

VPC

05 January 2026 07:03 PM

VPC

1. VPC is a logically **isolated visual network** inside AWS where you launch Resources

2. Core Properties

1. Defined by an **IPv4 CIDR block** (Classless Inter-Domain Routing) (e.g.,
2. Fully customizable networking
3. Scoped to **one Region**

3. Why VPC Exists

1. Gives customers **full control** over network design
2. Mirrors traditional on-prem enterprise networks.

4. What a VPC Contains

1. Subnets
2. Route Tables
3. Internet Gateways
4. NAT Gateways
5. Security layers (Security Groups, NACLs)

1. Subnets

i. A **Subnet** is a **range of IP addresses** within a VPC, mapped to **one Availability Zone only**.

ii. Subnet Types

1. Public Subnet

1. Has a route to the Internet Gateway
2. Used for: Load Balancers, Bastion Hosts

2. Private Subnet

1. No direct internet access
2. Used for: Application servers, Databases

iii. Key Rules

1. Subnets **cannot span AZs**
2. Public vs Private is determined by **route tables**, not a checkbox

CIDR Example

1. VPC: 10.0.0.0/16
2. Public Subnet: 10.0.1.0/24
3. Private Subnet: 10.0.2.0/24

Analogy

1. Subnets \approx **VLANs inside a data center**

2. Route Table:

i. A Route table defines **where network traffic is directed**

ii. Core Components

1. Destination CIDR
2. Target (IGW, NAT Gateway, VPC Peering, etc.)

iii. Default Route Example

1. 0.0.0.0/0 \rightarrow Internet Gateway

iv. Subnet Association

1. Every subnet must be associated with **one route table**
2. One route table can serve **multiple subnets**

v. Key Concept

1. Route tables determine **public vs private behaviour**
2. Equivalent to **routing tables on routers/switches**

3. Internet Gateway

i. An **Internet Gateway** allows **two-way internet communication** between a VPC and the internet.

ii. Key Properties

1. Horizontally scaled and highly available
2. **Attached to one VPC**
3. Enables inbound and outbound traffic

Requirements for Internet Access

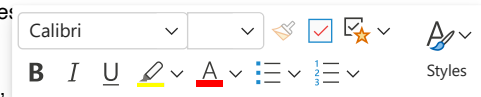
1. IGW attached to VPC
2. Route table entry: 0.0.0.0/0 \rightarrow IGW
3. Public IP or Elastic IP on the resource

4. NAT Gateway

i. A **NAT Gateway** allows **outbound internet access** for resources in **private subnets**, while blocking inbound traffic.

ii. Key Characteristics

1. Deployed in a **public subnet**
2. Uses an **Elastic IP**
3. Managed and highly available



iii. Traffic Flow

1. Private Subnet → NAT Gateway → Internet Gateway → Internet

iv. Why NAT Is Critical

1. Enables patching, updates, API calls
2. Keeps backend resources **non-exposed**

5. Security Groups

- i. A **Security Group** is a **stateful virtual firewall** attached to a resource (ENI).

ii. Key properties

1. Operates at **instance / ENI level**
2. **Stateful**:
 1. Return traffic is automatically allowed
3. Only supports **ALLOW rules**
4. Evaluated **before traffic reaches the OS**

iii. Rule types

1. **Inbound rules**
 1. Define **who can reach the resource**
2. **Outbound rules**
 1. Define **where the resource can connect**

