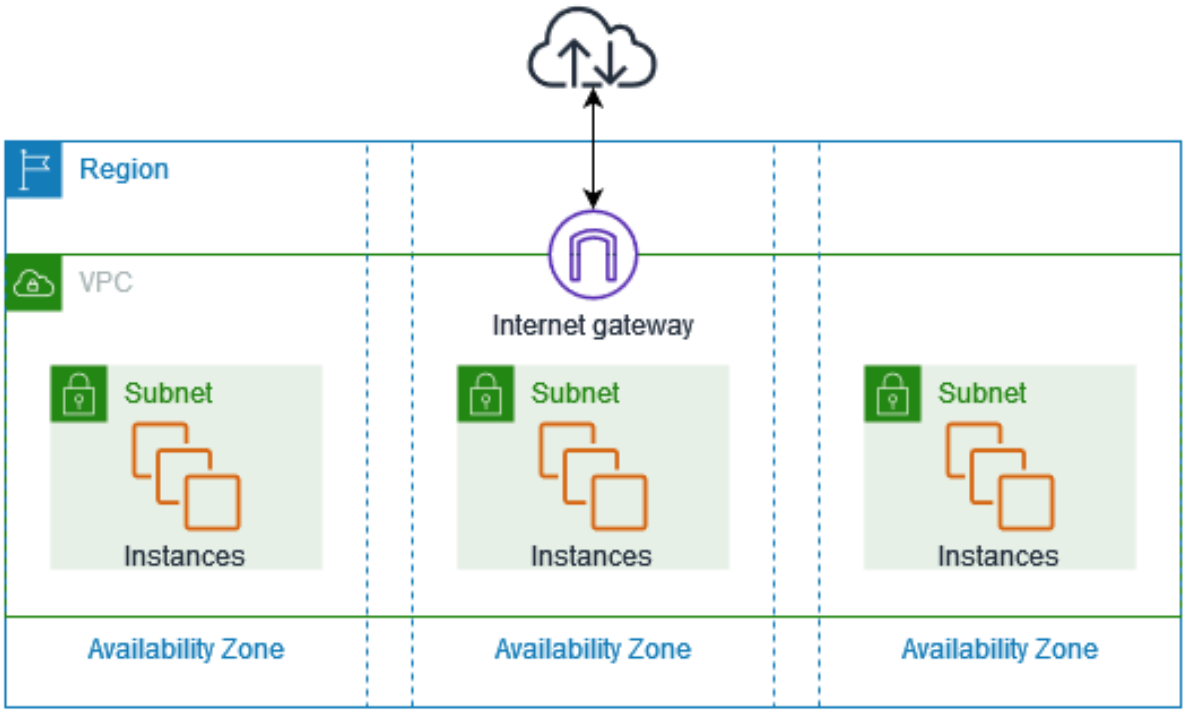
Amazon Web Services – Virtual Private Cloud (VPC)

Follow me Shaik Hari Sadia Anjum for more AWS learning content and cloud best practices! 🚀

Amazon Virtual Private Cloud (VPC) is a logically isolated section of the AWS cloud where you can launch AWS resources in a **custom-defined network**. It allows users to define **IP address ranges, subnets, route tables, security settings, and internet access rules**.

The following diagram shows an example VPC. The VPC has one subnet in each of the Availability Zones in the Region, EC2 instances in each subnet, and an internet gateway to allow communication between the resources in your VPC and the internet.



Why is AWS VPC Important?

- **Isolation:** Provides a **secure** environment for cloud resources.

- **Customization:** You can define **subnets, route tables, and gateways** to control traffic flow.
- **Security:** Uses **Security Groups and Network ACLs** for traffic control.
- **Scalability:** Can expand by adding **more subnets and peering connections**.

AWS VPC Use Cases

✅ **Hosting web applications** with public & private subnets.
✅ **Hybrid Cloud Connectivity** using VPN and Direct Connect.
✅ **Secure data processing** where only certain instances access the internet.

Core Components of AWS VPC

AWS VPC is made up of several components that define how traffic flows within the cloud network.

VPC (Virtual Private Cloud)

- A **private, logically isolated** network in AWS.
- Assigned a **CIDR block** (e.g., 10.0.0.0/16).
- Can have **multiple subnets across different Availability Zones (AZs)**.

Subnets

A **subnet** is a logical division within a VPC that helps organize instances.

🔹 **Types of Subnets:**

- **Public Subnet** → Connected to the internet via an **Internet Gateway (IGW)**.
- **Private Subnet** → No direct internet access; relies on a **NAT Gateway** for outbound traffic.

🔹 **Subnet Design Best Practices:**

- Use **multiple Availability Zones (AZs)** for high availability.
- Place **databases and sensitive data** in **private subnets**.

Route Tables

A **Route Table** contains rules (routes) that determine how network traffic is directed.

🔹 **Route Table Key Points:**

- Each **subnet must be associated** with a route table.
- **Main Route Table**: Default for the VPC.
- **Custom Route Table**: Can be created for specific routing needs.

Destination	Target	Usage
`0.0.0.0/0`	Internet Gateway	Public Subnet traffic
`10.0.1.0/24`	Local	VPC-internal traffic

Internet Gateway (IGW)

- A **managed AWS component** that allows communication between public instances and the internet.
- **Must be attached** to a VPC for internet access.
- Public subnets must have a **route to IGW** (0.0.0.0/0).

NAT Gateway vs. NAT Instance

Used to allow **private subnet instances** to access the internet **outbound**, without exposing them to incoming connections.

Feature	NAT Gateway	NAT Instance
Managed by AWS	✅ Yes	❌ No
High Availability	✅ Yes	❌ No (Manual)
Performance	✅ Scales automatically	❌ Limited to instance type

NAT Gateway is recommended for production workloads.

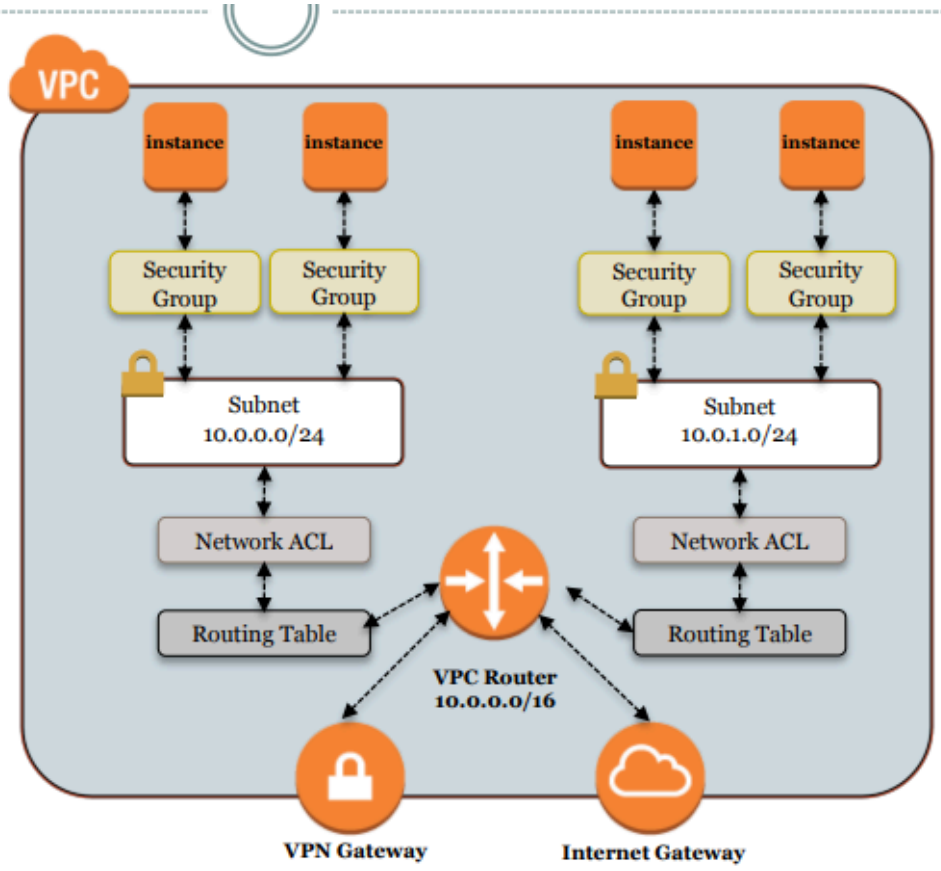
NAT Instance is only used when customization is needed.

Elastic IP (EIP)

- A **static, public IPv4 address** assigned to AWS resources.
- Used for **high availability** by reassigning it to a different instance if needed.

Security in AWS VPC

AWS VPC offers multiple layers of security to control inbound and outbound traffic.



Security Groups

- **Stateful:** Outbound responses are automatically allowed.
- Attached **to instances** (not subnets).
- Controls **inbound and outbound traffic** at the instance level.

✅ Example Security Group Rules for a Web Server

Rule Type	Protocol	Port Range	Source
SSH	TCP	22	Your IP
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

Network ACLs (Access Control Lists)

- **Stateless** (must define both inbound & outbound rules).
- Applied at **subnet level**.
- Used for **controlling fine-grained security** across subnets.

✅ Example Network ACL Rules

Rule #	Type	Protocol	Port Range	Source/Destination	Allow/Deny
100	HTTP	TCP	80	0.0.0.0/0	ALLOW
200	SSH	TCP	22	Your IP	ALLOW
300	All	All	All	0.0.0.0/0	DENY

📝 Key Difference Between Security Groups & NACLs

Feature	Security Groups	Network ACLs
Stateful/Stateless	Stateful	Stateless
Applied To	Instance Level	Subnet Level
Allow/Deny Rules	Only Allow Rules	Allow & Deny Rules
Default Behavior	Allow all outbound	Deny all inbound & allow all outbound

IP Addressing in AWS VPC

CIDR (Classless Inter-Domain Routing)

- Defines the **IP range** for a VPC or subnet.
- Example: 10.0.0.0/16 (65,536 IPs).
- Subnets must be within the **VPC CIDR block**.

Private vs. Public IPs

Type	Example	Scope
Public IP	3.123.45.67	Reachable via the internet
Private IP	10.0.1.23	Internal VPC communication

On Day 1, we covered the fundamentals of AWS VPC, including its core components, subnetting, routing, security groups, and IP addressing. Understanding these concepts is crucial before diving into VPC peering, hybrid connectivity, and monitoring, which will be covered on Day 2.