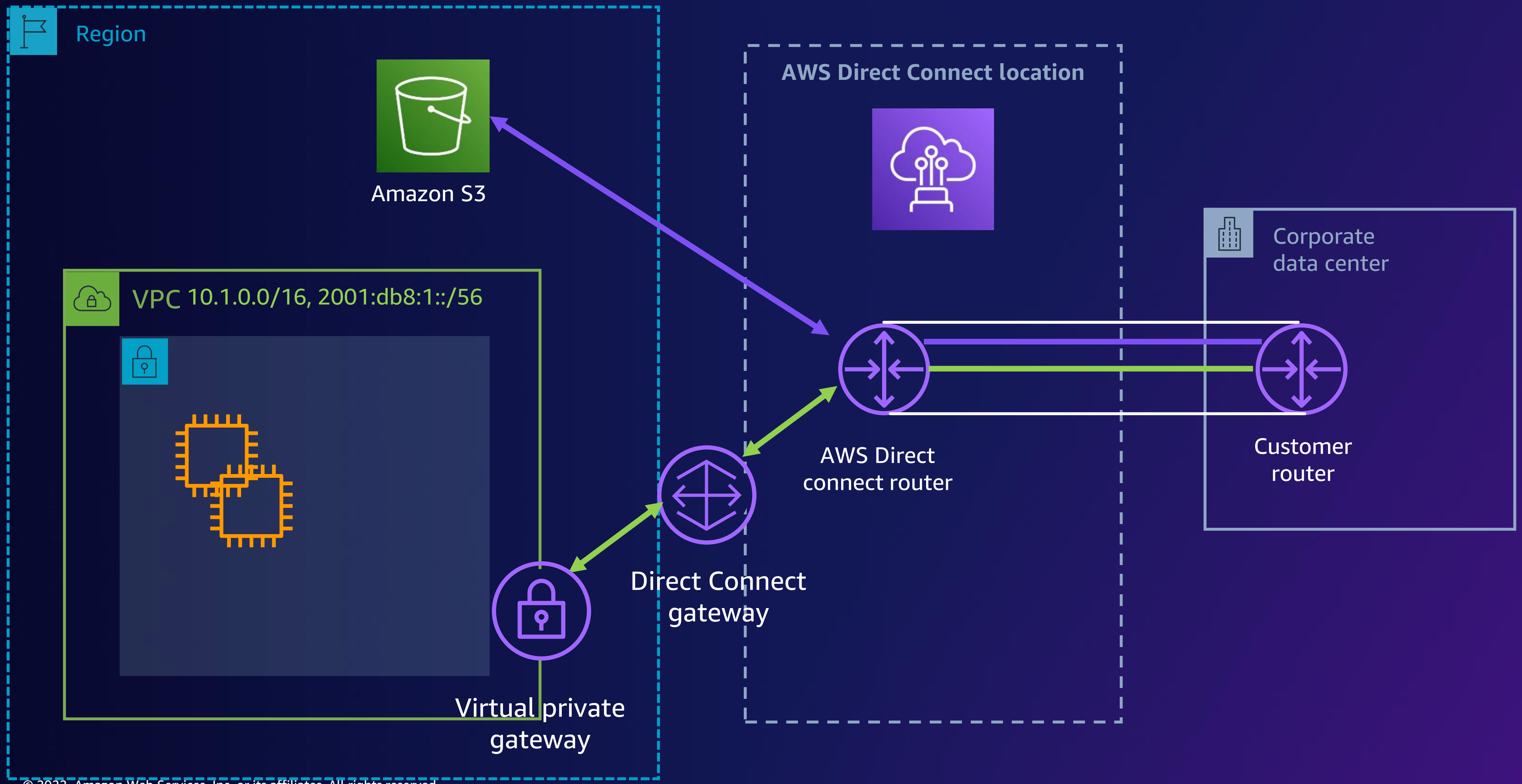
Option 2: EC2 instance

Option 3: Transit gateway

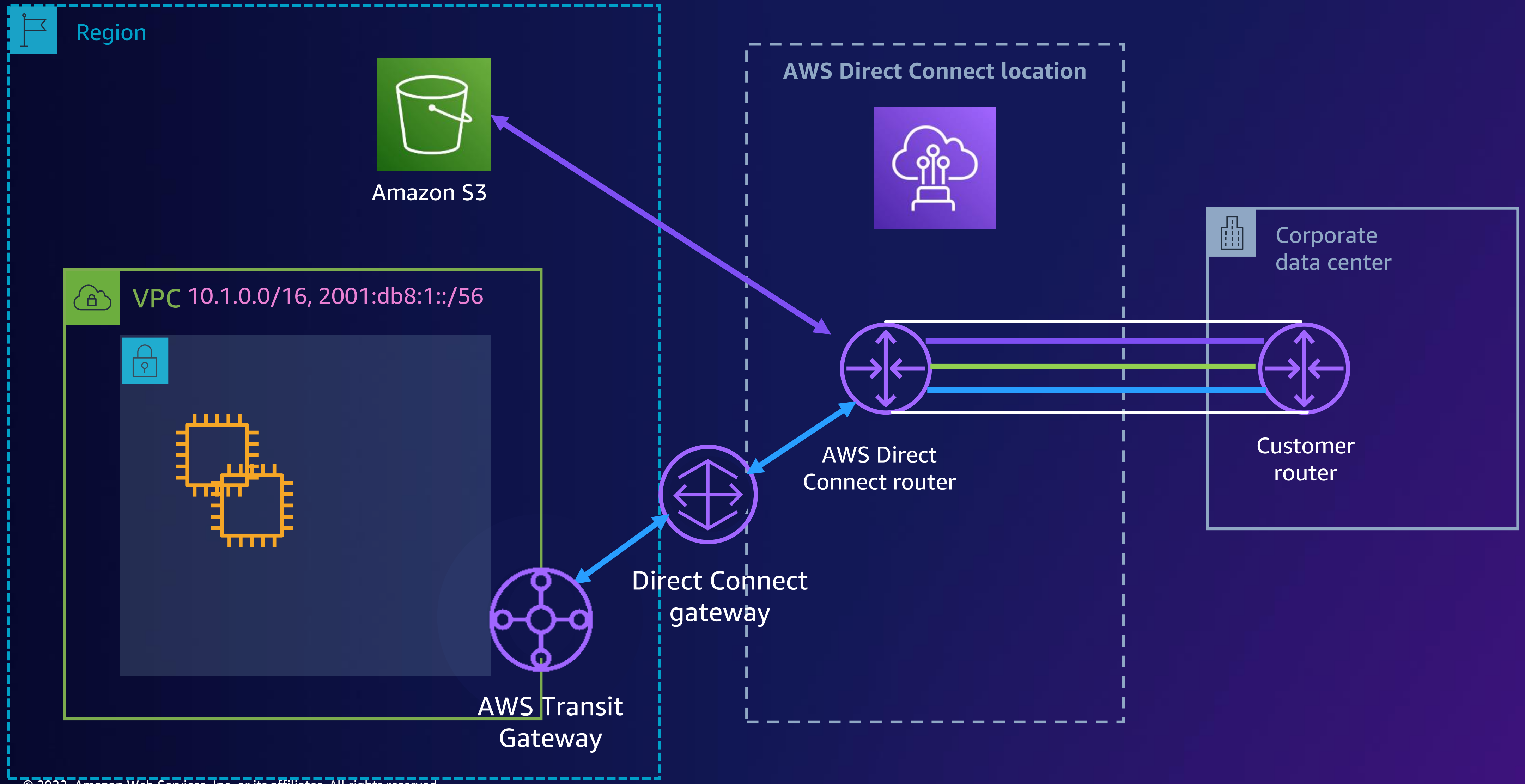
AWS Direct Connect


Region
Amazon S3
VPC 10.1.0.0/16, 2001:db8:1::/56
AWS Direct Connect location
Corporate data center
AWS Direct Connect router
Customer router
Direct Connect gateway

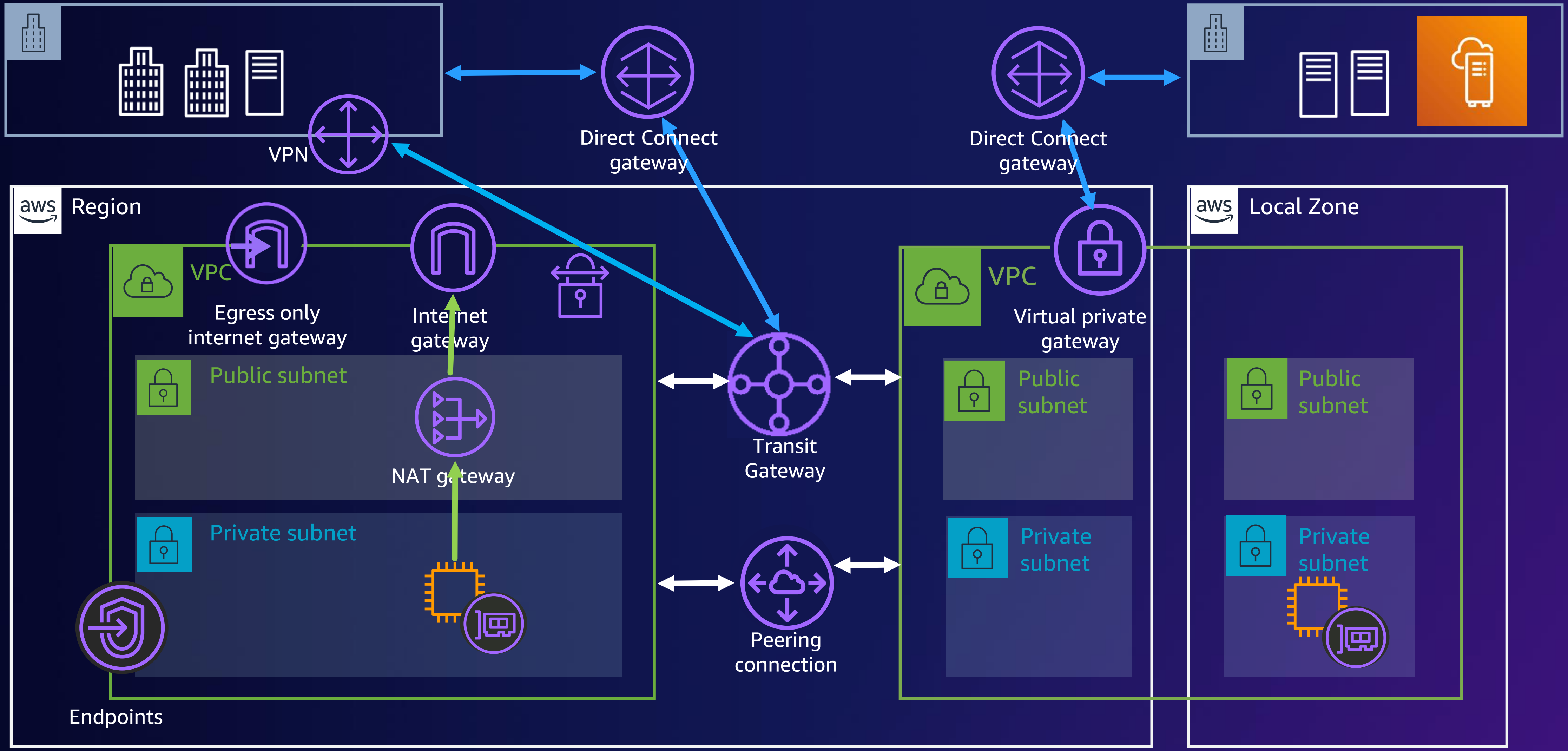
AWS Direct Connect



AWS Direct Connect



Bringing it all together



Learn in-demand AWS Cloud skills

AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

Thank you!

Laura Verghote

LinkedIn:
laura-verghote-6abb27155

Please complete the session survey