Task 3: SSH & Security Groups

Problem Statement:

Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

Tasks To Be Performed:

1. Create 2 EC2 instances in any public subnet of any VPC and name them

   Master and Client.

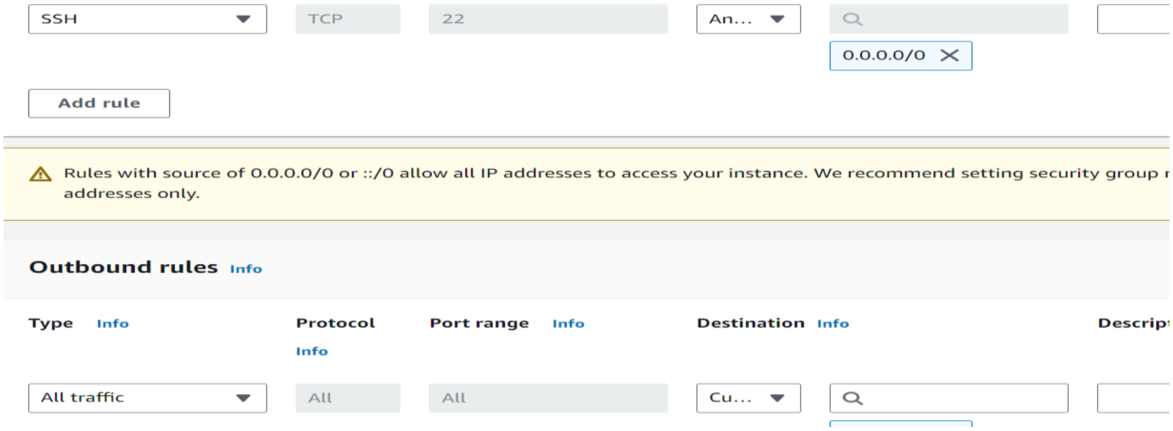
2. Using security groups, make sure that the Client instance can only be

   accessed (SSH) through the Master instance.

For this setup, you'll need to follow these below steps:

a. Create two security groups, with default VPC
   - A. One for the Master instance
   - B. One for the Client instance.

Name them Master_SG and Client_SG and add inbond rule type-ssh and source-anywhere.



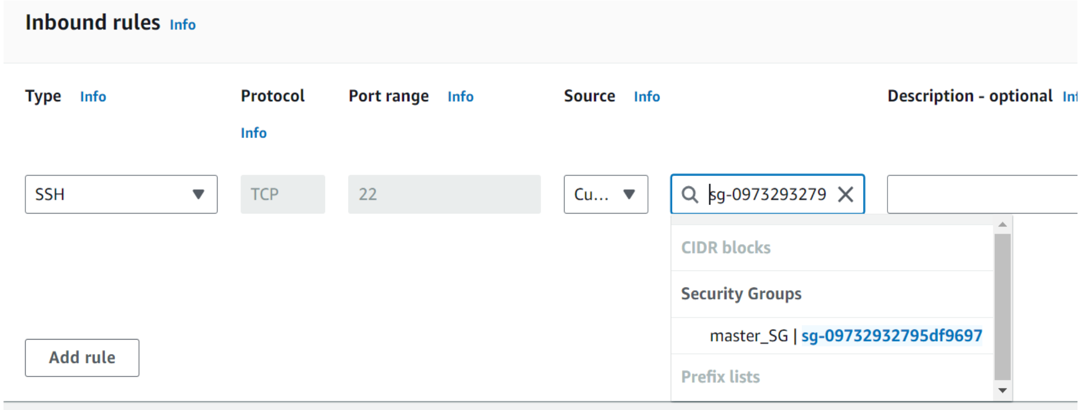
SSH | TCP | 22 | An... | 0.0.0.0/0

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group r
addresses only.

Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info	Descrip
All traffic	All	All	Cu...	

b. Same above process do for client security, ensuring that you configure the inbound rules as follows Choose the Type-SSH for the inbound rule and set the source _Master_SG.

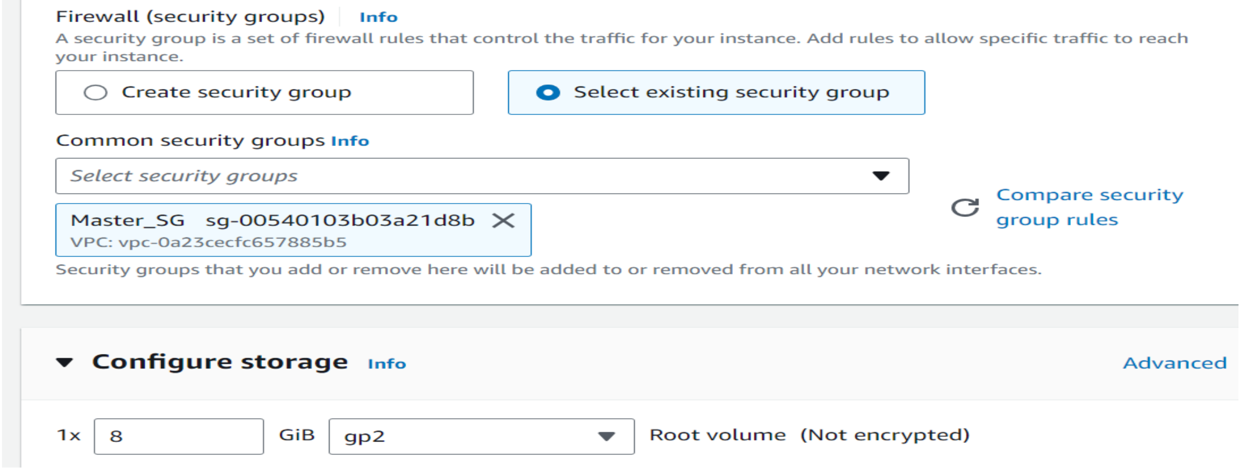


Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Inf
SSH ▼	TCP	22	Cu… ▼	sg-0973293279 ✕	

CIDR blocks
Security Groups
master_SG | sg-09732932795df9697
Prefix lists

c. Create Master EC2 Instance And Associate to Master_SG Group.



Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group   ● Select existing security group

Common security groups Info
Select security groups ▼

Master_SG sg-00540103b03a21d8b ✕
VPC: vpc-0a23cecfc657885b5

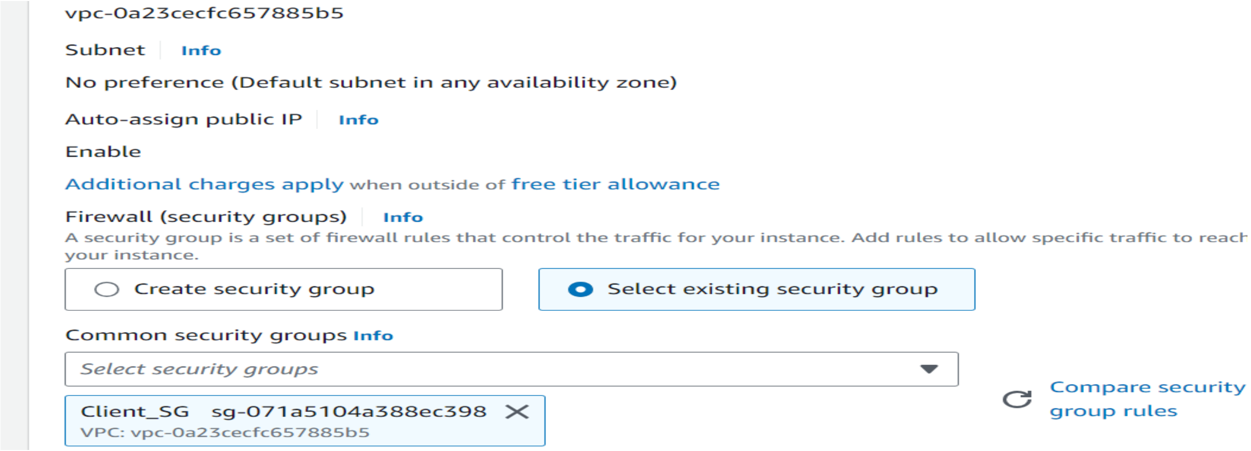
Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▼ Configure storage Info   Advanced

1x 8 GiB gp2 ▼ Root volume (Not encrypted)

d. Create Client EC2 Instance And Associate to Client_SG Group.



vpc-0a23cecfc657885b5

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

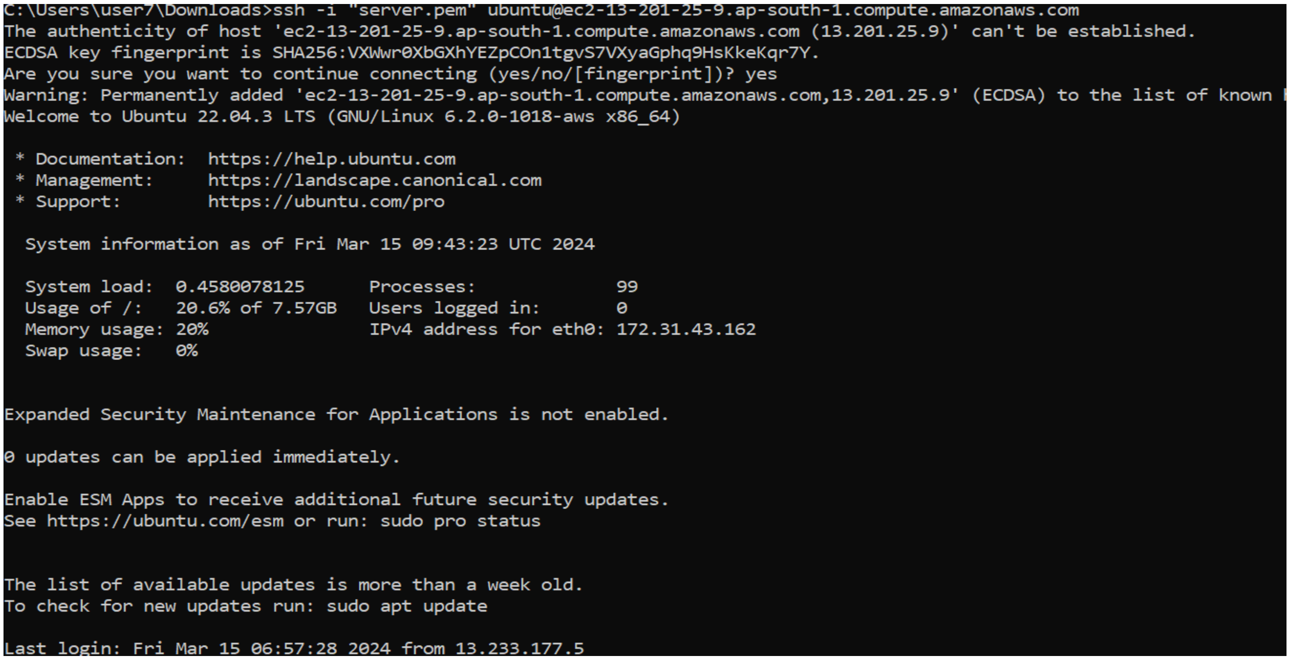
○ Create security group   ● Select existing security group

Common security groups Info
Select security groups ▼

Client_SG sg-071a5104a388ec398 ✕
VPC: vpc-0a23cecfc657885b5

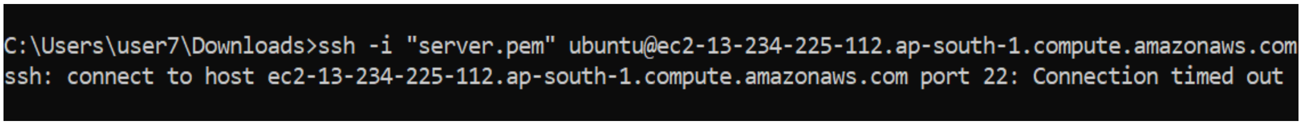
Compare security group rules

e. Login to the Master instance using SSH.



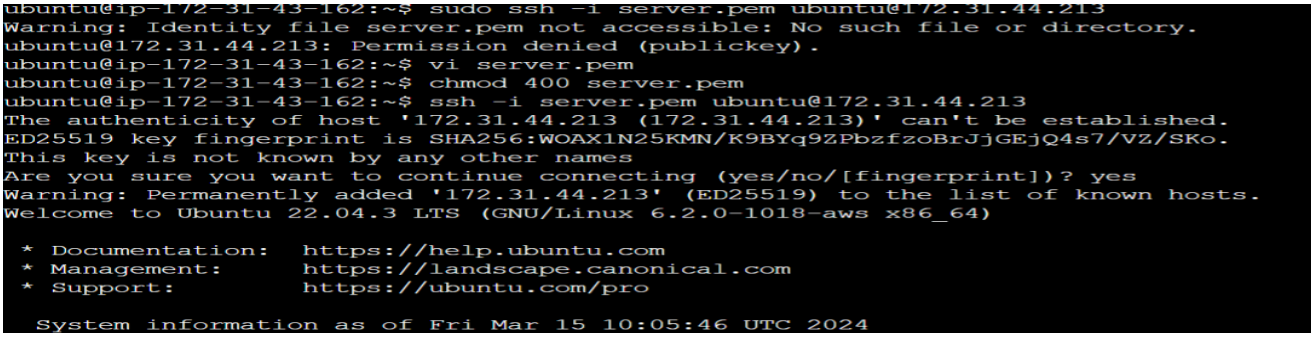
```
C:\Users\user7\Downloads>ssh -i "server.pem" ubuntu@ec2-13-201-25-9.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-201-25-9.ap-south-1.compute.amazonaws.com (13.201.25.9)' can't be established.
ECDSA key fingerprint is SHA256:VXWwr0XbGXhYEZpCOn1tgvS7VXyaGphq9HsKkeKqr7Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-201-25-9.ap-south-1.compute.amazonaws.com,13.201.25.9' (ECDSA) to the list of known
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Fri Mar 15 09:43:23 UTC 2024

  System load:  0.4580078125      Processes:             99
  Usage of /:   20.6% of 7.57GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 172.31.43.162
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Mar 15 06:57:28 2024 from 13.233.177.5
```

f. To Client instance from Local Machine using SSH not connectiong.

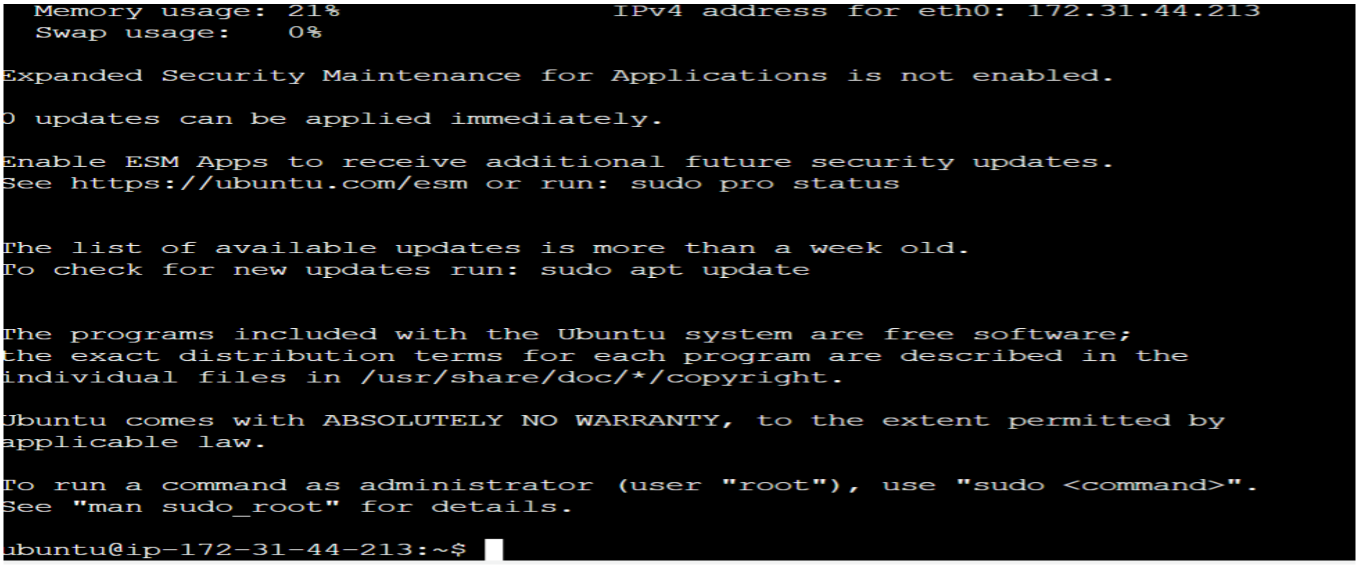


```
C:\Users\user7\Downloads>ssh -i "server.pem" ubuntu@ec2-13-234-225-112.ap-south-1.compute.amazonaws.com
ssh: connect to host ec2-13-234-225-112.ap-south-1.compute.amazonaws.com port 22: Connection timed out
```

g. Here connection is not working since the security group Client-SG associated with Client instance does not allow inbound SSH traffic from Internet.. Try to login to Client instance from Master Instance using SSH [Use private IP address of Client instance]



```
ubuntu@ip-172-31-43-162:~$ sudo ssh -i server.pem ubuntu@172.31.44.213
Warning: Identity file server.pem not accessible: No such file or directory.
ubuntu@172.31.44.213: Permission denied (publickey).
ubuntu@ip-172-31-43-162:~$ vi server.pem
ubuntu@ip-172-31-43-162:~$ chmod 400 server.pem
ubuntu@ip-172-31-43-162:~$ ssh -i server.pem ubuntu@172.31.44.213
The authenticity of host '172.31.44.213 (172.31.44.213)' can't be established.
ED25519 key fingerprint is SHA256:WOAX1N25KMN/K9BYq9ZPbzfzoBrJjGEjQ4s7/VZ/SKo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.31.44.213' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Fri Mar 15 10:05:46 UTC 2024
```



```
  Memory usage: 21%                IPv4 address for eth0: 172.31.44.213
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-44-213:~$ 
```