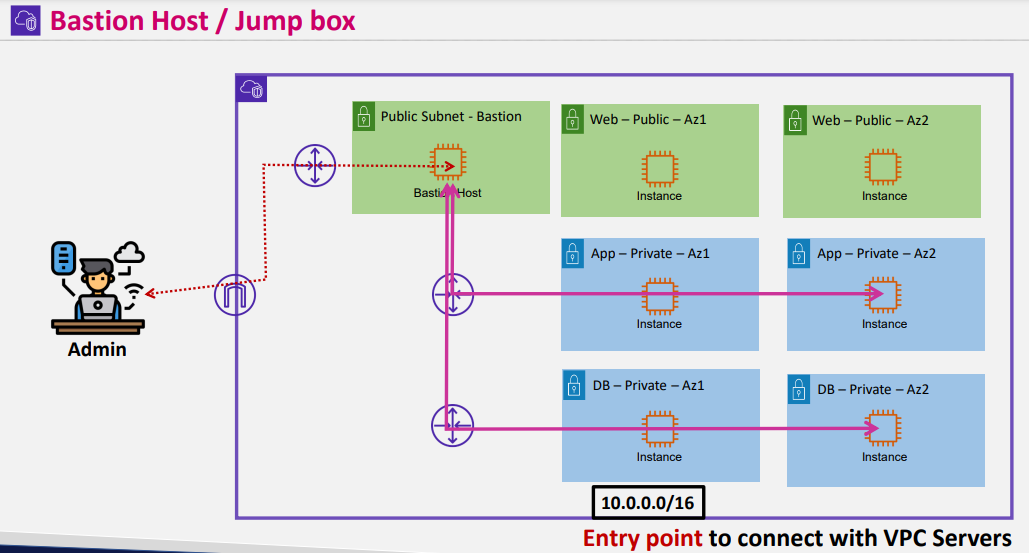


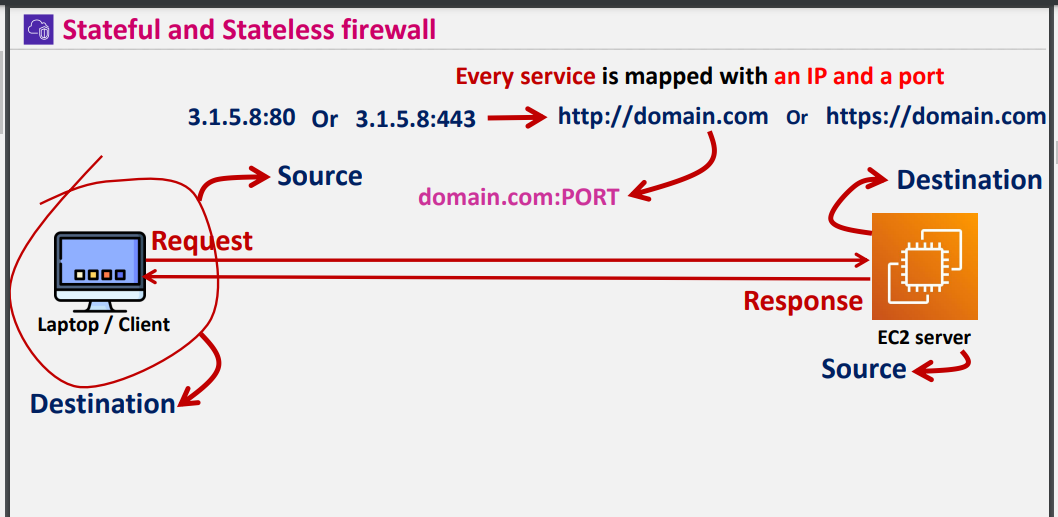
Admin can directly connect to private servers but not public servers directly

* As there is no IGW
* And there is no public IP



* In public subnet we place a bastion host and through that bastion host admin connects to other private servers
* Draw back here is there is no direct connectivity
* But through vpn we can directly connect to private servers
* In real time scenarios we use vpn

**Stafull and stateless firewall imp for exam**

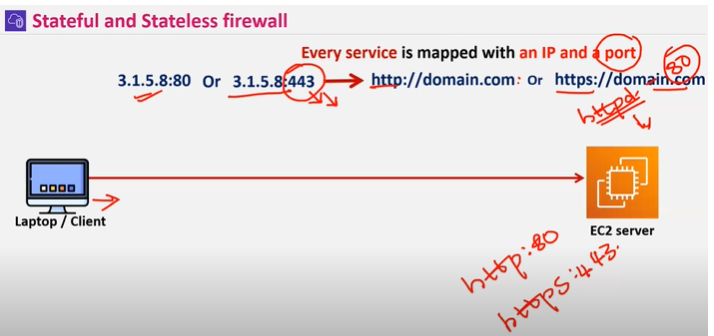
**Y def**

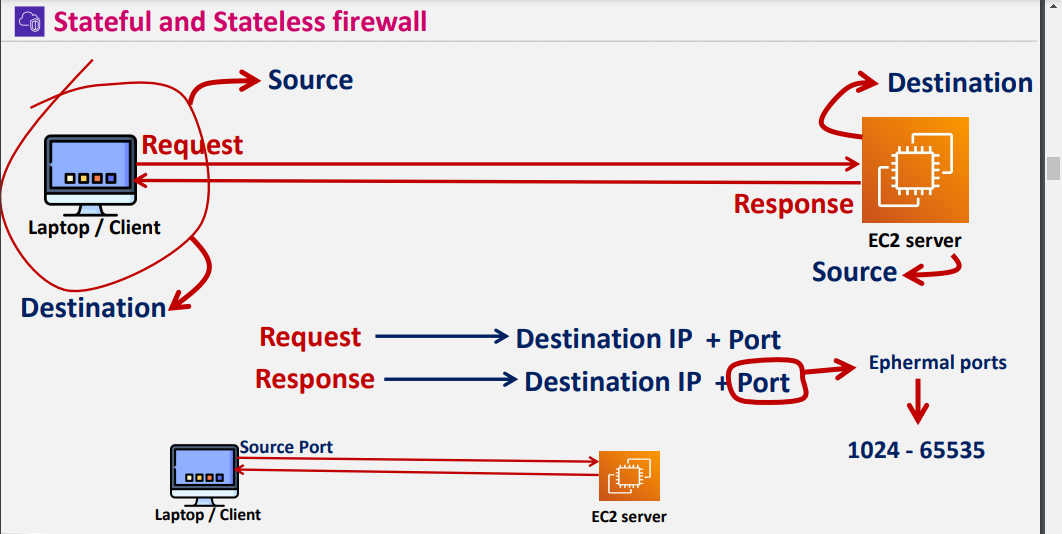
* **Through laptop which ever server you r connecting you will mentioning ip and port then on that particular port server gets request and it will give response**

**For example through http you are connecting IP <-3.1.5.8:80 -> port**

**By default browser adds its domain**

* **From lap request -> raised to server then laptop becomes source and server will be destination from lap top side**
* **And response will be given back to the server**
* **From ec2 point of view again ec2 will be source and again laptop will be destination in response time and its coming from ec2**

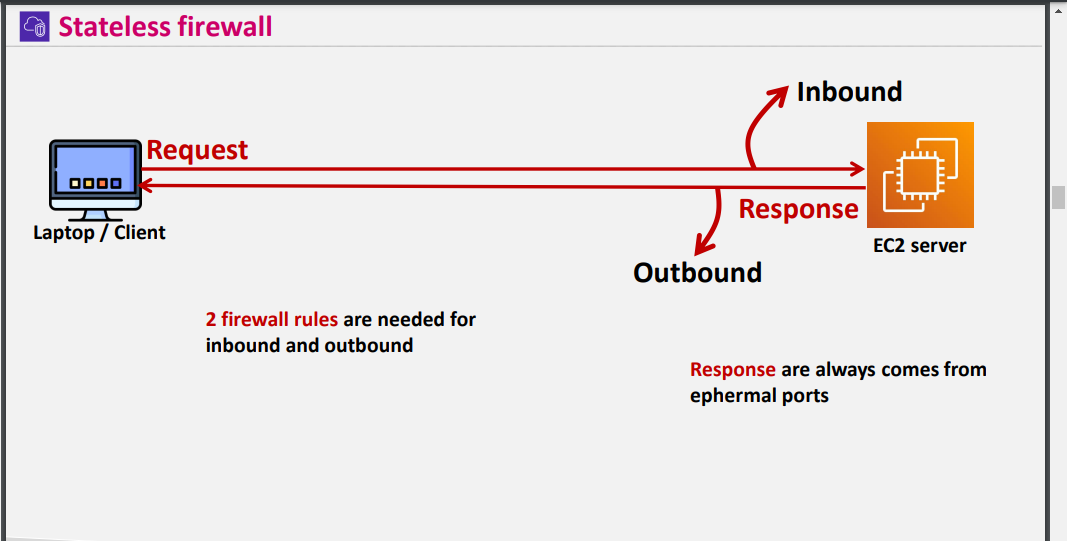
****

****

**IN request time we are mentioning destination ip I.e server ip and in the requesting time only temporary port from laptop gets in touch with vpc**

**So in response time taking that temporary port and laptop ip will receive the response**

* **Total 0-65535 port numbers will be there**
* **Ephemeral ports lies between 1024 – 65535 port no’s**
* **In NACL ephemeral ports will be there**
* **Without Ephemeral Nacl wont work**
* **In Nacl if ephemeral port is open then only response will be received if not no response**
* **Nacl (Stateless firewall)**

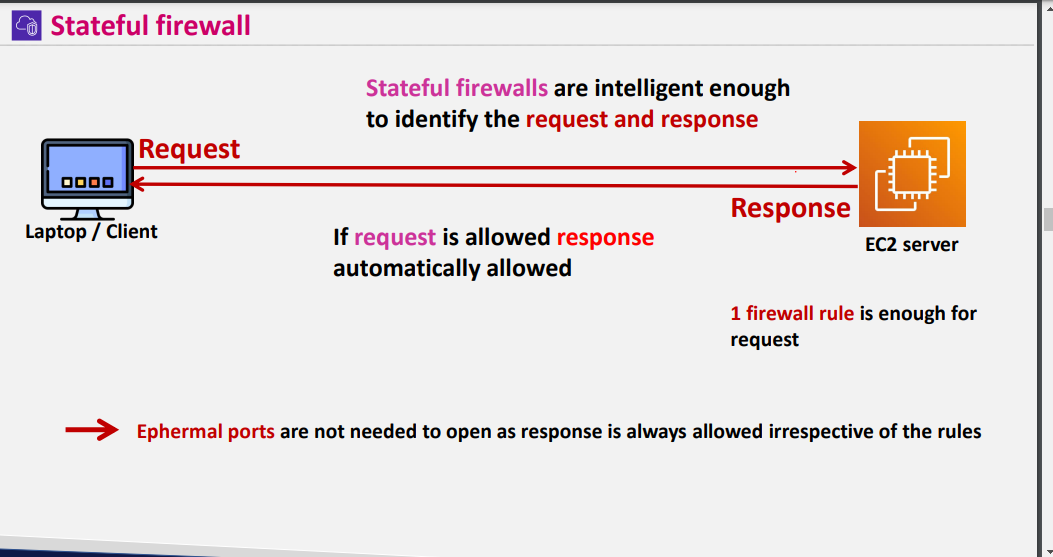
****

**In stateless firewall inbound and outbound should be there**

**REQUEST IS inbound**

**RESPONSE is Outbound**

**For outbound - Ephemeral ports are required**

****

**In statefull firewall only inbound should be allowed automatically it picks outbound and gives the response**

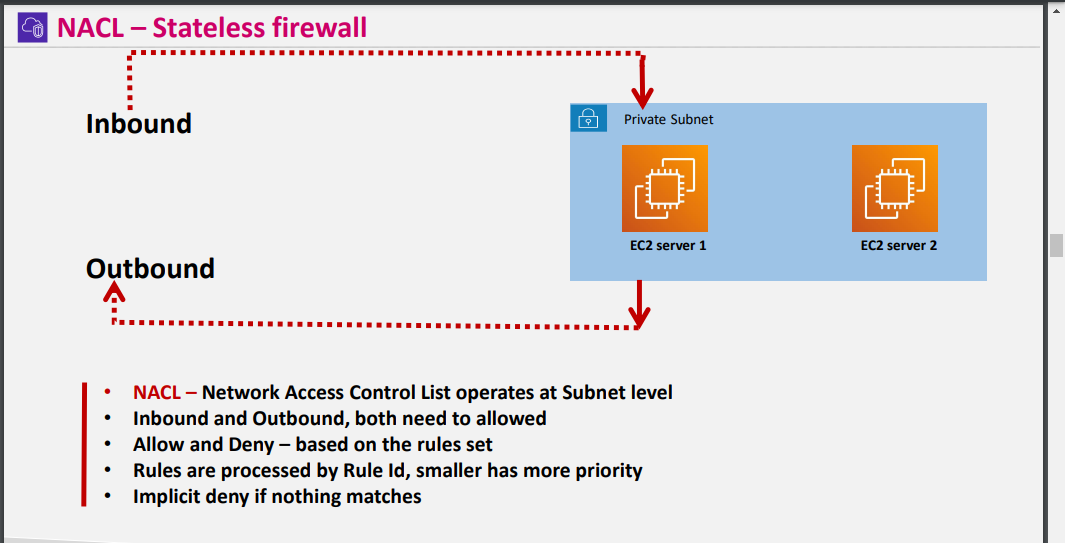
**Even if outbound is not allowed will receive response**

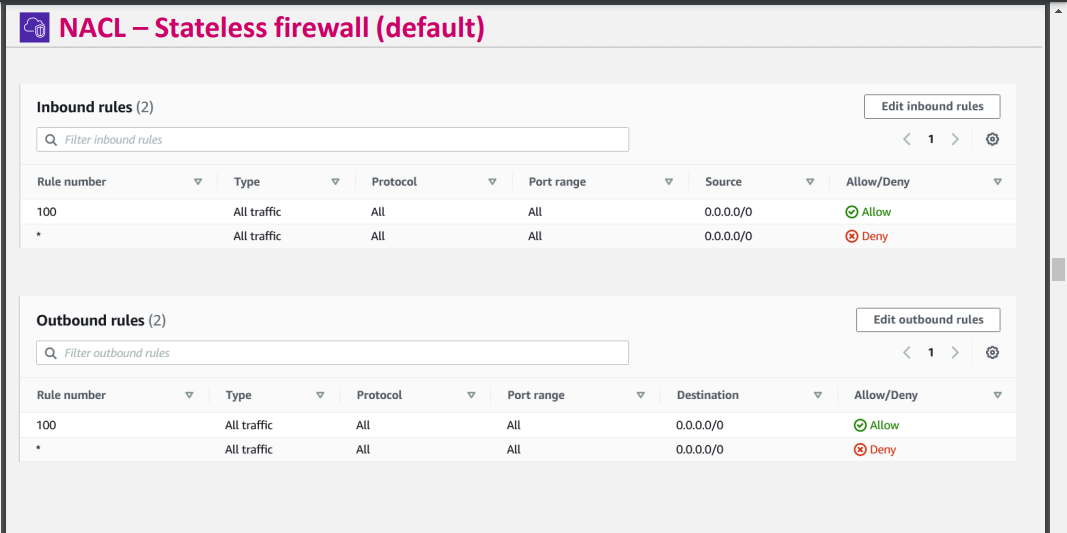
**Stateful firewall is (SG ) INSTANCE LEVEL**

**Stateless firwall is (NACL) SUBNET LEVEL**

* **IN NACL If you want to restrict certain ip’s we can do that**
* **But its not possible**
* ****

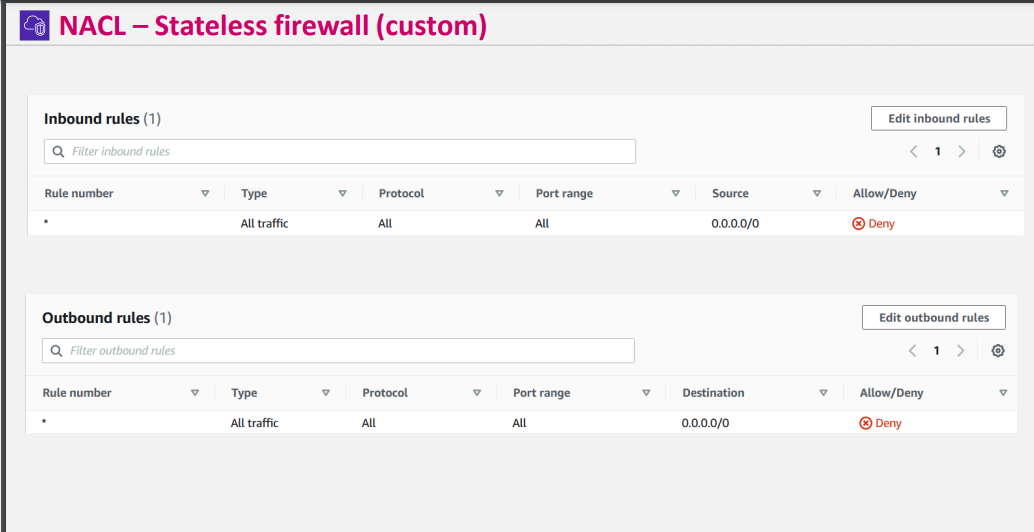
**If rule doesn’t pass by defaultly it takes as deny**

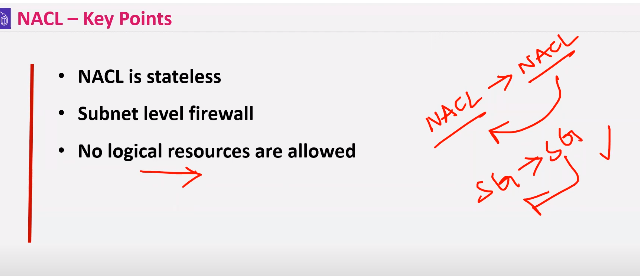
****

****

**NACL BYdefault**

**Nacl(custom) bydefault it will be deny**

****

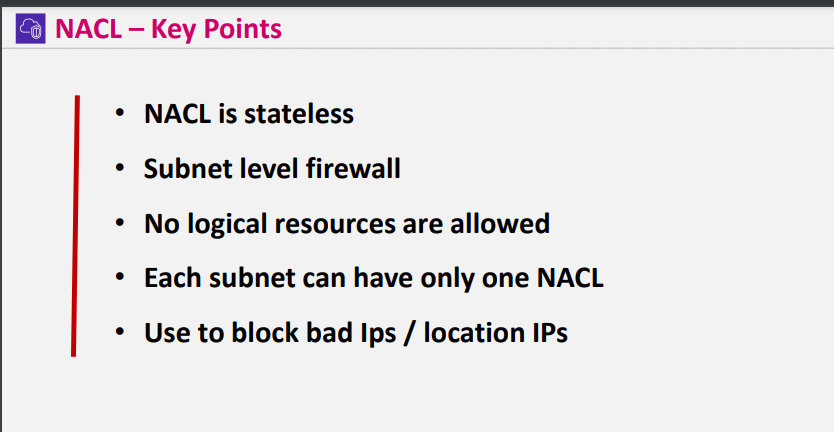
****

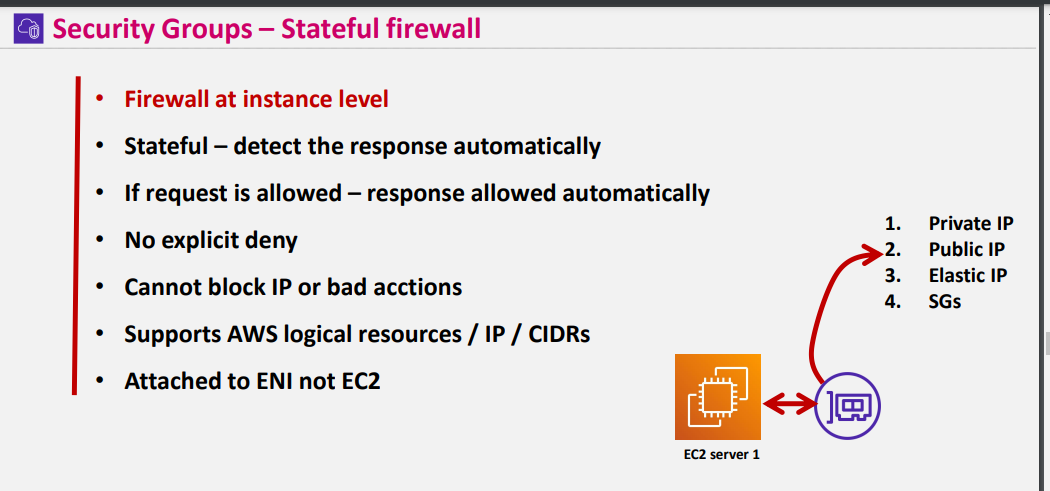
**IN Nacl from one NAcl rule to another NAcl wount be possible but in Sg(security groups its possible)**

**Basing Security grouos id we can allow**

**But in Nacl only Ip and port will be allowed or deny**

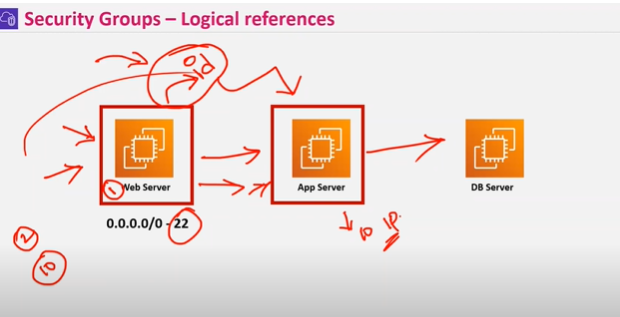
**In SG only allow will be there but no deny**

****

****

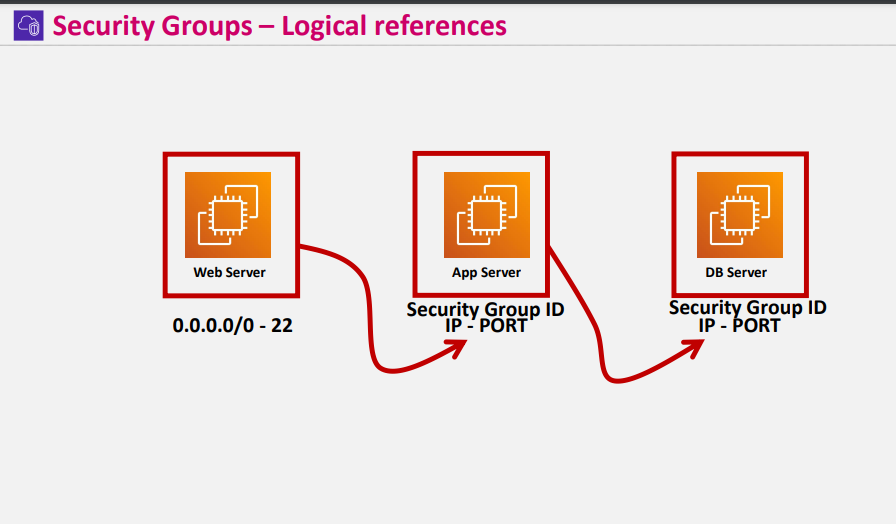
**For every server you are creating there will be NIC cards (network interface cards in aws we have Elastic network interface where sg gets connected to Eni**

**For every laptop or any decice there will be MAC id and that will be defined in ENI**

****

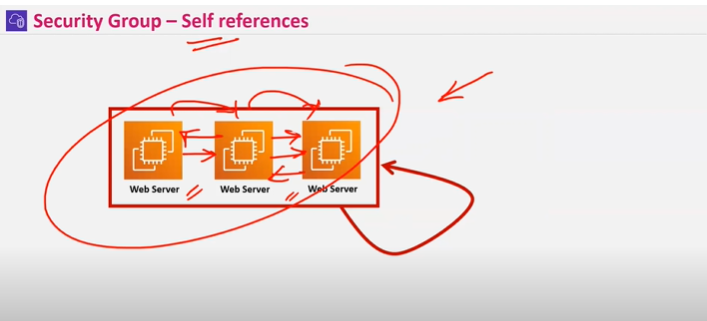
**For example if we have 10 web servers we don’t know the ip’s then we can directly give security group Id of web server to App server then directly connectivity will be created**

**And allowed**

****

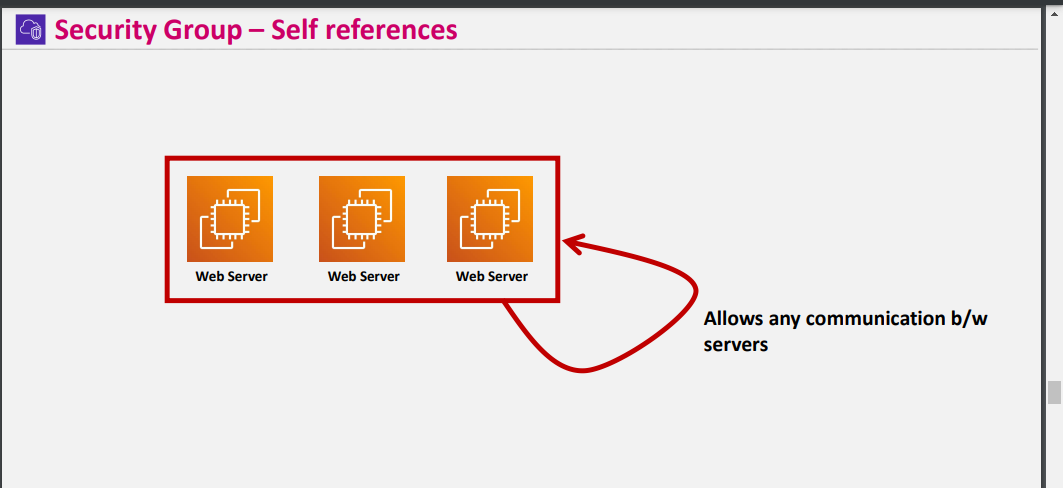
**For best practice Assigning security Group ID**

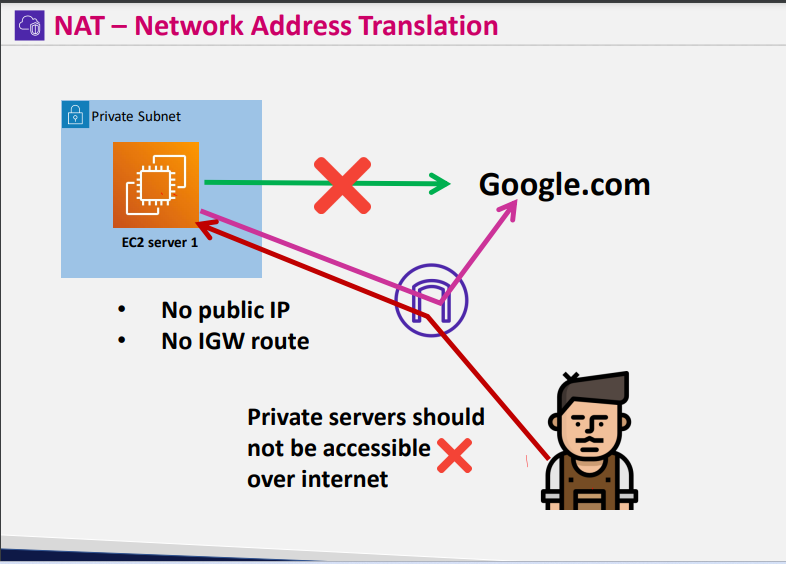
* **Bcz as we place web servers in public subnet**
* **And what ever servers will be there in web server from those only communications goes to private servers by defining web server security group ID**

****

**In same security group attahning to multiple servers for self references**

**And to connect each other easily**

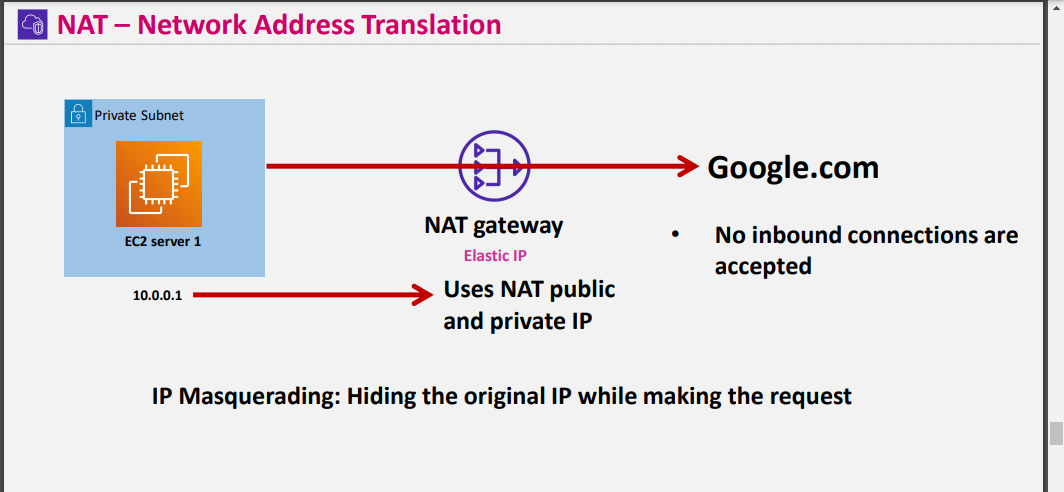
****

****

**Nat gateway is one way traffic**

**No public ip**

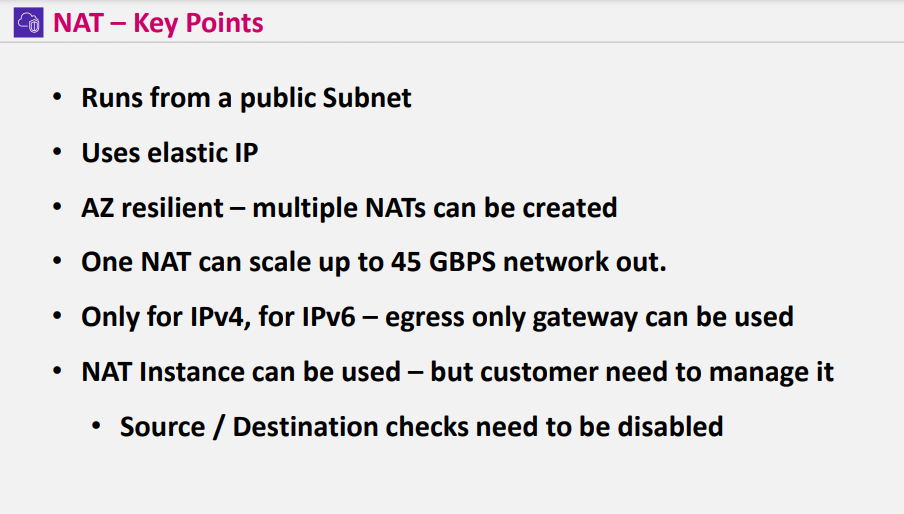
**No Igw**

* **By default you wont get connected to internet**
* **If IGW is attached to to private servers there is a chance for outsiders to connect private server**
* ****

**Nat Gateway should be created in public subnet if its created in private subnet it wont gets internet**

**While private server gets requests -> directly to internet there is a possibility to for threat**

**By using natgateway if an ec2 server is requesting something to internet it original ip will be masquerade by nat and nat ip will be visible**

****

**NAT uses elastic ip**

**Public ip & Elastic ip are same but if we terminate the instance public ip will also be removed**

**And elastic ip wont be removed and it will be reserved when instance is stopped**

* **Elatic ip is chargeable where as public ip wont be chargeable**
* **Nat is AZ resilent – if you want high availability need to create multiple nats according to your requirement**
* **For a Nat instance if you attach it to Eni source request will be visible from which ip request came from**
* **So need to be disable Source / destination checks**

**AGENDA**

* **Create Vpc and Igw and attach IGW To vpc**
* **Create 2 public subnets and 2 private subnets**
* **Create Route table – public & private**
* **Add routes to route table**
* **Create Nat Gateway for one hr (0.056$ per hour)**
* **CREATE Bastionhost server for windows and linux and private servers for windows and linux servers in prvate subnetand connect private servers through bastion host server**
* **In sg of private server remove existing security group and add public server security group id as reference - check inbound and outbound rules after creating**
* **In bastion host SG is created as Bastion host sg**
* **Create s3 bucket and upload key pair if u r using windows**
* **In connecting ping private server from bastion host as icmp ports should be opens**

**Commands wget object url --- of .pem file**

**Check with ls**

**Chmod 400 Bastionhostdemo.pem**

**Copy 4 th command and type**

**Then it connects to private instance from bastion host**

**From second server to 1st server ping**

**Ctrl d – logout to come back to server**

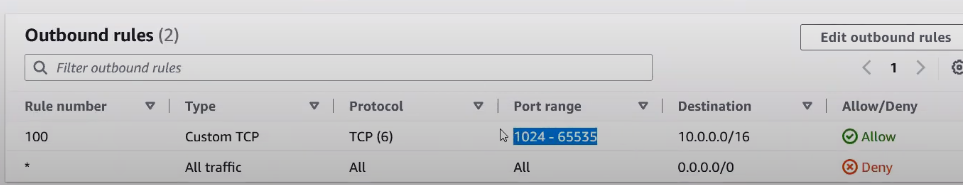
**Hostnamectl command- represents current hostname**

**From second server try to connect google.com by pinging it wont ping as its not connected to natgateway**

**Curl icanhazip.com to check which ip**

**Check by removing outbound rules**

**In Nacl rules**

****