AWS Networking & Compute Deep-Dive Tutorial

---

1. What is a VPC (Virtual Private Cloud)

Definition:

VPC (Virtual Private Cloud) is your **own isolated virtual network** inside AWS.
It's where you launch and manage your AWS resources (EC2, RDS, etc.) securely.

Each AWS account comes with:

- **Default VPC** (preconfigured for simplicity)
- **Custom VPCs** (you create them for control, security, and isolation)

VPC Components:

Component	Description
CIDR Block	Defines IP address range (e.g., `10.0.0.0/16`)
Subnets	Divide VPC into smaller IP ranges
Route Tables	Define how traffic moves between subnets
Internet Gateway (IGW)	Enables Internet access
NAT Gateway	Allows private instances to access Internet
Security Groups	Instance-level firewalls
Network ACLs	Subnet-level firewalls

Example VPC

```
VPC CIDR: 10.0.0.0/16
   ├── Public Subnet: 10.0.1.0/24
   ├── Private Subnet: 10.0.2.0/24
```

---

2. Subnets: Public vs Private

Subnets divide your VPC into **smaller address spaces** for better organization, isolation, and routing control.

Types of Subnets

Subnet

Type	Internet Access	Typical Resources	Route Target
Public Subnet	- Direct Internet Access	Web servers, Bastion hosts	**Internet Gateway (IGW)**
Private Subnet	- No direct Internet Access	App servers, Databases	**NAT Gateway (for outbound)**

Example CIDR Design

Name	CIDR Block	Type
`PublicSubnet`	`10.0.1.0/24`	Public
`PrivateSubnet`	`10.0.2.0/24`	Private

---

3. Internet Gateway (IGW)

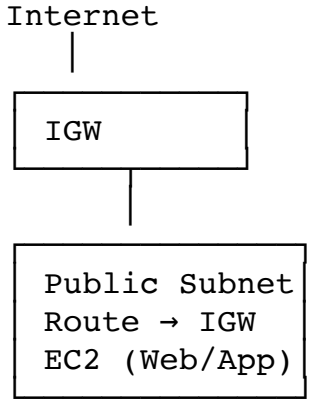
Definition:

Internet Gateway is a horizontally scaled, redundant AWS-managed gateway that allows **communication between your VPC and the Internet.**

Use Case:

- Attaches to your VPC.
- Provides outbound + inbound Internet access for **Public Subnets**.
- Works only if instances have **public IPs** or **Elastic IPs (EIPs)**.

Architecture:



---

4. NAT Gateway (Network Address Translation)

Definition:

NAT Gateway allows **instances in private subnets** to **initiate outbound Internet connections** (for updates, API calls, etc.)
—but it **blocks inbound Internet traffic**.

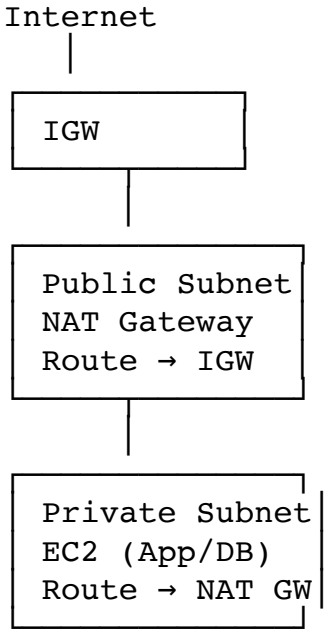
Setup:

- Deployed in **Public Subnet**.
- Must have an **Elastic IP**.
- Private Subnet's **route table** must point default route (0.0.0.0/0) → NAT Gateway.

Example:

Subnet	Route to 0.0.0.0/0	Internet Access
Public	IGW	- Direct
Private	NAT GW	- Outbound Only

Architecture:



---

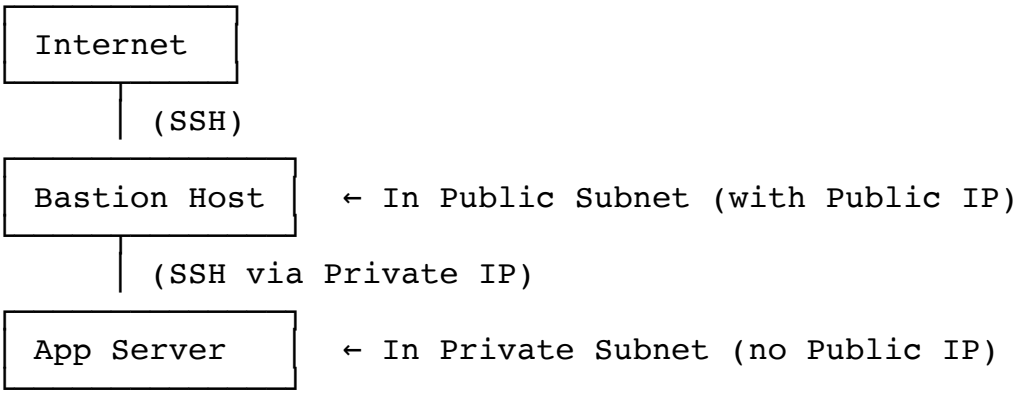
5. Bastion Host (Jump Box)

Definition:

A **Bastion Host** is a **secure jump server** in a **public subnet** that you use to **SSH (or RDP)** into private instances.

It acts as an **administrative gateway** — you connect to Bastion (public IP), then from there to private EC2s.

Architecture:



Security Best Practices:

- Restrict SSH access to your IP (`Security Group: MyIP only`).
- Disable direct Internet SSH on private EC2s.
- Use **AWS Session Manager** (instead of SSH) for modern setups.

---

6. IP Addressing in AWS

Type	Description	Scope	Example
Private IP	Internal-only communication (within VPC)	VPC	10.0.1.10
Public IP	Exposed to Internet; dynamic	AWS global	54.23.111.55
Elastic IP (EIP)	Static public IP assigned to your resource	AWS account	3.22.15.40

Key Facts:

- **Private IP**: Assigned automatically when EC2 is launched.
- **Public IP**: Automatically assigned only in **public subnets** (if "auto-assign public IP" enabled).
- **Elastic IP**: Persistent public IP that you can reattach across instances.

Example:

EC2 Instance	Subnet	Private IP	Public IP	Internet Access
Web Server	Public	10.0.1.10	54.23.111.55	- Direct
App Server	Private	10.0.2.12	—	- Outbound via NAT
DB Server	Private	10.0.2.20	—	- No Internet

---

7. EC2 Instance Details

EC2 (Elastic Compute Cloud) = Virtual Machine in AWS.

Launch Steps:

1. Choose AMI (Amazon Machine Image) → OS Template
2. Choose Instance Type → CPU + RAM
3. Configure VPC and Subnet
4. Assign IPs (private/public)
5. Configure Storage (EBS volume)
6. Set Security Group rules
7. (Optional) Add Key Pair for SSH

Typical Example Setup

Role	Subnet	Security Group	Internet Access
Bastion Host	Public	SSH from admin IP	- Direct
Web/App Server	Private	SSH from Bastion, HTTP to Public	- via NAT
DB Server	Private	MySQL from App subnet only	- No Internet

EC2 Key Components

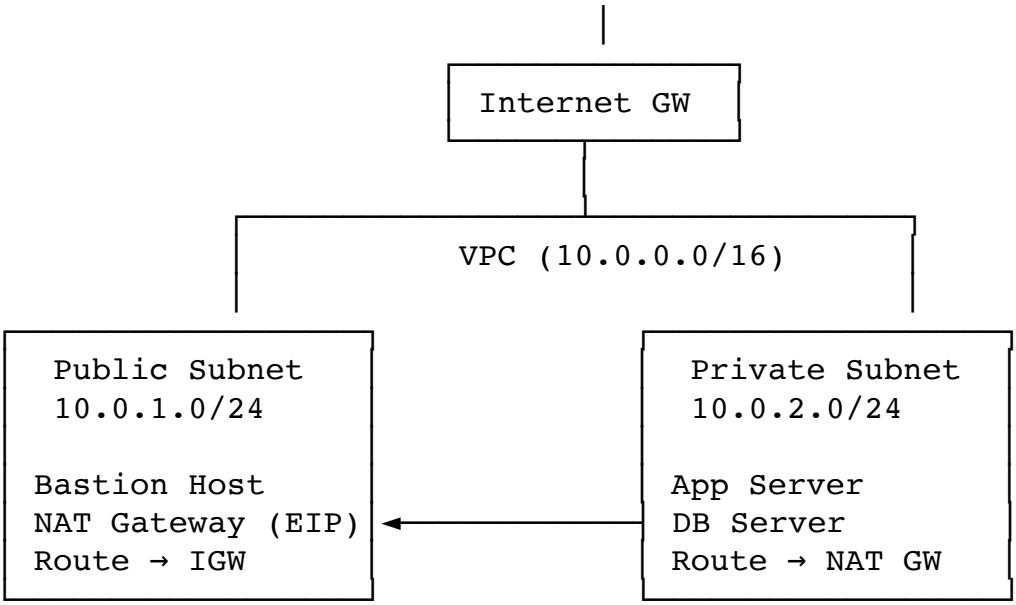
Component	Description
Instance Type	Defines compute power (e.g., `t3.micro`, `m5.large`)
AMI	Pre-configured OS template
EBS Volume	Block storage (persistent disk)
Elastic IP	Static public IP
Security Group	Virtual firewall controlling inbound/outbound
Key Pair	Used for SSH access
IAM Role	Grants EC2 permission to access AWS services

---

8. Putting It All Together

Final Architecture Diagram

```
Internet
```



---

9. Security Summary

Layer	Control	Description
VPC	Isolation	Logical network separation
Subnet	Scope	Public/Private separation
Security Group	Instance-level	Allow ports like 22, 80, 443
NACL	Subnet-level	Stateless rules
IAM Role	Identity	Who can access what
Key Pair	SSH Authentication	Secure access to EC2

---

10. Best Practices Checklist

- Use **private subnets** for internal services.
- Deploy **NAT Gateway** for outbound updates.
- Use **Bastion host or Session Manager** for admin access.
- Enable **VPC Flow Logs** for monitoring.
- Use **Security Groups** (not NACLs) as primary firewall.
- Use **Elastic IPs** only when static public IPs are required.
- Separate **environments** (Dev, Staging, Prod) into different VPCs.