**AWS VPC**

Amazon Virtual Private Cloud (Amazon VPC) is a service provided by Amazon Web Services (AWS) that allows you to create a logically isolated section of the AWS Cloud where you can launch resources in a virtual network that you define. It enables you to have complete control over your network environment, including IP address ranges, subnets, routing, and security.

**Features of AWS VPC:**

**1. Isolation:** VPC provides network isolation by allowing you to create your own private network within the AWS cloud. This isolation helps you control and secure your resources.

**2. Subnets:** You can divide your VPC into subnets, which are smaller IP address ranges within the VPC. Subnets can be public or private and can be spread across different availability zones to ensure high availability and fault tolerance.

**3. IP Addressing:** You have control over IP address ranges for your VPC and its subnets. You can choose and define IP ranges according to your requirements.

**4. Internet and Private Connectivity:** VPC allows you to connect your instances to the internet through an Internet Gateway for public access and NAT Gateway/NAT Instance for outbound traffic from private subnets.

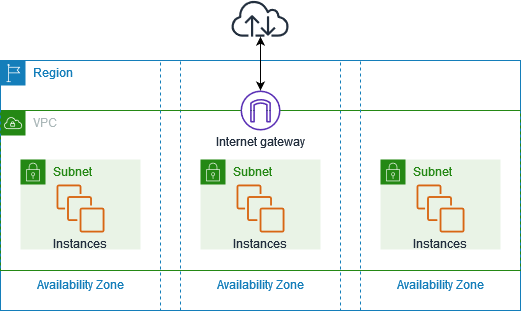
**5. Security:** Security Groups and Network Access Control Lists (NACLs) can be used to control inbound and outbound traffic at the instance and subnet level respectively.

**6. VPN and Direct Connect:** You can establish secure connections between your on-premises data center and your VPC using VPN (Virtual Private Network) or AWS Direct Connect for dedicated network connections.

**7. Peering:** VPC peering allows you to connect multiple VPCs together so that resources in different VPCs can communicate directly.

**8. Flow Logs:** VPC Flow Logs capture information about the IP traffic going to and from network interfaces in your VPC, helping you monitor and troubleshoot network activity.

Setting up and configuring a VPC involves defining its IP address ranges, creating subnets, setting up route tables, configuring security groups, and launching instances within those subnets.



**Subnets:**

Subnets allow you to segment your VPC's IP address space into smaller, manageable portions. Each subnet can be associated with a specific availability zone (AZ) within a region, providing high availability and fault tolerance for your resources.

**Key points of subnets:**

**1. Subnet IP Ranges:** When you create a VPC, you define an IP address range (CIDR block) for the entire VPC. Subnets are created within this range. For example, if your VPC has an IP range of 10.0.0.0/16, you can create subnets like 10.0.1.0/24, 10.0.2.0/24, etc.

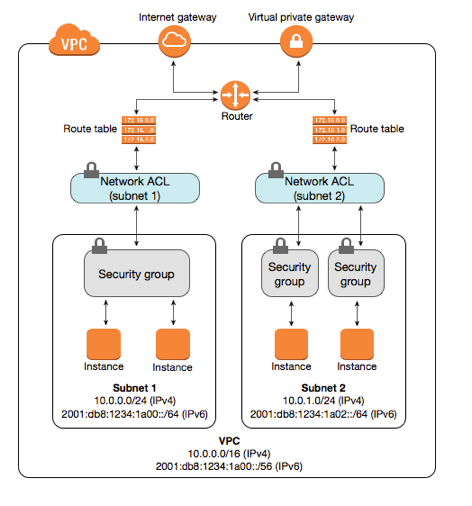
**2. Availability Zones:** AWS data centers are grouped into availability zones (AZs), which are distinct physical locations within a region. Each subnet must be associated with a single AZ. This enables you to deploy resources in different AZs to achieve high availability.

**3. Public and Private Subnets:** Subnets can be categorized as public or private. Public subnets are typically associated with resources that need direct internet access, while private subnets are used for resources that should not be directly accessible from the internet.

**4. Internet Gateway:** Resources in public subnets can communicate directly with the internet using an Internet Gateway. This allows instances in public subnets to have public IP addresses and route their traffic to and from the internet.

**5. Network Address Translation (NAT):** Private subnets do not have direct internet access. If resources in a private subnet need outbound internet access (e.g., for downloading software updates), you can use a NAT Gateway or a NAT instance. These act as intermediaries, translating outbound traffic from private instances and allowing them to access the internet.

**6. Route Tables:** Each subnet is associated with a route table that controls the routing of traffic. A route table contains rules that determine where network traffic should be directed. By default, a subnet's route table is set up to route traffic within the VPC. You can modify the route table to direct traffic to specific destinations, such as an Internet Gateway or a NAT Gateway.



**NACL**

**1. Subnet-Level Firewall:** NACLs are like firewalls for subnets in your AWS Virtual Private Cloud (VPC), allowing you to control inbound and outbound traffic flow at the subnet level.

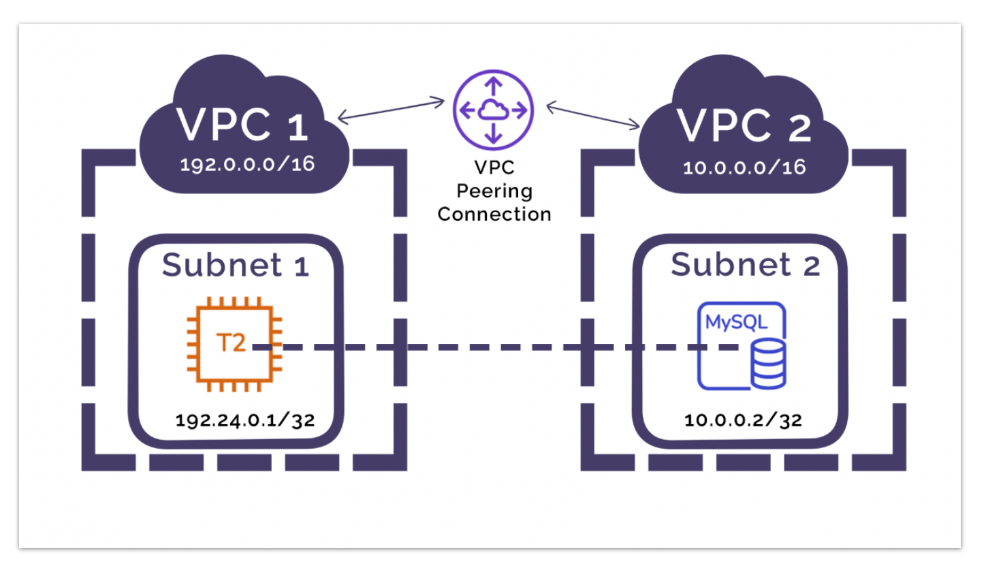
**2. Stateless Filtering:** NACLs are stateless, meaning that you must define separate rules for inbound and outbound traffic. Unlike stateful security groups, NACLs require explicit rules for responses to allowed traffic.

**3. Rule Order Matters:** Rules in NACLs are processed in sequential order based on rule numbers. The first matching rule is applied, which can allow or deny traffic. Lower rule numbers take precedence.

**4. Default NACLs:** Each VPC comes with a default NACL that allows all inbound and outbound traffic. It's a good practice to customize the default NACL or create custom ones based on your security requirements.

**5. Customizable Rules:** You can create custom NACLs and tailor rules to specific subnets. Define allowed IP ranges, protocols, port ranges, and actions (allow/deny) to enforce your desired security policies.

**6. Subnet Association:** Each subnet in a VPC is associated with a NACL. A NACL can be associated with multiple subnets, but each subnet can have only one NACL at a time.



**VPC Peering:**

Amazon Virtual Private Cloud (Amazon VPC) peering is a networking feature provided by Amazon Web Services (AWS) that allows you to connect two separate VPCs and enable communication between instances in those VPCs as if they were on the same network.

VPC peering provides a way to establish private connectivity between VPCs in the same region or in different AWS regions.

**Key points of VPC peering:**

**1. Private Communication:** VPC peering allows you to establish private communication between instances in different VPCs using private IP addresses, without the need to traverse the public internet.

**2. Same Region or Cross-Region:** VPC peering can occur within the same AWS region or across different regions, allowing you to connect resources in different geographic locations.

**3. Non-Transitive:** VPC peering is non-transitive, meaning that if VPC A is peered with VPC B and VPC B is peered with VPC C, VPC A and VPC C do not have direct connectivity through the peering connection.

**4. CIDR Blocks:** The IP address ranges (CIDR blocks) of the VPCs you want to peer must not overlap. They need to be distinct and non-overlapping.