**😊 Amazon Network Firewall**

In AWS, you can set up a network firewall using various services and tools provided by the platform. Here's a basic overview of how you can achieve this:

1. **Security Groups:** Security groups act as a basic form of network firewall in AWS. You can associate security groups with your EC2 instances, RDS instances, or other AWS resources to control inbound and outbound traffic. They operate at the instance level, allowing you to specify rules for traffic based on protocols, ports, and IP addresses.
2. **Network Access Control Lists (NACLs):** NACLs are another layer of defense in AWS. They operate at the subnet level and allow you to create rules that control traffic at the network level. NACLs are stateless, meaning that you need to define both inbound and outbound rules separately. They can be used to allow or deny traffic based on IP addresses, ports, and protocols.
3. **AWS WAF (Web Application Firewall):** AWS WAF helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. It lets you define customizable web security rules to filter and monitor HTTP and HTTPS requests before they reach your web applications.
4. **AWS Firewall Manager:** AWS Firewall Manager makes it easy to centrally configure and manage AWS WAF rules across all your AWS accounts and applications. It allows you to define firewall rules at the organization level and enforce them across multiple accounts and resources.
5. **Third-party Firewalls:** AWS Marketplace offers various third-party firewall solutions that you can deploy in your AWS environment. These solutions provide advanced firewall capabilities and often integrate with AWS services for better security and management.

When setting up a network firewall in AWS, it's essential to understand your security requirements and choose the appropriate combination of these tools and services to ensure comprehensive protection for your applications and data. Additionally, regularly reviewing and updating your firewall rules is crucial to adapt to evolving security threats and maintain a secure environment.

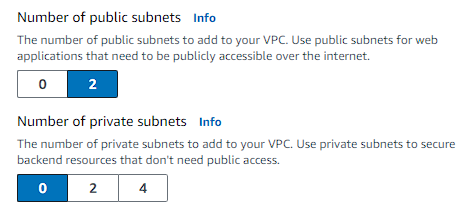
**😄 Use cases of Amazon Network Firewall:**

Amazon Network Firewall provides several use cases to enhance network security in AWS:

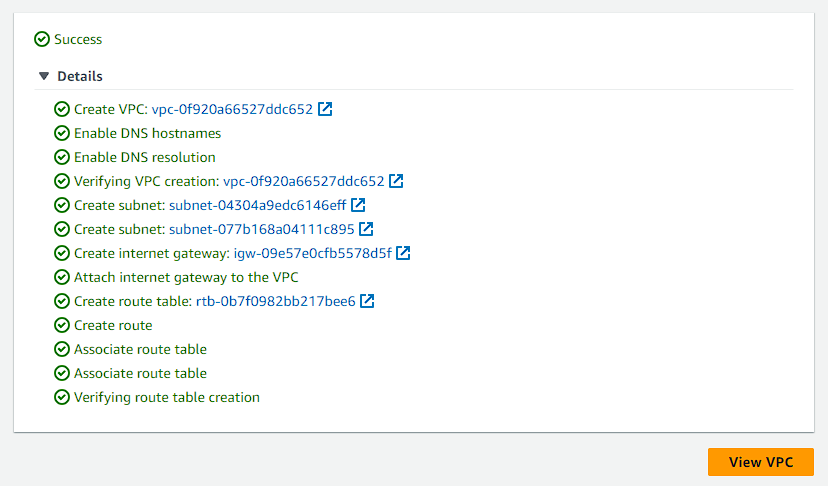
1. **Traffic Inspection and Filtering:** Amazon Network Firewall allows you to inspect and filter both inbound and outbound traffic at the network level. You can define rules based on protocols, ports, and IP addresses to allow or deny traffic, helping to enforce security policies and prevent unauthorized access to your applications and resources.
2. **Protection Against DDoS Attacks:** Network Firewall helps protect your AWS infrastructure from Distributed Denial of Service (DDoS) attacks by filtering and mitigating malicious traffic before it reaches your applications. It can detect and block suspicious traffic patterns associated with DDoS attacks, helping to maintain application availability and performance.
3. **Deep Packet Inspection:** Amazon Network Firewall supports deep packet inspection (DPI), allowing you to inspect the contents of network packets for malicious payloads or unauthorized activities. DPI enables you to identify and block threats such as malware, command-and-control traffic, and data exfiltration attempts, providing an additional layer of defense for your network.
4. **Application Layer Filtering:** Network Firewall allows you to apply advanced filtering rules at the application layer, such as inspecting HTTP headers or payloads for specific patterns or signatures. This enables you to enforce security controls tailored to the requirements of your applications, such as blocking SQL injection attacks or cross-site scripting (XSS) attempts.
5. **Integration with AWS Services:** Amazon Network Firewall integrates seamlessly with other AWS services, such as Amazon VPC, AWS WAF, AWS CloudFormation, and AWS Transit Gateway. This integration allows you to automate the deployment and management of network security policies across your AWS environment, improving operational efficiency and consistency.
6. **Centralized Management and Monitoring:** Network Firewall provides centralized management and monitoring capabilities through the AWS Management Console, AWS CLI, and AWS CloudWatch. You can view real-time logs and metrics, monitor traffic patterns, and gain insights into security events across your network, helping to identify and respond to security threats more effectively.

**😄 To begin with the Lab:**

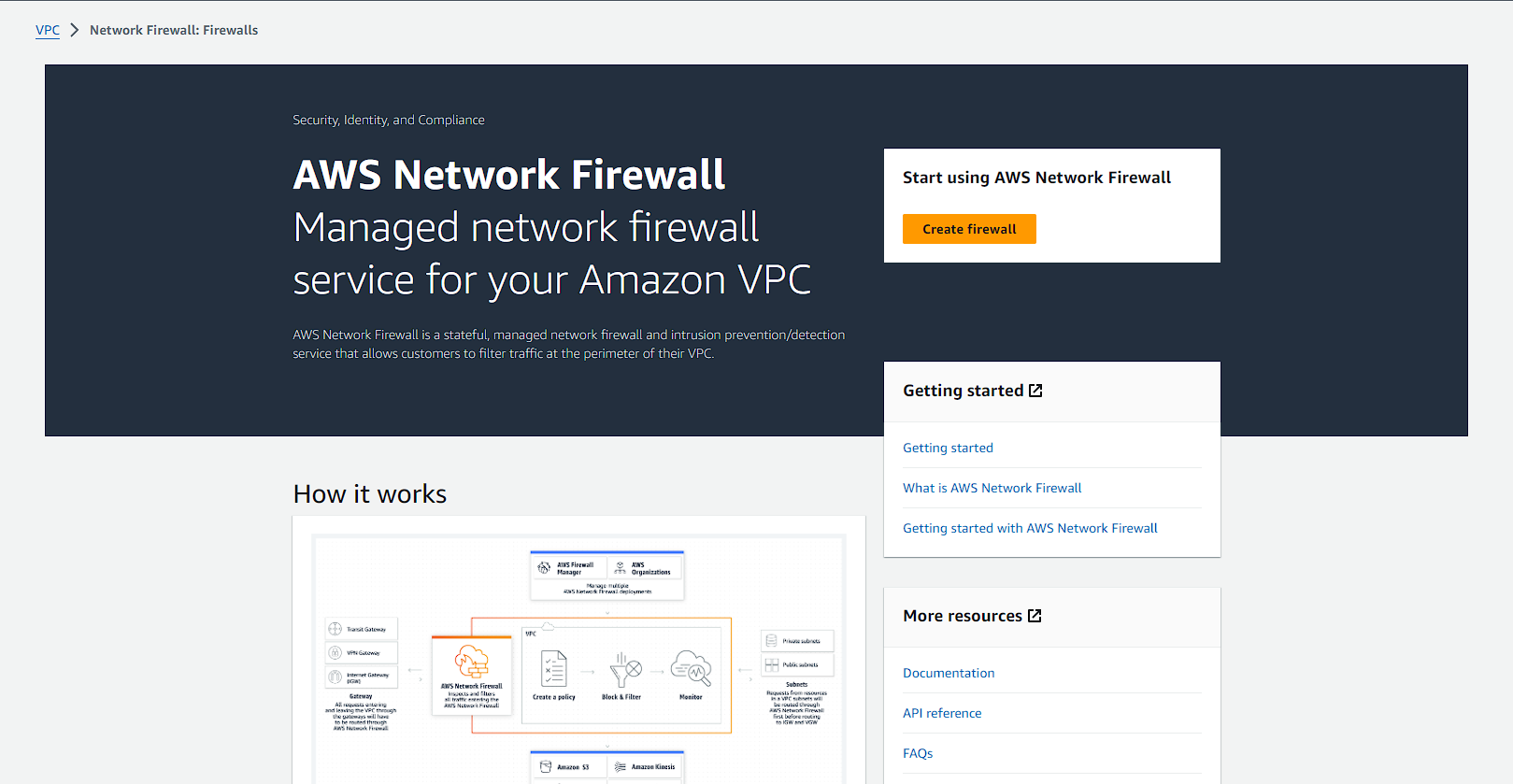
1. Log in to AWS Console and navigate to VPC.
2. There you are going to create a VPC for that select VPC and more option. Using this option, you can create a VPC quickly.
3. Now you have to select 0 (zero) private subnets, 2 public subnets and no need for NAT gateway or VPC endpoint.



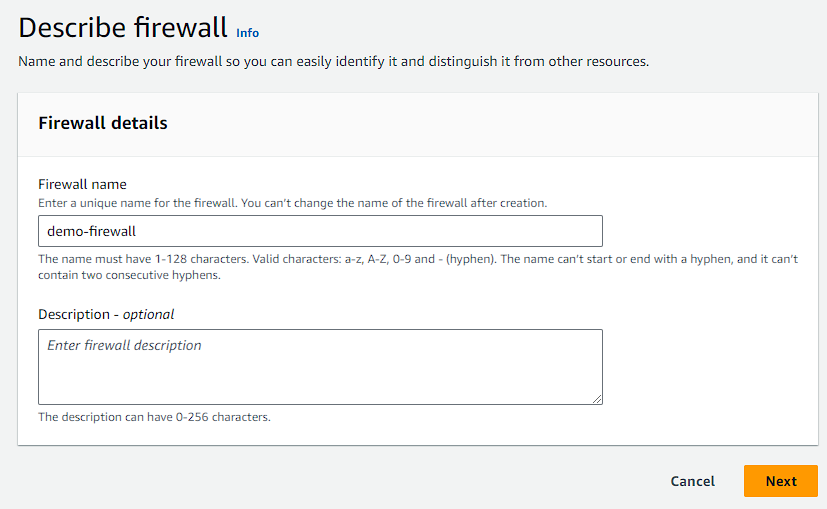
1. Then just create your VPC.



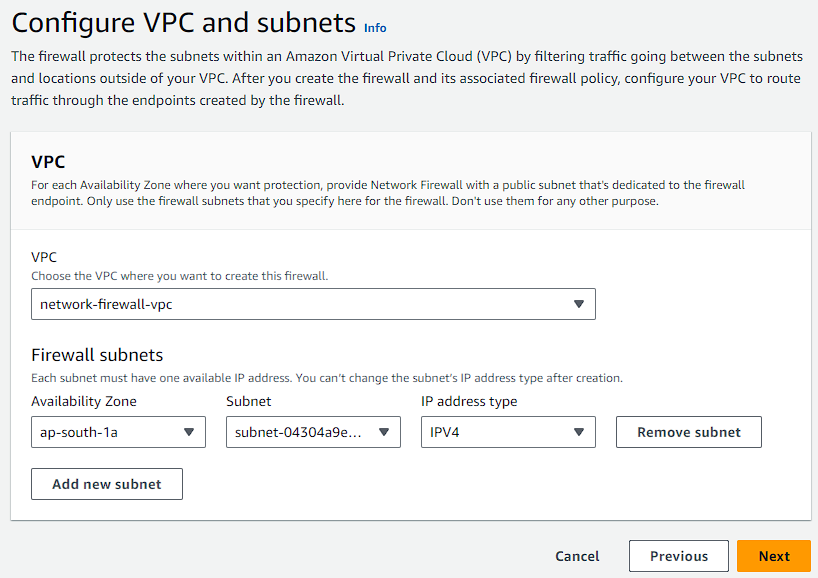
1. Now from the left pane if you scroll down a little you will see the options for Network Firewall. From there navigate to Firewalls. Click on create.



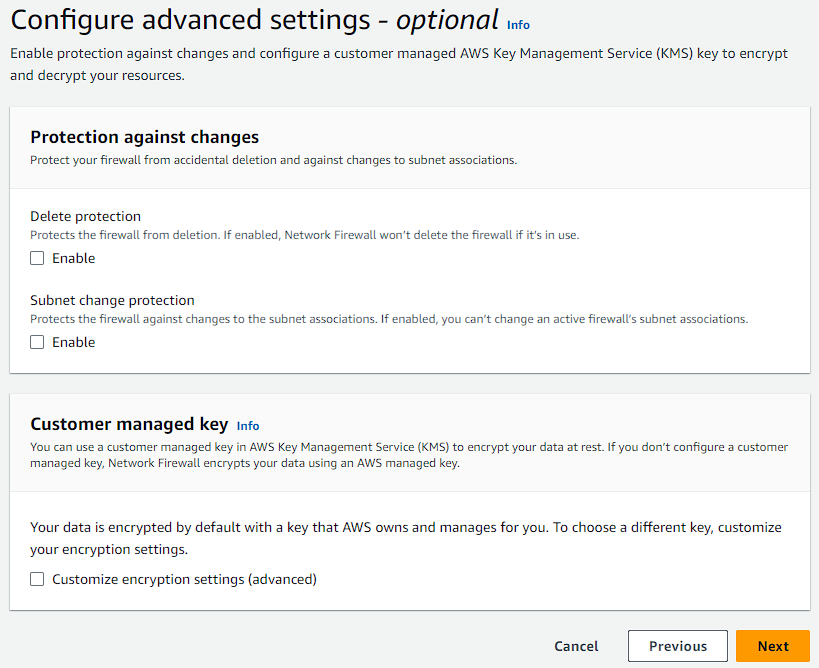
1. Now you have to give it a name and move forward.



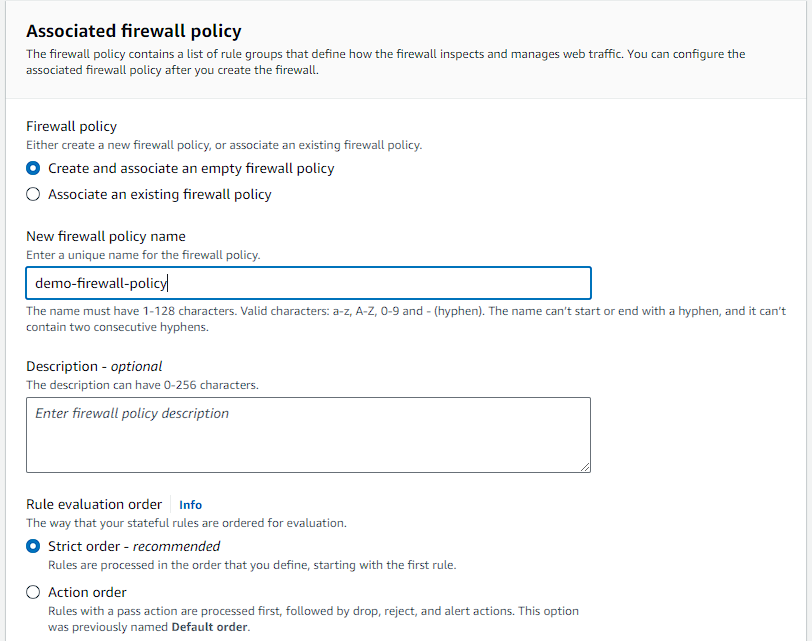
1. Then choose your newly created VPC, availability zone and subnet. In the last choose IP address and move to next page.



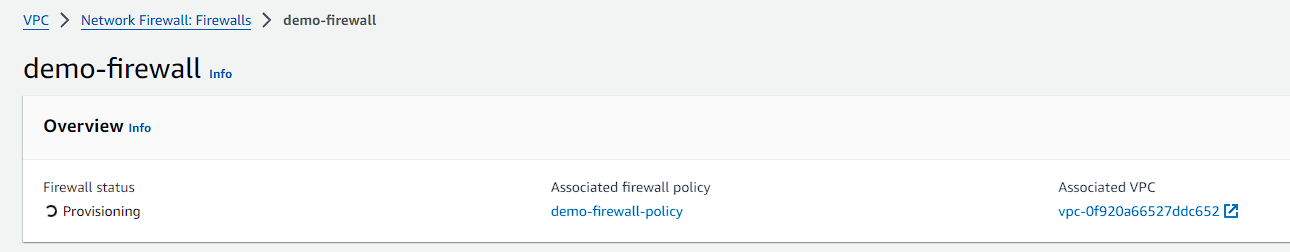
1. In the next step deselect delete protection and subnet change protection. We don’t need it for this demo. Then move to next page.



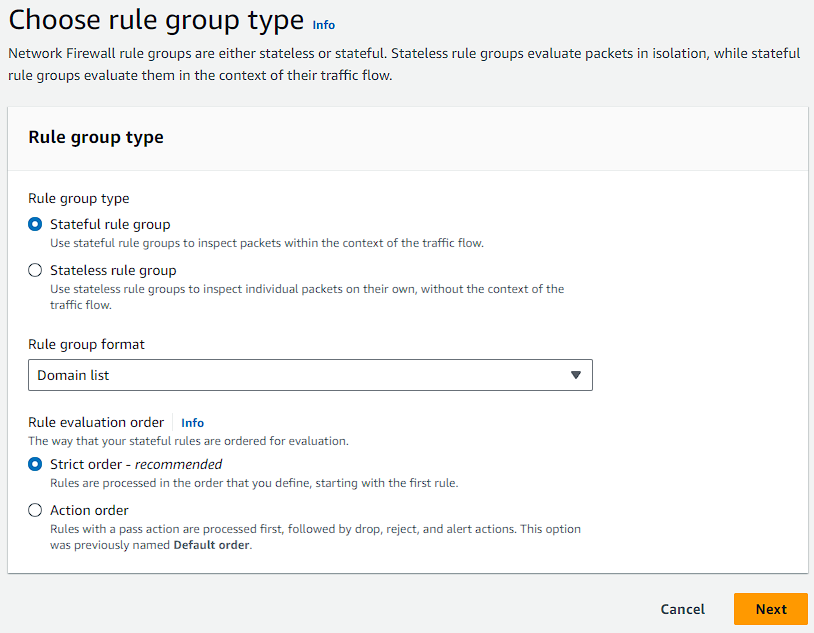
1. Now for the firewall policy choose the options below and give it a name then move to review page and create your firewall.



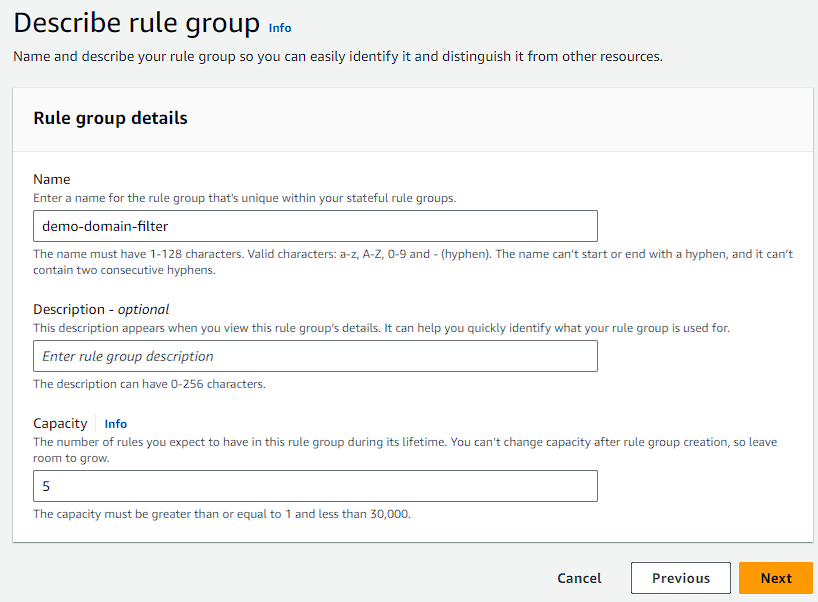
1. Currently you firewall will in provisioning state. As it takes some time for it get ready.



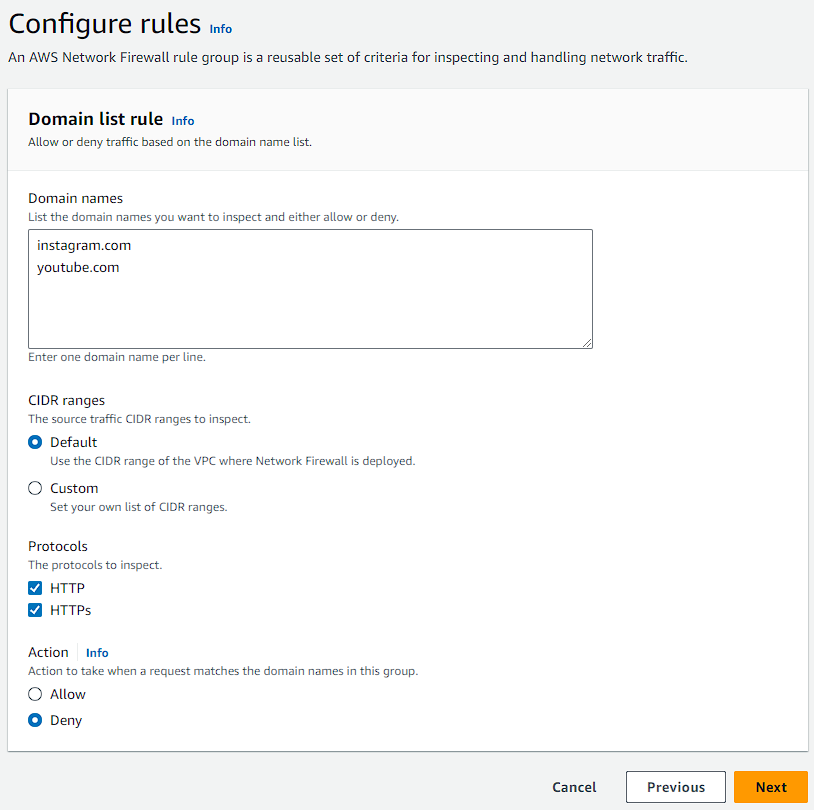
1. Since, it is in the provisioning state you can go ahead and create a rule group. For that go to the **network firewall rule group** option from the left pane and click on create.
2. There you need to select which type of rule group you want. Select stateful rule group and the format should be domain list and then click on next.



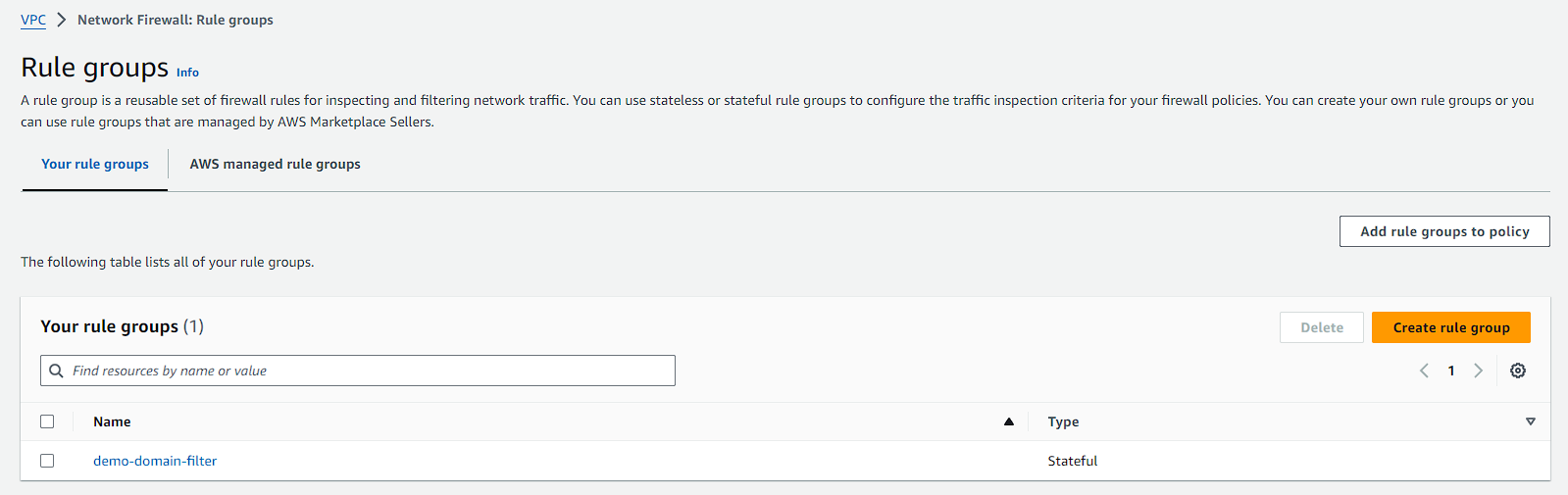
1. On the next page give it a name and select capacity to 5.



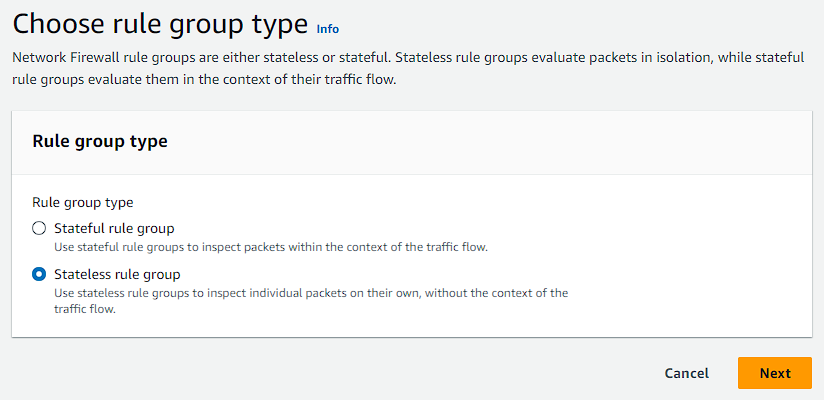
1. Then you are going to write the domain names of your choice and you can also decide what type action do you want whether you want to deny or allow the traffic towards it.
2. After just create your stateful rule group.



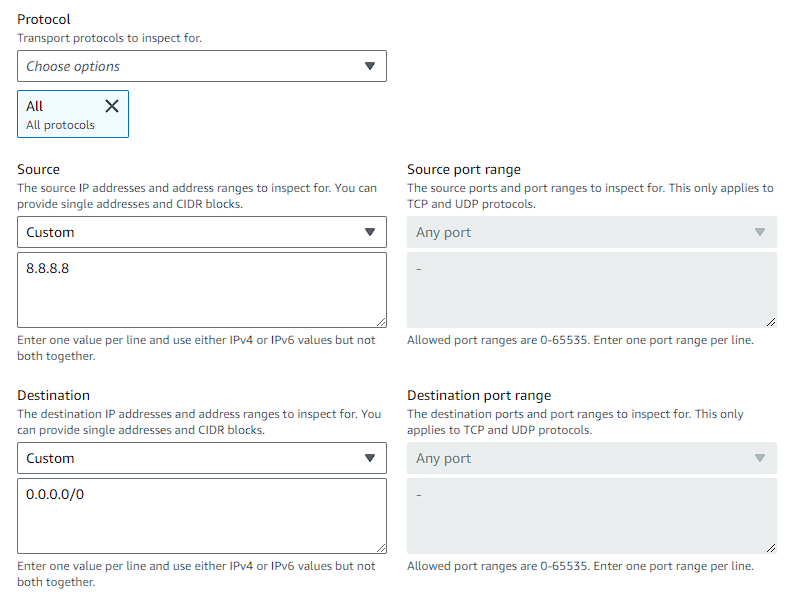
1. Here you can see that your rule group is now created.



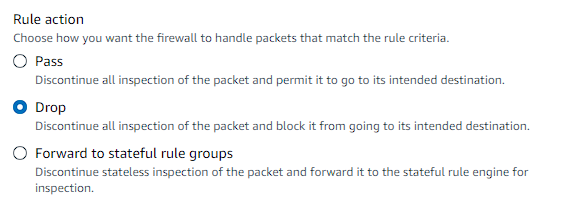
1. After that you are going to create another rule group which will be stateless.



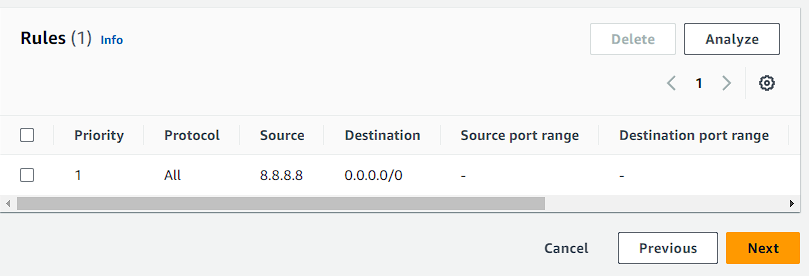
1. Now the steps are the same as before. Give it a name choose the capacity to 5 and move to next page.
2. On the next page or next step keep priority to default and for protocols choose all as default because there are so many protocols.
3. Then in the source and destination you can define the IPs shown below.



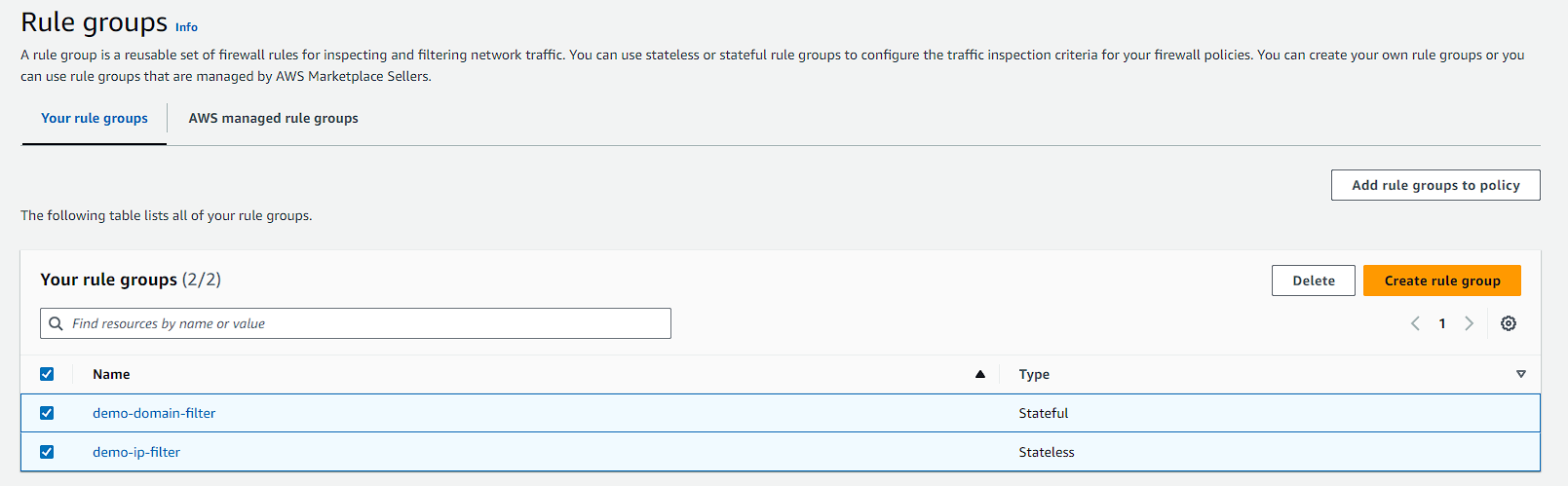
1. After that choose the rule action for drop and click on add rule.



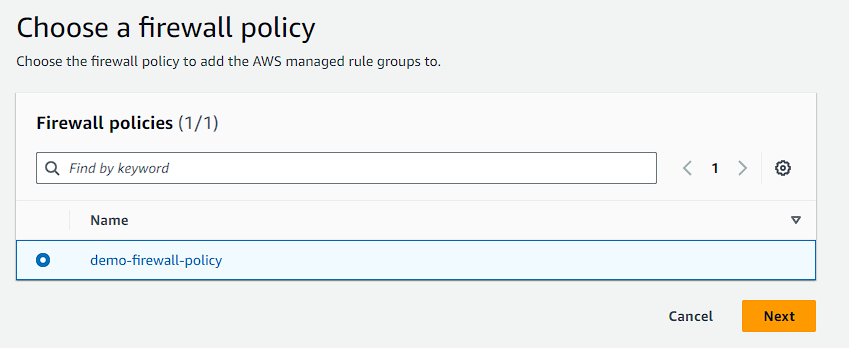
1. Then you will see this at the bottom of that page. Click on the next move to the review page and create your rule group.



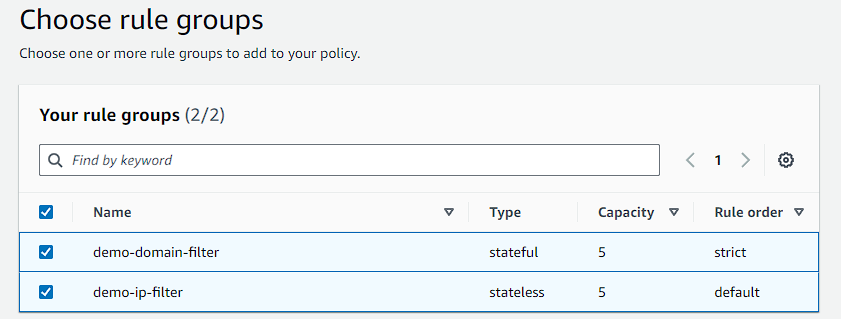
1. Now you have to add these you two rule groups to a firewall wall policy. For that you are going to select both of your rules and click on add rule groups to policy.



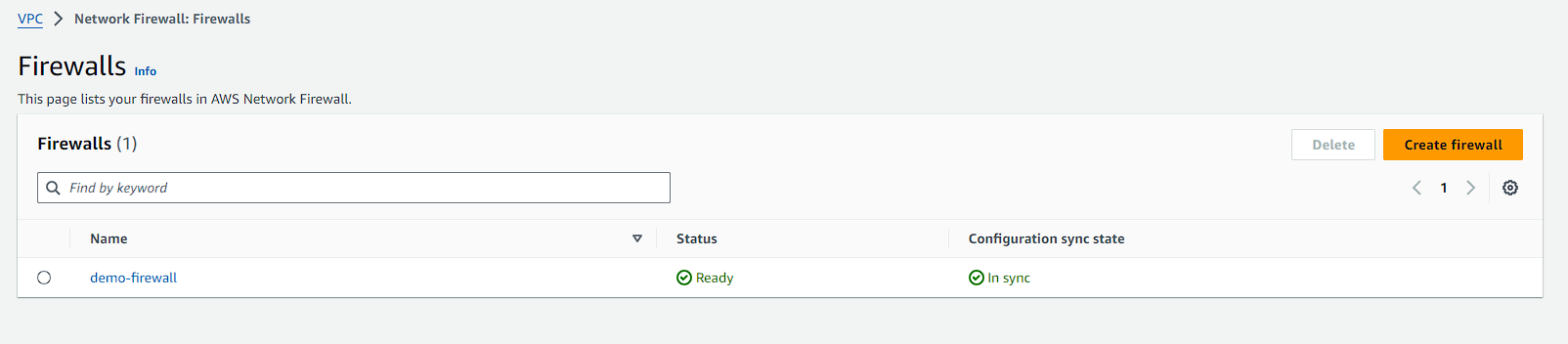
1. After that you will see a policy select it and click on next.



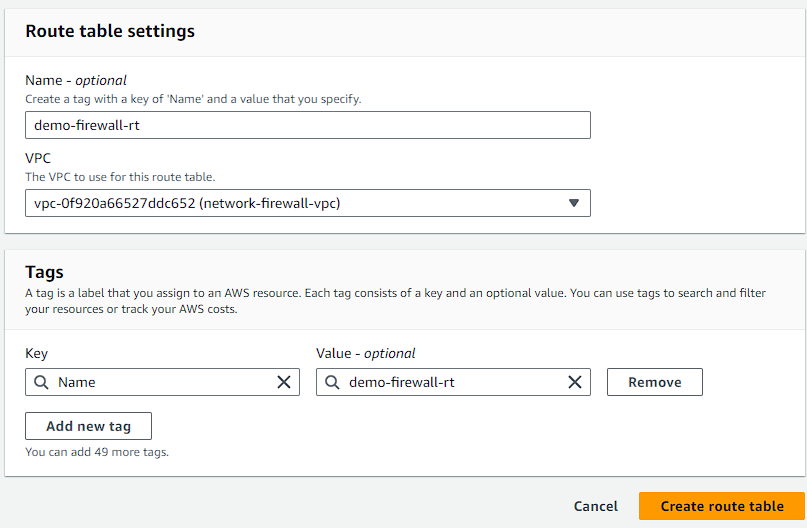
1. Then you have to select your rule groups. On this page you will many other rule groups just leave them and move to next page which is your review page and add your rule groups to your policy.



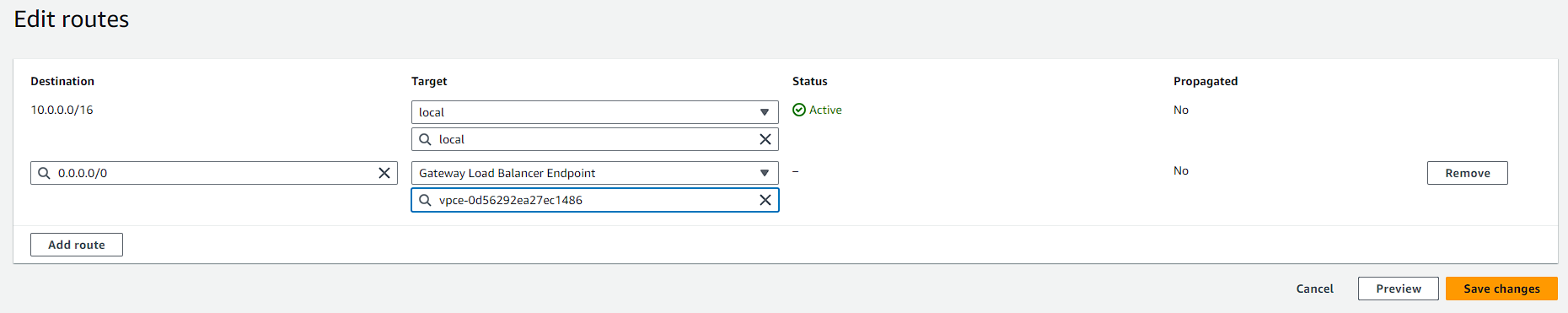
1. Now if you’ll go back to firewall, you will see that it is ready. Open it and you will see the details regarding your firewall.



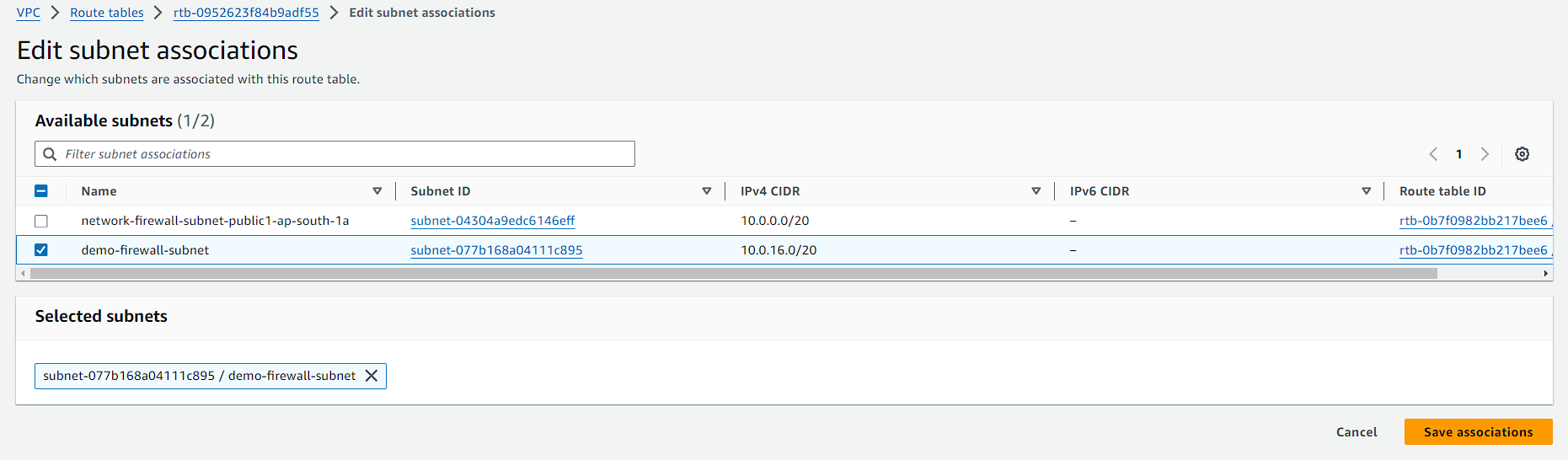
1. One thing that you have to remember is the subnet your firewall is associated with.
2. Now go to subnets and change the subnet name which is not associated to the firewall because you will use that subnet to launch your EC2 instance. Once it is done move to the route table.
3. Now you are going to create a new route table using the new VPC.



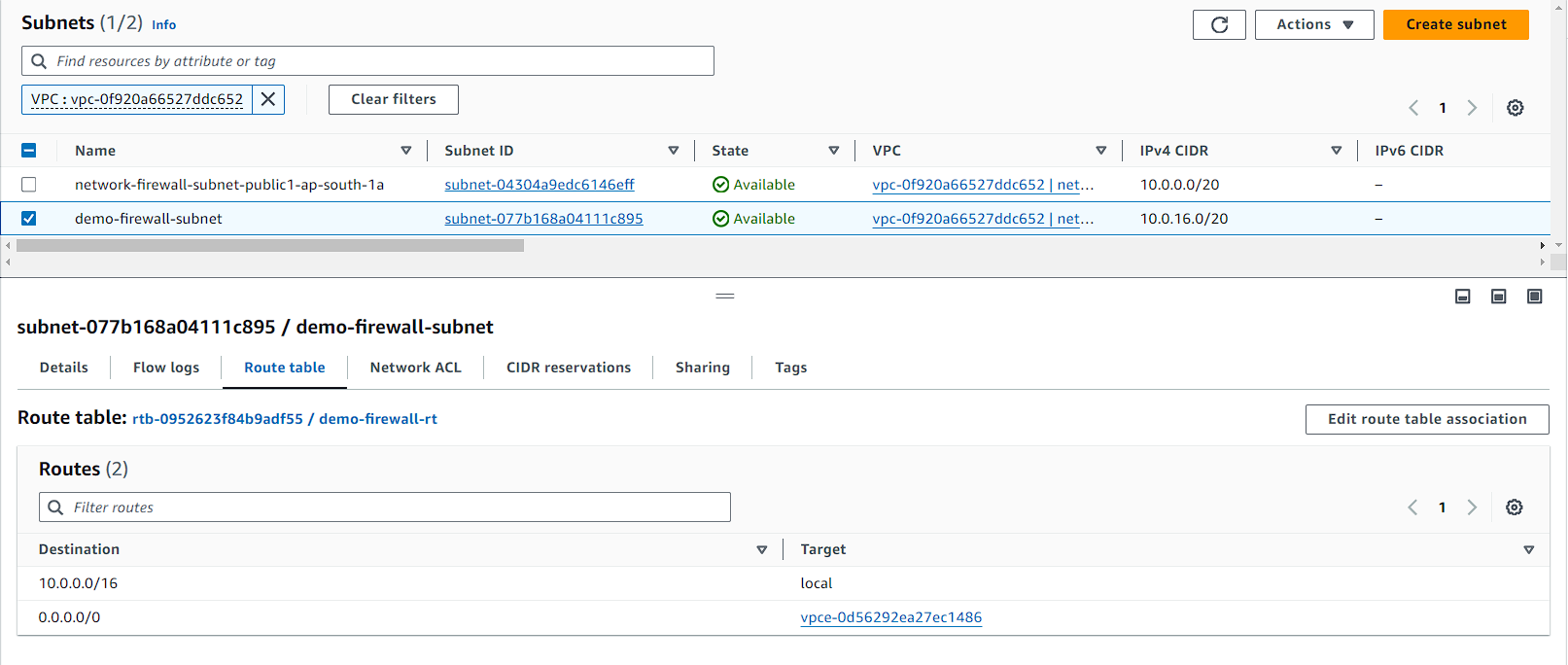
1. Now you are going to edit the routes. Let's add a new road towards the Internet and it should go towards the endpoint, which is your VPC endpoint and click on save changes.



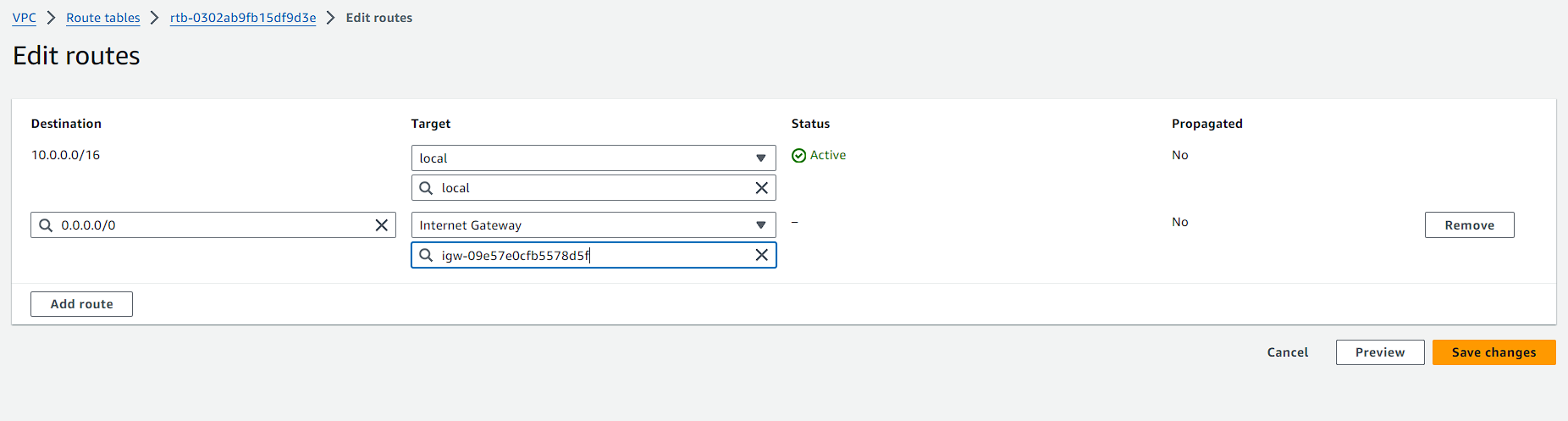
1. Then you are going to associate it with your subnet whose name you changed earlier. This subnet will be used for EC2.



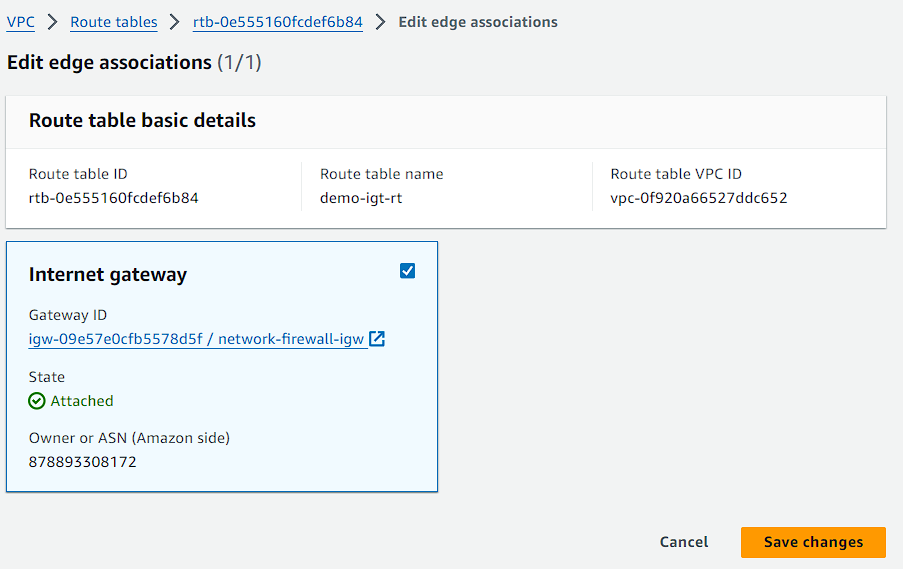
1. Then quickly verify your subnet there are two routes, one towards the local and the second towards the VPC endpoint.



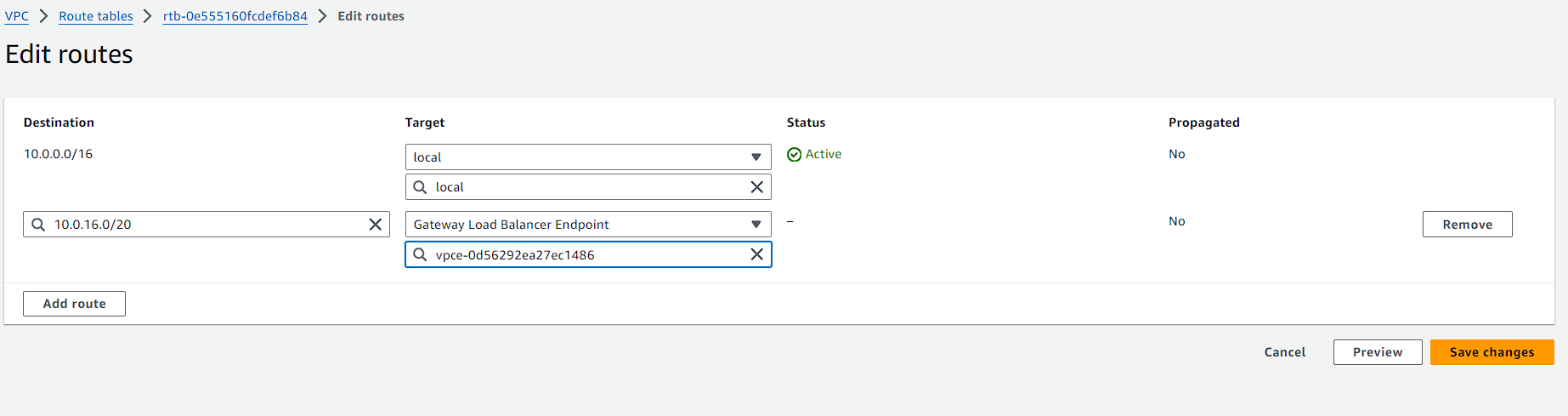
1. Once it is completed, now you are going to create a new route table for your firewall.
2. Now again you are going to edit the routes and this time you have to add the route toward the internet gateway.



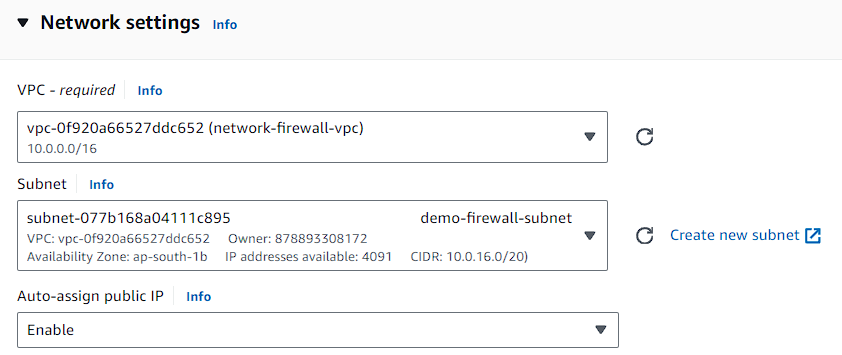
1. Now the third route is associated with the Internet gateway. So, you can use the Edge Association where any traffic going towards the customer subnet needs to go towards the VPC endpoint.
2. Again, you are going to create route table. Once your route table is created, this time you are going to use the edge association. Associate it with the internet gateway and click on save changes.



1. After that come back to routes and add a route for CIDR of subnet which you will use to launch EC2. Copy that here and the target will be your VPC endpoint. Click on save changes.



1. Till here your basic setup is completed, now to test things out navigate to EC2 quickly launch an instance in your VPC and choose the subnet that you prepared for it. Then enable the auto-assign public IP and launch your instance.



1. Once your instance is launched wait for it to get ready. Until then open the security group assigned to it and add inbound rule for All traffic from everywhere and remove port 22 if you want.