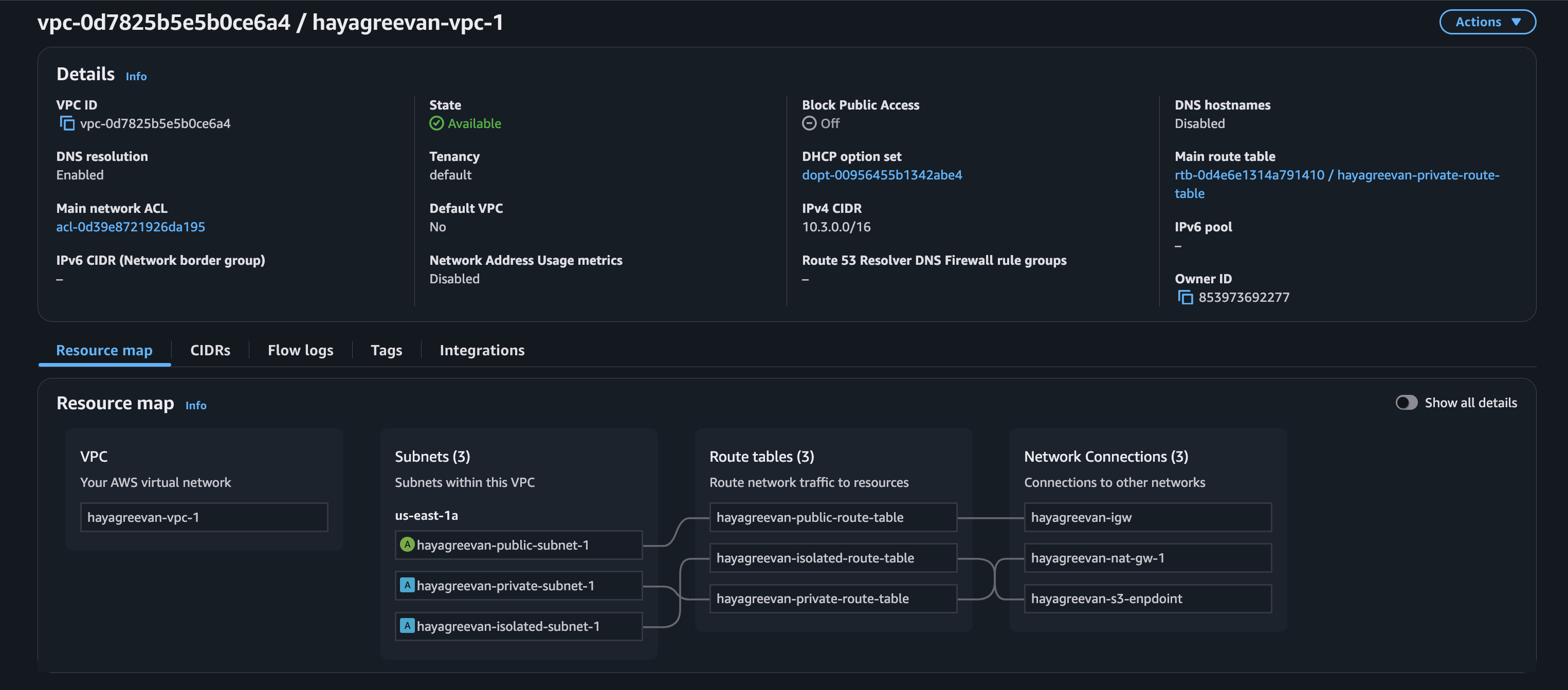
1. You are an AWS Cloud Engineer tasked with designing a secure and scalable network for an e-commerce platform hosted on EC2 instances. The platform requires public, private, and isolated subnets to separate internet-facing resources (e.g., web servers) from internal resources (e.g., application servers) and ensure robust segmentation.

**Requirements**:

* Spin up an Nginx server in private network and download packages via internet in secured way.
* Isolated subnets for internal resources with no direct internet access but secure access to AWS services like S3 via VPC endpoints.

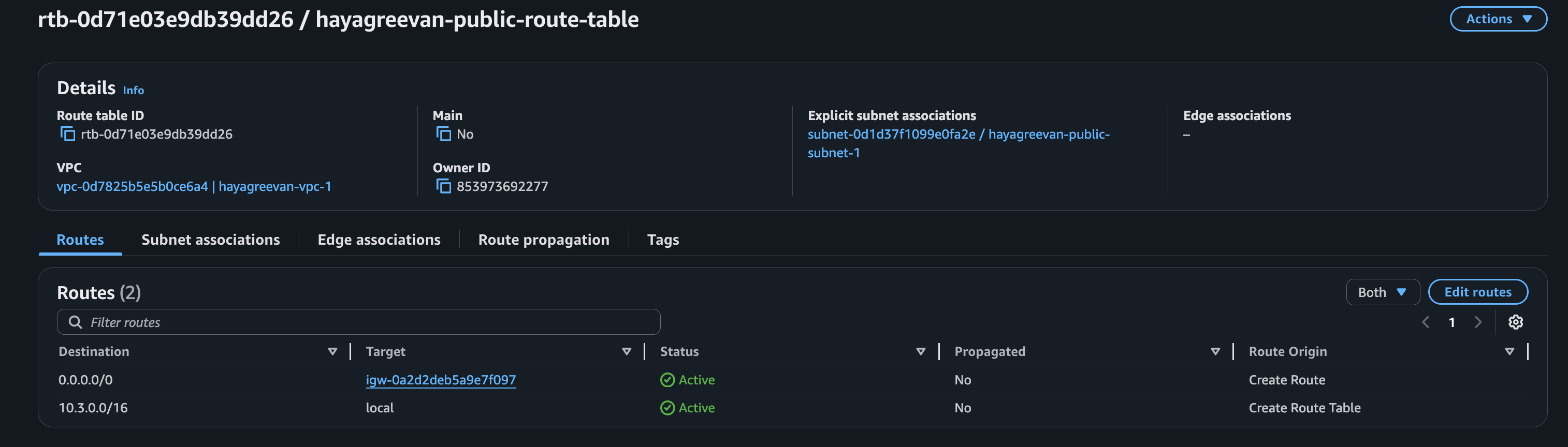
**Questions**:

* Design a VPC with public, private, and isolated subnets to ensure proper segmentation and security.

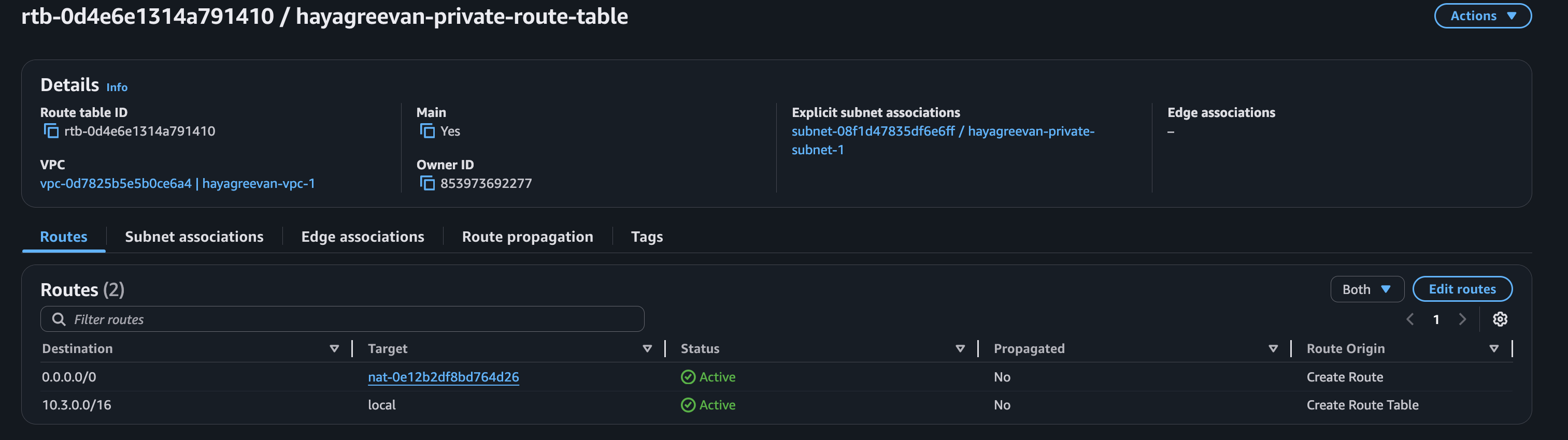


* What routing rules would you configure to provide internet access for public and private subnets while ensuring the isolated subnet remains secure?

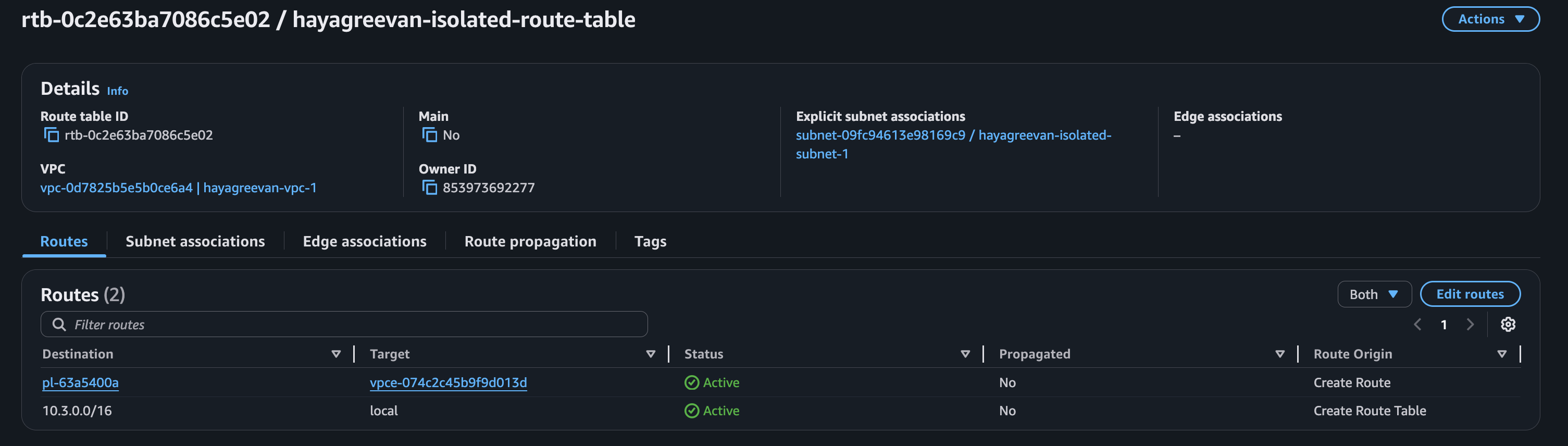
Public :



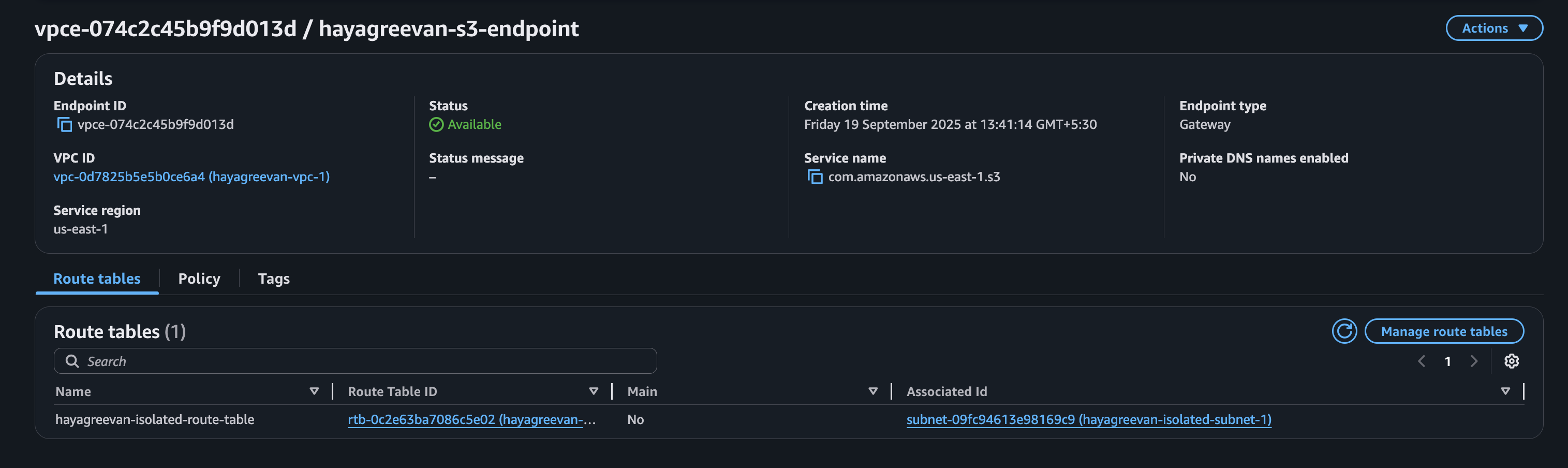
Private :



Isolated :

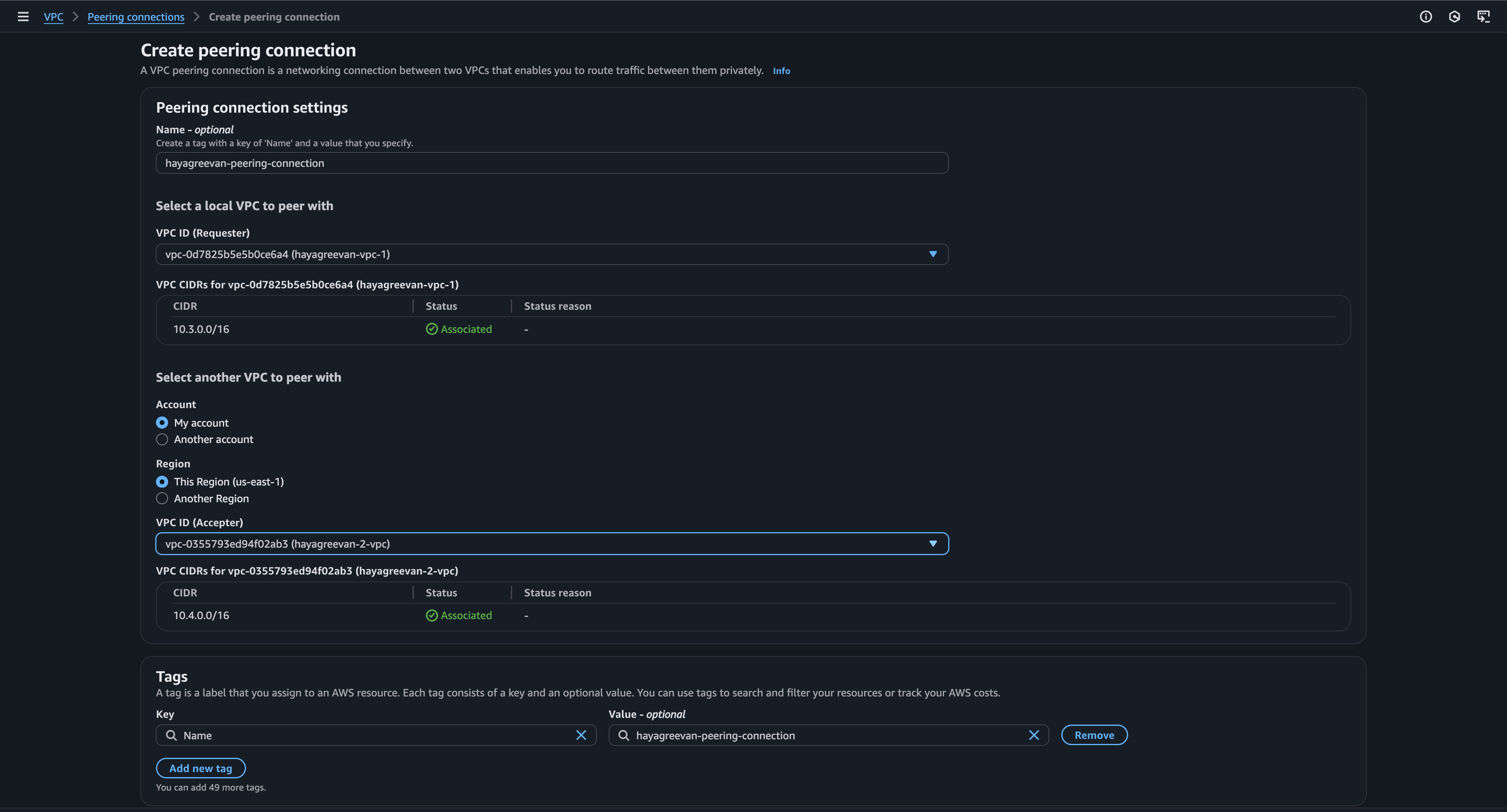


* Enable secure AWS service access for isolated subnets. WebServer 1 from Subnet A should be able to access S3 bucket and download/upload objects to S3.

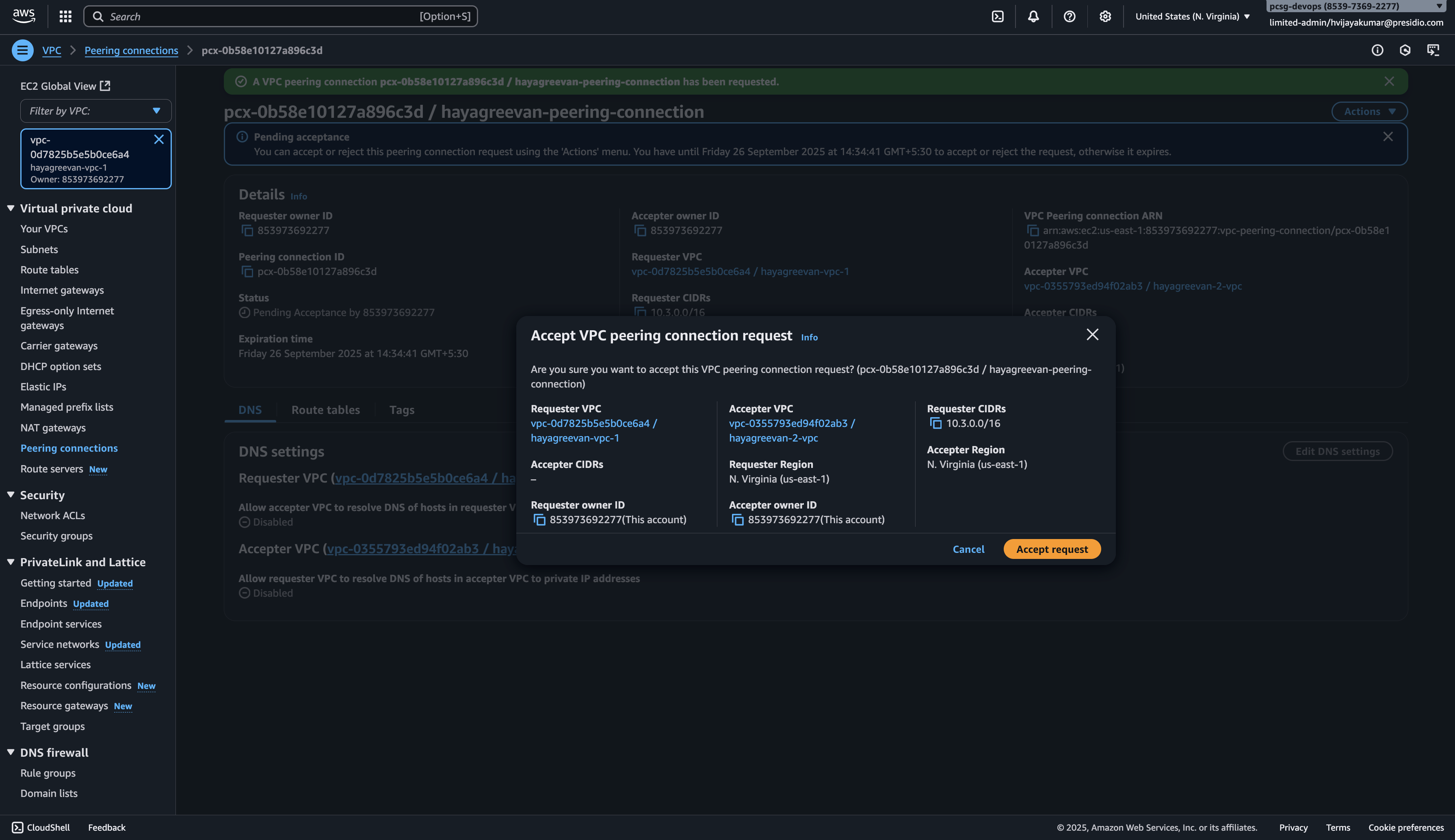


* Deploy VPC A & VPC B and spin up web serves in each VPC. Establish connection from Webserver 1 to Webserver 2.

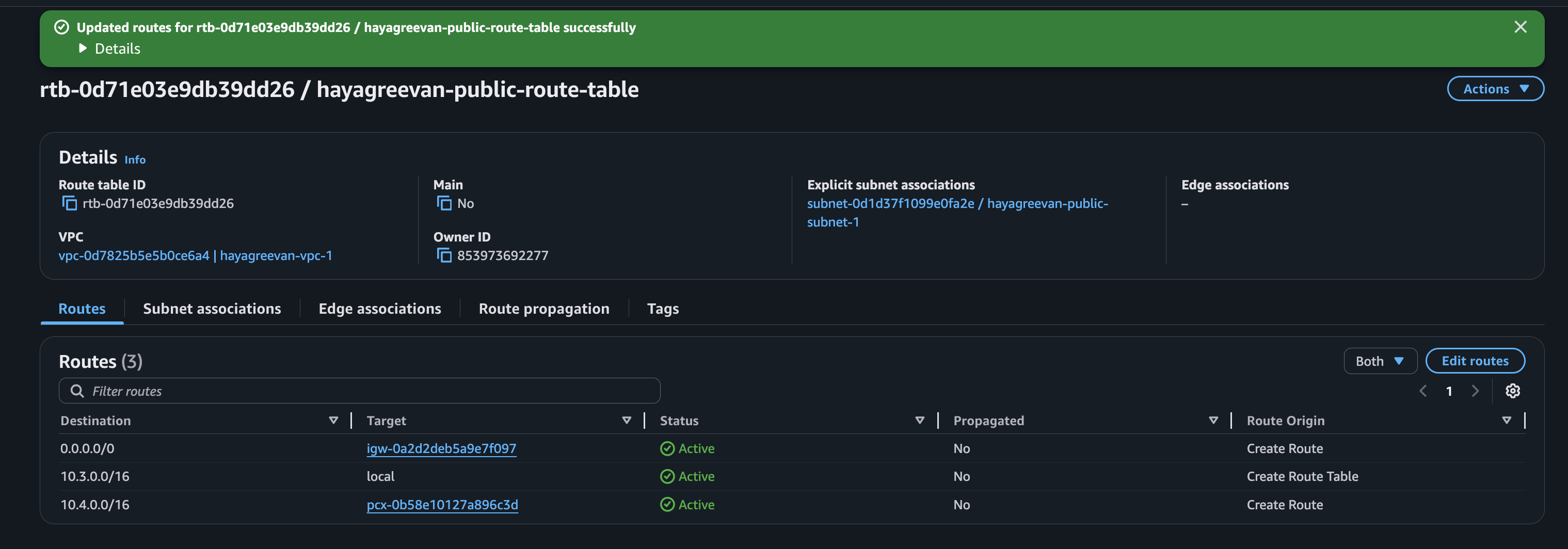
Creating VPC Peer Connection :



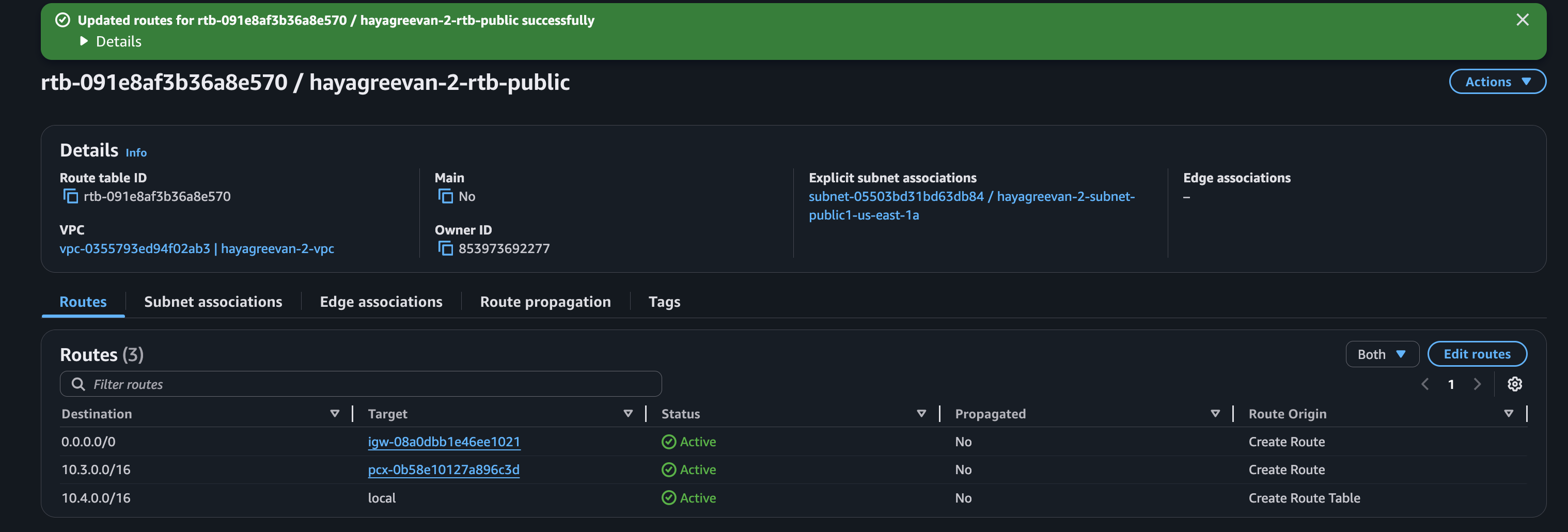
Accepting the VPC Peer Request :



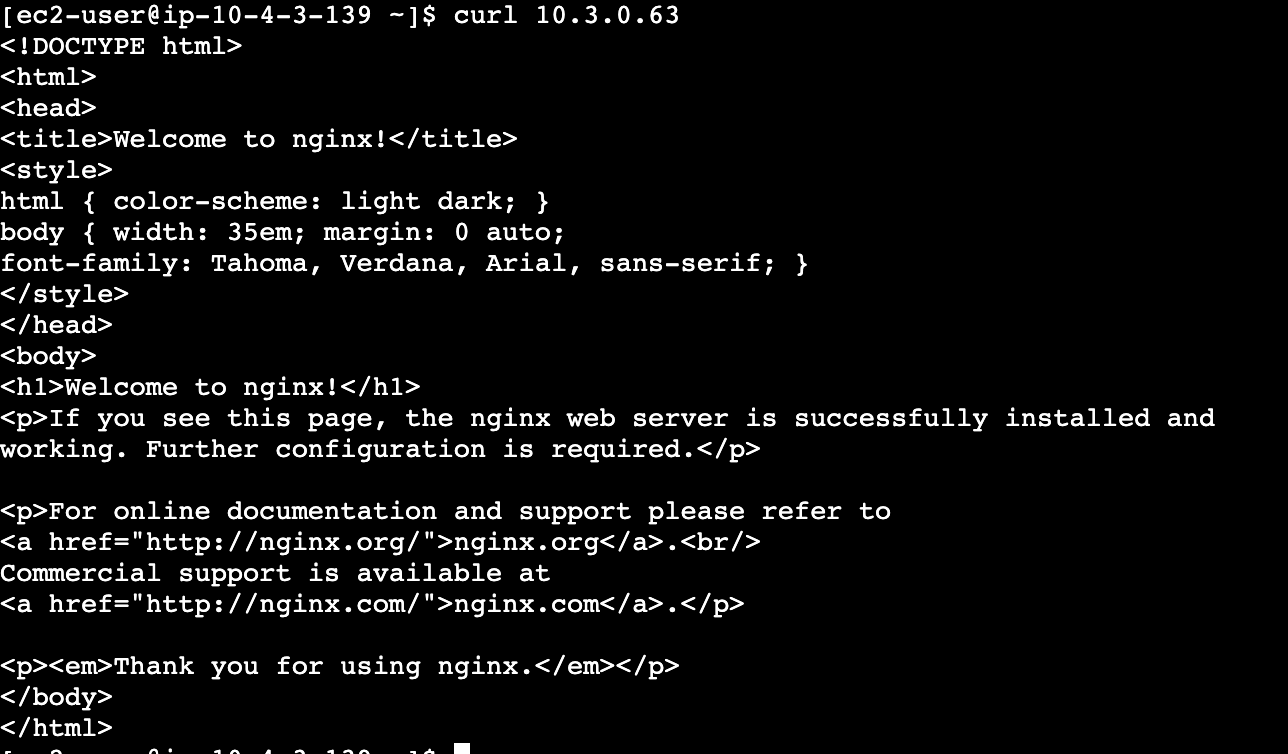
Adding Peer routes in hayagreevan-vpc-1 Public Route Table :



Adding Peer routes in hayagreevan-2-vpc Public Route Table :



Peer Connection Established Successfully :



**Explore and Provide solutions**

* Explore the difference between NAT instance vs Gateways vs Bastion Hosts and come up with solutions when to use those.

Ans :

NAT Instances are EC2 instances with NAT based AMI Images. It relies on Instance type. It acts as Bastion Host. It requires manual setup of Security Group.

NAT Gateway is an AWS Managed Service for NAT with high availability and scalability.

Bastion Host is an EC2 instance which is available in public subnet used to connect to other EC2 instances in private subnet of the VPC which cannot be accessed from internet directly.