Virtual Private Cloud

⇒ Provides a logically isolated section of the amazon web services cloud where you can launch AWS resources in a Virtual Network that you define.

⇒ Its a Virtual Datacenter in the cloud.

⇒ one Subnet == one Availability Zone.

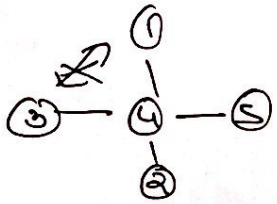
⇒ Soft limit is 5 VPC's for region.

⇒ one Internet gatway for one VPC

⇒ with Default VPC we get both Public & Private ID for EC2 whereas in Custom we only get Private IP

⇒ VPC Peering is connect one VPC with another via a direct network route using Private IP addresses.

⇒ we don't have transitive Peering in the VPC's.



→ when ever we create a new VPC these are generated by own

1) Security group
2) NACL
3) Route Table.

→ First 4, Last 1 in any CIDR block are used by Aws and user cannot use these.

NAT Instances

→ If we create a NAT instance then we can associate this to a route and then this EC2 will be accessing internet.

→ rely on single instance.

→ NAT gateway - IPV4
Egress NAT gateway - IPV6

→ A NAT gateway when added to Route Provides internet to Private Network

→ It is highly available

→ Bastion server is allowed by instances and not in gateways.

→ When creating a NAT instance, disable Source/destination check on the instance

→ NAT instances must be in Public Subnet

→ route out to Private Subnet

→ To increase amount of traffic, increase the instance size. To create high AVailibilty Zone using Autoscaling, multiple Subnets in different AZ to automate failure.

→ Behind a security group.

→ NAT gateway

- ↳ Scale automatically upto 10GBPS
- ↳ Not associated with Security group
- ↳ automatically assigned IP address
- ↳ remember to update route tables
- ↳ No need to disable Source/destination
- ↳ Secure than NAT instance.

Network ACL

→ 1 Subnet to only one Network ACL.

→ By default when we create NACL all inbound and outbound are denied.

→ Ephemeral Port

→ Rules are evaluated in numerical order.

→ These are used to block specific IP addresses.

→ Application Load Balancers need two Public Subnets Present in the VPC.

→ VPC flow logs: It is a feature that enables you to capture information about the IP traffic going to and from network interfaces in the VPC.

→ Stored in cloudwatch logs.

→ created at 1) VPC
2) Subnet
3) Network interface level.

→ You cannot enable flow logs for VPCs that are Peered with your VPC Until the Peered VPC's are in same account

→ You cannot tag a flow log.

→ once created a flow log cant change its Configuration.

→ Traffic which is not monitored is

1) Amazon DNS Server
2) windows instance for Amazon windows licence
3) 169.254.169.254
4) DHCP
5) From reserved IP address of defaut VPC.

→ Bastion Servers is used to give Connection for Private Servers in Private Subnets

→ Bastion is used to Securely administer EC2 instances. in Private Subnets.

→ Endpoints are internal gateways

1) Interface → Singe reource, entry Point
2) Gateway. → highly available. , target.