Lecture 4: AWS VPC & Routing

Maharishi International University

Department of Computer Science

M.S. Thao Huy Vu

Maharishi International University - Fairfield, Iowa

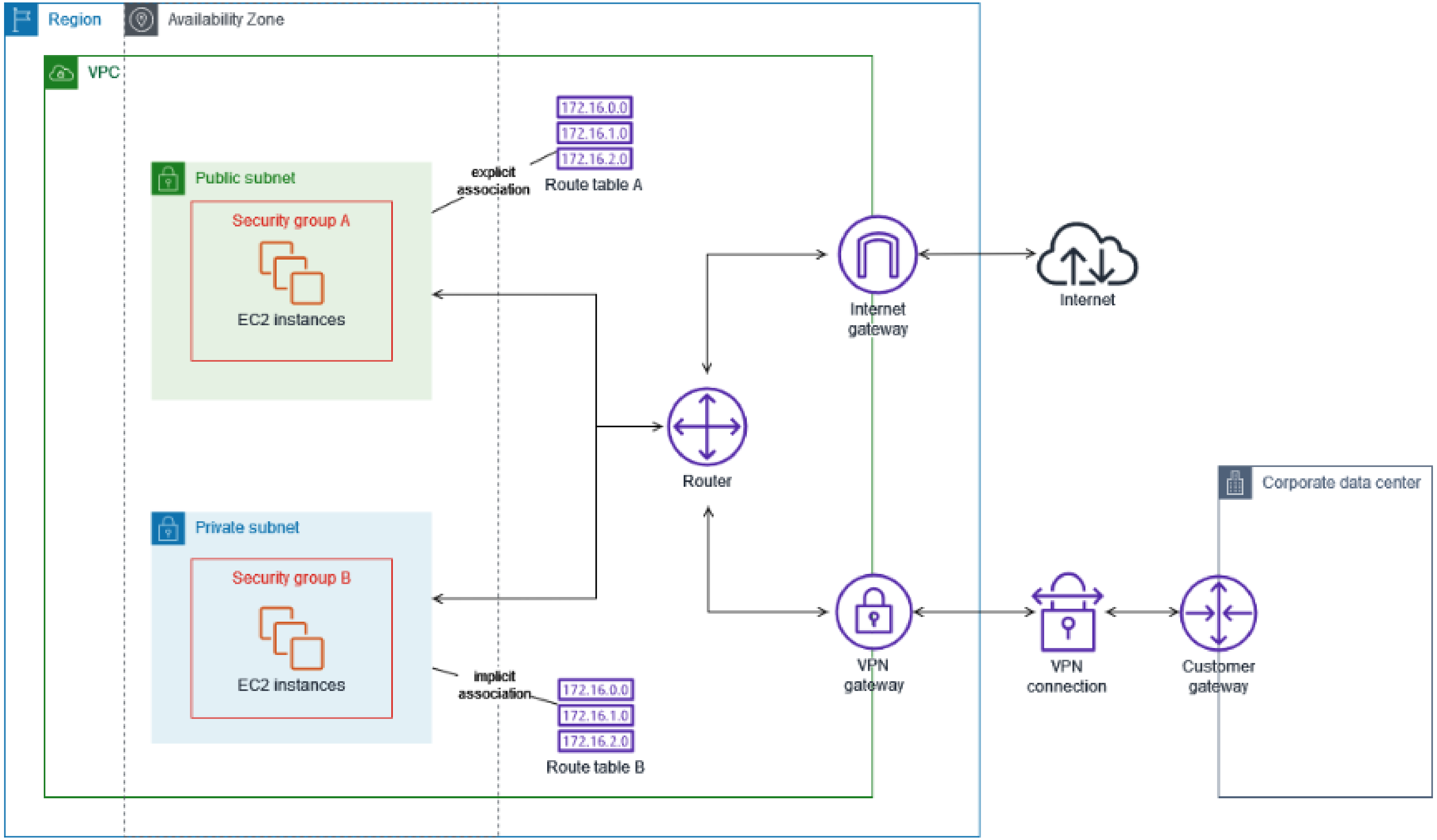
Agenda

- **Networking**
- **Route 53**

Networking Components

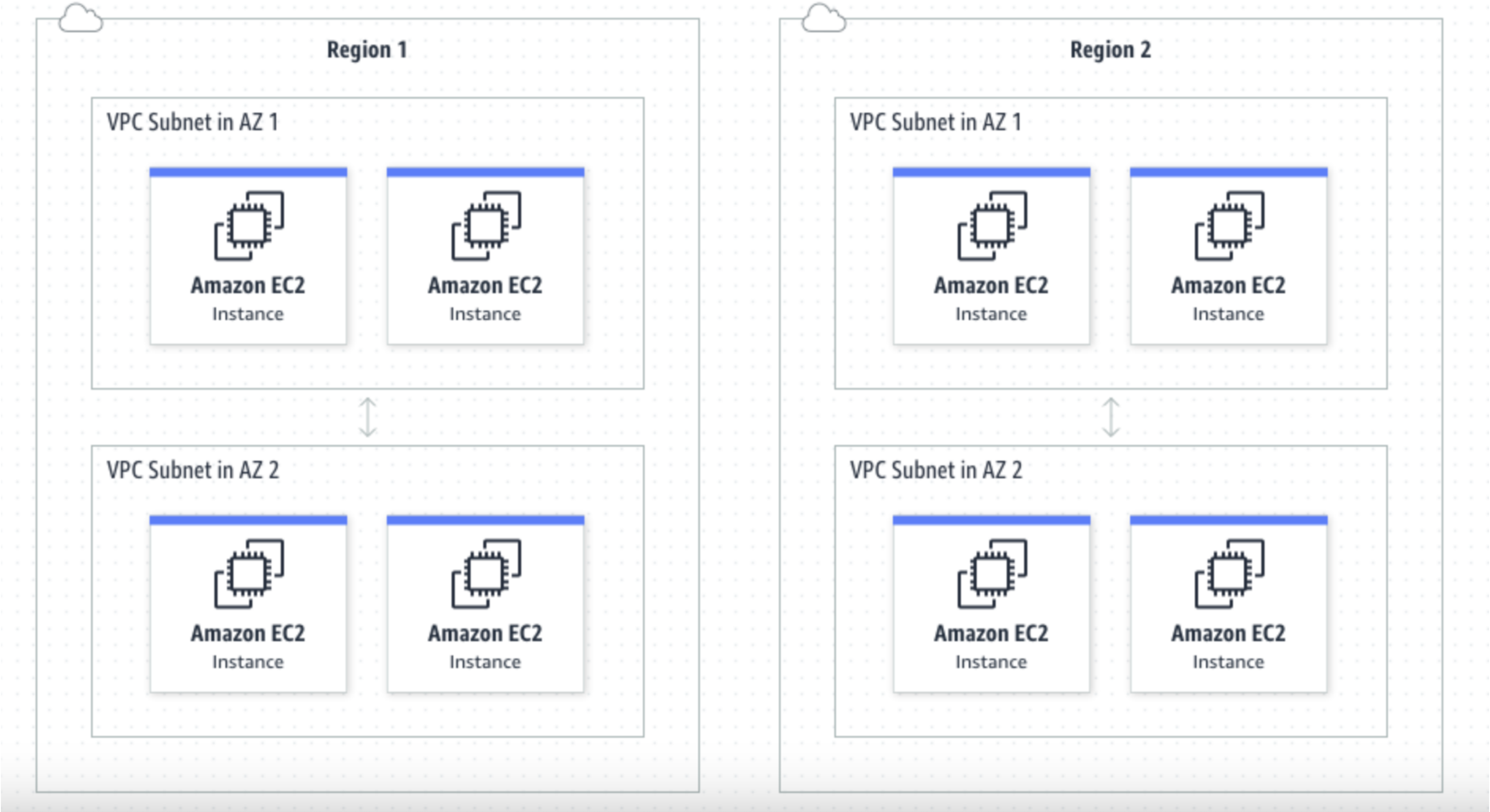
- **Virtual Private Cloud (VPC)**
- **Subnets**
- **Route Tables**
- **Internet Gateway (IGW)**
- **NAT Gateway**
- **Network ACLs (NACLs)**
- **Security Groups (SGs)**
- **VPC Peering**
- **Transit Gateway**

VPC



Region
Availability Zone
VPC
Public subnet
Security group A
EC2 instances
explicit association
172.16.0.0
172.16.1.0
172.16.2.0
Route table A
Internet gateway
Internet
Router
Private subnet
Security group B
EC2 instances
implicit association
172.16.0.0
172.16.1.0
172.16.2.0
Route table B
VPN gateway
VPN connection
Customer gateway
Corporate data center

VPC


Region 1
VPC Subnet in AZ 1
Amazon EC2
Instance
Amazon EC2
Instance
VPC Subnet in AZ 2
Amazon EC2
Instance
Amazon EC2
Instance
Region 2
VPC Subnet in AZ 1
Amazon EC2
Instance
Amazon EC2
Instance
VPC Subnet in AZ 2
Amazon EC2
Instance
Amazon EC2
Instance

VPC

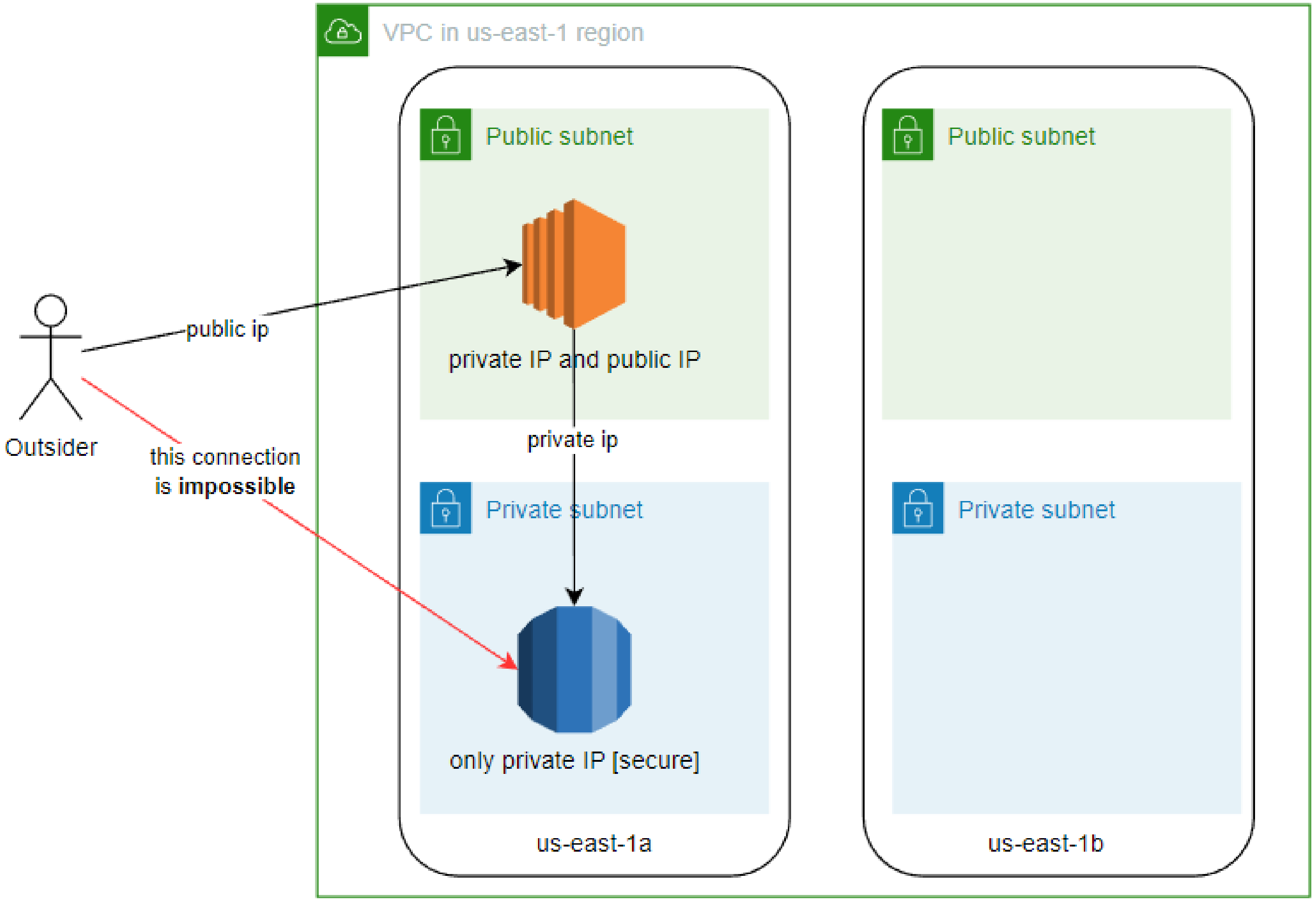
- A **VPC** is a logically isolated network in AWS.
- You can define **IP ranges**, subnets, route tables, and gateways.
- Each **AWS region** has multiple **Availability Zones (AZs)**, and a VPC can span multiple AZs.
- Default **AWS VPC** vs. Custom **VPC**

Subnets

- **Definition**: Subnets are subdivisions of a VPC that group resources within a specific IP address range.
- **Types**:
  - **Public Subnet**: Accessible from the internet (requires an Internet Gateway).
  - **Private Subnet**: Not directly accessible from the internet (uses a NAT Gateway/Instance for outbound traffic).
- **Association**: Each subnet is tied to a single Availability Zone (AZ).

Subnets

- **Public Requests**: Must pass VPC security layers (NACLs and Security Groups) on both the subnet and resource levels.
- **Private Subnet Access**: Direct public access is not allowed; access is only possible via public resources (e.g., bastion host or NAT Gateway).



Classless Inter-Domain Routing (CIDR)

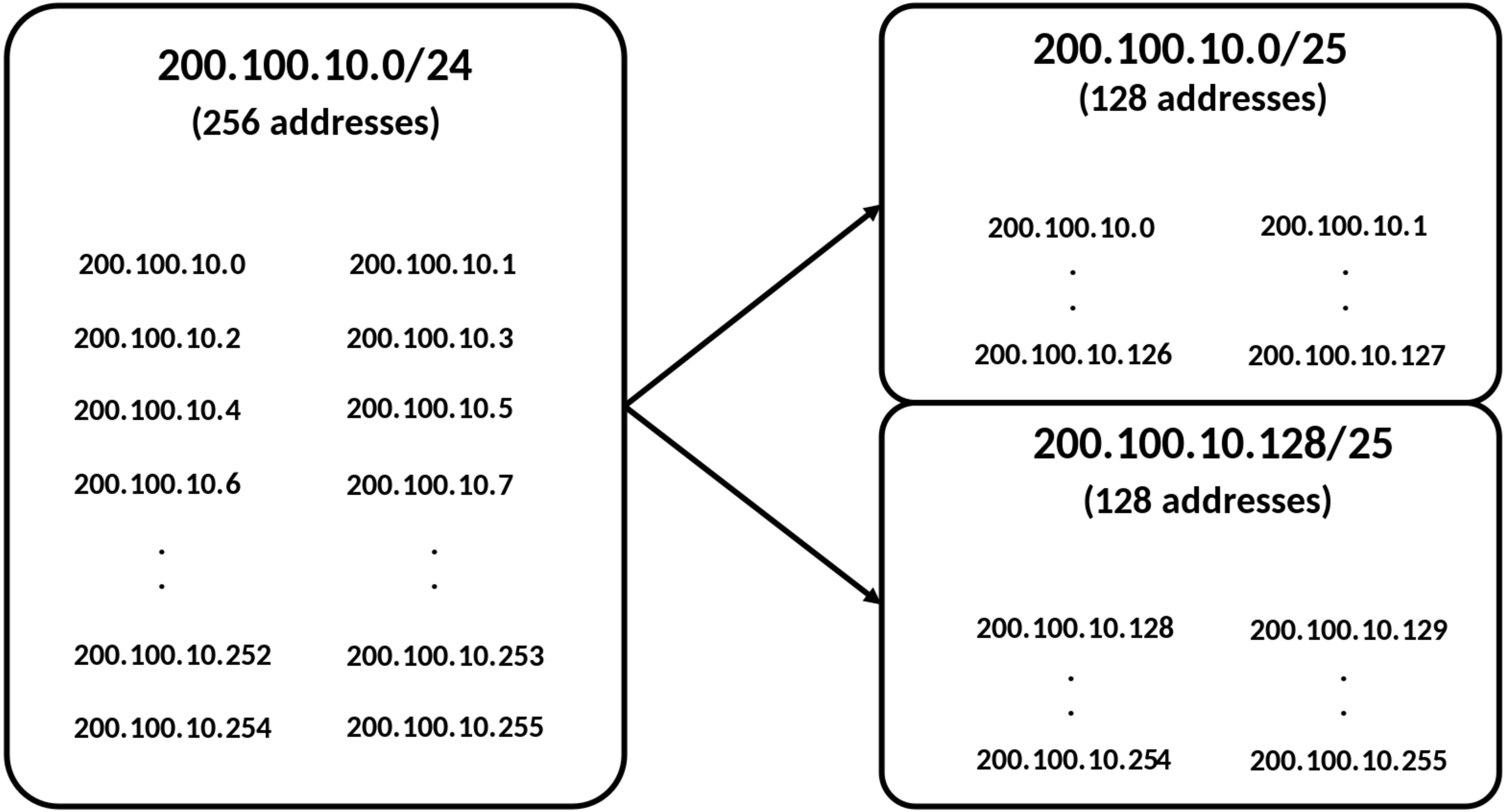
- CIDR is a method for allocating IP addresses and routing that replaced the class-based system.
- Notation: IP/prefix, in which prefix is number of bits in the network portion.
- **CIDR Block**: `192.168.0.0/26`.
  - **Subnet Mask**: `255.255.255.192`.
  - **Total IPs**: 64.
  - **Usable IPs**: 62 (2 reserved for network and broadcast).

VPC & Subnet - CIDR

- **VPC CIDR Block**:
  - When creating a VPC, you specify a **CIDR block** to define the range of private IP addresses for the VPC.
- **Subnet CIDR Block**:
  - Each subnet within a VPC gets a smaller CIDR block (a subset of the VPC CIDR).
  - AWS reserves the first 4 IPs and the last IP in each subnet for network and broadcast

Total address space

Partial address spaces



200.100.10.0/24

(256 addresses)

200.100.10.0	200.100.10.1
200.100.10.2	200.100.10.3
200.100.10.4	200.100.10.5
200.100.10.6	200.100.10.7
.	.
.	.
200.100.10.252	200.100.10.253
200.100.10.254	200.100.10.255

200.100.10.0/25

(128 addresses)

200.100.10.0	200.100.10.1
.	.
.	.
200.100.10.126	200.100.10.127

200.100.10.128/25

(128 addresses)

200.100.10.128	200.100.10.129
.	.
.	.
200.100.10.254	200.100.10.255

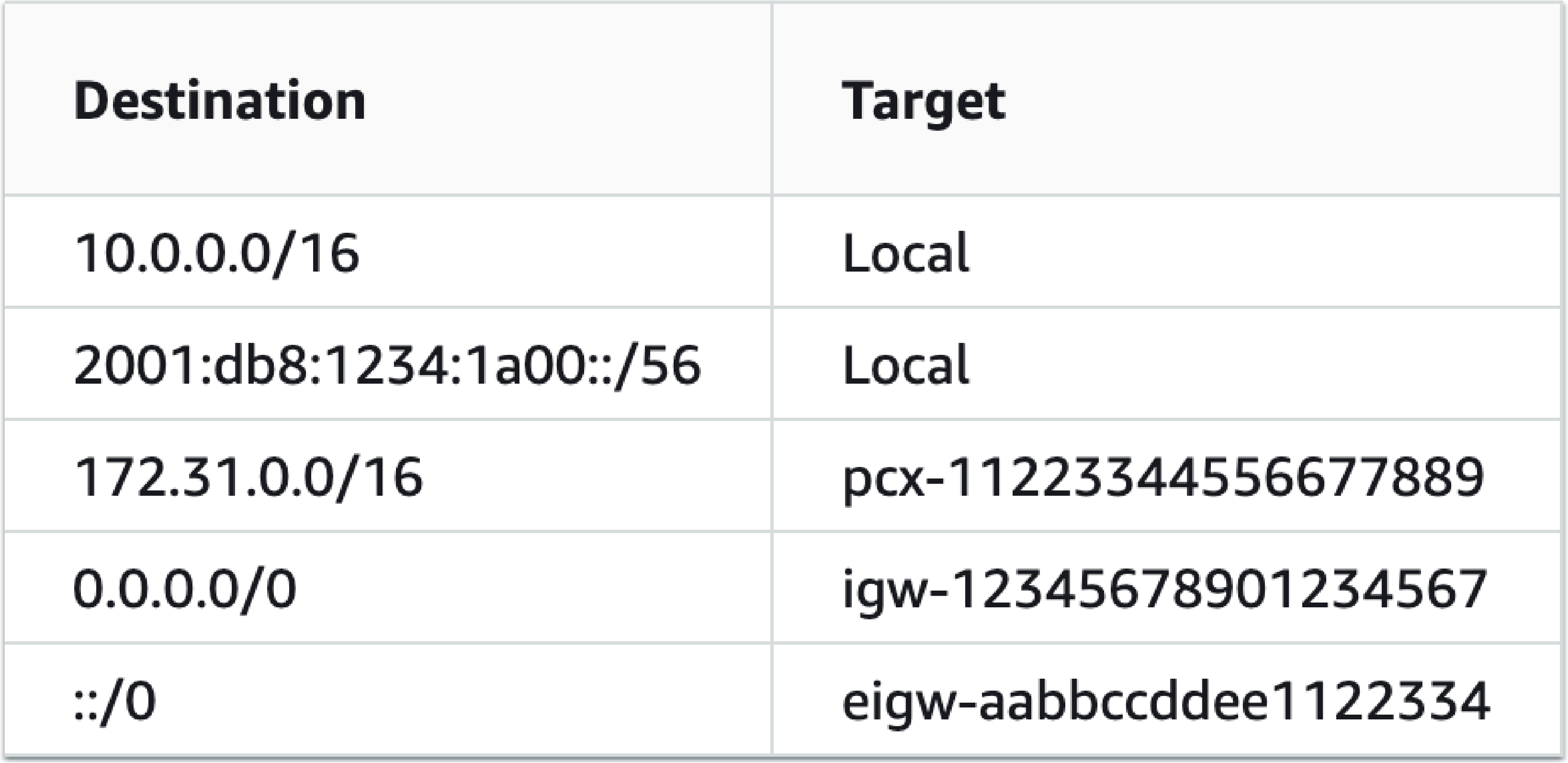
Before Subnetting

After Subnetting

Route tables

- **Definition**: Route tables define how network traffic is directed within a VPC and to external destinations.
- **Association**: Each subnet must be associated with a route table (explicitly or implicitly).
- **Rules**: Contain routes specifying destination IP ranges and target (e.g., IGW, NAT Gateway, VGW).
- **Default Route Table**: Automatically created for each VPC, directing local traffic within the VPC.

Route Tables

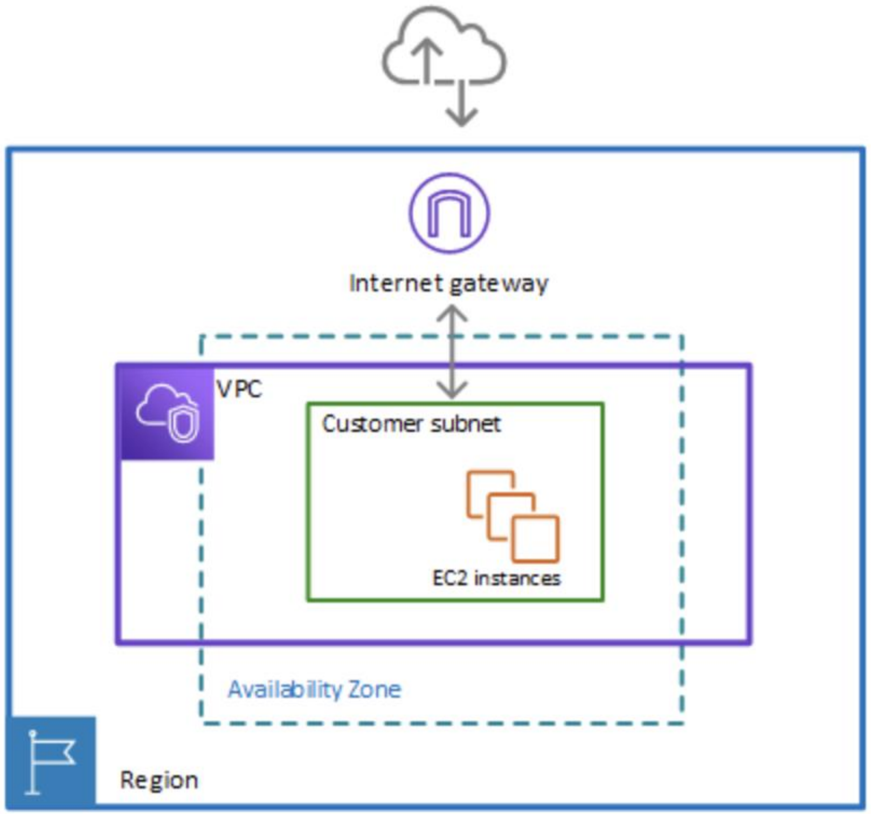


Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

Internet Gateway (IGW)

- **Definition**: A horizontally scaled, highly available gateway that allows VPC resources in public subnets to access the internet.
- **Purpose**: Enables two-way communication between VPC resources and the internet.
- **Attachment**: Must be explicitly attached to a VPC.
- **Routing**: Requires a route in the route table pointing to the IGW for internet-bound traffic.
- **Use Case**: Provides internet access for public-facing applications or services.

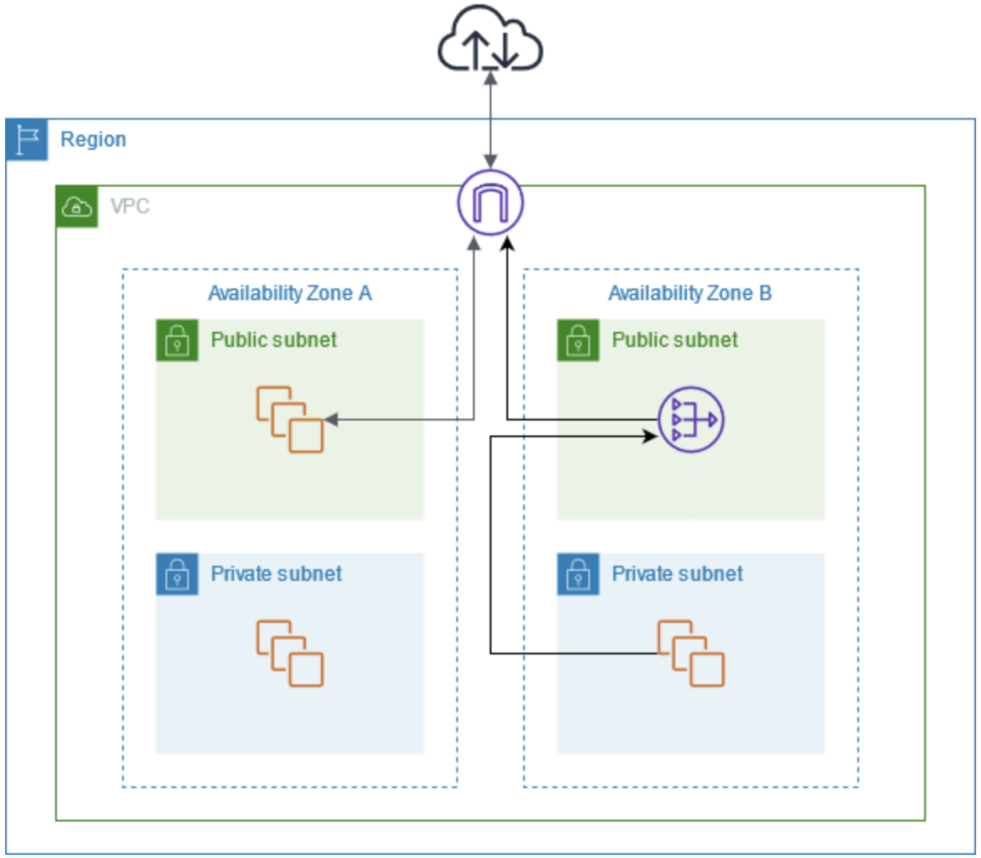
Internet Gateway (IGW)



NAT Gateway

- **Definition**: A managed AWS service that allows resources in private subnets to access the internet or other AWS services while keeping them inaccessible from the internet.
- **Purpose**: Facilitates outbound internet traffic for private resources without exposing them to inbound internet traffic.
- **Deployment**: Must be in a public subnet with an Elastic IP assigned.
- **Routing**: Requires a route in the private subnet's route table pointing to the NAT Gateway.
- **Use Case**: Enables private instances to download updates or communicate with external services securely.

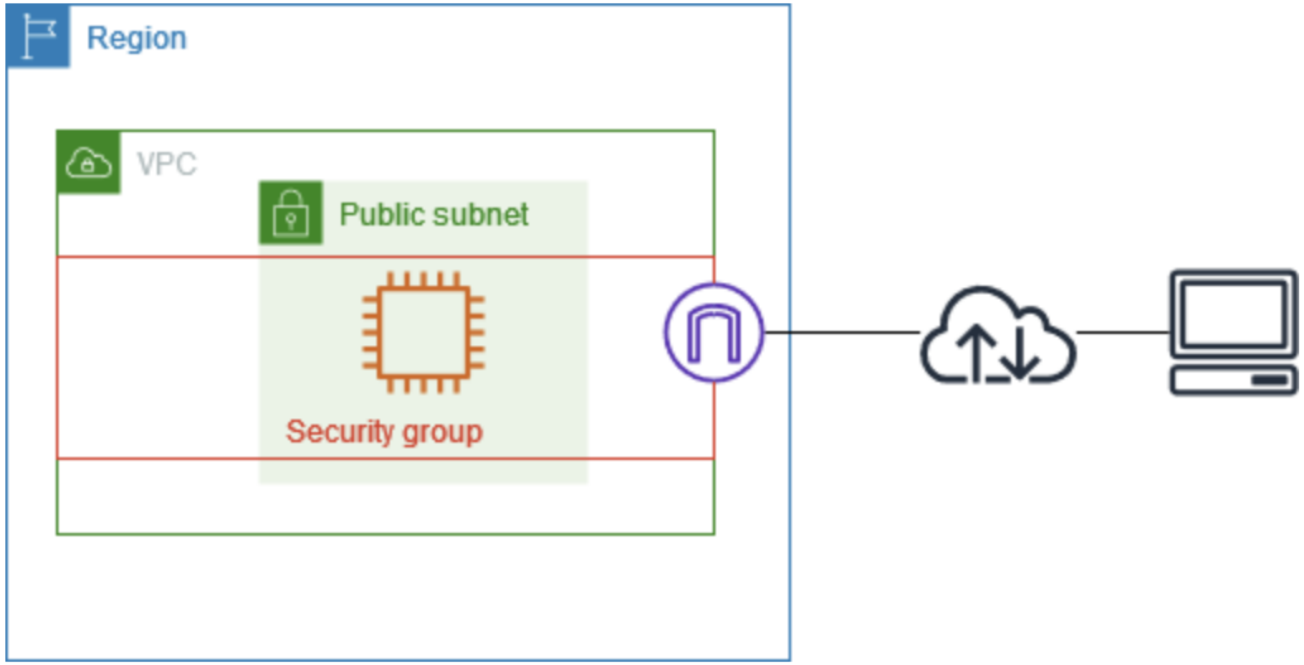
NAT Gateway


Region
VPC
Availability Zone A
Public subnet
Private subnet
Availability Zone B
Public subnet
Private subnet

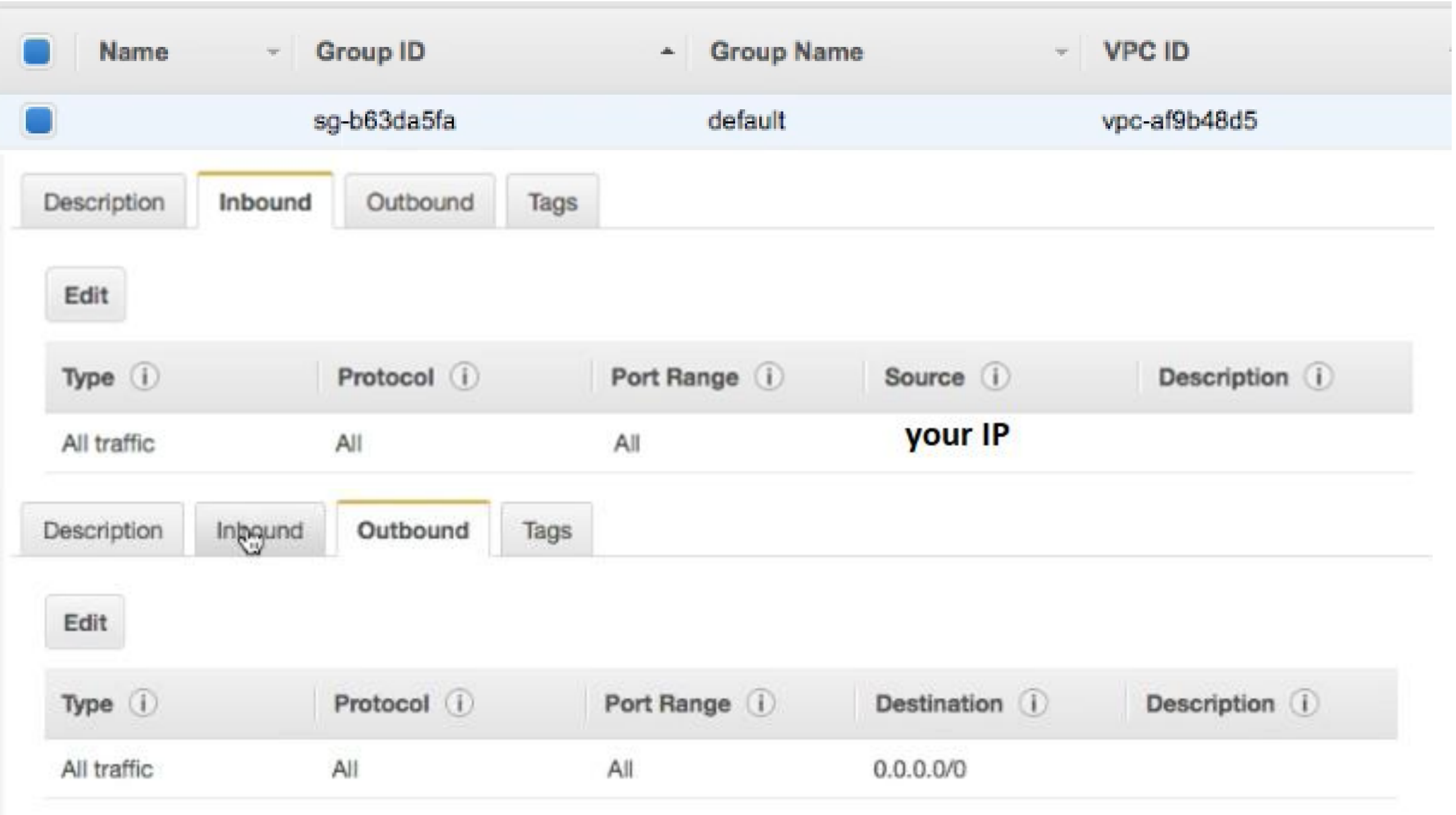
Security Group

- **Definition**: A virtual firewall at the instance level that controls inbound and outbound traffic.
- **Stateful (Automatic Response)**: Automatically allows response traffic for allowed inbound or outbound connections.
- **Rules**: Only supports allow rules; no deny rules.
- **Default Behavior**:
  - All inbound traffic is denied by default.
  - All outbound traffic is allowed by default.
- **Attachment**: Can be associated with one or more instances.
- **Collective Processing**:
  - Security groups evaluate all rules **together**, not sequentially.
  - If any rule allows the traffic, it is permitted. If no rule allows it, the traffic isdenied by default.

Security Group



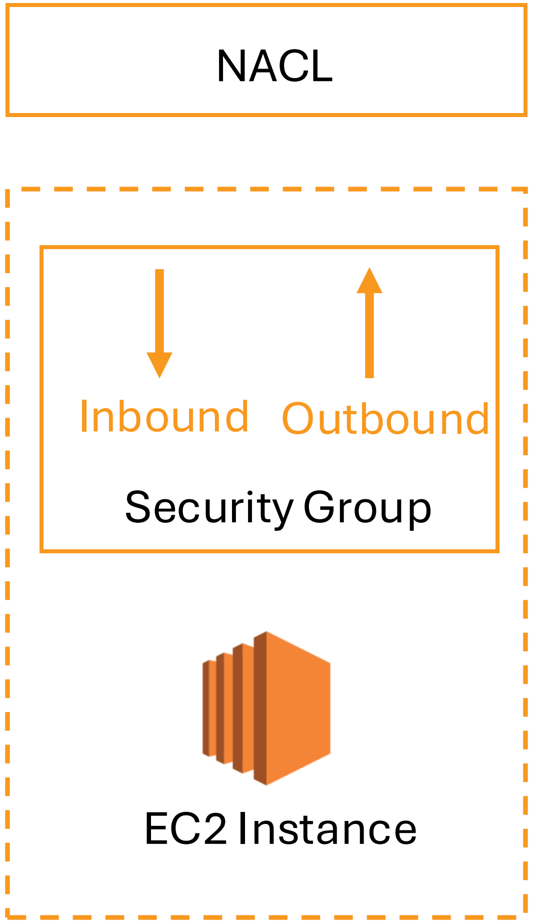
Inbound/Outbound Rules



Name	Group ID	Group Name	VPC ID
	sg-b63da5fa	default	vpc-af9b48d5

Type	Protocol	Port Range	Source	Description
All traffic	All	All	your IP	

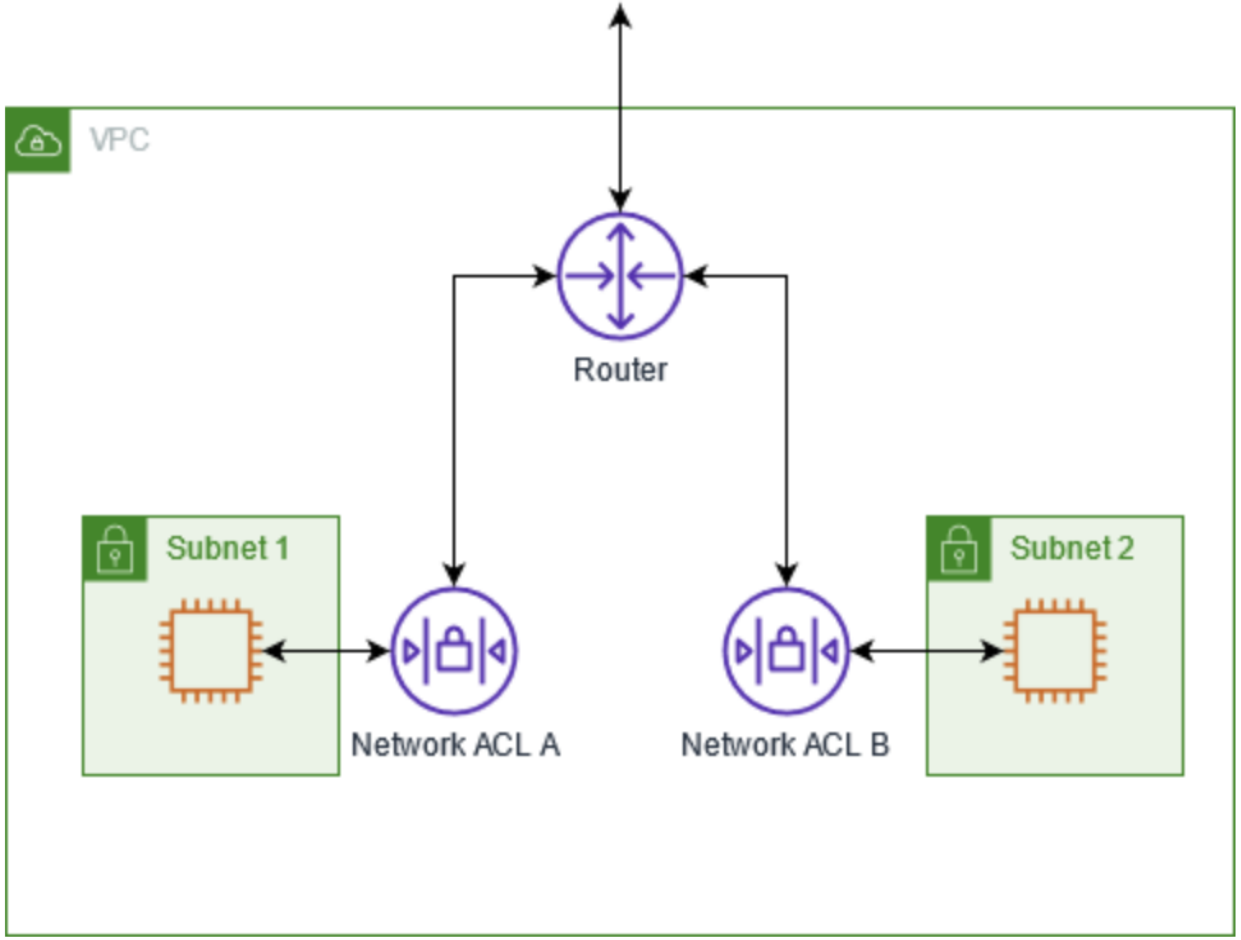
Type	Protocol	Port Range	Destination	Description
All traffic	All	All	0.0.0.0/0	



Network Access Control List (NACL)

- **Definition**: A stateless firewall at the subnet level that controls inbound and outbound traffic.
- **Stateless**: Requires explicit rules for both incoming and outgoing traffic.
- **Rules**: Supports both allow and deny rules, evaluated in numerical order.
- **Default Behavior**:
  - Default NACL allows all inbound and outbound traffic.
  - Custom NACL denies all traffic by default until rules are added.
- **Attachment**: Automatically associated with subnets.
- **Use Case**: Provide an additional layer of security for subnet traffic.

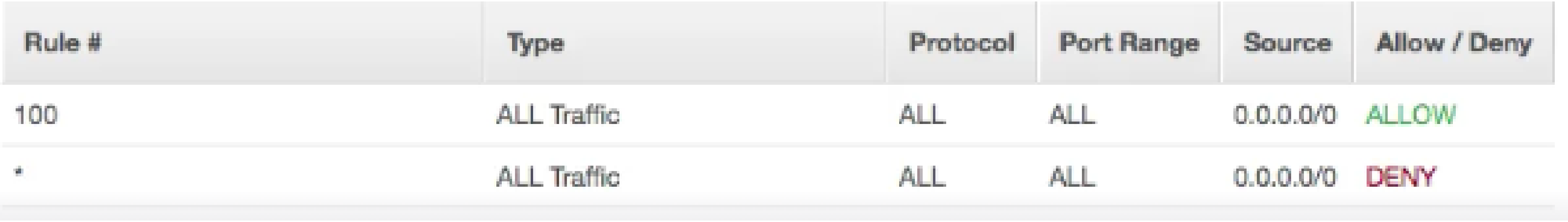
VPC Security Layers



NACL Rules

- Rules are evaluated from lowest to highest based on rule numbers. The first rule found that applies to the traffic type is immediately applied, regardless of any rules that come after it.
- You must explicitly define both **allow** and **deny** rules for inbound and outbound traffic.

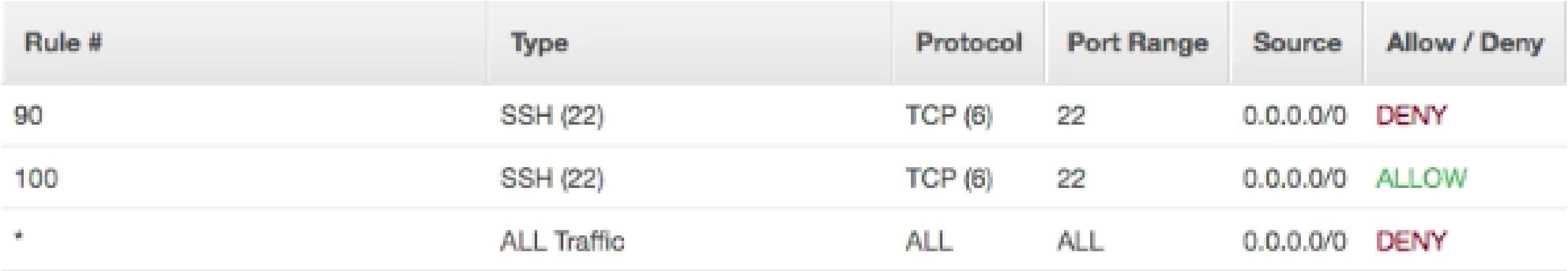
Inbound



Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

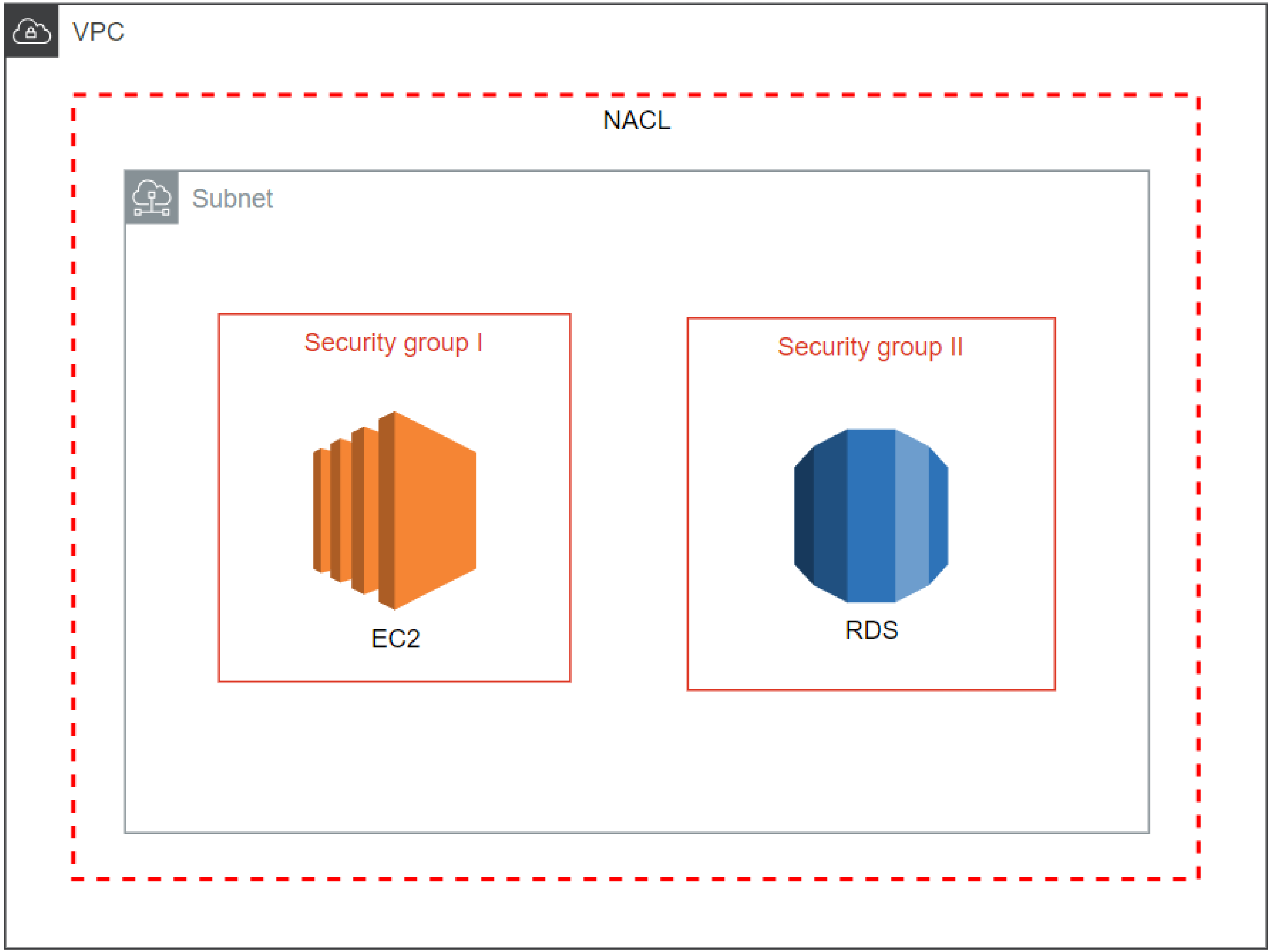
All traffic is allowed

Inbound



Rule #	Type	Protocol	Port Range	Source	Allow / Deny
90	SSH (22)	TCP (6)	22	0.0.0.0/0	DENY
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

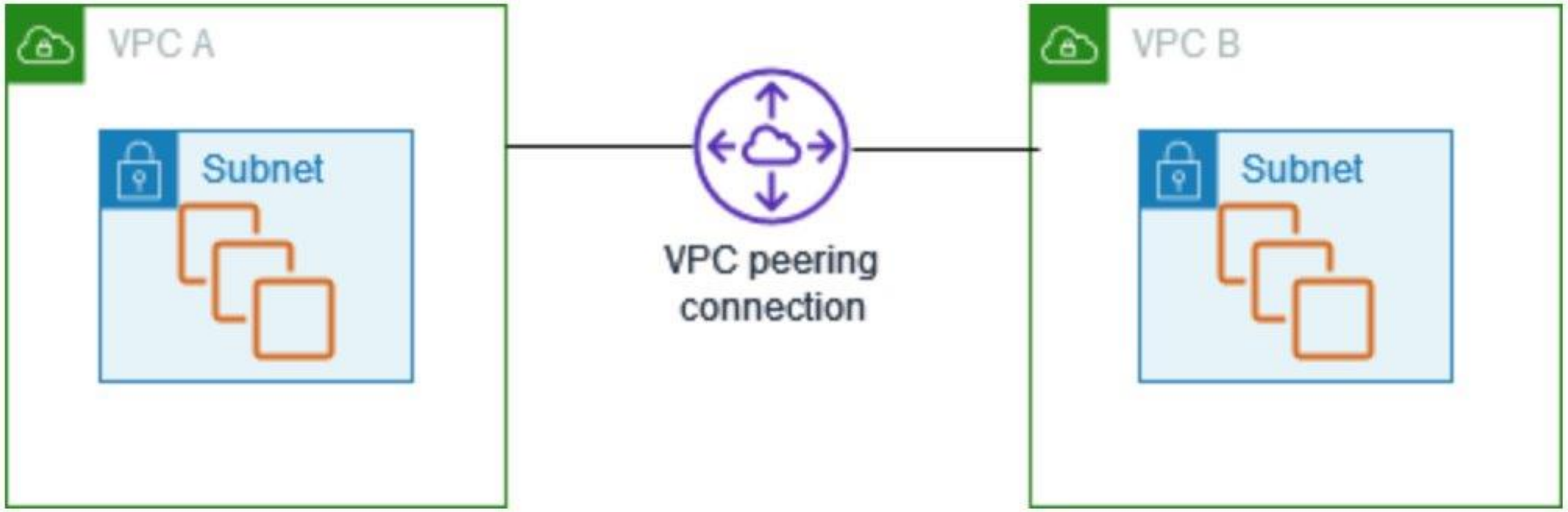
All traffic is denied


VPC
NACL
Subnet
Security group I
EC2
Security group II
RDS

VPC Peering

- **Definition**: A private network connection between two VPCs to enable secure communication without using the public internet.
- **Scope**: Can connect VPCs within the same AWS account or across different accounts, even in different regions (inter-region peering).
- **Traffic**: Peered VPCs communicate directly using private IP addresses.
- **Routing**: Requires route table updates to direct traffic between the VPCs.
- **Limitations**: No transitive peering (VPC A cannot communicate with VPC C through VPC B).
- **Use Case**: Share resources, such as databases or services, between VPCs securely.

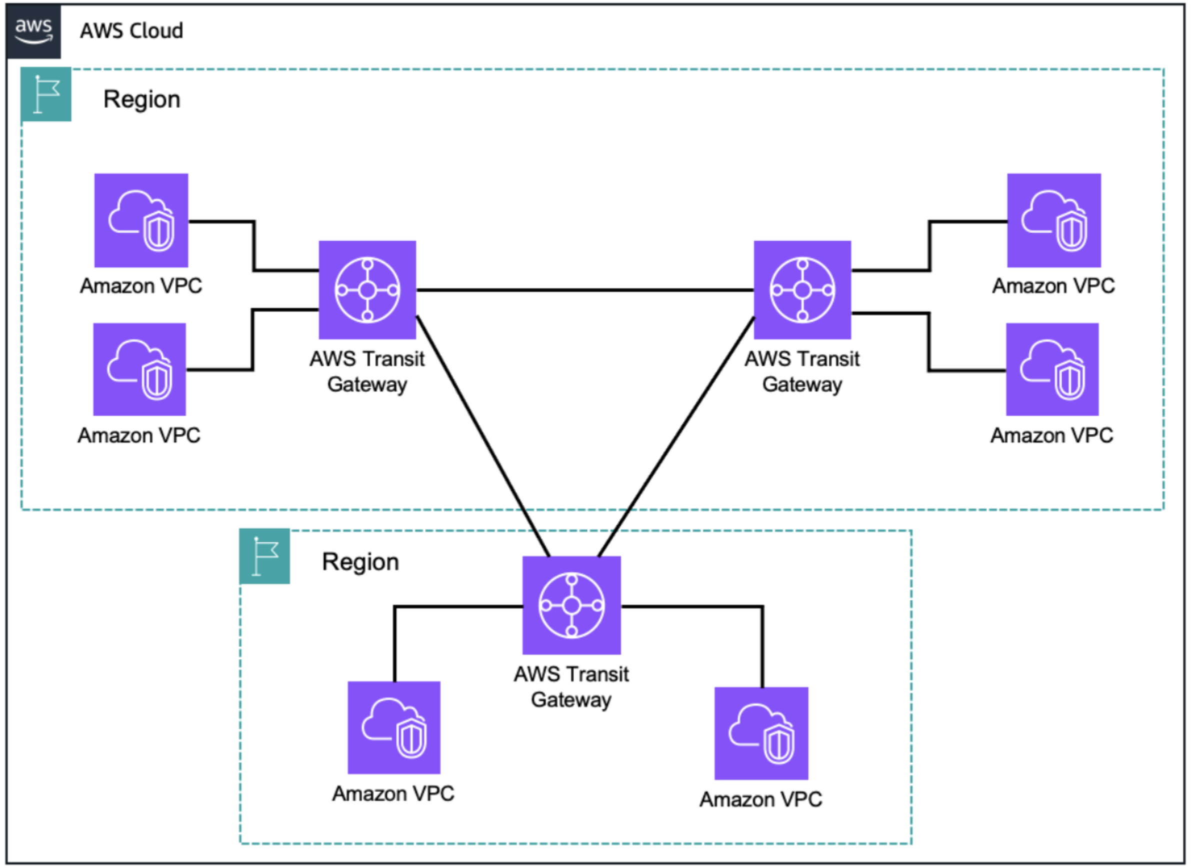
VPC Peering



Transit Gateway

- **Definition**: A central hub that connects multiple VPCs and on-premises networks to simplify network architecture.
- **Scope**: Supports communication across multiple VPCs, accounts, and regions (multi-region peering).
- **Routing**: Manages traffic flow using route tables for connected networks.
- **Scalability**: Highly scalable, supporting thousands of VPCs and VPN connections.
- **Transitive Routing**: Allows communication between connected networks (e.g., VPC A to VPC B via Transit Gateway).
- **Use Case**: Simplifies large-scale hybrid or multi-VPC architectures.

Transit Gateway



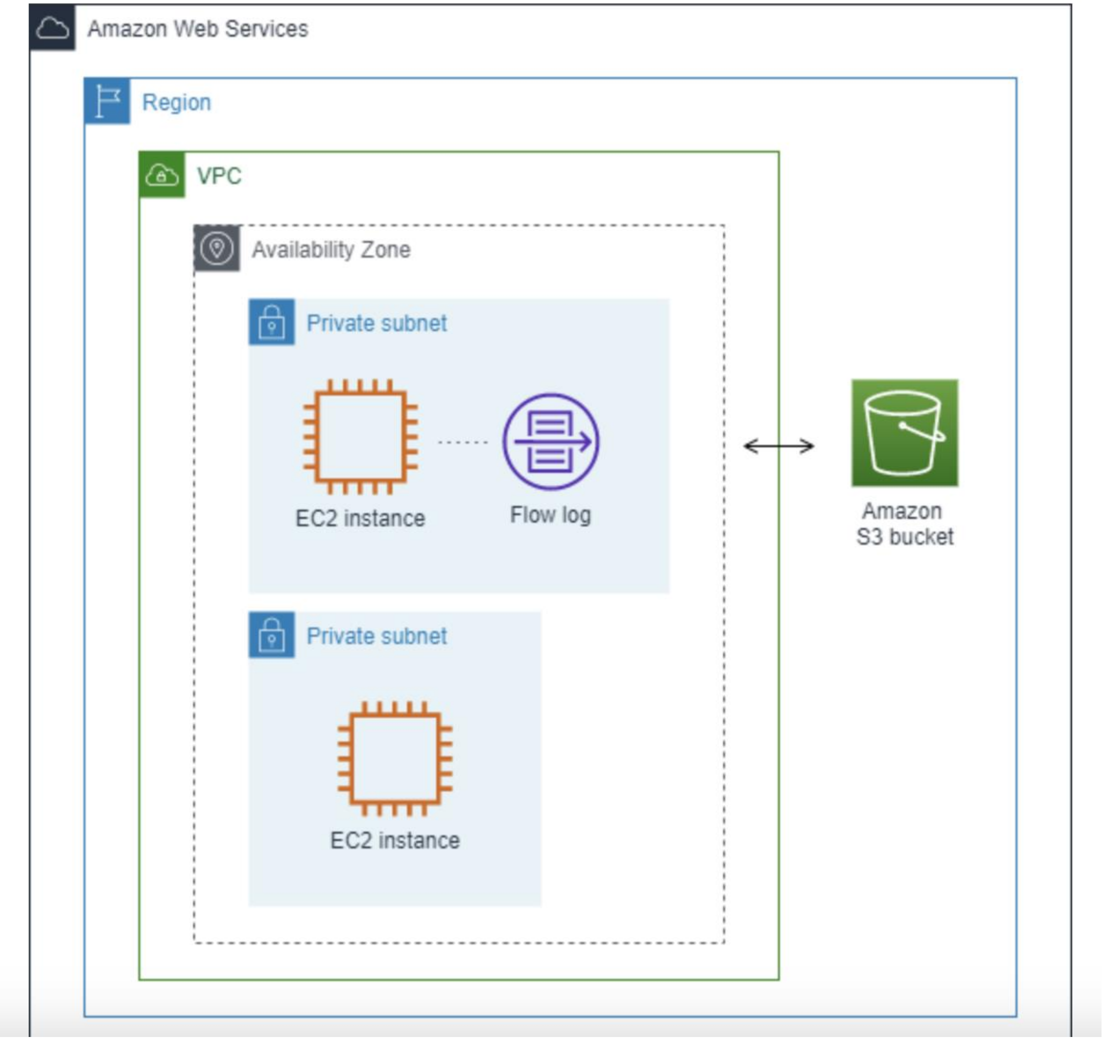
VPC Peering vs. Transit Gateways

- Choose the right architecture:
  - Network Complexity: Number of VPCs
  - Cross-region connectivity: Intra-region vs. Inter-region
  - Connection:
    - VPC Peering: No cost for connections
    - Transit Gateways: Fee per VPC attachment ($0.005)

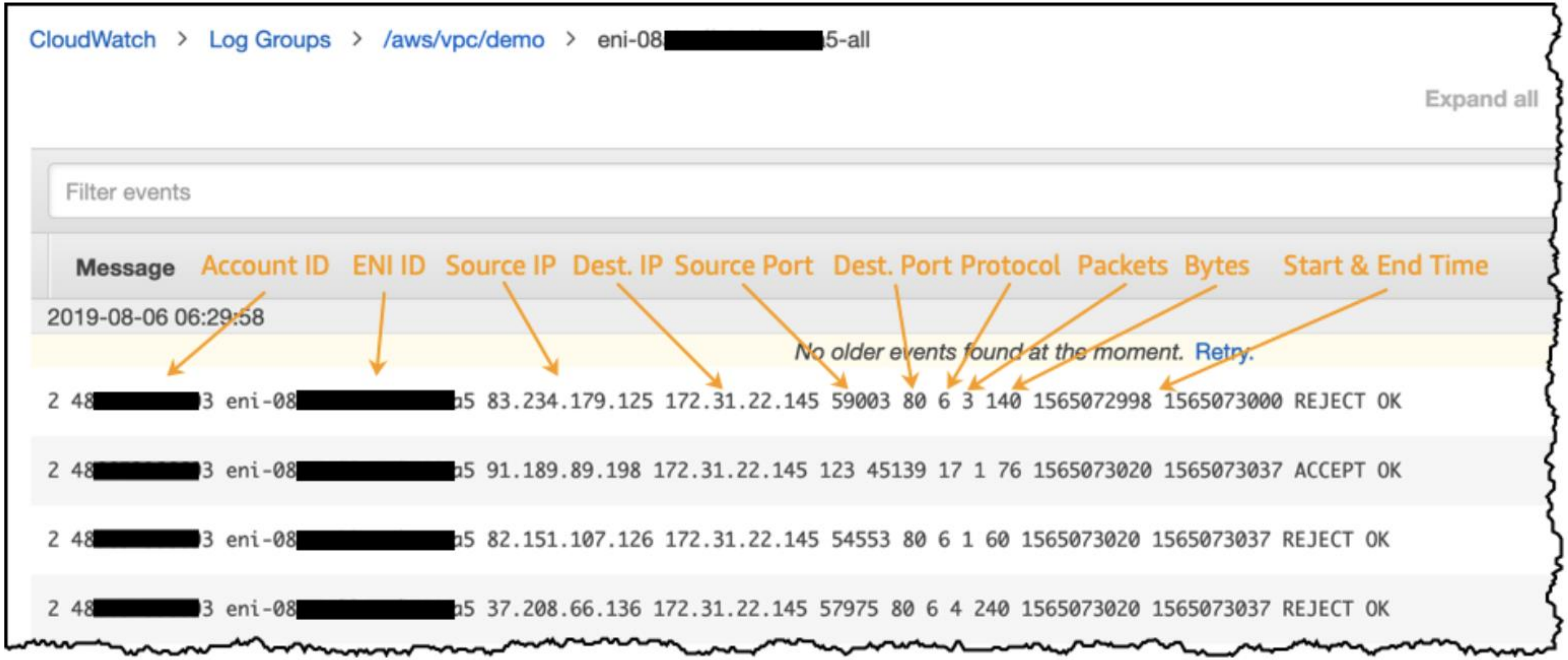
VPC Flow logs

- **Definition**: A feature that captures network traffic information within a VPC for monitoring and troubleshooting.
- **Scope**: Logs traffic at the VPC, subnet, or network interface level.
- **Details Captured**: Source/destination IPs, traffic type, port, and action (accept or reject).
- **Storage**: Logs can be sent to Amazon CloudWatch Logs or S3 for analysis.
- **Use Case**: Helps monitor network traffic, diagnose connectivity issues, and enhance security.
- **Limitations**: Does not capture all traffic (e.g., DNS traffic to Amazon DNS resolver).

VPC Flow Logs



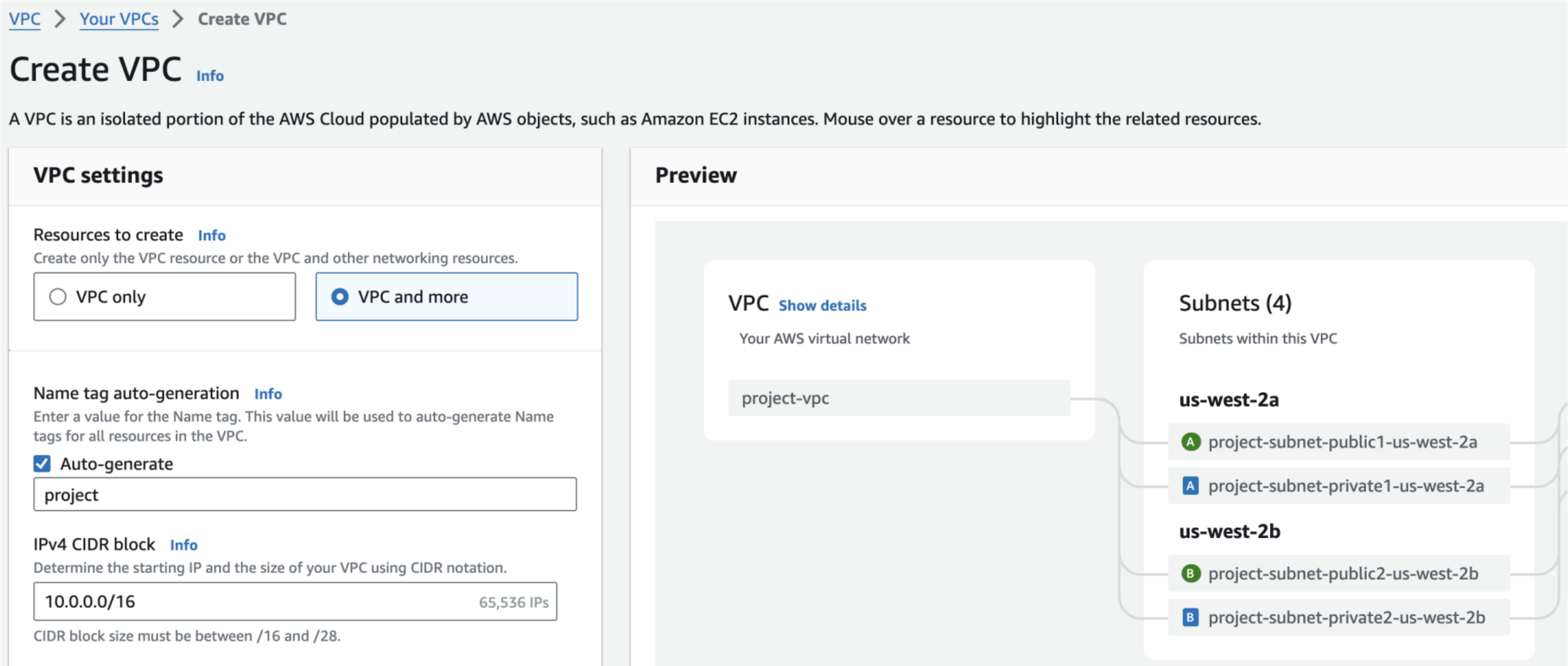
VPC Flow Logs



```
2 48[redacted]3 eni-08[redacted]a5 83.234.179.125 172.31.22.145 59003 80 6 3 140 1565072998 1565073000 REJECT OK
2 48[redacted]3 eni-08[redacted]a5 91.189.89.198 172.31.22.145 123 45139 17 1 76 1565073020 1565073037 ACCEPT OK
2 48[redacted]3 eni-08[redacted]a5 82.151.107.126 172.31.22.145 54553 80 6 1 60 1565073020 1565073037 REJECT OK
2 48[redacted]3 eni-08[redacted]a5 37.208.66.136 172.31.22.145 57975 80 6 4 240 1565073020 1565073037 REJECT OK
```

VPC

- Demo



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

○ VPC only ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

project

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

Preview

VPC Show details

Your AWS virtual network

project-vpc

Subnets (4)

Subnets within this VPC

us-west-2a

A project-subnet-public1-us-west-2a

A project-subnet-private1-us-west-2a

us-west-2b

B project-subnet-public2-us-west-2b

B project-subnet-private2-us-west-2b

Amazon Route 53

- A highly available and scalable cloud Domain Name System (DNS) service designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications.
- Connect user requests to infrastructure running in AWS, such as EC2, ELB, S3, etc.
- Can be used to route users to infrastructure outside of AWS.

Amazon Route 53

- Domain Registration: Purchase and manage domains in Route 53
- DNS Service: Convert domain names into IP addresses
- Routing Policies: Determine how Route 53 responds to DNS queries.
- Health Check: Route 53 performs health checks on specified resources (e.g., web servers, email servers).
- DNS Failover: Increase the availability by redirecting traffic to healthy endpoints or to a static site if all endpoints fail.

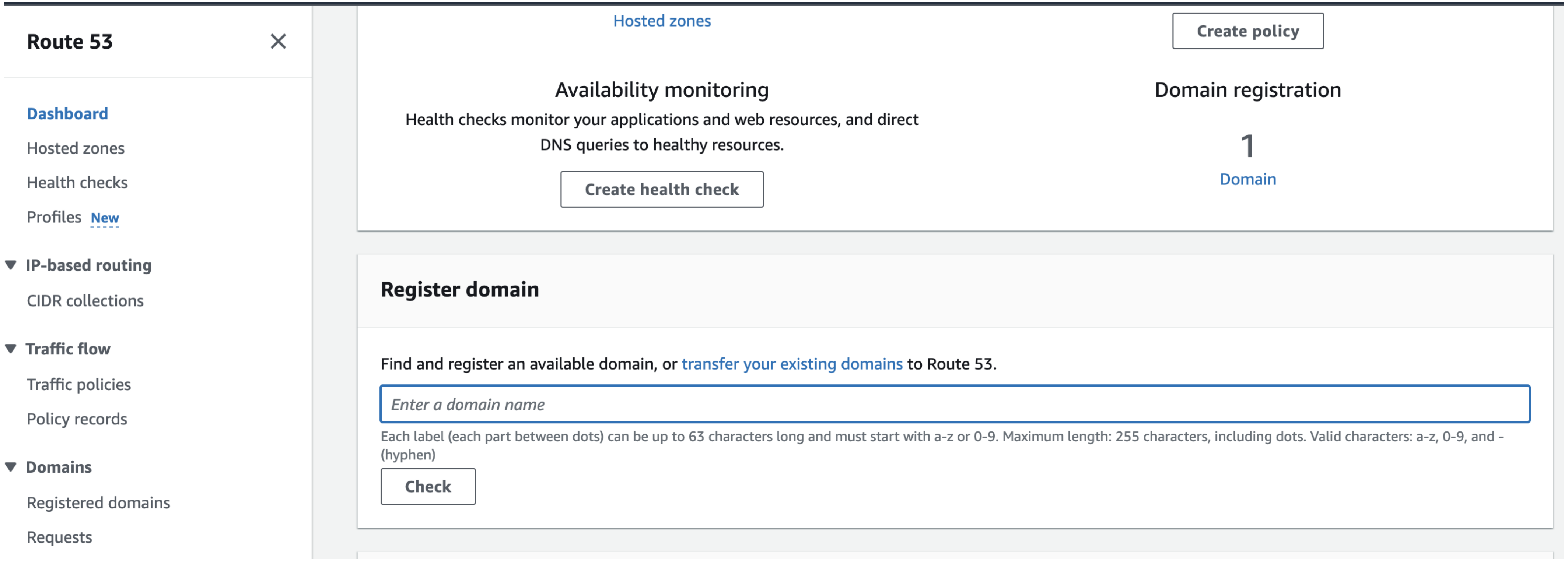
Amazon Route 53

- **Simple Routing**: Single resource; straightforward response (e.g., one IP address).
- **Weighted Routing**: Distributes traffic by weight (e.g., 70% to Server A, 30% to Server B).
- **Latency-Based Routing**: Directs users to the resource with the lowest network latency.
- **Geolocation Routing**: Routes traffic strictly based on the user’s geographic location (e.g., country/region).
- **Geoproximity Routing**: Routes traffic to resources closest to users, with optional bias to specific regions).
- **Failover Routing**: Routes to a primary resource, switching to a secondary in case of failure.
- **Multi-Value Answer Routing**: Returns multiple healthy resource values for load balancing and redundancy.
- **IP-Based Routing**: Routes traffic based on the client’s IP address (used with services like Global Accelerator).

Amazon Route 53 – Hosted Zone

- A **Hosted Zone** is a container for DNS records that define how traffic is routed for a specific domain
- **Public Hosted Zone**: Routes traffic on the internet for a domain and its subdomains.
- **Private Hosted Zone**: Routes traffic within a private Amazon VPC.
- **DNS Records**:
  - **A Record**: Maps domain to IPv4.
  - **AAAA Record**: Maps domain to IPv6.
  - **CNAME**: Maps domain to another domain name.
  - **MX**: Mail exchange record for email.
  - Others: TXT, SRV, NS, etc.
- **Scalability & Reliability**:
  - Supports health checks and failover.
  - Integrates with AWS services like ELB, S3, and CloudFront.
- **Cost**:
  - First 25 hosted zones: $0.50 per hosted zone per month.
  - Additional hosted zones: $0.10 per hosted zone per month.

Amazon Route 53



Availability monitoring

Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

Domain registration

1

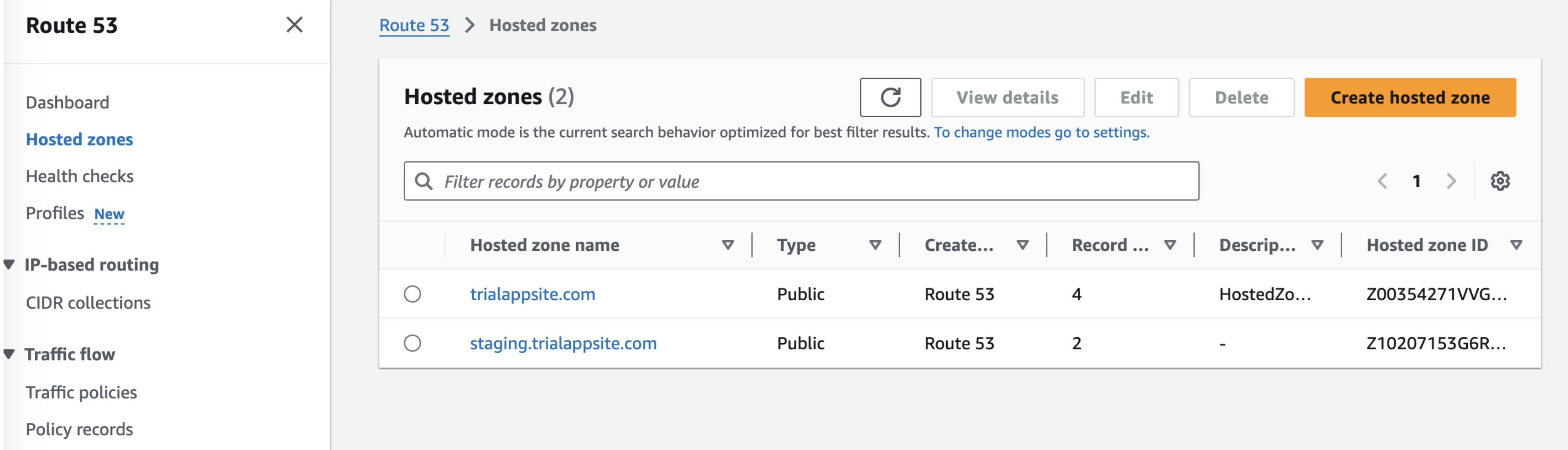
Domain

Register domain

Find and register an available domain, or transfer your existing domains to Route 53.

Each label (each part between dots) can be up to 63 characters long and must start with a-z or 0-9. Maximum length: 255 characters, including dots. Valid characters: a-z, 0-9, and - (hyphen)

Route 53 - Hosted Zone



Hosted zones (2)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

	Hosted zone name	Type	Create...	Record ...	Descrip...	Hosted zone ID
○	trialappsite.com	Public	Route 53	4	HostedZo...	Z00354271VVG...
○	staging.trialappsite.com	Public	Route 53	2	-	Z10207153G6R...

References

- https://docs.aws.amazon.com/
- ChatGPT: https://chatgpt.com/
- Google AI: https://gemini.google.com/app