**VPC**

**IP Addresses in AWS**

• IPv4 — Internet Protocol version 4 (4.3 Billion Addresses)

• Public IPv4 — can be used on the Internet

• EC2 instance gets a new a public IP address every time you stop then start it (default)

• Private IPv4 — can be used on private networks (LAN) such as internal AWS networking

(e.g., 192.168.1.1)

• Private IPv4 is fixed for EC2 Instances even if you start/stop them

Elastic IP — allows you to attach a fixed public IPv4 address to EC2 instance

• Note: all public IPv4 on AWS will be charged $0.005 per hour (including EIP)

• Free Tier: 750 hours usage per month

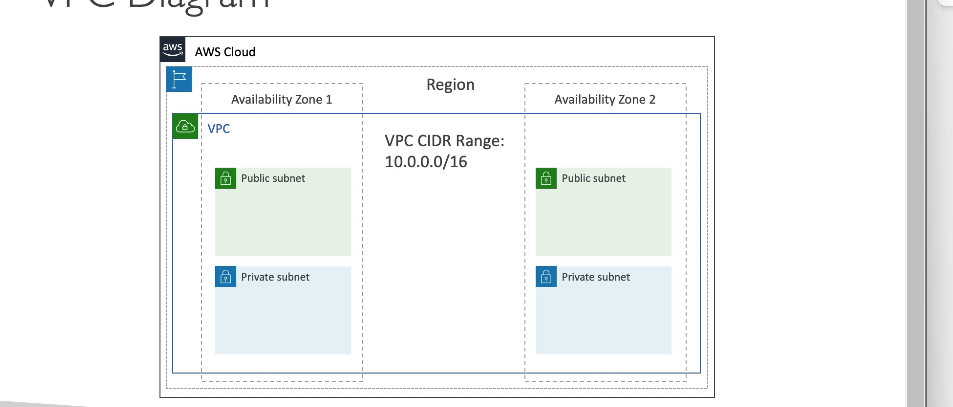
• IPv6 — Internet Protocol version 6 (3.4 x 1038 Addresses)

• Every IP address is public in AWS (no private range)

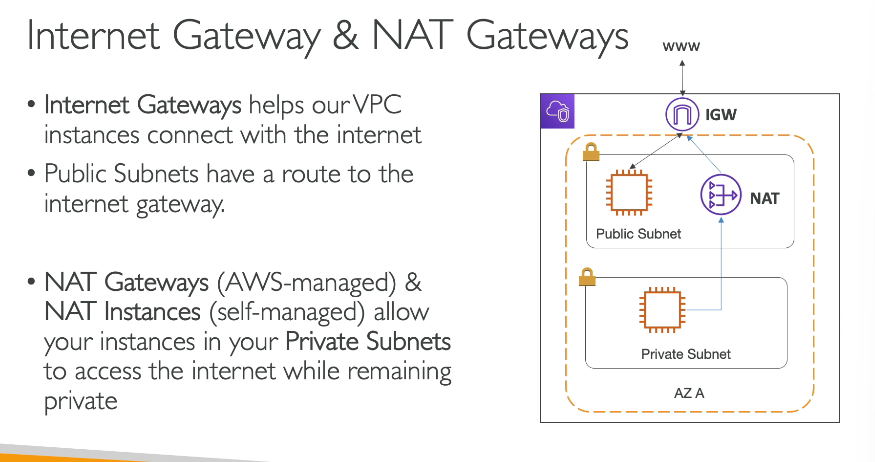
• Example: 2001 :db8:3333:4444:cccc:dddd:eeee:ff

**VPC & Subnets Primer**

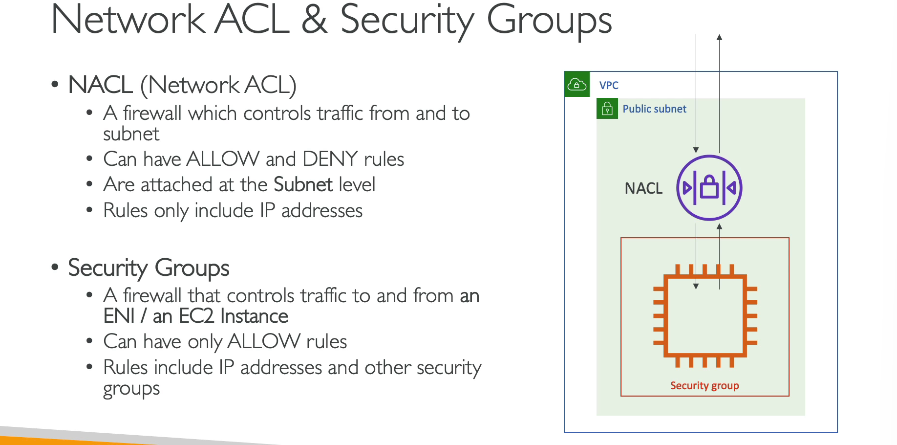
* VPC -Virtual Private Cloud: private network to deploy your resources (regional resource)
* Subnets allow you to partition your network inside your VPC (Availability Zone resource)
* A public subnet is a subnet that is accessible from the internetA private subnet is a subnet that is not accessible from the internet define access to the internet and between subnets, we use Route Tables.



**Internet Gateway & NAT Gateways**

* Internet Gateways helps our VPC instances connect with the internet
* Public Subnets have a route to the internet gateway.
* NAT Gateways (AWS-managed) & NAT Instances (self-managed) allow your instances in your Private Subnets to access the internet while remaining private
* 

**Network ACL & Security Groups**

* NACL (Network ACL)
  + A firewall which controls traffic from and to subnet
  + Can have ALLOW and DENY rules
  + Are attached at the Subnet level
  + Rules only include IP addresses
* Security Groups
  + A firewall that controls traffic to and from an ENI / an EC2 Instance
  + Can have only ALLOW rules
  + Rules include IP addresses and other security groups
  + 

### Network ACLs vs Security Groups

| **Security Group** | **Network ACL** |
| --- | --- |
| Operates at the instance level | Operates at the subnet level |
| Supports allow rules only | Supports allow rules and deny rules |
| Is stateful: Return traffic is automatically allowed, regardless of any rules | Is stateless: Return traffic must be explicitly allowed by rules |
| We evaluate all rules before deciding whether to allow traffic | We process rules in number order when deciding whether to allow traffic |
| Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on | Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group) |

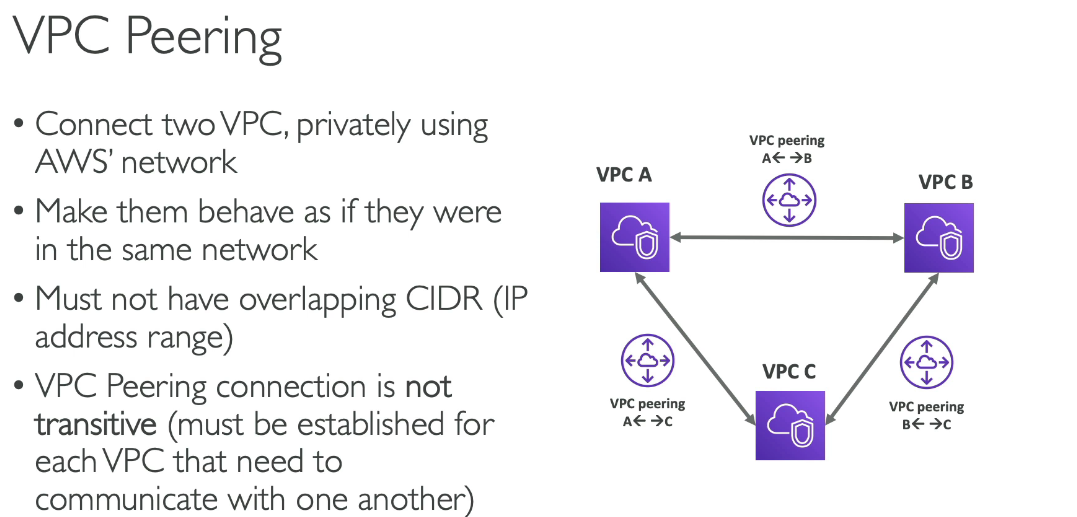
**VPC Flow Logs**

* Capture information about IP traffic going into your interfaces:
  + VPC Flow Logs
  + Subnet Flow Logs
  + Elastic Network Interface Flow Logs
* Helps to monitor & troubleshoot connectivity issues. Example:
  + Subnets to internet
  + Subnets to subnets
  + Internet to subnets
* Captures network information from AWS managed interfaces too: Elastic Load Balancers, ElastiCache, RDS, Aurora, etc…
* VPC Flow logs data can go to S3 / CloudWatch Logs

**VPC Peering**

* Connect two VPC, privately using AWS’ network
* Make them behave as if they were in the same network
* Must not have overlapping CIDR (IP address range)
* VPC Peering connection is not transitive (must be established for each VPC that need to communicate with one another)

In the given diagram on connection between [A,B],[A,C],[B,C][B,A][C,A][C,B]



**VPC Endpoints**

* Endpoints allow you to connect to AWS Services using a private network instead of the public www network
* This gives you enhanced security and lower latency to access AWS services
* VPC Endpoint Gateway: S3 & DynamoDB
* VPC Endpoint Interface: the rest

