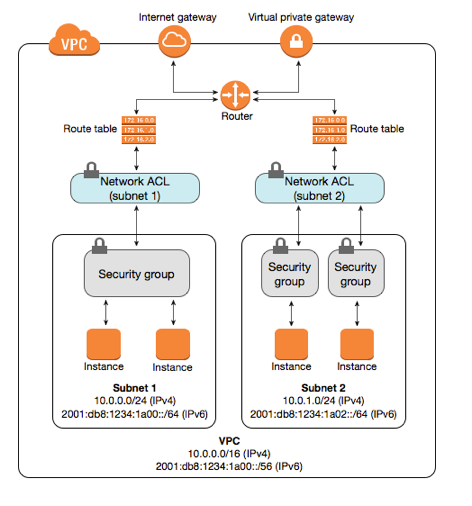
Class 10

**NACL: Network access control lists**

NACL is same as security group that allows the traffic, but security group acts as a firewall for instances where as NACL acts as a firewall for subnets.

NACL is a stateless firewall

Security group is stateful firewall



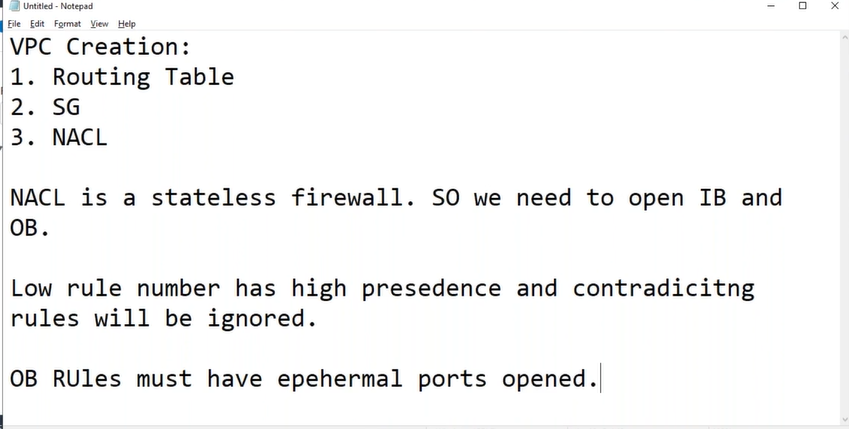
* When we install VPC with that default

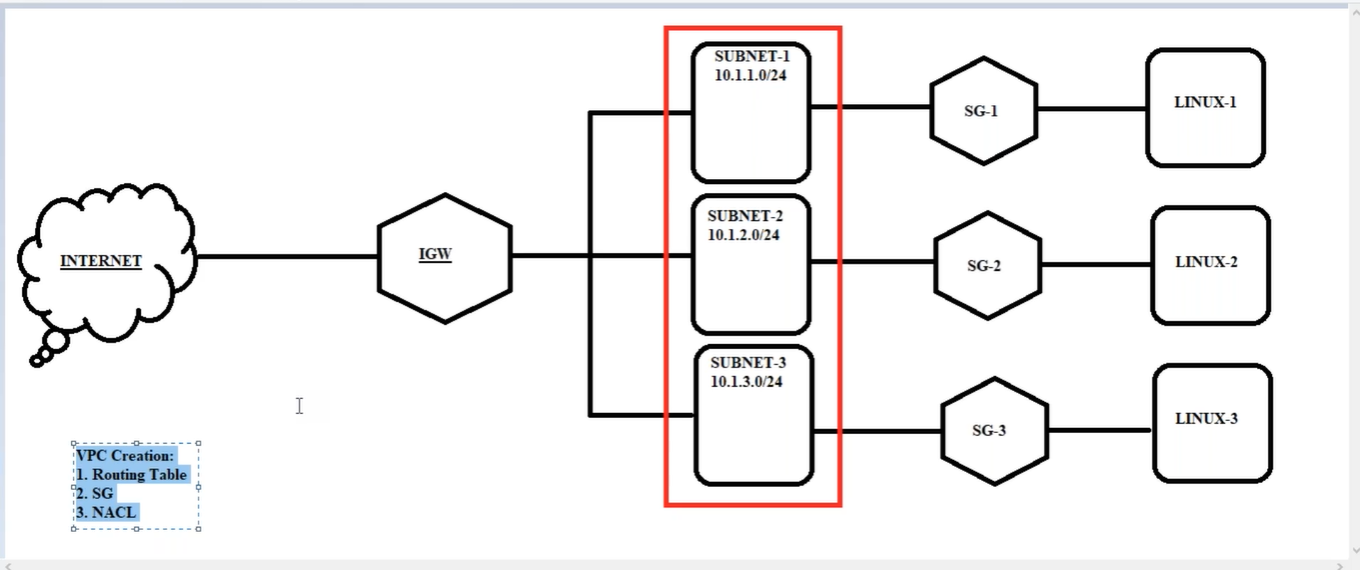
Routing table

Security group

NACL

Are created





Lab:

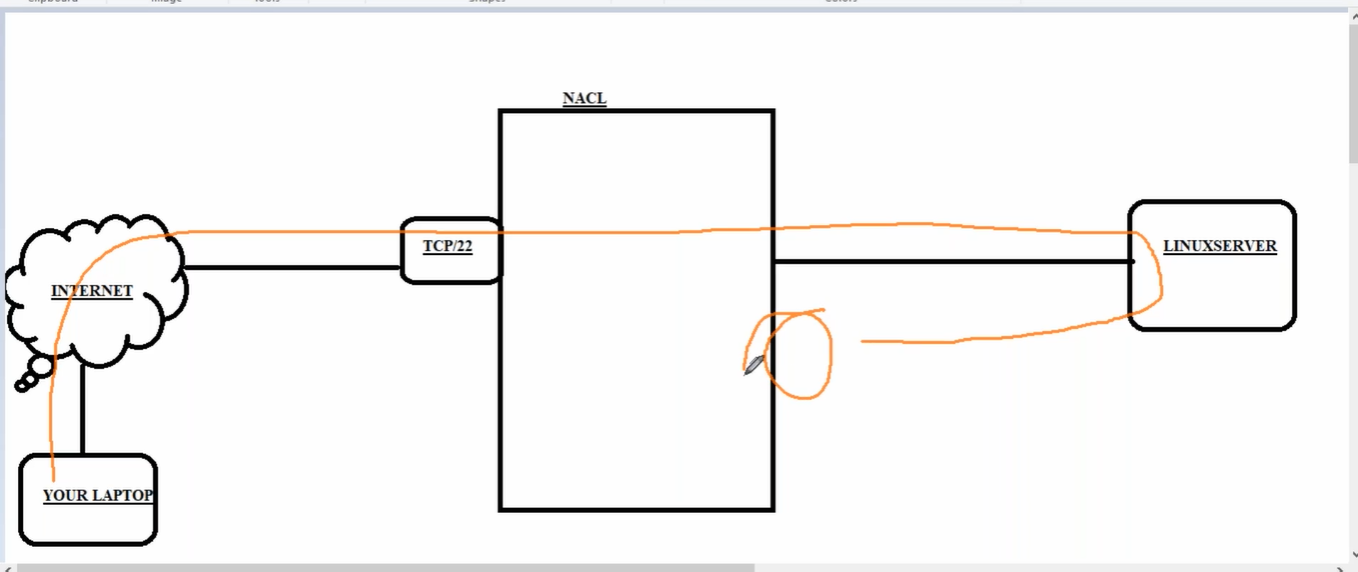
1, VPC navigation

Under “SECURITY”

Network ACLs -> Create network ACL -> Name tag: AWSB26-NACL & VPC\*

AWSB26-NACL -> Edit subnet associations -> AWSB26-VPC-Private-subnet3 (private subnet3) -> Edit

* [we will have all public & private subnets in default NACL, now by creating new NACL and “edit” subnet, means we are moving private subnet 3 to newly created NACL]
* if we see Inbound Rules & Outbound Rules rules will be “DENY” by default



Note: Since NACL is stateless firewall we should ALLOW outbound rules also, whereas Security Group is stateful firewall we no need to ALLOW outbound rules separately it automatically allowed.

* creating two instances in two public subnets and security group allow all (now we have to allow rules or traffic or ports on NACL)

2, Ec2 -> public subnet 1 (which is in **default NACL** with 5 subnets)

Putty -> ec2-user@Public DNS (it connects)

Cmd: ping **PublicDNS** -t (**-t** for continues ping)

* Now go to default NACL list and remove allow all in outbound (since outbound means server to internet when I remove Allow all ping stop)

1, VPC navigation

Under “SECURITY”

Network ACLs -> select default network ACL (which is having 5 subnets) -> Outbound Rules -> Edit outbound rules -> remove ALL Traffic -> save

* Now we can see Cmd: ping **PublicDNS** -t stops

We get **Request timed out.**

Putty also disconnects (because there is no traffic)

1, Network ACLs -> select default network ACL (which is having 5 subnets) -> Inbound Rules -> Edit inbound rules -> allow only **ssh (22)**

**Still it doesn’t ping, still it gets “Request timed out.” Because**

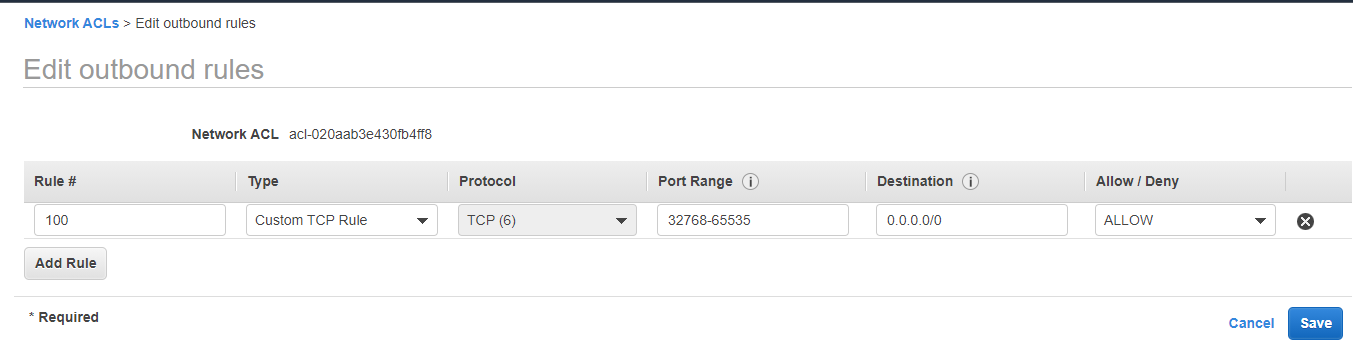
**ICMP: internet control message protocol (this should allow firewall to ping)**

* Here traffic is going to server-1 through ssh(22) port, but to return from server-1 to internet i.e, outbound, takes one random **ephemeral port** between **32768 to 60999**

**[for Linux server range of ephemeral ports** arebetween **32768 to 60999** [**https://en.wikipedia.org/wiki/Ephemeral\_port**](https://en.wikipedia.org/wiki/Ephemeral_port) **]**

**[Traffic that comes inside and goes outside will not work on same port]**

1, Network ACLs -> select default network ACL (which is having 5 subnets) -> Outbound Rules -> Edit outbound rules -> Custom TCP Rule & **32768-65535**



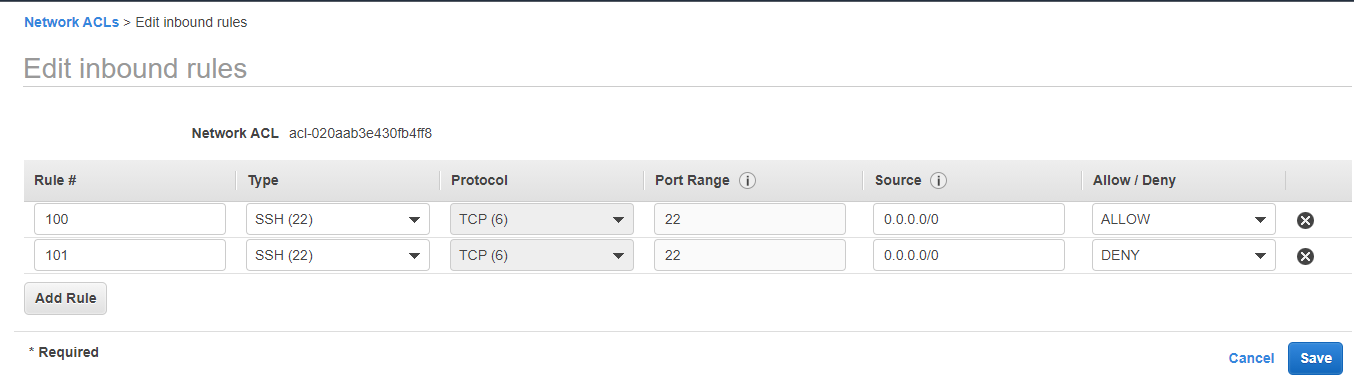
2, go to server putty -> Restart session -> here it get logged in through ssh(22)

Now we know through ssh(22) port traffic goes to server-1 but we don’t know on which port number it comes back.

For that go to - > putty -> netstat (give netstat command) -> Foreign Address -> here out traffic is on port 57448 c-73-119-241-21.h:**57448**

**And each time when we start new session traffic comes in different ports** between **32768 to 65535**

* **In NACL lower Rule number has higher value. For e.g.,**



**Here though we given port ssh(22) Allow and Deny also it Allow rule only because Rule 101 is greater than 100**

**----------------**

**Make all Allow\_ALL after lab**

* **Create another instance and keep in private subnet 3 which is in newly created NACL**

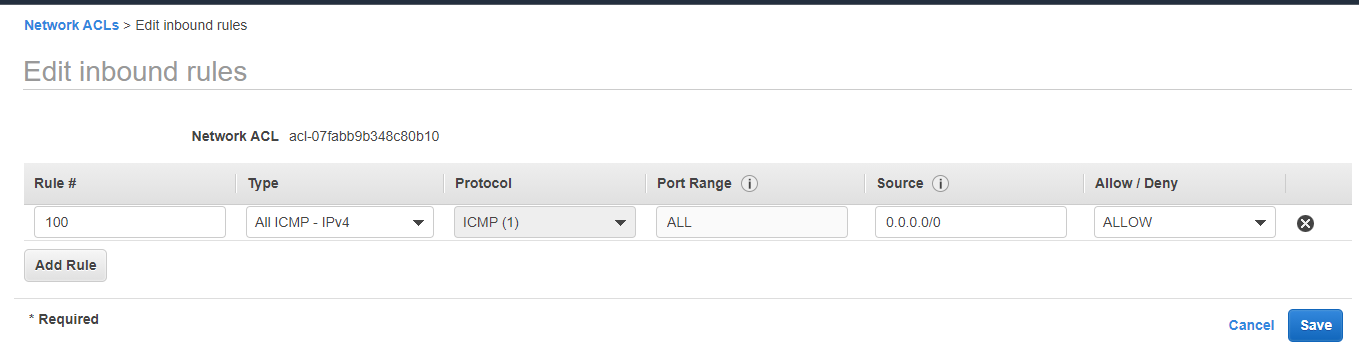
Lab:

1, EC2 -> Server-2

Server-1 -> putty -> ping server-2

* It doesn’t ping because these two subnets are in different NACL’s
* So, we need to allow inbound rules server-2

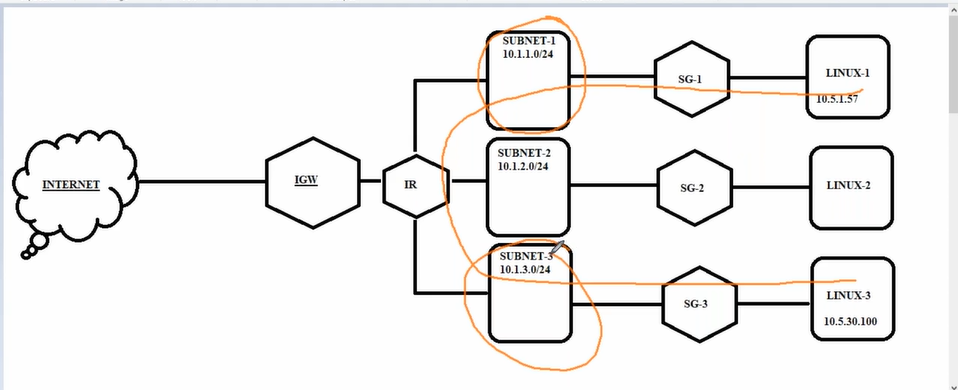
Note: in real-time we don’t use NACL Traffic rules, because it becomes more headache for maintenance



So, in server-2, private-subnet-3, NACL and change in inbound & outbound rules

And it pings only on IP, not on DNS name because we given ICMP-IP

Now it pings………….



**Elastic ip:**

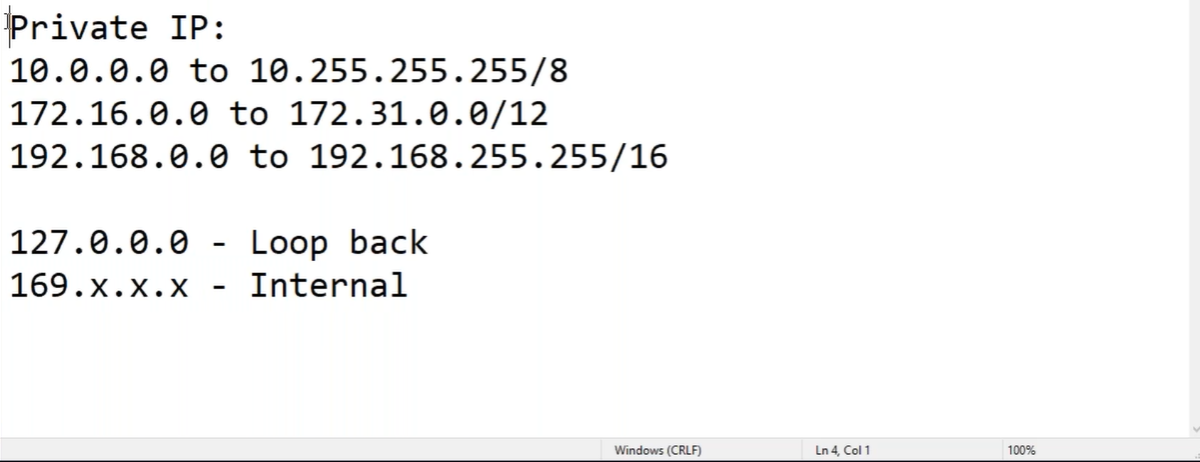
Elastic ip is like a permanent ip we can create it and use of any server

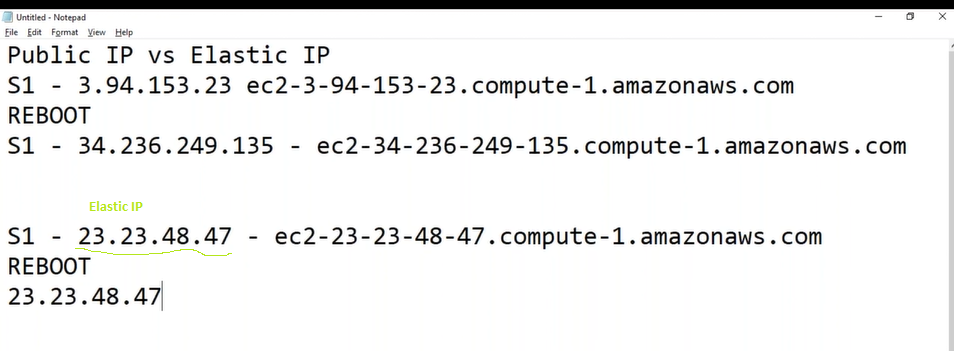
We have 3 types of IP’s

Private IP

Public IP

Elastic IP





* When ever we stop & start our instances our Public IP changes
* To keep it permanent we create **Elastic IP** and assign to server

Note: if we create **Elastic IP,** it is charged

If we assign that **Elastic IP** to server, we get only server price, and we can remove **Elastic IP** and assign to another server, that is why it is called as elastic.

Lab:

1, VPC -> Elastic ips -> Allocate Elastic IP address -> Actions -> Associate Elastic IP address

And also, to delete: disassociate Elastic IP address -> Release Elastic IP address