**09.AWS-B30-SG-NACL-ADCreationAzure**

**State full and state less firewall**

--- **security group** - state full firewall.

--- **NACL** – State less firewall.

**Security group (State full firewall)**

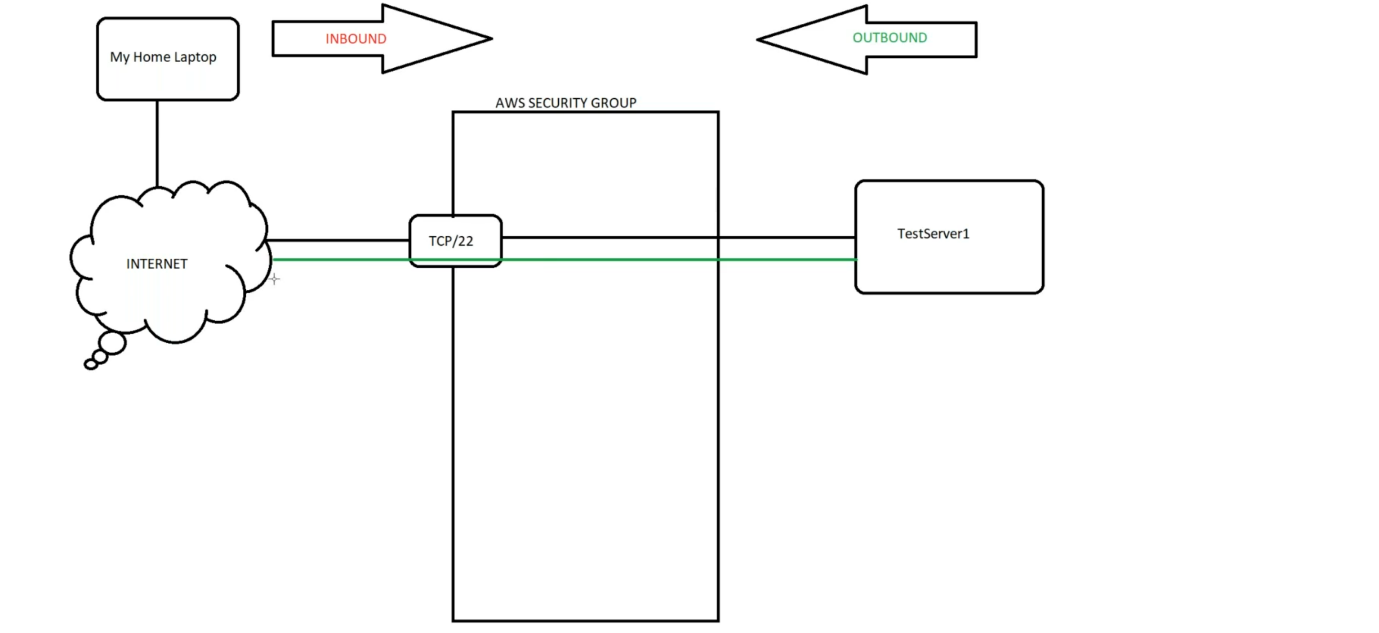
--- security group is state full firewall

--- applicable all services except subnets in aws.

--- default deny and we can allow traffic only

--- restricted to vpc only means, one security group works for single vpc.

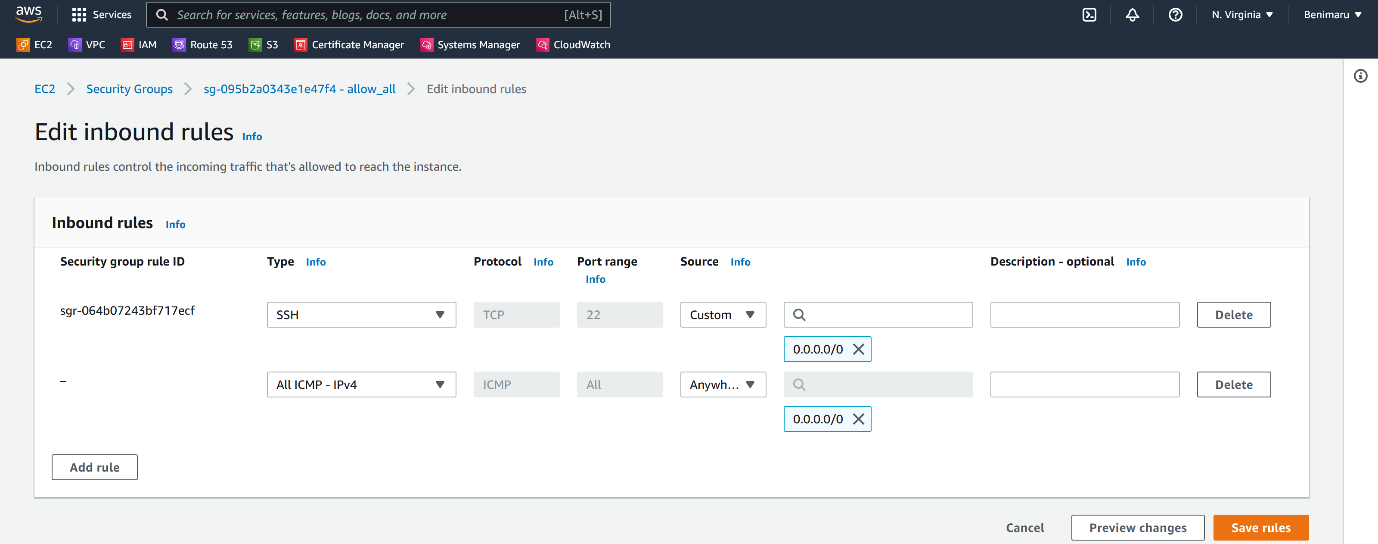
--- can add source form subnets, ip addresses and another security group as well.



--- **note** – if you open port in inbound then you do not need to open the port in outbound.

Eg security group. Applied to EC2, RDS, ELB etc.

**Rule added to Ping server**



--- if you want to ping the server then we need to add icmp rule in security group.

--- **how do you check the server is up…?**

Do not say I will ping the server, because if the ICMP rule not added in the security group then the servers will not be pinged. Due to security reason the ICMP port will be disabled.

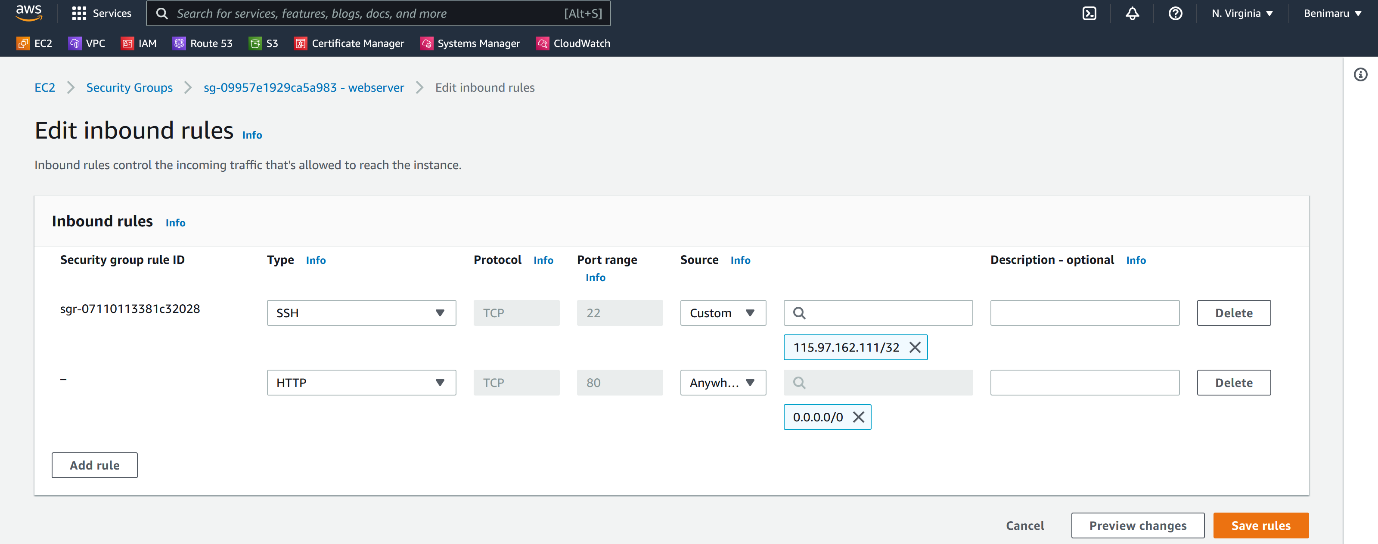
If you really want to see if the server is up then we will use telnet.

--- **telnet <ipaddress of server>:22**

--- **scenario** – we have webservers, app servers and db servers. We have below requirements needs full fill.

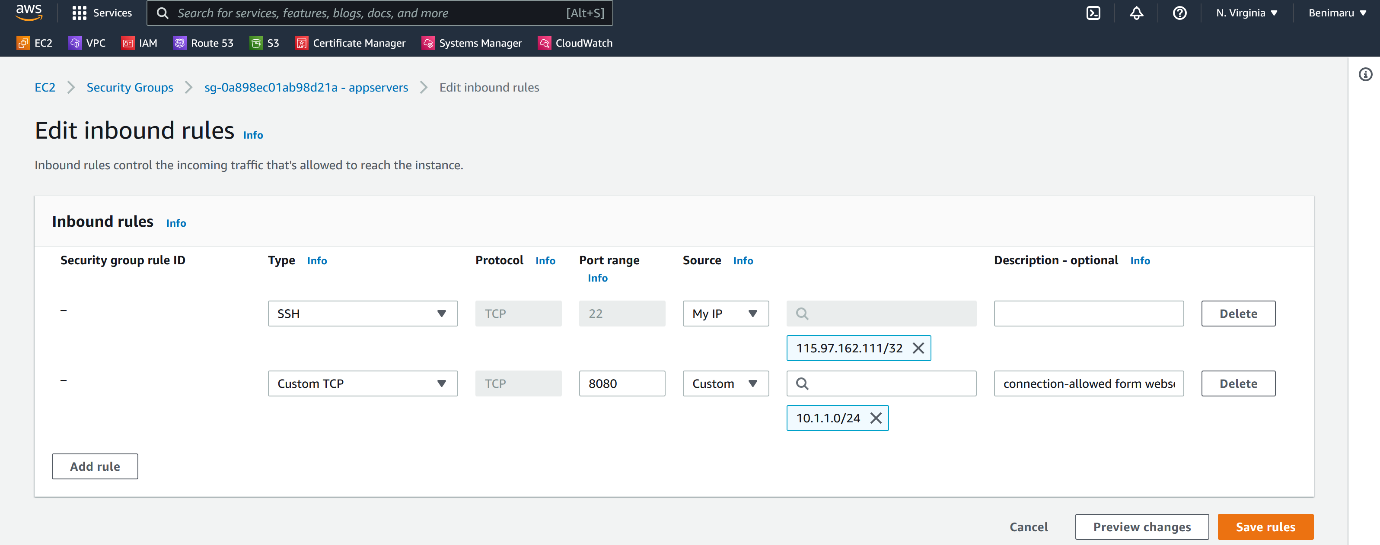
1. Webservers (10.1.1.0/24) - Anyone from internet must connect on port 80.
2. Appservers (10.1.2.0/24) – only webservers must connect to appservers on port 8080.
3. Dbservers (10.1.3.0/24) – only appservers must connect to Dbservers on mysql port 3306.

**Webservers security group**



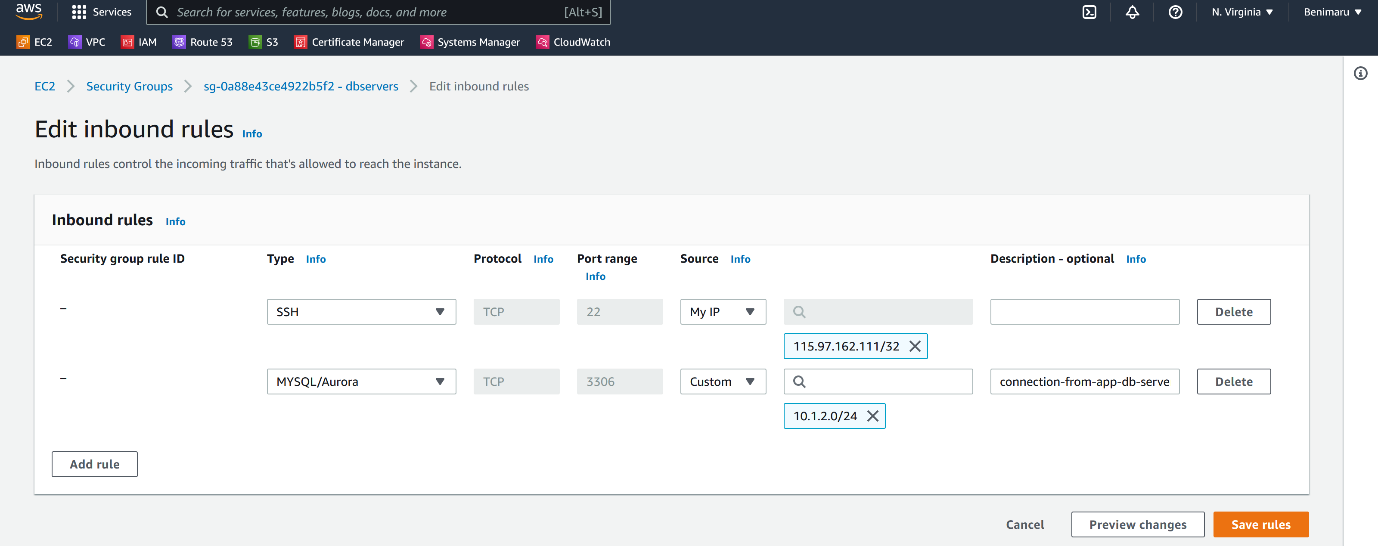
--- **note** - Webservers (10.1.1.0/24) - Anyone from internet must connect on port 80.

**Appservers security group**



--- **note** - Appservers (10.1.2.0/24) – only webservers must connect to appservers on port 8080.

**Dbservers security group**



--- **note** - Dbservers (10.1.3.0/24) – only appservers must connect to Dbservers on mysql port 3306.

**NACL (network access control list) Sate less firewall**

--- **note** – you need to open the port in inbound and outbound as well.

**Eg** NACL – only applied to subnets. We apply outbound to subnets only.

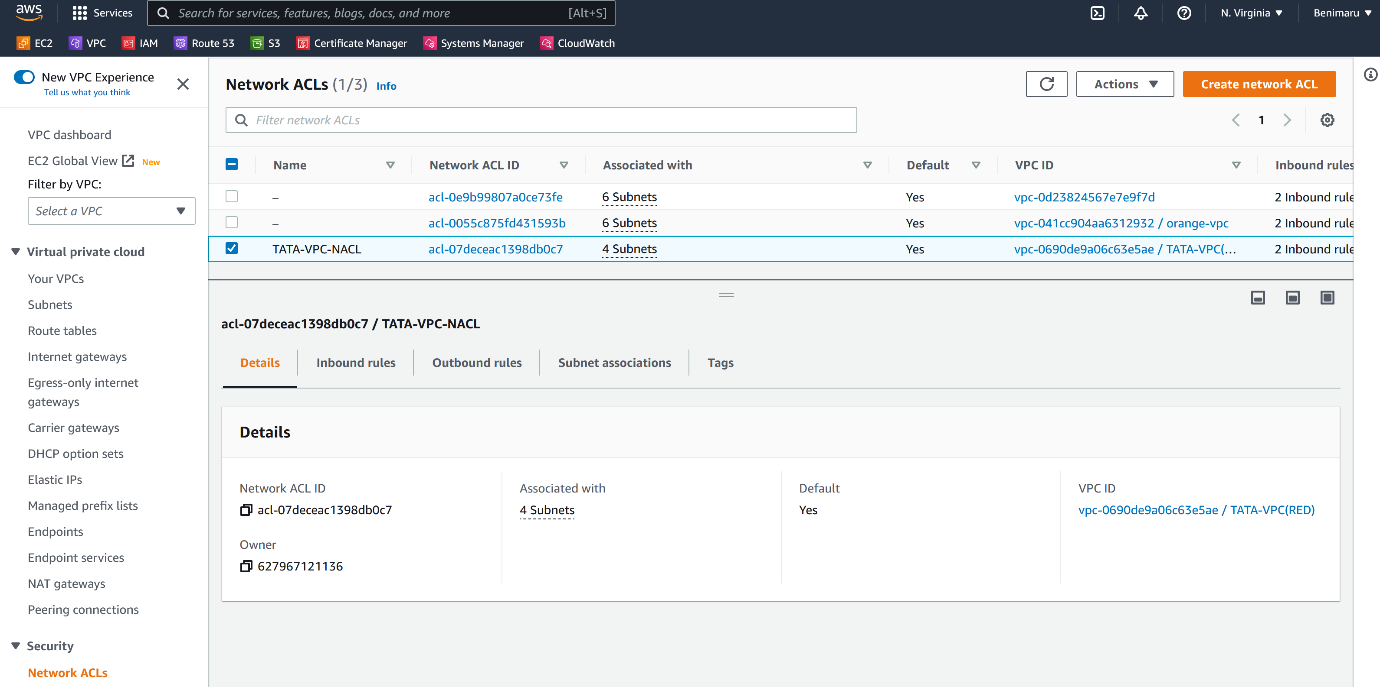
--- only applicable to subnets

--- we can allow and deny traffic

--- restricted to vpc only means, one NACL works for single vpc.

--- the lower the value rule gets higher priority.

**Create NACL**

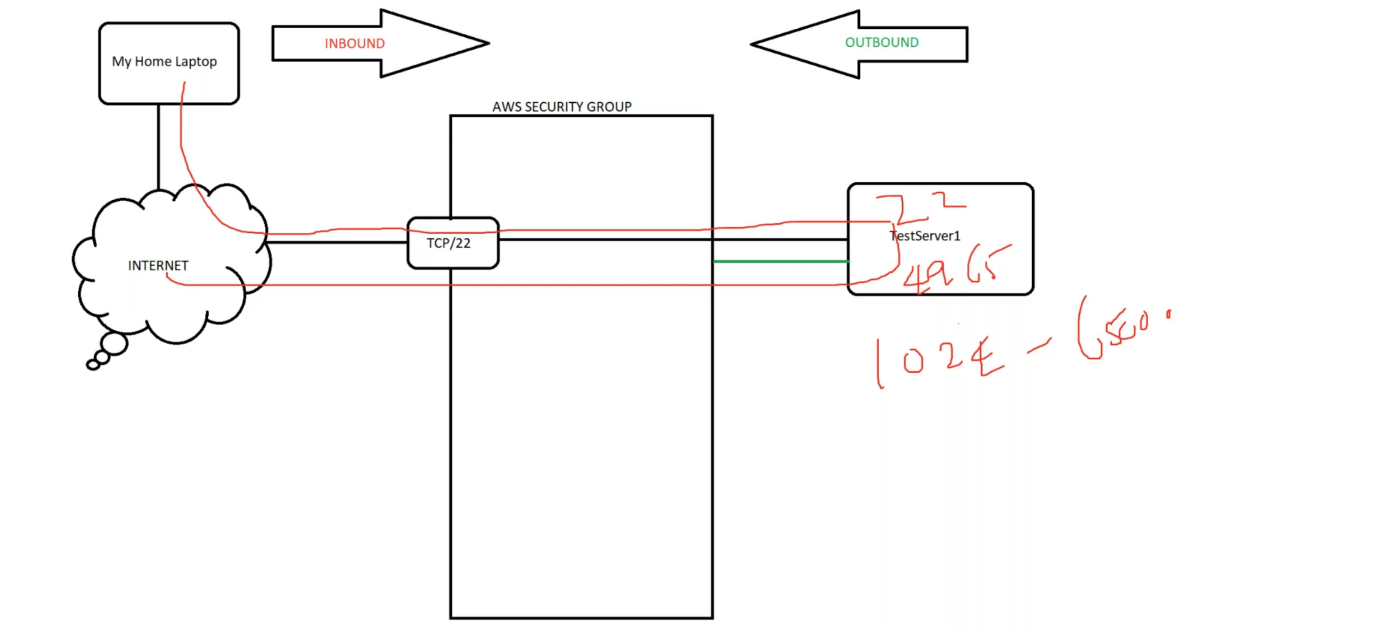


--- I have created NACL.

--- **NOTE** – 4 subnets are associated with this VPC.

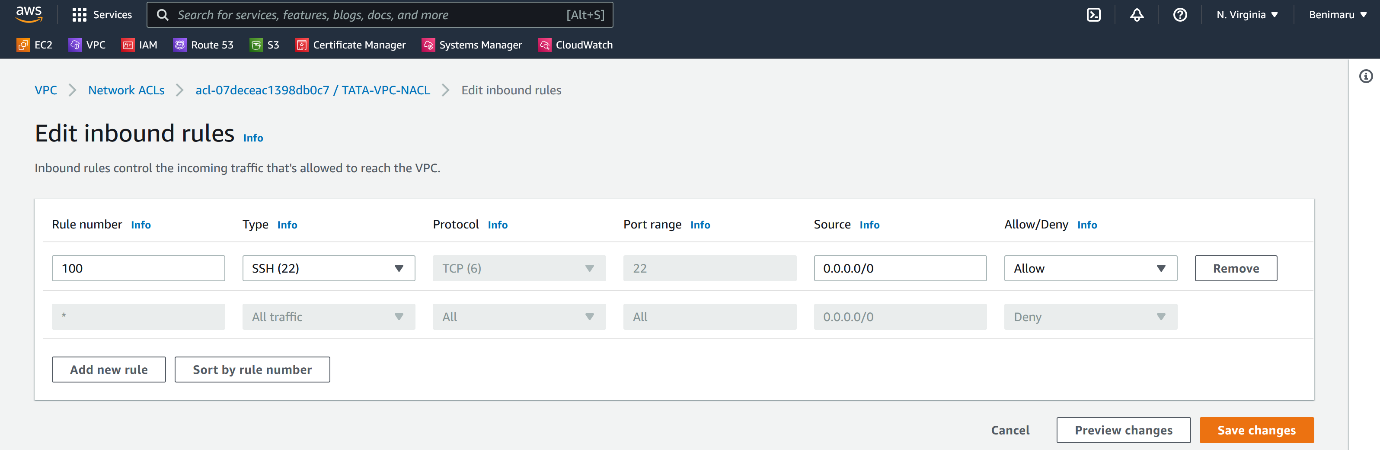
--- **NOTE** – all inbound and outbound traffic.

**Add inbound and outbound rule**



--- **note** – if you open 22 ports in inbound, you also need to specify the port in outbound as well

--- **inbound**



--- **outbound**

