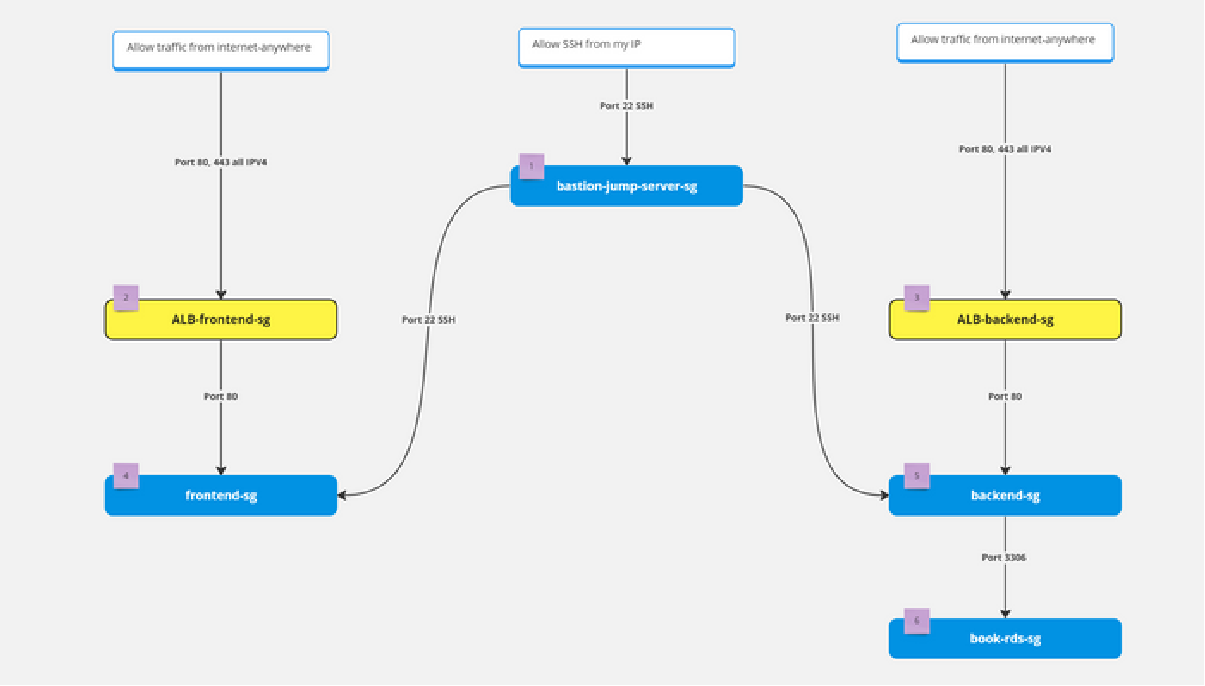
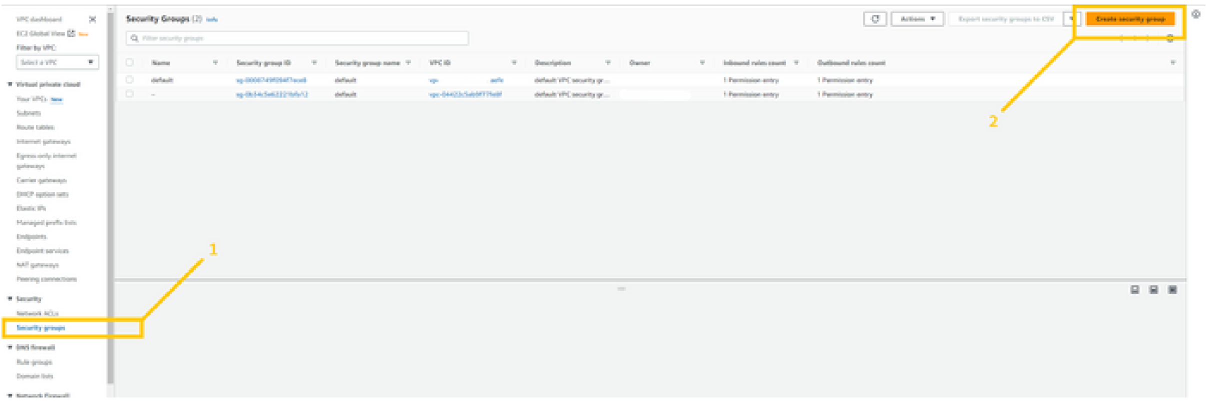
◆ Security Groups (SG)

Security groups are very essential part of the infrastructure. Because it can secure the resources in the cloud. SGs are a kind of firewall that allow or block incoming and outgoing traffic. SGs are applied to the resources like ALB, ec2, rds., etc. One resource can have more than one SG.

So let's first understand. How SG will be used in our architecture and how we are going to apply that. Please see the below image you will get all the ideas. Which resource depends on what. And what are the port numbers we need to allow etc.

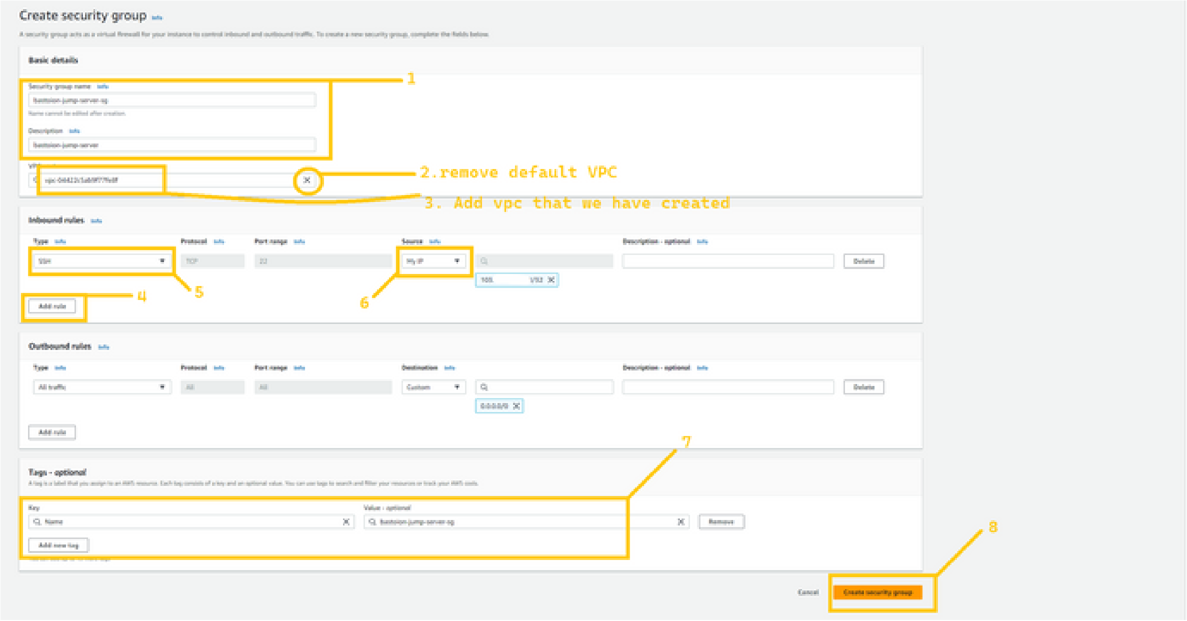


To create SG, click on the security groups tab on the left panel and here you will see the **Security Groups** button. Note that SGs are specific with VPC. So we can’t use SG which is created in a different VPC. So when you create SG please make sure that you choose the right VPC. click on the crate security button on the top right corner.



Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
default	[illegible]	default	[illegible]	default VPC security gr...		1 Permission entry	1 Permission entry
–	[illegible]	default	[illegible]	default VPC security gr...		1 Permission entry	1 Permission entry

We will create our first SG for **bastion-jump-server**. Give any name and description you want but please remove the default VPC and add VPC that we have just created. Then click on the **Add rule** button in inbound rules. And add SSH rule and add your IP in the destination. Please don’t do anything with the outbound rule if you don't have a good understanding. And then click on the **create security group** button.



Create security group

Basic details

Security group name: bastion-jump-server-sg

Description: bastion-jump-server

VPC: vpc-0d422c5ab9f77fe8f

Inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	My IP	

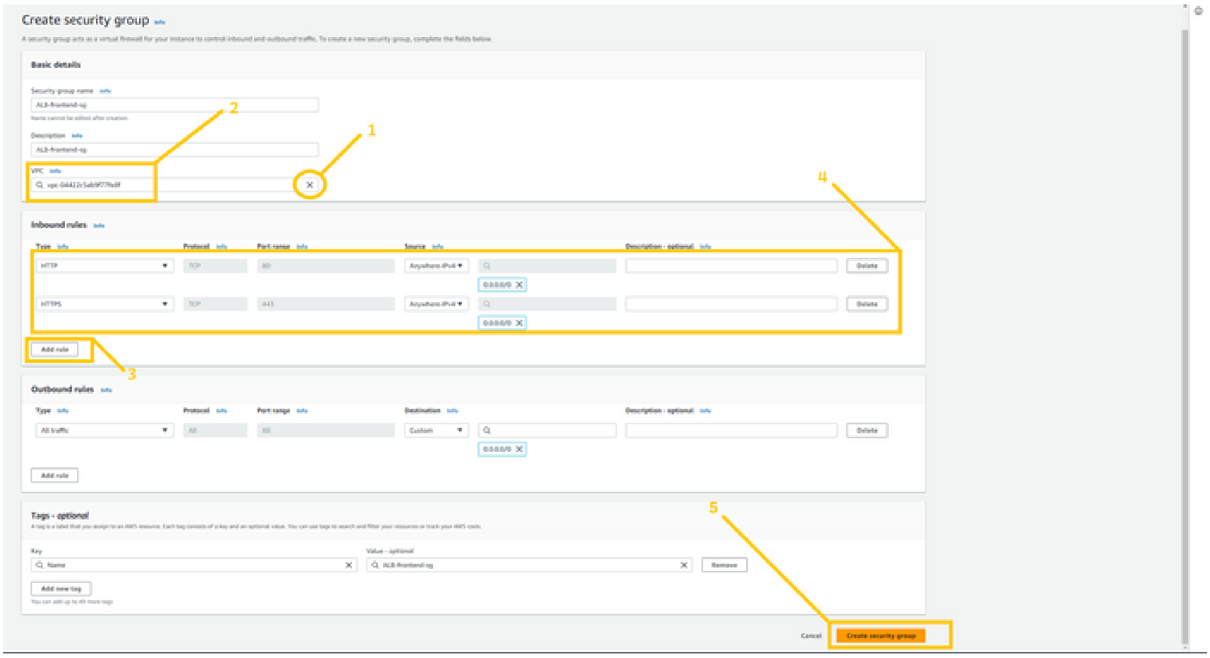
Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom 0.0.0.0/0	

Tags - optional

Key: Name Value - optional: bastion-jump-server-sg

Now let's create SG for the **ALB-frontend**. Again steps are similar but add the rule HTTP AND HTTPS from anywhere on the internet because both ALB are internet facing. But please select the right VPC.



Create security group

Basic details

Security group name: ALB-frontend-sg

Description: ALB-frontend-sg

VPC: vpc-0d422c5ab9f77fe8f

Inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Anywhere-IPv4 0.0.0.0/0	
HTTPS	TCP	443	Anywhere-IPv4 0.0.0.0/0	

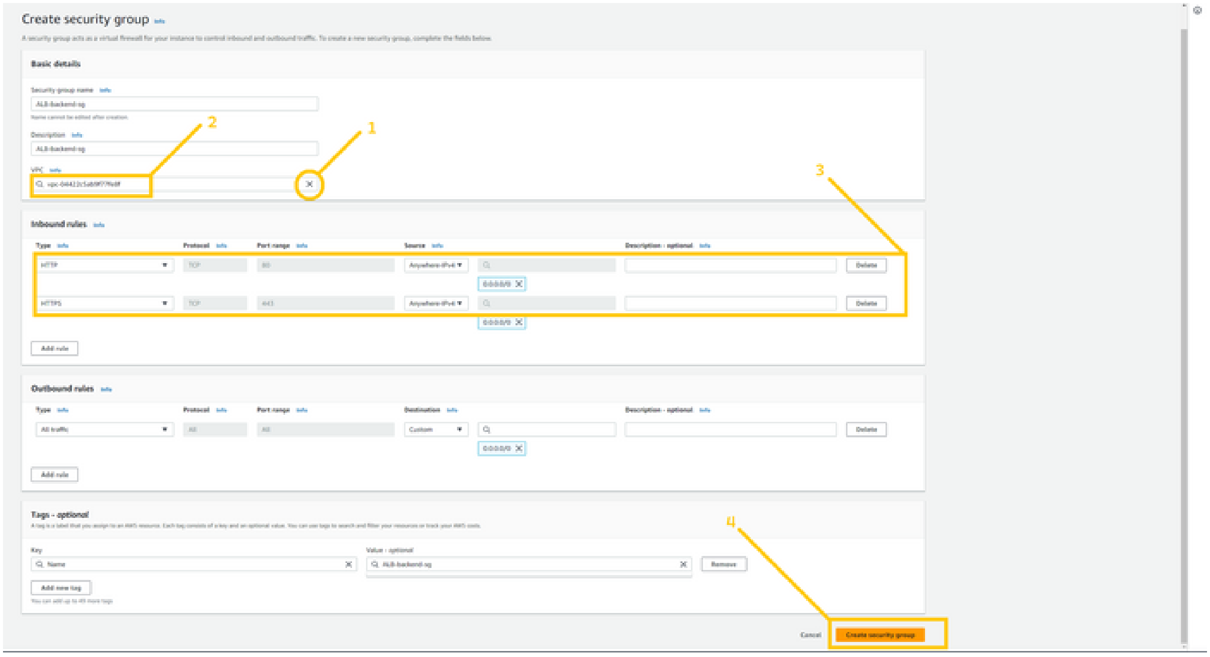
Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom 0.0.0.0/0	

Tags - optional

Key: Name Value - optional: ALB-frontend-sg

Create SG for **ALB-backend**. ALB-backend is also internet-facing. Again allow HTTP and HTTPS from anywhere.



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name: ALB-backend-sg

Name cannot be edited after creation.

Description: ALB-backend-sg

VPC: vpc-04422c5ab9f77fe8f

Inbound rules

Type	Protocol	Port range	Source		Description - optional
HTTP	TCP	80	Anywhere-IPv4	0.0.0.0/0	
HTTPS	TCP	443	Anywhere-IPv4	0.0.0.0/0	

Outbound rules

Type	Protocol	Port range	Destination		Description - optional
All traffic	All	All	Custom	0.0.0.0/0	

Tags - optional

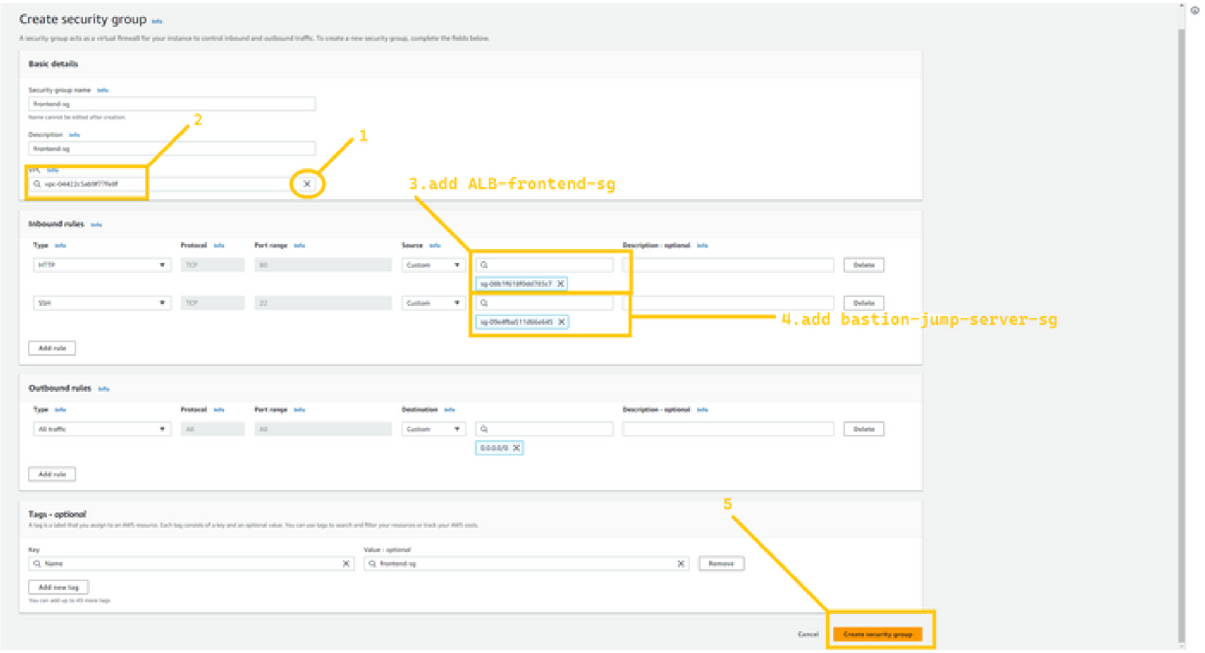
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name

Value - optional: ALB-backend-sg

You can add up to 49 more tags.

Create SG for frontend servers. Our frontend server will be in a private subnet so add the HTTP rule and select the source as **ALB-frontend-sg**. So only ALB-frontend can access the frontend server on port 80. You have to add one more rule SSH allows from **bastion-jump-server-sg**. So that the bastion host can log in to web servers.



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name: frontend-sg

Name cannot be edited after creation.

Description: frontend-sg

VPC: vpc-04422c5ab9f77fe8f

Inbound rules

Type	Protocol	Port range	Source		Description - optional
HTTP	TCP	80	Custom	sg-08b1f6189dd785c7	
SSH	TCP	22	Custom	sg-0fe4fba511d66e645	

Outbound rules

Type	Protocol	Port range	Destination		Description - optional
All traffic	All	All	Custom	0.0.0.0/0	

Tags - optional

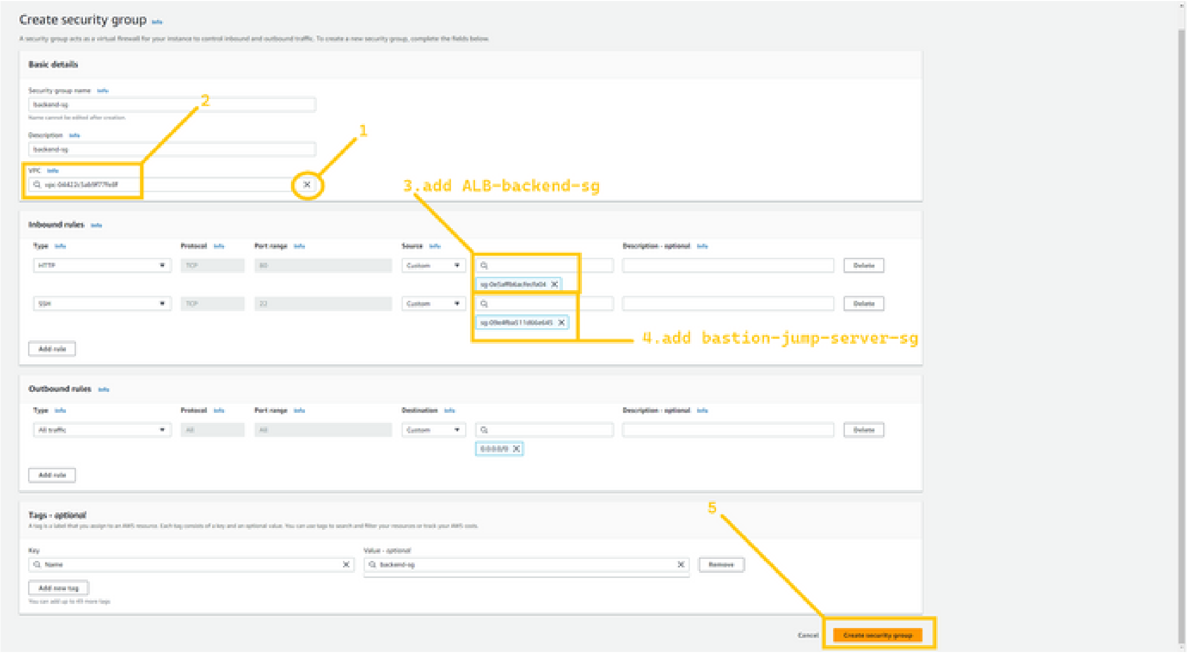
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name

Value - optional: frontend-sg

You can add up to 49 more tags.

Let's create SG for the backend server. Again steps are completely similar to **frontend-sg**. You have to allow port 80 from **ALB-backend-sg** so that only **ALB-backend** can request to the backend server and add the rule SSH allows from **bastion-jump-server-sg**. So that the bastion host can log in to backend servers.



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info: backend-sg

Name cannot be edited after creation.

Description Info: backend-sg

VPC Info: vpc-0d6412c5ab9f77fe8f

Inbound rules Info

Type	Protocol	Port range	Source		Description - optional
HTTP	TCP	80	Custom	sg-0e5af9b6acfecfa04	
SSH	TCP	22	Custom	sg-09ed8fba511d66e645	

Outbound rules Info

Type	Protocol	Port range	Destination		Description - optional
All traffic	All	All	Custom	0.0.0.0/0	

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

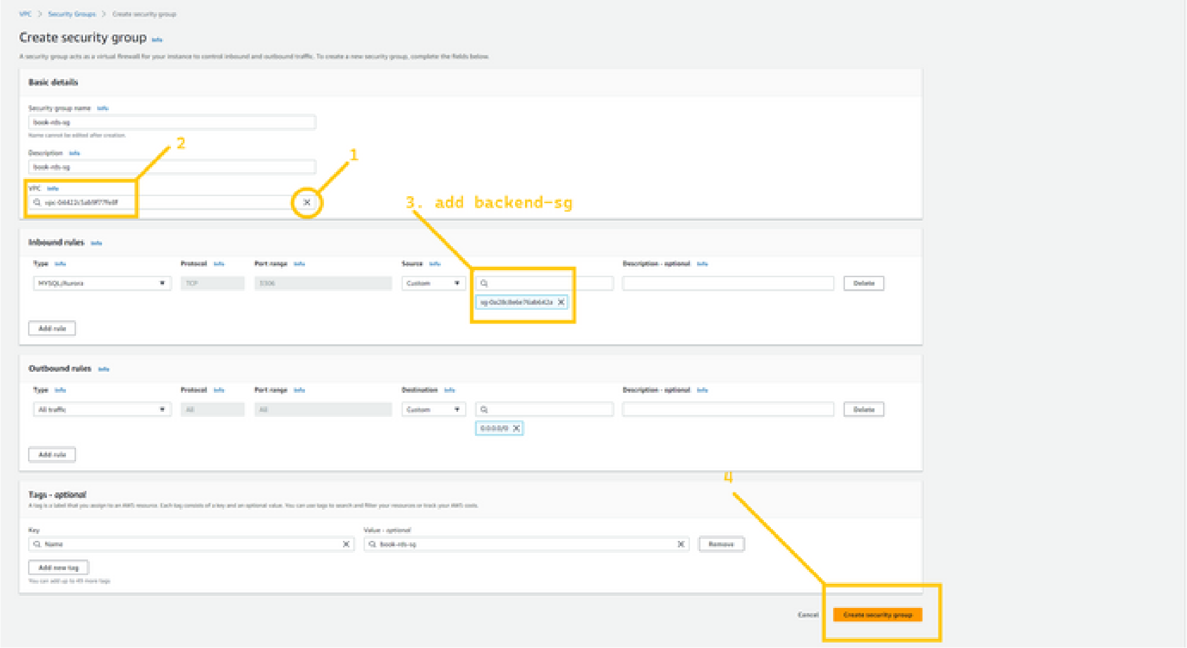
Key	Value - optional
Name	backend-sg

You can add up to 49 more tags.

3.add ALB-backend-sg

4.add bastion-jump-server-sg

Lastly, we are going to create SG for RDS instance. Allow port 3306 MySql/Arrora from **backend-sg** so that only the backend server will be able to access it. and no one else can access our database.



VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info: book-rds-sg

Name cannot be edited after creation.

Description Info: book-rds-sg

VPC Info: vpc-0d6412c5ab9f77fe8f

Inbound rules Info

Type	Protocol	Port range	Source		Description - optional
MYSQL/Aurora	TCP	3306	Custom	sg-0a28c8ebe76ab642a	

Outbound rules Info

Type	Protocol	Port range	Destination		Description - optional
All traffic	All	All	Custom	0.0.0.0/0	

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Name	book-rds-sg

You can add up to 49 more tags.

3. add backend-sg

And here our SG setups are complete now. Your task is to do the complete same setup for the secondary region. In my case, it is **Oregon (us-west-2)**