**VPC- Virtual Private Cloud:**

a VPC is a virtual network dedicated to an **AWS** account. It allows users to launch and manage their AWS resources, such as virtual servers (**EC2** **instances**), in an isolated and customizable network environment.

**VPC’s introduced “Privat Cloud” in the world of “Public Cloud”**

Users can define their own IP address range, create subnets, configure route tables, and control inbound and outbound traffic using security groups and network access control lists (ACLs).

In initial time, Companies or like start-ups tries to maintain there own ‘**Data** **Centre’** by a region throughout the world. For maintaining huge number of data for the small companies or start-ups it has been hectic.

AWS as its own data centre , companies just request like we want 1 or 10 virtual machine(instances) and for that aws will get paid .

If **1** **company** requests **10** **instance** to Data Centre in one specific region (inside the Data Centre there also be physical server) in server 1, also if another company requests 5 instance to same server (server1) and also same as company3 . if company3 is not maintain security there might be hacker comes , company3 is in same server whereas company1 and company2 there is an easy chances to hack other companies also

To solve the security breach it was security community it AWS terms its called ‘**VPC’**. For defining size of vpc there is a ‘**IP** **ADDRESS** **RANGE’** .

Security for “Instance” level is “Security Group” , Security for “Subnet” Level is “NACL”

**Steps to create VPC:**

* Login to AWS Console
* Search VPC
* Create VPC
* Select VPC and More
* Select ipv4 CIDR block and Availability Zones
* Create

**Components Of VPC’s**

1. **VPC (Virtual Private Cloud):** The overarching term that refers to the virtual network dedicated to an AWS account.
2. **Subnet:** A range of IP addresses in your VPC. Subnets can be either public or private, based on their accessibility to the internet.
3. **Internet Gateway:** A component that allows communication between instances in your VPC and the internet.
4. **Route Table:** A set of rules, called routes, that are used to determine where network traffic is directed.
5. **CIDR Block:** Classless Inter-Domain Routing block, representing a range of IP addresses in the VPC.
6. **Security Group:** Acts as a virtual firewall for your instances to control inbound and outbound traffic.
7. **Network ACL (Access Control List):** An optional layer of security that acts as a firewall for controlling traffic at the subnet level.
8. **Elastic Load Balancer (ELB):** Distributes incoming application traffic across multiple instances, improving availability and fault tolerance.
9. **Peering:** The connection of one VPC to another, allowing instances in the connected VPCs to communicate with each other.
10. **VPN (Virtual Private Network):** A secure way to connect a VPC to an on-premises data center or another VPC over the internet.
11. **Direct Connect:** A dedicated network connection from your on-premises data center to AWS.
12. **NAT Gateway (Network Address Translation):** Allows instances in a private subnet to initiate outbound traffic to the internet while preventing incoming traffic from reaching them.
13. **VPC Endpoint:** Enables private connectivity to services such as Amazon S3 or DynamoDB from within a VP C, without using an internet gateway, VPN, or Direct Connect.
14. **VPC Flow Logs:** Captures information about the IP traffic going to and from network interfaces in your VPC.
15. **Customer Gateway:** Represents a physical device or software application on your side of the VPN connection.
16. **Virtual Private Gateway:** Represents the VPN connection on the AWS side.
17. **Route Propagation:** The automatic updating of route tables in response to changes in the associated subnets.
18. **DHCP Option Set:** Specifies custom Domain Name System (DNS) servers and NTP servers for your VPC.

**EXAMPLE:**

**Real-World Example: The Digital Neighborhood**

1. **Your Digital Home (VPC**):
   * Your digital home is your VPC. It's like your own private piece of land on the internet. You get to decide the layout, the rules, and who's allowed in.
2. **Your Address (IP Address):**
   * Your home has an address, just like an IP address in a VPC. It's unique to you, and it helps others find you on the internet.
3. **Rooms in Your House (Subnets):**
   * Inside your home, you have different rooms for different purposes. In your VPC, these are called subnets. For example, you might have a living room (public subnet) for everyone to access and a bedroom (private subnet) that's more secure and private.
4. **Your Security System (Security Groups and ACLs):**
   * You have a security system in your house to control who can come in and out. In your VPC, you use security groups and access control lists (ACLs) to decide who and what can communicate with your digital resources.
5. **Internet Access (Internet Gateway):**
   * If you want to access the outside world, you use a door (Internet Gateway) to go in and out. It's like having a front door to your digital home.
6. **Inviting Guests (Elastic Load Balancer):**
   * Sometimes, you have friends over. An Elastic Load Balancer (ELB) is like a friendly but smart greeter who directs incoming guests (internet traffic) to different parts of your house (instances) to keep things running smoothly.
7. **Private Conversations (VPC Peering):**
   * Your neighbors might have their own homes. VPC peering is like having a secret tunnel (private connection) between your homes, allowing you to chat without going through the public street (internet).
8. **Security Cameras (Monitoring and Logging):**
   * You have security cameras in and around your house to monitor activities. Similarly, AWS provides tools for monitoring and logging to keep an eye on what's happening in your VPC.