Networking in AWS

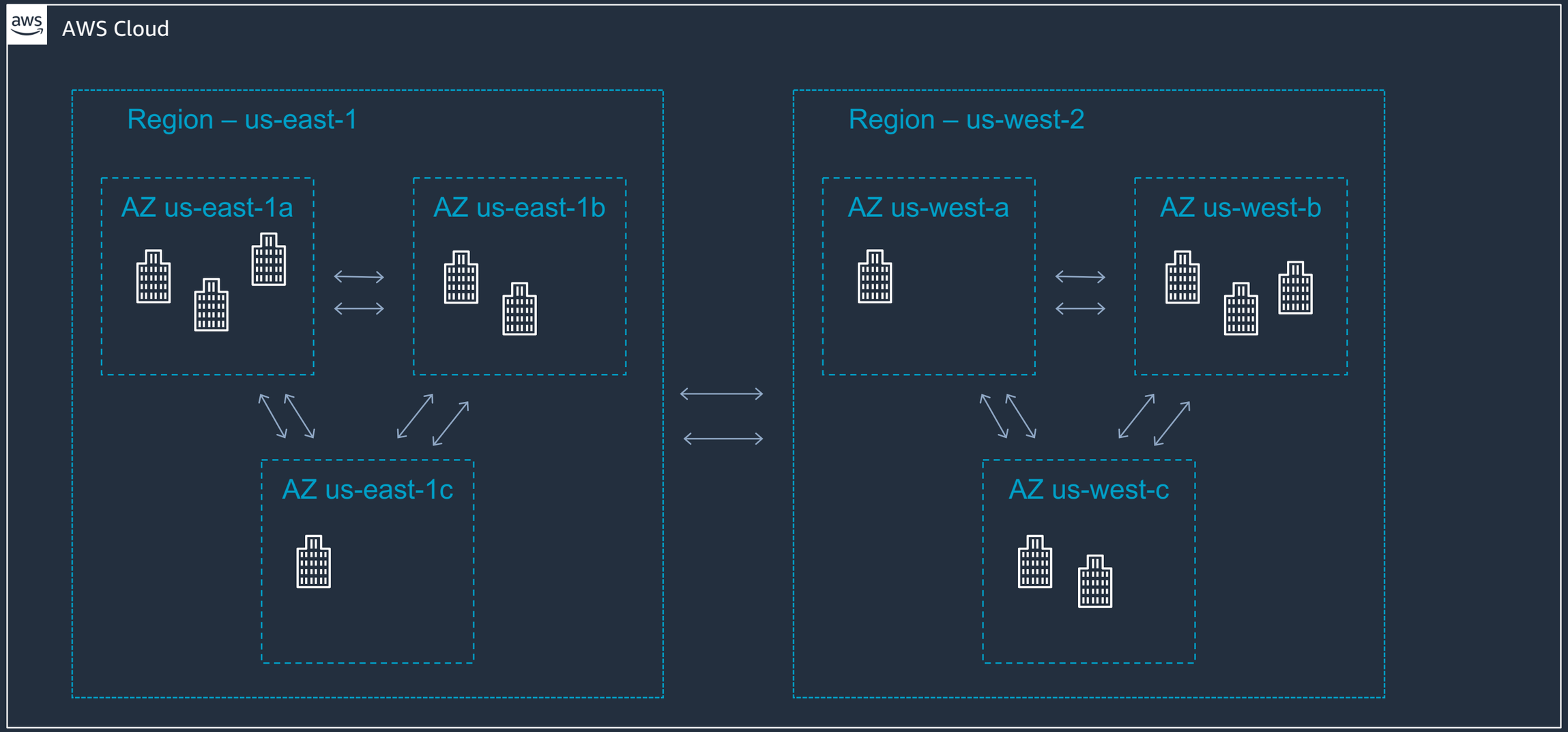
November 19, 2021

Michelangelo Markus
Solutions Architect - WWPS
markumi@amazon.com

Table of contents

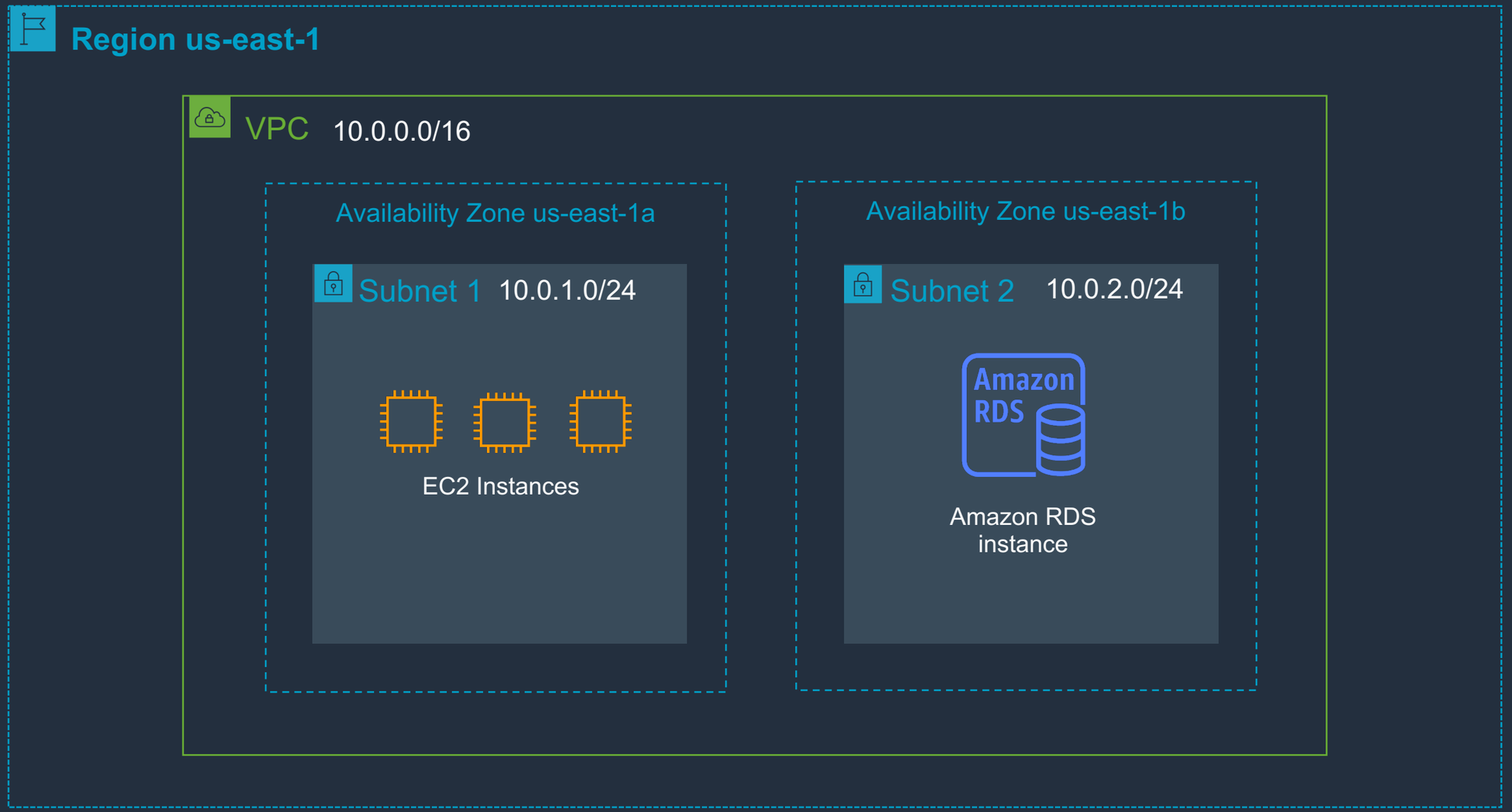
aws

Regions and Availability Zones (AZs)

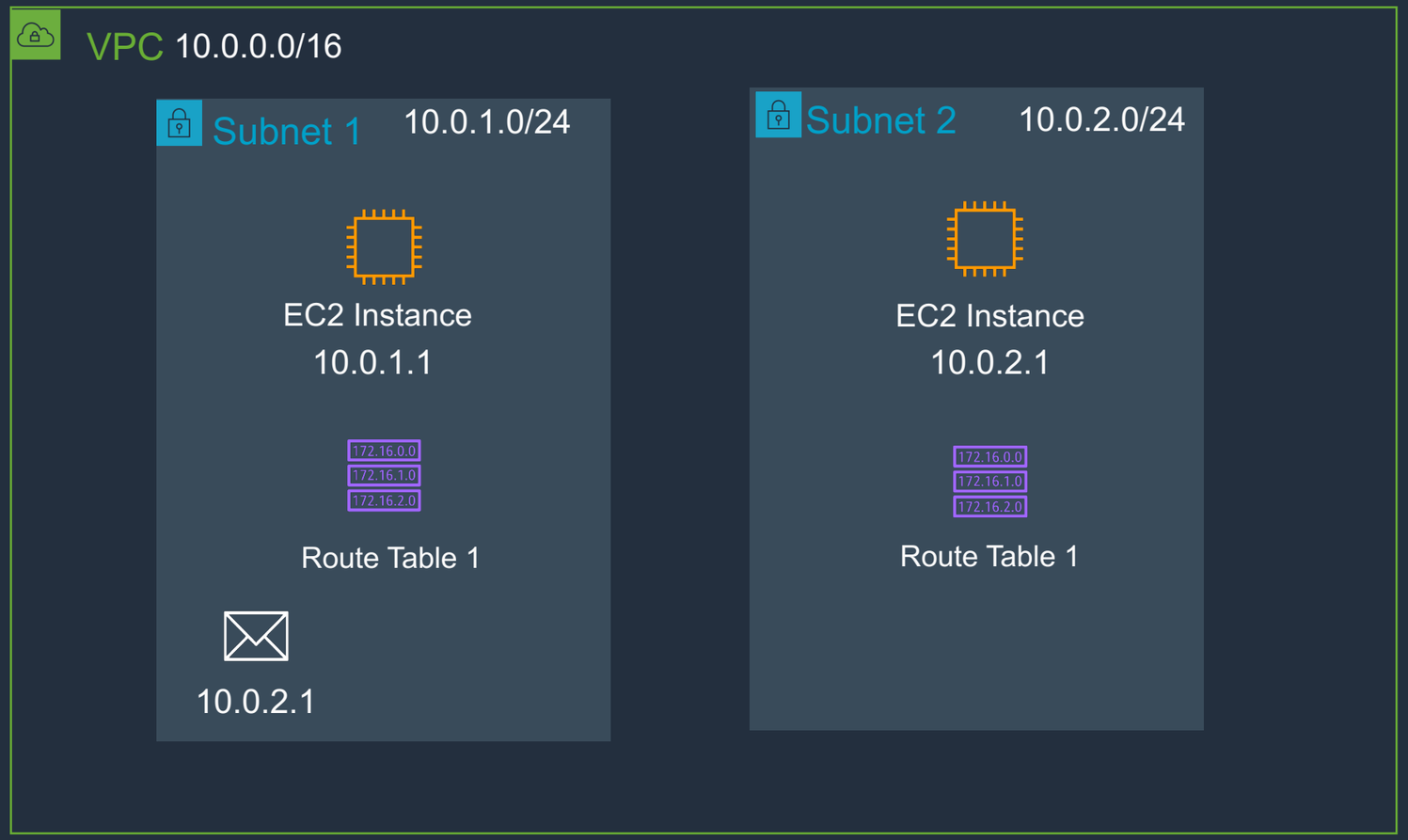


AWS VPC - Overview

Subnets and AZs



Route Tables – Internal VPC Traffic

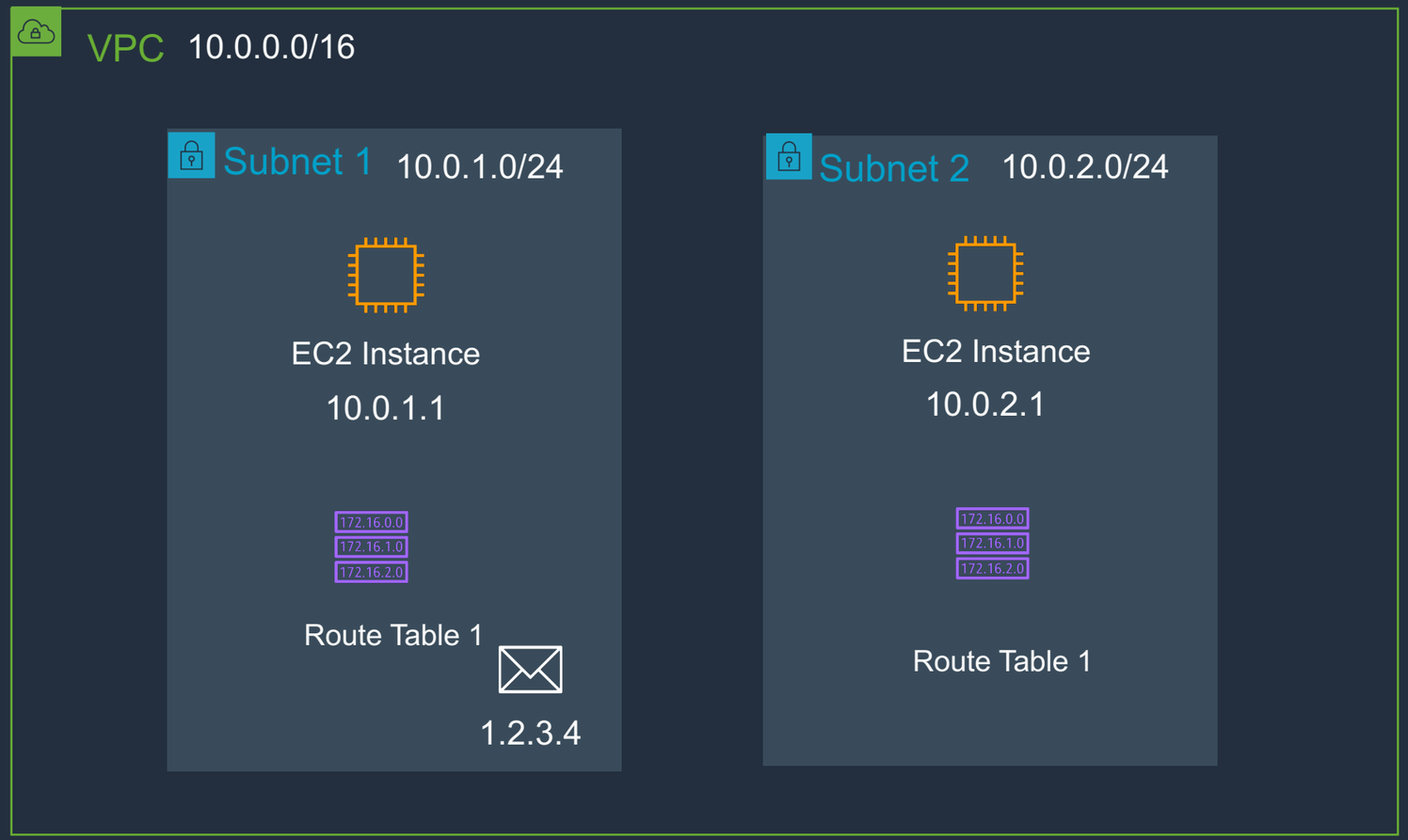


Route Table 1 - Rules

Destination	Target
10.0.0.0/16	*local*

aws

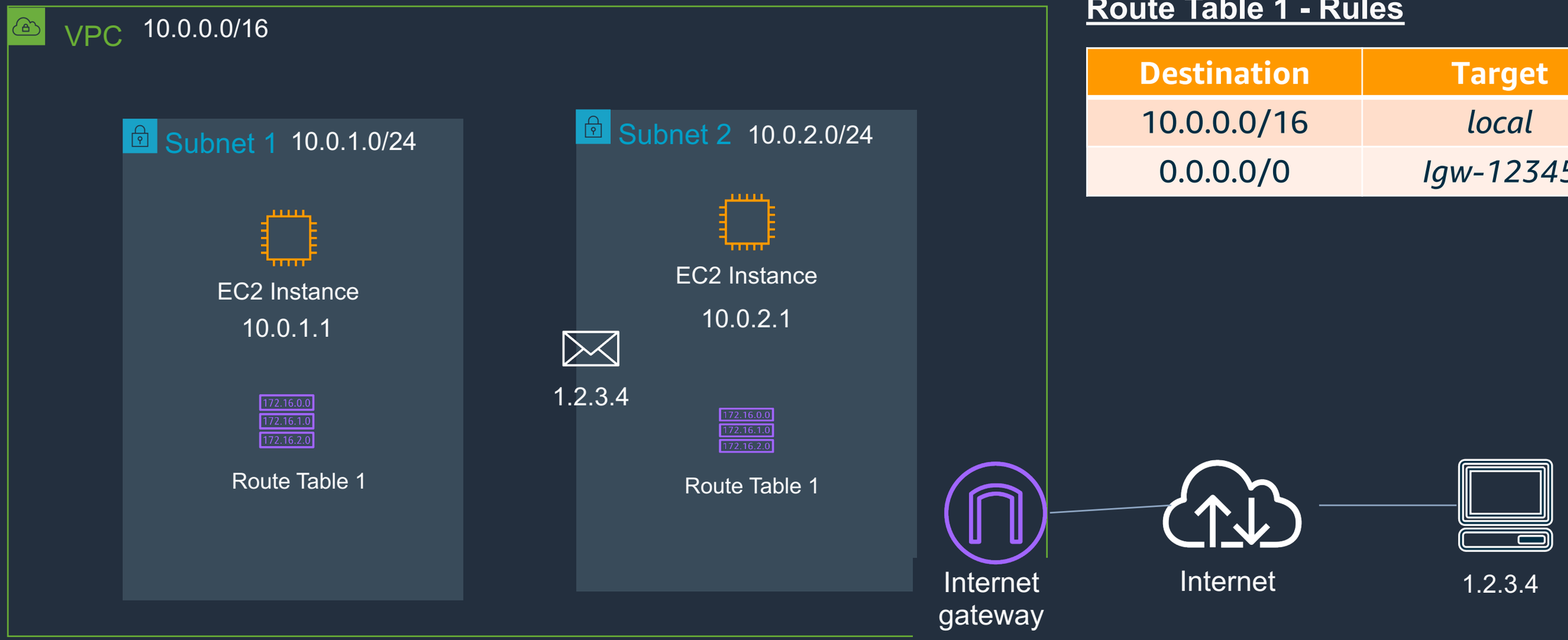
Route Tables – Internet Traffic



Route Table 1 - Rules

Destination	Target
10.0.0.0/16	*local*

Route Tables – Internet Traffic



Route Table 1 - Rules

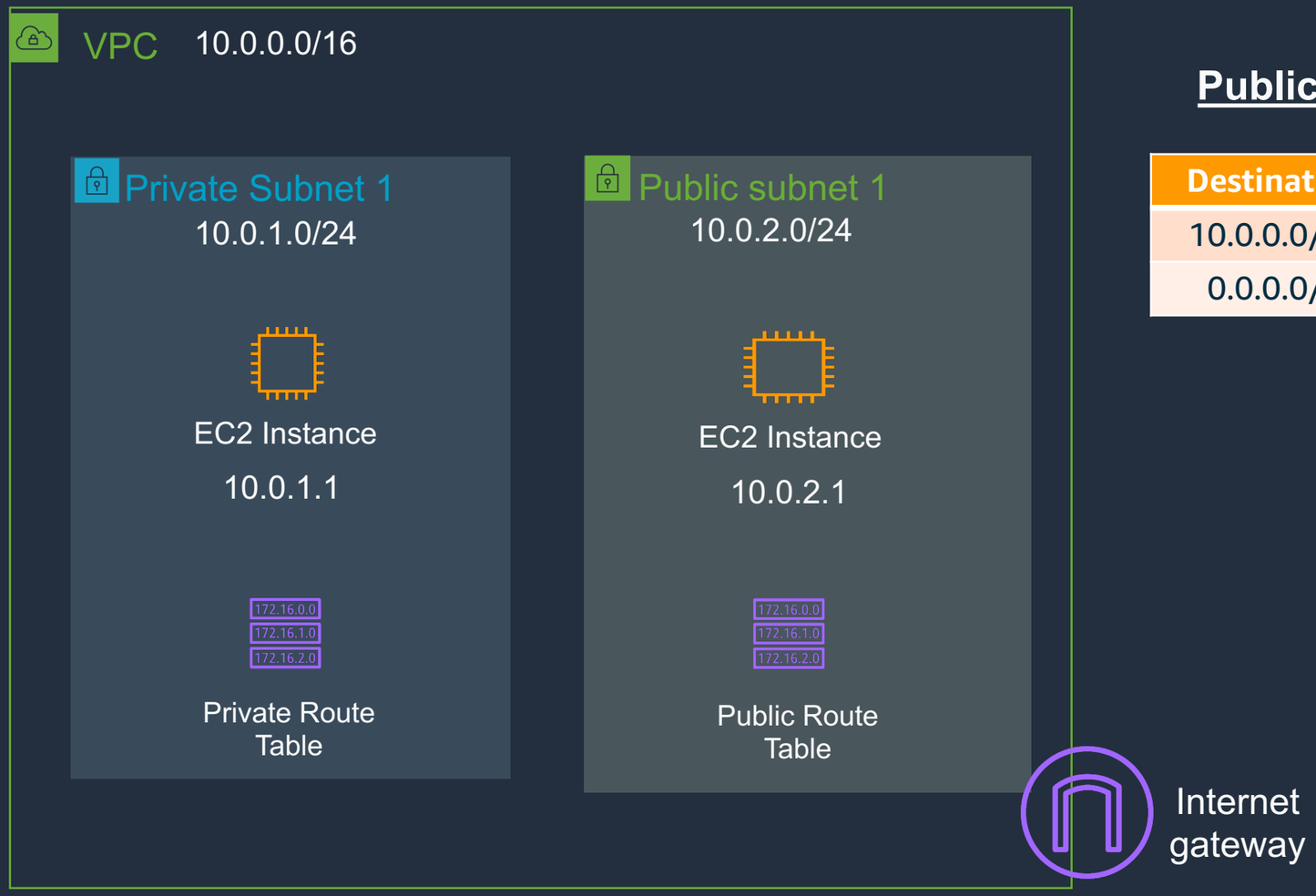
Destination	Target
10.0.0.0/16	*local*
0.0.0.0/0	*igw-12345*

aws

Public vs. Private Subnet

Private Route Table

Destination	Target
10.0.0.0/16	*local*

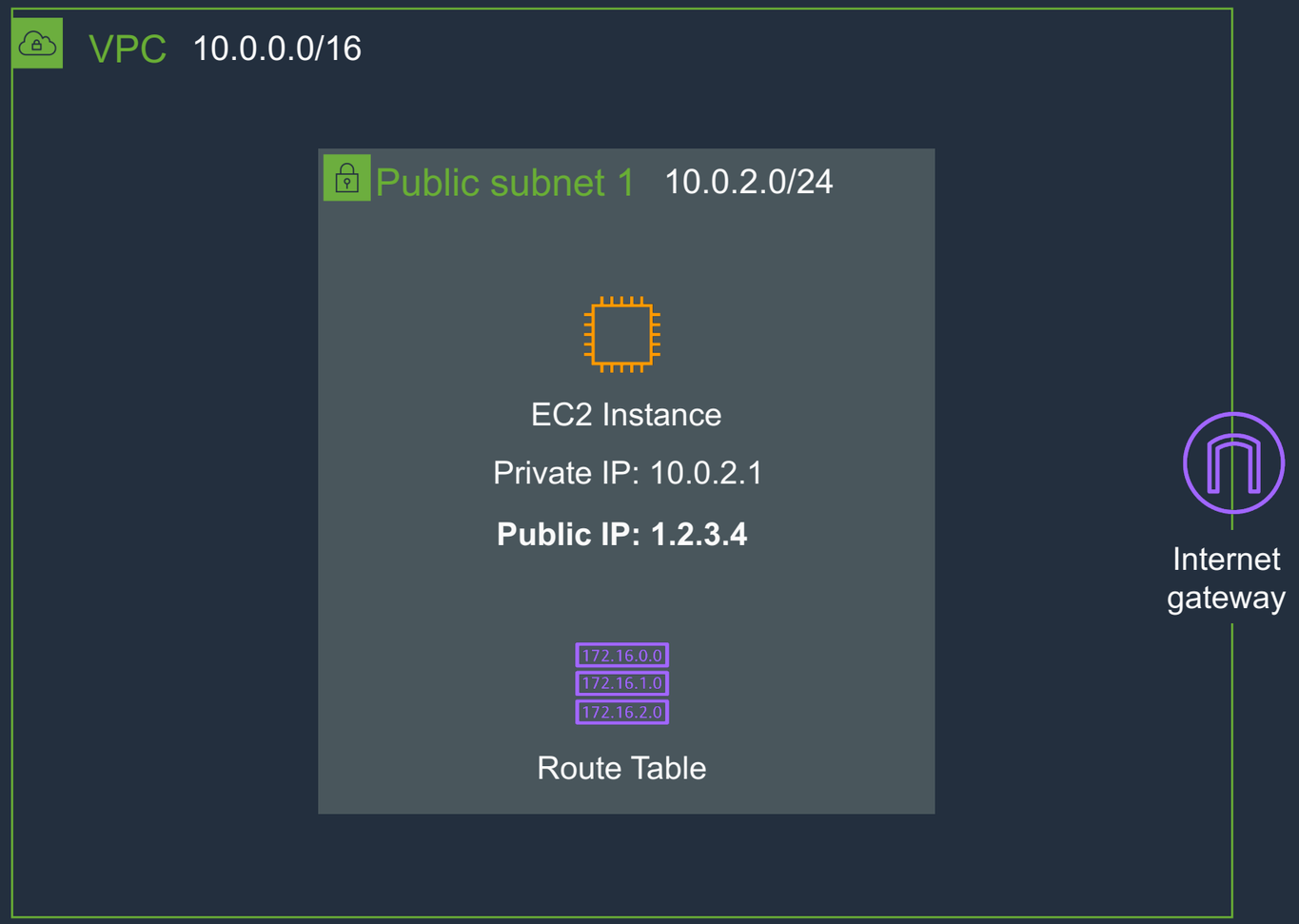


Public Route Table

Destination	Target
10.0.0.0/16	*local*
0.0.0.0/0	*Igw-12345*

aws

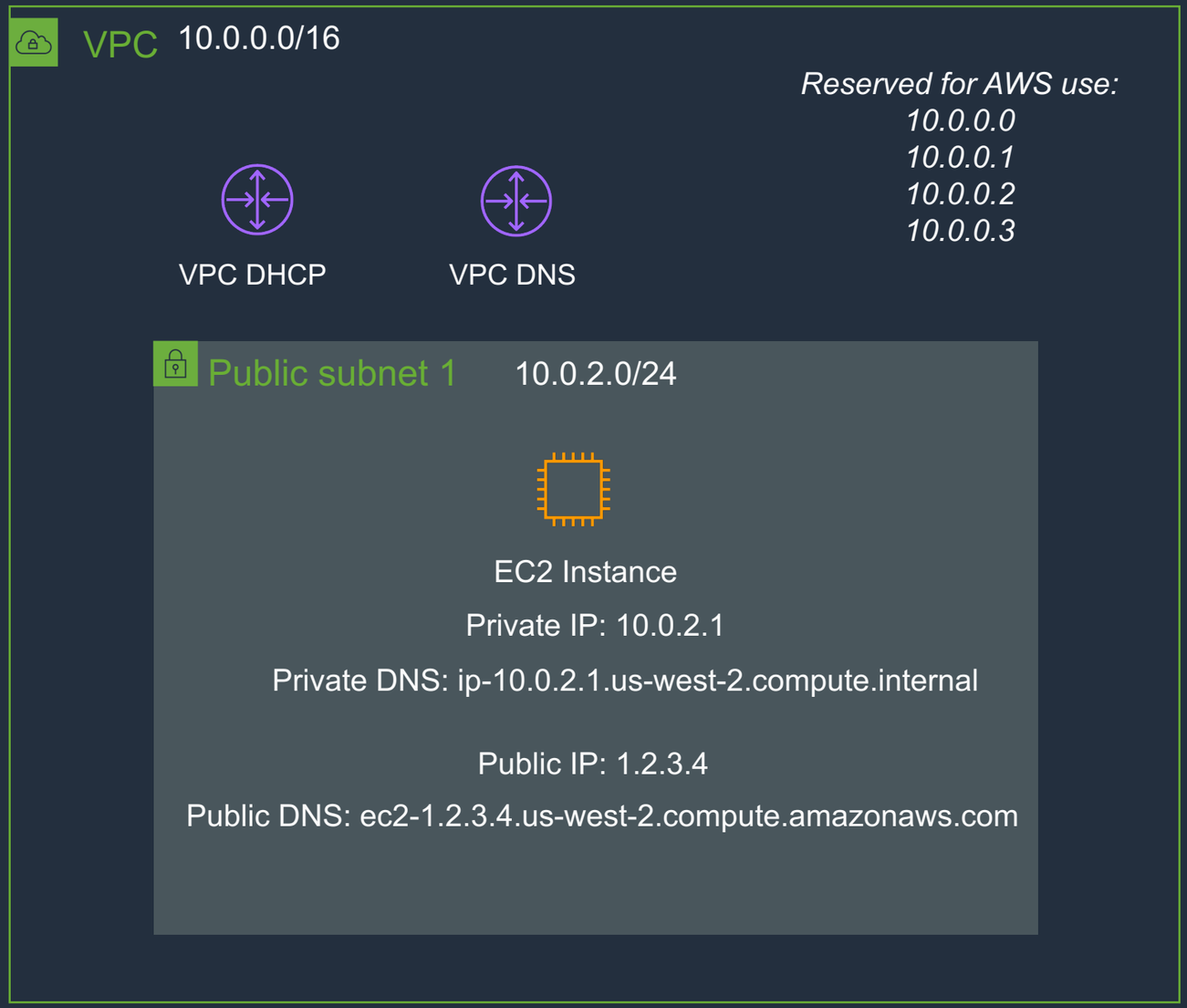
Public IPs



Public Route Table

Destination	Target
10.0.0.0/16	*local*
0.0.0.0/0	*Igw-12345*

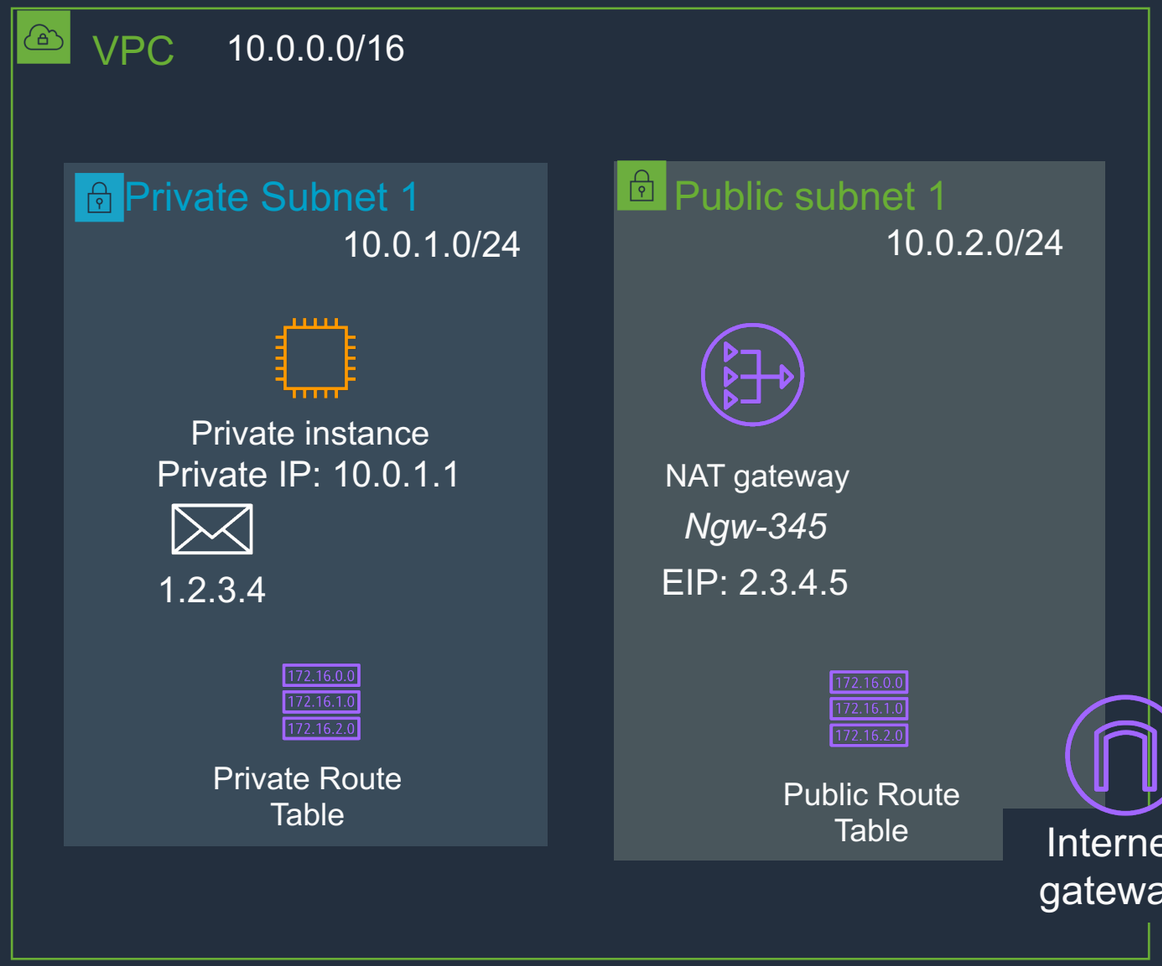
VPC - DNS & DHCP



Internet Access for Private Subnets – NAT Gateway

Private Route Table

Destination	Target
10.0.0.0/16	*local*
0.0.0.0/0	*ngw-345*

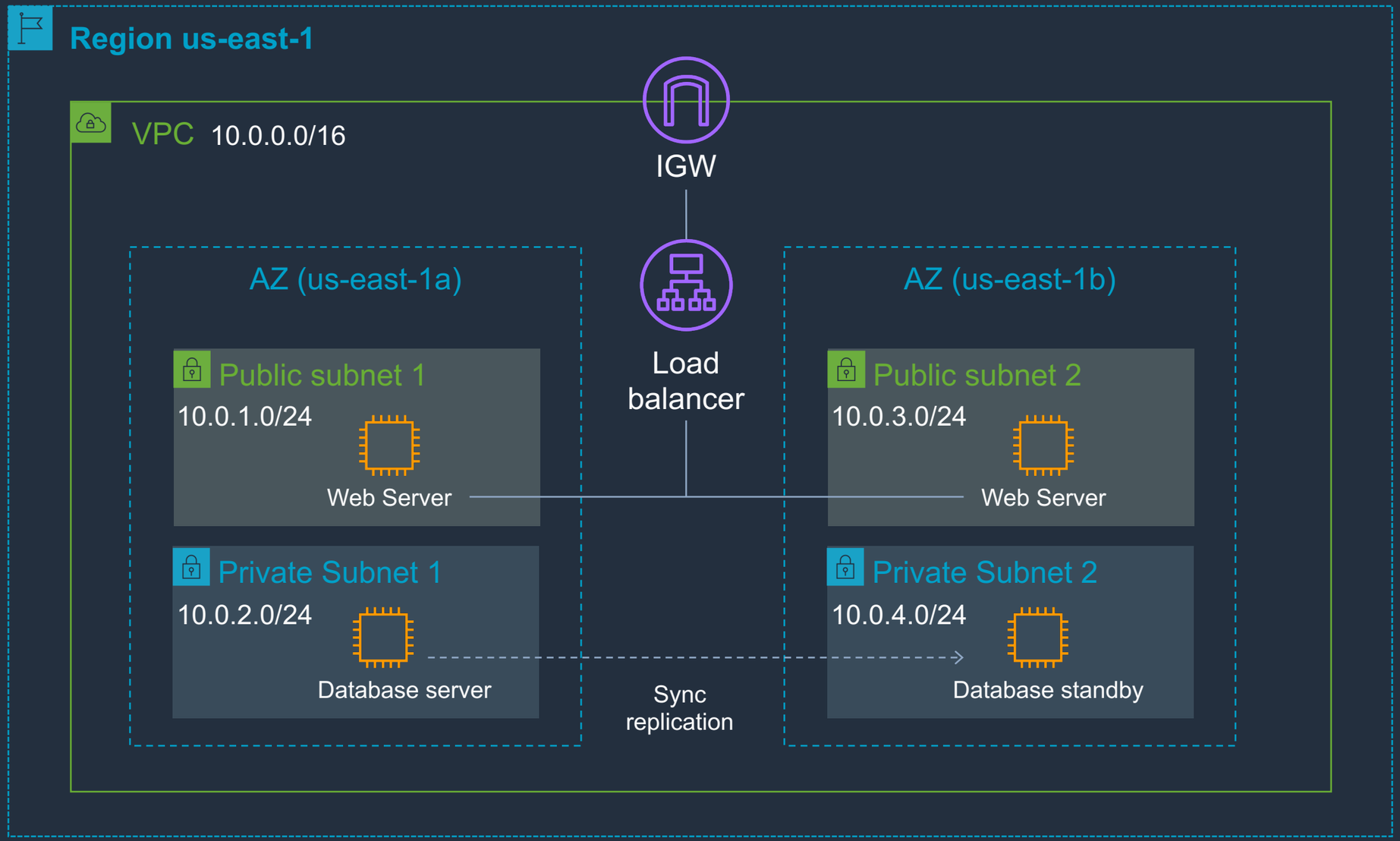


Public Route Table

Destination	Target
10.0.0.0/16	*local*
0.0.0.0/0	*Igw-12345*

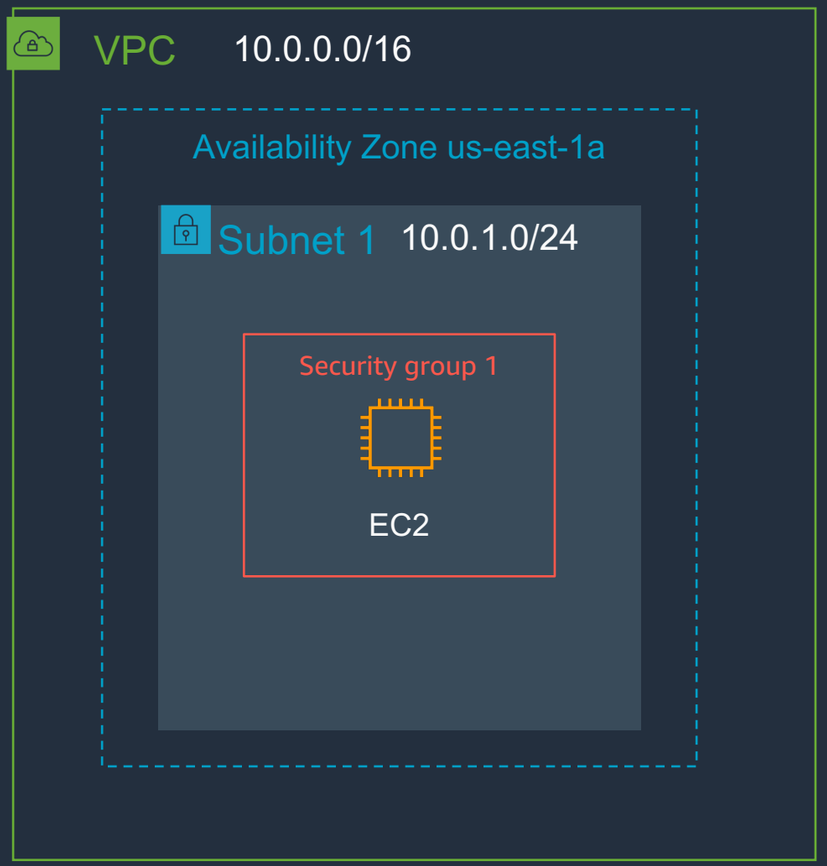
aws

Multi-AZ Best Practices



aws

Security Groups – Default Group Rules



Security Group 1

Inbound Rules

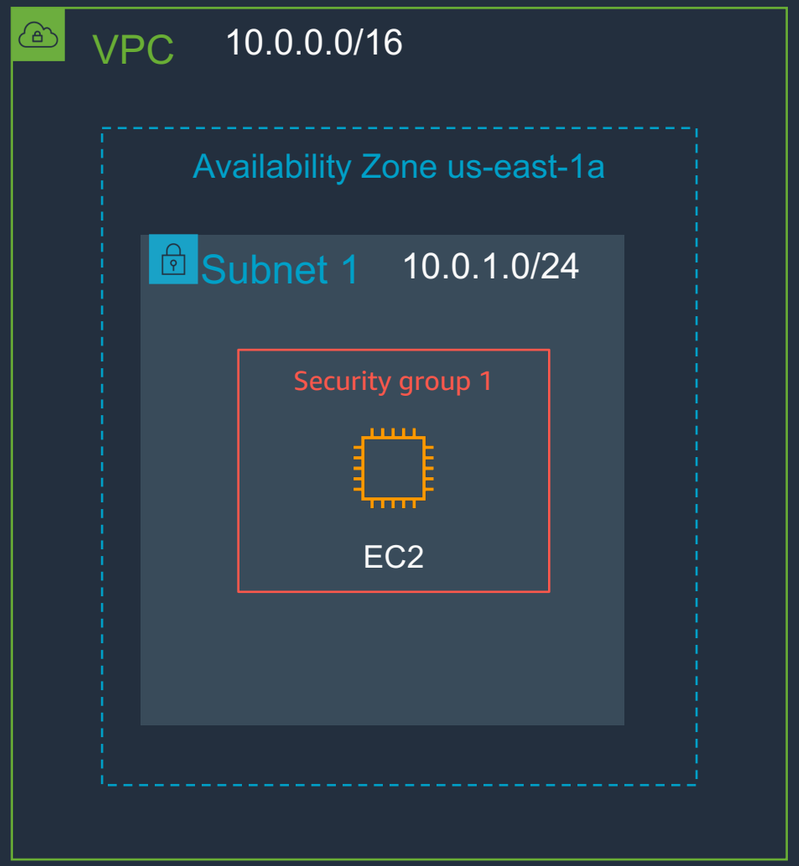
Protocol	Port	Source

Outbound Rules

Protocol	Port	Destination
All	*All*	*0.0.0.0/0*

aws

Security Groups – Web Server Example



Security Group 1

Inbound Rules

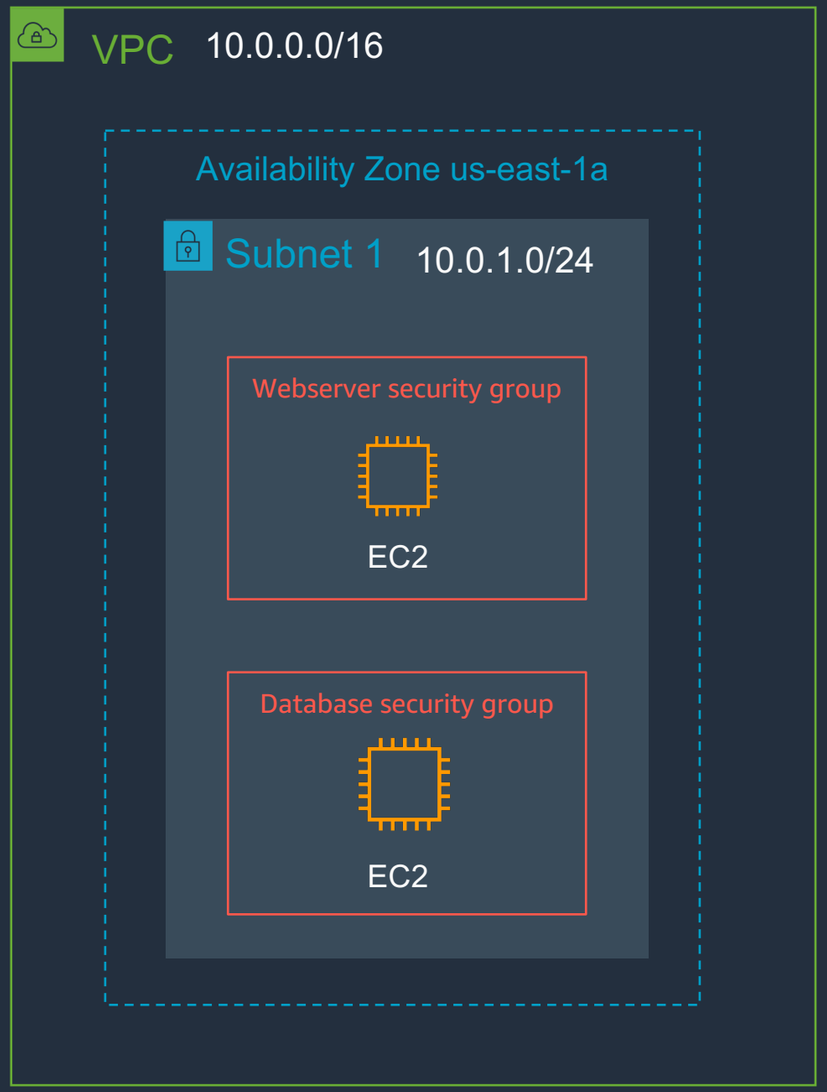
Protocol	Port	Source
TCP	*80*	*0.0.0.0/0*

Outbound Rules

Protocol	Port	Destination
All	*All*	*0.0.0.0/0*

aws

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

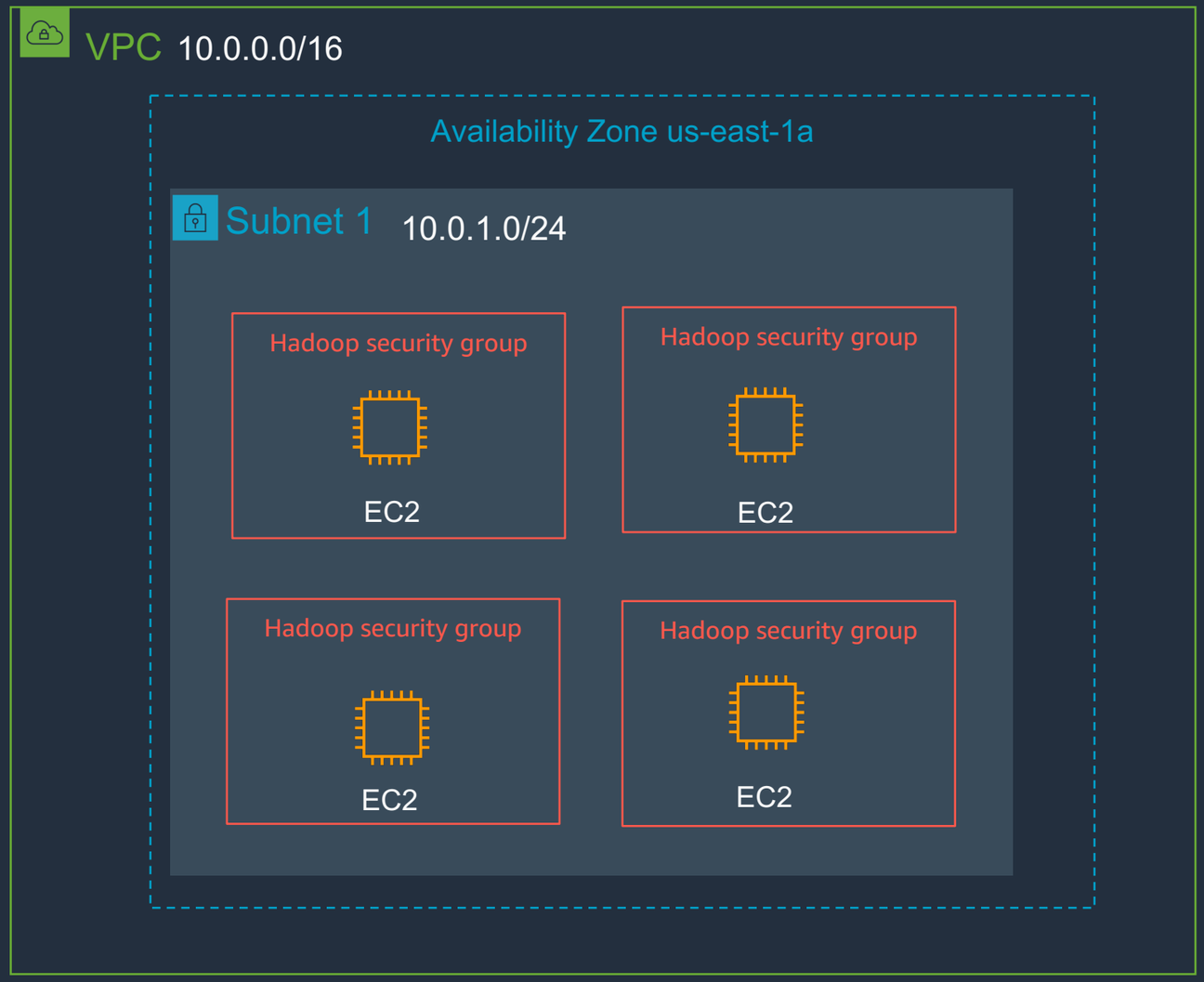
Protocol	Port	Source
TCP	*3306*	*sg-webserver*

Outbound Rules

Protocol	Port	Destination
All	*All*	*0.0.0.0/0*

aws

Security Groups – Self-referencing rules



Hadoop Security Group

Inbound Rules

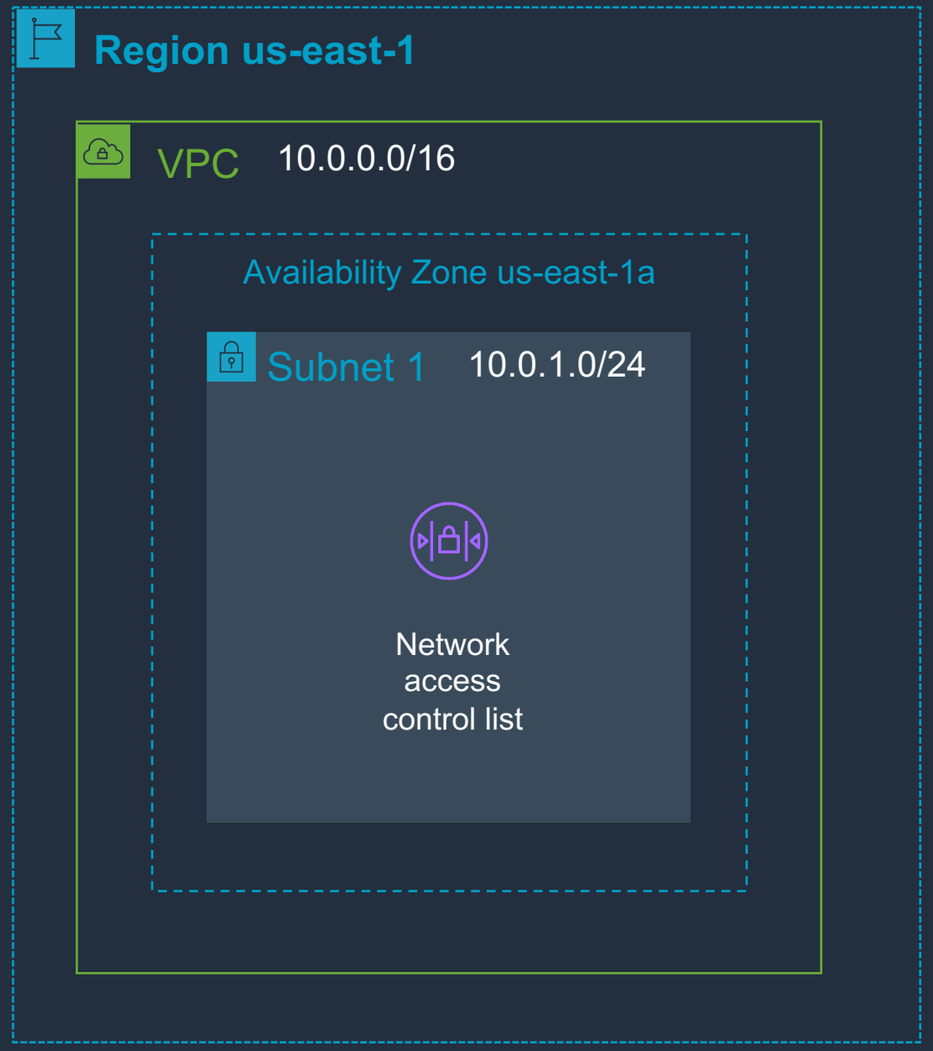
Protocol	Port	Source
TCP	*80*	*sg-hadoop*

Outbound Rules

Protocol	Port	Destination
All	*All*	*0.0.0.0/0*

aws

Network Access Control Lists (NACLs)



NACL Configuration

Inbound Rules

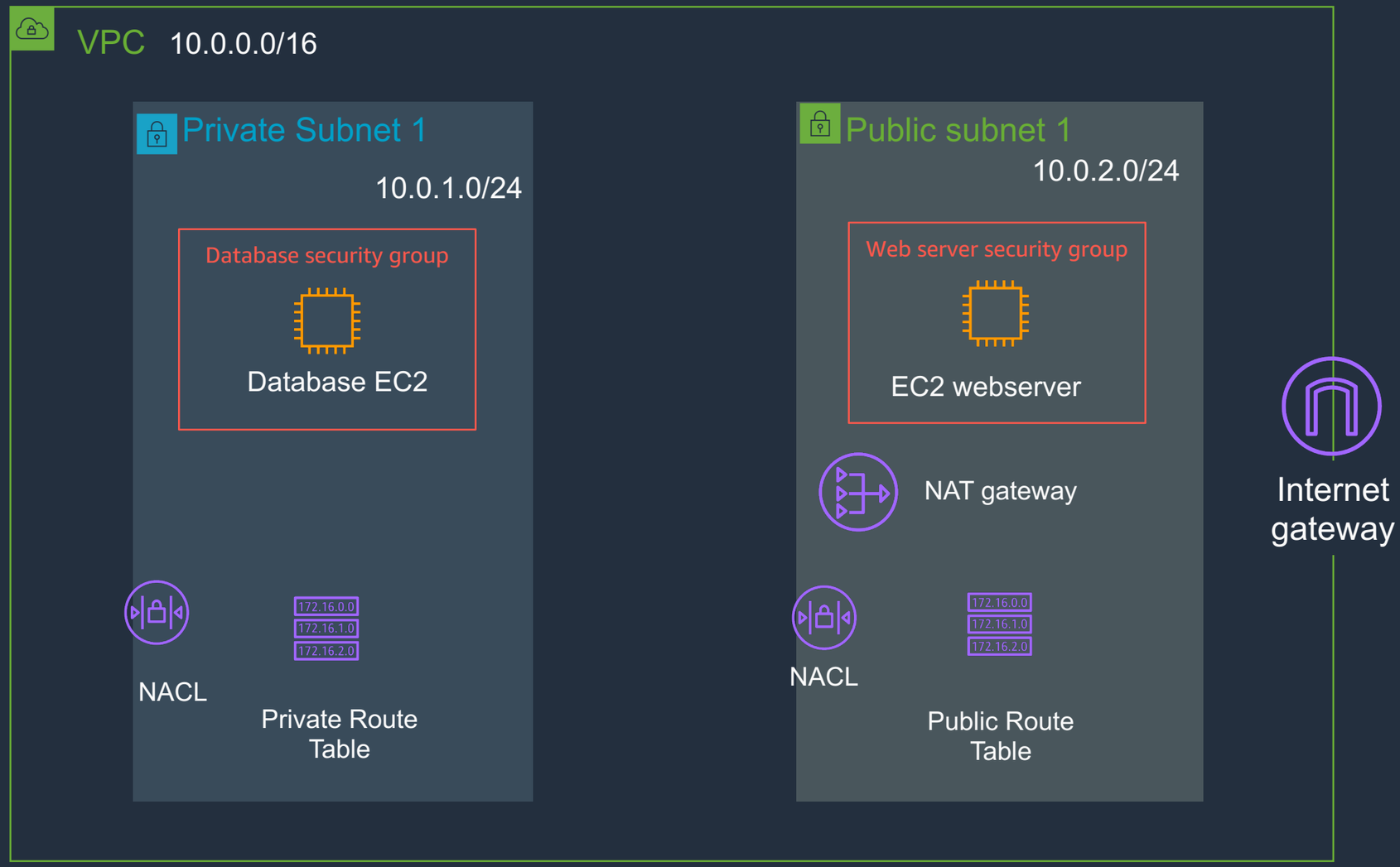
Rule #	Protocol	Port	Source	Effect
1	All	*All*	*0.0.0.0/0*	*Allow*

Outbound Rules

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

aws

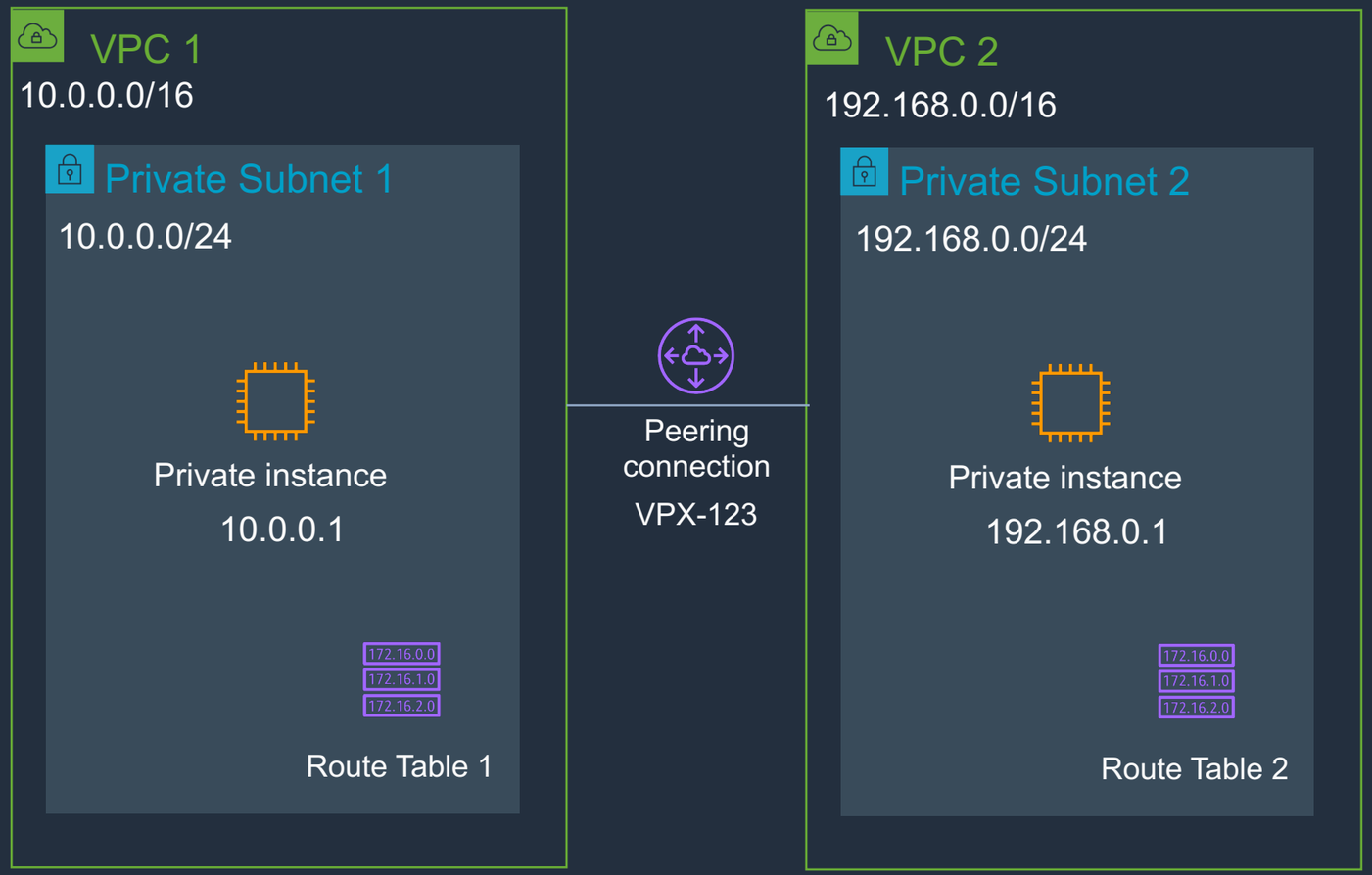
VPC Building Blocks - Summary



VPC Peering

Route Table 1

Destination	Target
10.0.0.0/16	*local*
192.168.0.1	*VPX-123*

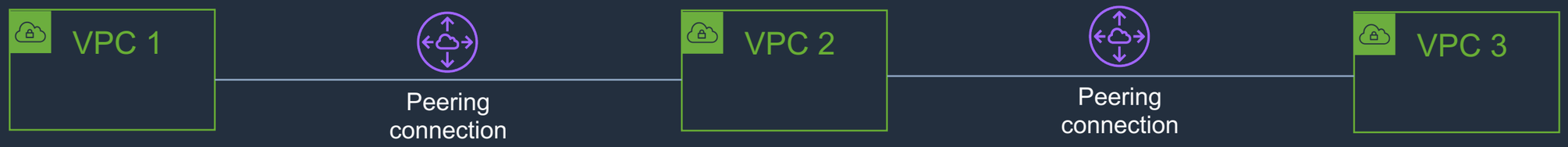


Route 2 Table

Destination	Target
192.168.0.0/16	*local*
10.0.0.0/16	*VPX-123*

aws

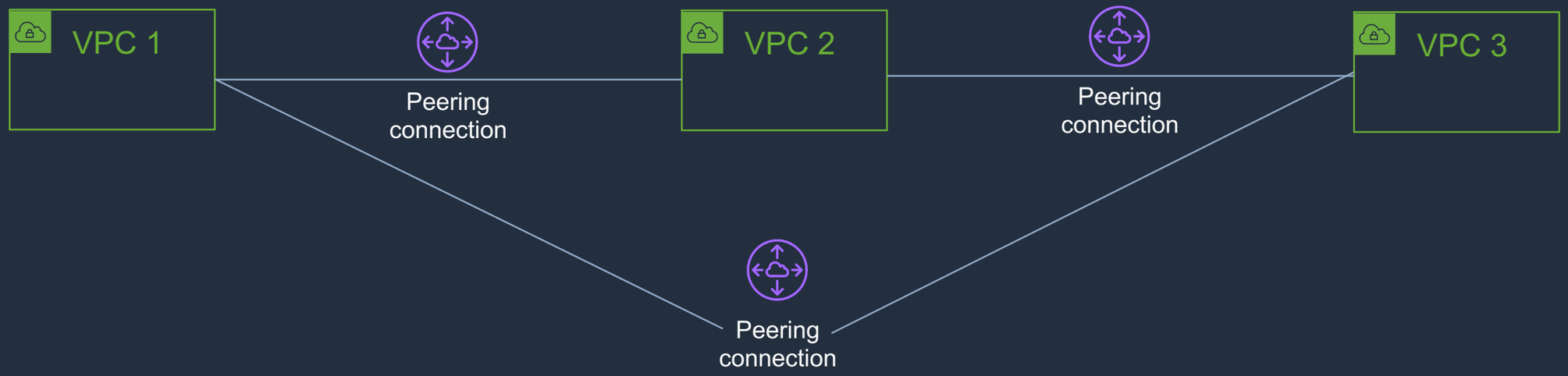
VPC Peering – No Transitive Routing



- VPC 1 can reach VPC 2
- VPC 1 **cannot** reach VPC 3

aws

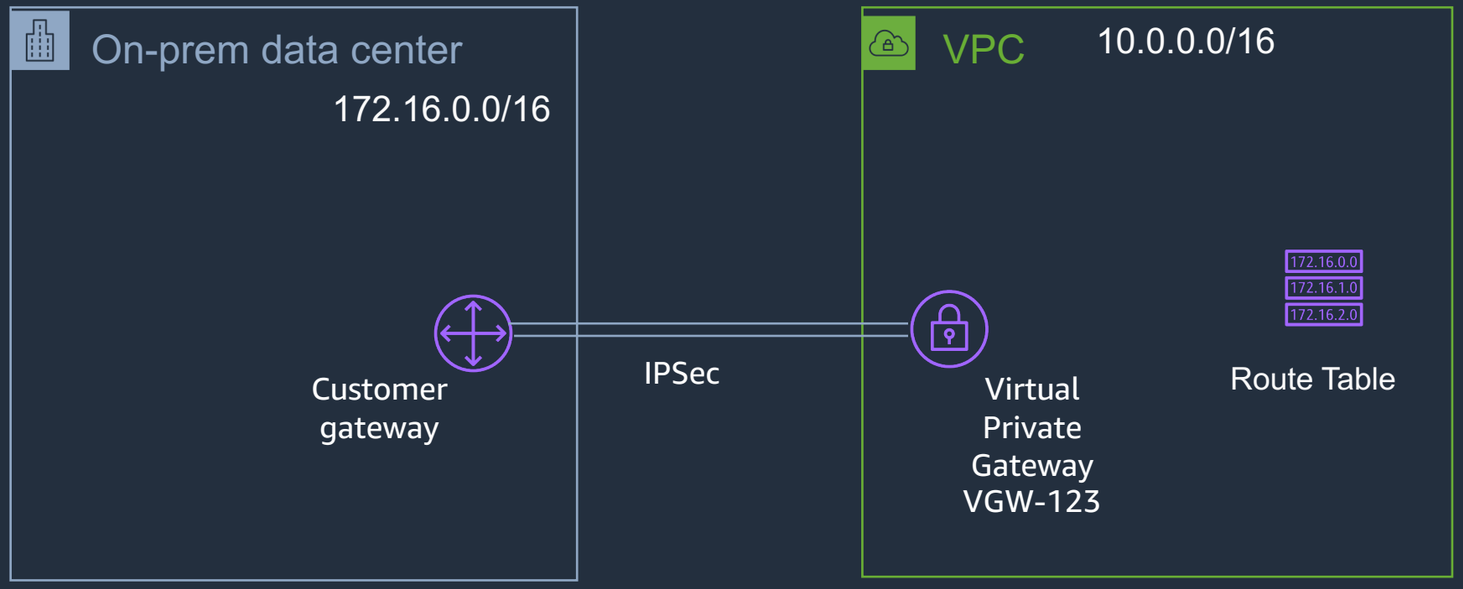
VPC Peering – No Transitive Routing



- VPC 1 can reach VPC 2
- VPC 1 **can** reach VPC 3

aws

AWS Site-to-Site VPN

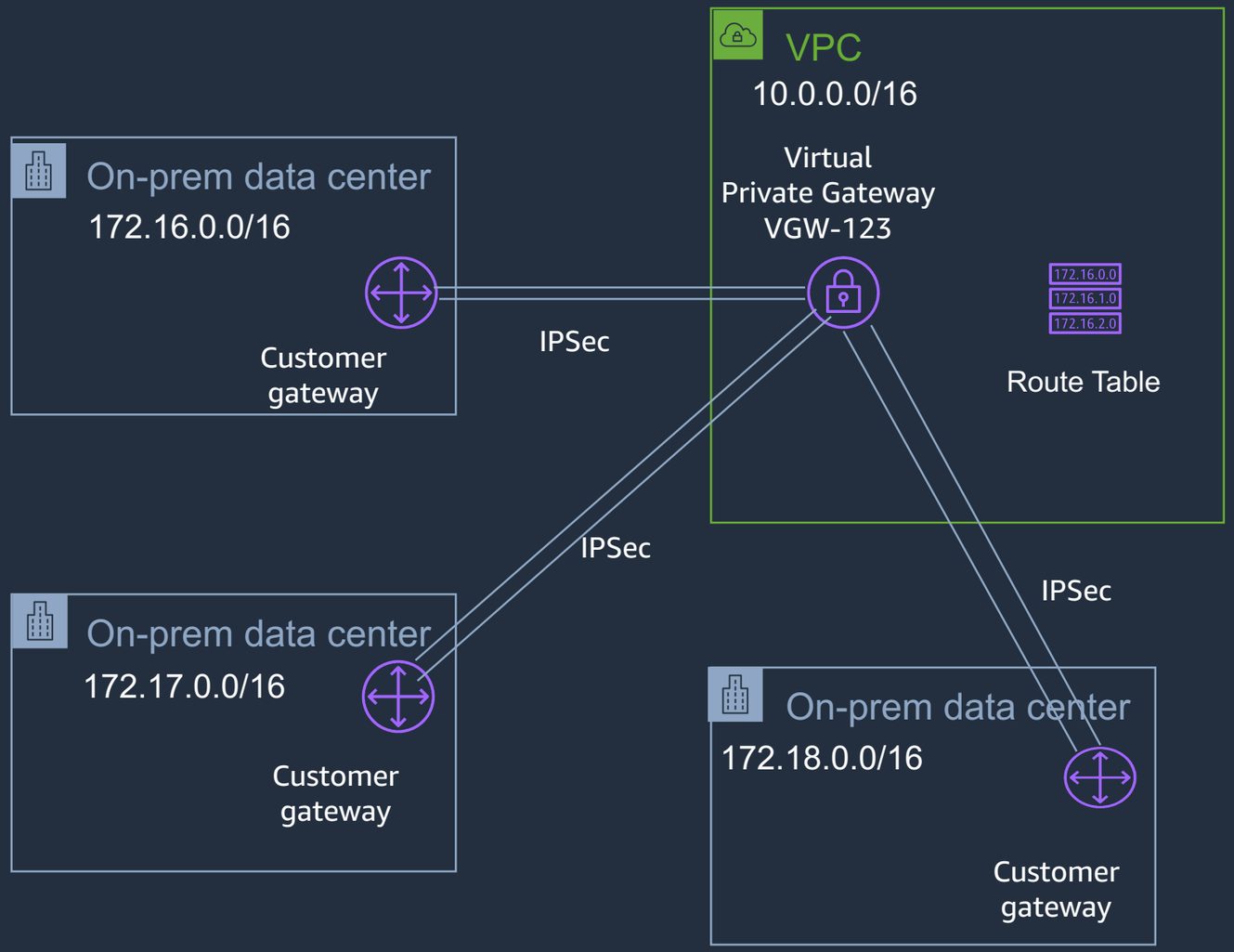


VPC Route Table

Destination	Target
10.0.0.0/16	*local*
172.16.0.0/16	*VGW-123*

- One VGW per VPC
- BGP or static routes
- Redundant IPSec tunnels
- Redundant routers across two AZs

AWS Site-to-Site VPN

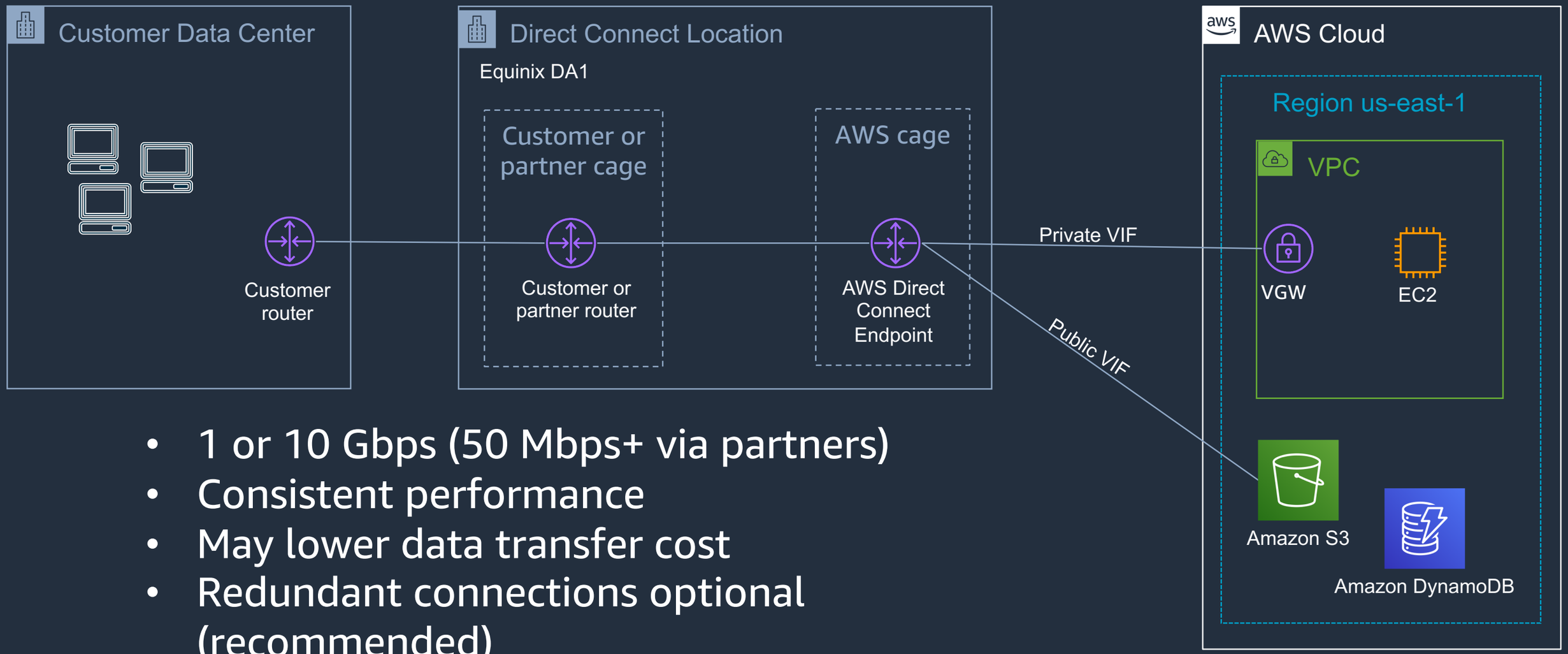


VPC Route Table

Destination	Target
10.0.0.0/16	*local*
172.16.0.0/16	*VGW-123*

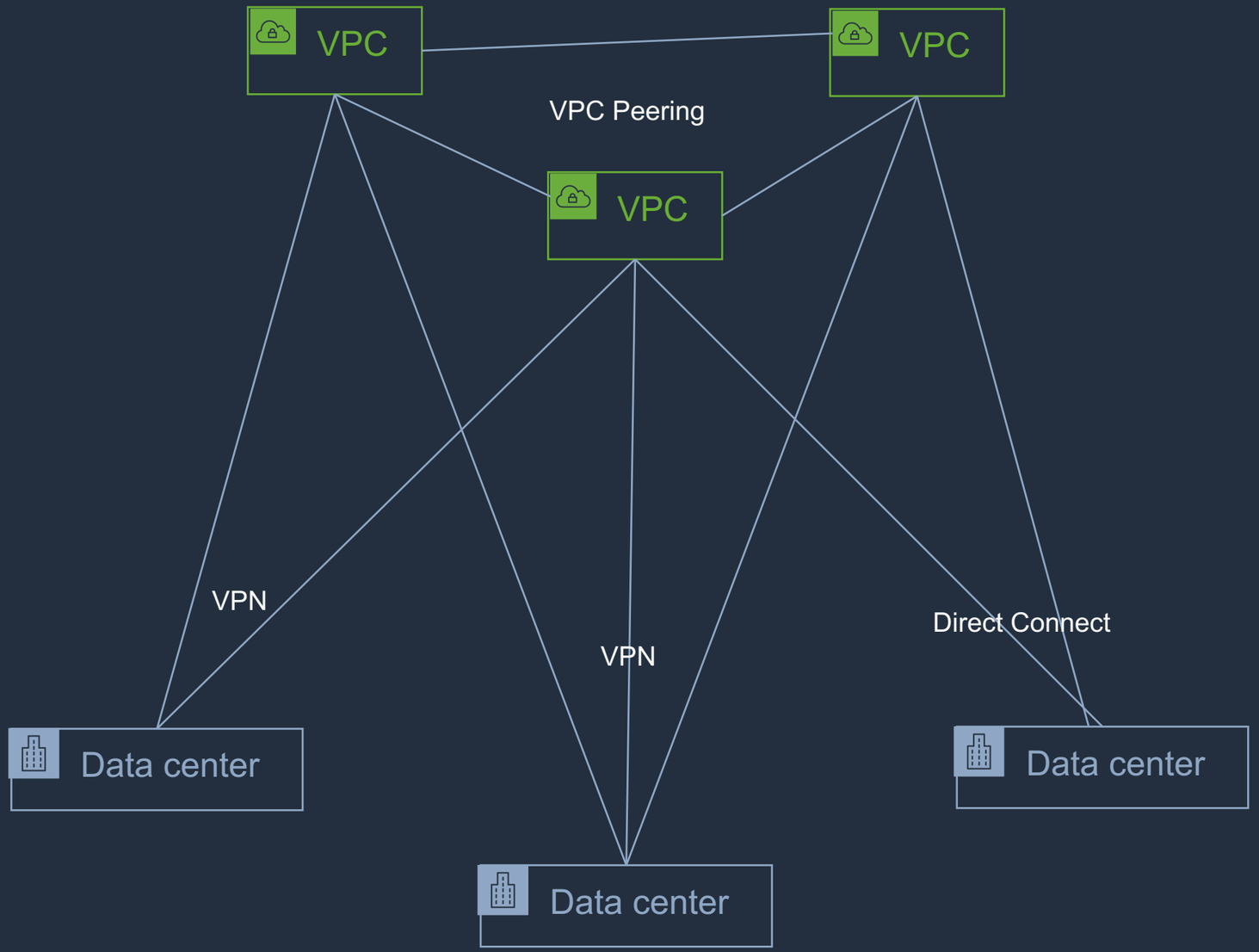
aws

AWS Direct Connect

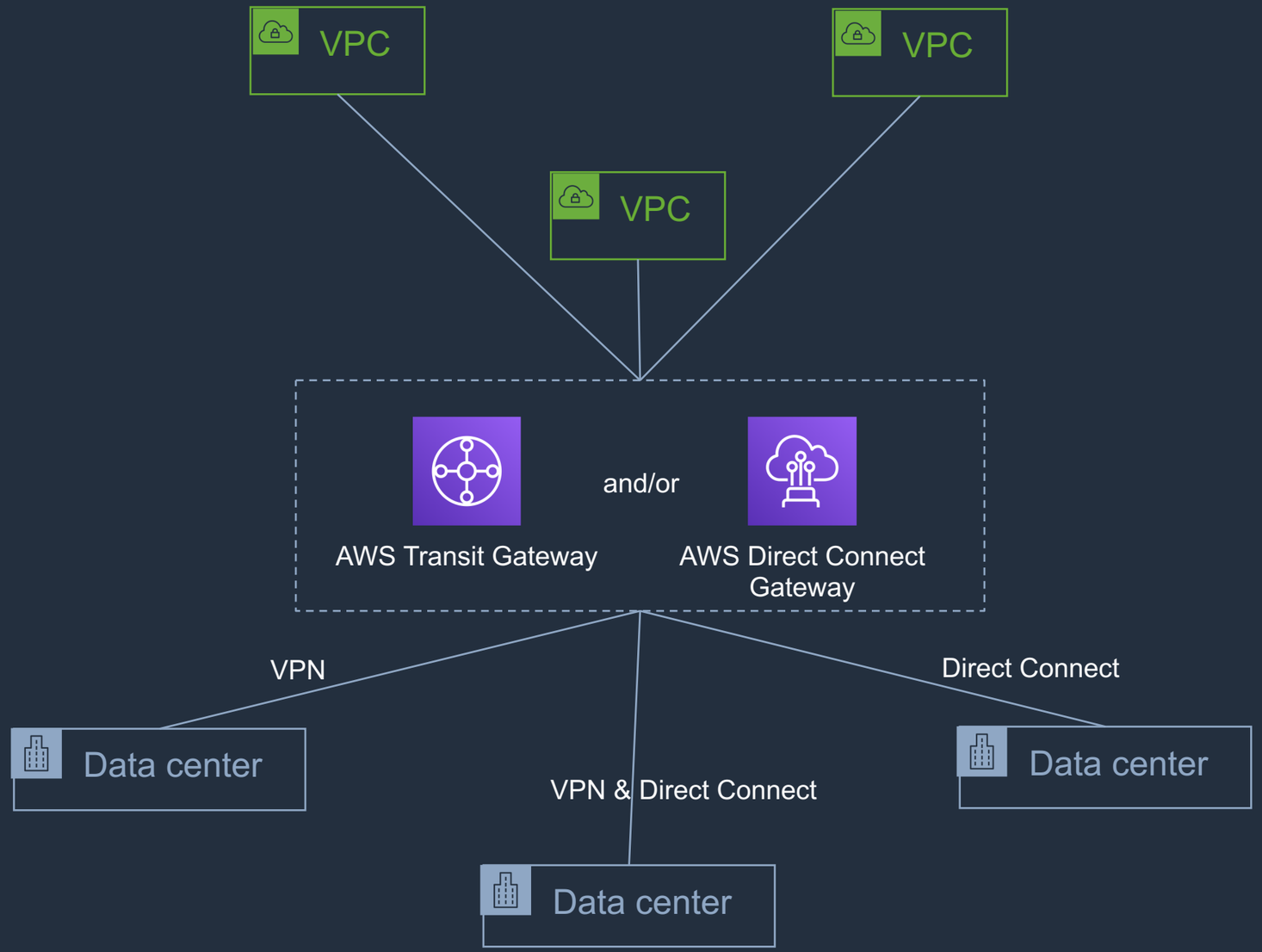


- 1 or 10 Gbps (50 Mbps+ via partners)
- Consistent performance
- May lower data transfer cost
- Redundant connections optional (recommended)

VPN & Direct Connect - Mesh Topology



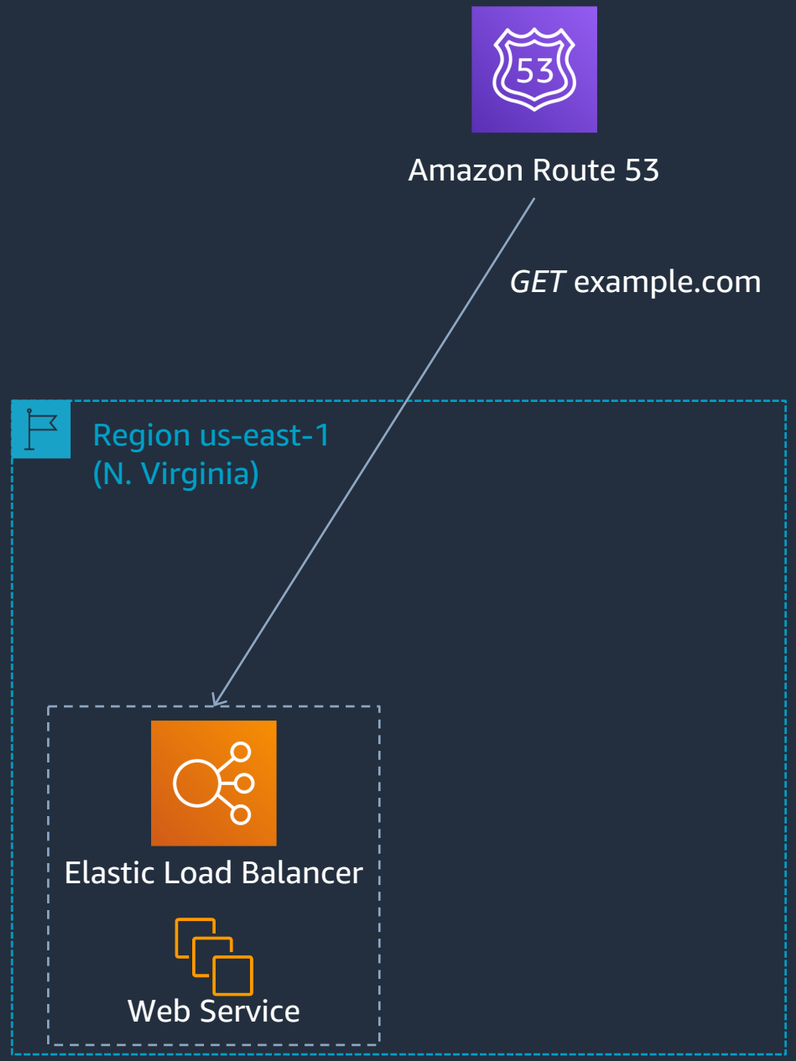
Transit Gateway & Direct Connect Gateway



DNS with Amazon Route 53

- Global DNS service
- 100% Availability SLA
- Domain registrar
- Public and private DNS zones

- Supports
  - Health checks
  - DNS failover
  - Round-robin routing
  - Weighted routing
  - Geolocation
  - Latency-based routing

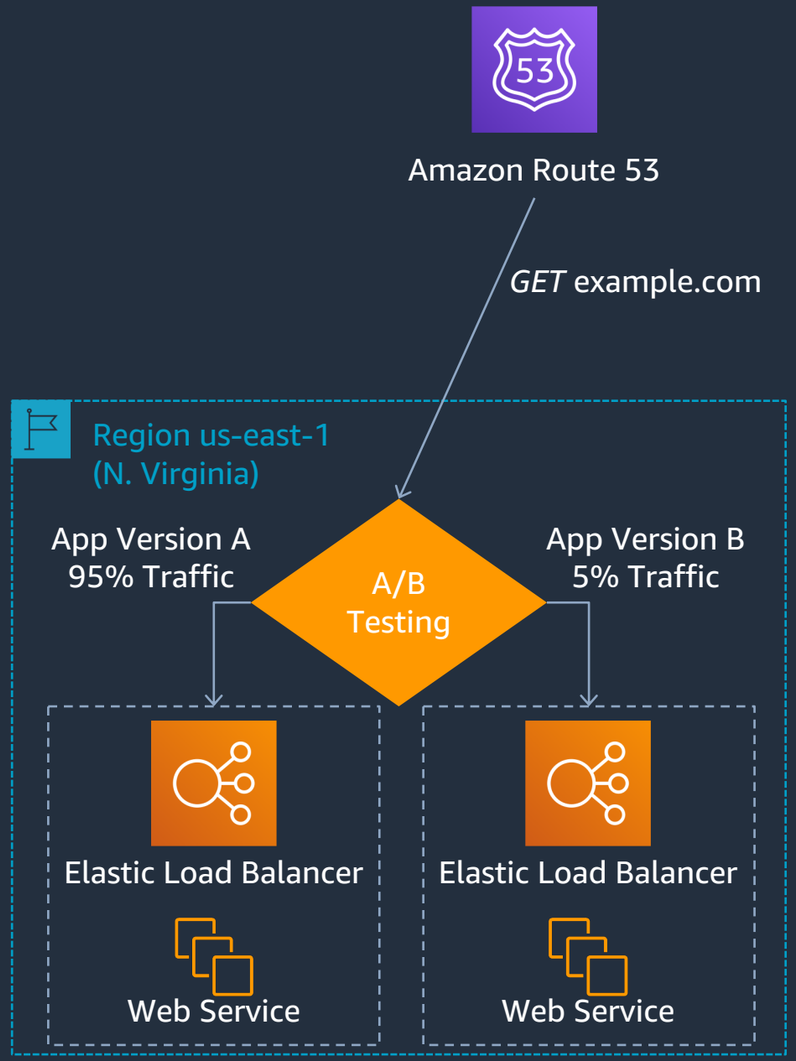


aws

DNS with Amazon Route 53

- Global DNS service
- 100% Availability SLA
- Domain registrar
- Public and private DNS zones

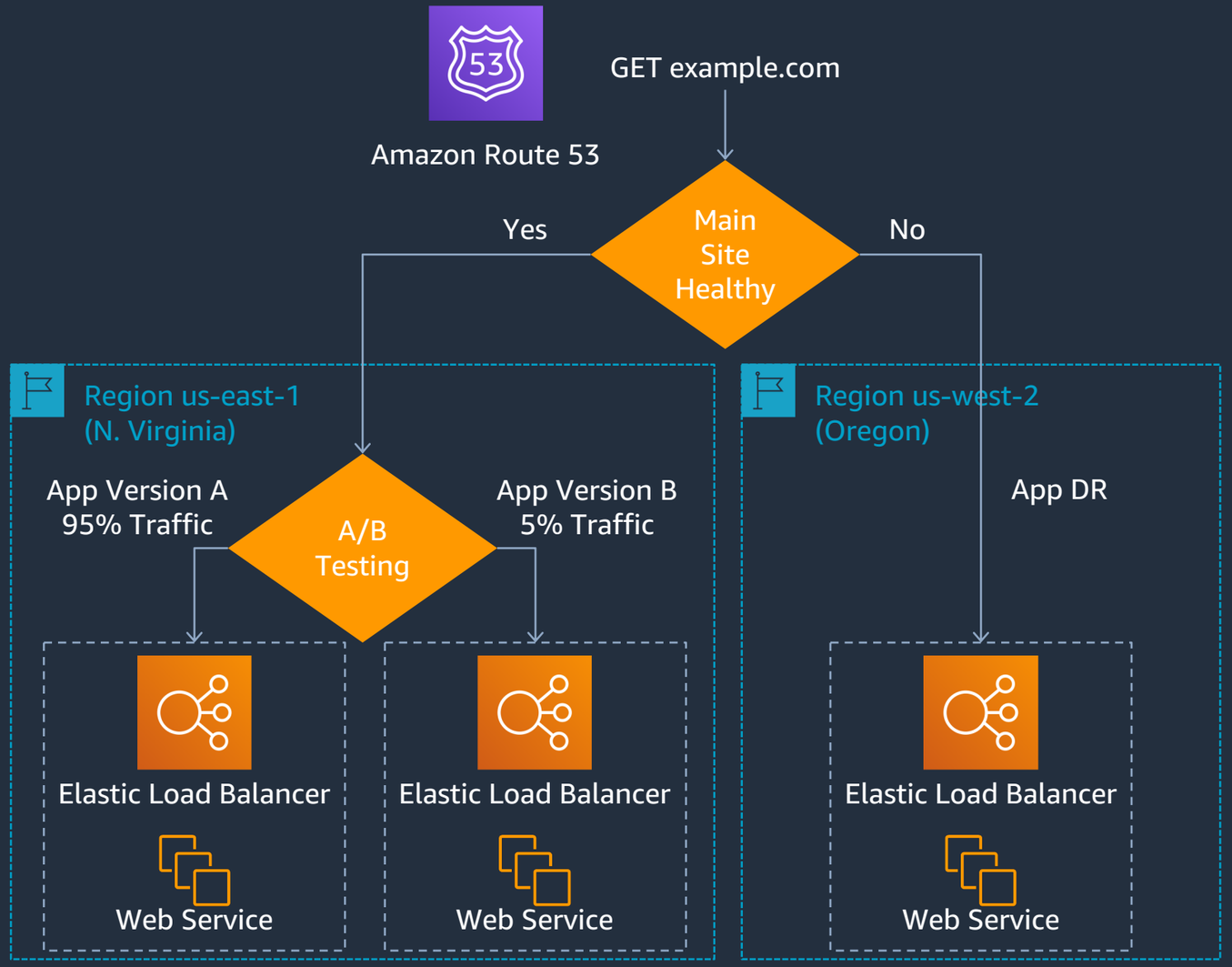
- Supports
  - Health checks
  - DNS failover
  - Round-robin routing
  - Weighted routing
  - Geolocation
  - Latency-based routing



DNS with Amazon Route 53

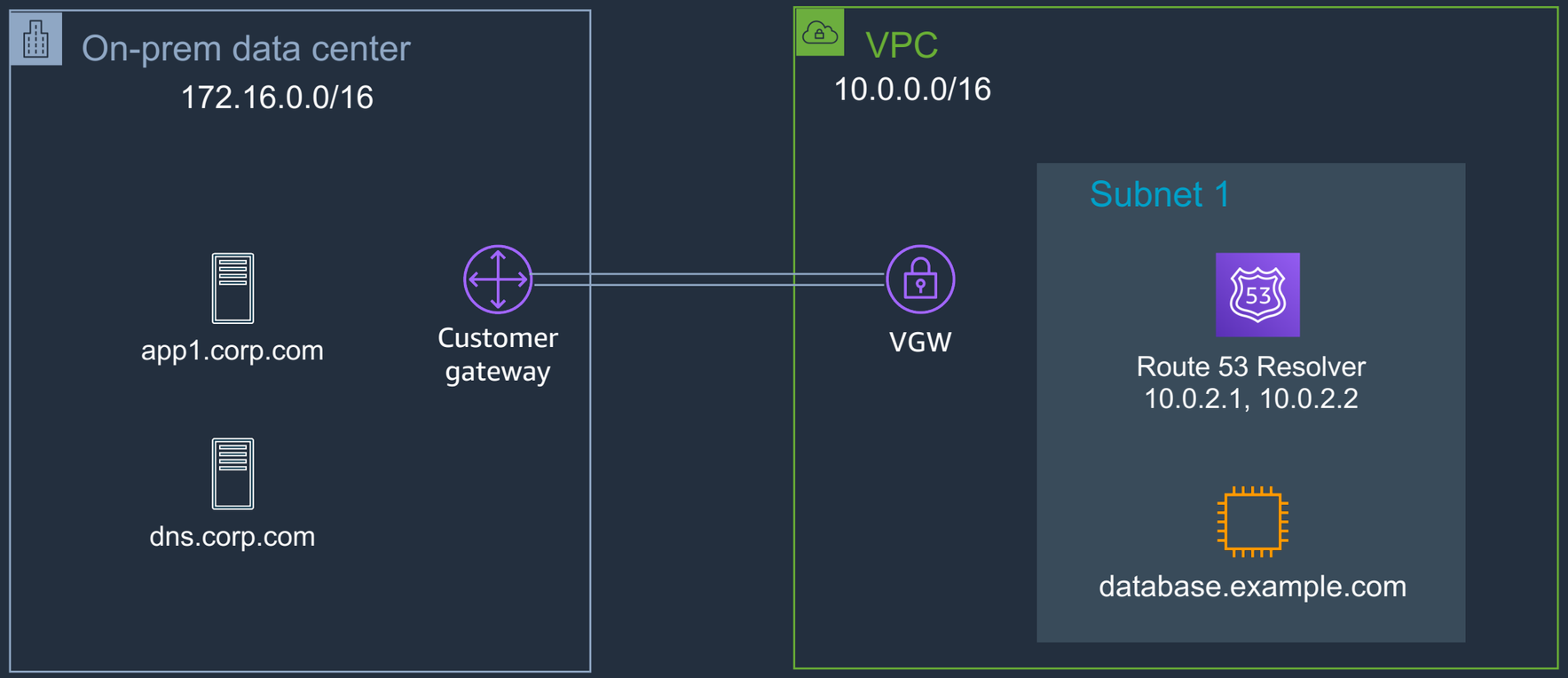
- Global DNS service
- 100% Availability SLA
- Domain registrar
- Public and private DNS zones

- Supports
  - Health checks
  - DNS failover
  - Round-robin routing
  - Weighted routing
  - Geolocation
  - Latency-based routing



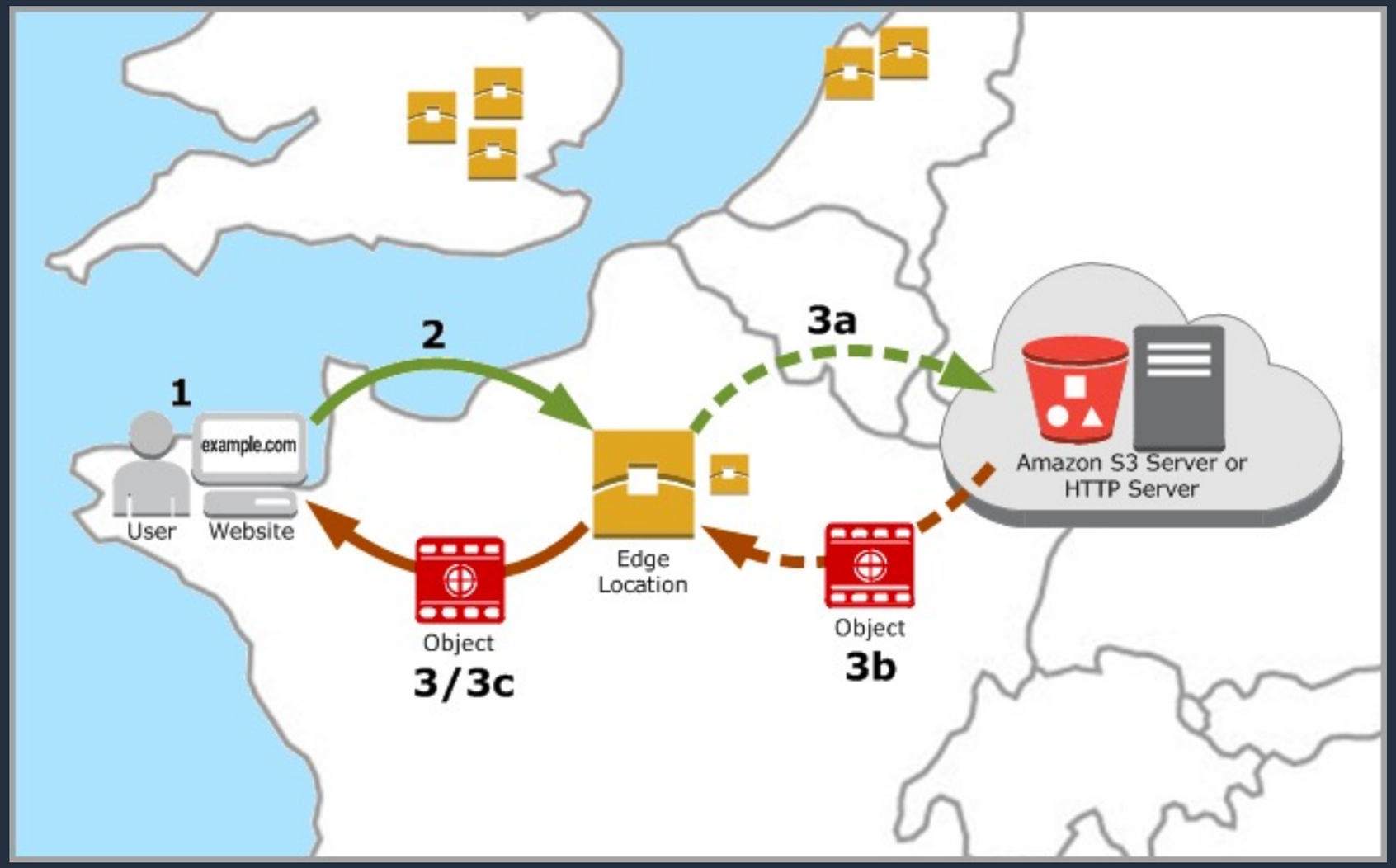
aws

Hybrid DNS Resolution - Route 53 Resolvers



aws

Amazon CloudFront



- Global CDN
- 220+ Points of Presence

- ➢ User makes request
- ➢ Routed to edge location
- ➢ Edge gets from origin
- ➢ Origin returns to edge
- ➢ Edge caches response
- ➢ Edge returns to user

aws

Questions

Up Next… VPC Lab