😊 Amazon Network Firewall

AWS Network Firewall is a managed service that provides network protections for your Amazon Virtual Private Cloud (VPC). It allows you to deploy essential network security features to protect your workloads and applications running in the cloud. Here's an overview of what AWS Network Firewall offers:

Key Features:

1. **Stateless and Stateful Rule Engine:**
    - **Stateless Rules:** These rules are simpler and apply to individual packets without considering previous packets in the flow. They are ideal for tasks like packet filtering based on IP address, protocol, and port.
    - **Stateful Rules:** These rules track the state of network connections and can filter traffic based on entire sessions, not just individual packets. This allows for more complex security policies, such as intrusion prevention.
2. **Domain Name Filtering:**
    - You can block or allow traffic based on domain names, which is useful for preventing access to malicious websites.
3. **Centralized Management:**
    - You can manage and deploy network security policies across multiple VPCs and accounts within your AWS environment.
4. **Deep Packet Inspection:**
    - AWS Network Firewall supports deep packet inspection (DPI) to detect and block specific types of content or application protocols, providing advanced threat detection capabilities.
5. **Integration with AWS Services:**
    - It integrates seamlessly with other AWS services like AWS CloudWatch, AWS CloudTrail, and AWS VPC Traffic Mirroring for logging, monitoring, and threat detection.
6. **Scalability and Availability:**
    - As a managed service, AWS Network Firewall scales automatically based on traffic and ensures high availability without the need for manual intervention.

Use Cases:

- **Intrusion Detection and Prevention:** Monitor and block malicious traffic in real time.
- **Web Filtering:** Control access to websites and prevent data exfiltration.
- **Network Segmentation:** Secure your VPC by segmenting different parts of your network based on security needs.

- **Compliance:** Helps meet regulatory requirements by enforcing specific security policies and monitoring network traffic.

How It Works:

AWS Network Firewall is deployed within your VPC, and it inspects and filters traffic between subnets within the VPC or between the VPC and the internet or other networks. You define rules and policies that specify the allowed and denied traffic, and the firewall enforces these rules.

Benefits:

- **Ease of Use:** As a fully managed service, it eliminates the need to manage and maintain firewall infrastructure.
- **Customizable:** You can tailor the rules to meet specific security needs.
- **Cost-Effective:** You pay only for the traffic processed by the firewall and the resources consumed, with no upfront costs.

AWS Network Firewall is ideal for organizations looking to enhance the security of their cloud infrastructure with a scalable, managed solution that integrates well with other AWS services.

This guide walks you through setting up and managing a basic AWS Network Firewall within a Virtual Private Cloud (VPC). You start by creating a VPC, subnets, and an Internet Gateway, then configure route tables to control traffic flow. After launching an EC2 instance in your VPC, you install necessary services and ensure internet connectivity.

The key steps involve setting up firewall rule groups (both stateful and stateless) that define which domains and protocols are allowed or blocked. You then create a firewall policy and apply it to your firewall. The firewall is configured to allow or block specific traffic, such as permitting access to certain websites (like Google and Microsoft) while blocking others (e.g., YouTube).

Finally, you verify the firewall's effectiveness by testing website access from your EC2 instance and adjusting the rules as needed. The process concludes with the cleanup of all resources.

End Goal: The goal is to set up a secure VPC environment where internet access is tightly controlled by an AWS Network Firewall, allowing or blocking traffic based on specified rules.

😄 To begin with the Lab:

1. In your AWS Console navigate to VPC and click on Create VPC. Here you have to choose VPC only, give it a name then give your IPv4 CIDR block as you can see below, and click on Create VPC.

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

(•) VPC only ( ) VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

demo-firewall-VPC

IPv4 CIDR block Info

(•) IPv4 CIDR manual input

( ) IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

(•) No IPv6 CIDR block

( ) IPAM-allocated IPv6 CIDR block

( ) Amazon-provided IPv6 CIDR block

( ) IPv6 CIDR owned by me

Tenancy Info

Default

2. Then we are going to create our Subnet. So, go to subnets and click on Create Subnet.
3. First, choose your VPC then scroll down give your subnet a name, and give the IPv4 subnet CIDR block.

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-0f9d5a647c360d3d1 (demo-firewall-VPC)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

demo-public-subnet

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Singapore) / ap-southeast-1a

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.2.0/24 256 IPs

4. Now we are going to create another subnet for the firewall. Choose your VPC and then give your subnet a name chooses the AZ and give the CIDR block as shown below.

VPC

VPC ID

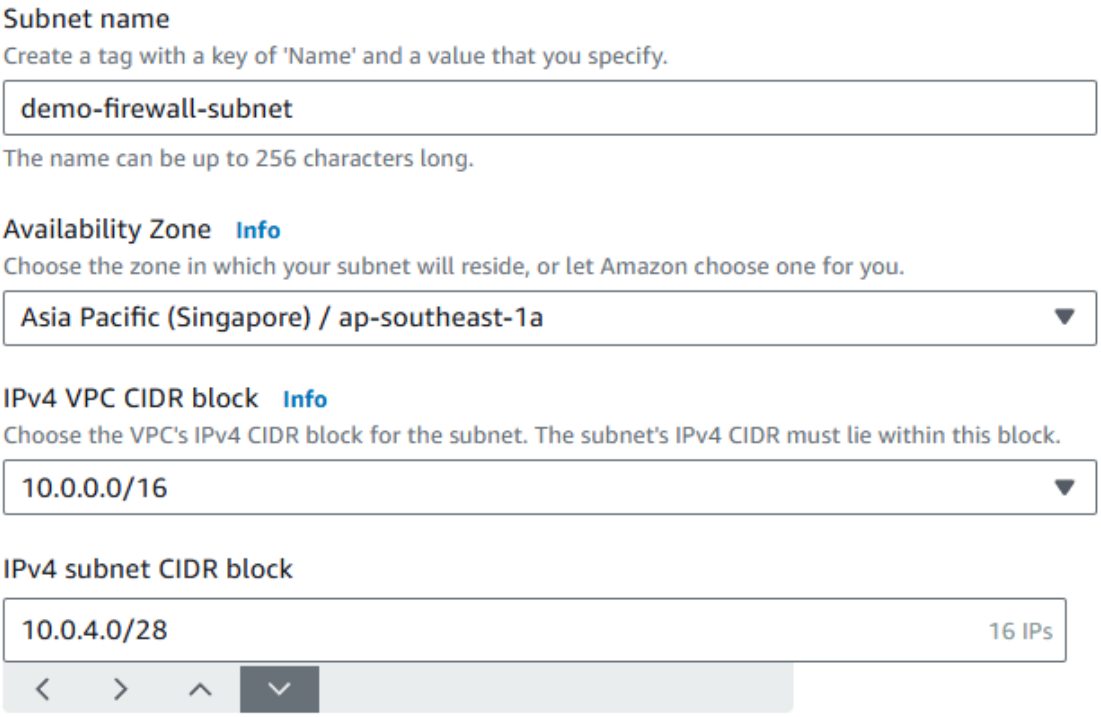
Create subnets in this VPC.

vpc-0f9d5a647c360d3d1 (demo-firewall-VPC)

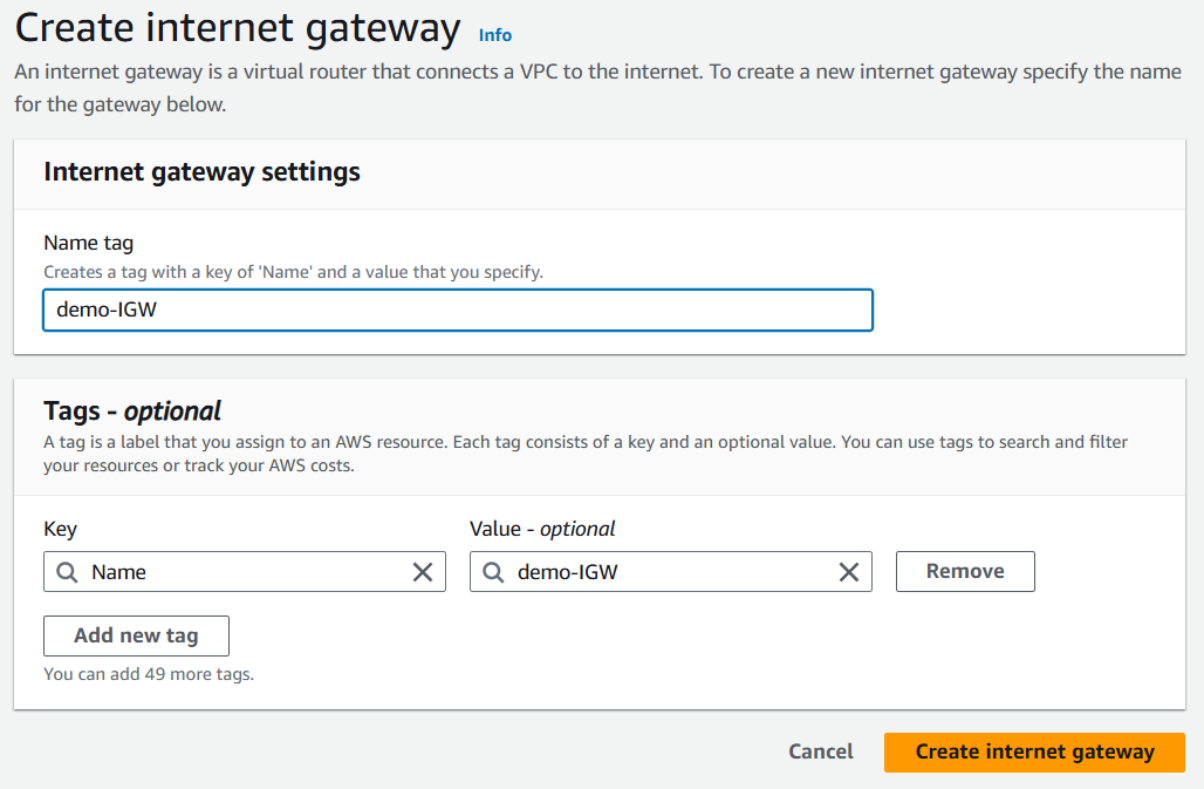
Associated VPC CIDRs

IPv4 CIDRs

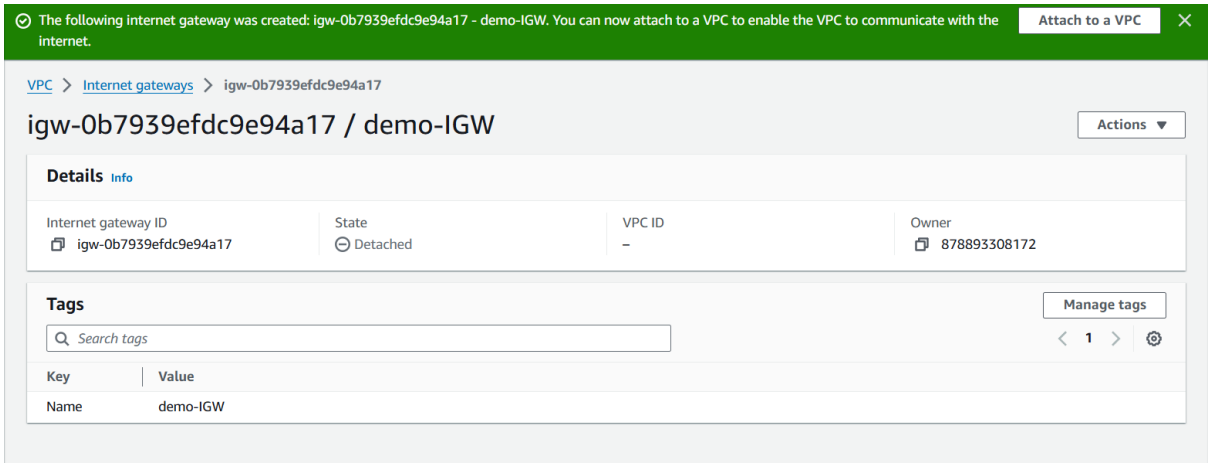
10.0.0.0/16

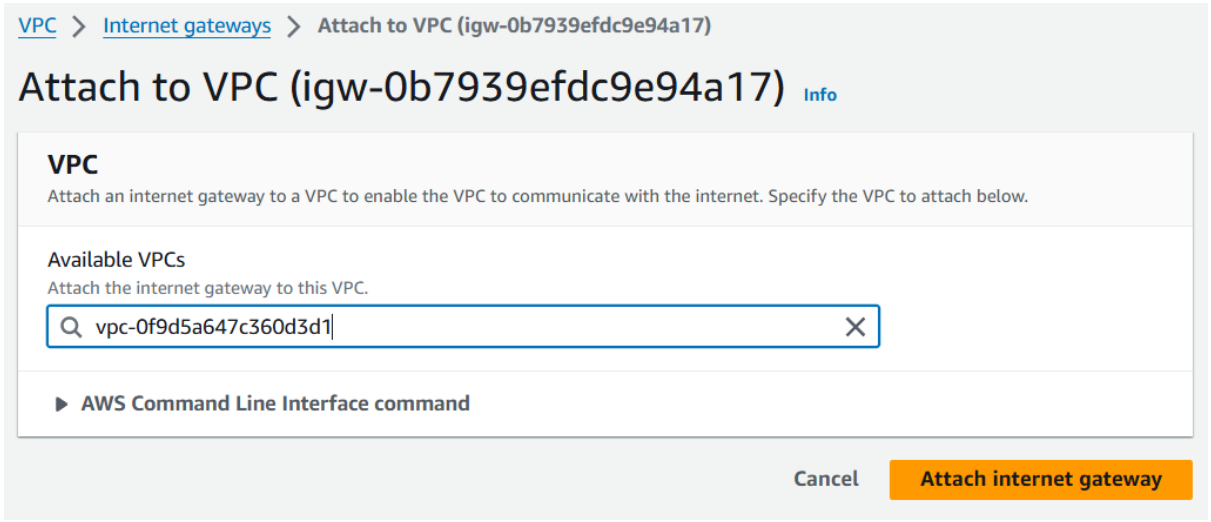


5. After creating your subnet, you need to create an Internet Gateway. So, go and click on create. Just give it a name and click on create IGW.

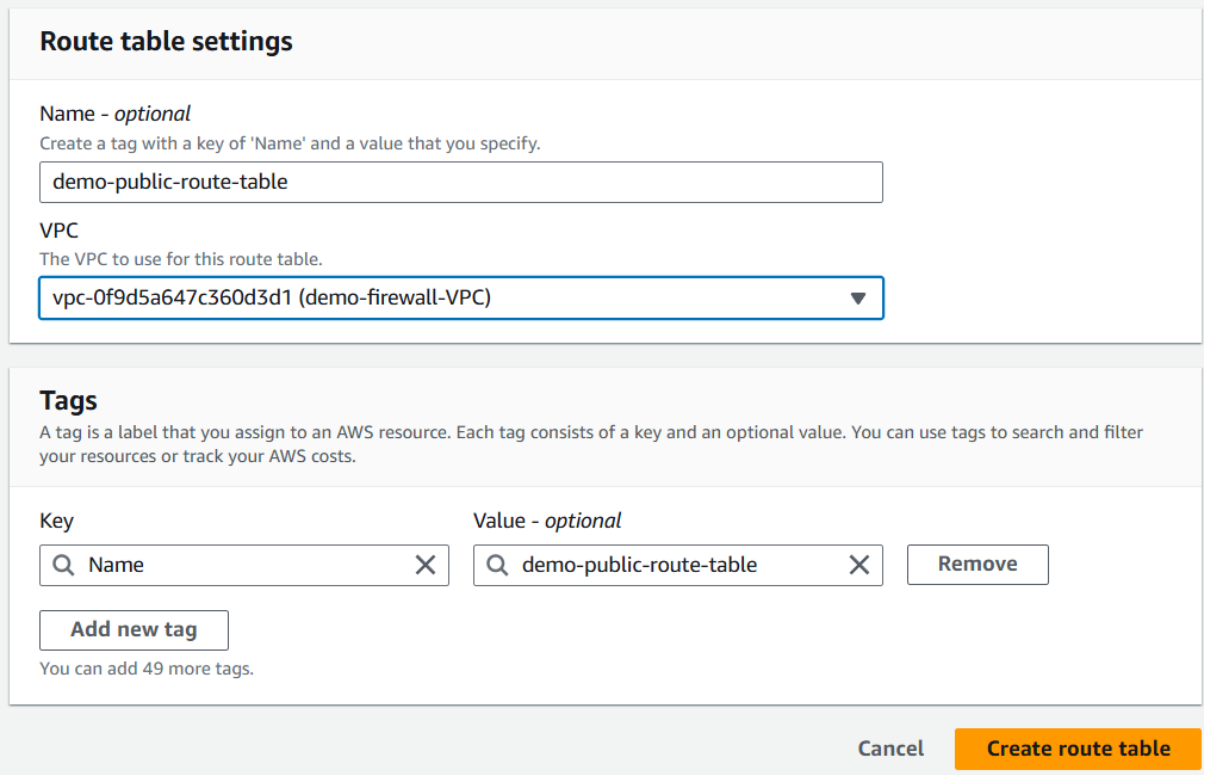


6. Now attach it with your VPC.

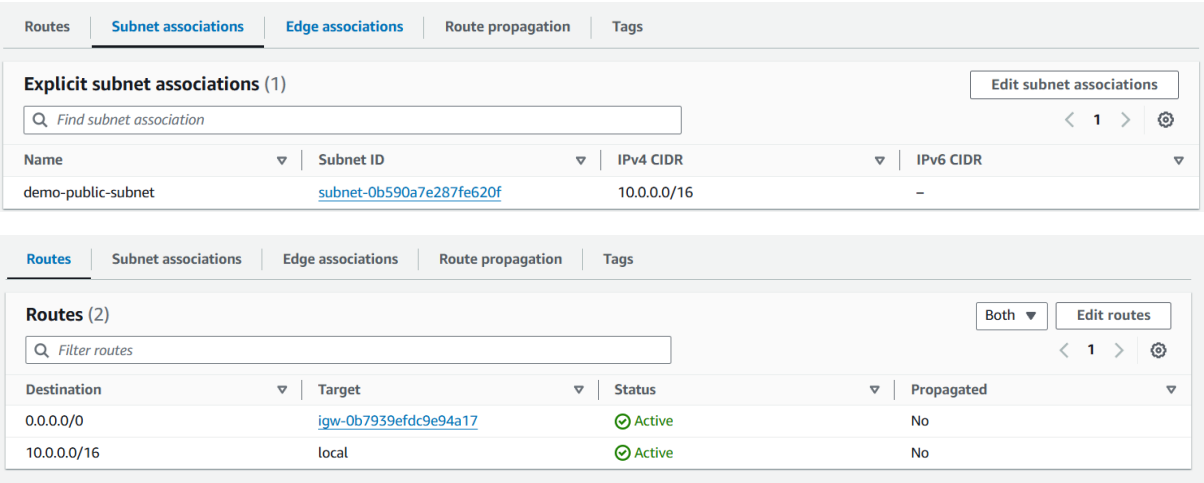




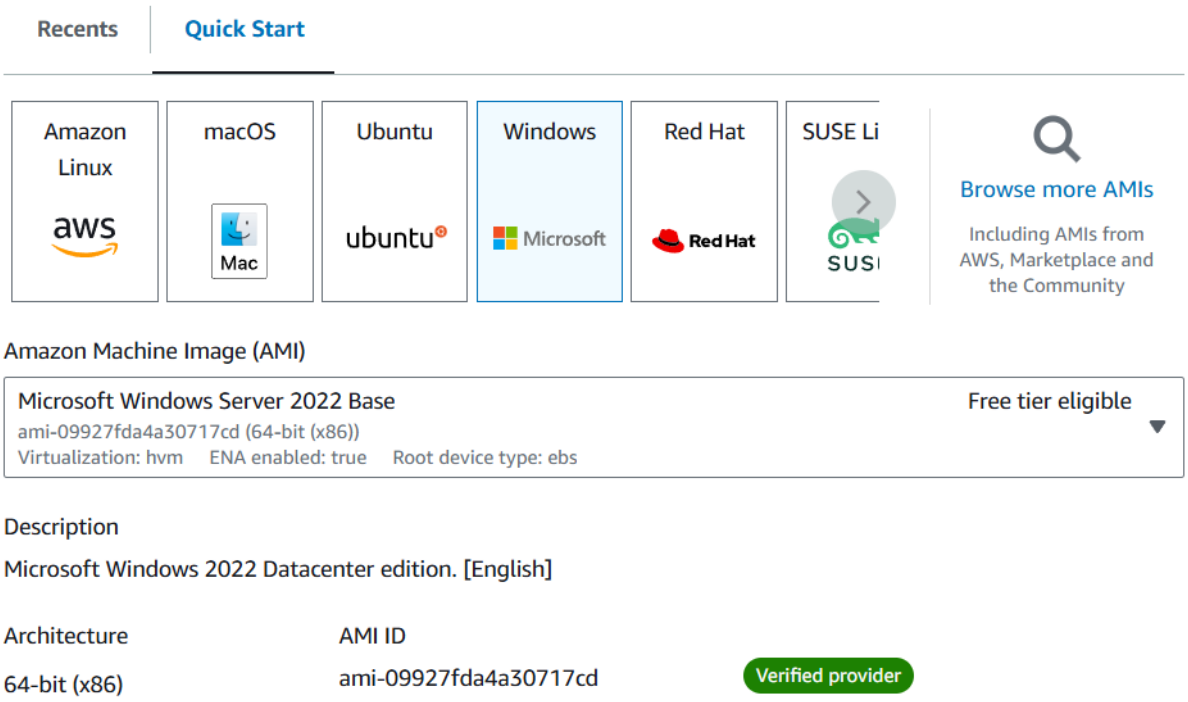
7. Now we are going to create a public route table and associate our subnet with it. So, give it a name and choose your VPC, click on create.



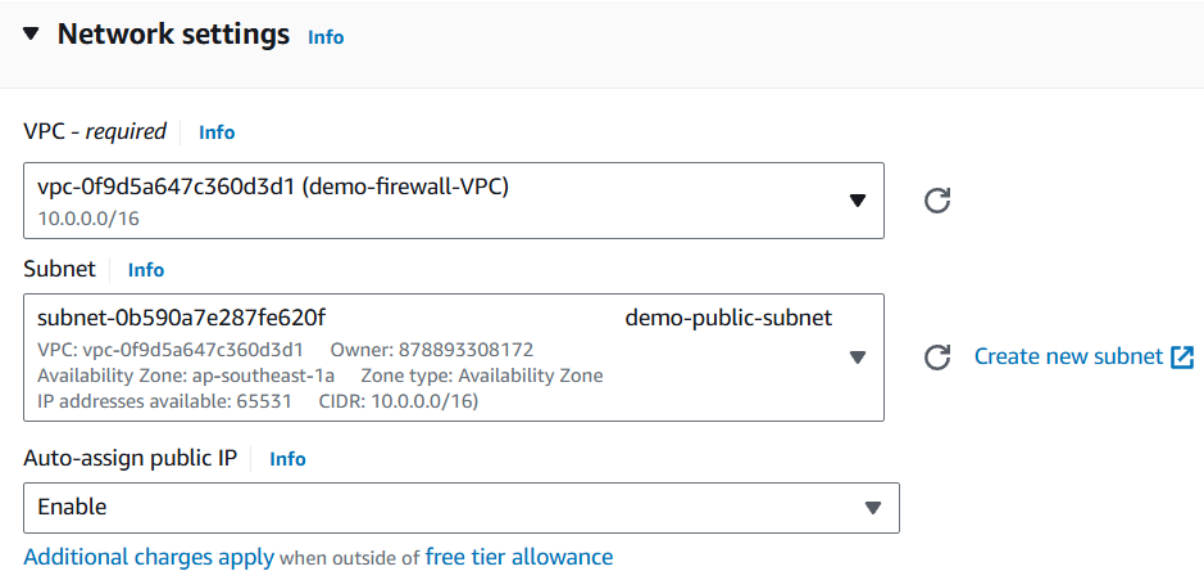
8. Now you need to associate your subnet with the route table. After that create a route for internet gateway and choose the destination as 0.0.0.0/0.



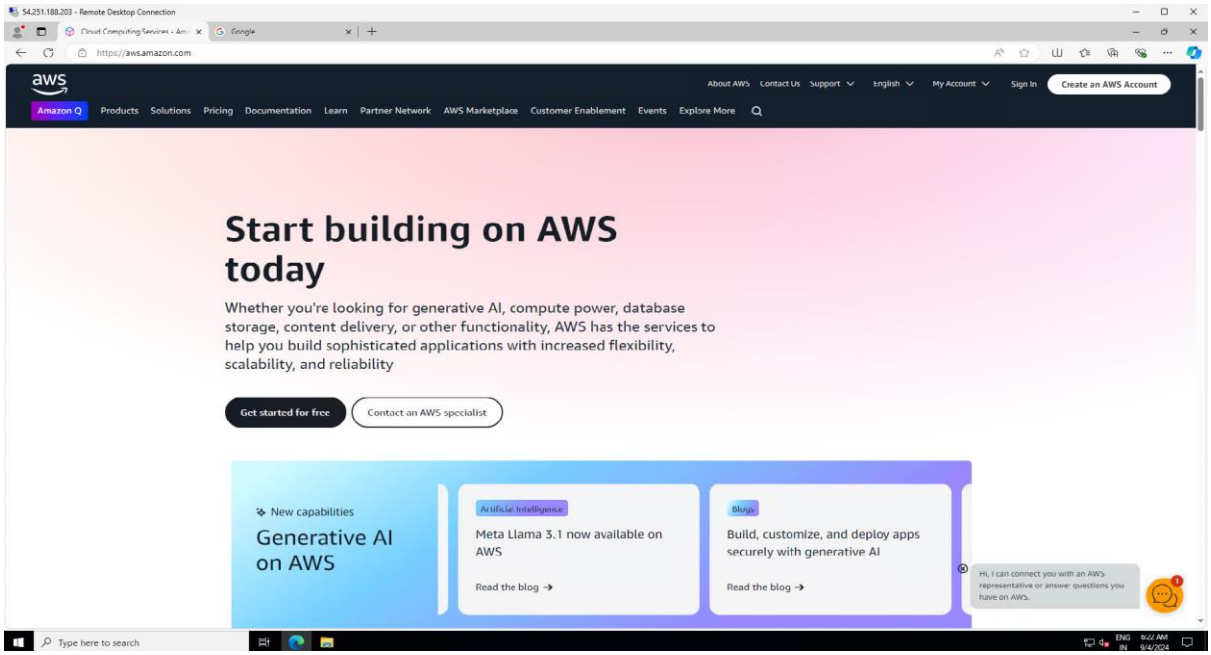
9. Now we are done with our VPC, **so navigate to EC2** and create an EC2 instance.
10. Choose Windows Machine, your instance type, and the key pair.



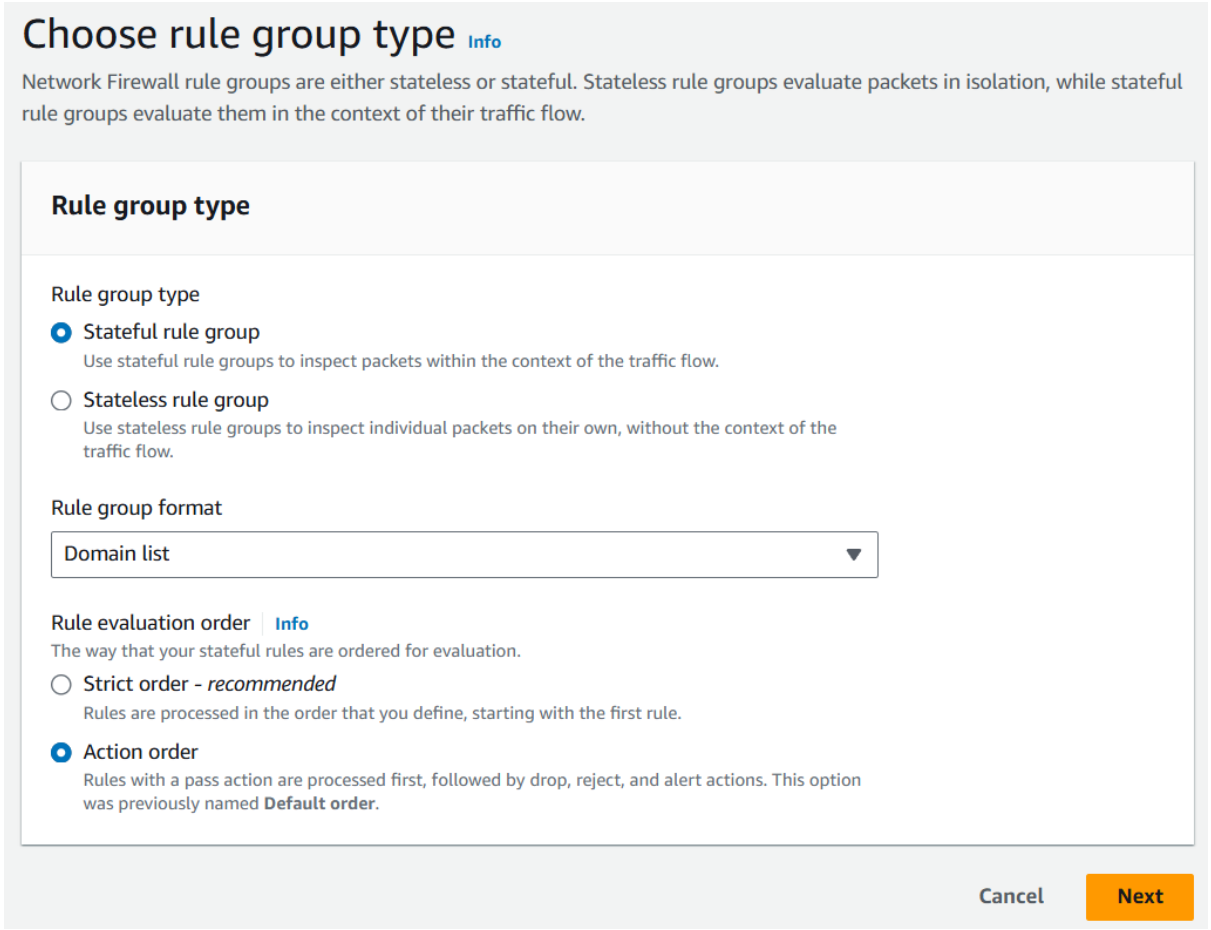
11. Just remember to choose your VPC and the subnet. Create your instance.



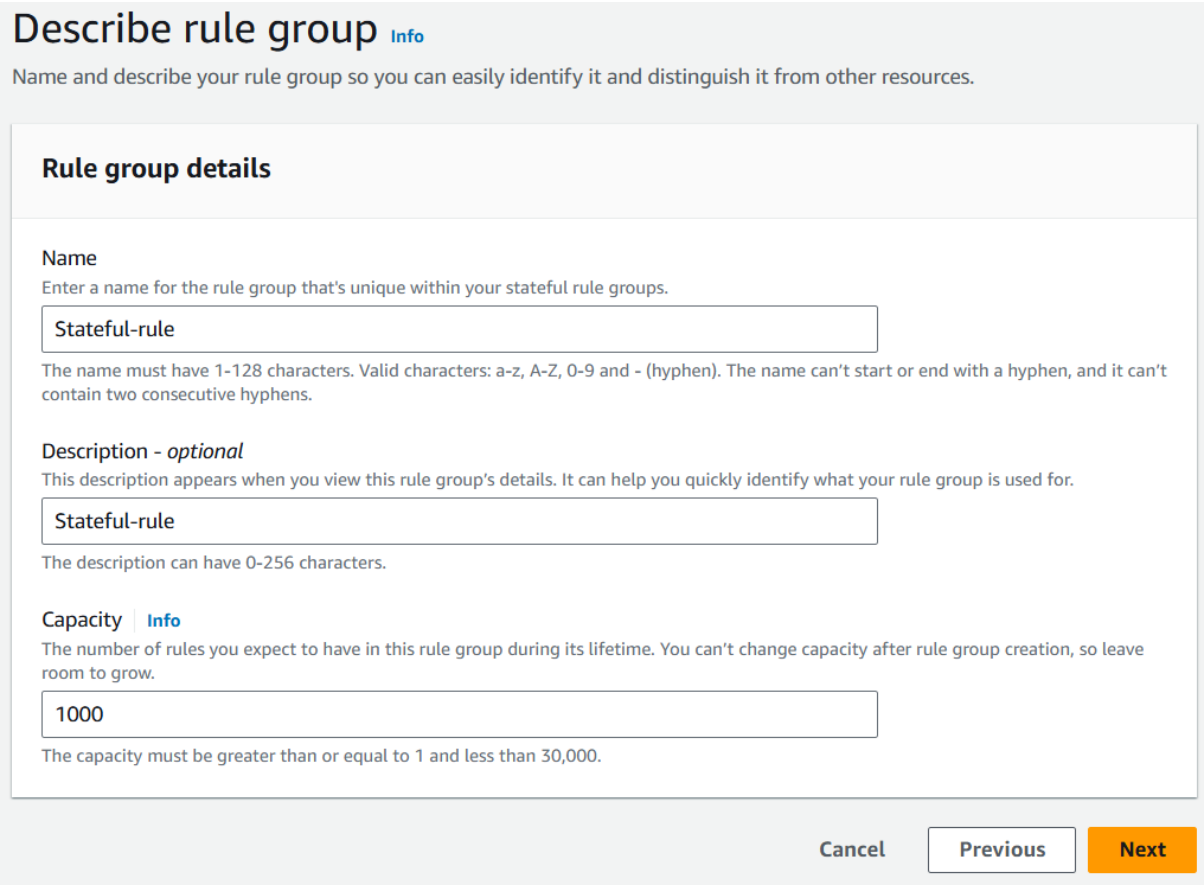
12. Once your instance is created login to it then open the internet browser in your VM.
13. Below you can see that on our machine we can reach the internet.
14. Also, install the IIS service on your instance.



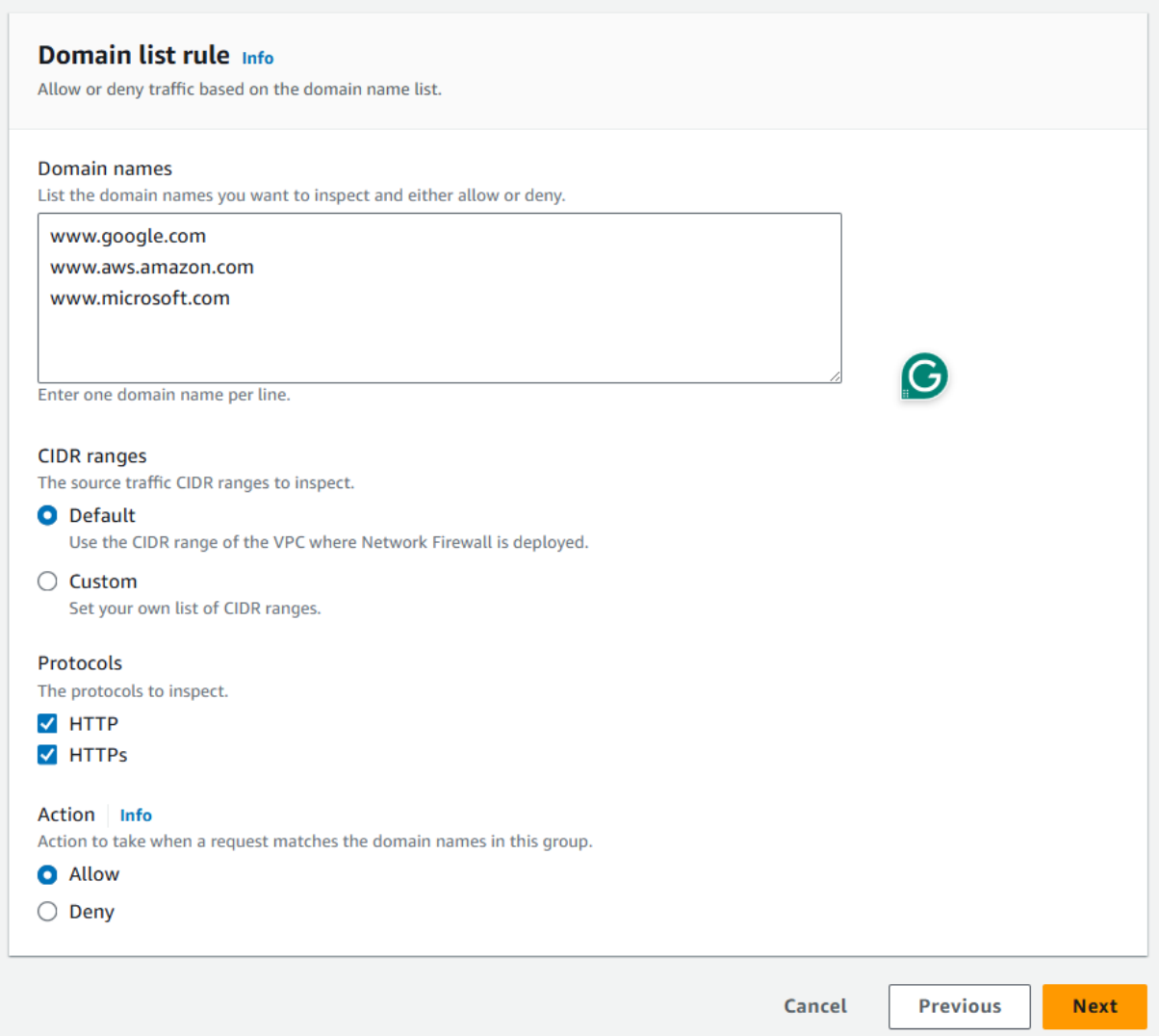
15. Now we are going to set up the Network Firewall. So, come back to your VPC, and from the left pane scroll down to Network Firewall, then open network firewall rule groups. Click on Create rule groups.
16. In step 1, choose Stateful rule groups and in the format choose domain list. In rule evaluation order choose Action order. Click on next.



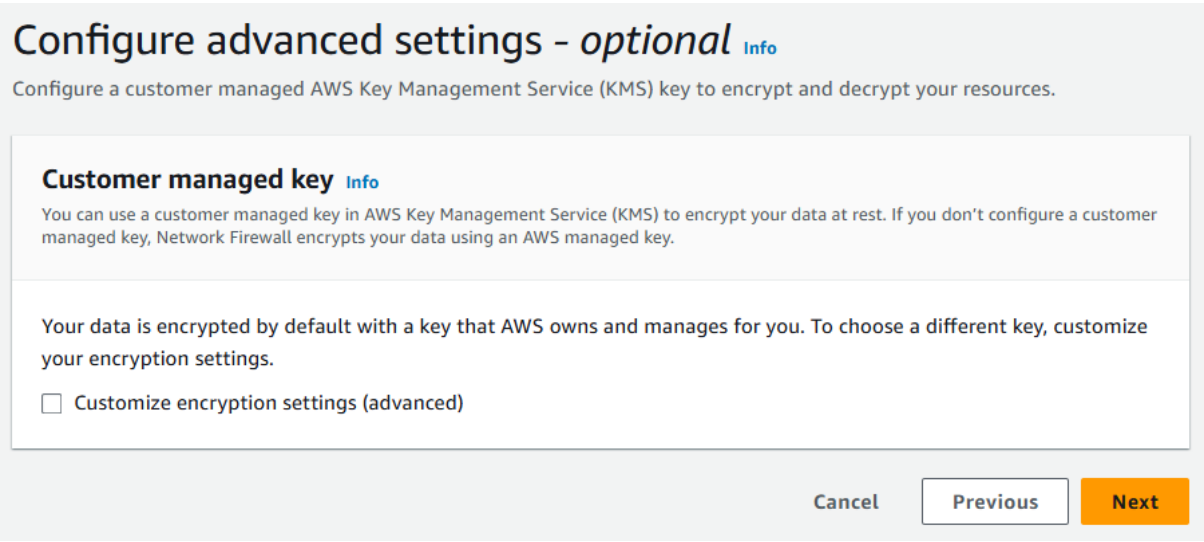
17. After that give it a name and capacity as you see below. Click on next.



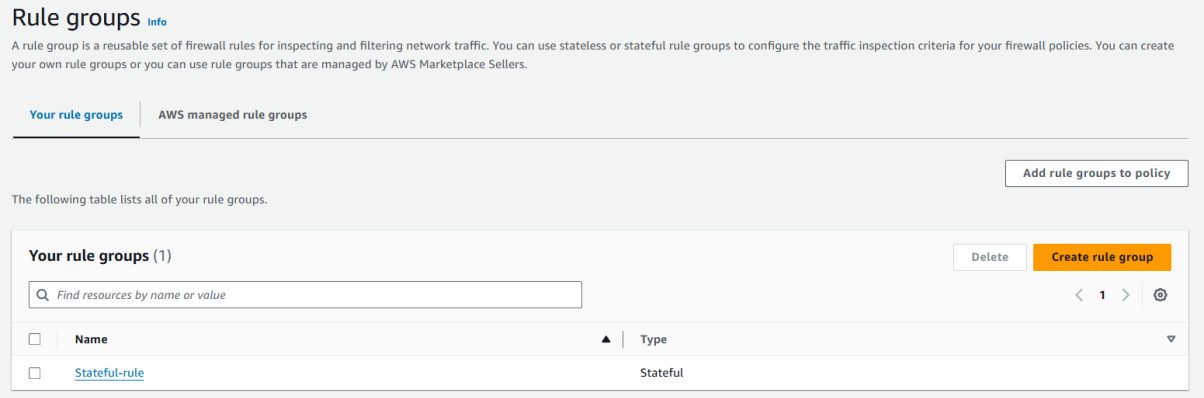
18. Now in step 3, give the domain names that you want to allow. Keep CIDR ranges to default, protocols to default and in action choose Allow.



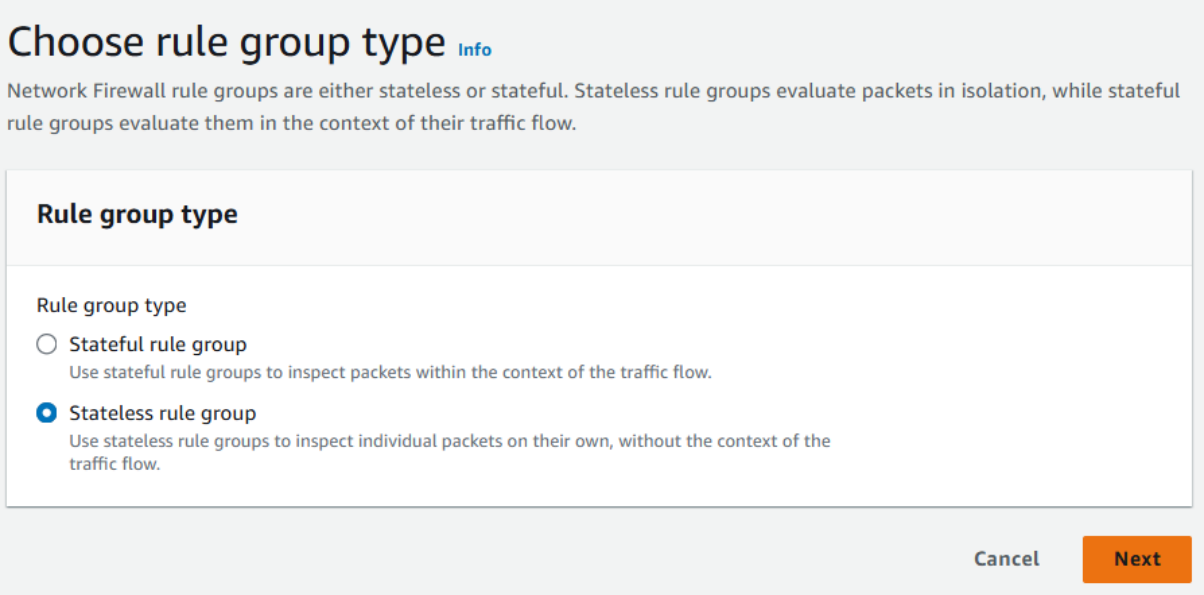
19. For step 4, skip it and move to the review page then create your firewall rule groups.



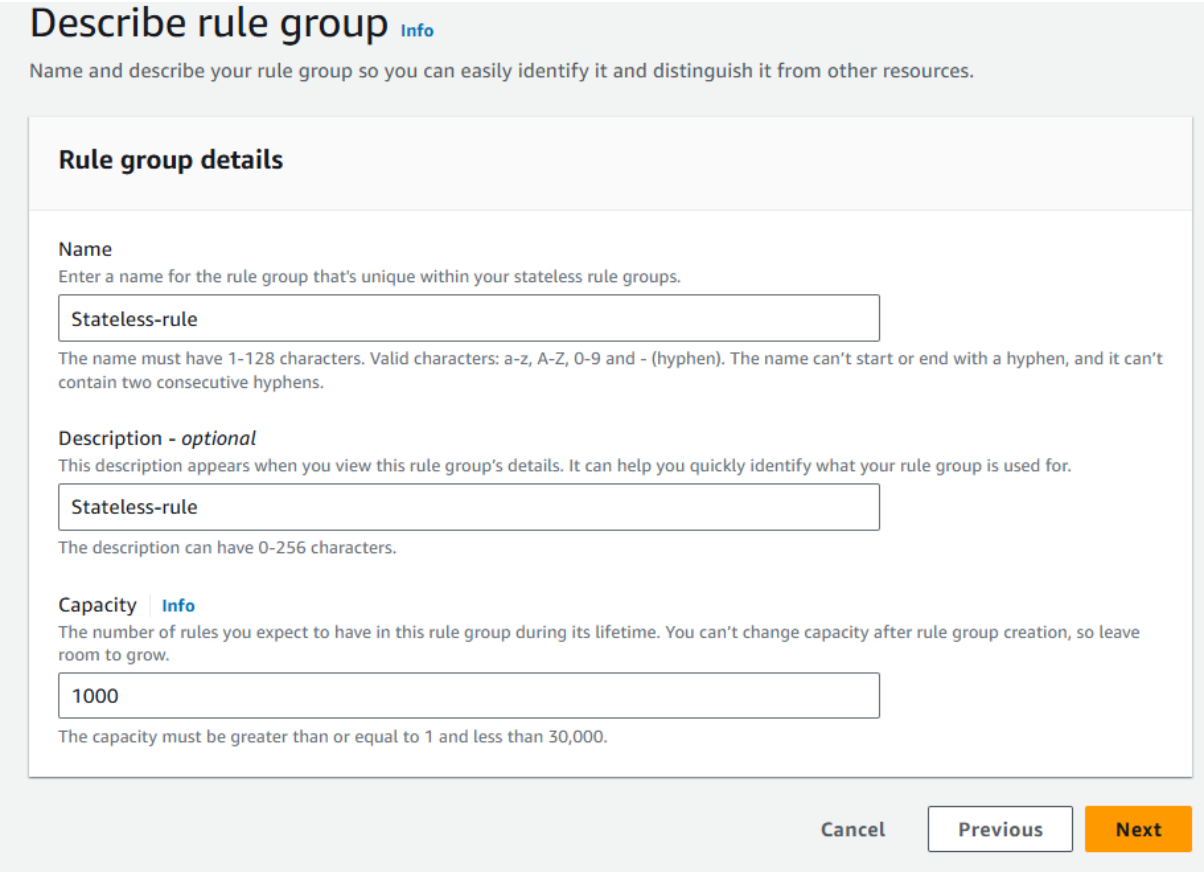
20. Below you can see that our Stateful rule group has been created now we are going to create a stateless rule group. Click on create rule group.



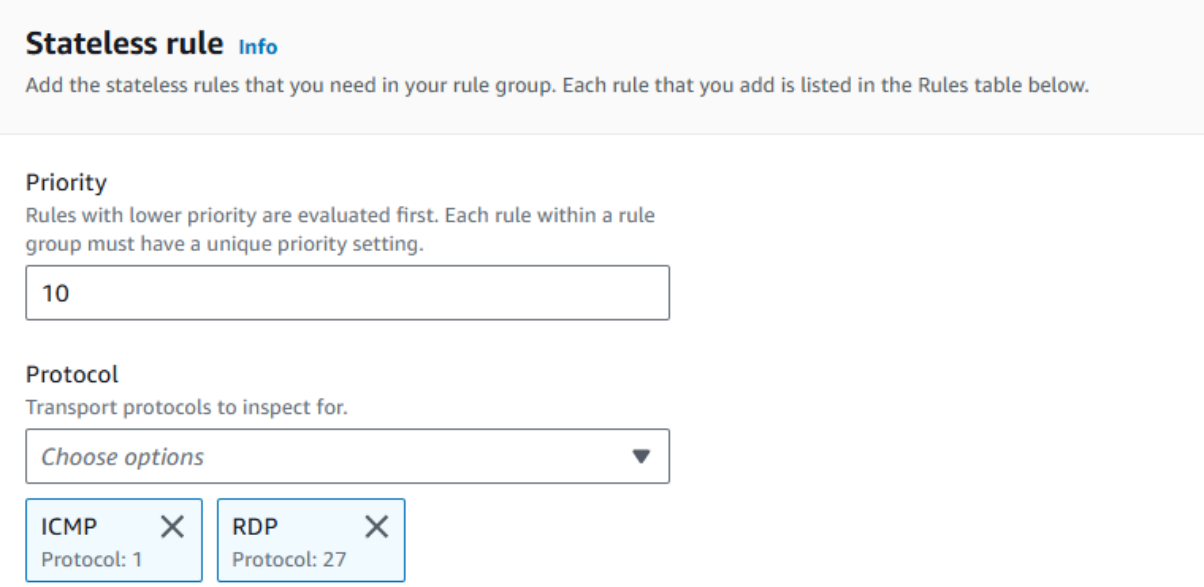
21. Here in step 1 you need to choose the Stateless rule group and click on next.

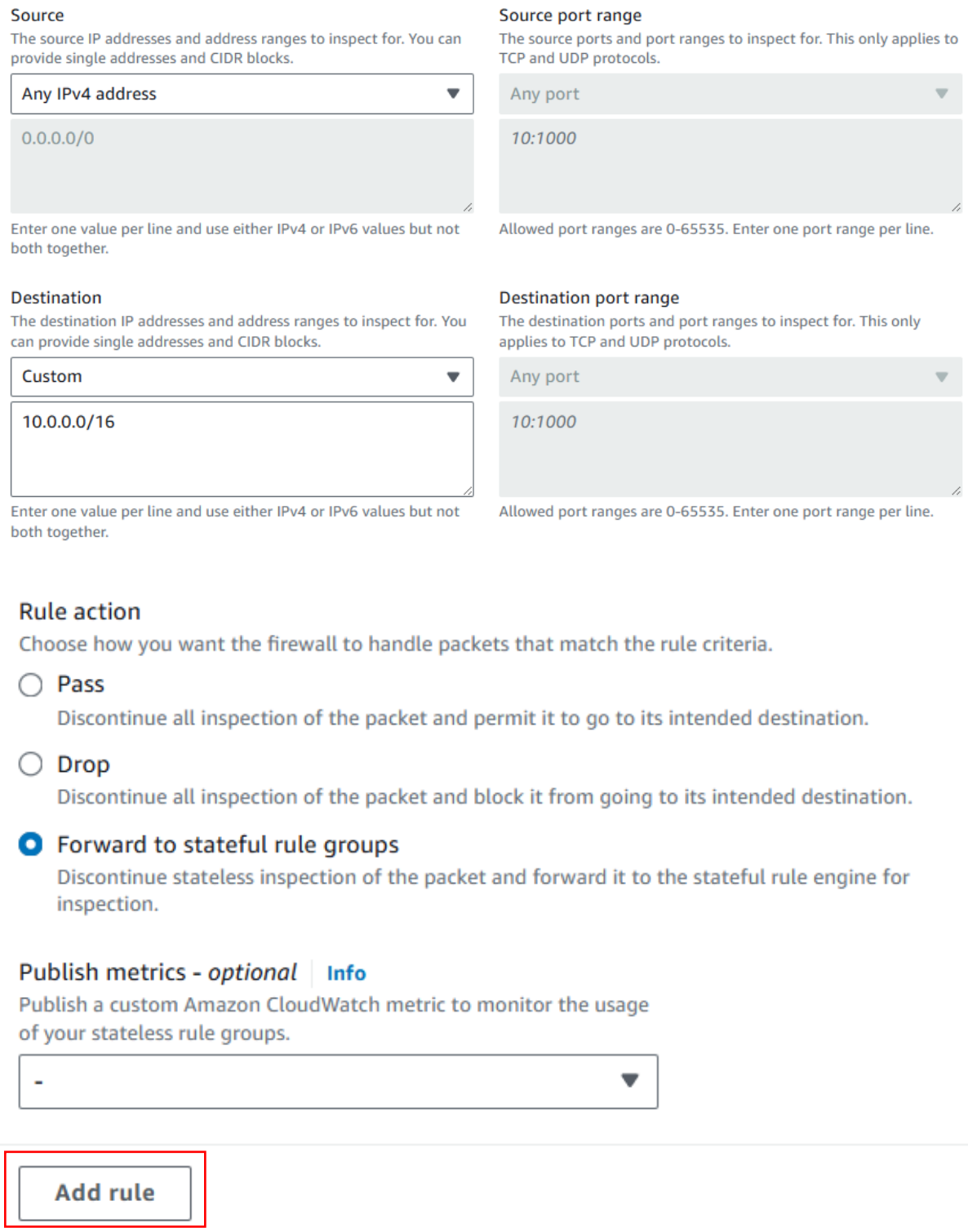


22. Then give it a name and capacity as you can see below.

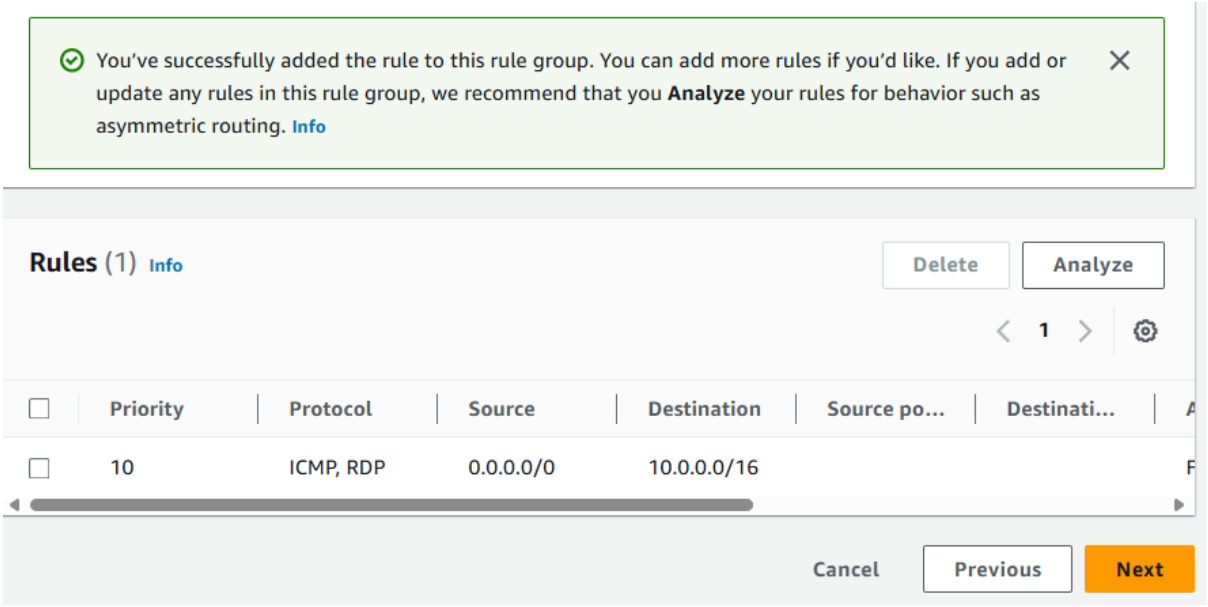


23. Now on step 3, first set its priority and choose ICMP and RDP protocol then scroll down. In the source and destination choose as shown below in the snapshot. Lastly, in the rule actions choose forward to stateful rule groups. Then click on add.

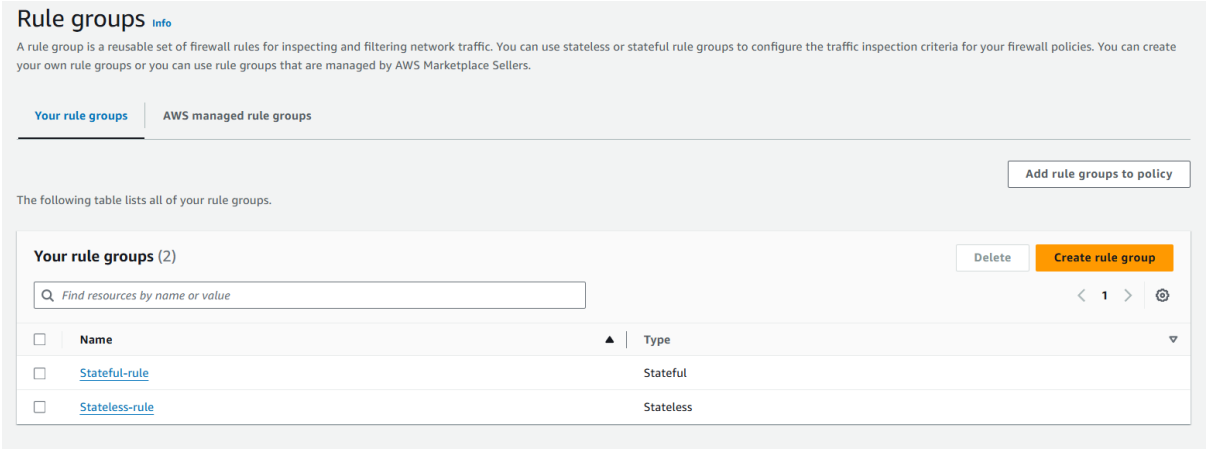




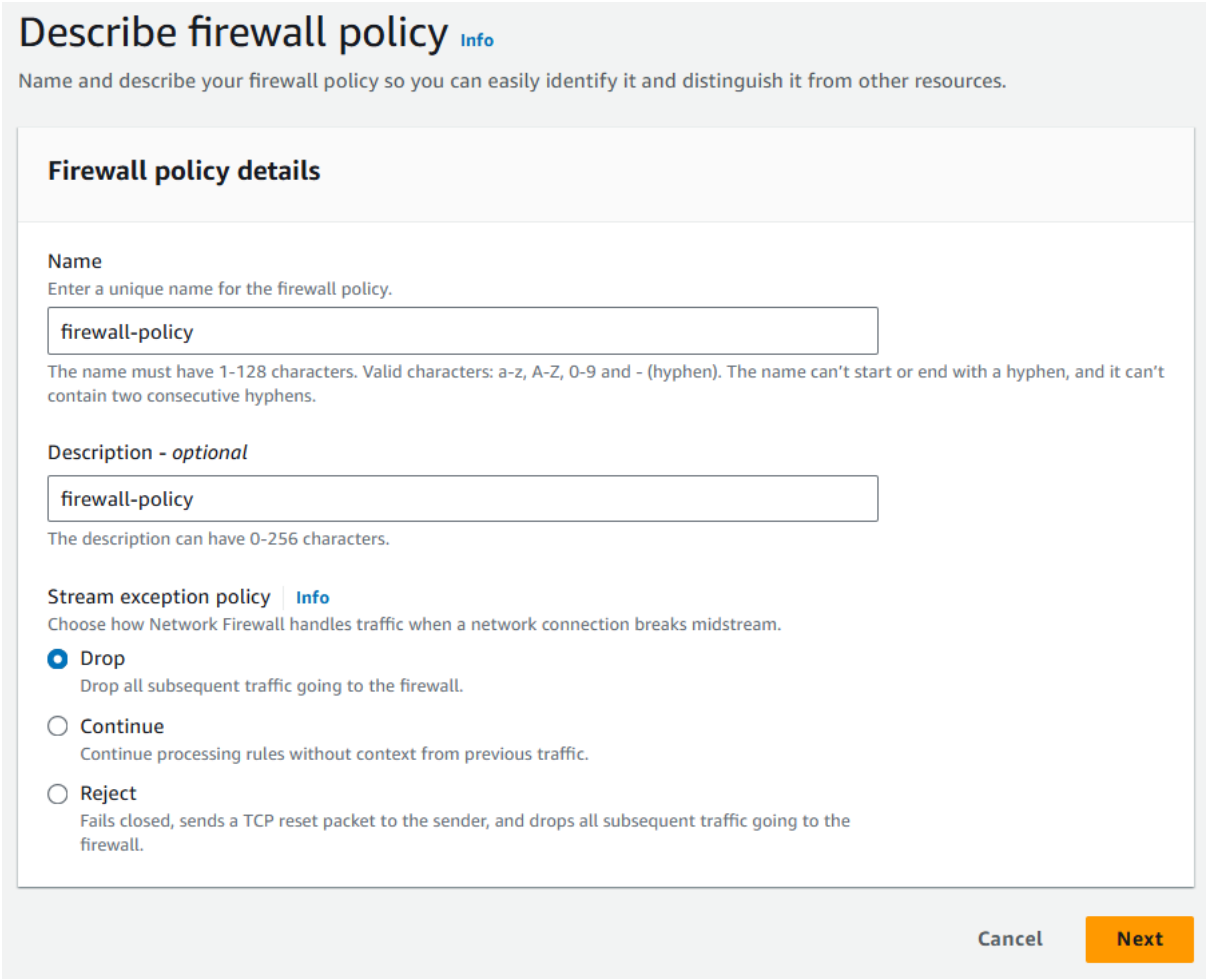
24. Then in the rules you will see your rule and click on next. Move to the review page and create your stateless rule group.



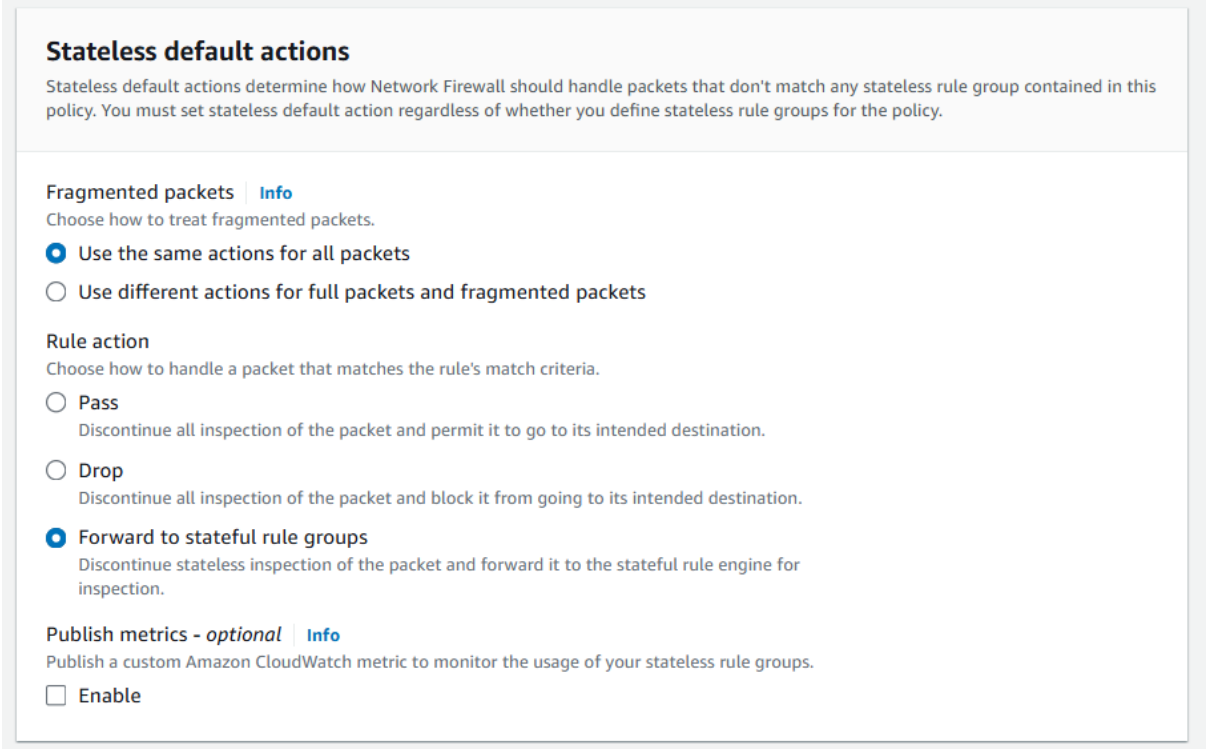
25. Below you can see that we have create both of our rule groups.



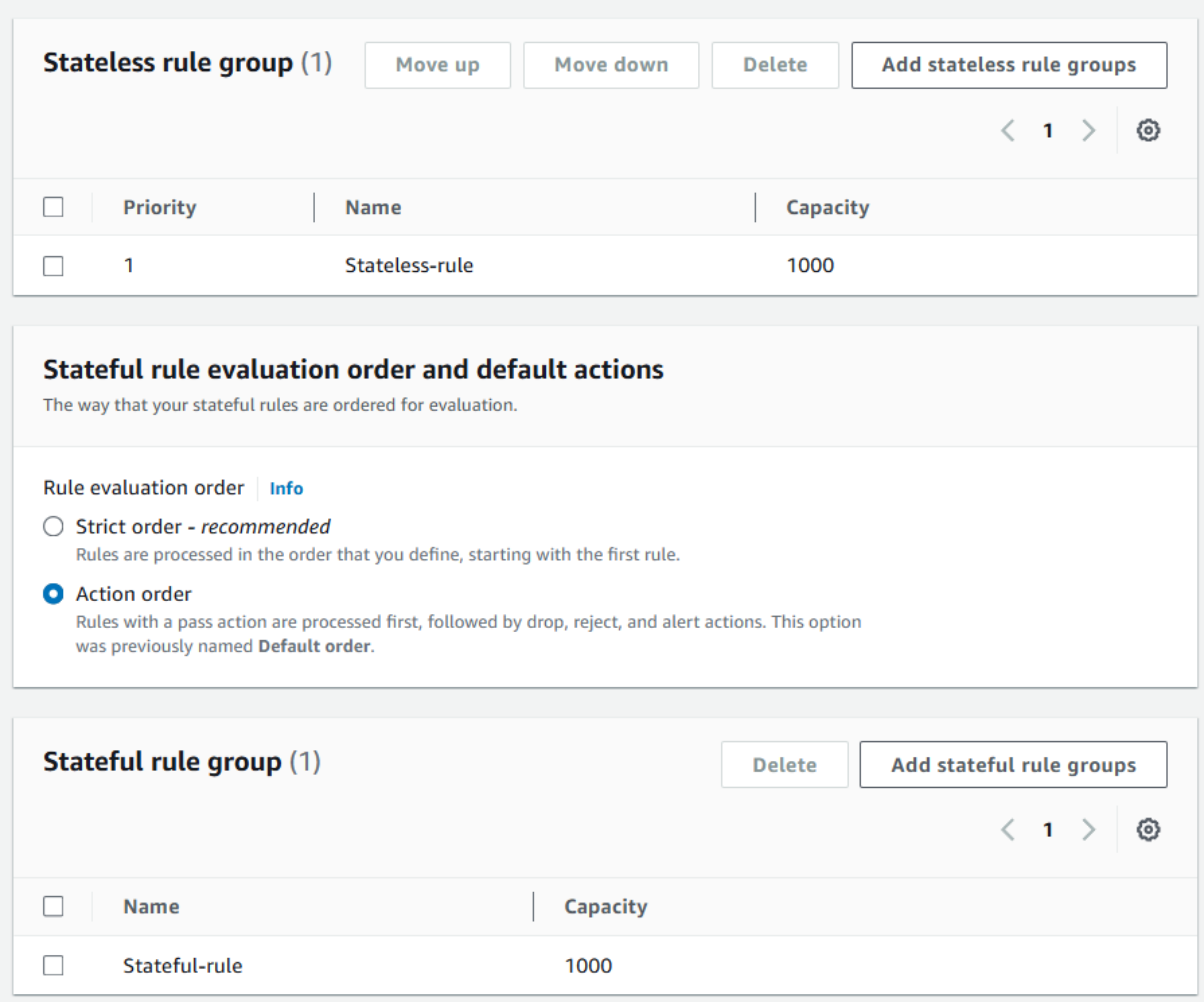
26. Now we need to create a firewall policy. So, in step 1 give it a name and click on next.



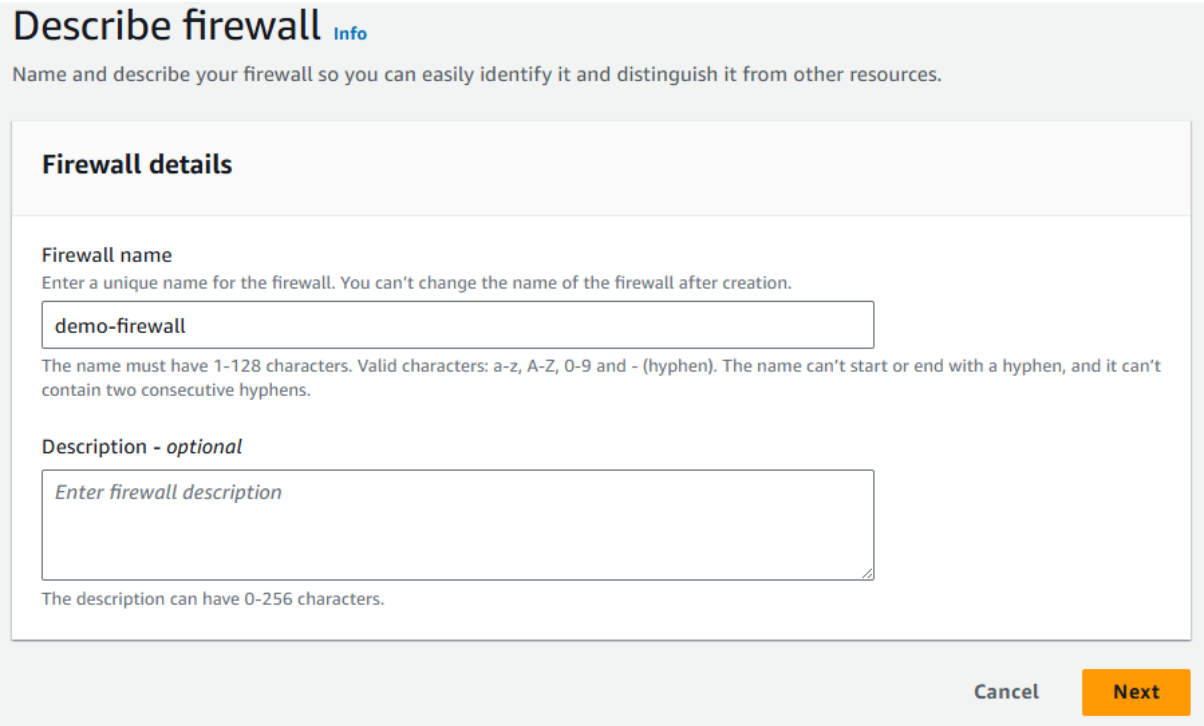
27. Then in step 2, keep default settings for stateless default actions.



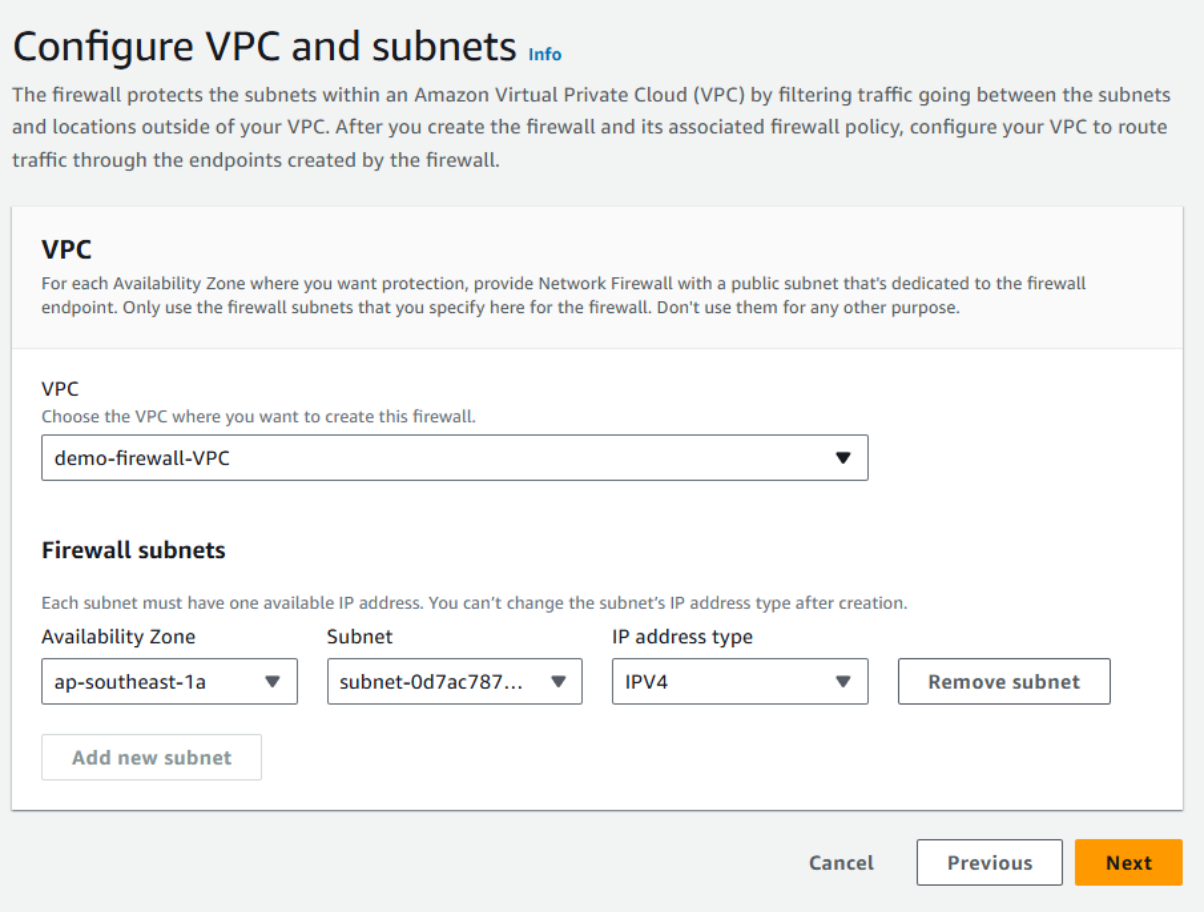
28. After that you need to add your stateless rule groups and choose Action order in stateful rule evaluation order. In the end, choose your stateful rule group. Move to review page and create your firewall policy.



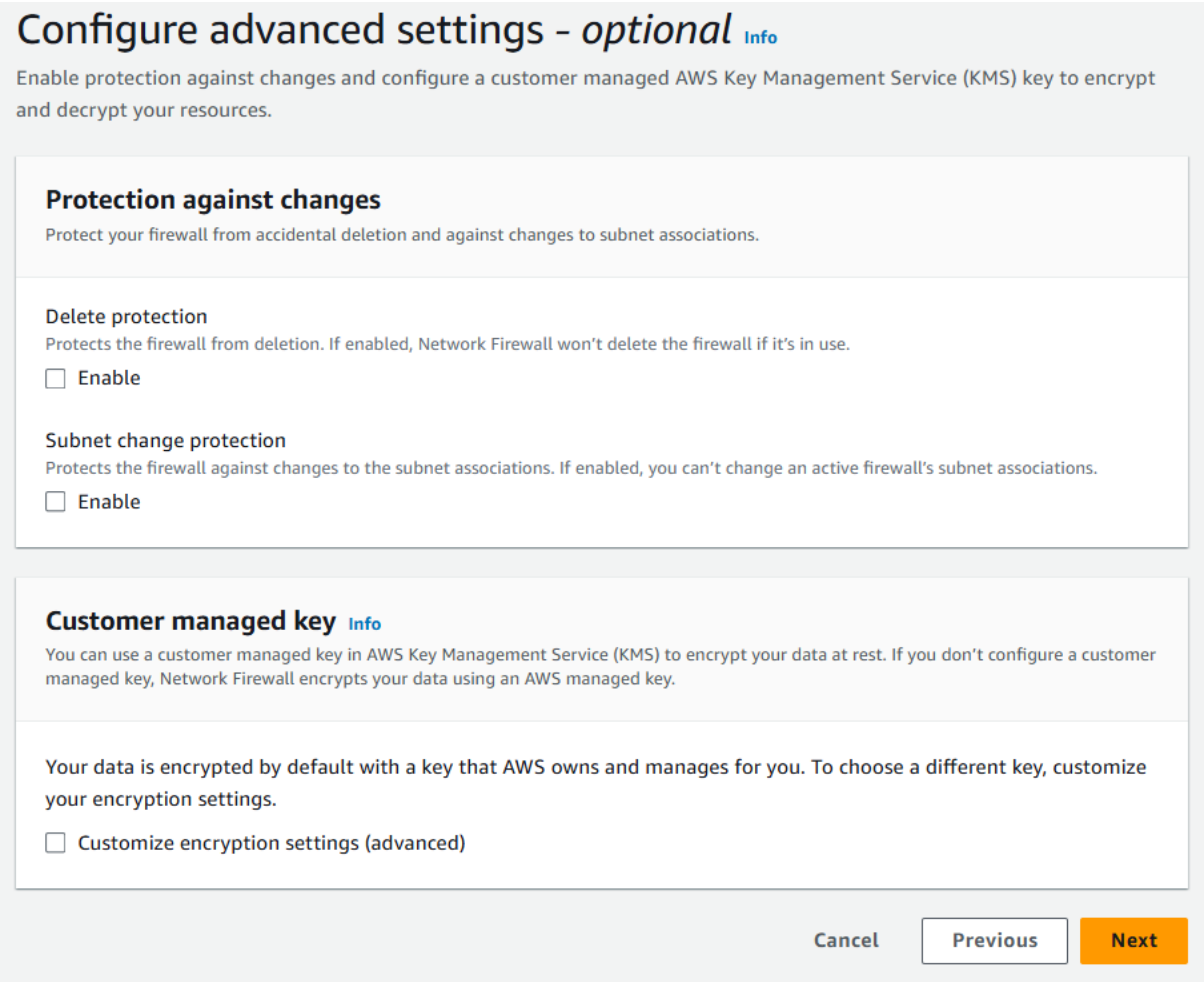
29. Now we are going to create our Firewall. So, go to Firewalls and click on Create. Give a name to your firewall and click on next.



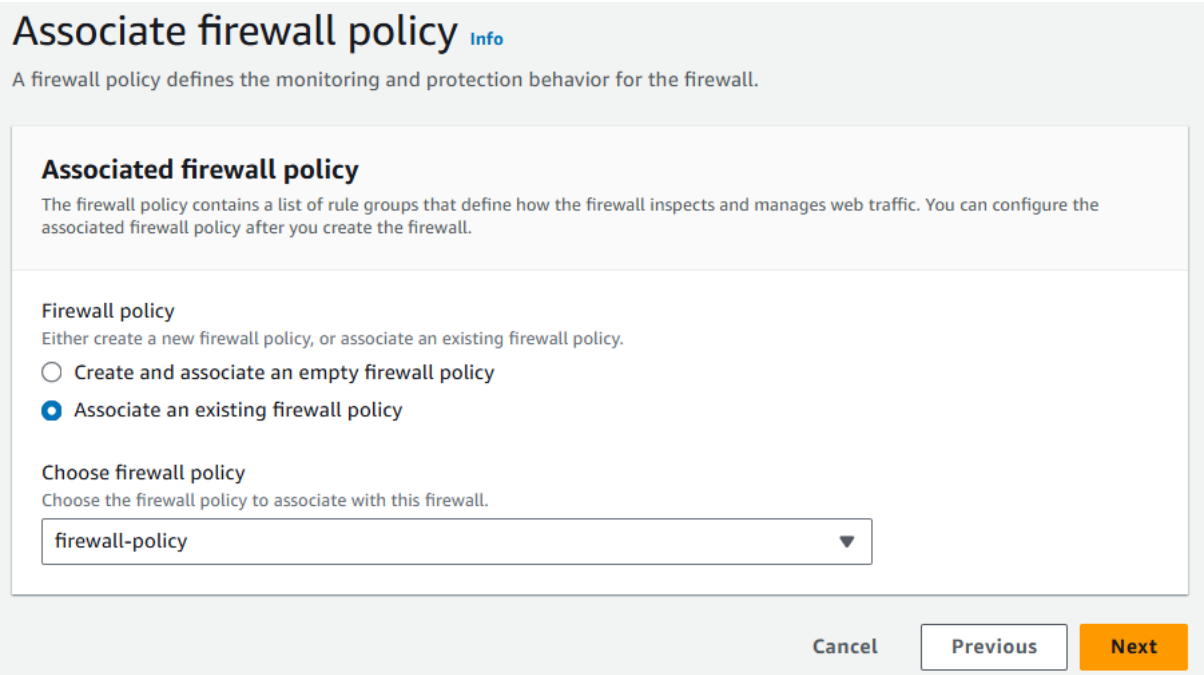
30. Then in the step 2 choose your AZ, your firewall subnet and the IP address type, click on next.



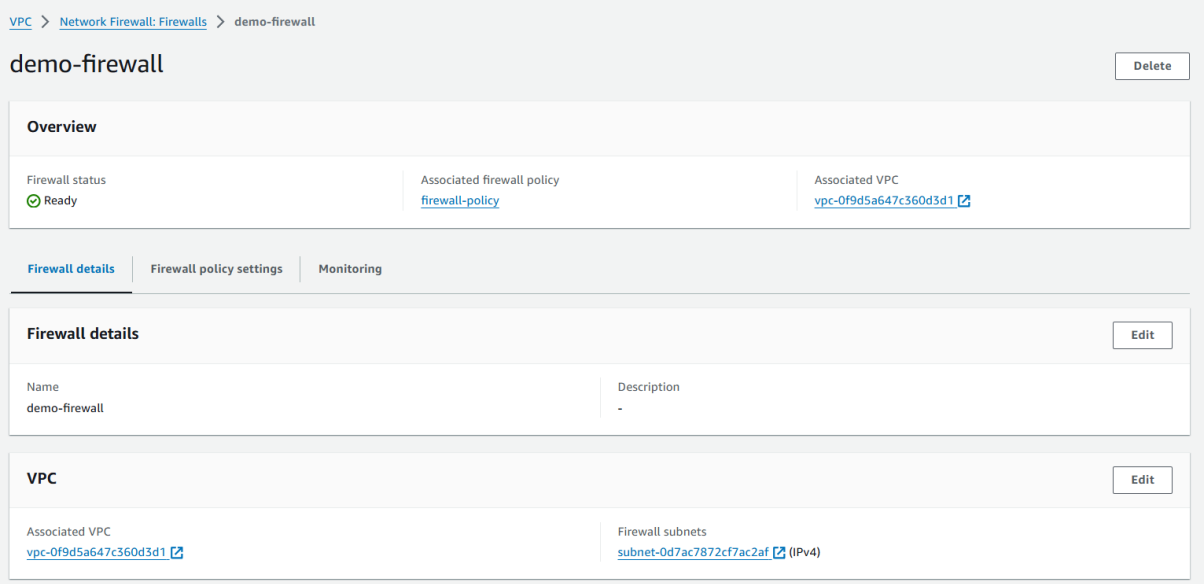
31. For step 3, disable the protection. Click on next.



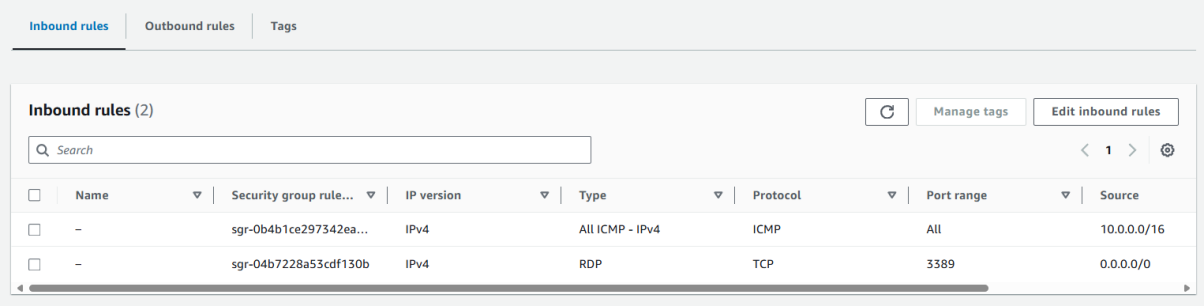
32. Then choose your existing firewall policy. Move to the review page and create your firewall. It will take some to create your firewall.



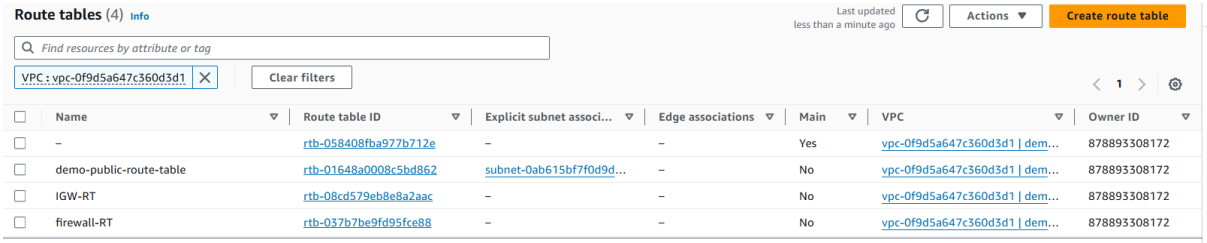
33. Below you can see that our firewall is now ready.



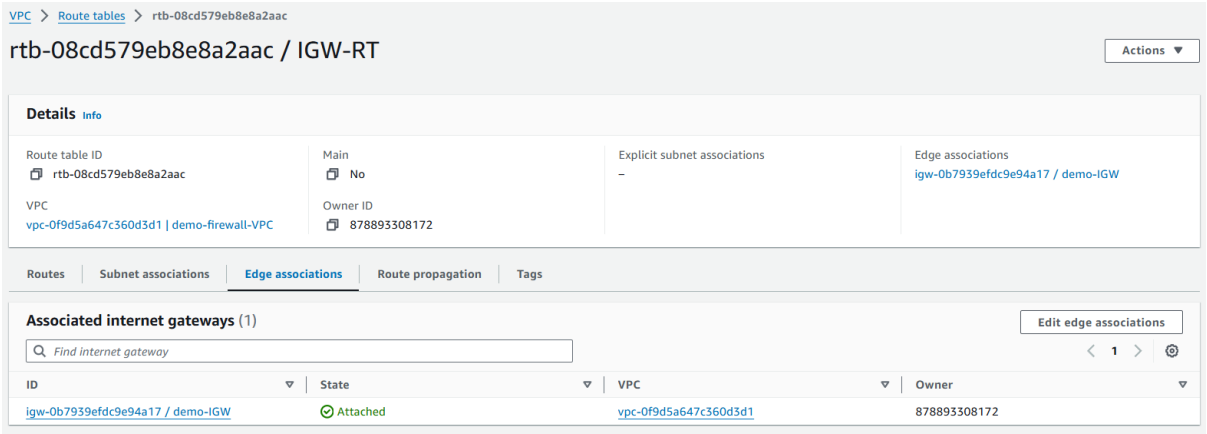
34. Go to your EC2 instance and in the security group you need to add an ICMP port for source CIDR 10.0.0.0/16.

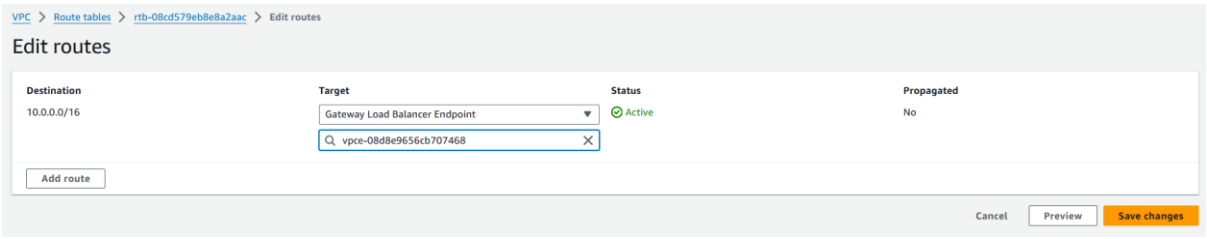


35. Now move to the route table and create route tables to change the routing. So, we are going to create two route tables, one for the firewall and another for the internet gateway.
36. Below you can see that we have created both of our route tables.

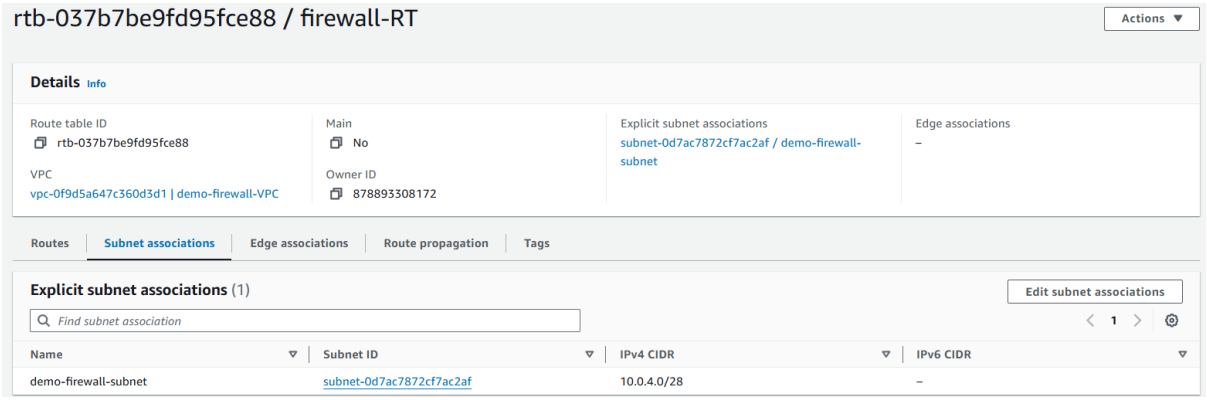


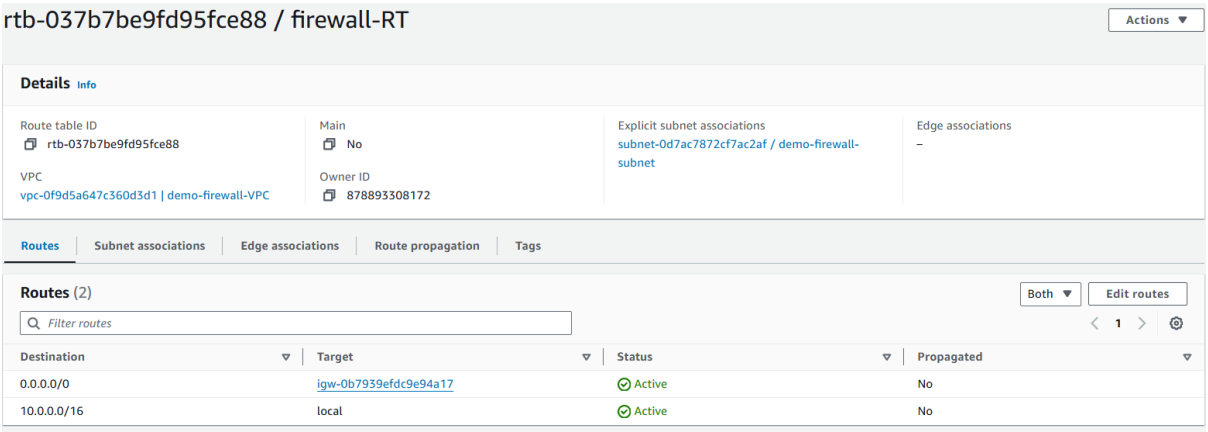
37. So, in your Internet gateway route table go to edge association and associate it with your Internet gateway. Then go to route, click on edit, and in the target choose gateway load balancer, click on save.



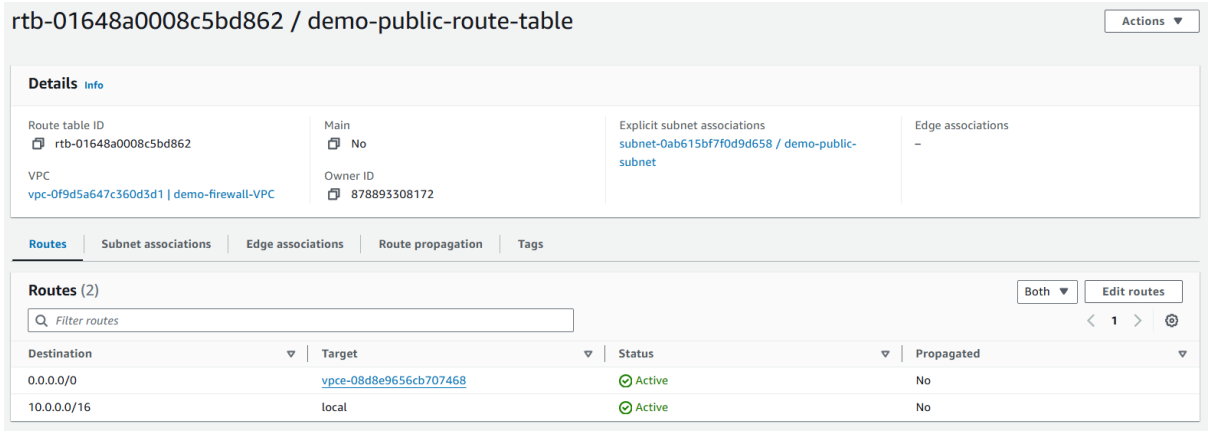


38. Now go to the firewall route table, in the subnet association, associate your firewall subnet with your firewall route table.
39. After that go to the routes and create a route for internet gateway from destination 0.0.0.0/0.

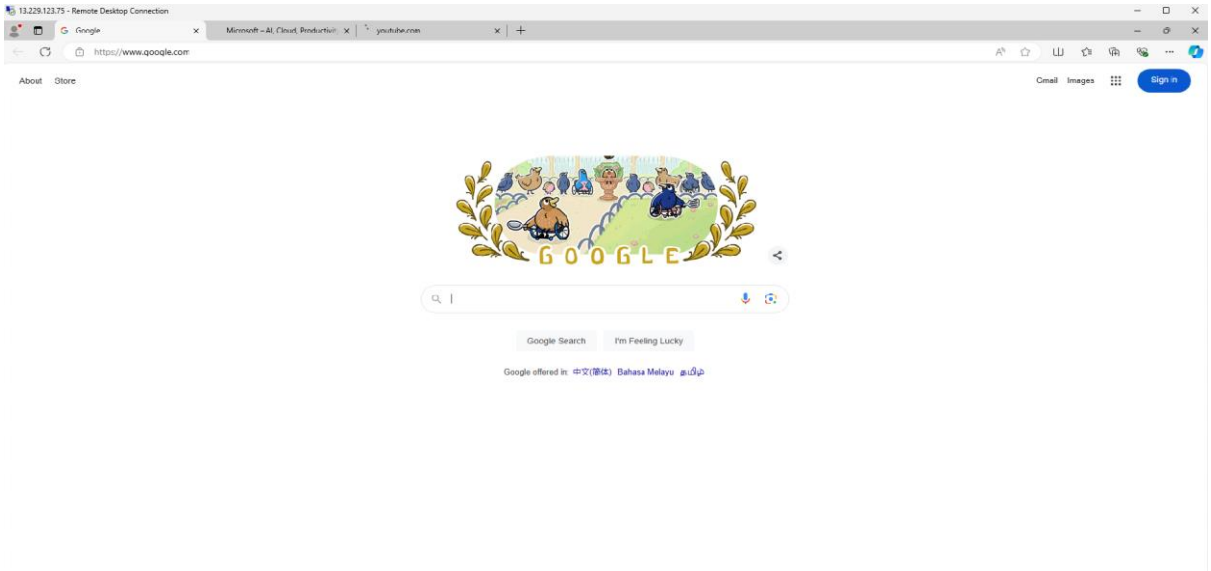




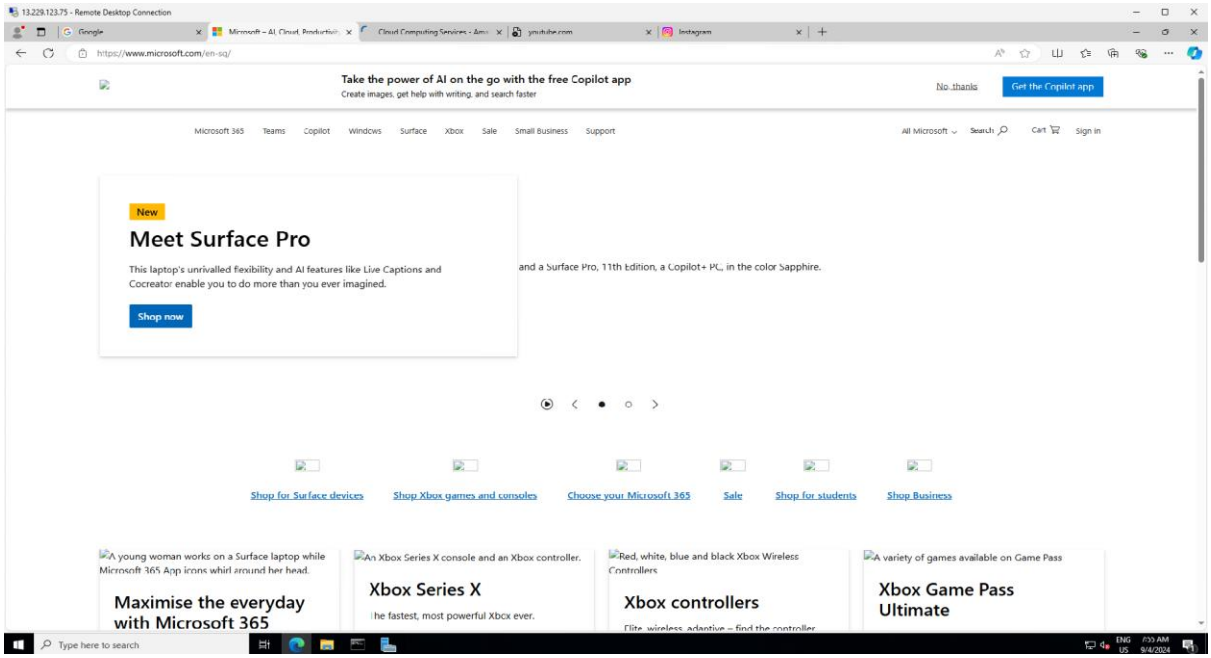
40. Finally, go to your public route table, in the route we'd added the route for the internet gateway, but now we will change it to the gateway load balancer. As you can see below.

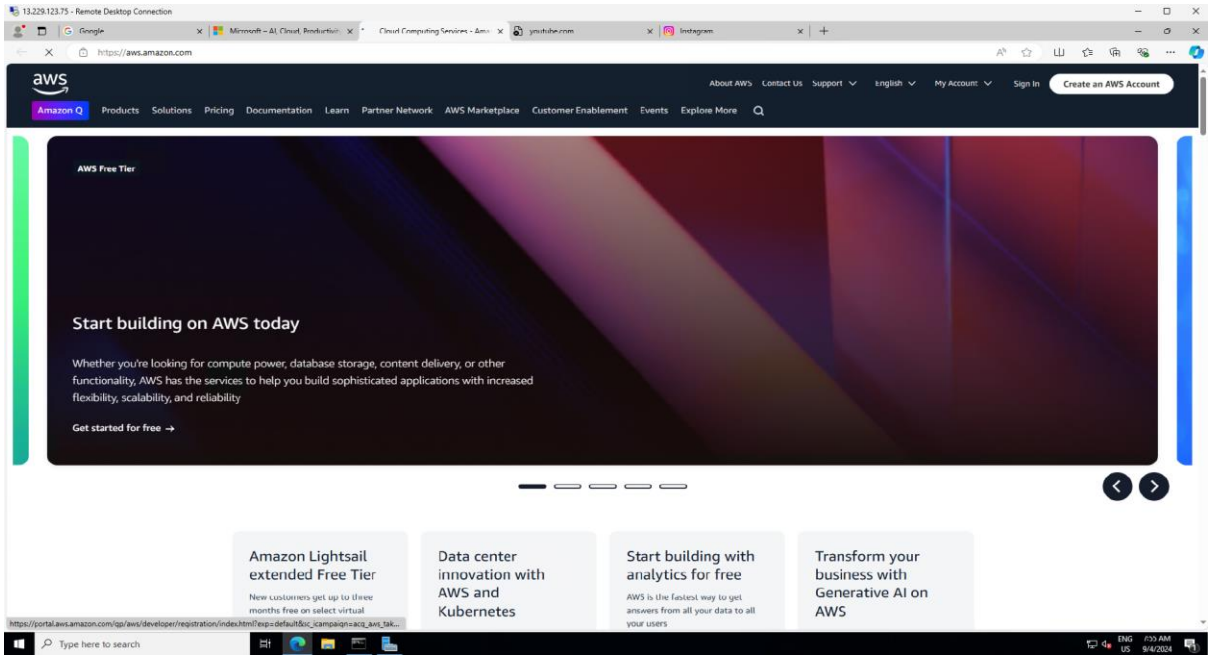


41. After all this connect with your instance again and open your browser in it. Then try to reach google.com you will see that you can reach it.

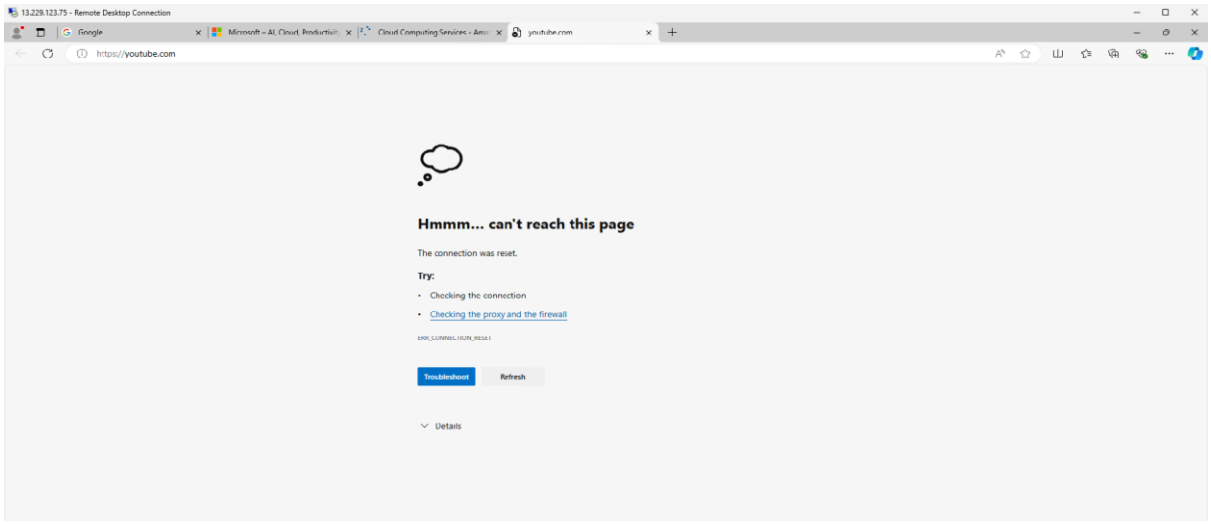


42. It goes the same for Microsoft.com and aws.amazon.com.

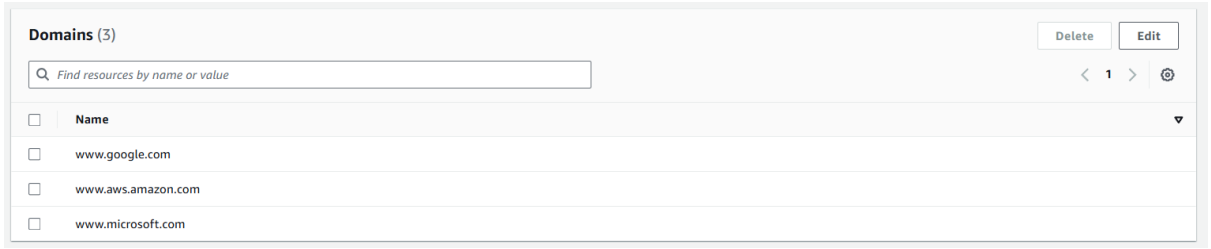




43. But if you try to reach any other website other then these three. For example, youtube.com, you will get an error message for this.

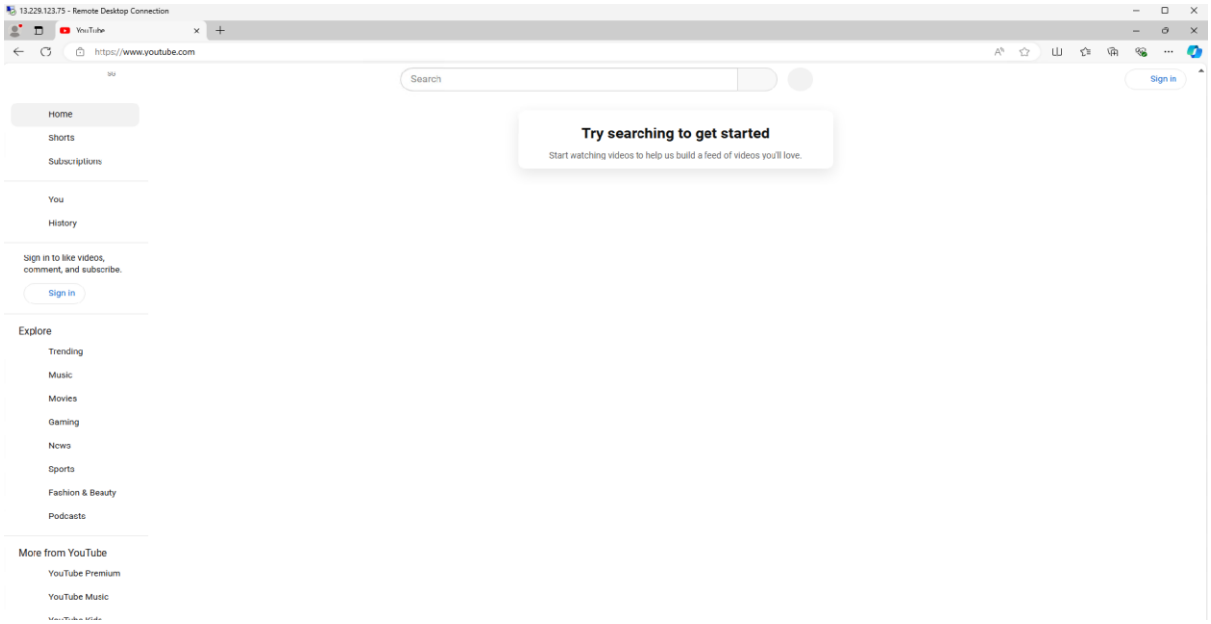


44. Now comeback to your VPC and navigate to firewall rule groups and open your stateful rule group. In the domains section click on edit.



45. In the domain list add youtube.com and click on save. Then go back to your instance and refresh the page for YouTube.

46. You will see that you can reach the youtube.com now.



47. Once you are done delete all your resources.

First, you need to delete the gate load balancer routes from the route table. Then delete your firewall, firewall policy, and firewall rule groups. Terminate your instance. Delete your VPC (Optional)