**AWS EXPERIMENT NO:-5**

**Aim:** To Create and modify the firewall rules of Virtual Private Cloud.

**Learning Objectives:**

* Learn fundamentals of firewalls
* Create and modify the rules of firewall

**Software/Tools Used:** Amazon Web Services (AWS)

**Theory:** Within AWS, you may build and manage your own network configurations thanks to the Virtual Private Cloud (VPC), a network environment that is highly configurable. Managing firewall rules, which are governed by security groups and network access control lists (NACLs), is a crucial part of maintaining a VPC's security. For individual instances (EC2, for example), security groups function as virtual firewalls, and NACLs manage traffic at the subnet level. The inbound and outgoing traffic flow is governed by firewall rules, which specify the traffic that can reach and leave your resources.

Setting parameters like IP ranges, protocols (including TCP, UDP, and ICMP), and port numbers to allow or deny traffic is part of creating firewall rules in AWS. For example, when you build a security group, you may configure outgoing rules to regulate traffic leaving your instances and provide rules to enable inbound traffic from specific IP addresses (like SSH on port 22). However, NACLs offer an additional degree of protection by letting you create stateless rules that are applicable at the subnet level. NACLs, in contrast to security groups, demand specific allow and deny rules for both incoming and outgoing traffic.

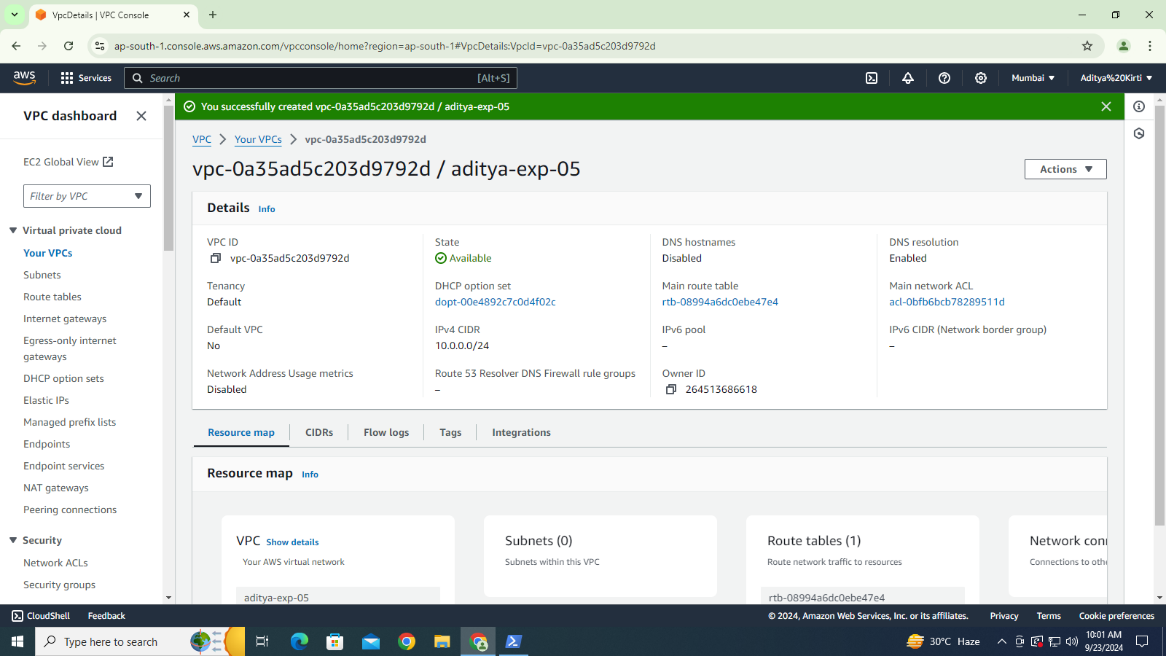
Firewall rules must be modified as your VPC develops and your security needs shift. To permit access from various IP addresses or protocols, you might need to add new rules, delete unnecessary ones from your existing rules, or both. It is simpler to adjust to shifting security requirements when you can alter firewall rules dynamically with AWS since it doesn't need restarting or disturbing the related resources. While updates to NACLs impact all resources inside the designated subnet, changes to security groups immediately impact all instances associated with that group.

To keep a cloud environment safe, firewall rules in a VPC must be managed correctly. It's crucial to adhere to best practices, such as the concept of least privilege, which states that you should only grant access to the bare minimum and that you should routinely check and audit your policies to make sure they meet security requirements. For successful security management in AWS VPCs, continuous testing and monitoring are essential.

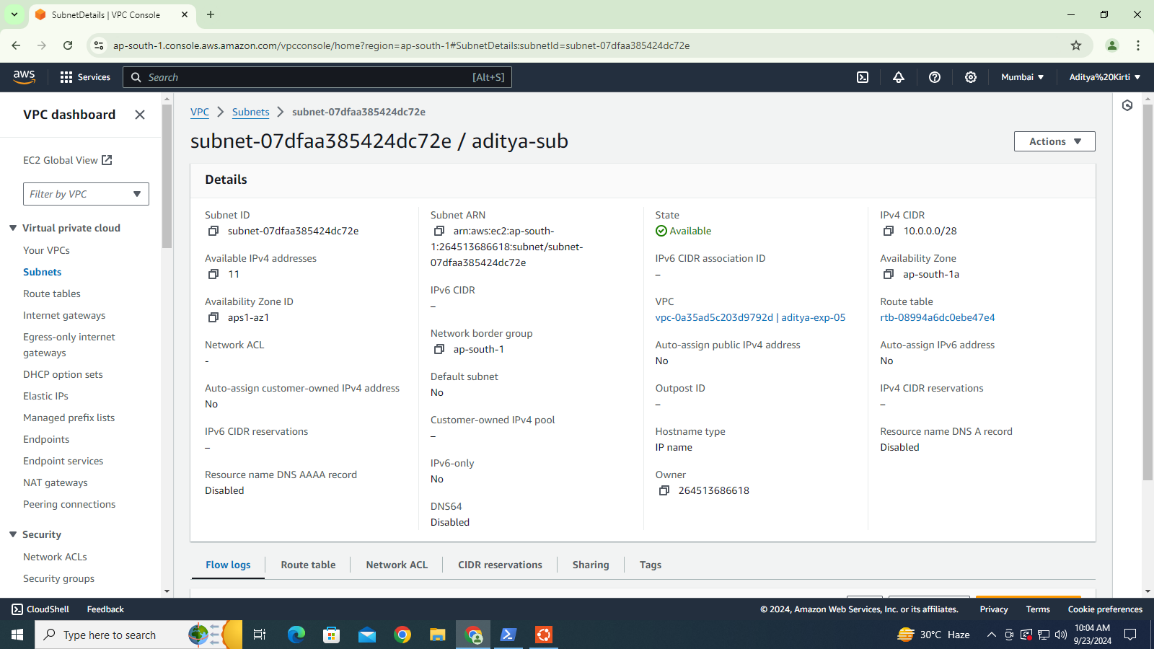
Misconfigurations in firewall rules can result in vulnerabilities like unauthorized access or data breaches.

**Implementation/Output:**

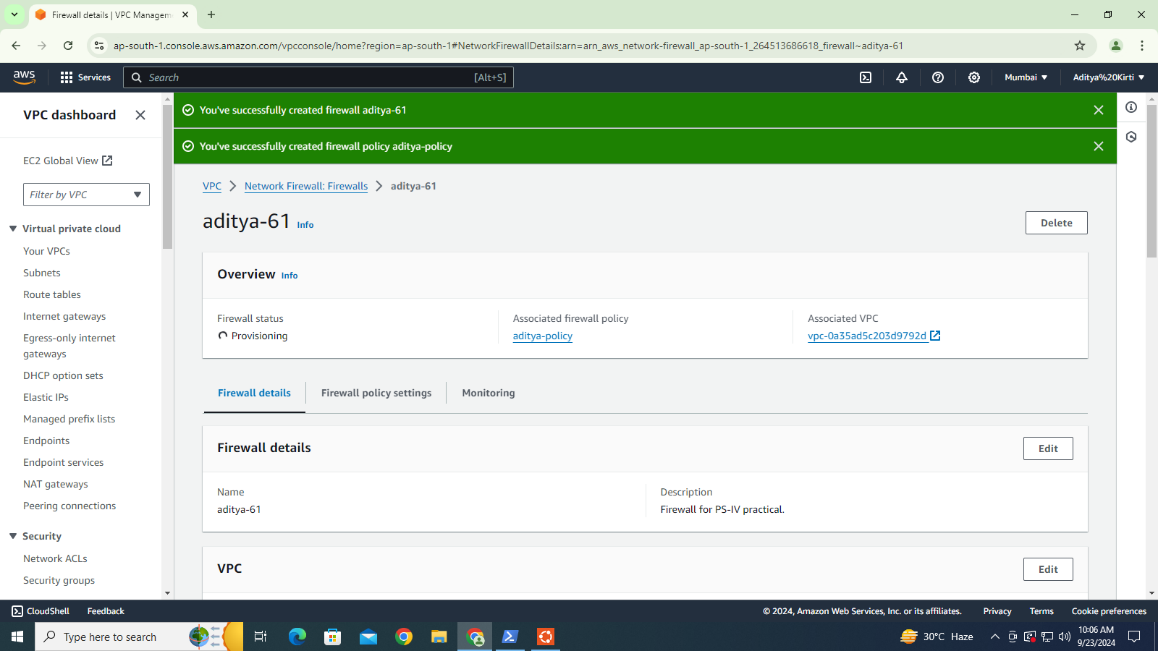
Step 1: Create VPC



Step 2: Create a Subnet



Step 3: Create Firewall



**Conclusion:** To sum up, the security of cloud infrastructure depends on the creation and modification of firewall rules within an AWS Virtual Private Cloud (VPC). Only authorized access to your resources can be ensured by efficiently administering security groups and network access control lists (NACLs) to regulate the flow of inbound and outbound traffic. Maintaining a safe, legal, and adaptable cloud environment that changes to meet changing security requirements requires frequent firewall rule updates, adherence to best practices like the principle of least privilege, and continuous monitoring.