Virtual Private Cloud (VPC)

Imagine you want to set up a private, secure, and isolated area in the cloud where you can run your applications and store your data. This is where a VPC comes into play.

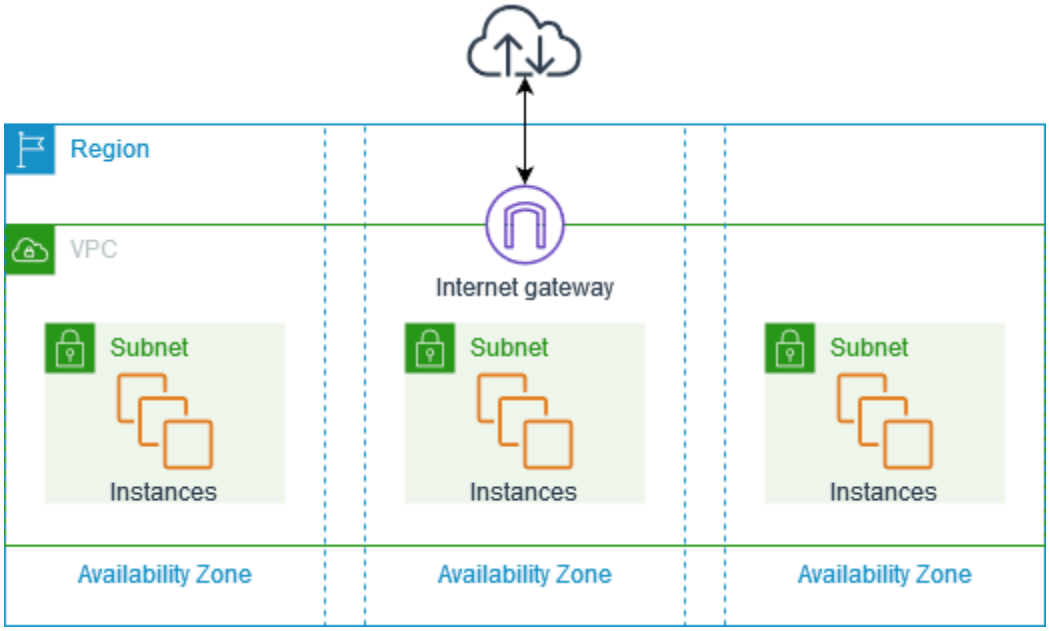
A VPC is a virtual network that you create in the cloud. It allows you to have your own private section of the internet, just like having your own network within a larger network. Within this VPC, you can create and manage various resources, such as servers, databases, and storage.

Think of it as having your own little "internet" within the bigger internet. This virtual network is completely isolated from other users' networks, so your data and applications are secure and protected.

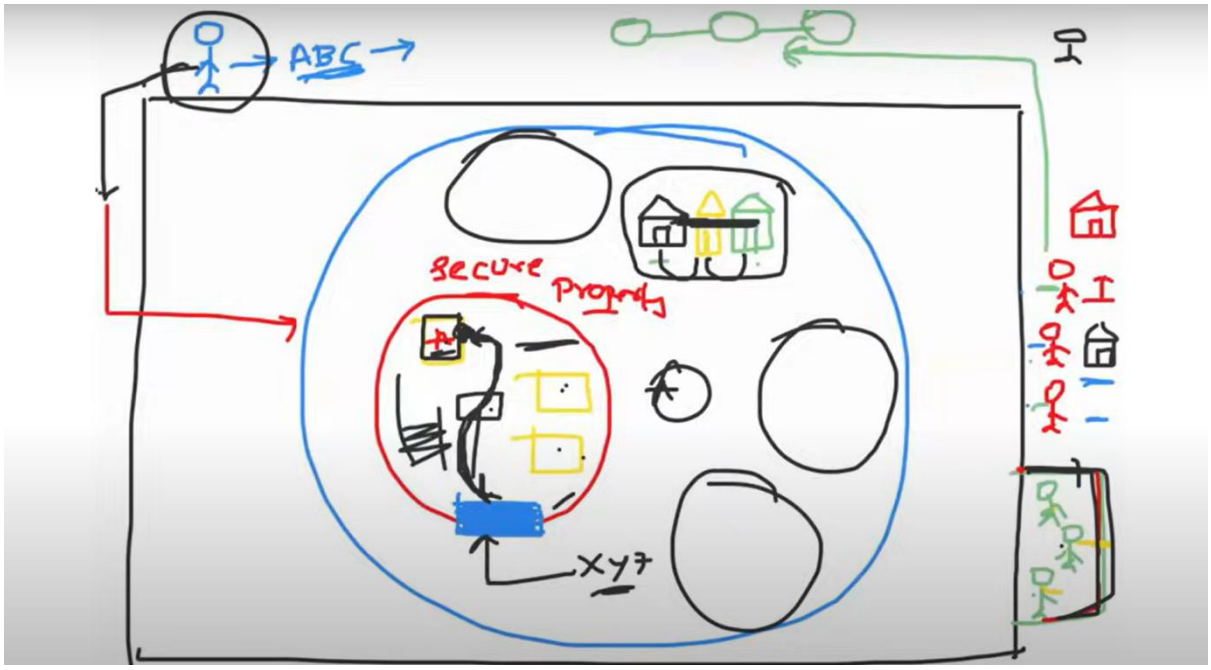
Just like a physical network, a VPC has its own set of rules and configurations. You can define the IP address range for your VPC and create smaller subnetworks within it called subnets. These subnets help you organize your resources and control how they communicate with each other.

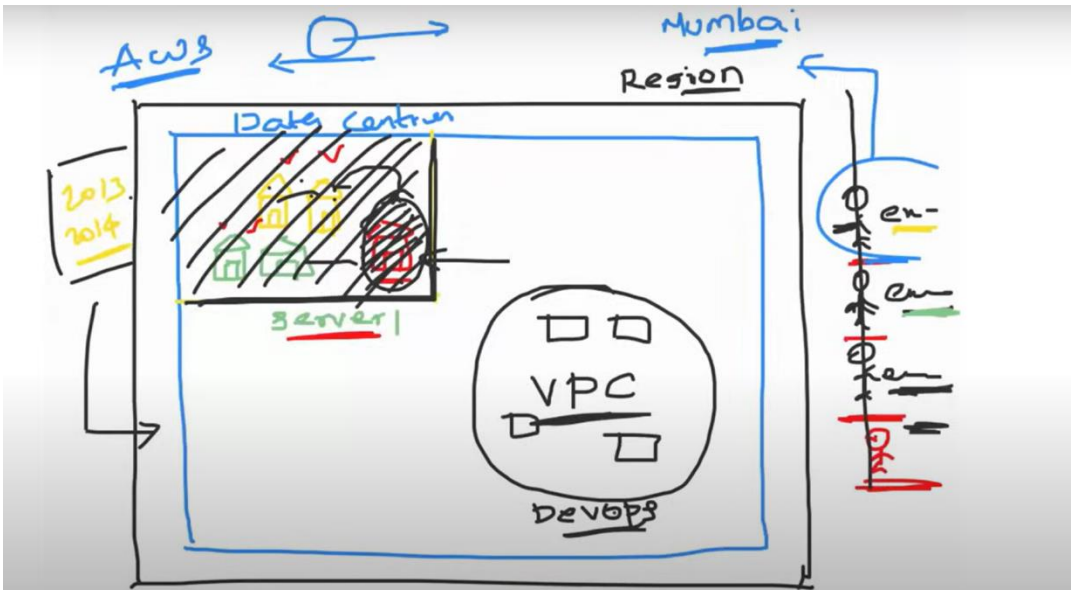
To connect your VPC to the internet or other networks, you can set up gateways or routers. These act as entry and exit points for traffic going in and out of your VPC. You can control the flow of traffic and set up security measures to protect your resources from unauthorized access.

With a VPC, you have control over your network environment. You can define access rules, set up firewalls, and configure security groups to regulate who can access your resources and how they can communicate.



By default, when you create an AWS account, AWS will create a default VPC for you but this default VPC is just to get started with AWS. You should create VPCs for applications or projects.





Internet Gateway

- Internet Gateway (IGW) is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.
- Internet Gateway enables resources (like EC2 instances) in public subnets to connect to the internet. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public.
- If a VPC *does not* have an Internet Gateway, then the resources in the VPC cannot be accessed from the Internet (unless the traffic flows via a Corporate Network and VPN/Direct Connect).

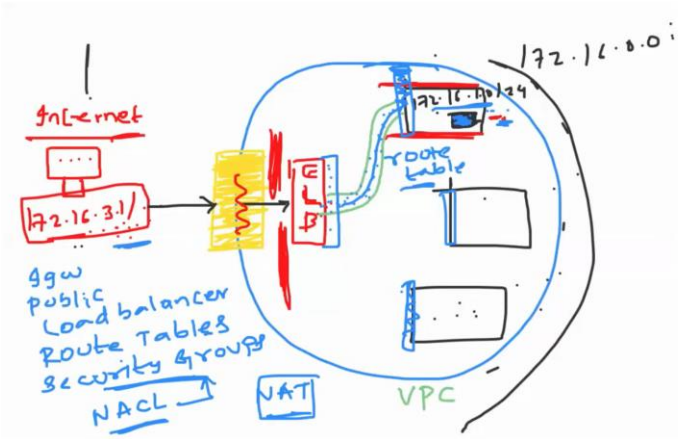
- Internet Gateway supports IPv4 and IPv6 traffic.
- Internet Gateway does not cause availability risks or bandwidth constraints on your network traffic.
- In order to make subnet public, add a route to your subnet's route table that directs internet-bound traffic to the internet gateway.
- You can associate exactly one Internet Gateway with a VPC.
- Internet Gateway is not Availability Zone specific.
- There's no additional charge for having an internet gateway in your account.

NAT Gateway

- NAT Gateway (NGW) is a managed Network Address Translation (NAT) service.
- NAT Gateway does something similar to Internet Gateway (IGW), but it only works one way: Instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.
- NAT gateways are supported for IPv4 or IPv6 traffic.
- NAT gateway supports the following protocols: TCP, UDP, and ICMP.
- Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone.
- If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access.
- To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone.
- You can associate exactly one Elastic IP address with a public NAT gateway.
- You are charged for each hour that your NAT gateway is available and each Gigabyte of data that it processes.

NAT gateway replaces the source IP address of the instances with the IP address of the NAT gateway.

- *WHEN The application in private subnet want to download any packages from the internet. In this case NAT gateway is helpful. It mask the Ip address server/application. It helps to secure download of packages from the internet.*



Public Subnet :

The subnet has a direct route to an internet gateway. Resources in a public subnet can access the public internet.

Private Subnet:

Private subnet – The subnet does not have a direct route to an internet gateway. Resources in a private subnet require a NAT device to access the public internet.

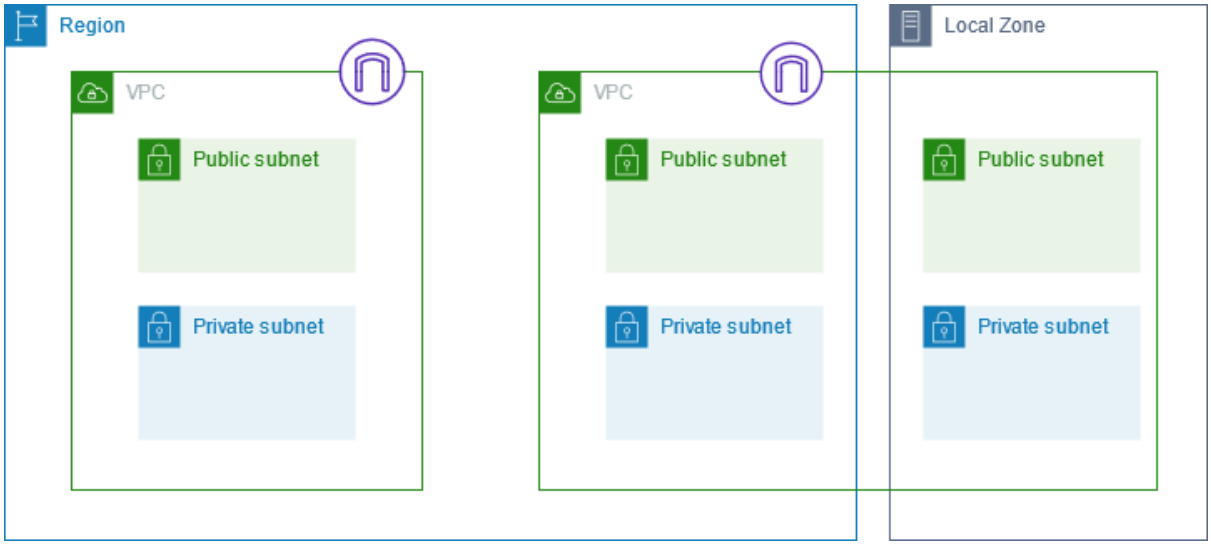
A *load balancer* serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application

Route Table:

A *route table* contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed.

Security Groups:

A *security group* controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.



VPC components

The following features help you configure a VPC to provide the connectivity that your applications need:

Virtual private clouds (VPC)

A VPC is a virtual network that closely resembles a traditional network that you'd operate in your own data center. After you create a VPC, you can add subnets.

Subnets

A subnet is a range of IP addresses in your VPC. A subnet must reside in a single Availability Zone. After you add subnets, you can deploy AWS resources in your VPC.

IP addressing

You can assign IP addresses, both IPv4 and IPv6, to your VPCs and subnets. You can also bring your public IPv4 and IPv6 GUA addresses to AWS and allocate them to resources in your VPC, such as EC2 instances, NAT gateways, and Network Load Balancers.

Network Access Control List (NACL)

A Network Access Control List is a stateless firewall that controls inbound and outbound traffic at the subnet level. It operates at the IP address level and can allow or deny traffic based on rules that you define. NACLs provide an additional layer of network security for your VPC.

Security Group

A security group acts as a virtual firewall for instances (EC2 instances or other resources) within a VPC. It controls inbound and outbound traffic at the instance level. Security groups allow you to define rules that permit or restrict traffic based on protocols, ports, and IP addresses.

Routing

Use route tables to determine where network traffic from your subnet or gateway is directed.

Gateways and endpoints

A gateway connects your VPC to another network. For example, use an internet gateway to connect your VPC to the internet. Use a VPC endpoint to connect to AWS services privately, without the use of an internet gateway or NAT device.

Peering connections

Use a VPC peering connection to route traffic between the resources in two VPCs.

Traffic Mirroring

Copy network traffic from network interfaces and send it to security and monitoring appliances for deep packet inspection.

Transit gateways

Use a transit gateway, which acts as a central hub, to route traffic between your VPCs, VPN connections, and AWS Direct Connect connections.

VPC Flow Logs

A flow log captures information about the IP traffic going to and from network interfaces in your VPC.

VPN connections

Connect your VPCs to your on-premises networks using AWS Virtual Private Network (AWS VPN).

Resources

VPC with servers in private subnets and NAT