😊 Network Access Control List

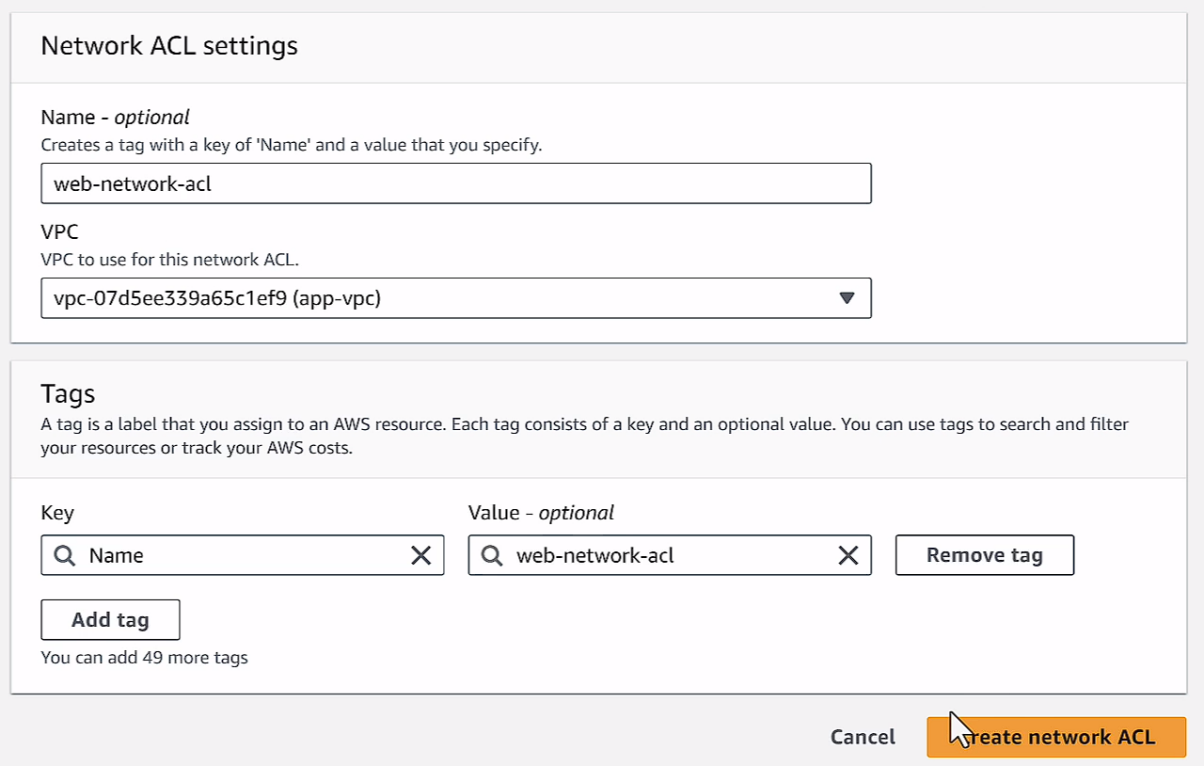
A Network Access Control List (ACL) is a set of rules or filters that control the traffic entering or leaving a network. ACLs are commonly used in networking devices such as routers, switches, and firewalls to manage and secure network traffic. These lists define what type of traffic is allowed or denied based on various criteria, such as source and destination IP addresses, ports, and protocols.

Here are some key points about Network Access Control Lists:

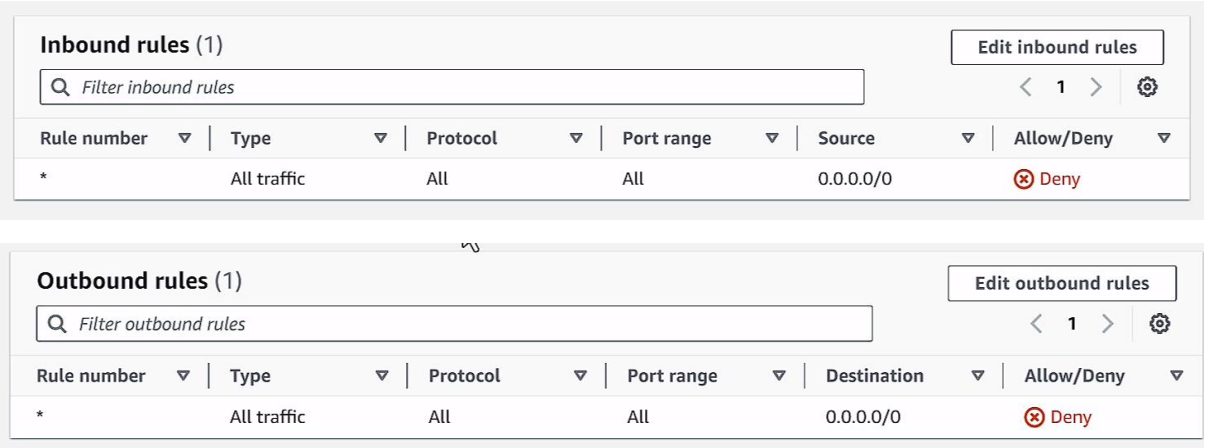
- **Filtering Criteria:** ACLs use filtering criteria to make decisions about network traffic. These criteria can include source and destination IP addresses, port numbers, and protocols.
- Types of ACLs:
- **Standard ACL:** These ACLs only consider the source IP address for making filtering decisions. They are simpler but less flexible compared to extended ACLs.
- **Extended ACL:** These ACLs can consider both source and destination IP addresses, as well as port numbers and protocols. They provide more granular control over network traffic.
- **Inbound and Outbound ACLs:** ACLs can be applied to inbound or outbound traffic on a network interface. Inbound ACLs control traffic coming into a network, while outbound ACLs control traffic leaving a network.
- **Implicit Deny:** If a packet does not match any of the criteria specified in the ACL, it is typically implicitly denied. This means that, by default, traffic is blocked unless explicitly allowed.
- **Sequential Processing:** ACLs are typically processed sequentially, and the first matching rule is applied. Once a match is found, further processing stops, so the order of rules in the ACL is important.
- **Logging:** Some ACLs allow logging of denied traffic, providing a record of attempts to access or communicate with restricted resources.
- **Security and Access Control:** ACLs are a crucial component of network security. They help in implementing access control policies, preventing unauthorized access, and protecting against various types of network attacks.

😁 To begin with the Lab

1. On the VPC dashboard navigate to **Network ACLs**.
2. Here you need to click on create network ACL and attach it to the web subnet.
3. Now give it a name and then select your VPC.
4. Then just click on create Network ACL.

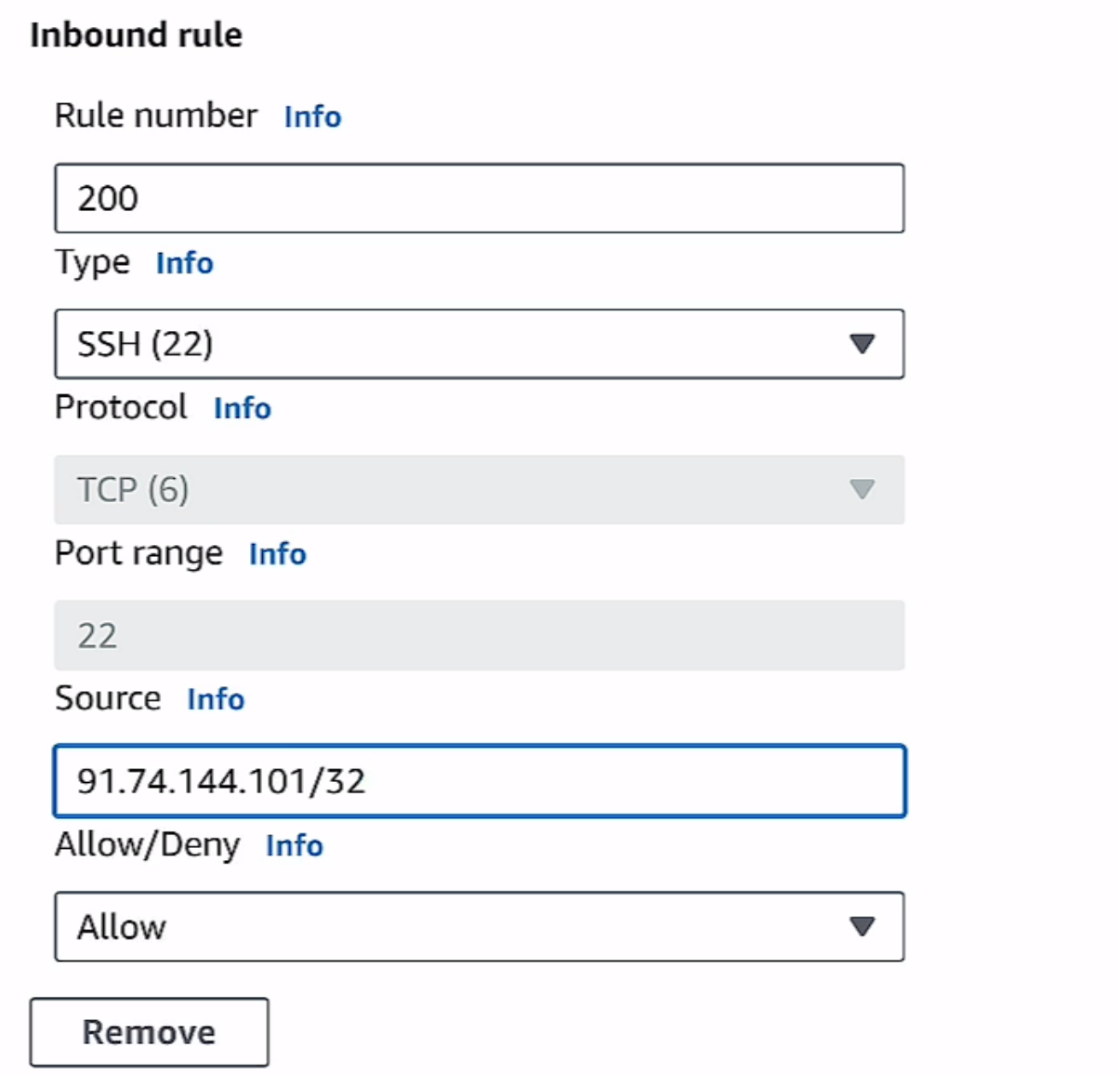


5. So, once it is created, select it and you will see that by default on a new Network ACL there is a rule to deny all traffic.
6. And this deny rule applies on both inbound and outbound rules.

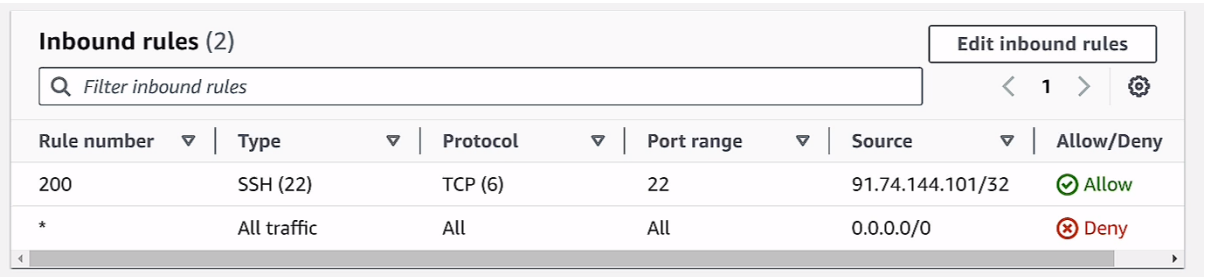


7. Now you are going to attach this Network ACL to your web instance machine.
8. For that go to inbound rules then to edit inbound rules. There you need to click on add new rule.

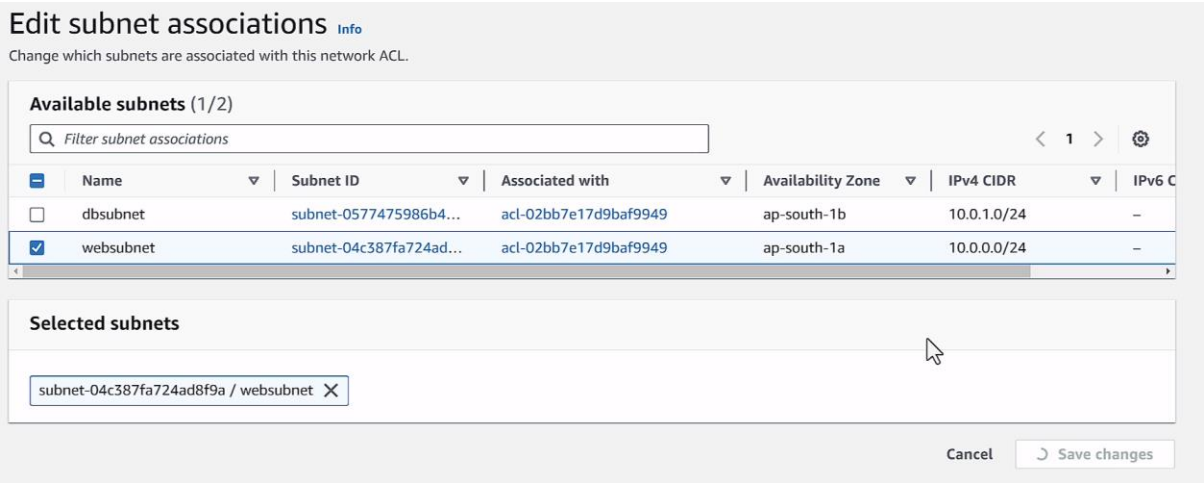
9. Now you need to give a rule number, then select your port and in the source put your local machine Public IP address.
10. After click on save changes.



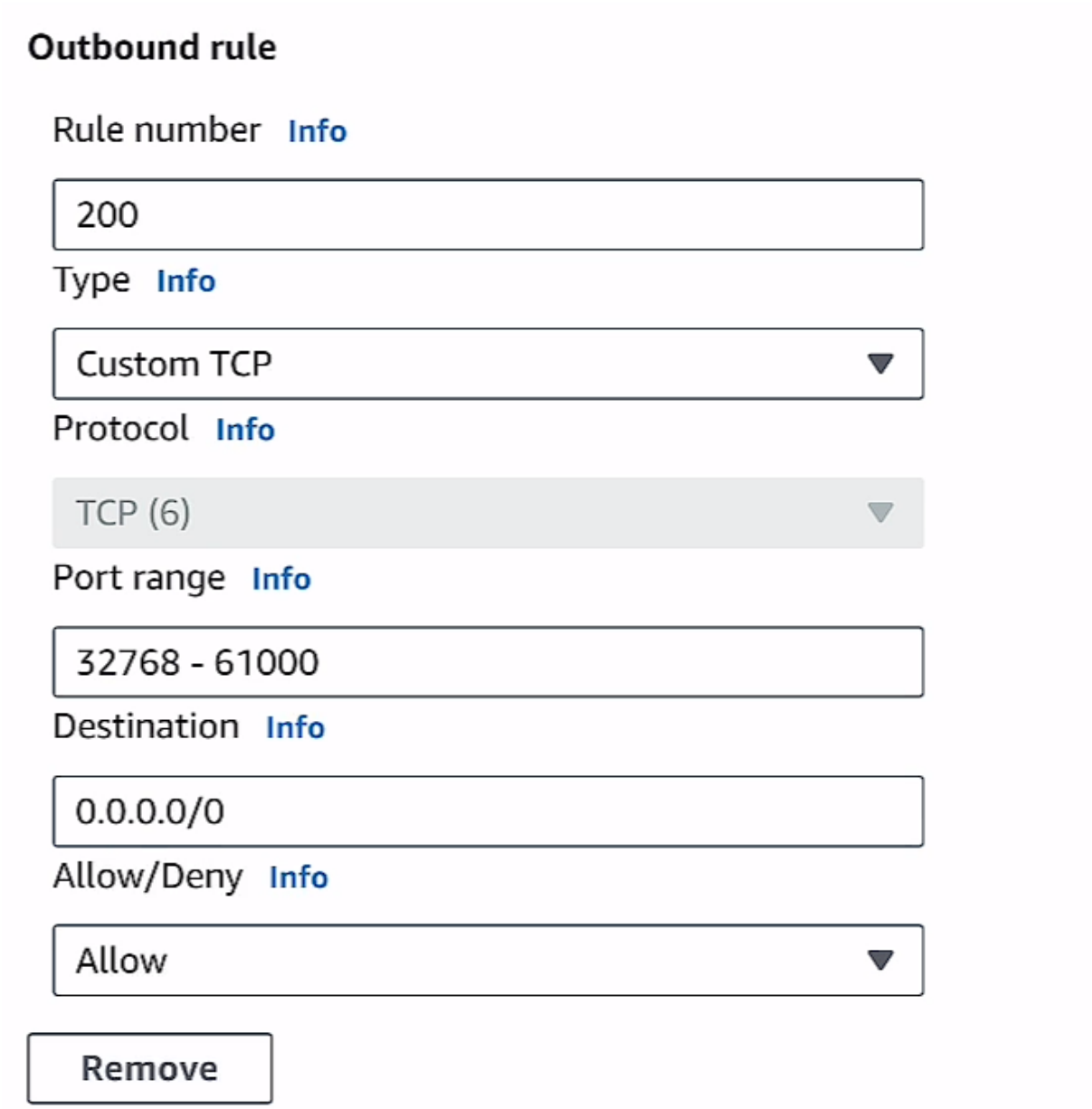
11. Now you have an inbound rule to connect your session via SSH.



12. Now go to subnet association in Network ACL, and click on edit subnet association. Then you need associate it with your websubnet. Click on save changes.



13. Now if you will go to Putty tool and try to connect with your web instance, it will try to connect but it will fail to do that.
14. See, with network Access control list. This is stateless in nature. You have added a rule to allow traffic on Port 22 on the machine. But you also need to add a rule that will allow outbound traffic from web instance on to your laptop.
15. Now you need to go back to Network ACL and navigate to outbound rules. Then click on outbound rules.
16. Again, you need to give rule number but this time it is for outbound rule. Choose custom TCP in type.
17. Now, in the port range, I'm going to give a dynamic port range that's given in the documentation. See when your client machine wants to connect onto another device so, we are connecting onto Port 22 on the Linux machine that is Web VM zero one, our own laptop, our client will also use a port number. This is going to be a temporary port number.
18. Once the changes are made save them.



19. Now if you will try to connect your instance in the Putty tool, this time you will be able to connect it with the putty tool.