Networking

Thao Huy Vu

Maharishi International University - Fairfield, Iowa

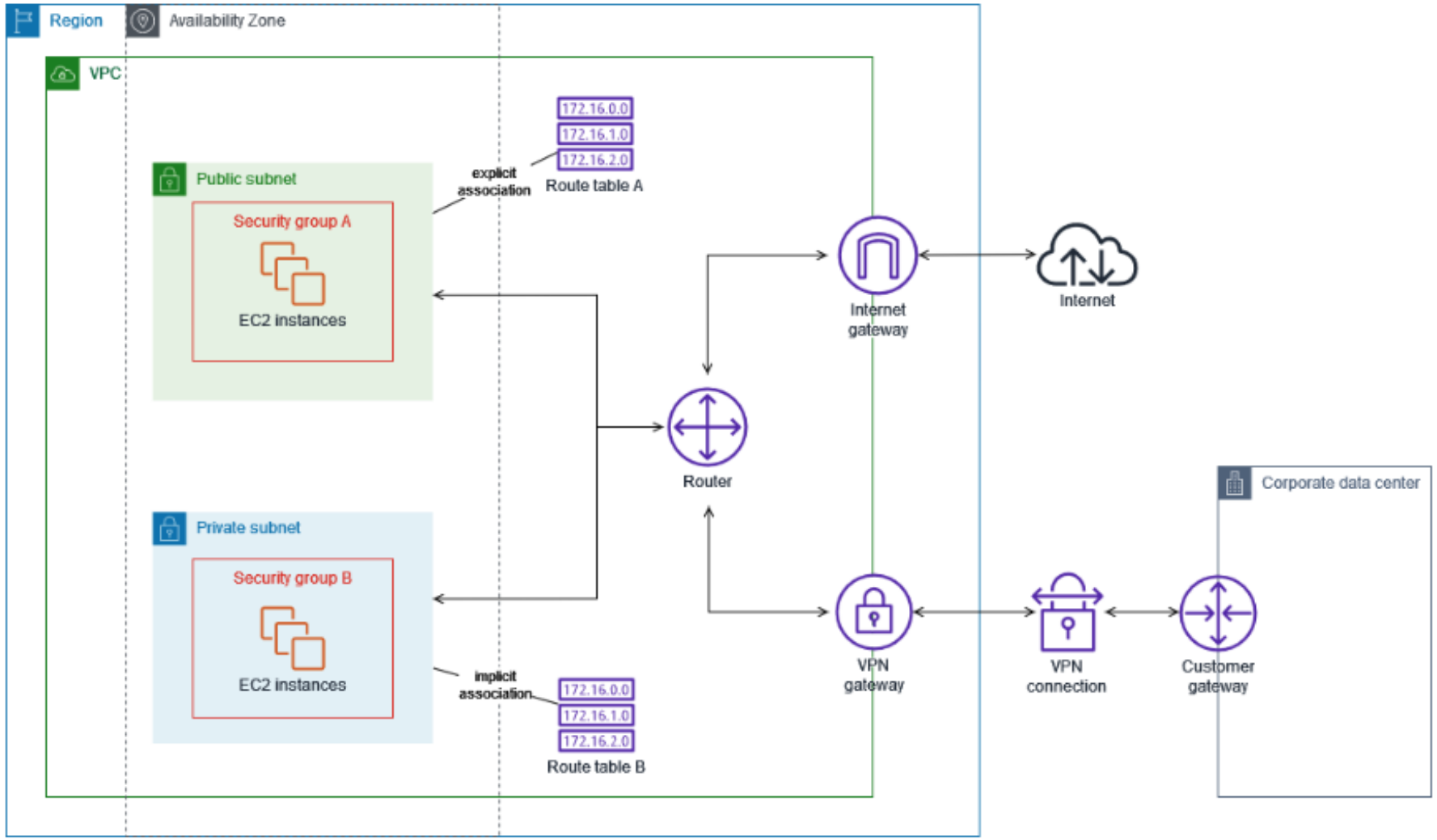
Agenda

- VPC
- Subnet
- EC2

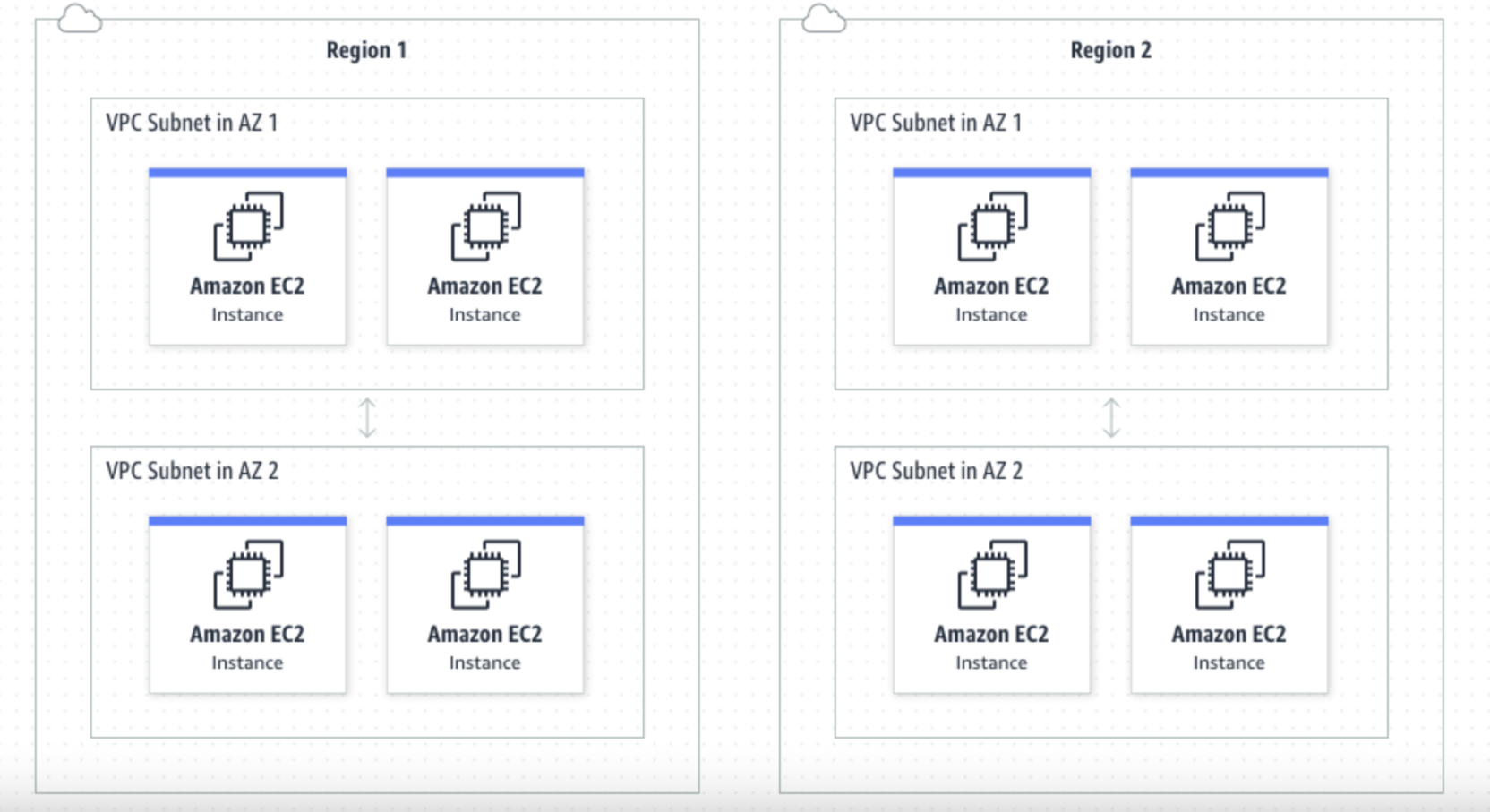
Networking Components

- **VPC**
- **Subnets**
- **Route Tables**
- **Internet Gateway (IGW)**
- **Security Groups (SGs)**

VPC


Region
Availability Zone
VPC
172.16.0.0
172.16.1.0
172.16.2.0
Public subnet
explicit association
Route table A
Security group A
EC2 instances
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

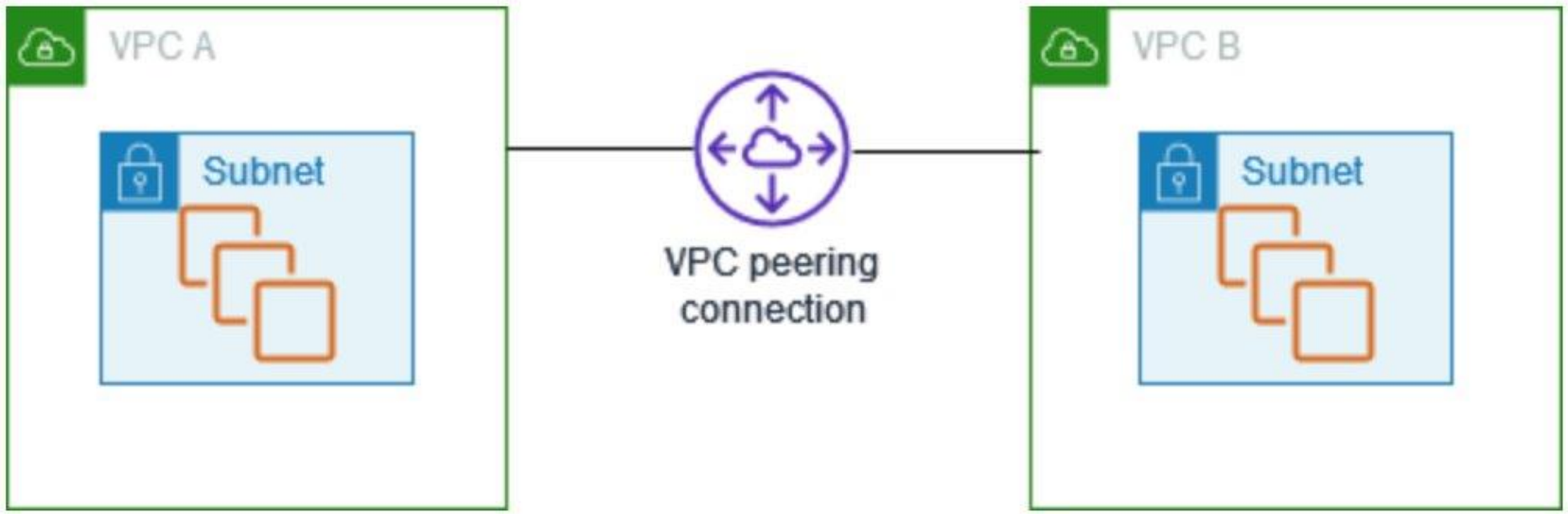
VPC


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**

VPC Peering

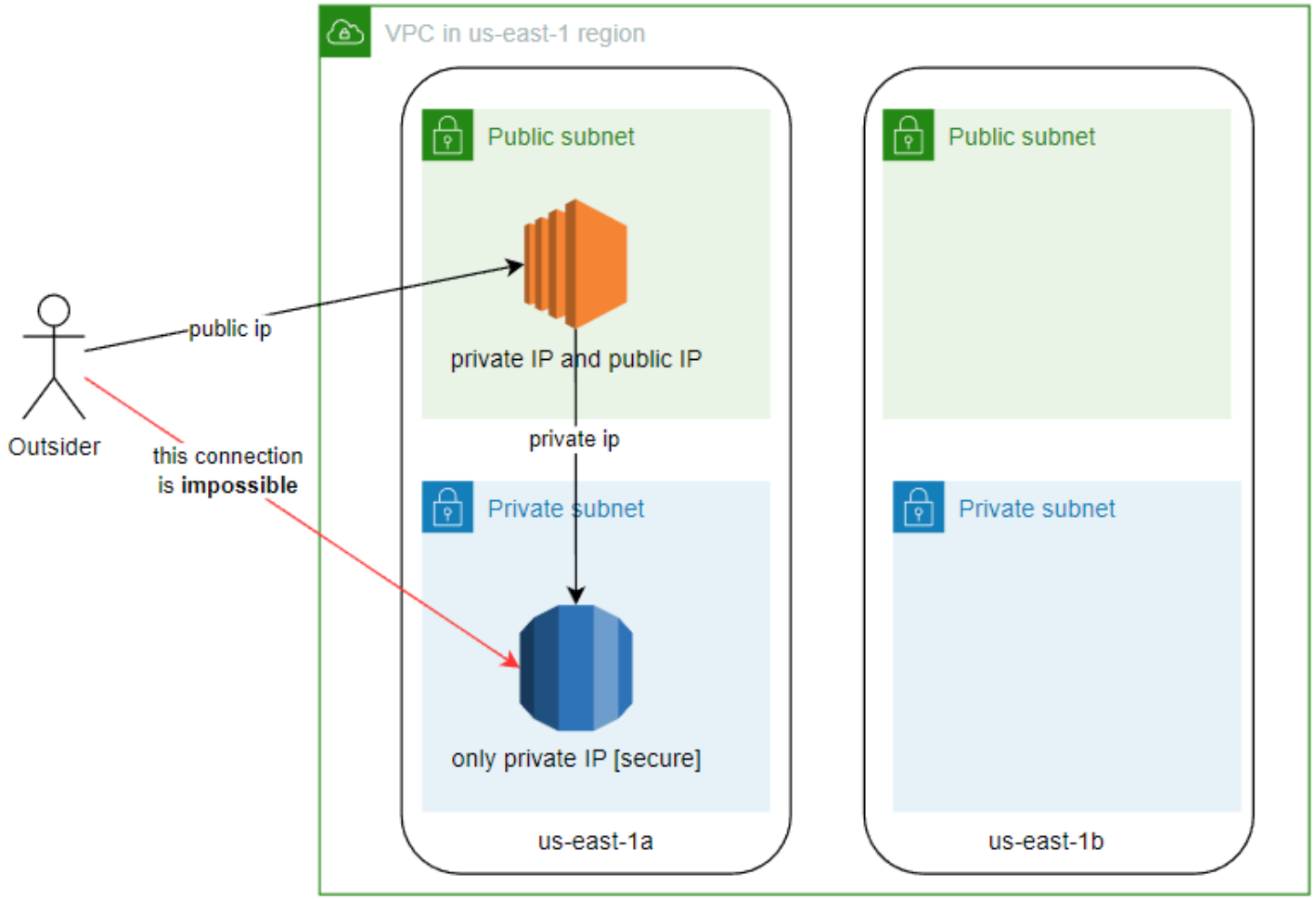


Subnets

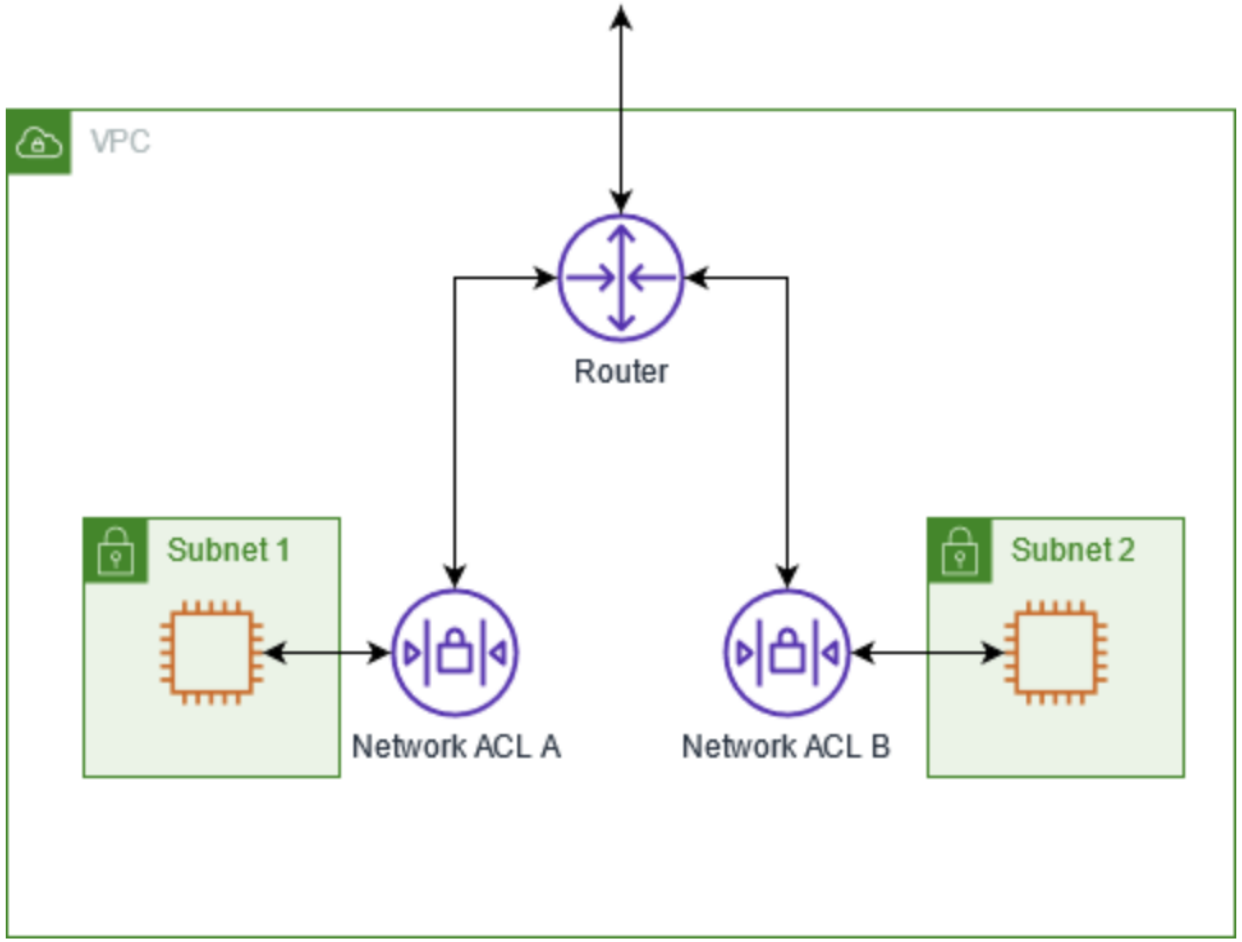
- **Definition**: Subnets are subdivisions of a VPC that group resources within a specific IP address range.
- **Types**:
  - **Public Subnet**: Accessible from the internet (requires an Internet Gateway).
  - **Private Subnet**: Not directly accessible from the internet (uses a NAT Gateway/Instance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

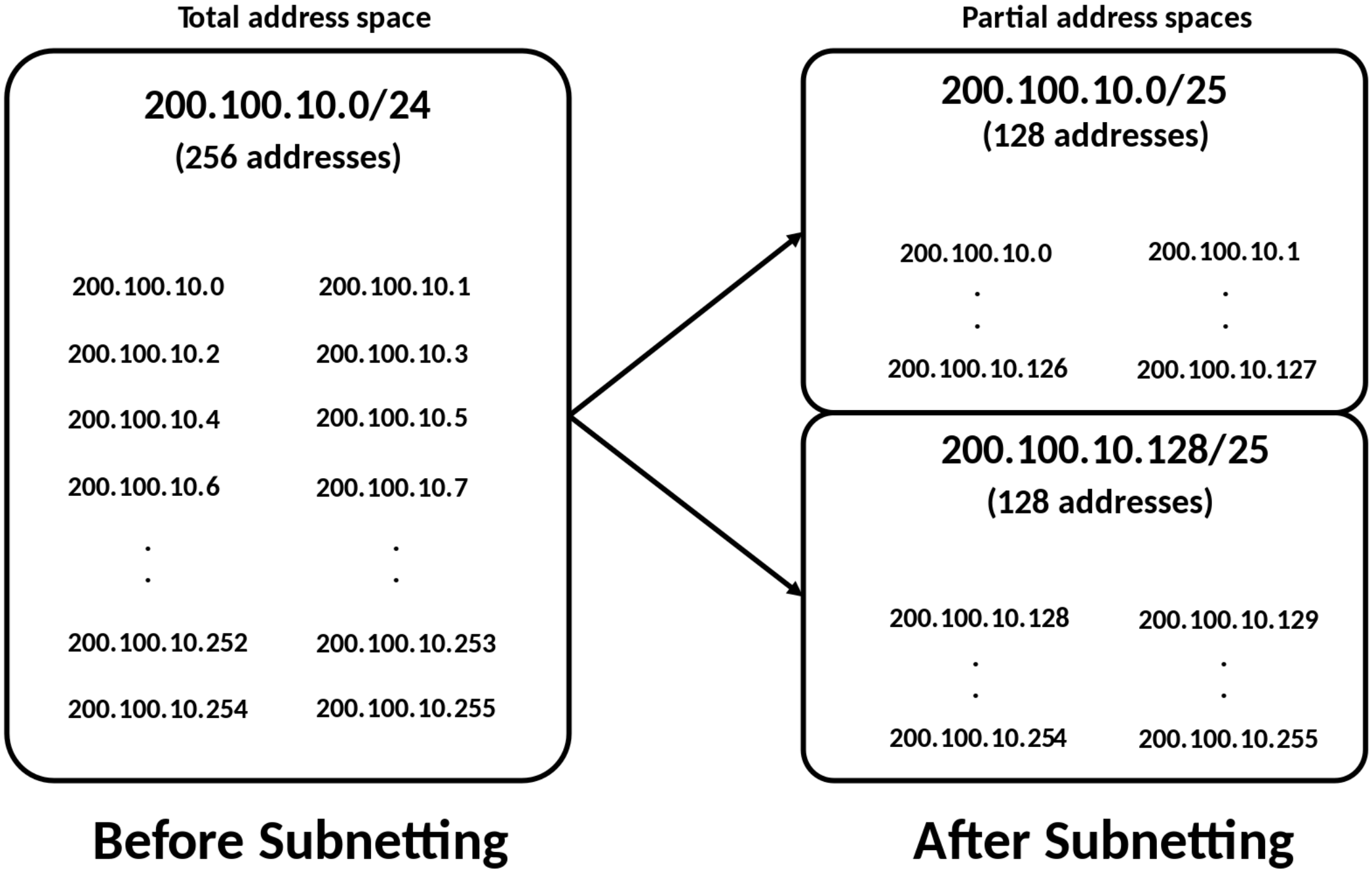
Subnets

- **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).

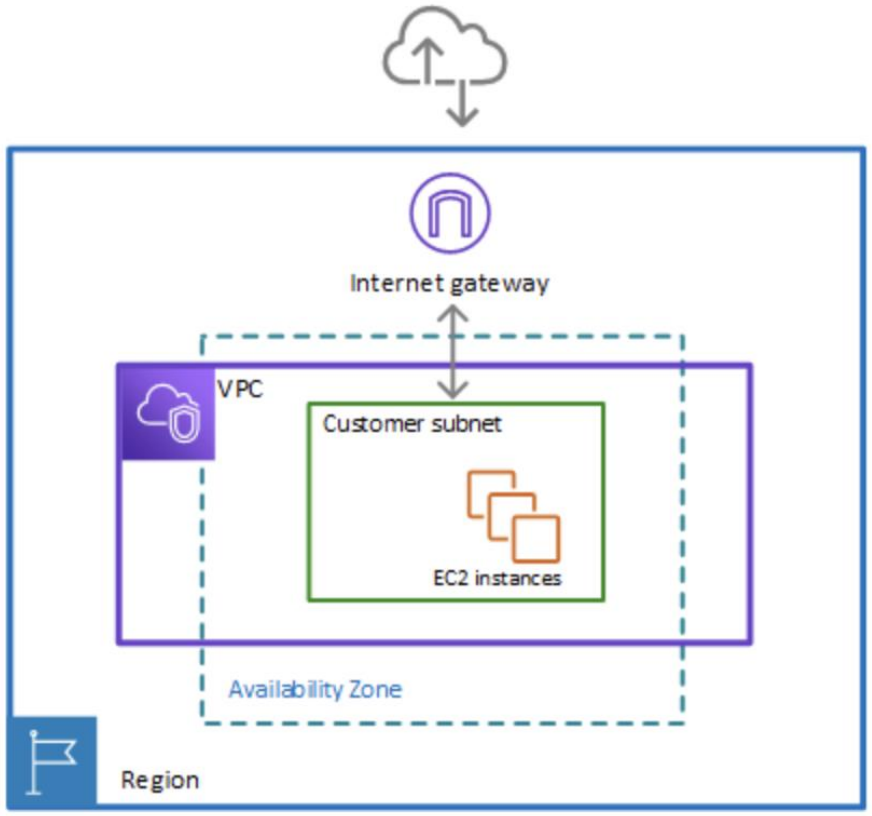


Subnet Security




Total address space
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
Partial address spaces
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

Internet Gateway (IGW)



Route Tables

- **Controls how traffic is routed** inside a VPC.
- Each subnet must be associated with **a route table**.
- A **default route table** exists but can be customized.

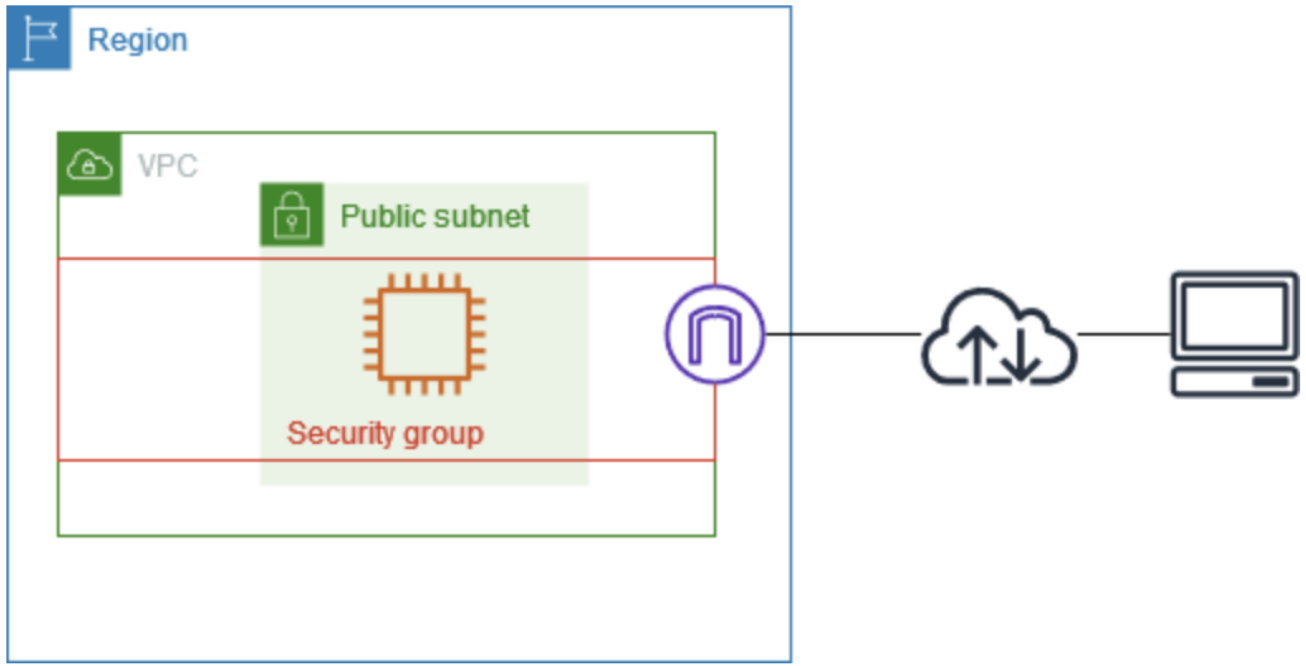
Route Tables

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

Security Group

- **Definition**: A virtual firewall at the instance level that controls inbound and outbound traffic.
- **Stateful**: 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.
- **Use Case**: Manage access to and from individual instances securely.

Security Group



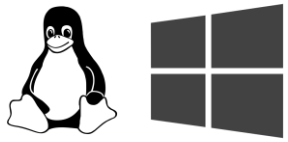
Amazon EC2 (Elastic Compute Cloud)

- **Virtual Private Server (VPS)**: Provides fully customizable cloud-based virtual servers.
- **Network of Servers**: Build distributed systems or load-balanced networks with multiple EC2 instances.
- **Flexibility**: Wide range of instance types, operating systems, and configurations to suit various workloads.
- **Scalability**: Scale resources up or down dynamically with Auto Scaling and Load Balancing.
- **Cost-Effective**: Pay-as-you-go pricing with multiple cost-saving options (e.g., Spot Instances, Reserved Instances).

Computer and EC2 Instance

Computer

EC2 Instance

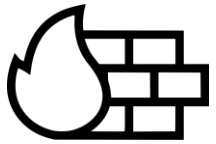


Operating System
AMIs
(Linux or Windows)

CPU & RAM
Instance Type

Hard Drive
EBS

Network Adapter
ENI



Firewall
Security Groups

Amazon EC2 (Elastic Compute Cloud)

- Key features
  - Instance Types
  - Amazon Machine Images (AMIs)
  - IP Addresses
  - Security Group: Inbound, Outbound rules
  - Instance Store: Internal memory

IP Addressing

An IP address is the EC2 instance address on the network.

Private IP Address:

- EC2 instance receives the private IP from the subnet.
- All EC2 instances (all devices in the network) have a private IP address.
- Private IP addresses allow instances to communicate with resources in the same network.
- No cost

Public IP address:

- All EC2 Instances can be launched with or without a public IP address.
- Public IP addresses are required for the instance to communicate with the Internet.
- It is dynamic as it is changed when restarting the instance
- No cost

Reference

- AWS: https://docs.aws.amazon.com
- ChatGPT: https://chatgpt.com
- Google AI: https://gemini.google.com
- Practical Tutorials: https://thaovu.org