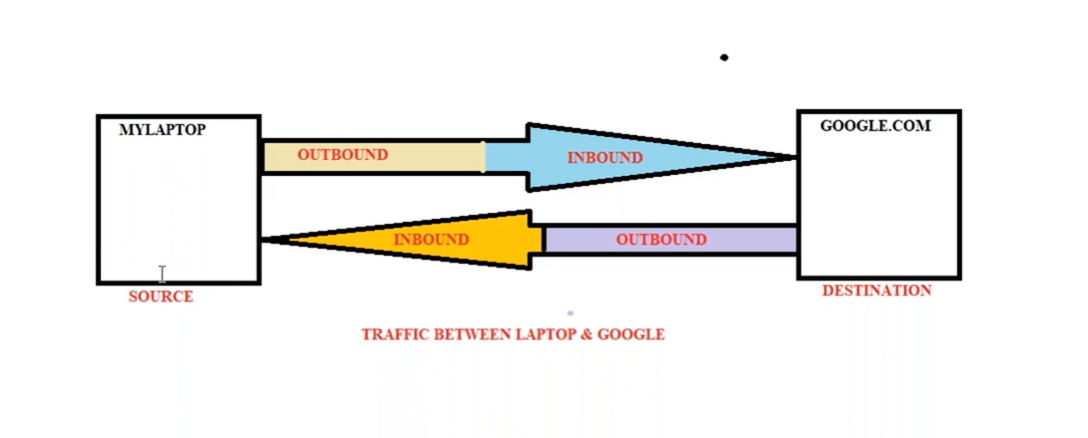
Class9: security groups



1, Traffic

2, Source & Destination

3, Inbound & Outbound



4, Ports

Web instance

* App1 ------------------------------- ssh (service) 22 (port)
* App2
* App3

**How to enable telnet**: So, for that Control Panel\Programs\Programs and Features\turn feature windows on or off\telnet client.

🡺If security group is configured ports 22 & 80

🡪We can check port 22 Is working or not for our instance, for that

[Remote] [ setup box ] [channel no]

Goto windows cmd admin: telnet 34.233.71.221 22 - (To know port 22 is working on that server or not)

| |

Public server port

Public IP

🡪To work port 80 that is for our website (eg, nginx http:// which is port 80)

Putty -> copy server DNS name (to run sample website on port 80 we need to install following cmd)

**Yum update -y && yum install nginx -y**

**Service nginx start**

Now if we want to check port 80 is working or not check : : telnet 34.233.71.221 80

* Tcp/80 -> HTTP (web url)
* Tcp/22 -> ssh (to login into server)
* Tcp/3306 -> mysql (mysql)

Total ports are 0 to 65535 that we use for applications

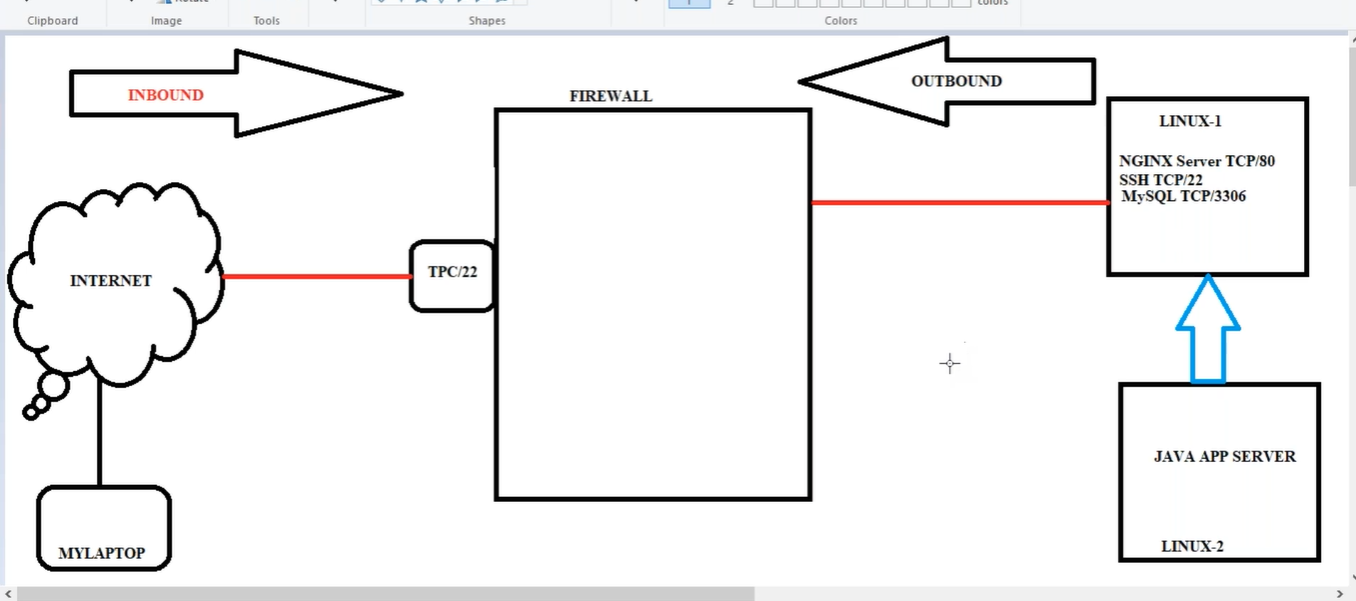
* Standard ports 0 – 1024
* Ephemeral ports 1024 – 65535

5, Firewall

Firewall can control or restrict, inbound or outbound traffic, there are 2 types

1. Stateful firewall
2. Stateless firewall

Security group is stateful firewall, it can be applied to all AWS resources like EC2, RDS, Lambda etc.… except subnets, in simple words Security group is like a server firewall.



**Create security group to restrict with firewall:**

VPC -> Security group -> Allow\_access\_webserver tcp/80 -> inbound rules HTTP 80-> -> HTTP & 0.0.0.0/0

We no need to give outbound, because in stateful firewall, we allow traffic inside, again comes outside no control.

**Server-1**

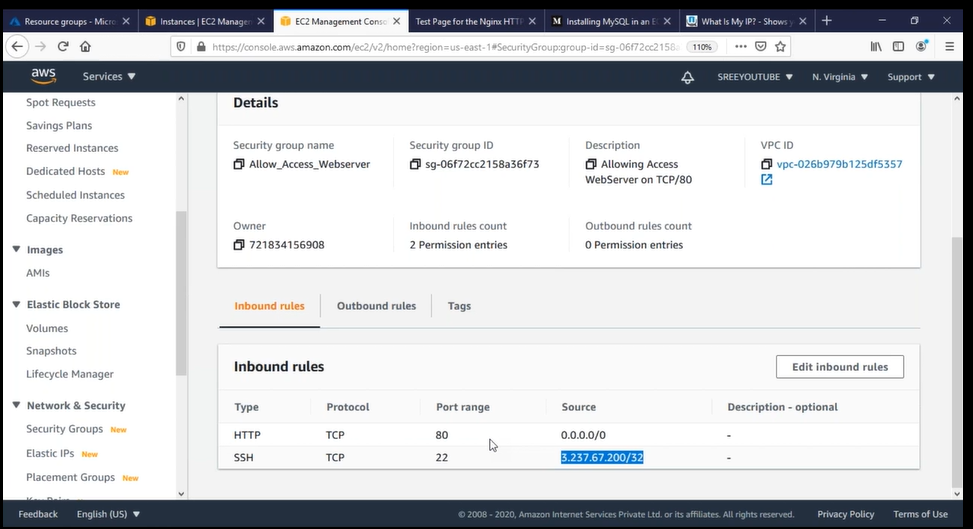
**Port 80**: Go to Linux-1 server (80/22/3306) -Rc- Security– change security groups -> HTTP & 0.0.0.0/0 (this allows all servers if there are).

So, this server access TCP/80 port only, if we go to putty and connect this server, we get error because it runs on ssh 22

**Port 22**: Now if we want to login to server, we should allow port 22 also

so, go VPC -> Security group -> Allow\_access\_webserver -> inbound rules ->add Tcp/22 & 0.0.0.0/0 ssh in inbound rules, 22 get access for all servers,

if I want to restrict port 22 for only my internet router server, we can go to google and type “what is my ip address” and give IP/32. In place of 0.0.0.0/0 we give 73.119.241.21/32 it will work in only my home network



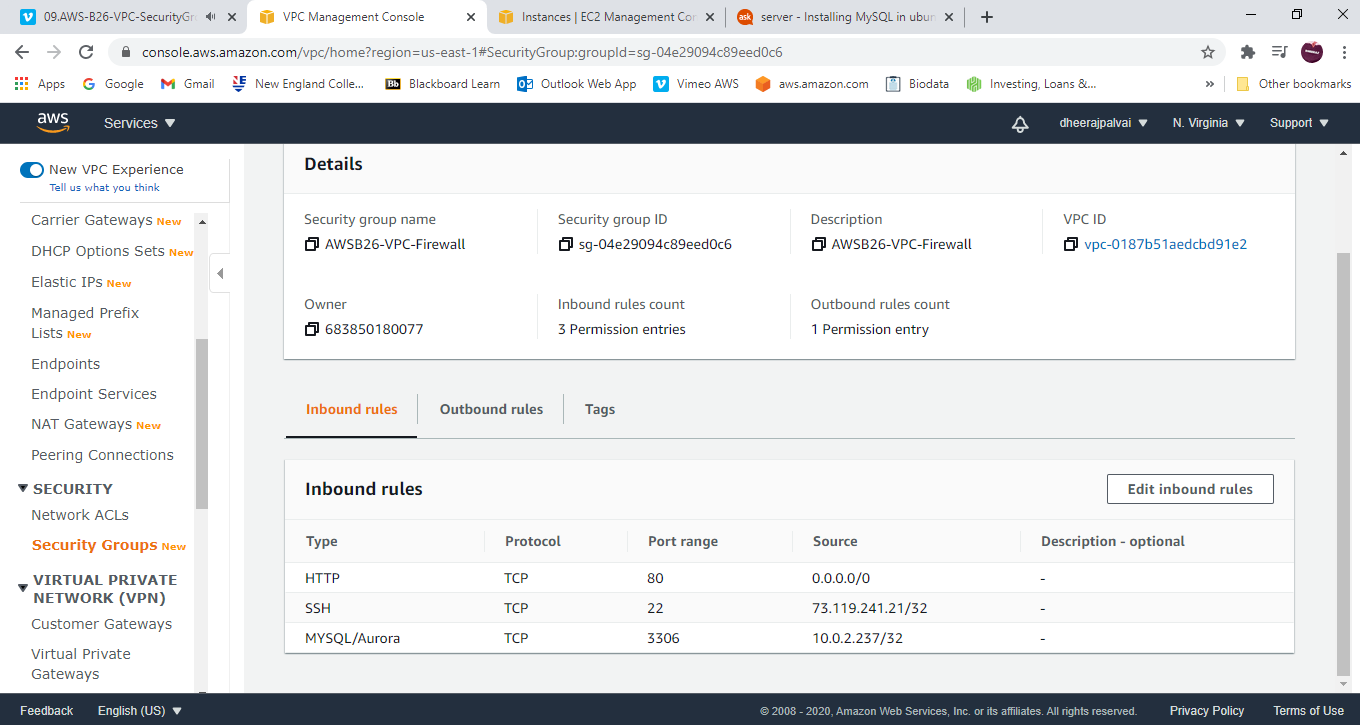
**Outbound**: Now if I go to severer 1 through putty, and give : telnet localhost 3306 menace it does not allow because in stateful firewall traffic comes from and out to inside server and goes out, here in stateless firewall it doesn’t come from server to outside, server 1 is not allowing MySQL server

As per Lab, in Security groups we gave inbound but not given outbound that’s why telnet is not allowing

Go to -> Security group -> Allow\_access\_webserver -> outbound rules ->add Allow all traffic

Install my-sql: Yum install mysql-server -y

Go to -> Security group -> Allow\_access\_webserver -> inbound rules ->add MySQL-> allow server 2 ip (to access MySQL which is in server1)



**Server-2**

Go to install Linux-2 java app server – in subnet 3

Putty -> yum install -y telnet

Now my server 2 must connect to DB in server 1

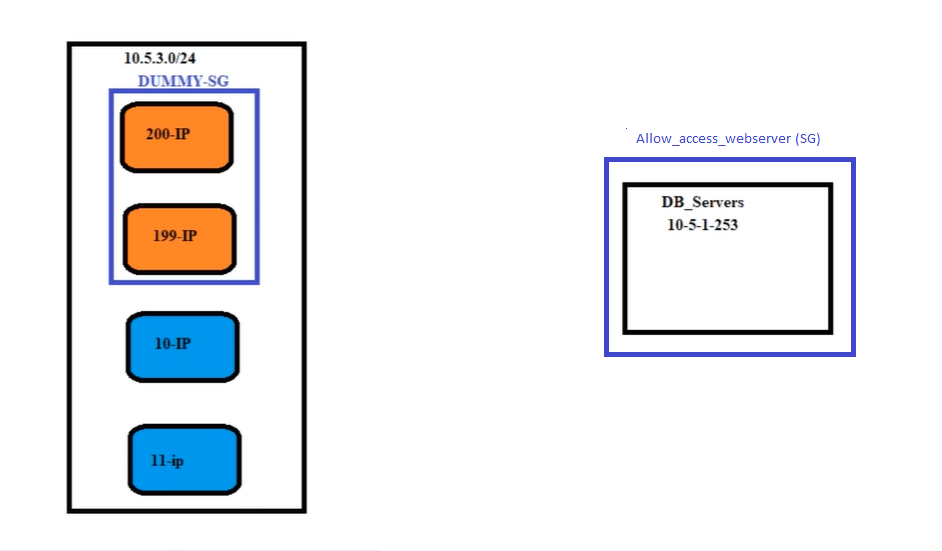
Putty -> telnet server1ip 3306 it does not allow because port is not open (go to server1 and allow security group for my-sql for server2 ip)

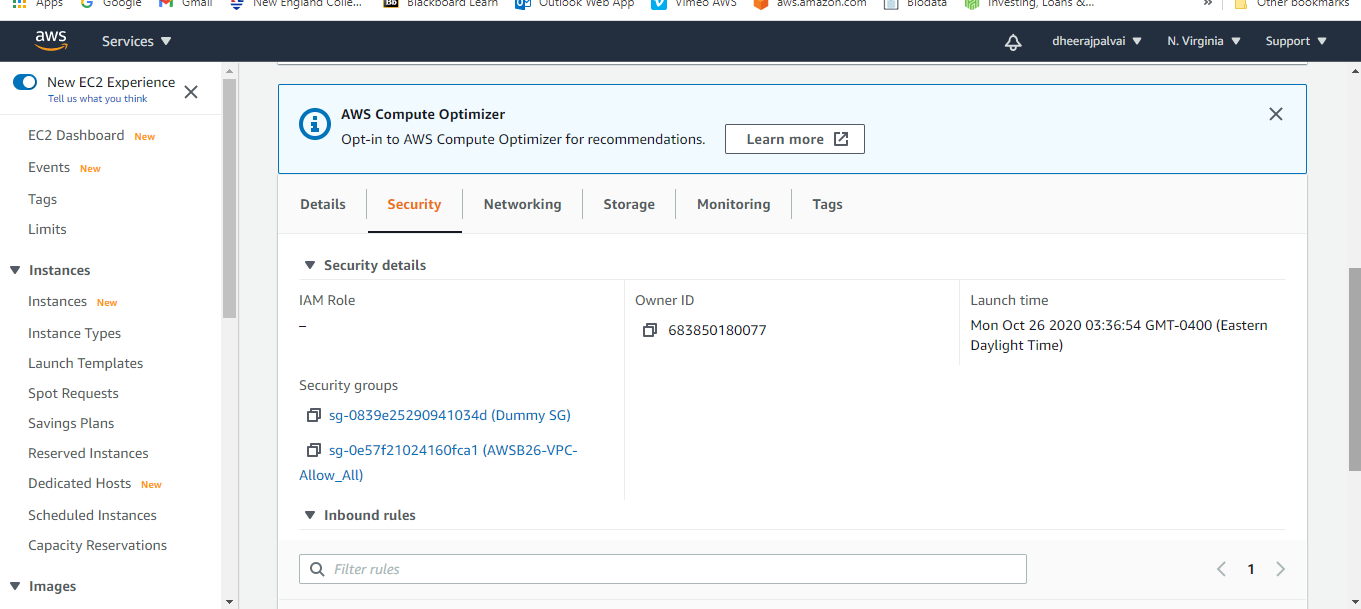
After adding server 2 ip in server 1 security group Inbound

-> telnet server1ip 3306 (now it allows)

\* Here if I want to allow all servers in subnet 3 for server 1 in subnet1. in security group (server1) instead of server2 ip I will give subnet 3 ip range.

\* But if I want to give only few servers, we keep the set of particular ips in Dummy security group and in server1 security group we allow Dummy security group





Q, what is the need to create two security groups?

A: It we want to access one DB server of subnet 1 with multiple App servers of subnet 3, for that we create one more security group and keep required App servers in that security group and assign this to Db server’s security group.

We can assign up to 5 Security group for one server

* We can allow traffic from server ip’s, subnet ip ranges, also from security groups

