Friday
04/03/2022

VPC

classmate
Date
Page

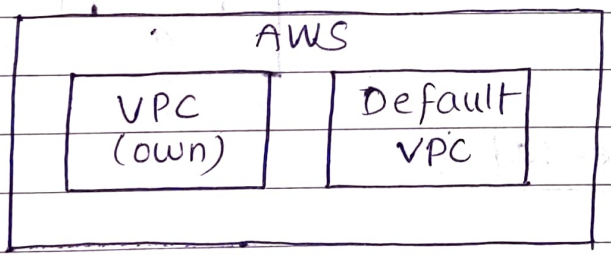
★ **VPC :-** Virtual Private Cloud

- It helps you to create a virtual isolated environment in the same cloud.

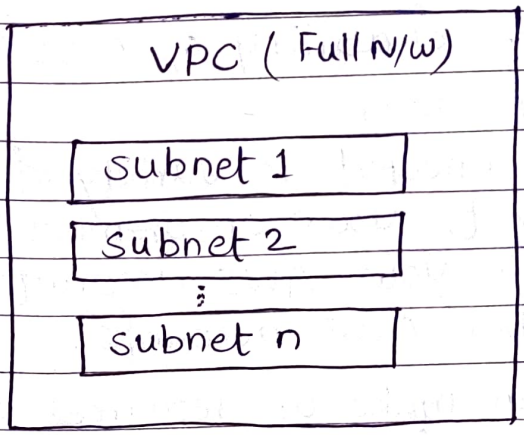
- Multiple virtual isolated env. are also possible.

- Amazon Virtual Private Cloud is a commercial cloud computing service that provides users a virtual private cloud, by provisioning a logically isolated section of Amazon Web Services Cloud.

- VPC gives you complete control over your virtual networking env, including resource placement, connectivity and security.



VPC → Full Network → divided based on IP CIDR blocks (Classless Inter-Domain Routing) into Subnets (Subnetworks)



Date
Page

* Subnets :-

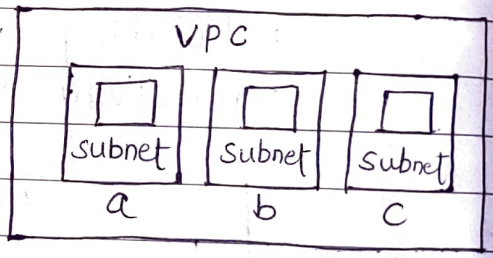
- It is a network inside a Network.
- When we break down n/w into smaller networks it is called as subnet or subnetwork.
- This breaking down of n/w is based on IP (CIDR)
- 2 Types of subnets are there.

① Public Subnet

- It is a subnet under VPC which is connected to / has a route to internet gateway
- It can connect to internet directly.

② Private Subnet

- It can't connect / communicate to internet directly.



ap-south-1

* Why VPC is needed ?

- It keeps your servers safe from the ravages of the public internet.
- Secure
- Simple
- All the scalability & reliability of AWS is available
- Multiple Connectivity Options :-
  - It can be connected to variety of resources, such as internet, your on-premise DC, other VPCs in your AWS account or VPCs in other AWS accounts.

Once created you can make ur resources accessible or inaccessible in your VPC from outside of your VPC based on ur requirement.

Use cases :

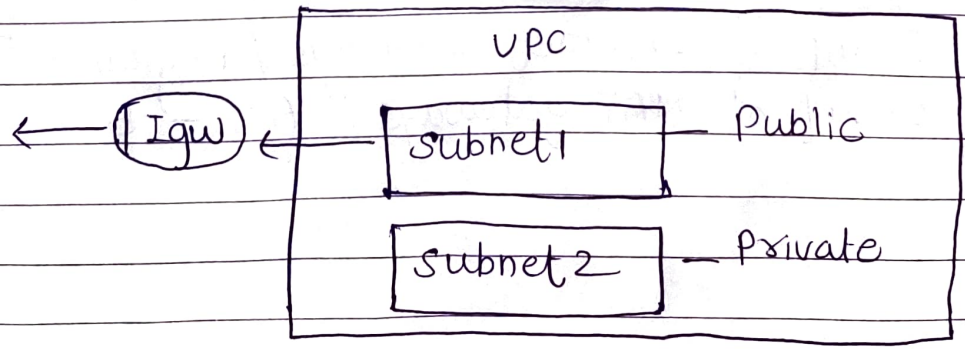
- Host a public facing website
- Host a multi-tier application, such as it will have web-layer, LB layer, DB layer etc.
- Hosting of scalable web applications in your cloud
- Manage multiple projects, create isolated networks for those projects.

* Imp :-

VPC → Full Isolated network.

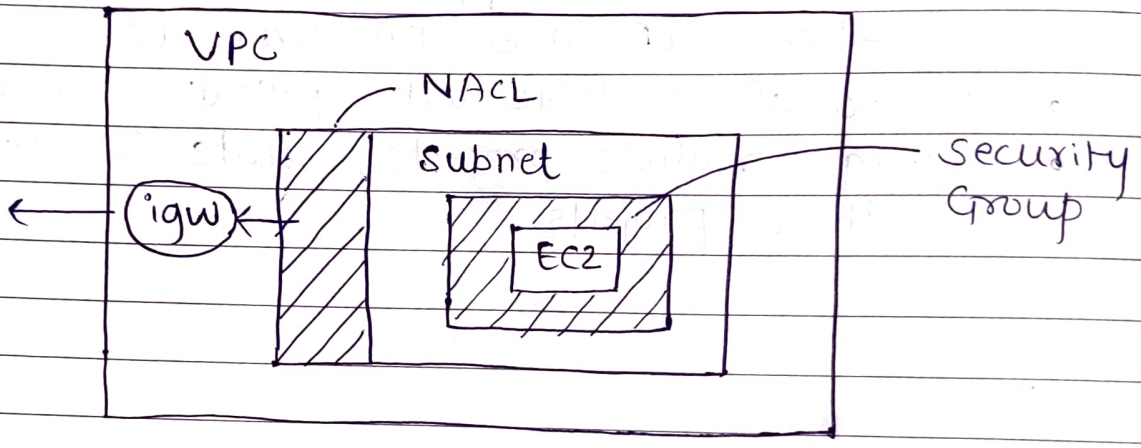
Default VPC	Non-default VPC
have standard routing rules	- We have to create everything from scratch
- It is created by Amazon	- Customer/User have to create it

→ Internet gateway is a device which helps your VPC to connect to internet



NACL is an layer of security for your VPC that acts as a firewall for controlling traffic in & out of one or more subnets.

* Network ACL (Access Control list) :-
  - This acts as a firewall for associated subnets
  - It controls both incoming & outgoing traffic at the subnet level
  - It's the 1st firewall at the network level



From EC2 point of view → NACL is a 2nd layer of firewall of EC2-instance

From n/w point of view → NACL is a first layer of firewall of subnet

* Default limits :-

- We can have only upto 5 non-default amazon VPC/region
- You can create upto 200 subnets / VPC
- We can create upto 200 Network ACL / amazon VPC
- We can have upto 5 Elastic IPs / Amazon Account / Region
- Count of IPV4 CIDR blocks / VPC – 5
- Count of IPV6 CIDR blocks / VPC – 1
- Count of Internet gateways / Region – 5
- Count of NAT gateways / AZ – 5

* Route Table :-

- A route table contains a set of rules, called routes that are used to determine where n/w traffic from your subnet or gateway is directed.
- route table tells network packets which way they need to go to get their destination.

- Types :-
  1) Public routing → Is where we can route to the internet with the help of igw.
  2) Private routing → In this we can route between private subnets or internal network only.

* Internet Gateway :-

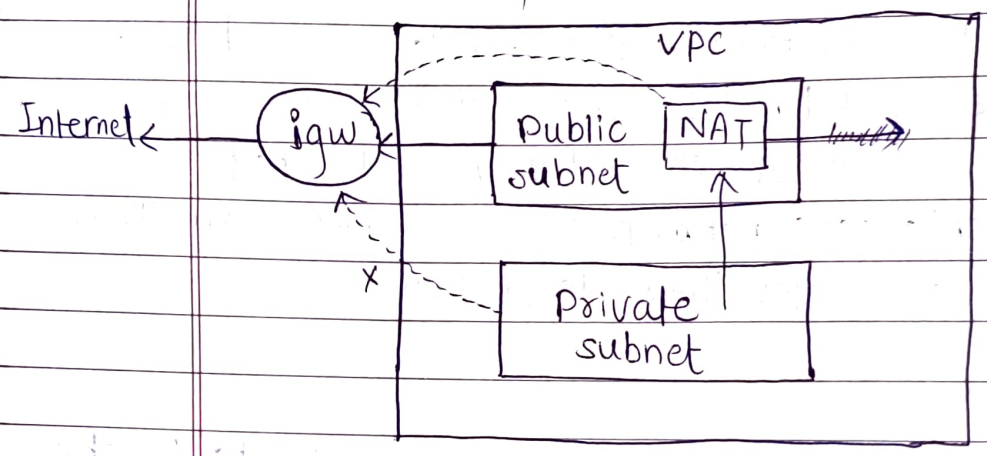
- Igw is a horizontally scaled, redundant & highly available VPC component that allows communicat" between your VPC & the internet.

- If a VPC doesn't have an igw, then the resources in the VPC cannot be accessed from the internet.

- A public subnet is a subnet that is associated with route table that has a route to an igw.

- Igw has a Public IP attached to it.
- There is no additional charge for having an igw in your account.

* NAT gateway :- (~~Network Address Transmission~~)

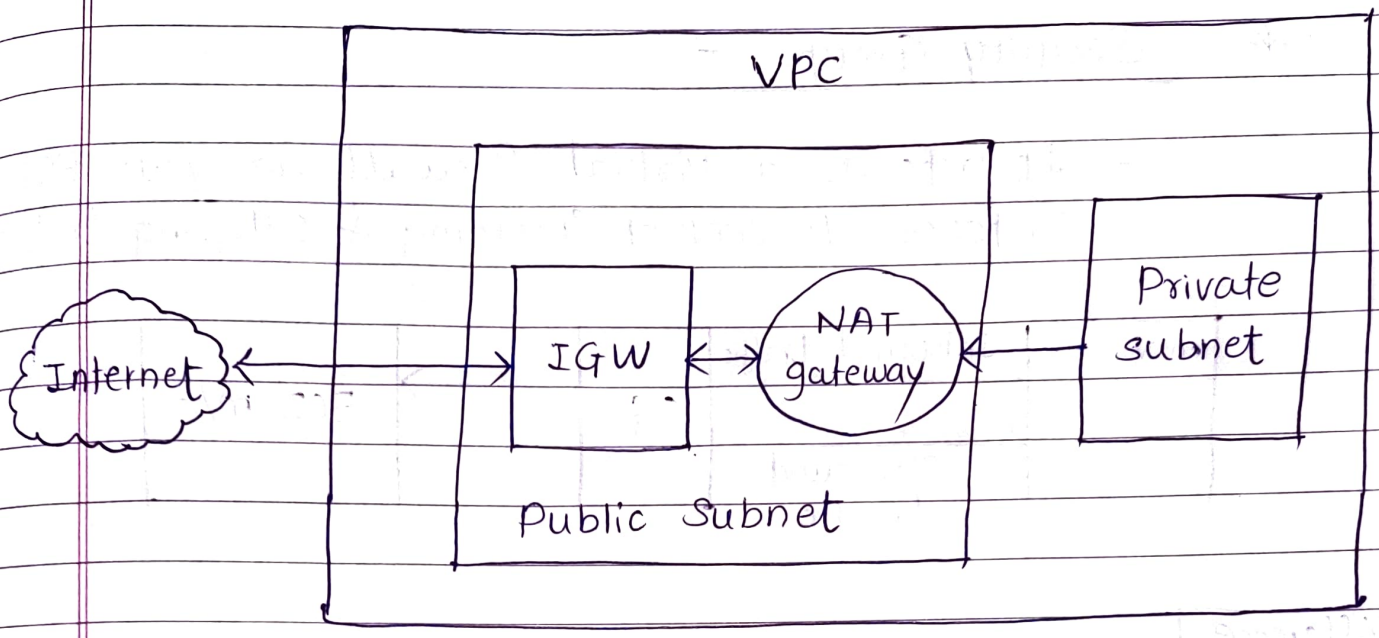


from Internet - EC2 & EC2 - internet

Igw → 2-way communication → EC2 →

NAT → 1-way communication
(Private to public)
Public entity cannot access private n/w
EC2 - Internet ✓
Internet - EC2 X

- NAT → Network Address Translation
- This will translate your private IP to public IP so that you can access internet from private IP
- NAT gateway is usually created in public subnet with a public IP of its own.
- Ideally, NAT gateway will sit bet" your IGW and private subnet.
- NAT gateway will accept all the packets from private subnet & attach its own IP address to it and forward the packets to the IGW.

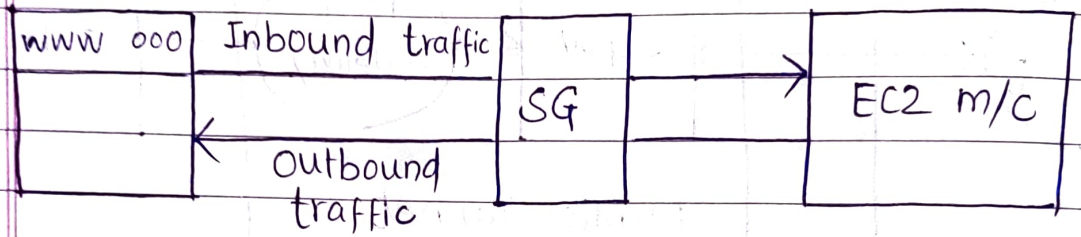


* Difference :-

IGW	NAT gateway
• It allows instances with public IPs to access the internet	• It allows instances with no public IPs to access the internet
• IGW allows resources within your public sub-net to access internet, and the internet to access said resources	• It only works one way. Through NAT, we can go from private to public but a public entity cannot access the private n/w.
• Two-way communication	• One-way Communication If we want 2-way NAT, then we have to setup reverse NATing. – In cloud computing, we do not go for reverse NATing which is a standard.

* Security Groups :-

- It acts as a virtual firewall for your EC2 instances to control incoming & outgoing traffic



Difference

*	Security Group	Network ACL's
•	Operates at instance level	Operates at subnet level
•	Supports only allow traffic	Supports both allow and deny traffic
•	Its stateful - return traffic is automatically allowed.	It's stateless - return traffic must be explicitly allowed
•	Evaluates all the rules before deciding whether to allow traffic or not	It processes rules in numeric order when deciding whether to allow traffic or not