Virtual Private Cloud(VPC)

What is a VPC?

- A **Virtual Private Cloud (VPC)** is a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define.
- It provides **complete control over your virtual networking environment**, including selection of IP address ranges, creation of subnets, route tables, gateways, and configuration of network access.

Key Components of a VPC

Subnets

- **Definition**: Subnets are subdivisions of your VPC IP address range. They allow you to segment your network within a VPC.
- **Types**:
  - **Public Subnet**: A subnet associated with a route to the internet via an internet gateway.
  - **Private Subnet**: No direct access to the internet.
- **Use Case**: Deploy web servers in public subnets and databases in private subnets for better security and isolation.

Route Tables

- **Definition**: Route tables control the traffic routing for subnets in a VPC.
- **Function:** Maps destination IP ranges to target resources (like gateways or NAT devices).
- **Subnet Association:** Every subnet must be associated with one route table.

Internet Gateway(IGW)

- **Definition:** A horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.
- **Function:** Required for internet-bound traffic from public subnets.
- **Use Case:** Attach an IGW to the VPC and update the route table to route outbound traffic to the IGW.

NAT Gateway

- **Definition:** A network address translation (NAT) service that allows instances in private subnets to access the internet without allowing inbound traffic from the internet.
- **Elastic IP:** Requires an Elastic IP address.
- **Use Case:** Instances in private subnets can download software updates or access external services securely.

Security Groups

- **Definition:** Virtual firewalls that control inbound and outbound traffic to AWS resources like EC2 instances.
- **Rules:** Stateful — response traffic is automatically allowed, even if the rule isn't explicitly defined.
- **Use Case:** Allow only SSH (port 22) from your IP to an EC2 instance.

Network Access Control Lists (NACLs)

- **Definition:** Optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.
- **Rules:** Stateless — both inbound and outbound rules must be defined explicitly.
- **Use Case:** Block specific IP addresses or ranges at the subnet level.

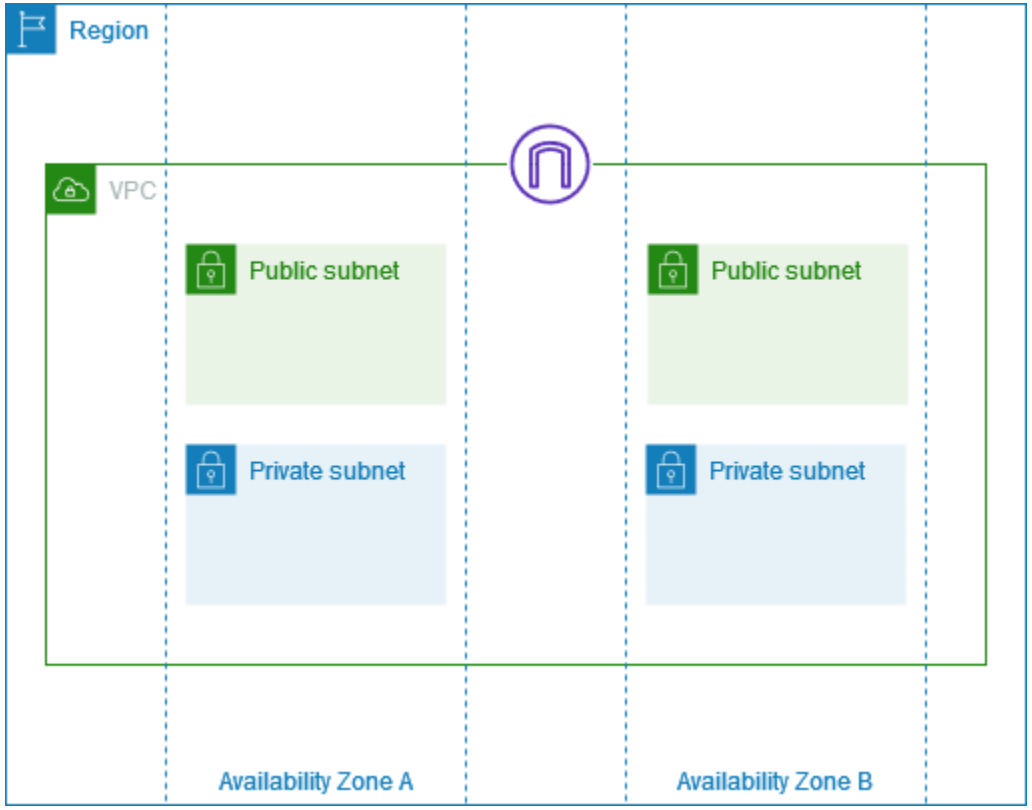
Subnet Associations

- Subnets must be associated with a route table and a NACL.
- One route table per subnet (but one table can be shared across multiple subnets).
- Each subnet can only be associated with one NACL at a time.

Best Practices

- Use multiple Availability Zones (AZs) for high availability.
- Implement least privilege security with minimal access via security groups and NACLs.
- Use flow logs to monitor traffic for analysis and troubleshooting.
- Regularly audit route tables and access controls to ensure optimal configuration.

Visualizing an AWS VPC Architecture



Visualizing an AWS VPC Architecture