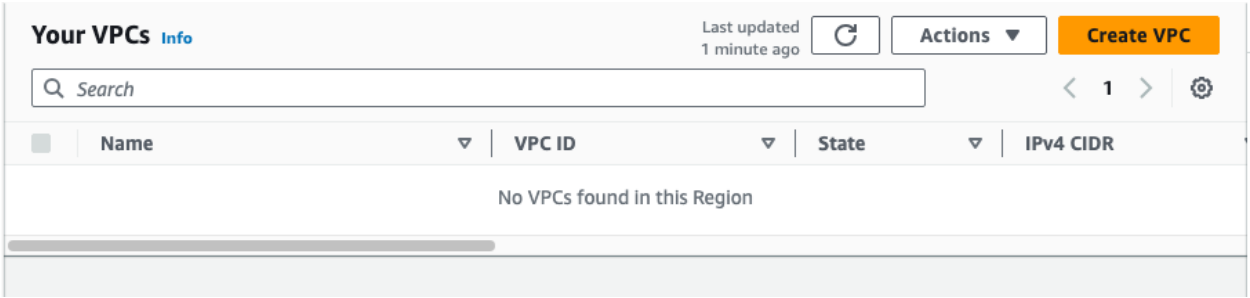
Virtual Private Network & Security Groups

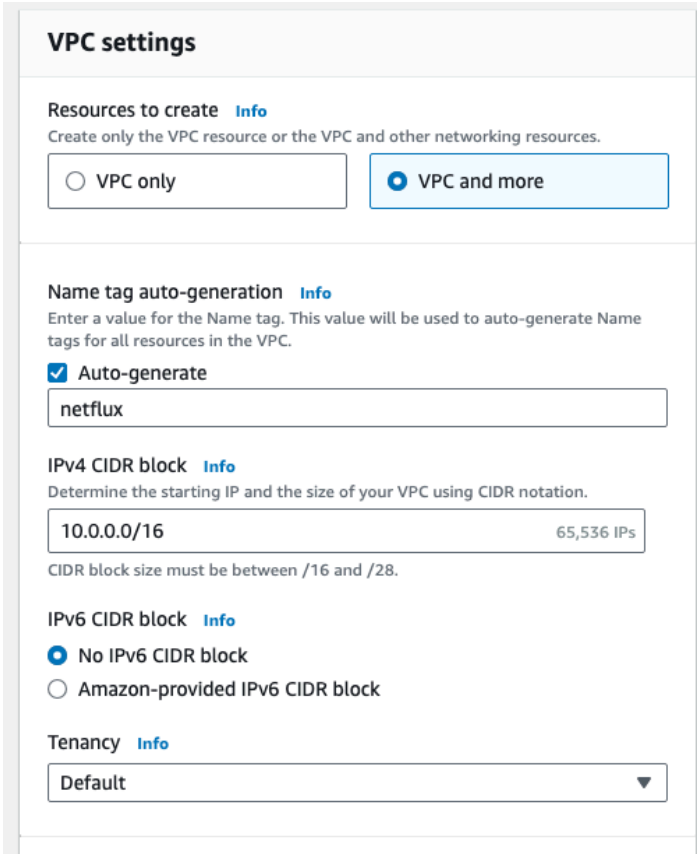
VPC 1
Security Group for ALB 6
Security Group for Application / Backend Microservices 7
Security Group for DB 8

VPC

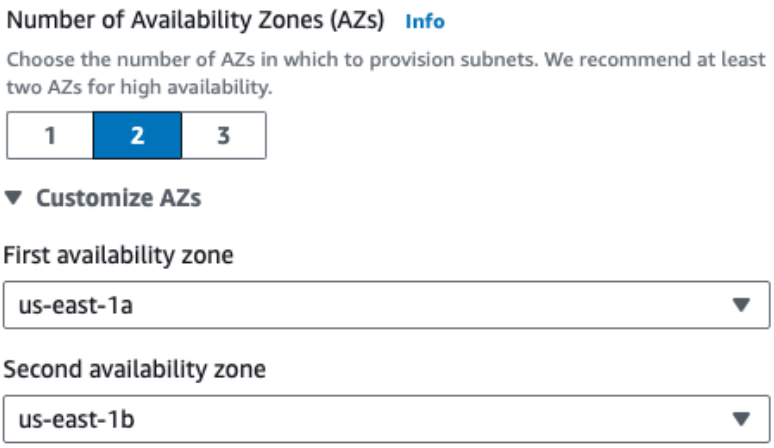
- Delete the default VPC to avoid confusion.
    - No worries, you can always create the default VPC when you need it!
- Let's start from scratch.



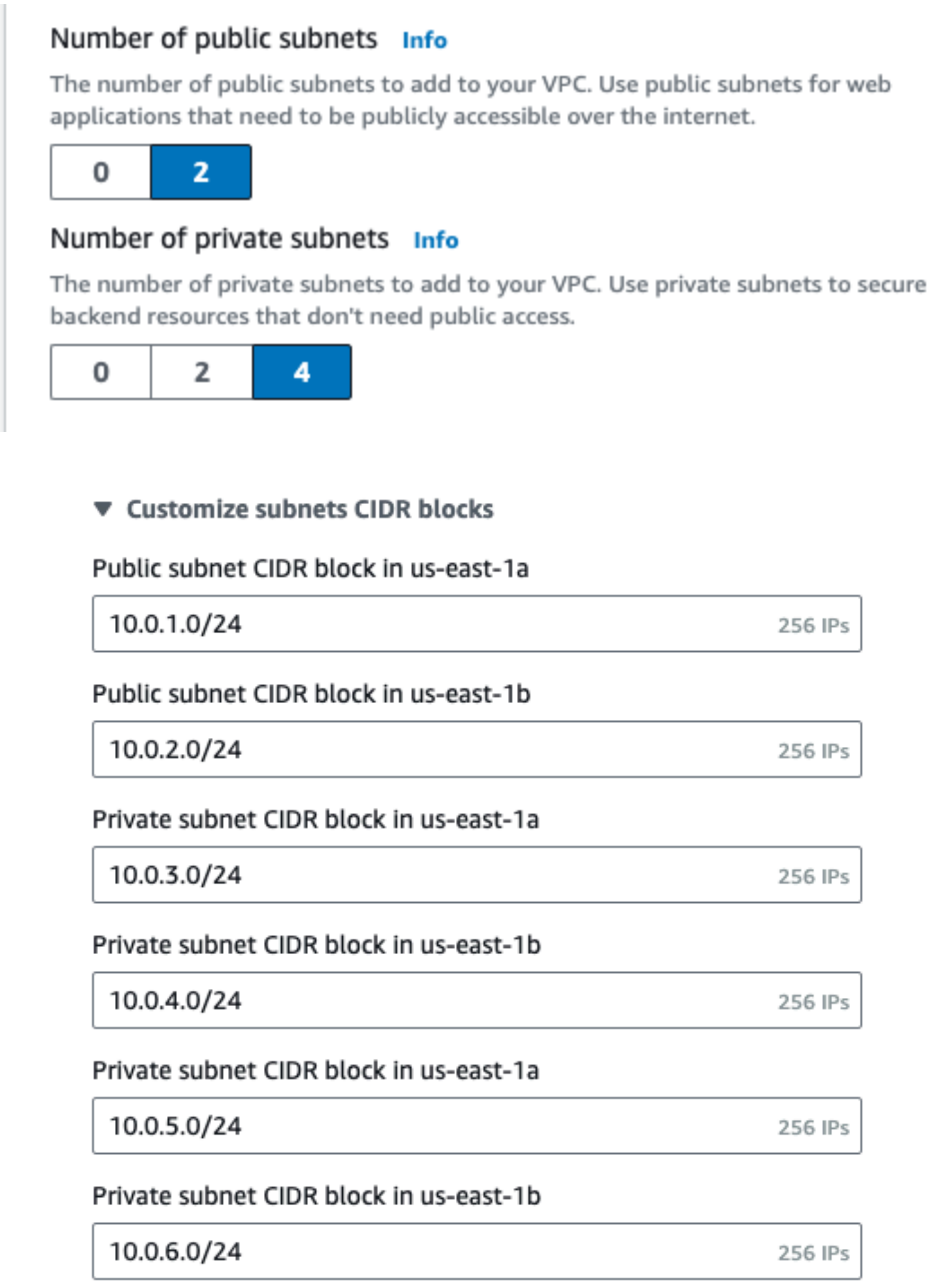
- VPC Settings
    - I give the VPC name as “netflux”.



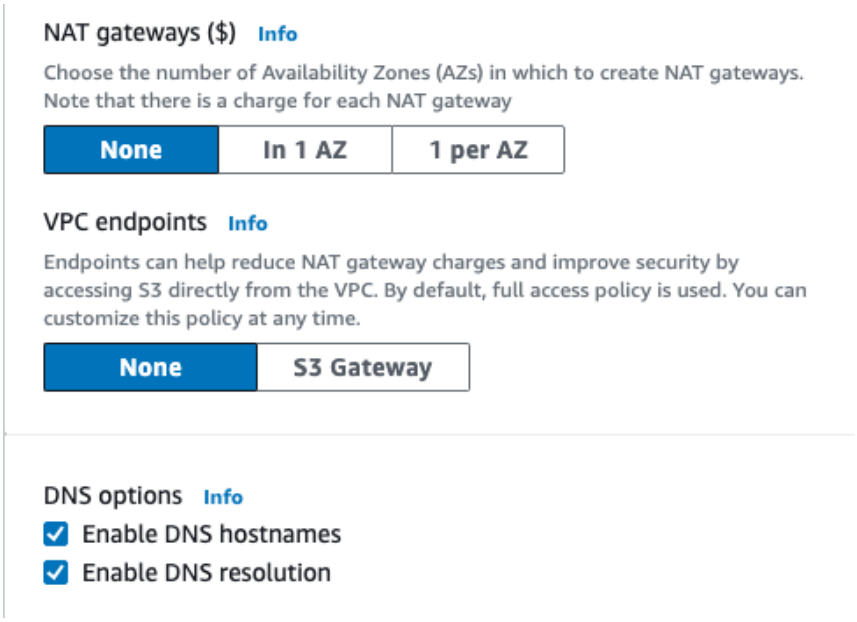
- For high availability, let's use at least 2 AZs.



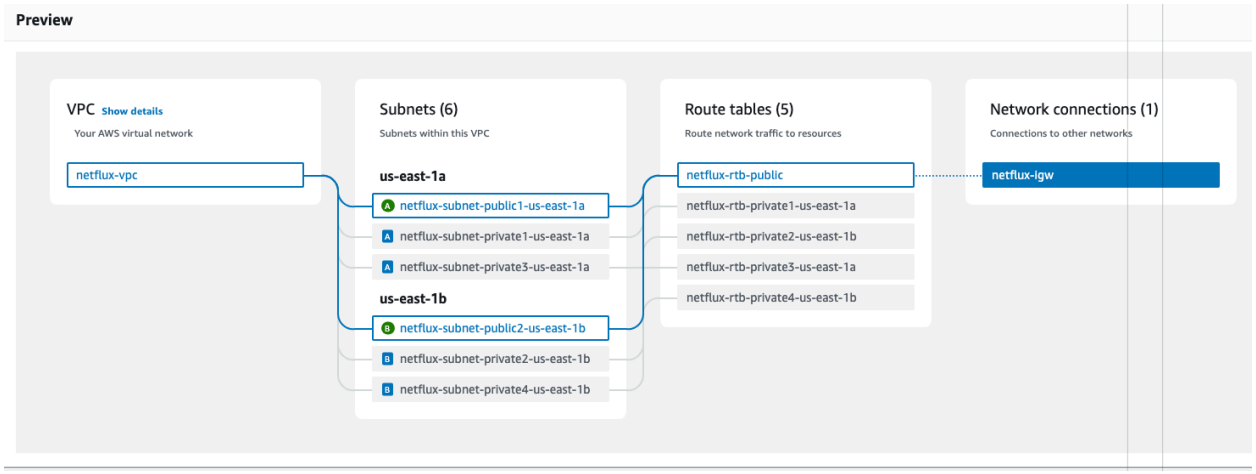
- We need
  - 2 public subnets. 1 for each AZ.
  - 2 private subnets for our backend microservices. 1 for each AZ.
  - 2 DB subnets.



- We also need a NAT gateway. **It costs money**. We can do it later when the time comes! Let's ignore it for now.
    - Enable the DNS options.



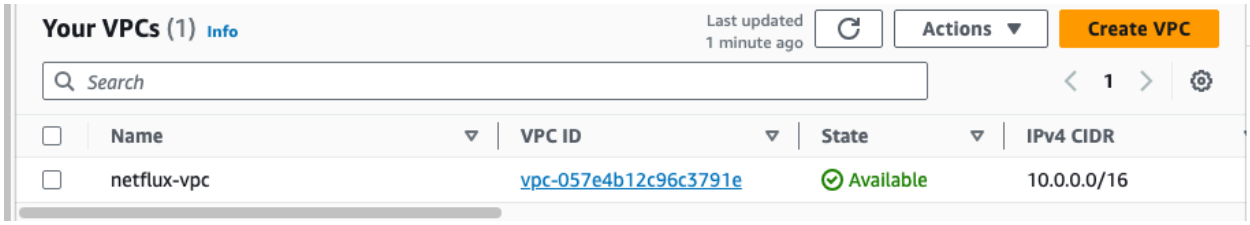
- The network we create would look like this.



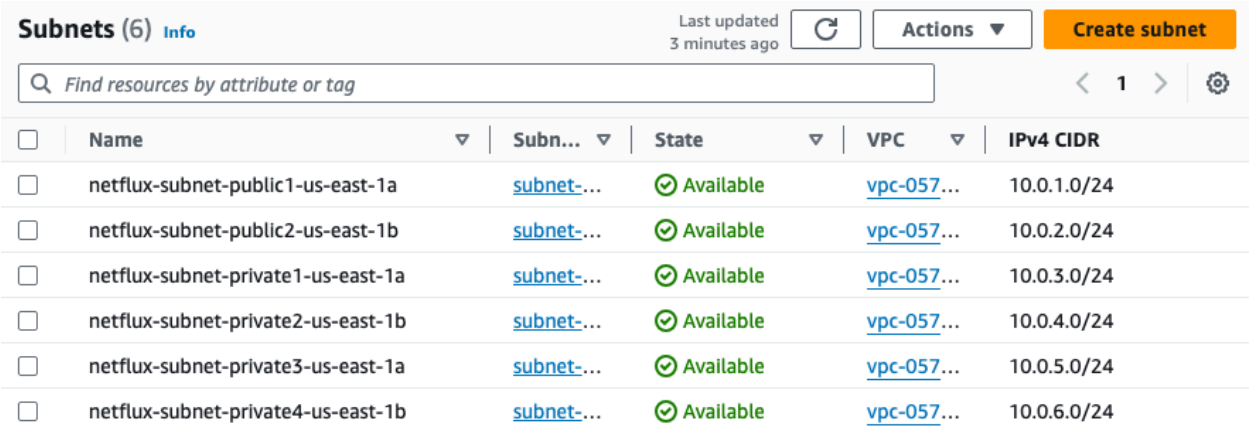
- Create VPC.
- Once it is created, do a “hard browser refresh”. AWS Console refresh does NOT seem to work well in some cases.

Verify What We Have Created:

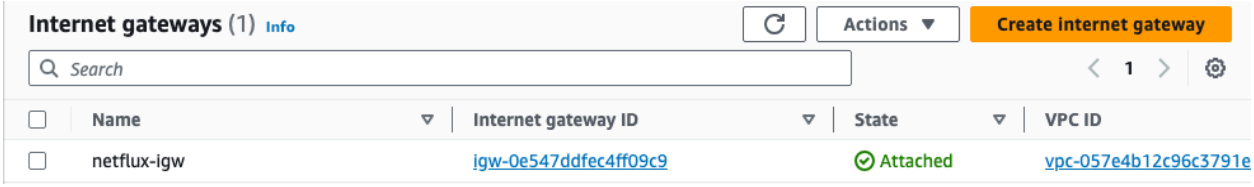
- VPC



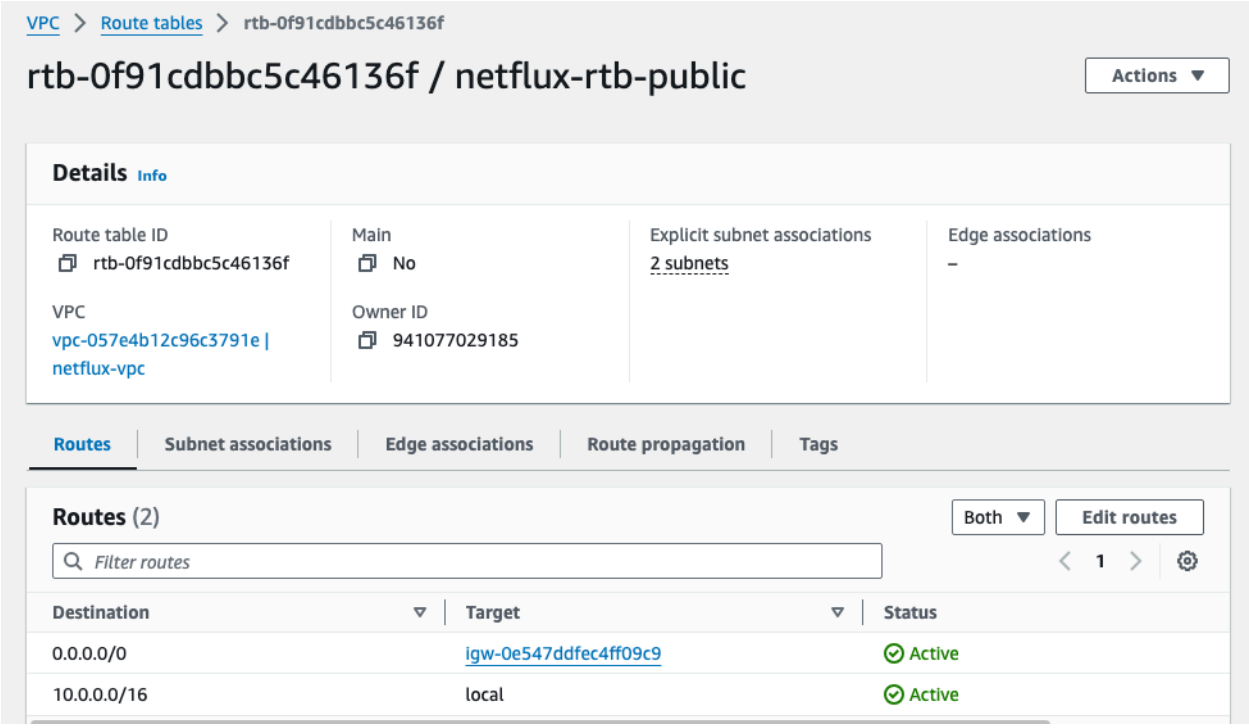
- Subnets



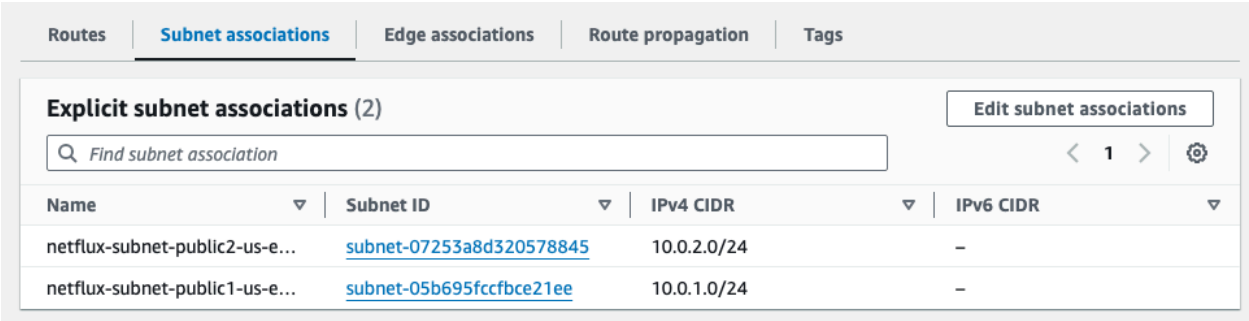
- Internet Gateway should have been attached to the VPC.



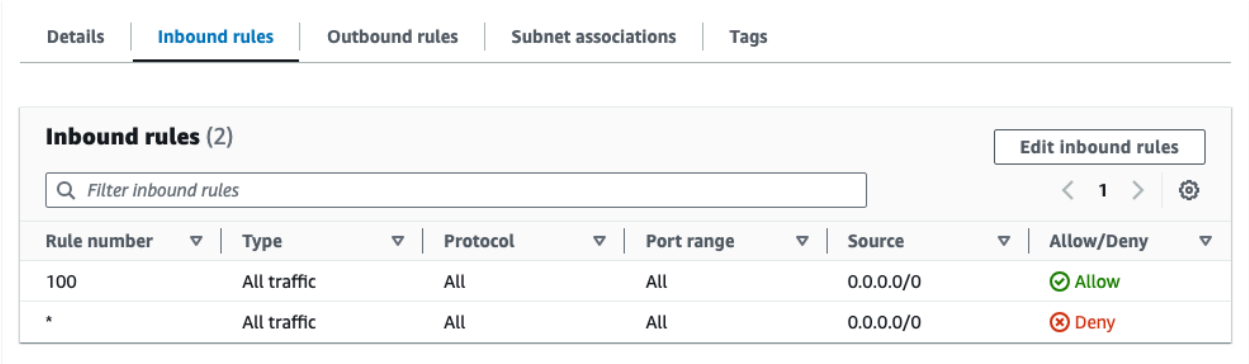
- Check the route tables. The public route table should have a route to 0.0.0.0/0 to Internet Gateway.



- Check the subnets association. 2 public subnets should have been associated with this route table!



- **Network ACL**. By default we allow all the inbound requests!

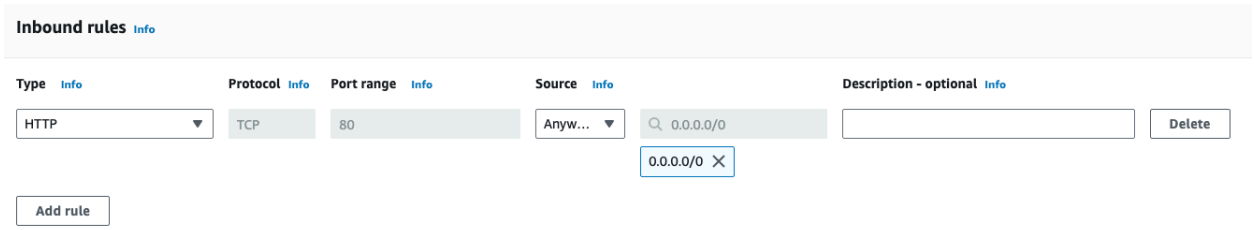


Security Groups

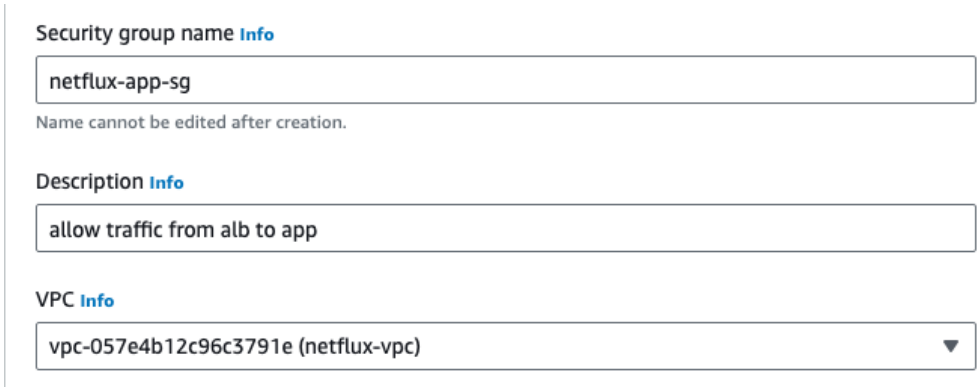
- We need 3 security groups.
    - external traffic → ALB → APP → DB

Security Group for ALB

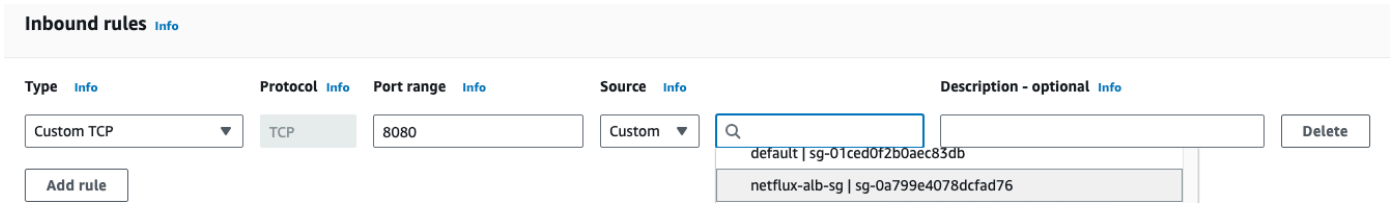
- Inbound Rule
    - allow requests from anywhere 0.0.0.0/0 for port 80



Security Group for Application / Backend Microservices

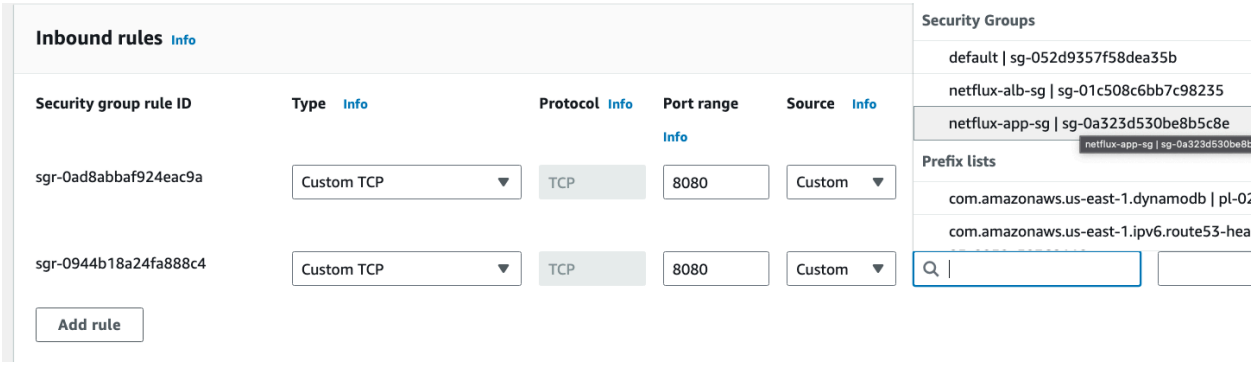


- Inbound Rule to allow traffic from ALB.
    - Port: **8080**
    - Source: Select the “**netflux-alb-sg**”



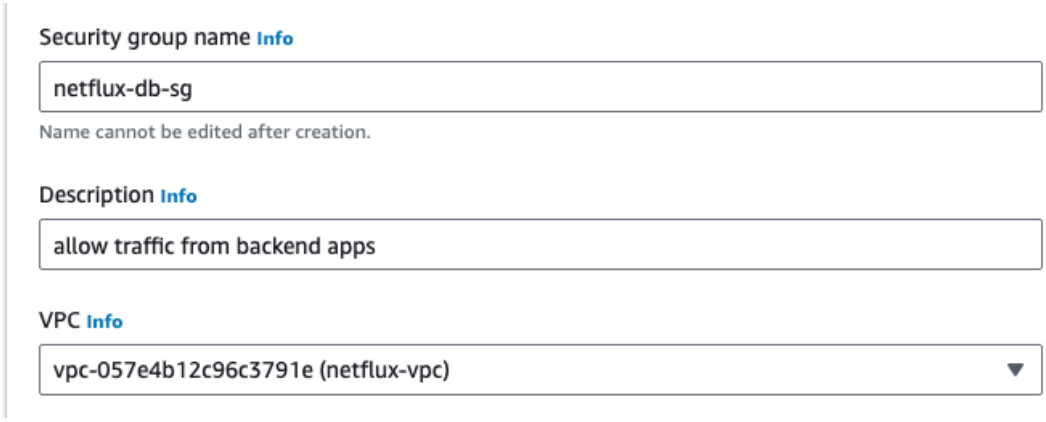
- Create the Security Group
- Remember that apps can talk among themselves! ***customer-service*** will want to talk to ***movie-service*** to get the movie information. However the current rule is explicitly to allow the traffic only from ALB. So, let’s add another inbound rule.
- Click on “Edit Inbound Rules” to add another rule as shown below.

We allow 8080 among backend applications



Security Group for DB

- Enter the details



- We add this inbound rule.
  - port: **5432**
  - source: “**netflux-app-sg**”