AWS Documentation

No:-	Documentation of performed task
1.	**Security Groups**

Security Groups:

Cybersecurity has grown to be a crucial component of any business in the modern digital age. Access management is a fundamental element of cybersecurity. Controlling access includes deciding who has access to what resources and for what goals. The management of resource access in the cloud is done using security groups. We shall define security groups in this article and explain how they operate and may be created in Amazon Web Services (AWS). We'll also define a few crucial terms related to security groups, offer pertinent examples, and give step-by-step directions with screenshots.

An example of one of these features is the security group, which functions as a virtual firewall to regulate the inbound and outgoing traffic for Amazon EC2 instances or other AWS resources in a VPC. We shall go over a security group's definition and formation in this article.

1. **Security Group**: It performs the function of a virtual firewall, managing the inbound and outbound traffic for one or more Amazon EC2 instances or other AWS services within a VPC.

2. **Inbound Rules:** These outline the types of traffic that are permitted to use the resources. It serves as a virtual firewall, controlling the traffic going in and coming out of a VPC for one or more Amazon EC2 instances or other AWS services.

3. **Outbound Rules:** These regulate the traffic that is permitted to depart from the resources. The destination for incoming traffic is dealt with by outbound rules. They may be forwarded to an alternative Security Group, a CIDR block, a single IPv4 or IPv6 address, or all three.

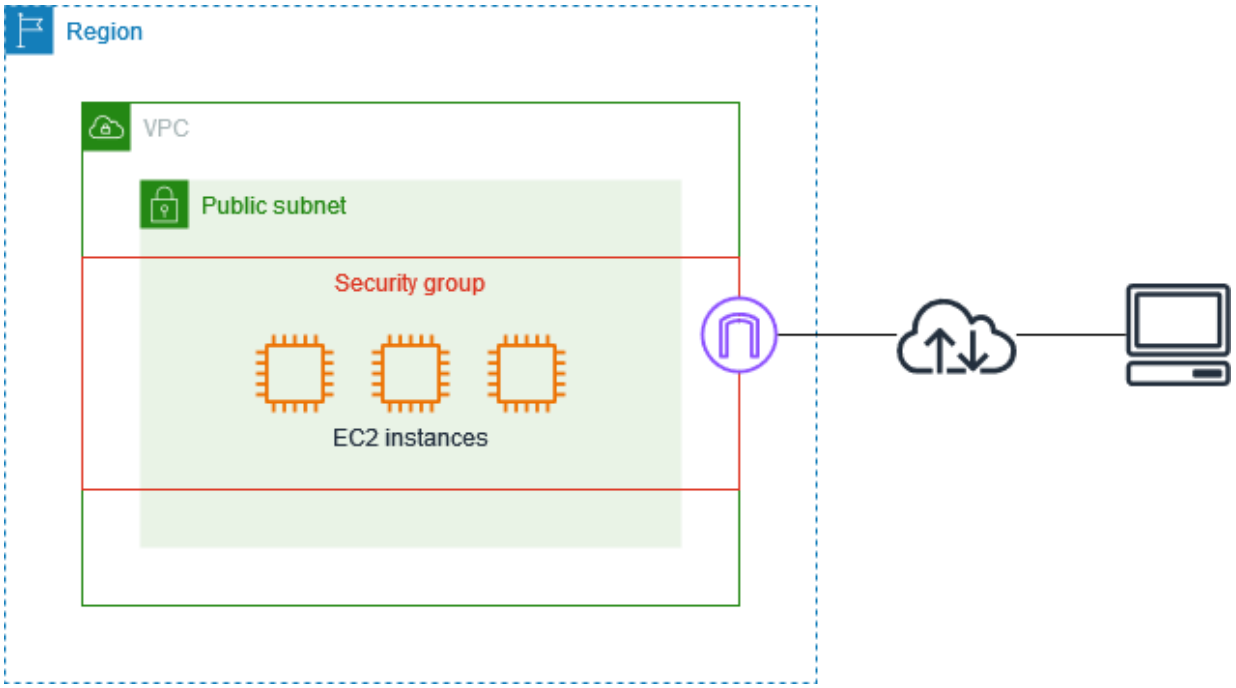
4. **Amazon EC2:** A web service called Amazon Elastic Compute Cloud offers scalable computation capability in the cloud. For developers, it is intended to make web-scale cloud computing simpler.

5. **VPC:** A virtual network called a virtual private cloud enables you to launch Amazon resources into a defined virtual network.

6. **CIDR:** A technique for allocating IP addresses and rerouting Internet Protocol packets is called classless inter-domain routing (CIDR).

7. **Protocol:** A protocol is a collection of guidelines that controls how two devices communicate with one another.

8. **Port:** A port on a computer serves as the communication endpoint for a particular process or service.



HTTP: Allows web traffic on port 80 for serving web pages.

HTTPS: Allows secure web traffic on port 443 for encrypted communication.

ICMP: Used for diagnostic tools like ping to check connectivity.

SSH: Enables secure shell access on port 22 for remote management.

RDP: Allows Remote Desktop Protocol traffic on port 3389 for accessing Windows instances remotely.

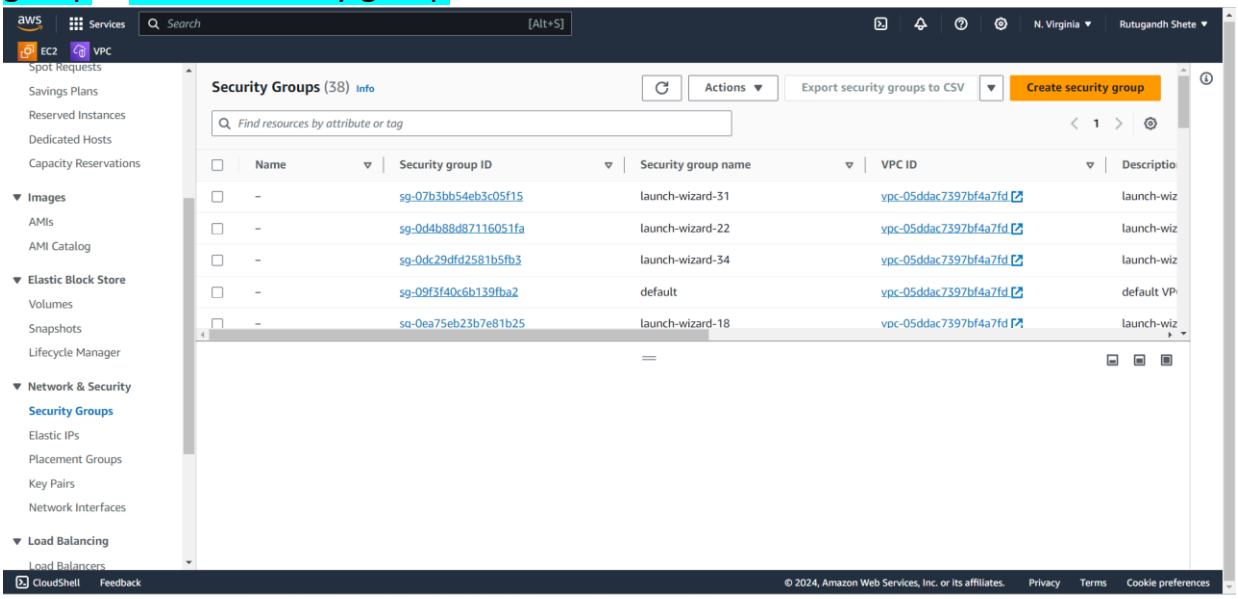
All Traffic: Allows any type of network traffic, regardless of protocol, to pass through.

UDP (User Datagram Protocol): Allows connectionless, fast, but less reliable data transmission, often used for streaming and gaming.

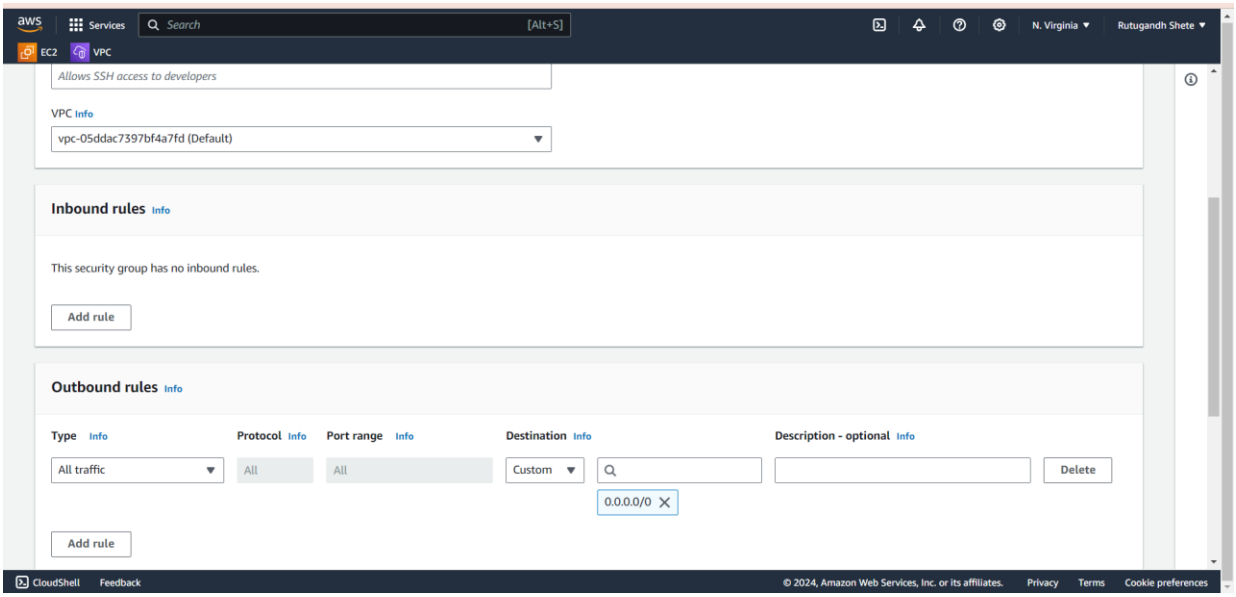
TCP (Transmission Control Protocol): Enables reliable, connection-based data transmission, commonly used for most internet traffic like web browsing and emails.

Steps:

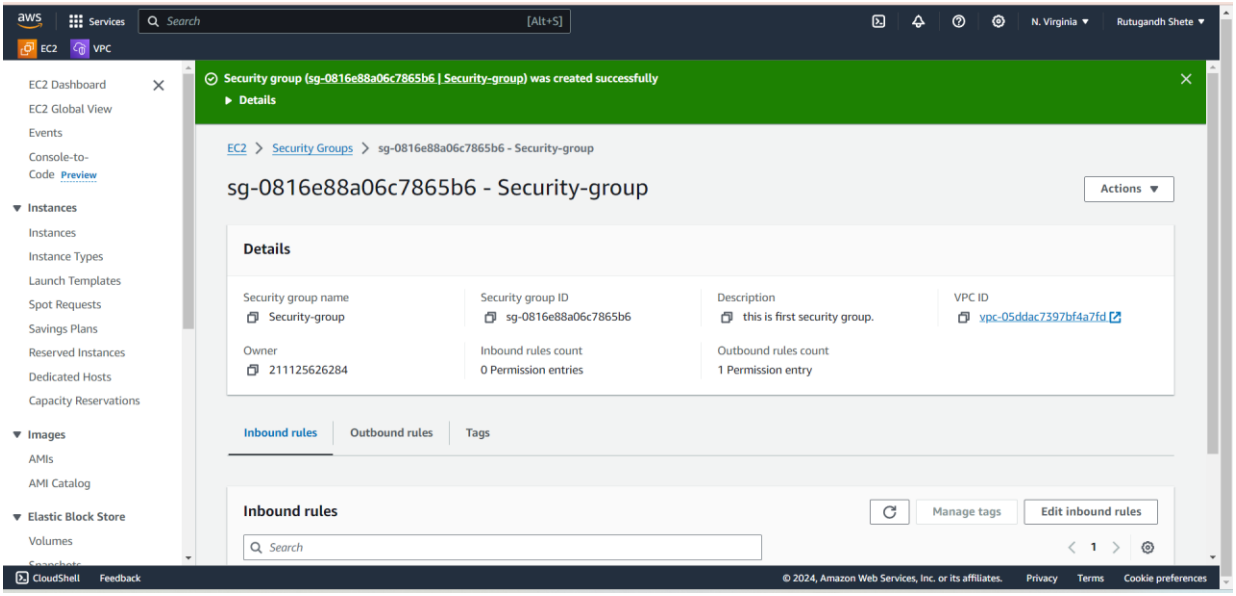
- To enable this service click on to Network & Security→ security group→create security group



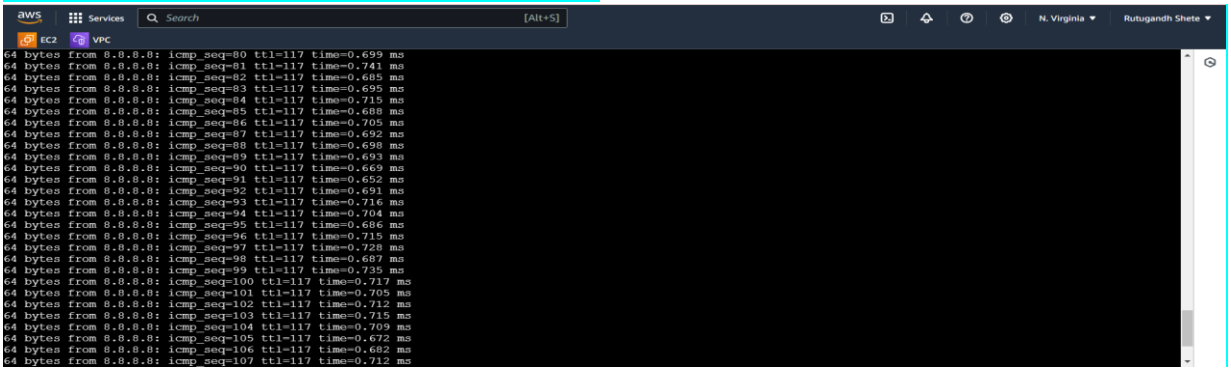
- Create security group→add name →description→inbound is specified→outbound is specified to all traffic→create.



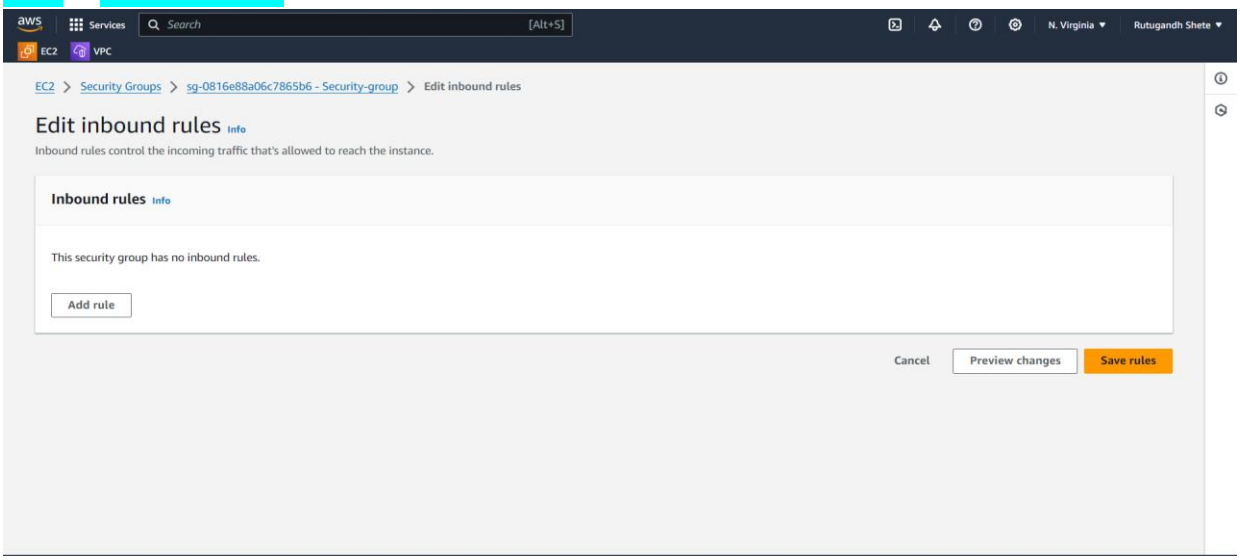
- After creation.



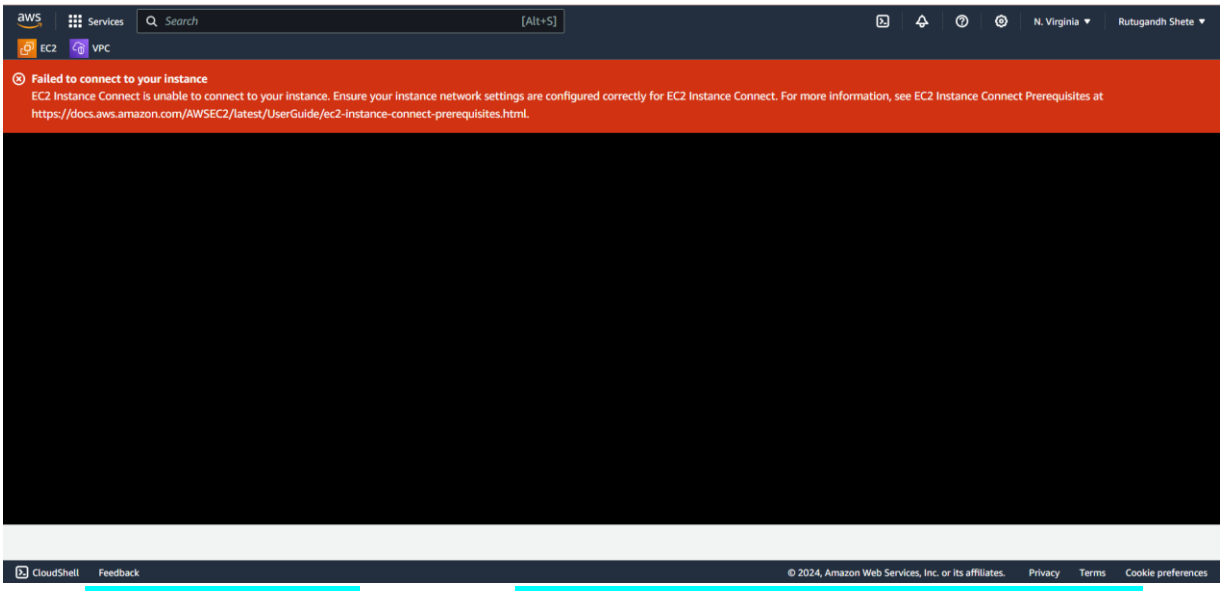
- Launch EC2 insatance →connect to it terminal→check using ping command. We are able to connect to instance and we can access internet because of the both rules are specified.



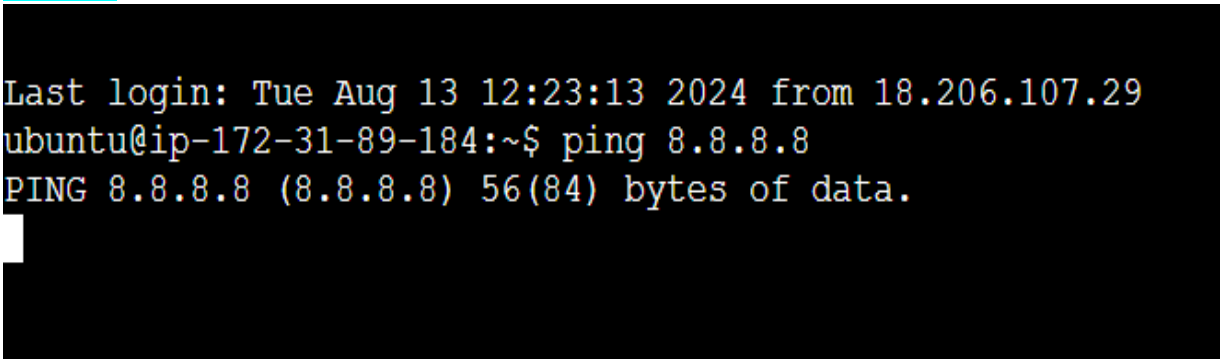
- If inbound rule is removed from security then instance terminal will not be able to connect . Security group→Name→Actions→edit inbound rule→remove rule.



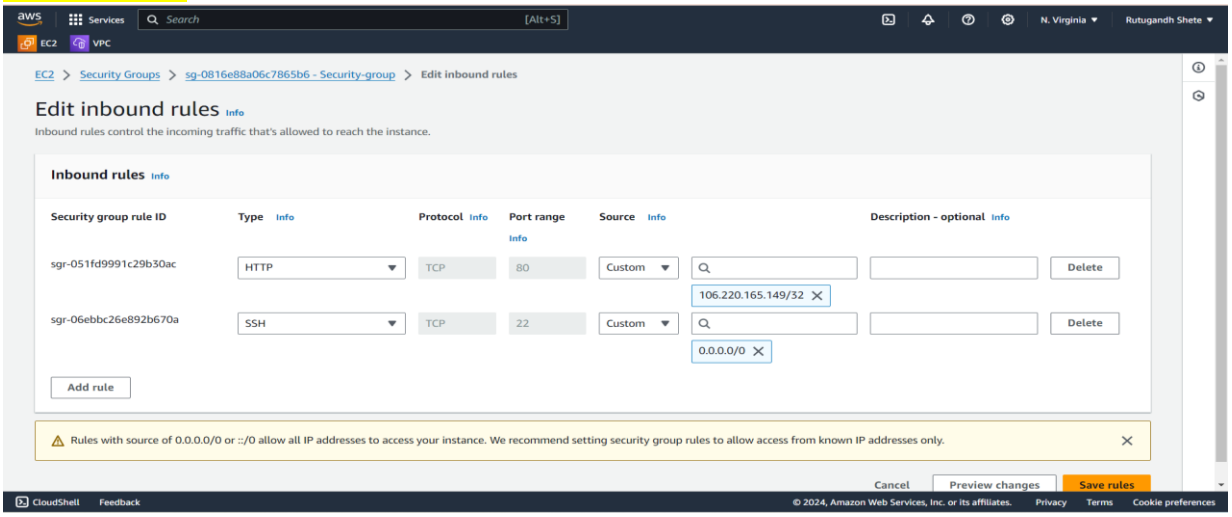
- We are not able to connect terminal to internet.



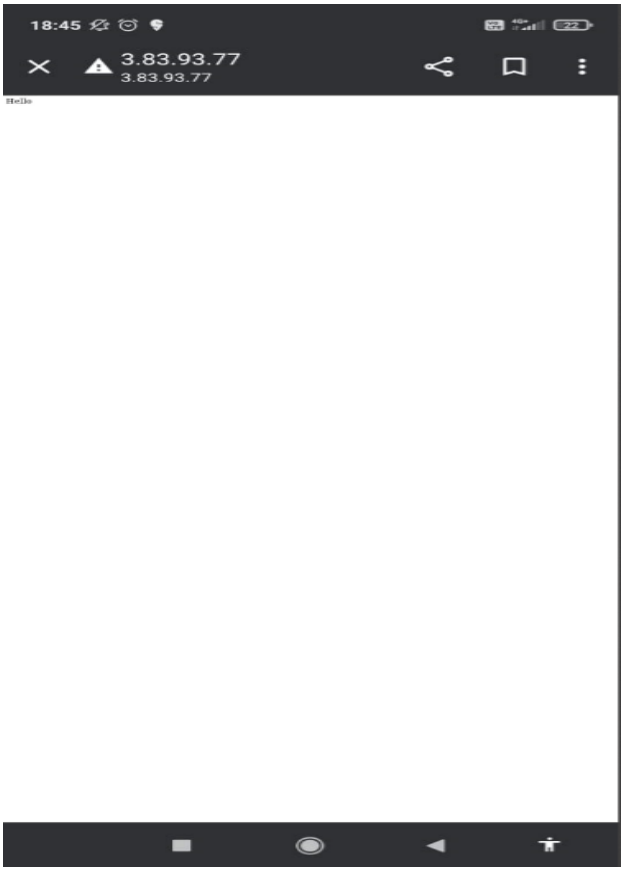
- If we remove outbound rule then we will be not able to connect to internet. Security group name→actions→edit outbound rule→remove rule→ping 8.8.8.8.



- If we want to show content of web browser to only specific user then edit inbound and add user IP. Give ssh connection and CIDR 0.0.0.0 which will connect instance and by adding another rule it will help to show content to specific user.



- User IP is “106.220.165.149” so this user is able to see the content.



- Others are not able to see.