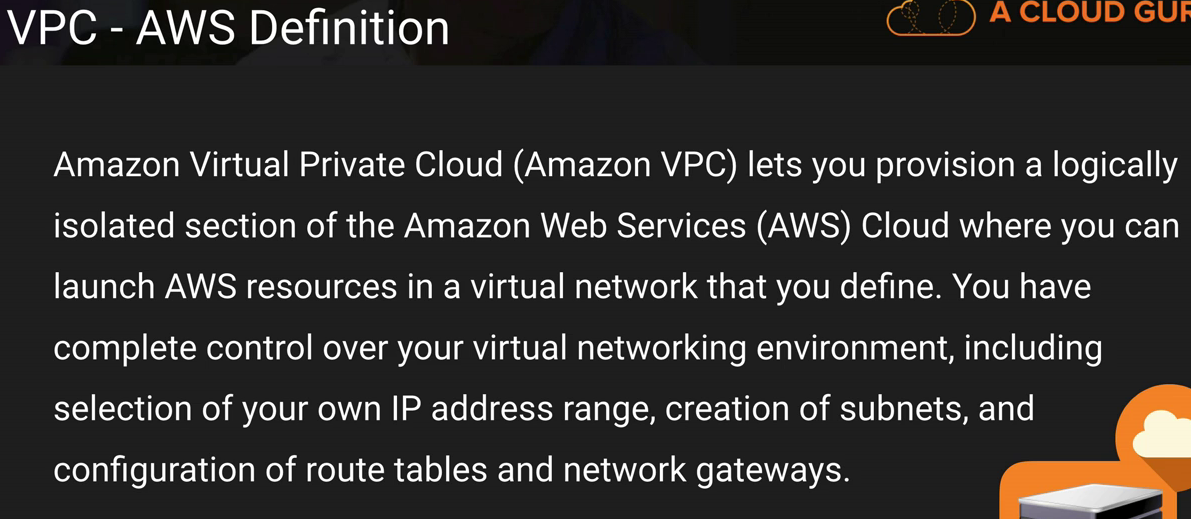
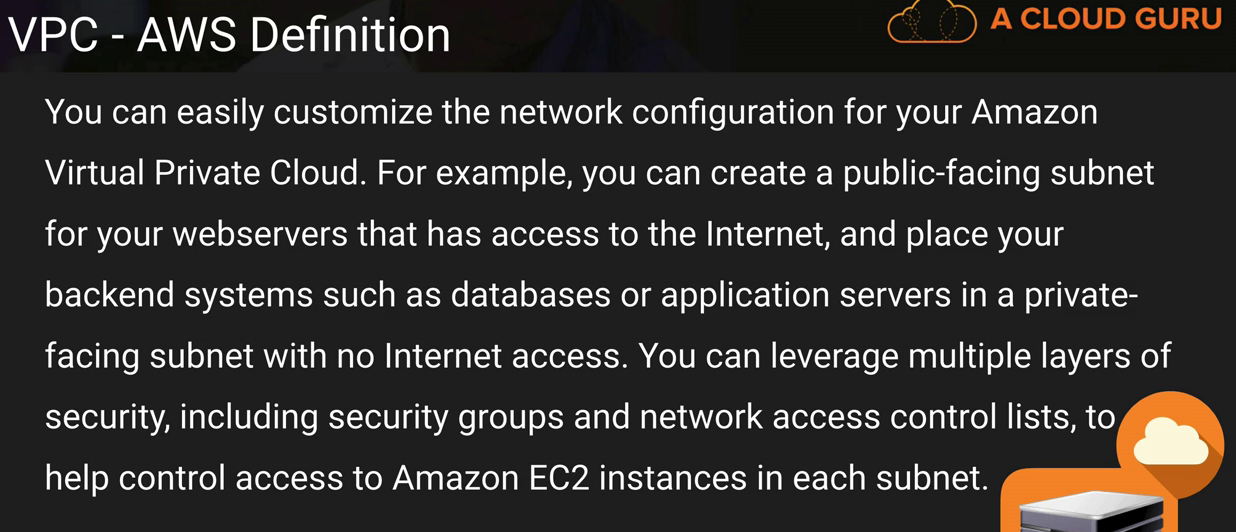
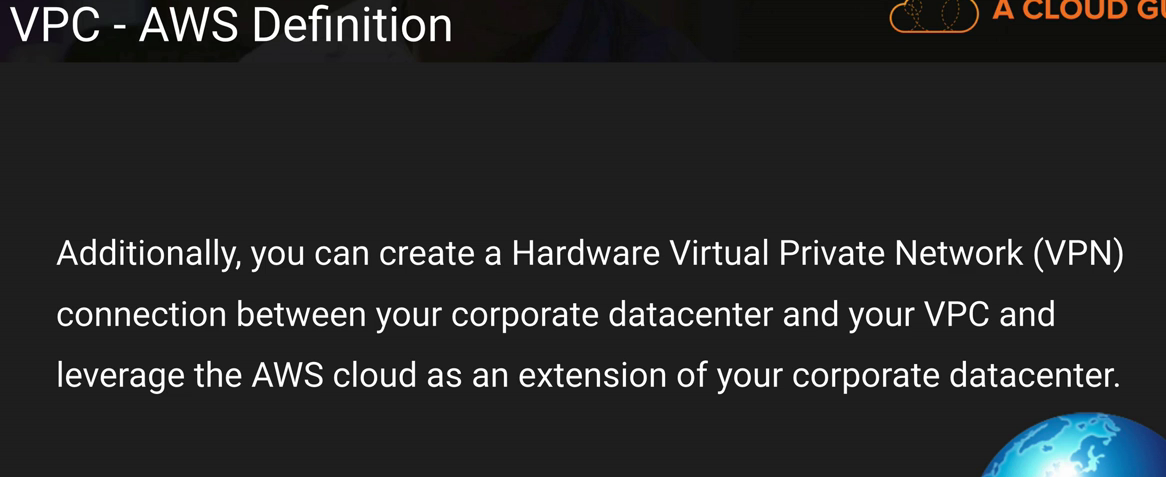
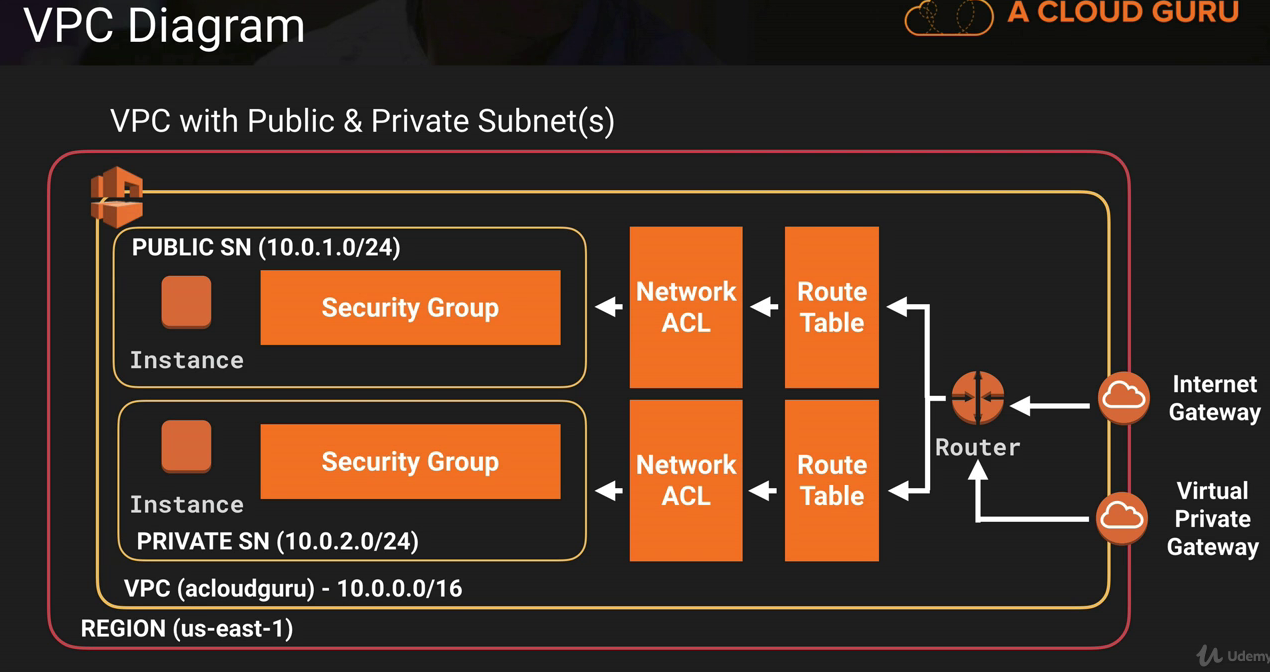
VPC





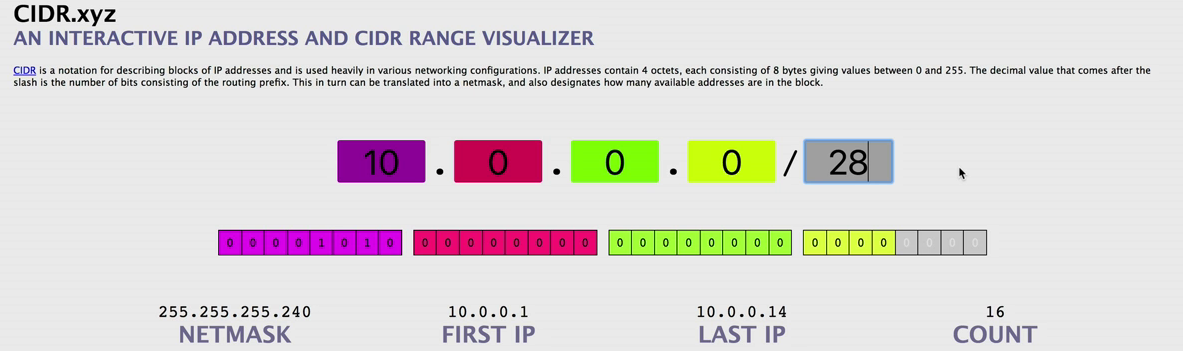




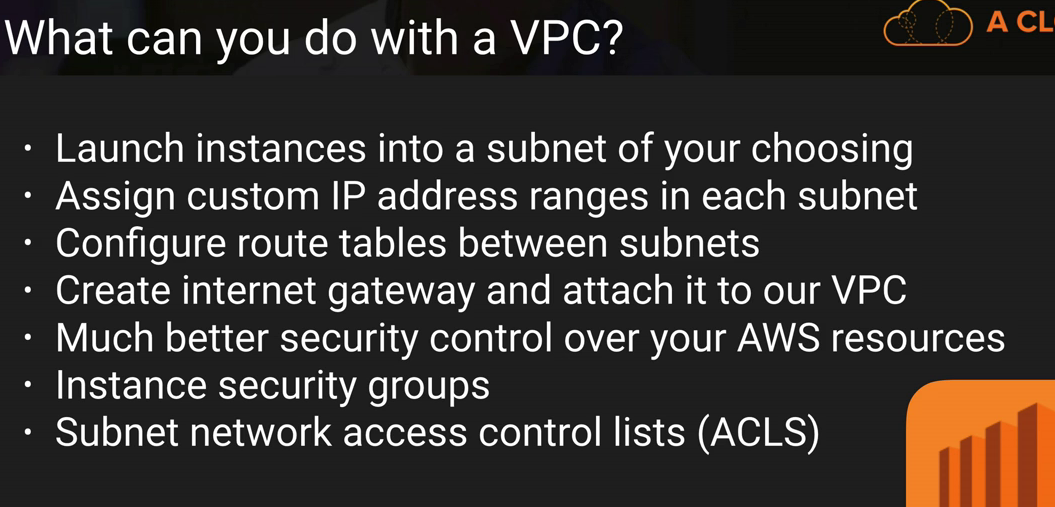
There are two ways to connect to VPC

1. Internet Gateway – Using Internet, It provides internet access.
2. Virtual Private Gateway – Connecting using a VPN(Virtual Private Network)

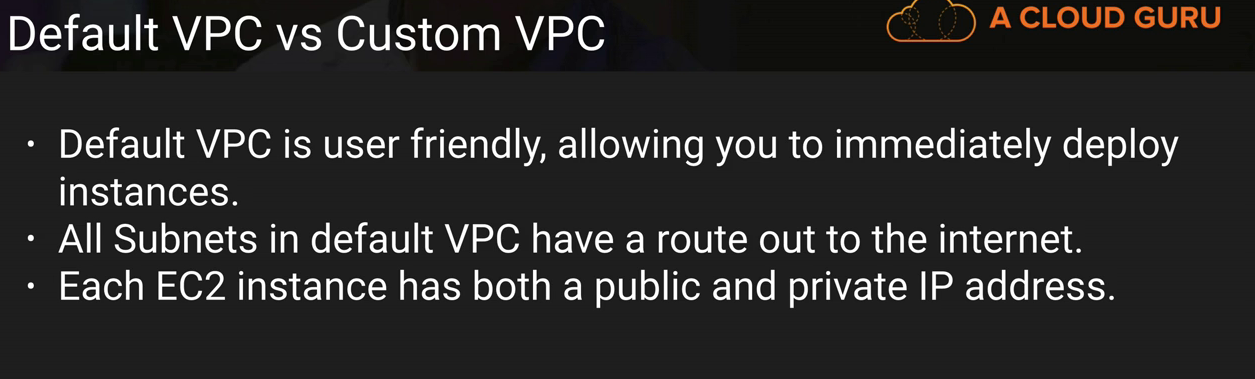


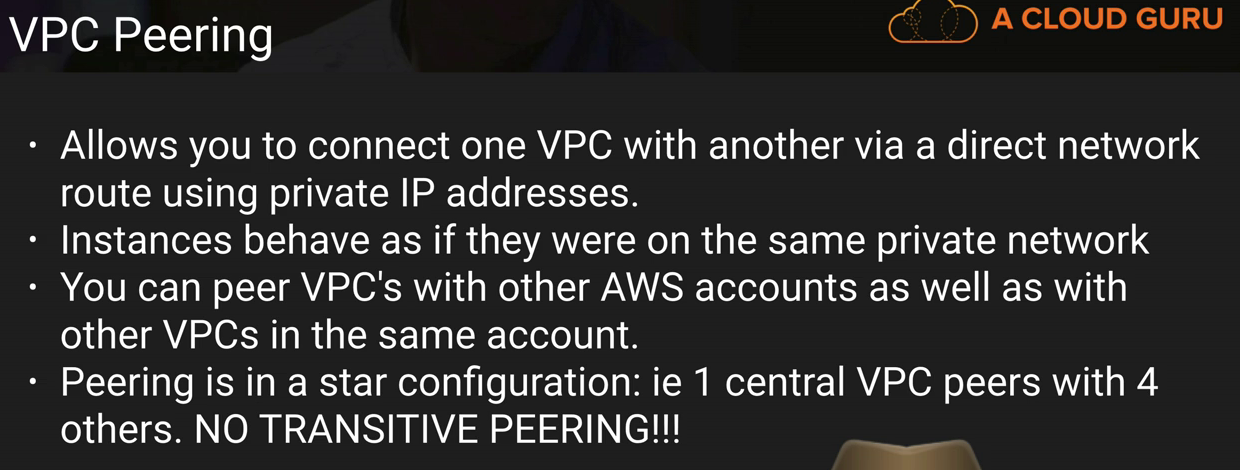


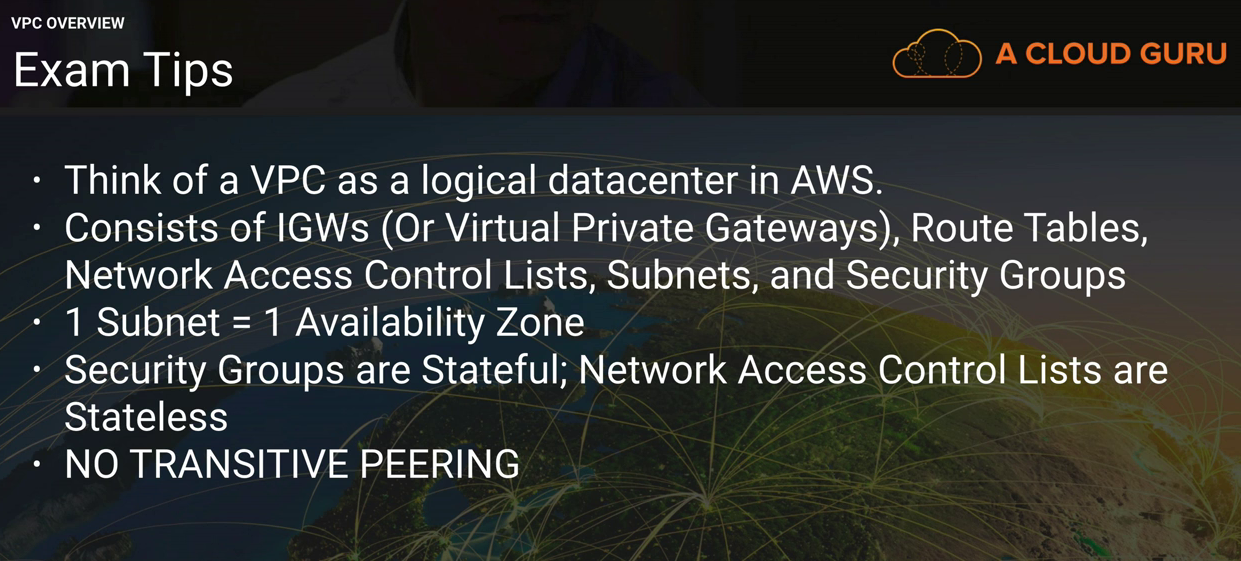
One Internet Gateway per VPC



Did not get private subnets in default VPC





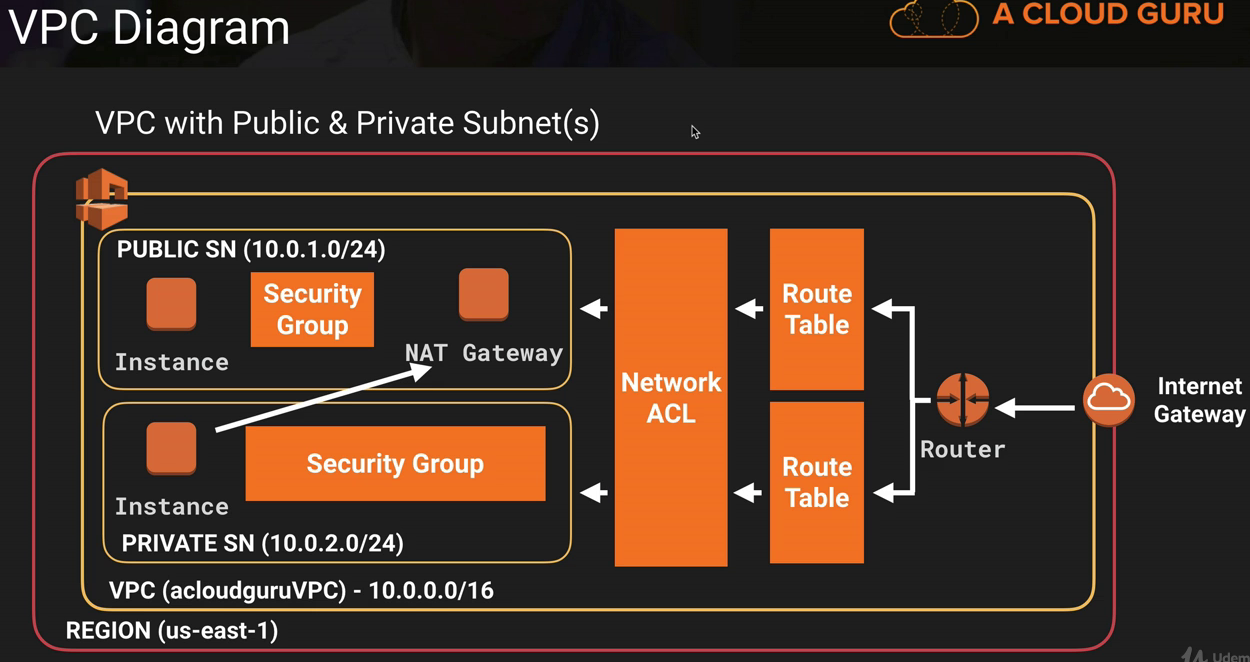


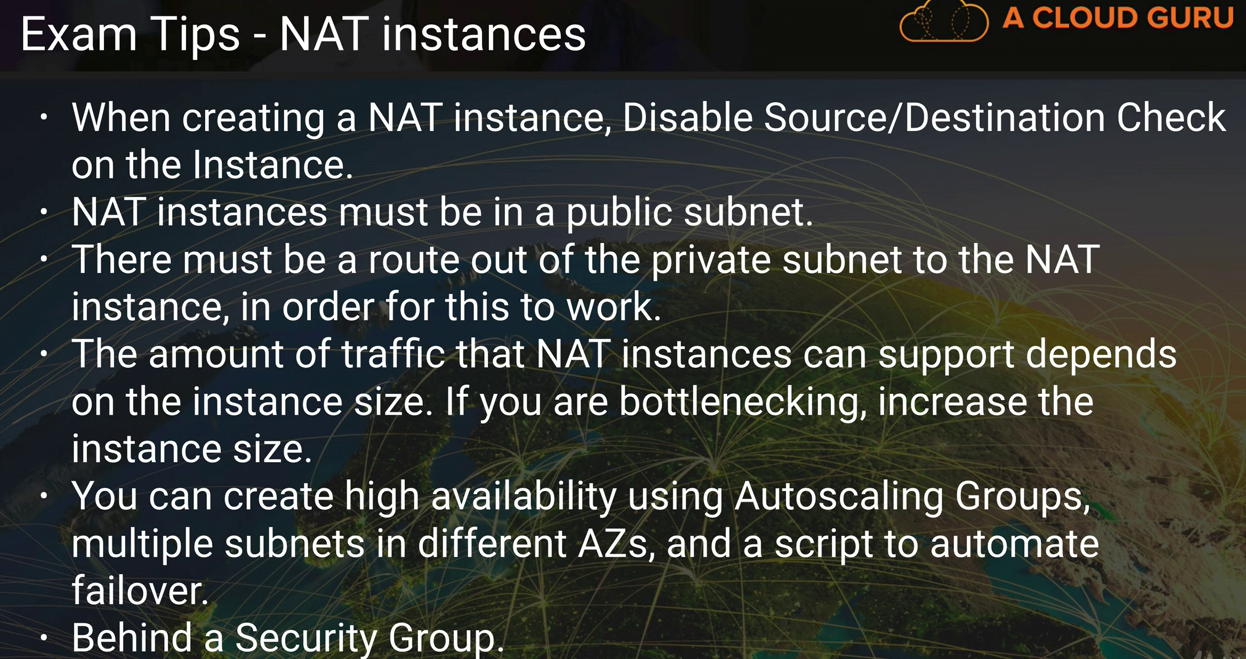
When we create a new VPC, it will create default Security Group, NACL and Route Table for that particular VPC.

When creating subnets (\*.\*.\*.\*/24), 256 ips will be allocated out of which 251 ip’s can be used.

1. The first 4 ip and last 1 ip address of each subnet are not available for use.
   1. 1st ip is Network address
   2. 2nd ip is reserved by AWS for VPC Router.
   3. 3rd ip is reserved by AWS for DNS.
   4. 4th ip is reserved by AWS for future use.
   5. Last ip is network broadcast address.
2. Auto assign public ip address is yes for subnets in default VPC whereas it is no for subnets other than default VPC.
3. Using private key, we can connect to instance which are present inside private subnet.
4. NAT instance
   1. We should keep NAT instance in public subnet.
   2. NAT instance must be able to send and receive traffic when the source or destination is not itself.
   3. Go to the default route table(Private Route table) and add NAT entry here(0.0.0.0/0)
5. NAT Gateway/Egress only Internet Gateway
   1. NAT gateway works on ipv4 whereas egress gateway works on ipv6

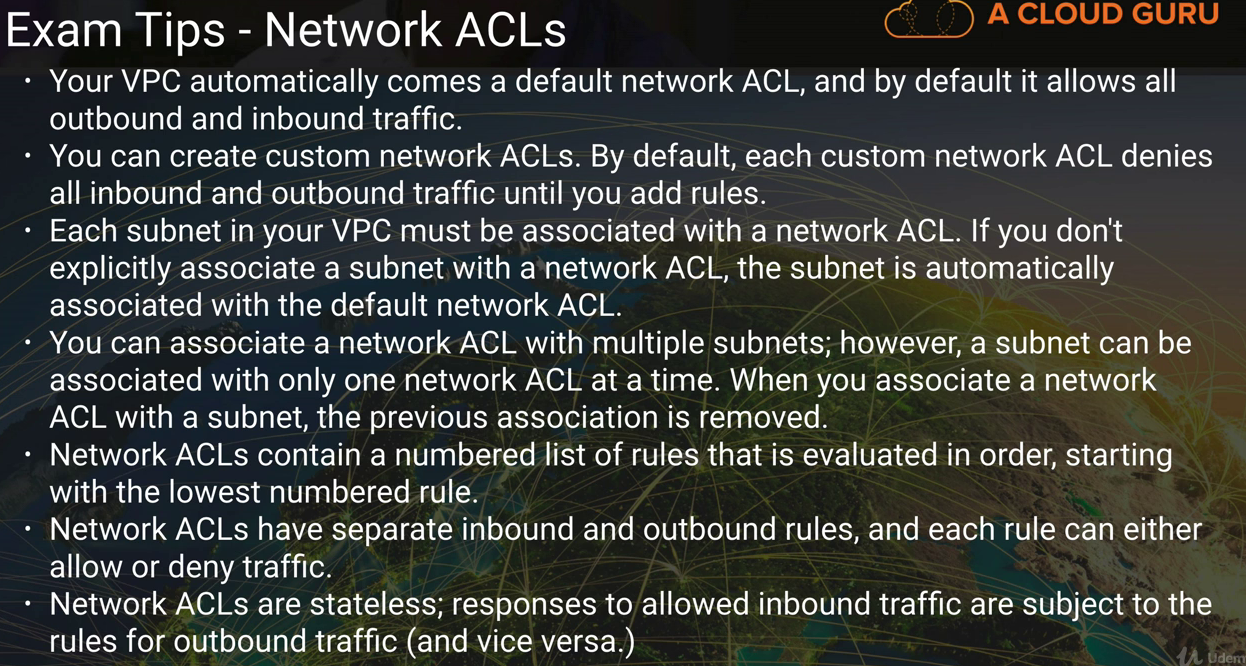


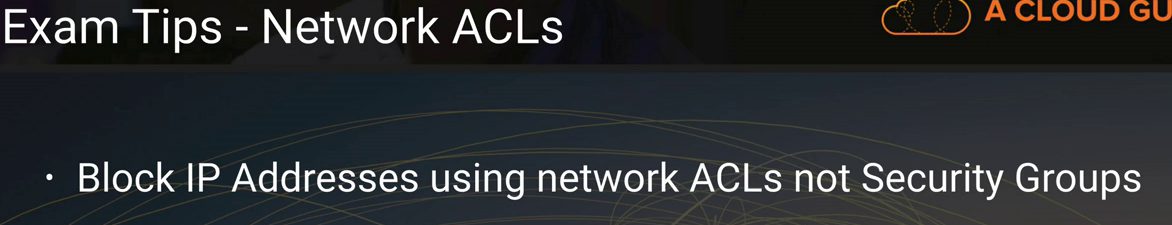


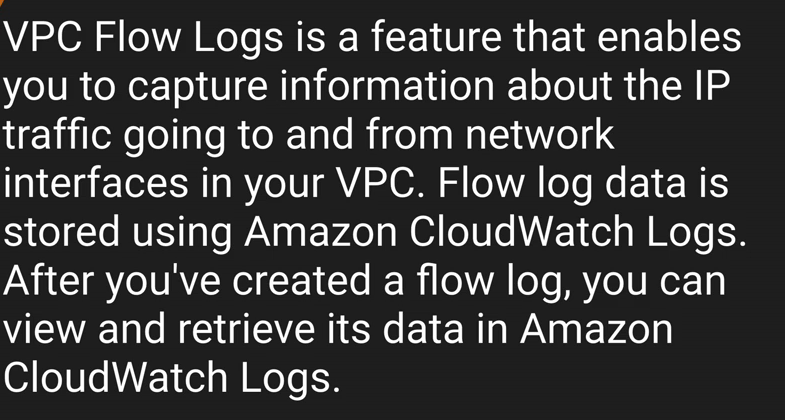


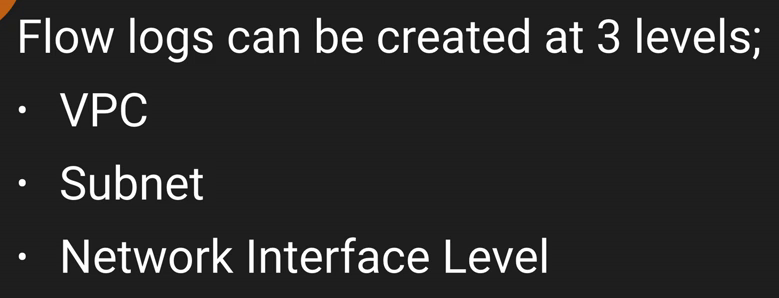


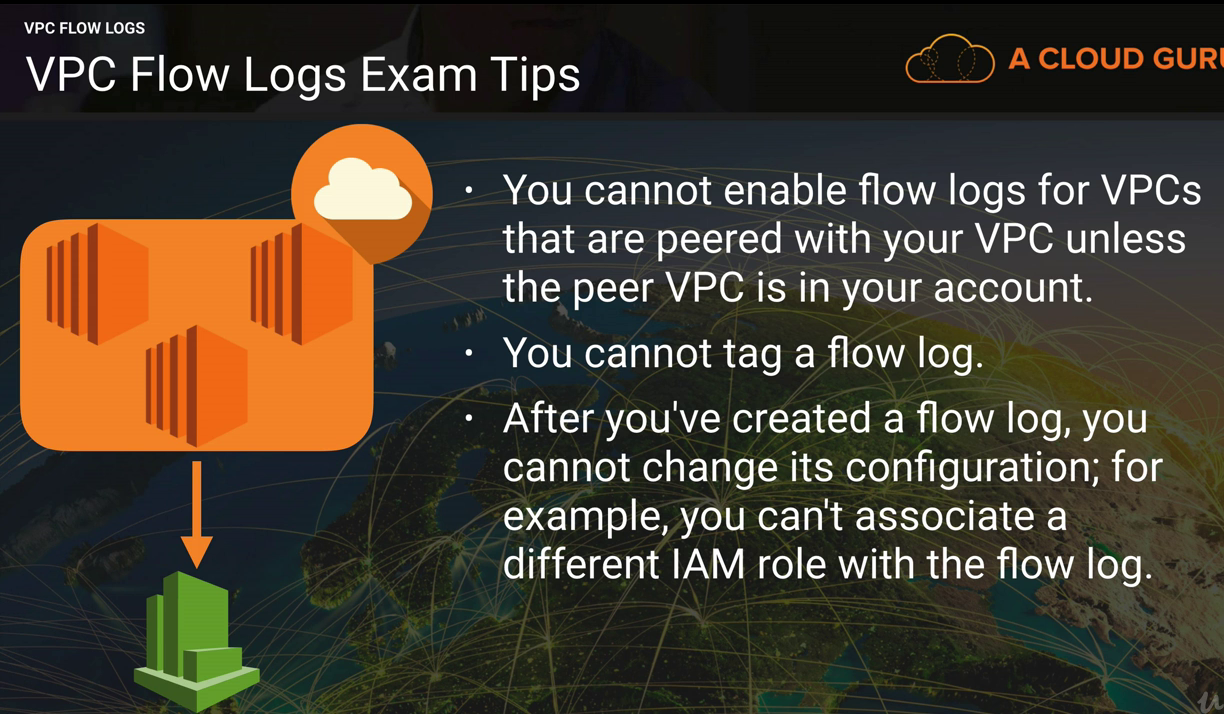
We can assign subnet to 1 NACL.

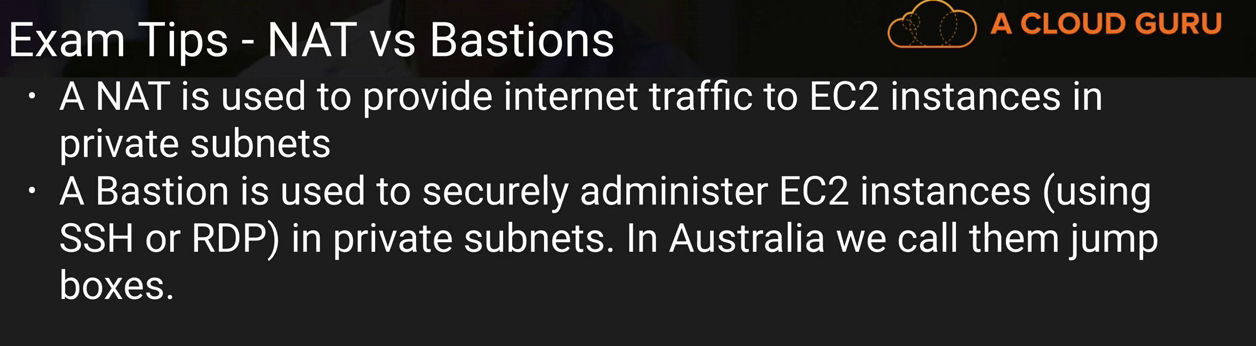












1) Endpoints

a) A VPC endpoint allows you to securely connect your VPC to another service.

b) An interface endpoint is powered by [PrivateLink](https://docs.aws.amazon.com/console/vpc/endpoints/privatelink" \t "_blank), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.

c) A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses.