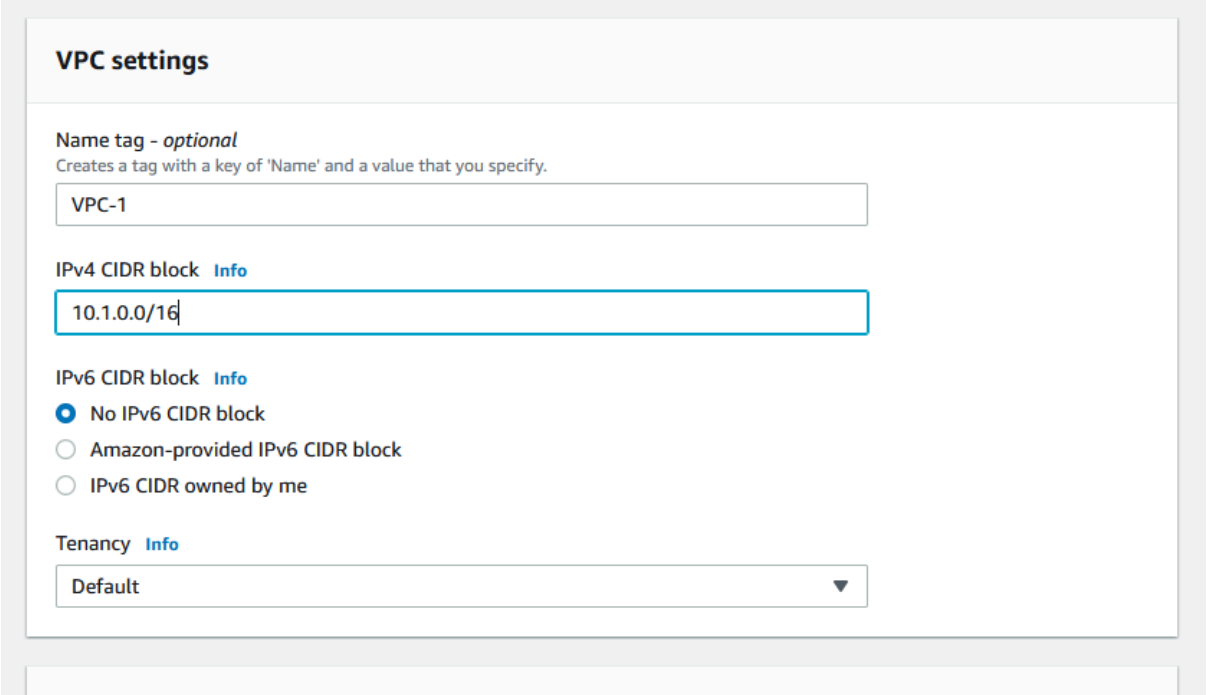
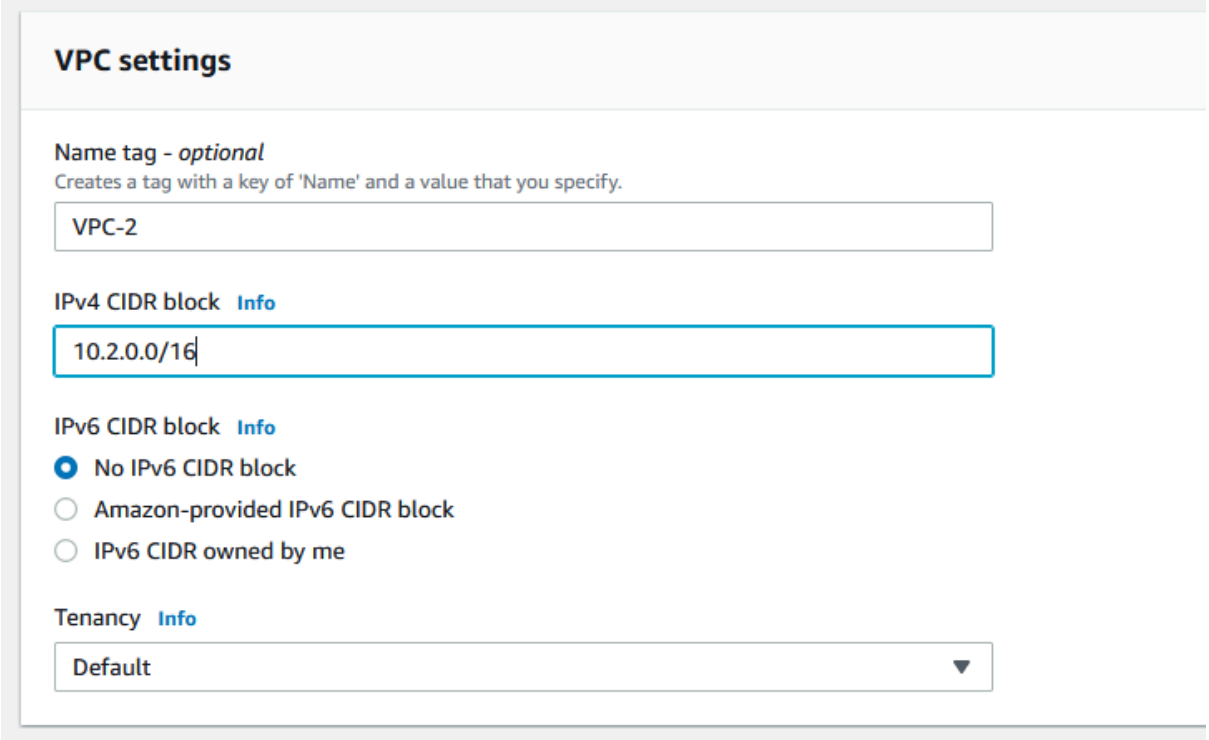
Handson steps:

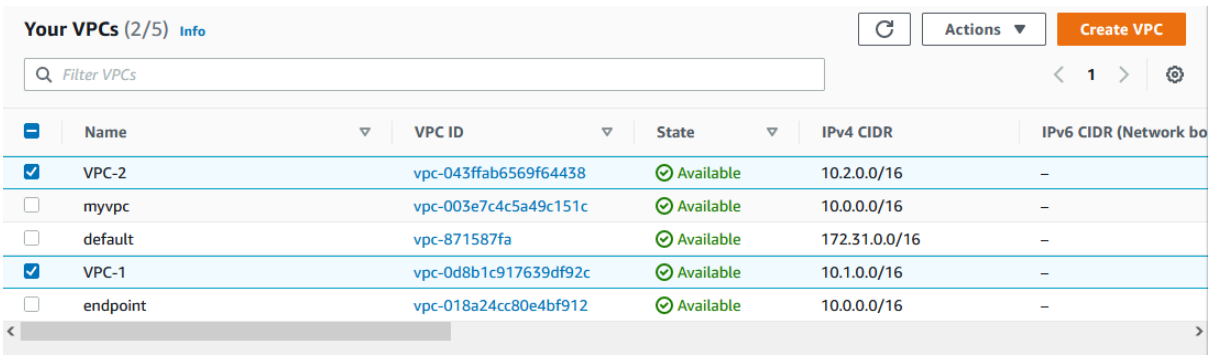
1. Create a VPC with name VPC1 (10.1.0.0/16)
2. Create a second VPC with name VPC2 - 10.2.0.0/16)
3. Create public subnet in VPC1 (VPC1-publicsubnet1 - 10.1.1.0/24)
4. Create private subnet in VPC-2 (VPC2-privatesubnet2 - 10.2.1.0/24)
5. Create VPC1 Route table (VPC1-RT)
6. Create VPC2 Route table (VPC2-RT)
7. Associate VPC1 Route table with its subnet
8. Associate VPC2 route table with its subnet
9. Create an IGW and attach it to VPC-1. (VPC1-IGW)
10. Configure public route for VPC 1 public route table
11. Complete step 21 to show that connection is impossible without the TGW
12. Navigate to transit gateway and create a transit gateway (JJTECH-TGW). Give it a name and uncheck default route table association and default route table propagation.
13. Create a TGW attachment for VPC1 and VPC2
14. Create one TGW route table
15. Delete the TGW association and propagation from the defautl RT if it exists.
16. Create 2 TGW Route table associations. For VPC 1 attachment and VPC 2 attachment. Using the RT you created in step 13.
17. Create 2 TGW Route table propagation. For VPC 1 attachment and VPC 2 attachment. Using the RT you created in step 14.
18. Click on routes to double check and make sure that both routes have been propagated
19. Go to the public subnet RT in VPC 1 and edit route. Destination is VPC2 10.2.0.0/16 and target is TGW
20. Do the same for the VPC2 private subnet RT. Destination 10.1.0.0/16 and target is TGW.
21. Test connectivity between the 2 VPCs:
    a. Spin up an instance in VPC1 with public IP enabled. (VPC1-Server), and connect to instance using AWS Instance Connect
    b. Spin up instance in VPC2 (VPC2-Server) No public IP needed since this is in a private subnet. In the security group create an allow rule for all ICMP and the source should be the cidr of VPC1.

Transit Gateway

Create VPC 1 and VPC 2

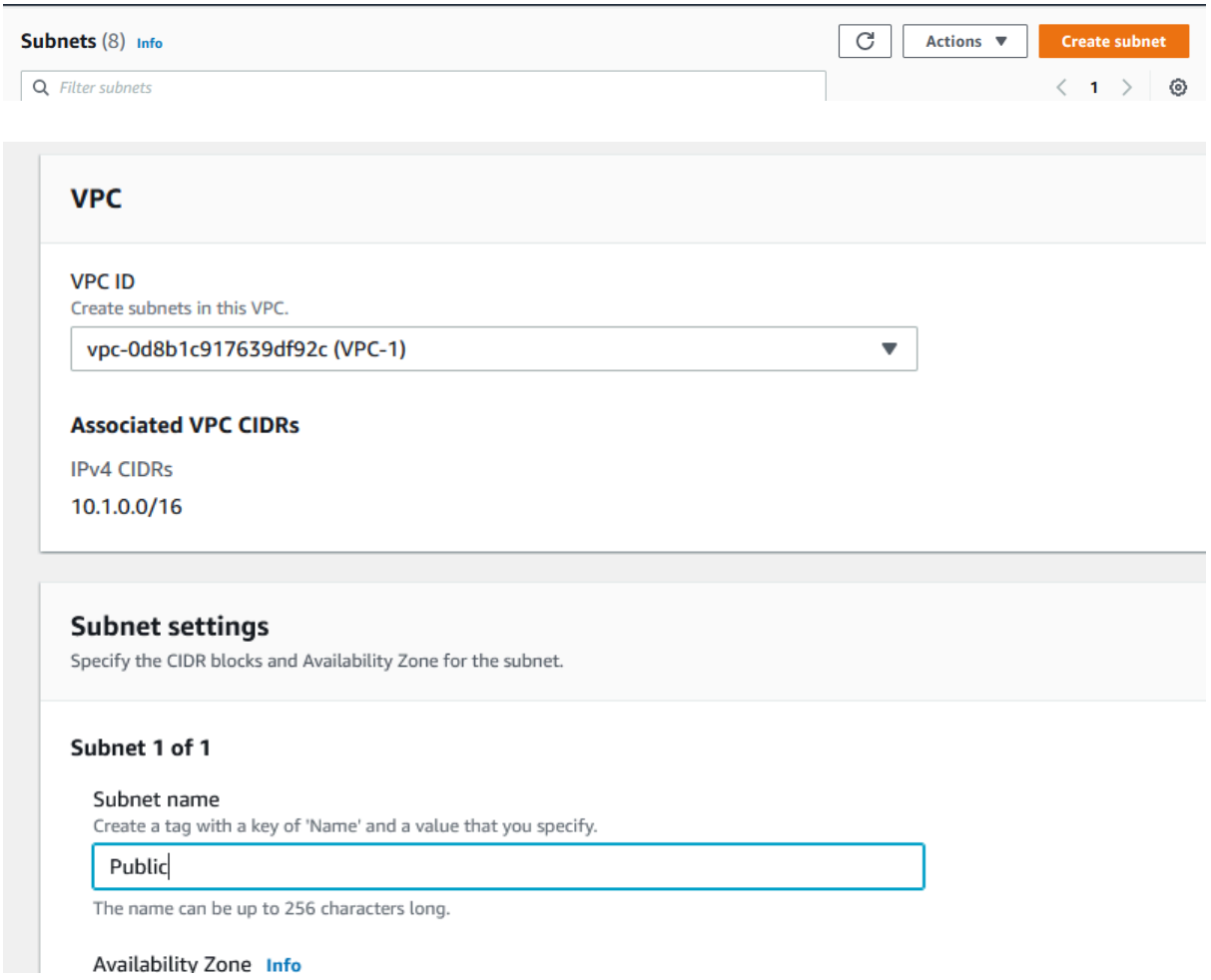


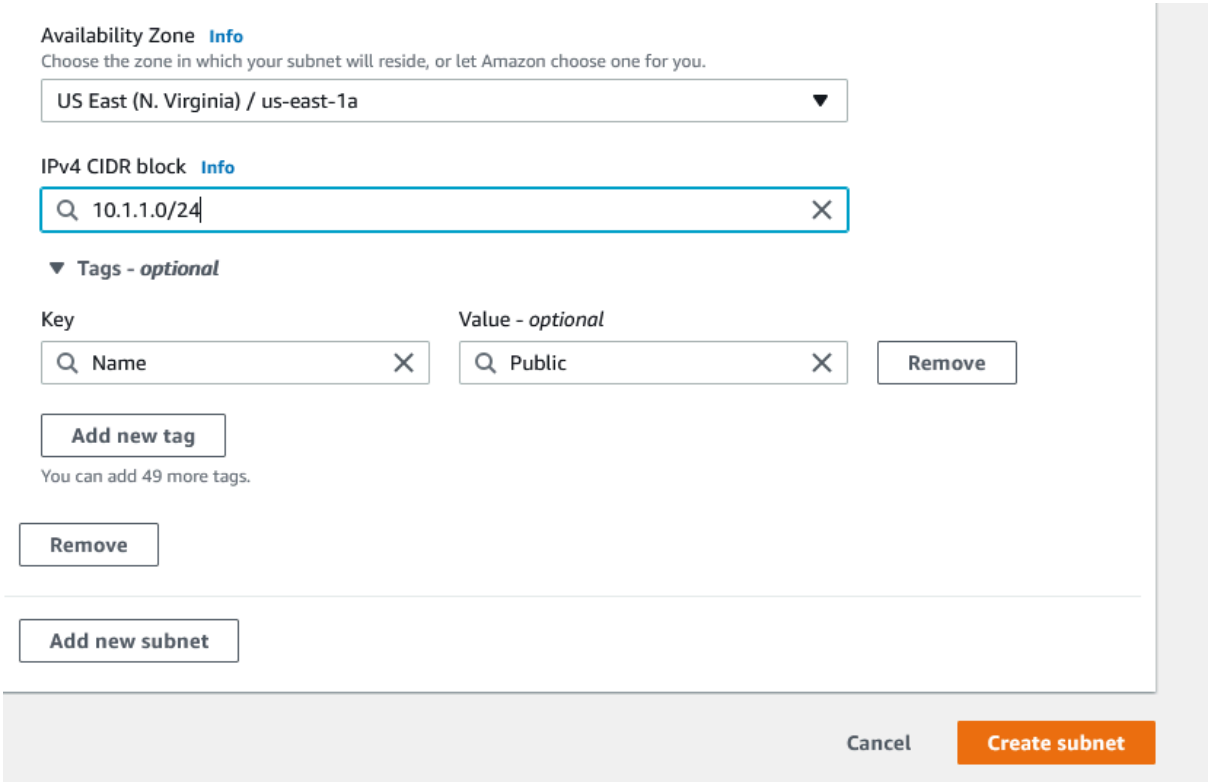




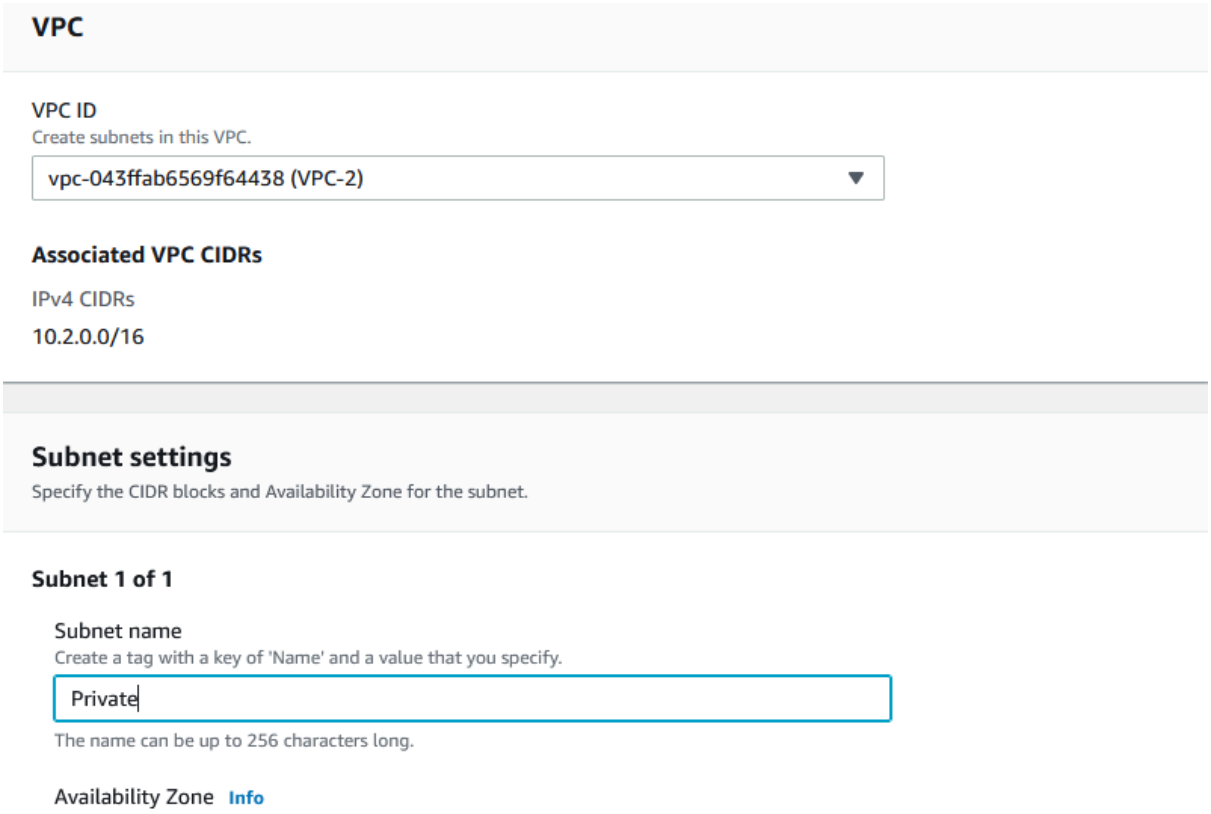
Create Public subnet in VPC-1

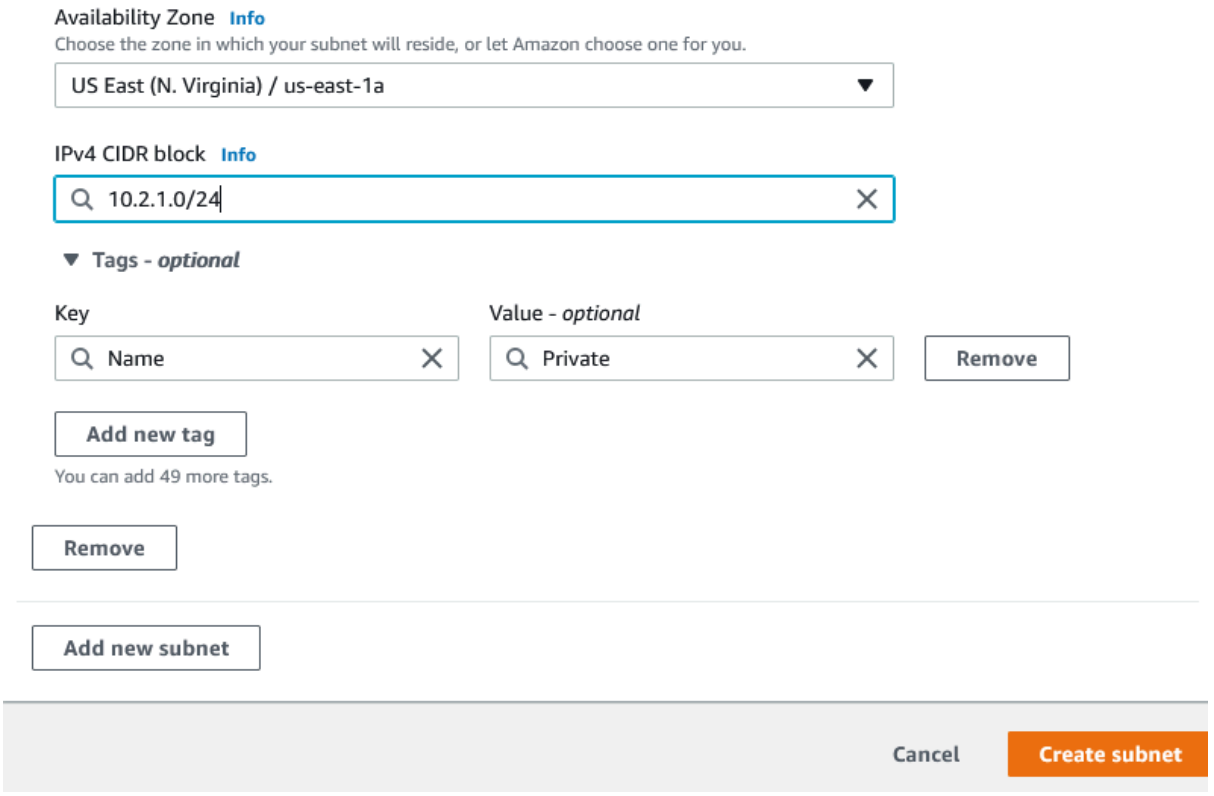
Click on create subnet

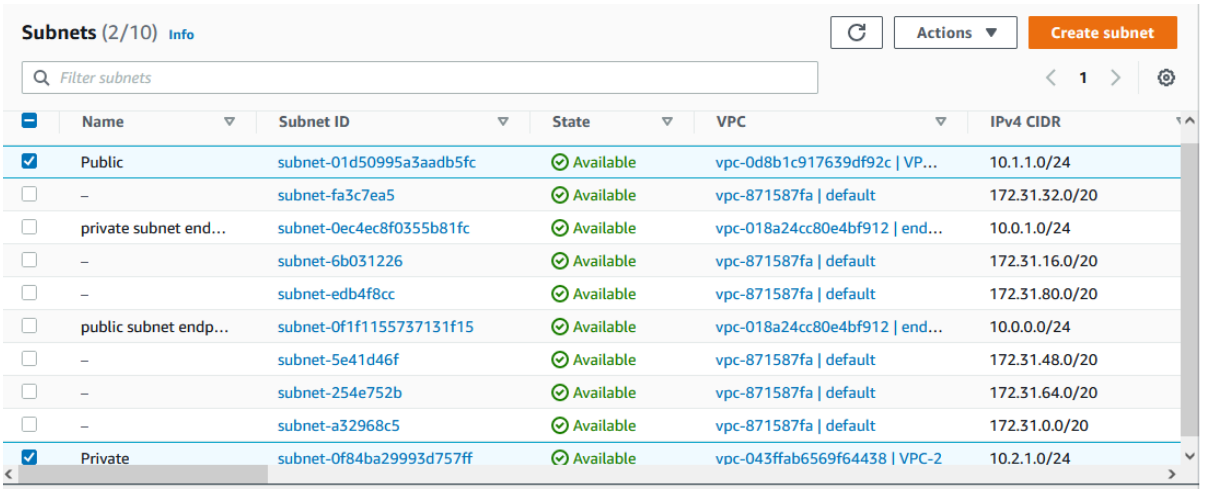




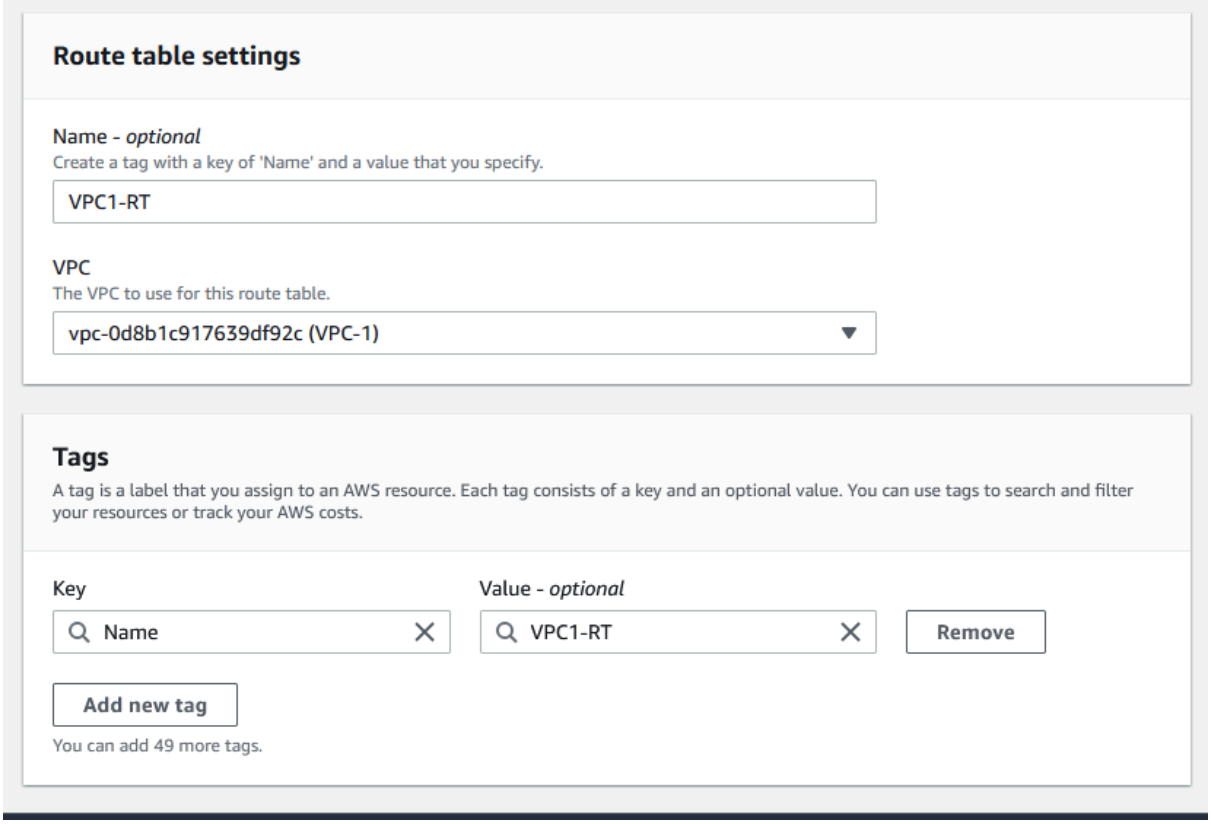
Create private subnet in VPC-2



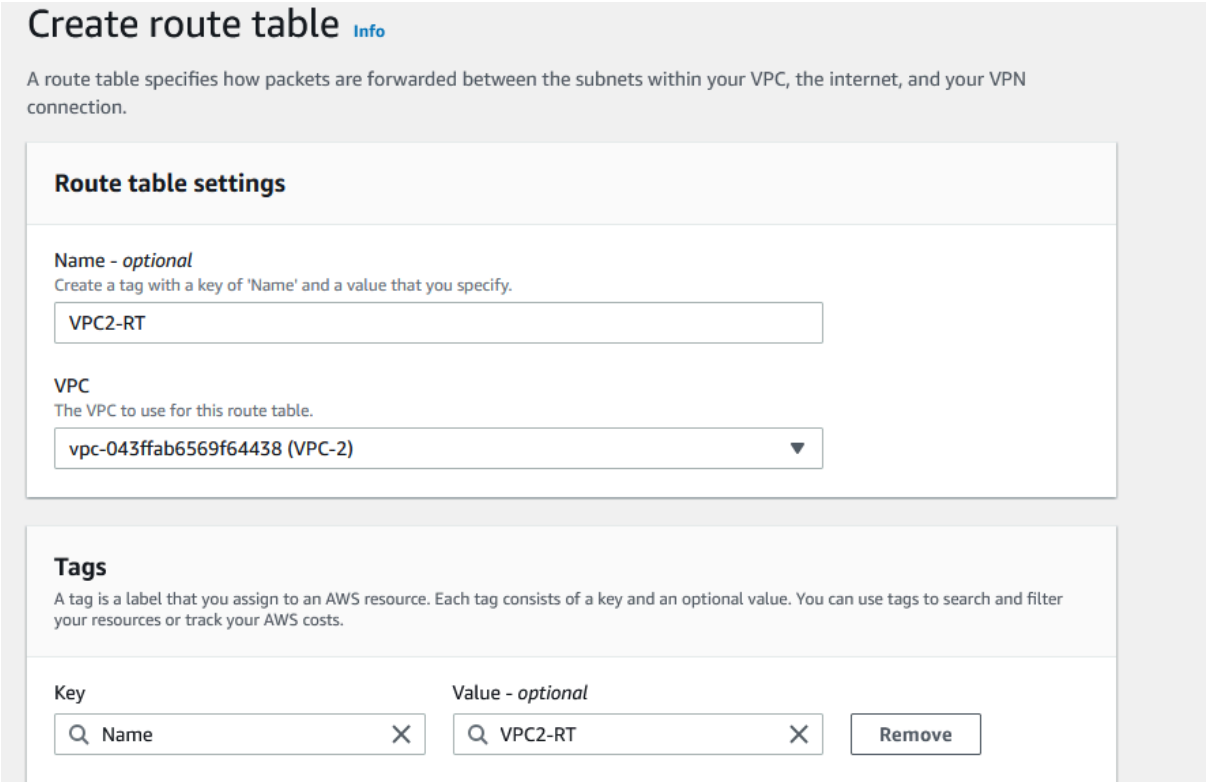


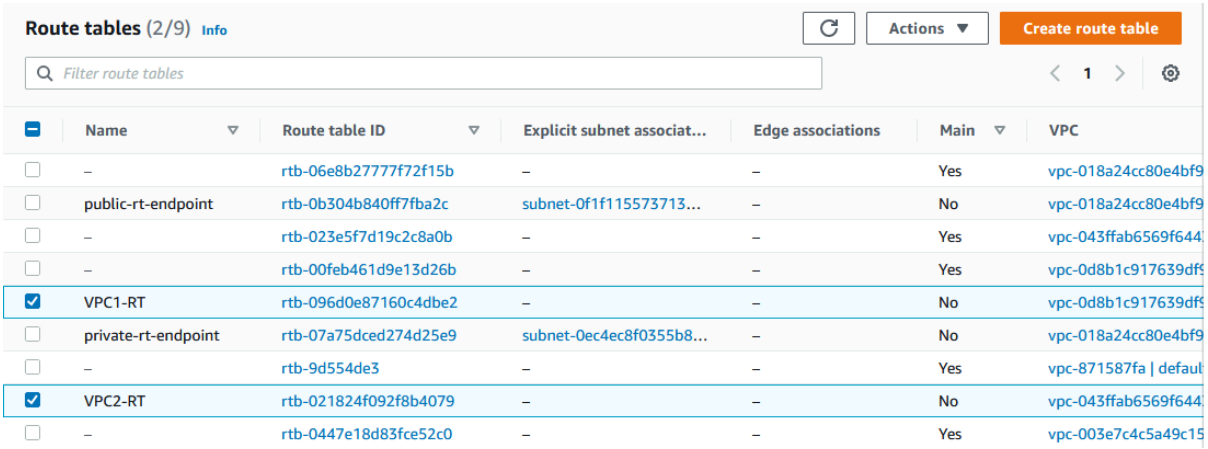


Create VPC-1 Route Table



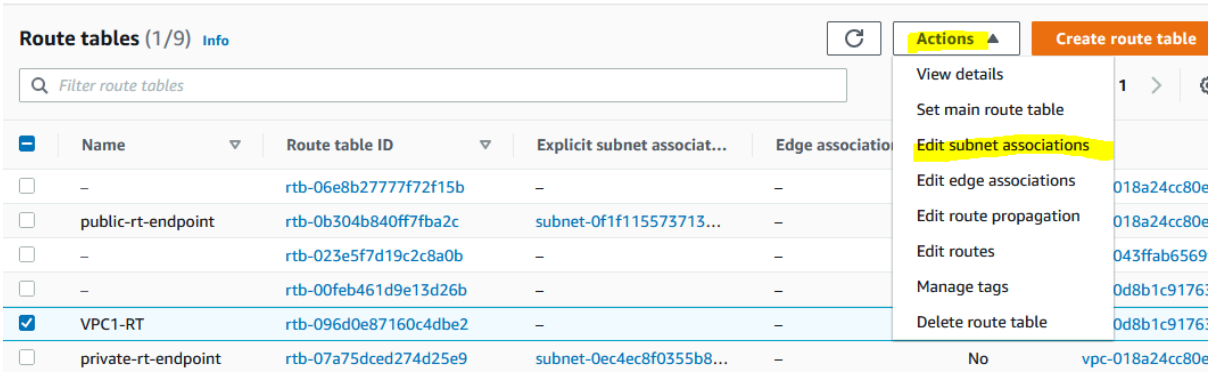
Create VPC-2 Route Table



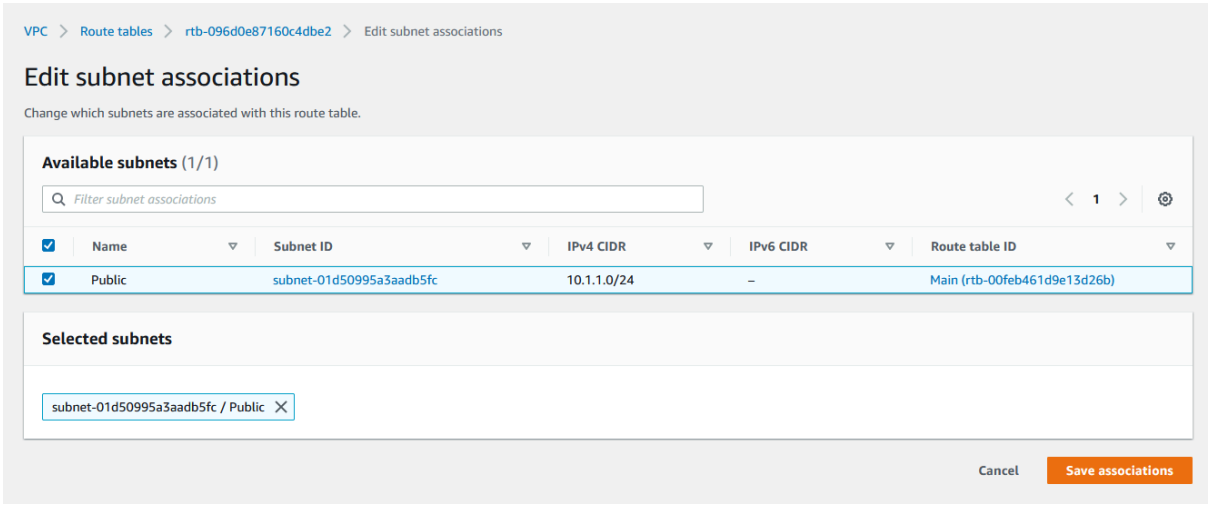


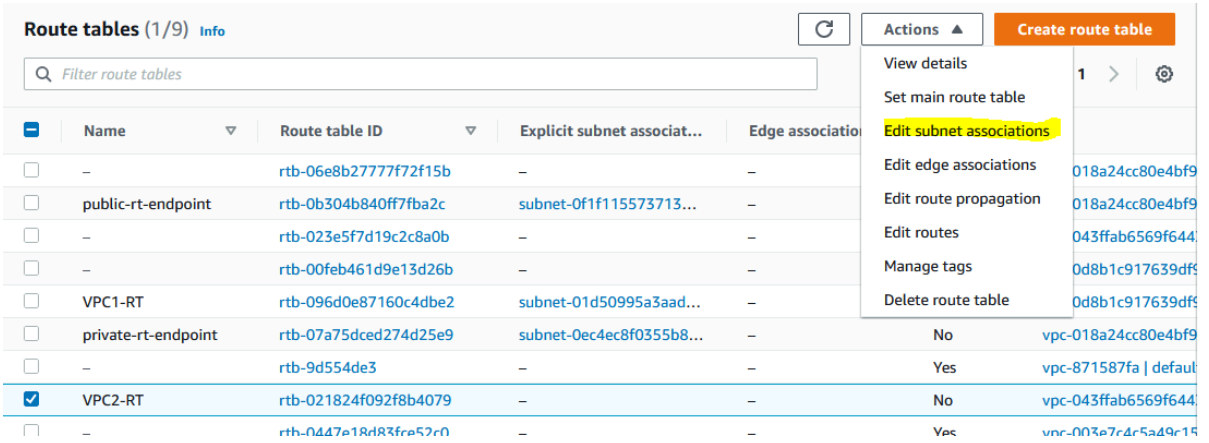
Associate VPC-1 route table with it's subnet and VP-2 route table with it's subnet

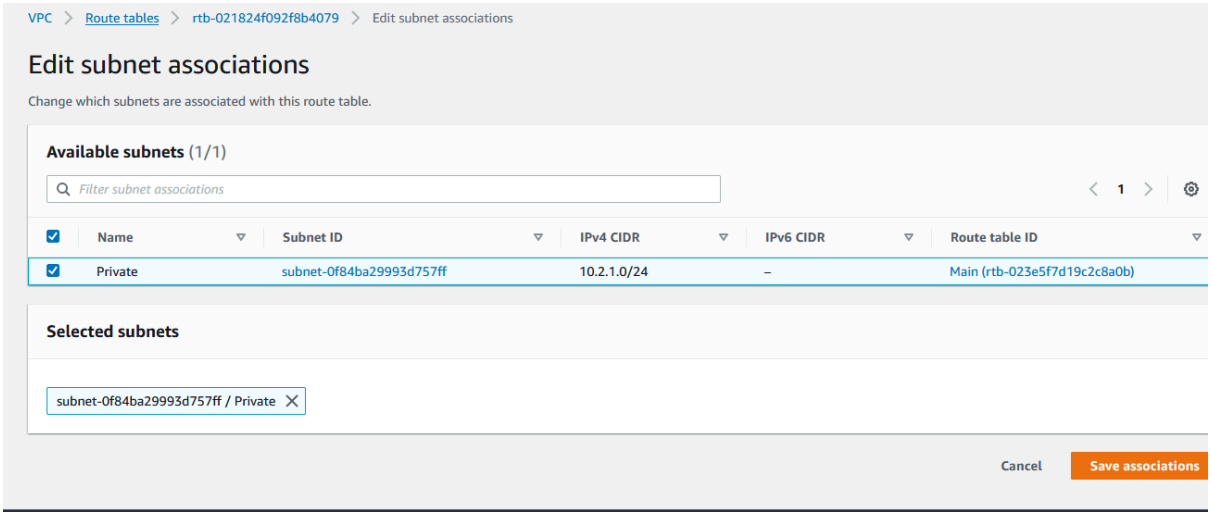
Select the RT and select actions and then subnet associations



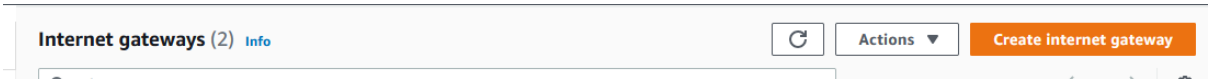
Choose the subnet and click save

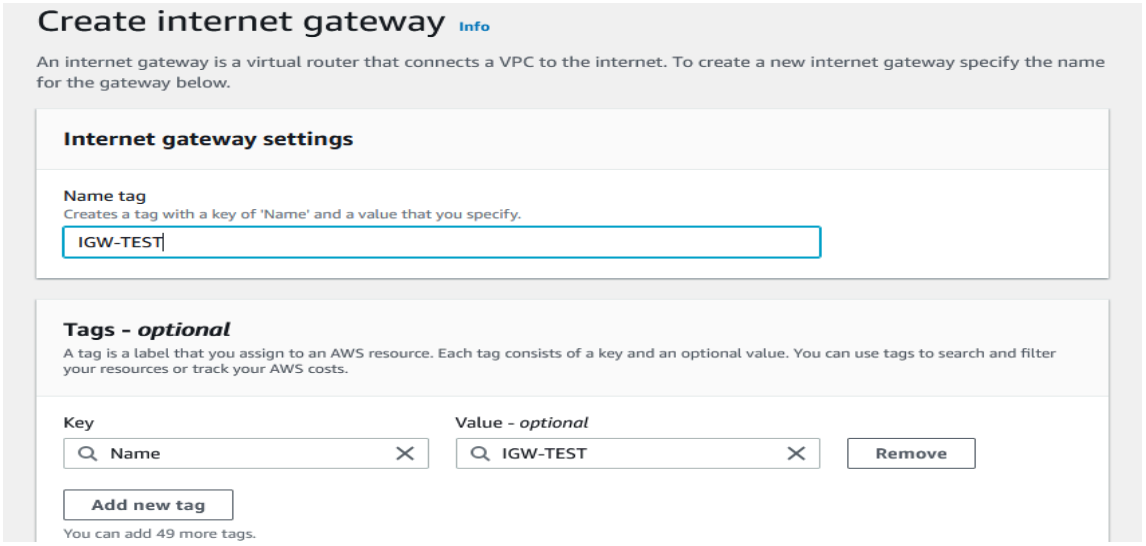


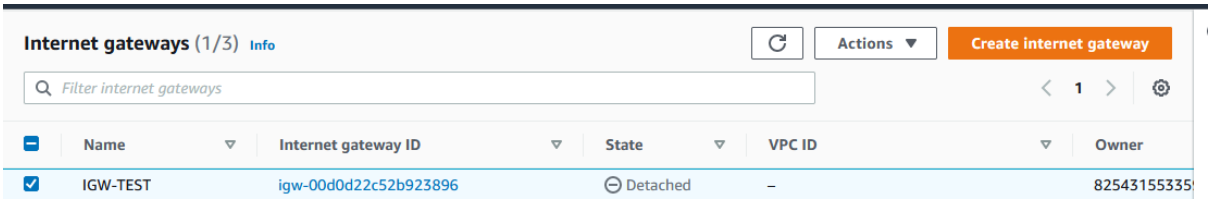


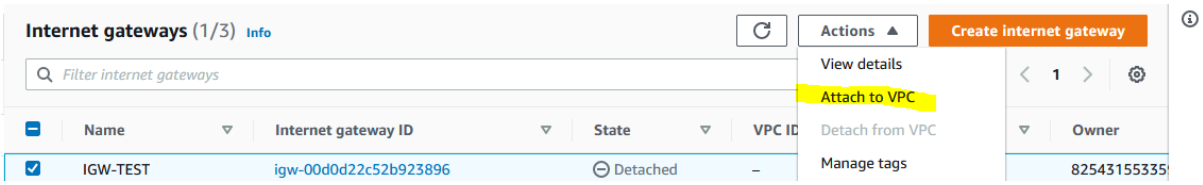


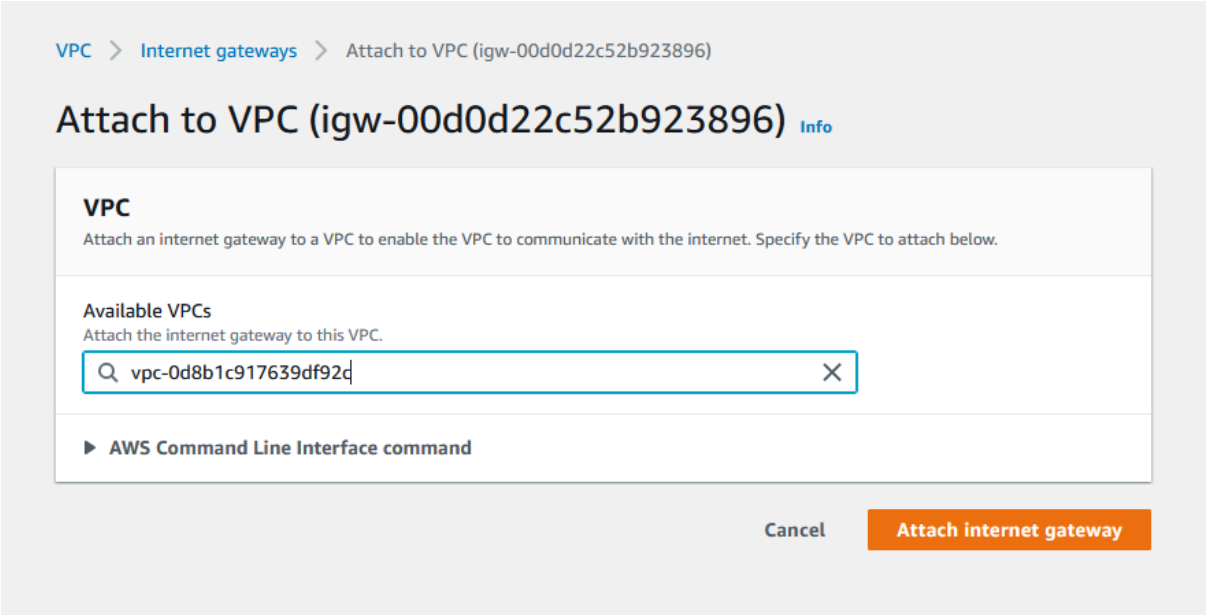
Create IGW and attach it to VPC-1

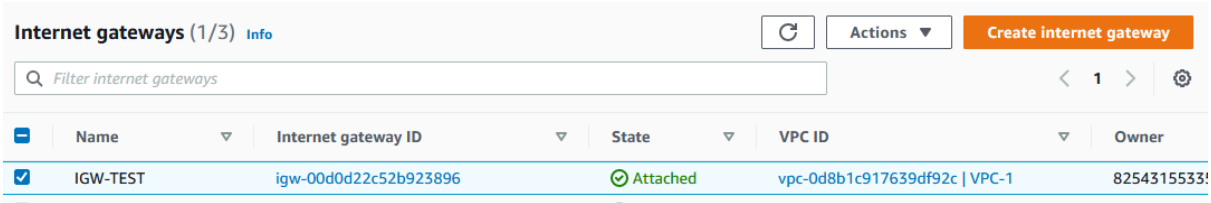






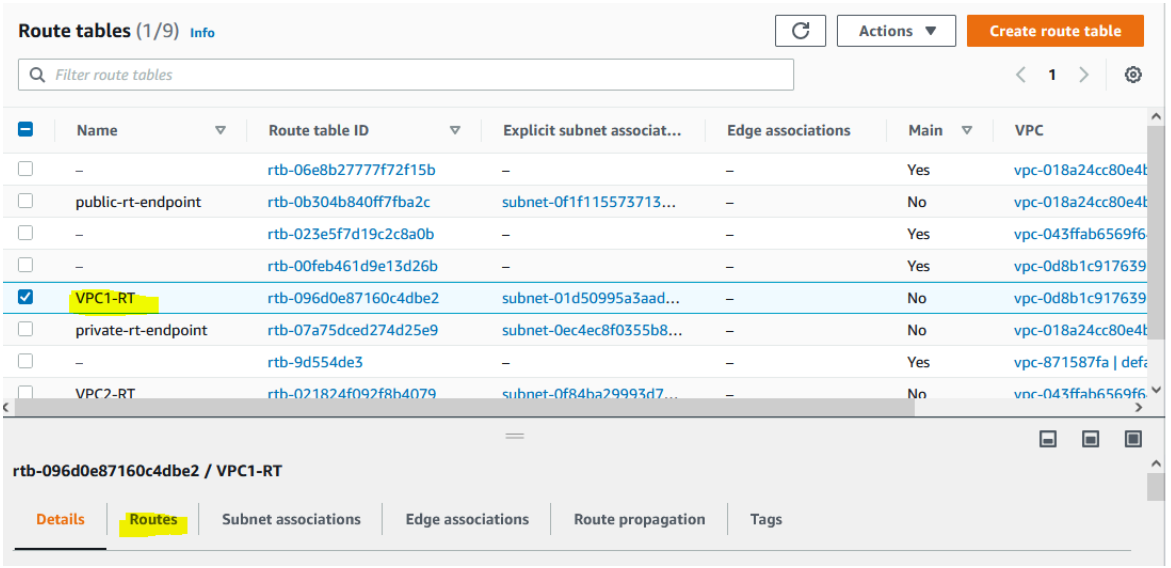


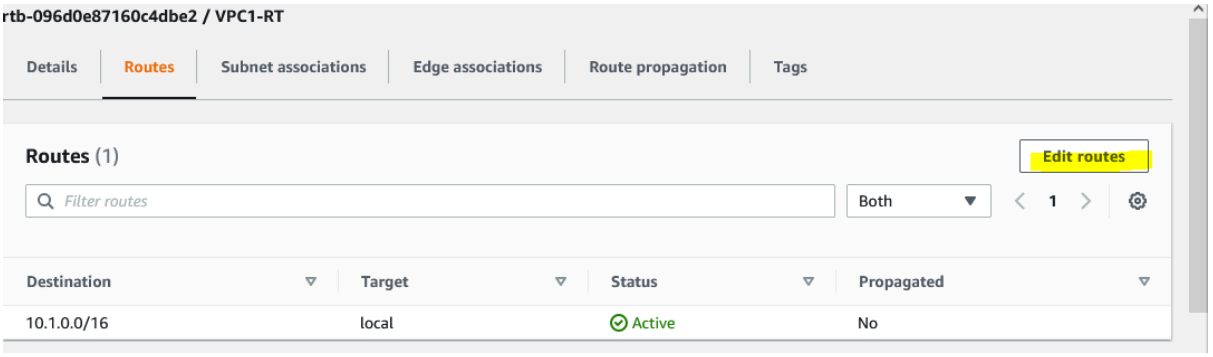




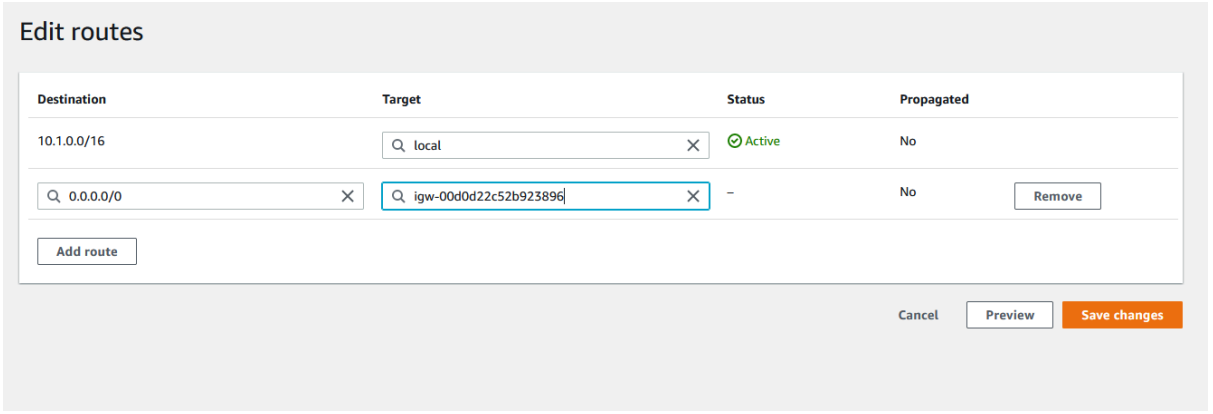
Edit VPC-1 Public Route table and configure public route

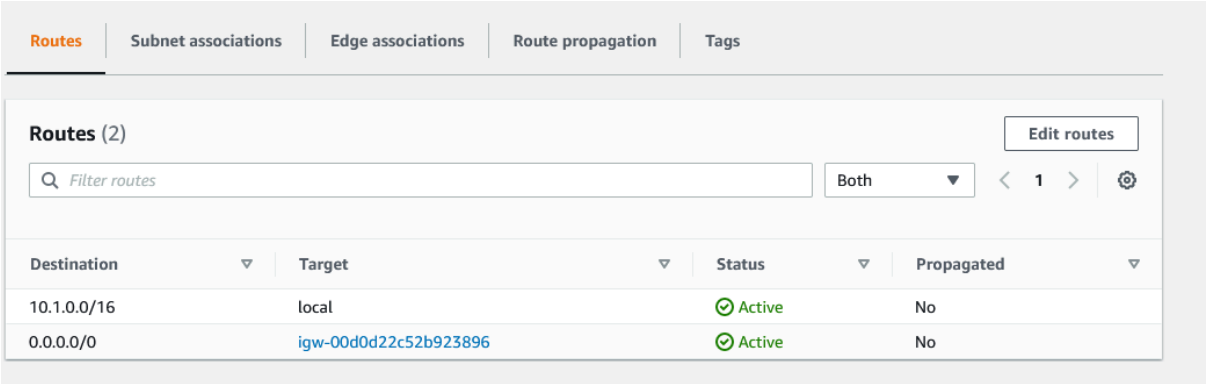
Select the public RT and click on routes



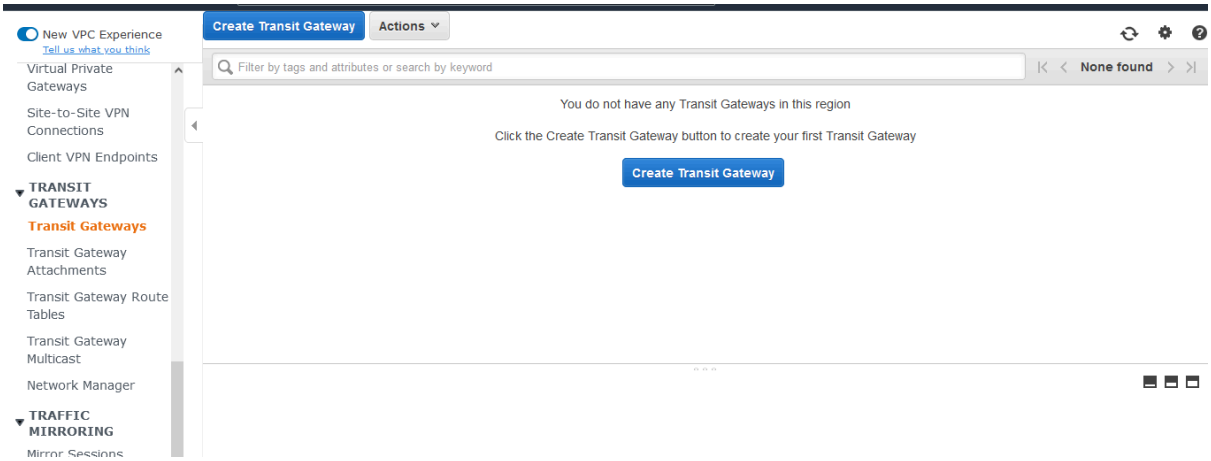


Add the IGW path





Navigate to Transit Gateways



Create a Transit Gateway

Be sure to uncheck default route table association and default route table propagation.

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag JJTECH -TGW

Description Transit gateway

Configure the Transit Gateway

Amazon side ASN 64512

DNS support enable

VPN ECMP support enable

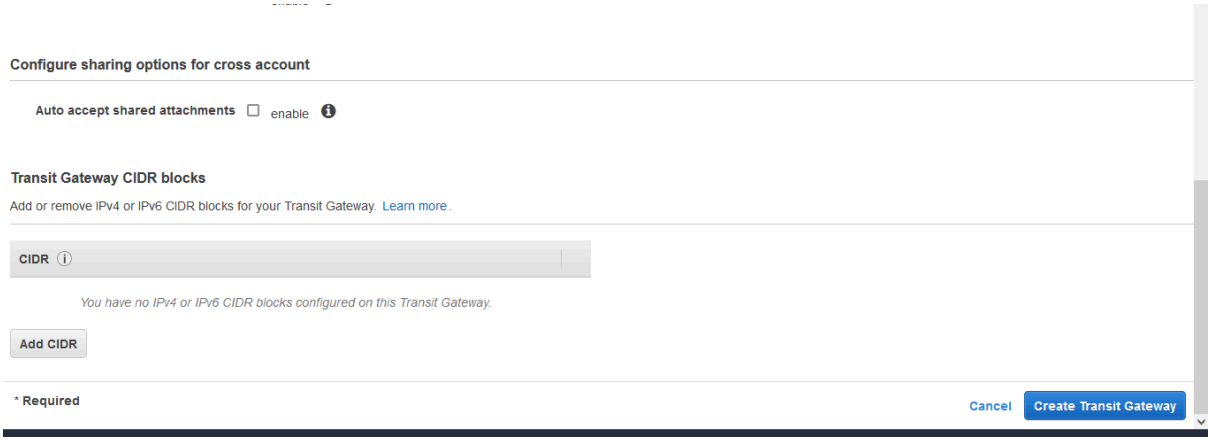
Default route table association enable

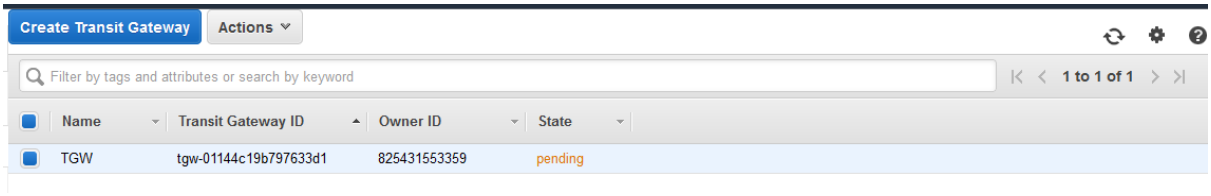
Default route table propagation enable

Multicast support enable

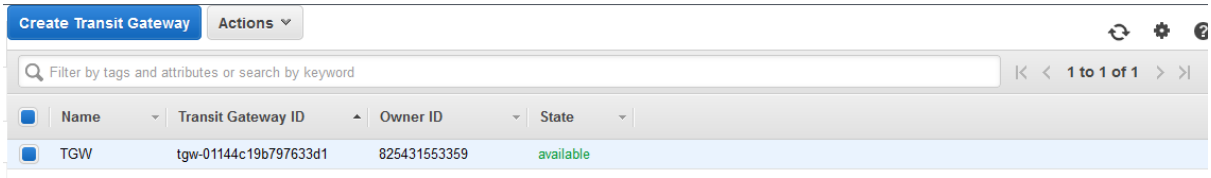
Configure sharing options for cross account

Auto accept shared attachments enable

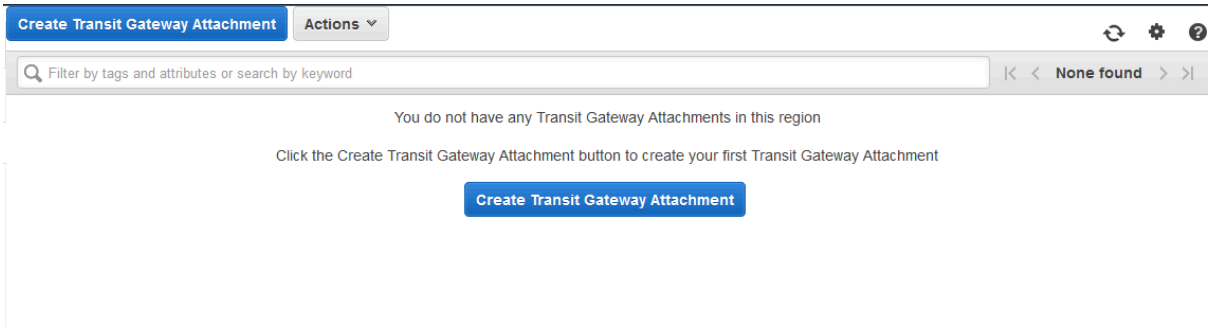




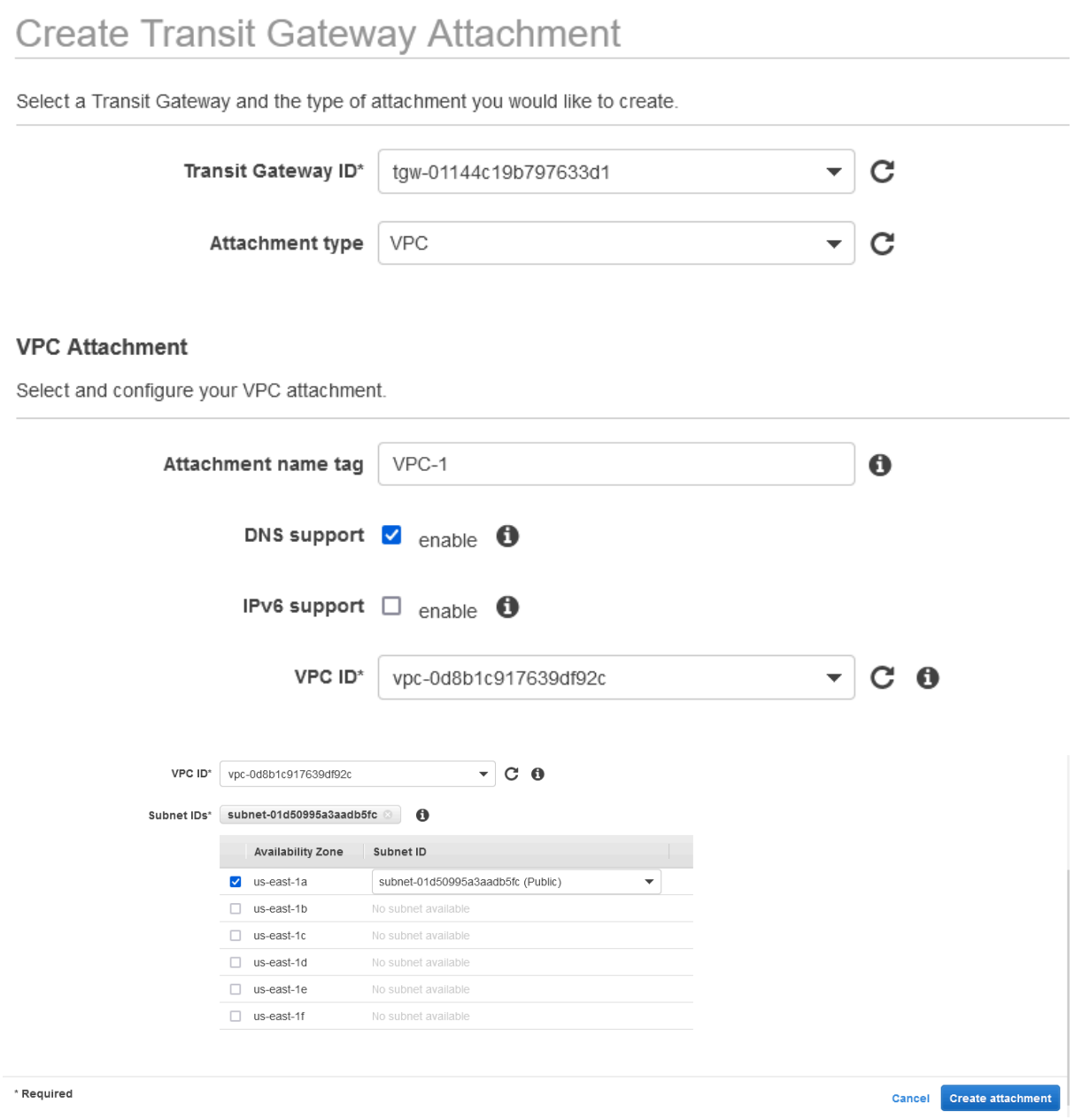
It takes some time to go for available state



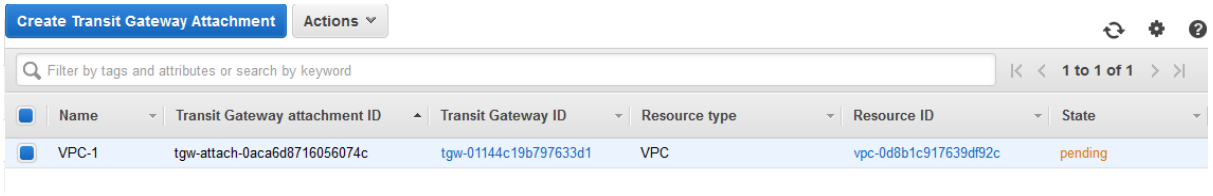
Create a transit gateway attachment for VPC-1 and VPC-2



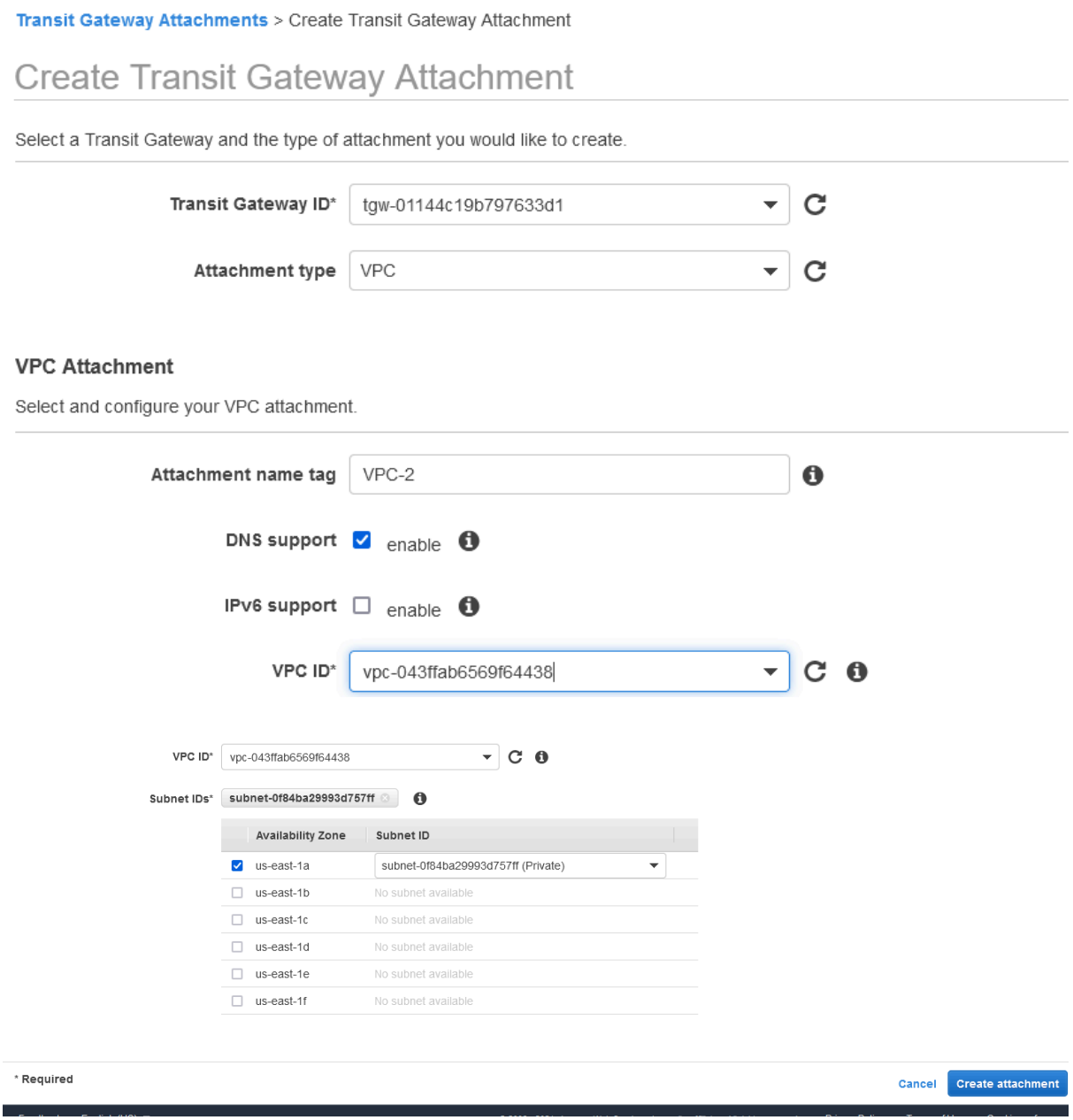
Click on create Transit Gateway Attachment

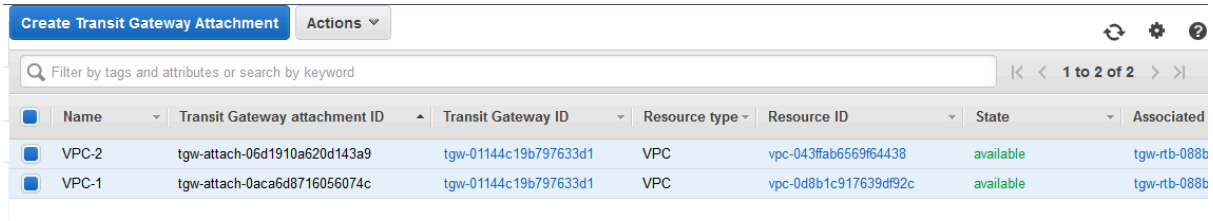


Click on create attachment

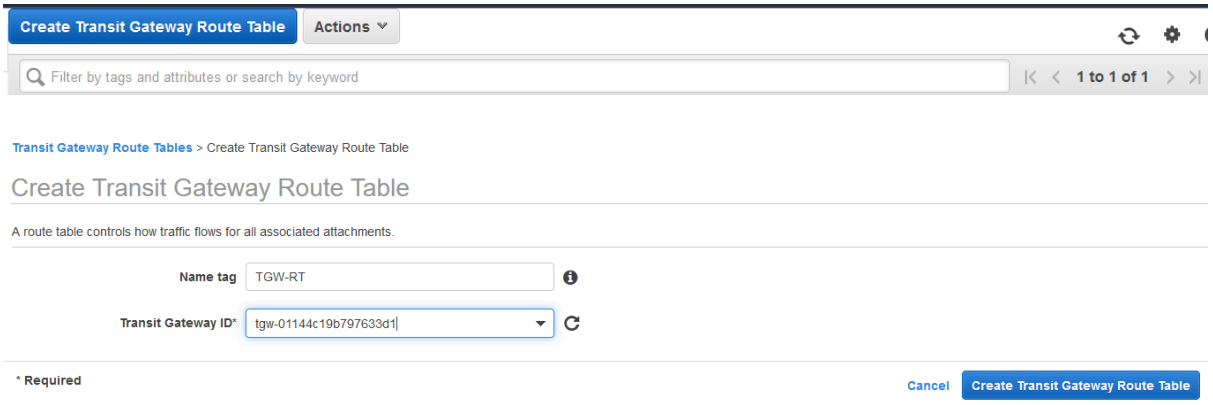


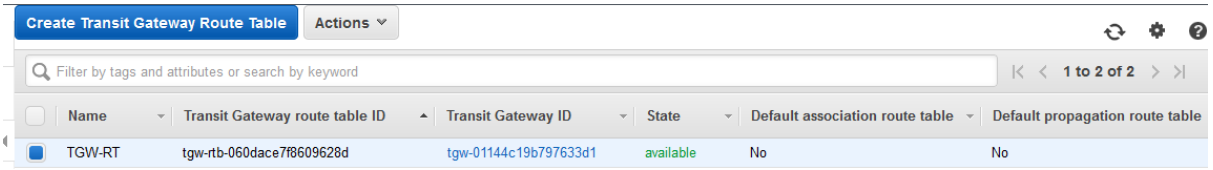
It takes some time to go to available state





Create a single transit gateway route table



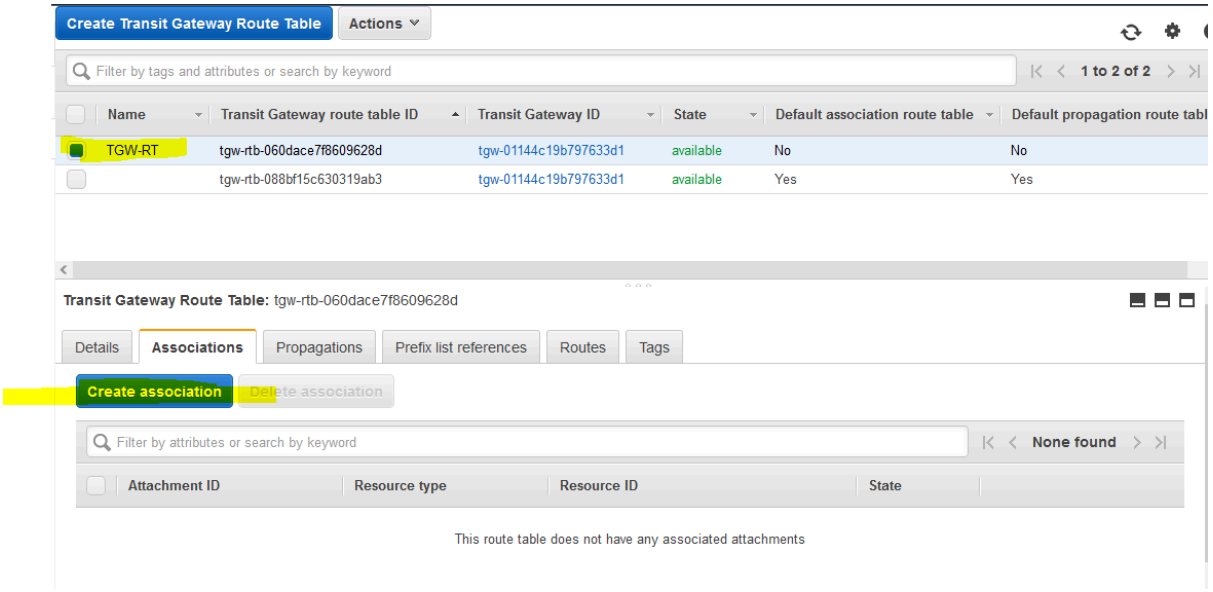


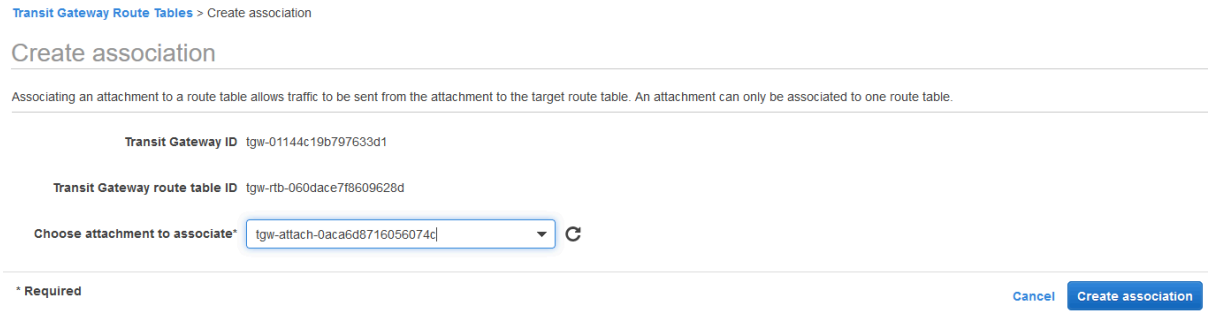
Create 2 transit gateway route table associations

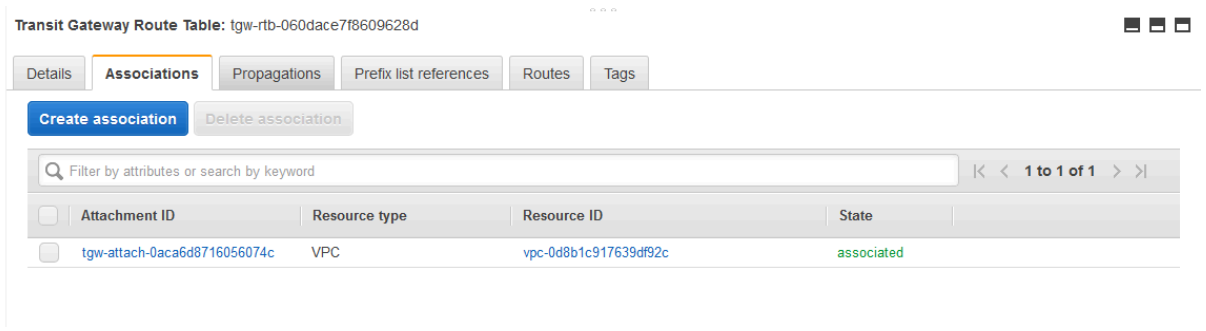
(for VP-1 attachment and VPC-2 attachment)

Select the TGW Route table and in the association tab select create association

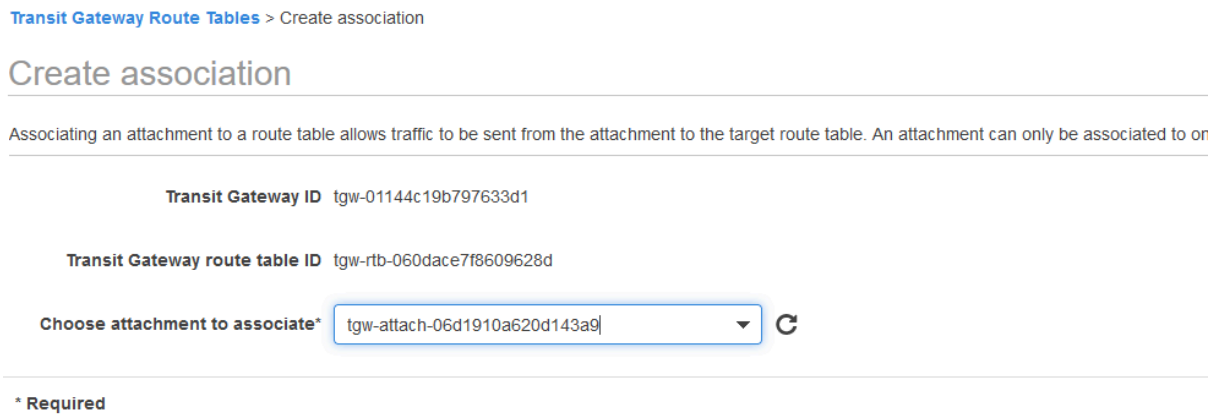
Before attaching route table associcate,when u create a TGW and TGW attachment then all association and propagation will be attached to default RT.Make sure from default RT u delete those association and propagation from those default RT.

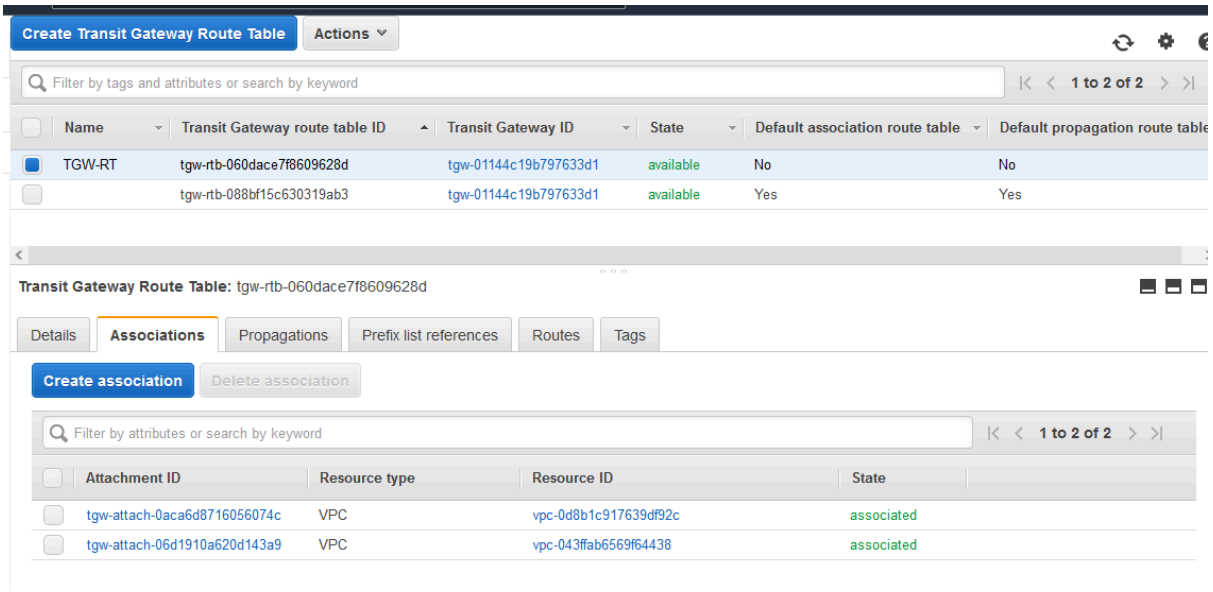




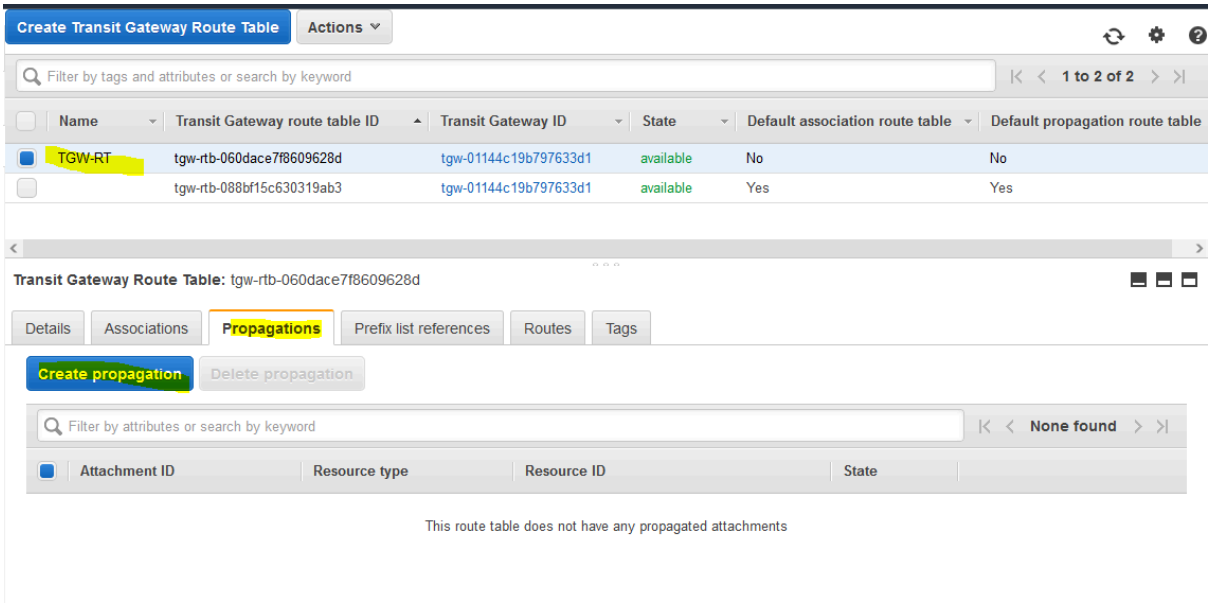


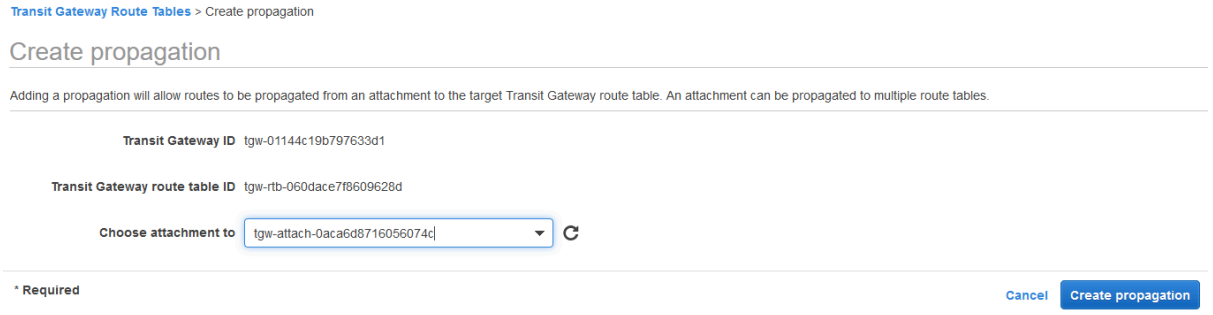
Similarly create for VPC-2

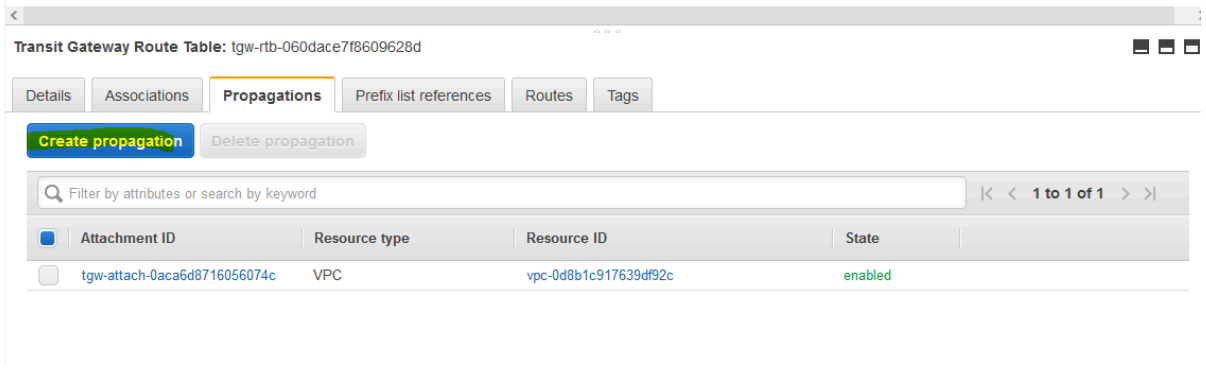




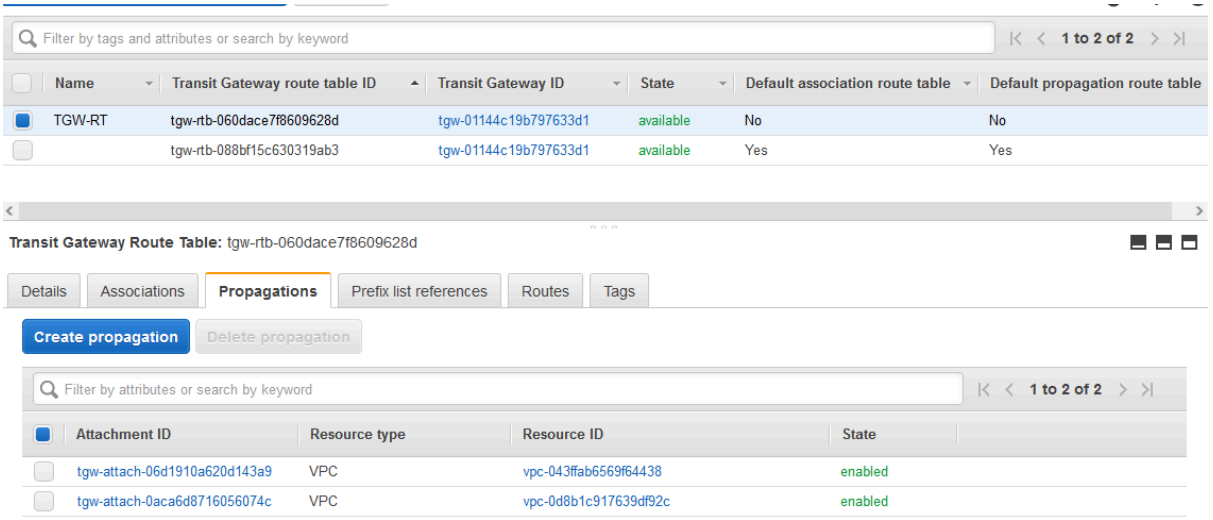
Create 2 transit gateway route table propagation (or VP-1 attachment and VPC-2 attachment)


Create Transit Gateway Route Table
Actions
Filter by tags and attributes or search by keyword
1 to 2 of 2
Name
Transit Gateway route table ID
Transit Gateway ID
State
Default association route table
Default propagation route table
TGW-RT
tgw-rtb-060dace7f8609628d
tgw-01144c19b797633d1
available
No
No
tgw-rtb-088bf15c630319ab3
tgw-01144c19b797633d1
available
Yes
Yes
Transit Gateway Route Table: tgw-rtb-060dace7f8609628d
Details
Associations
Propagations
Prefix list references
Routes
Tags
Create propagation
Delete propagation
Filter by attributes or search by keyword
None found
Attachment ID
Resource type
Resource ID
State
This route table does not have any propagated attachments

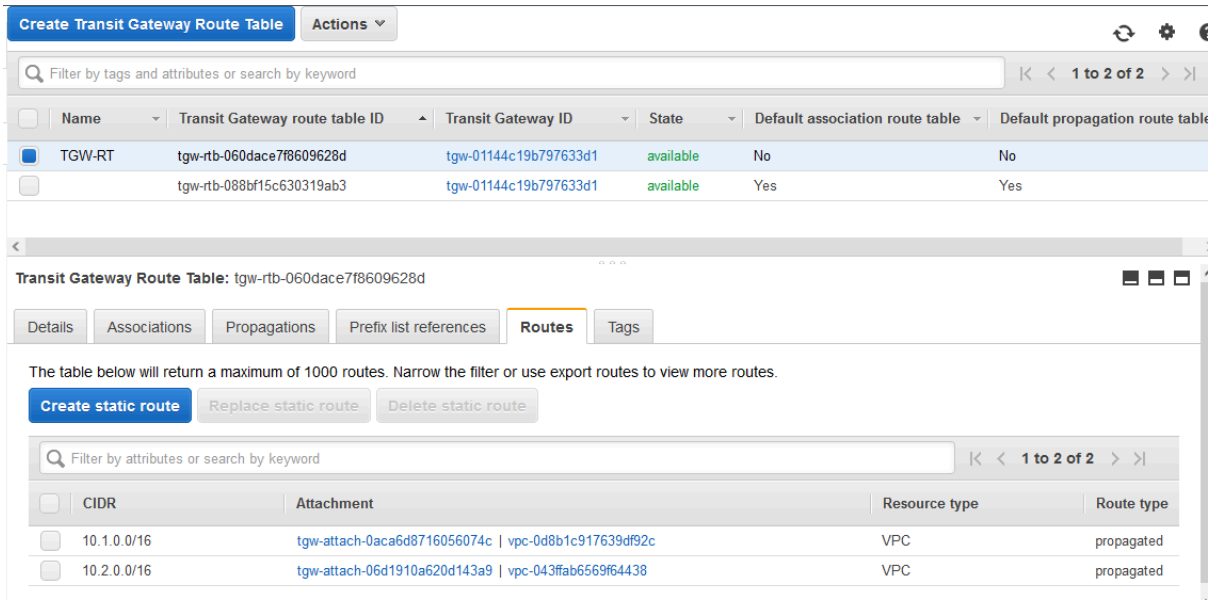

Transit Gateway Route Tables > Create propagation
Create propagation
Adding a propagation will allow routes to be propagated from an attachment to the target Transit Gateway route table. An attachment can be propagated to multiple route tables.
Transit Gateway ID tgw-01144c19b797633d1
Transit Gateway route table ID tgw-rtb-060dace7f8609628d
Choose attachment to tgw-attach-0aca6d8716056074c
* Required
Cancel
Create propagation


Transit Gateway Route Table: tgw-rtb-060dace7f8609628d
Details
Associations
Propagations
Prefix list references
Routes
Tags
Create propagation
Delete propagation
Filter by attributes or search by keyword
1 to 1 of 1
Attachment ID
Resource type
Resource ID
State
tgw-attach-0aca6d8716056074c
VPC
vpc-0d8b1c917639df92c
enabled

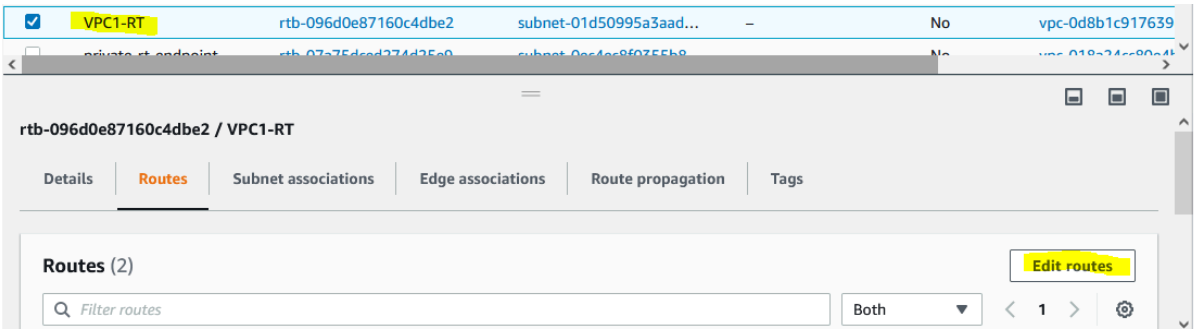
Choose VPC-2



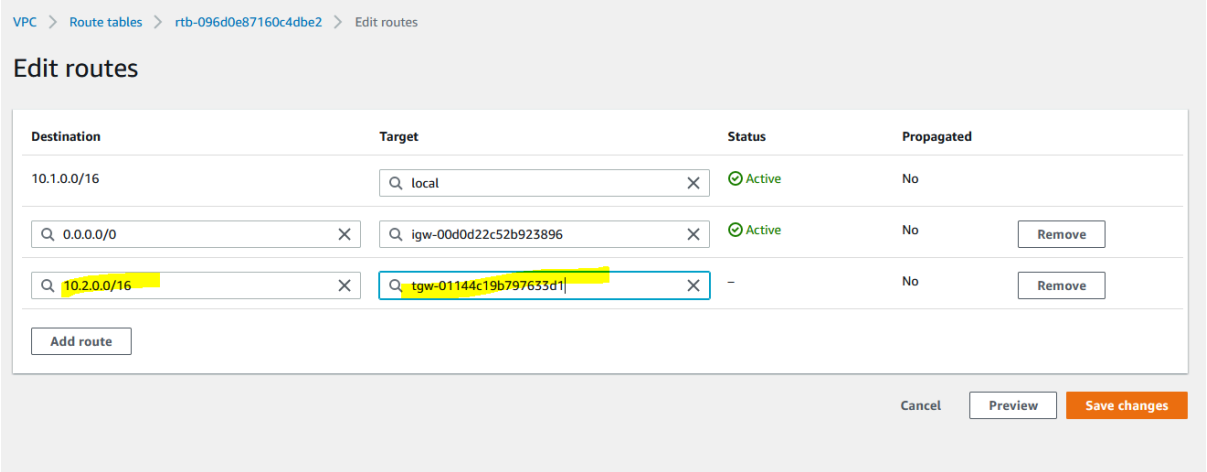
Double check and make under both VPC routes have been propagated “click on routes”

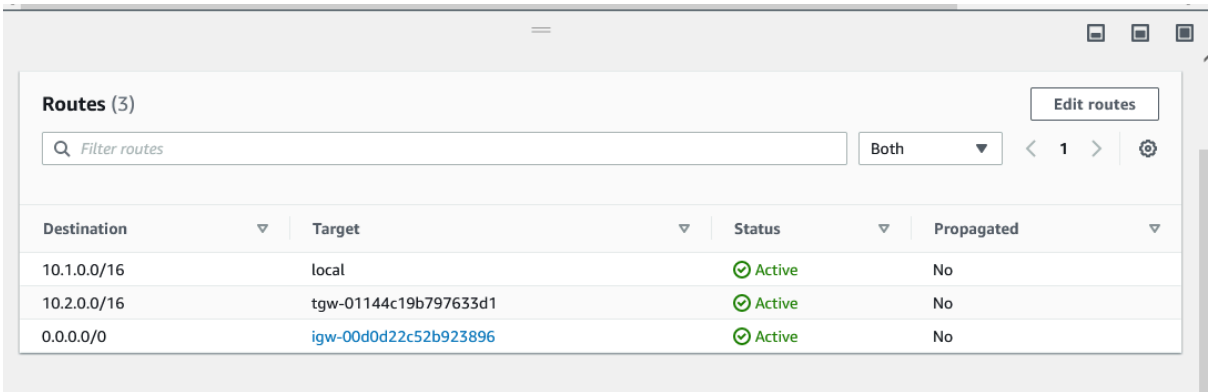


Go to VPC RT and select VPC-1 RT and click on edit routes

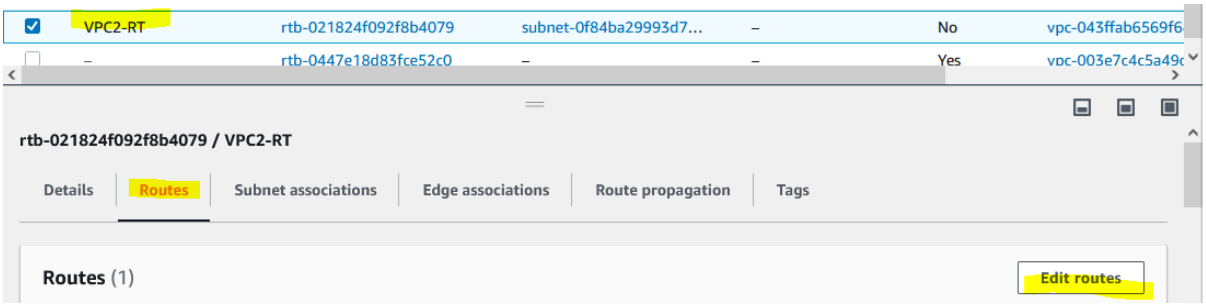


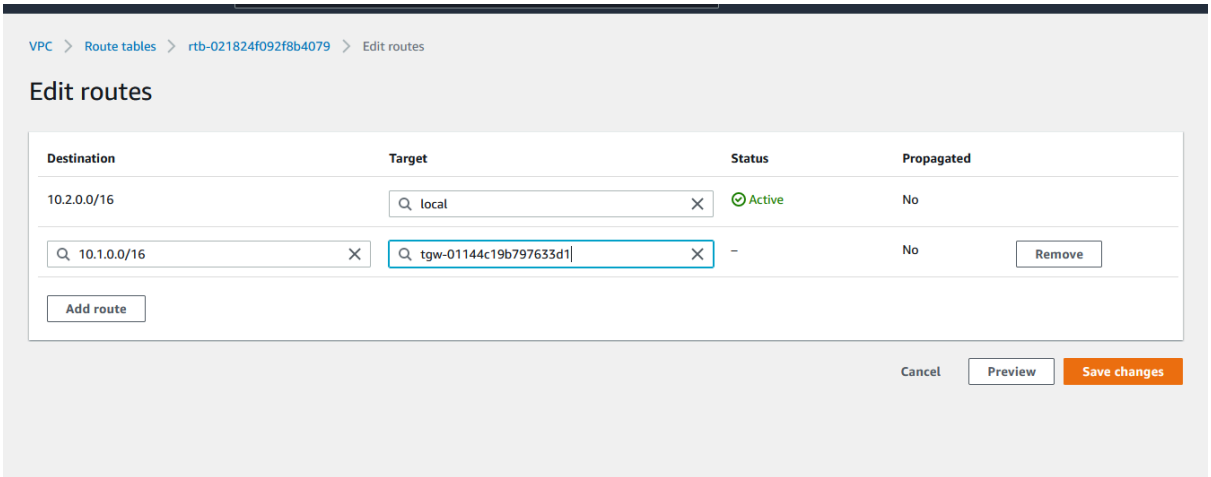
Add the path for VPC-2 CIDR

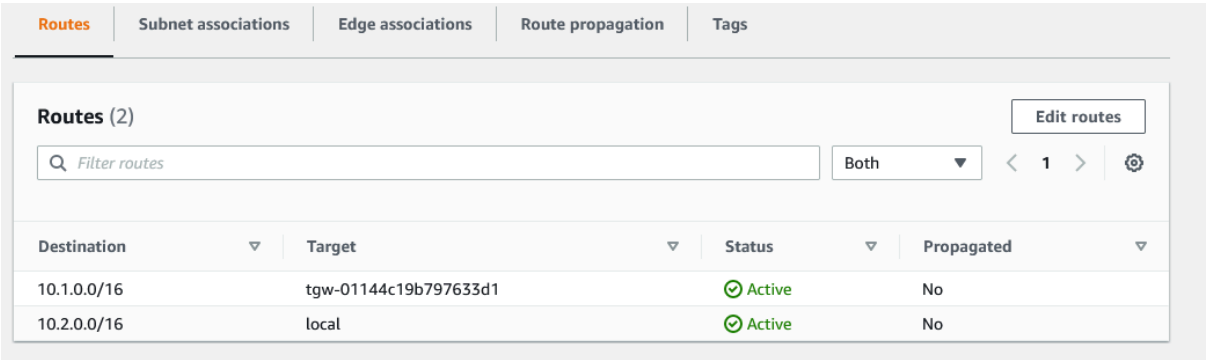




Similarly do for VPC2-RT



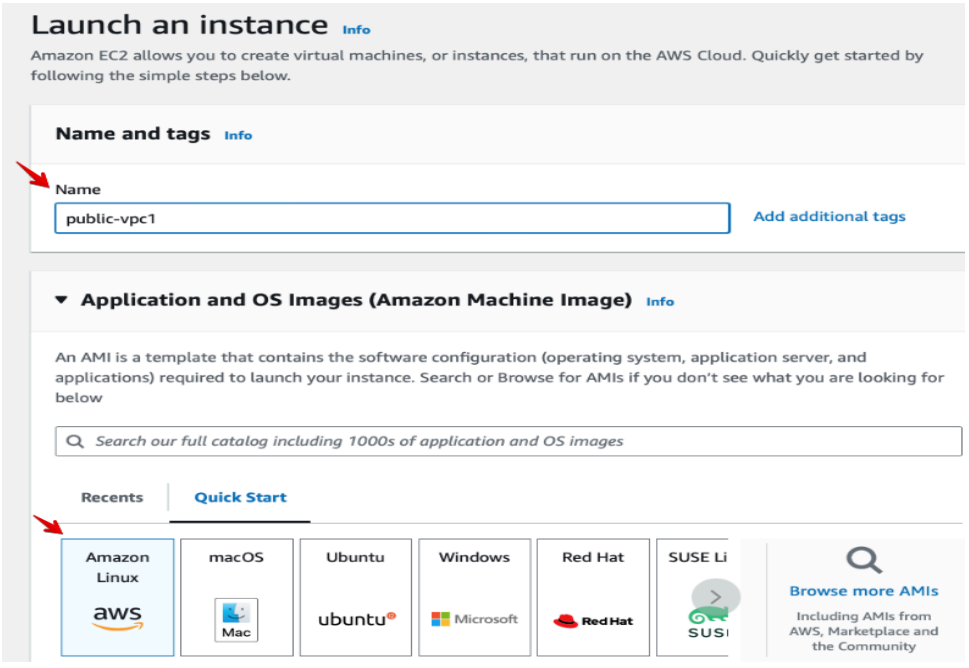




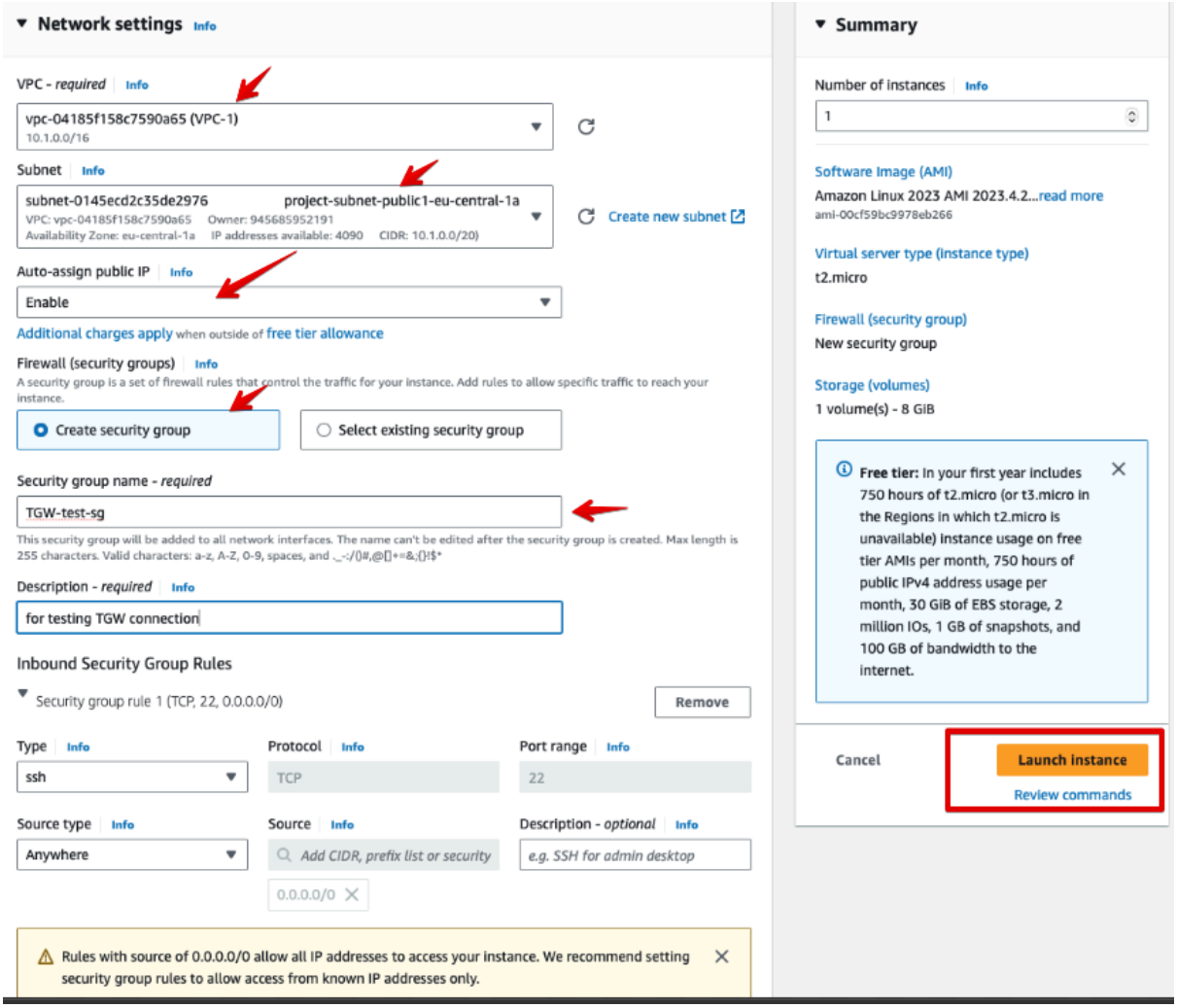
Test connectivity and confirm everything is working as expected

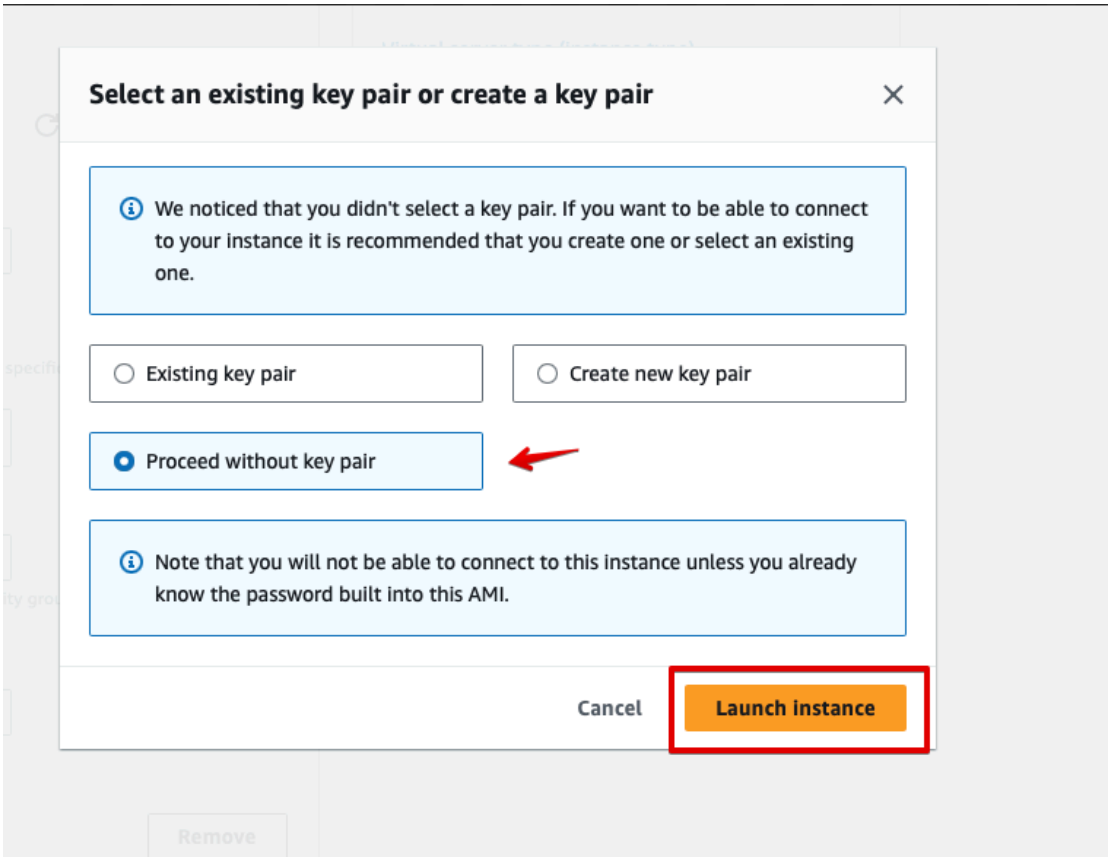
Create 1 instances in VPC-1 and 1 Instance in VPC-2 using the EC2 console

In VPC-1, create public instance

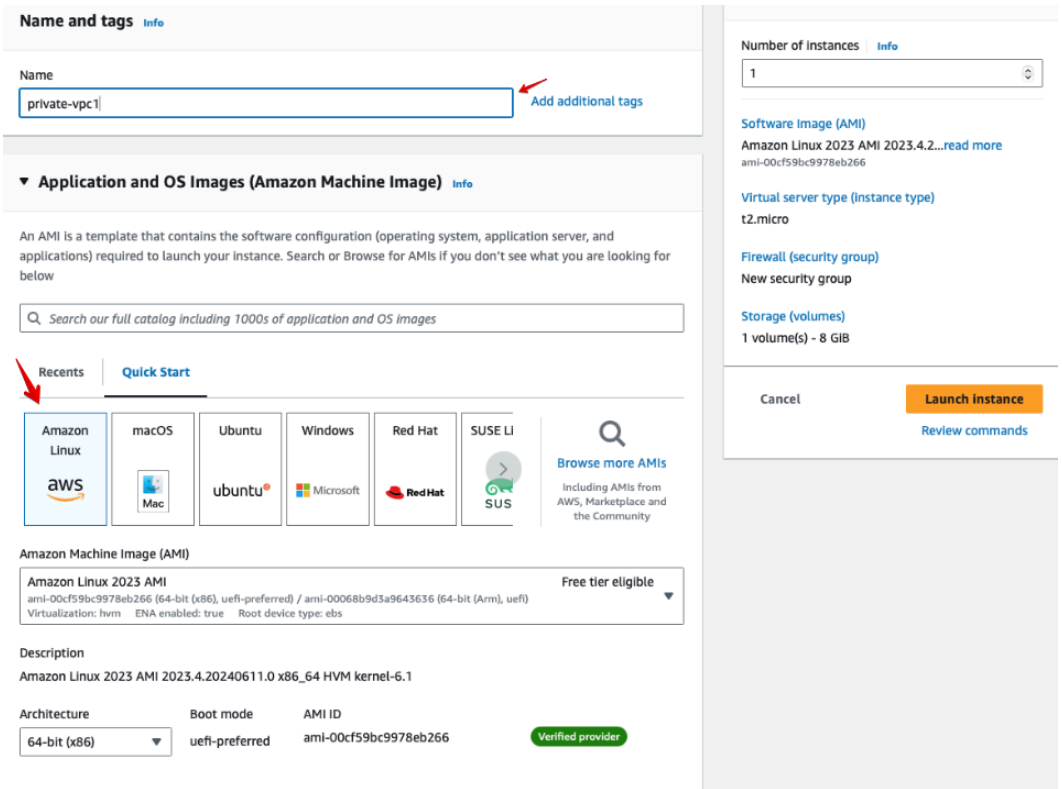


- Leave other settings as default
- Under Network Settings, click on **Edit** and make the following adjustments

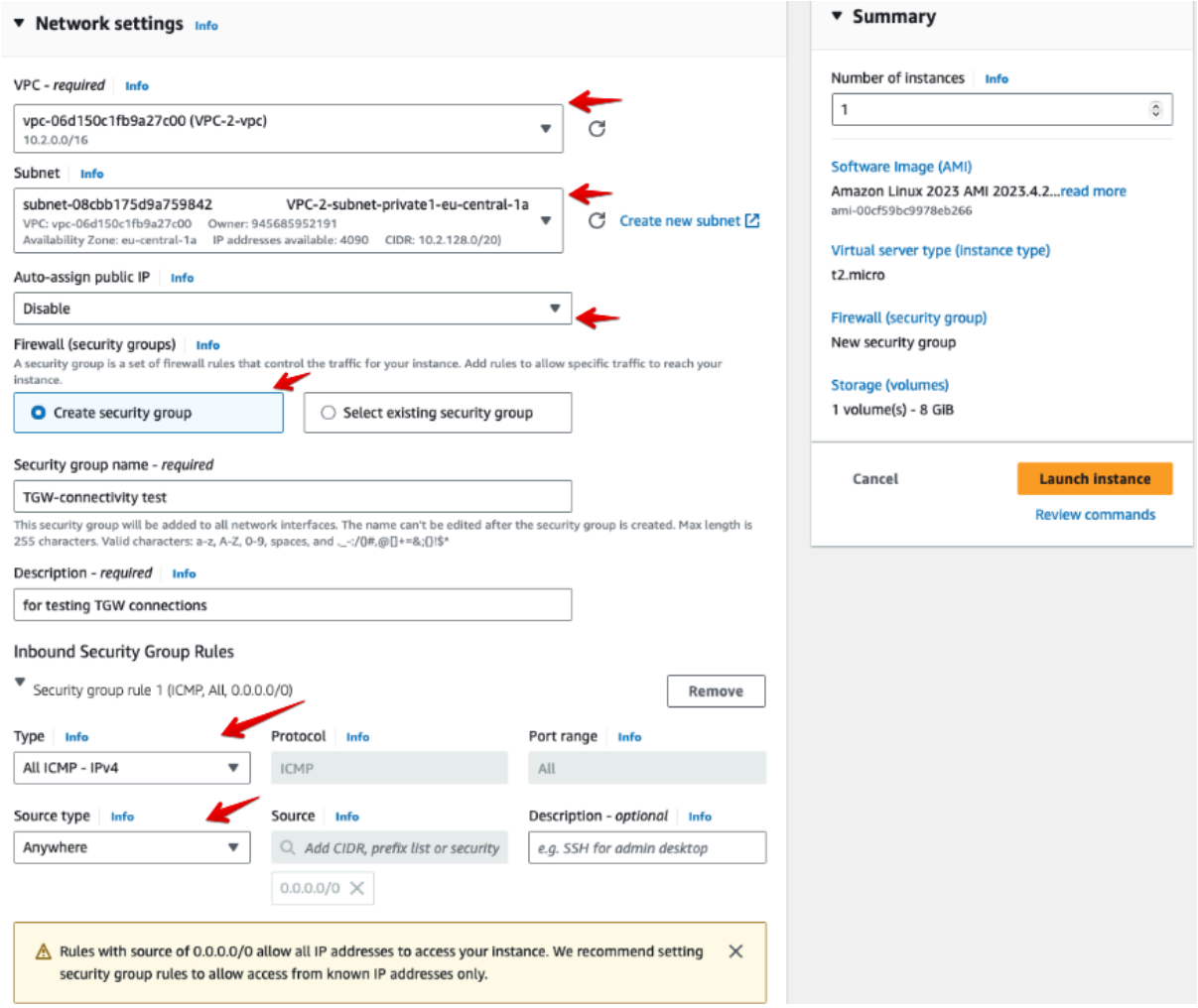




In VPC-2, create private instance

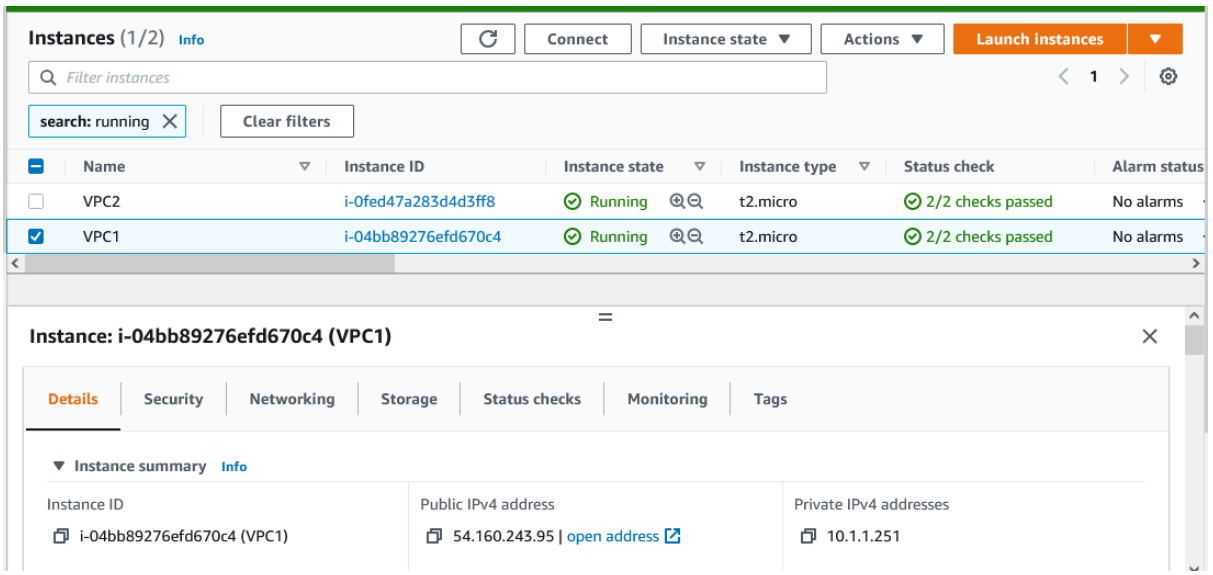


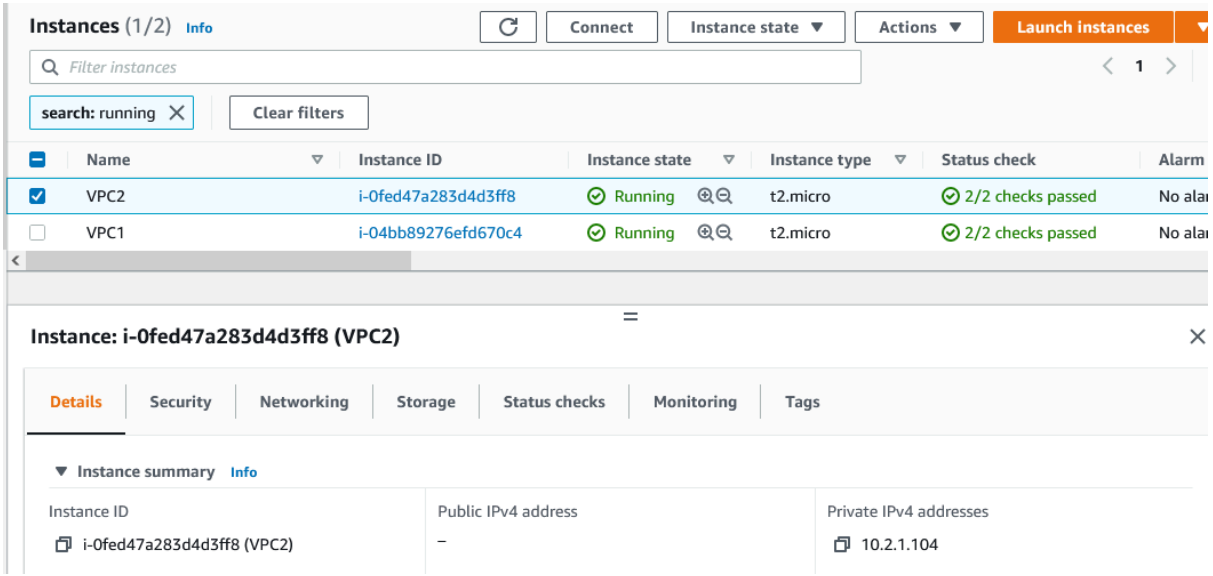
Similar to VPC-1, leave other settings as default and only adjust the network settings in order to create the server (instance) in VPC-2 as shown



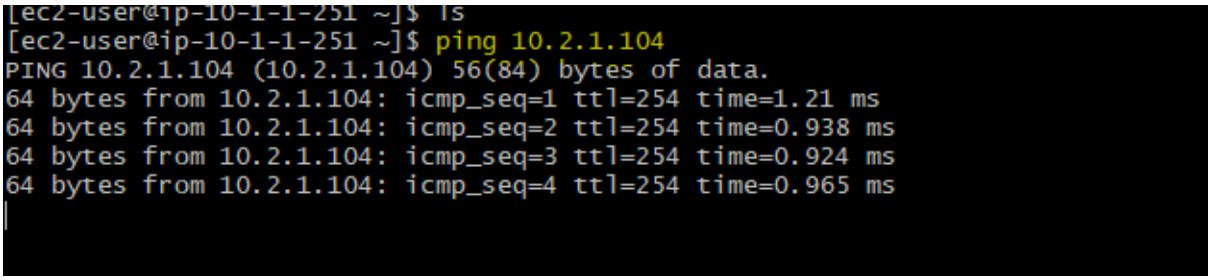
Accept to proceed without keypair and create instance (same as above)

And try to ping instance of VPC_2 from VPC-1 instance



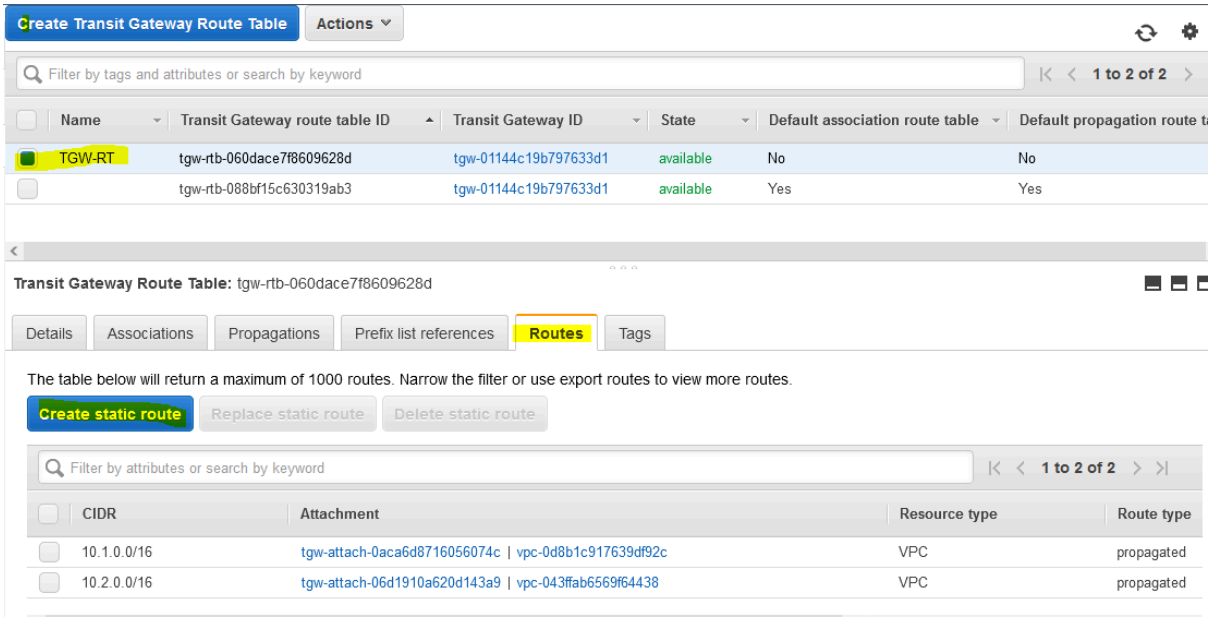


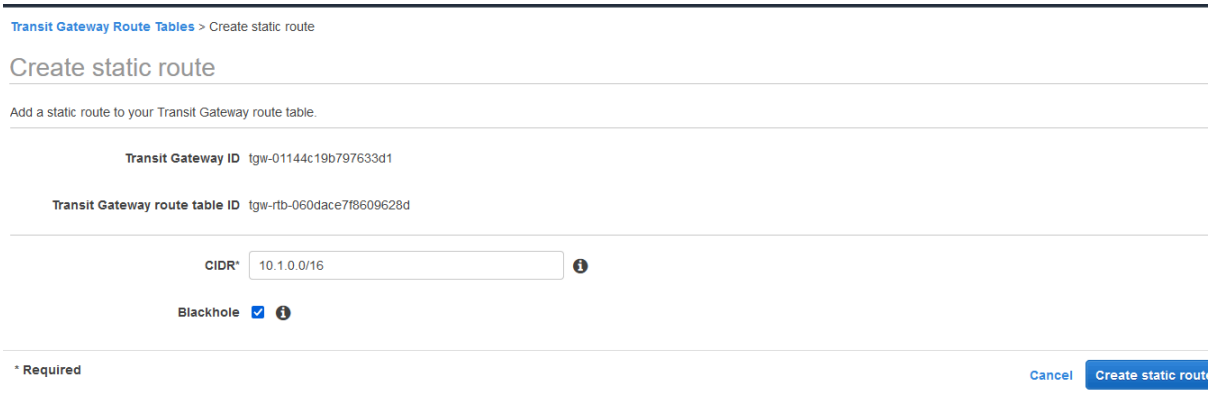
Pinging instance of VPC-2 via private ip of VPC-2 instance

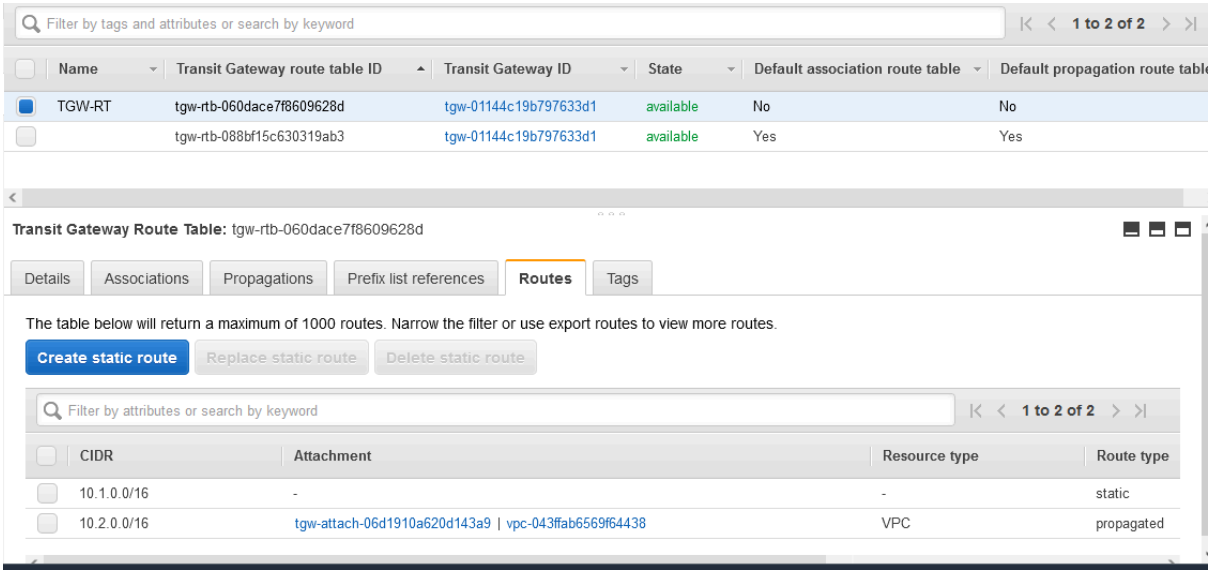


VPC-1 instance is able to connect to VPC_2 instance

Create a static blackhole route to DENY back-to-back communication between VPC-2 and VPC-1

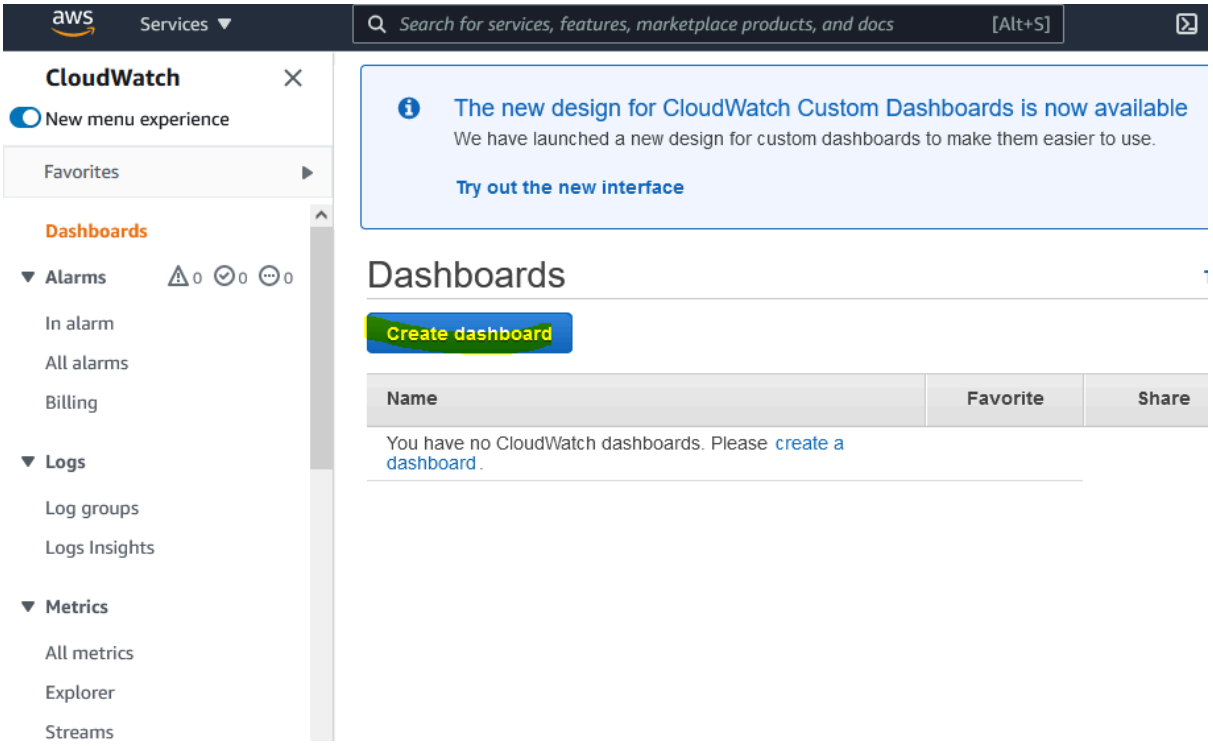


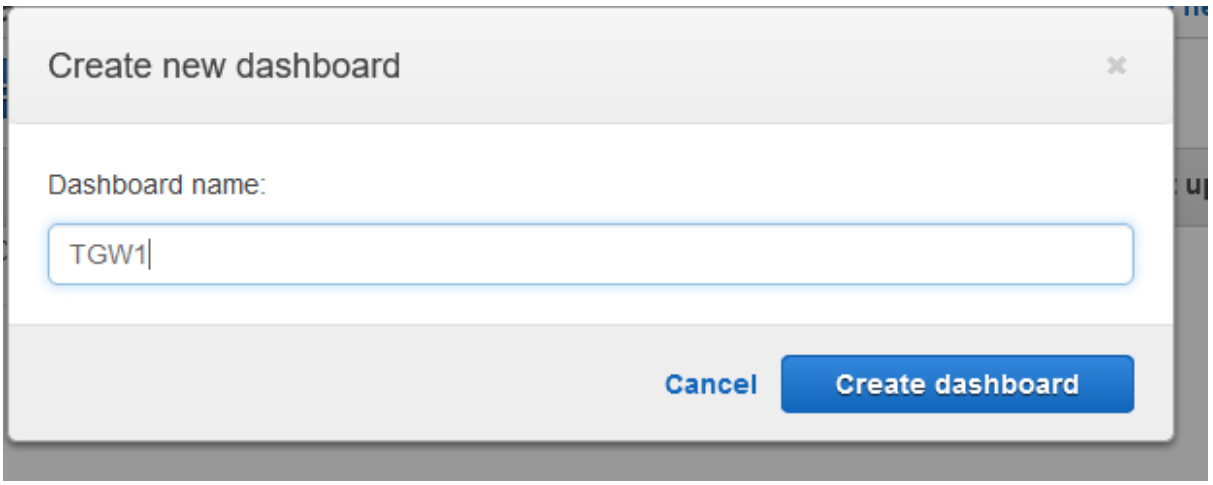


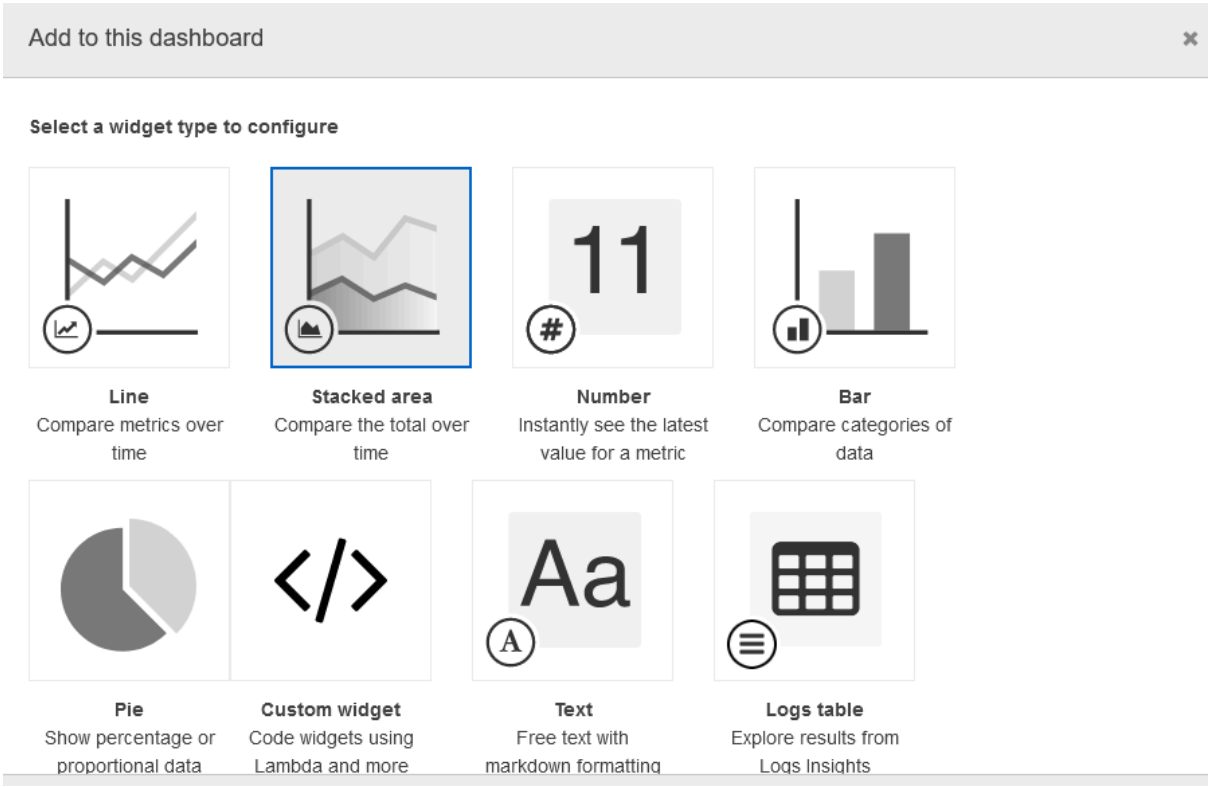


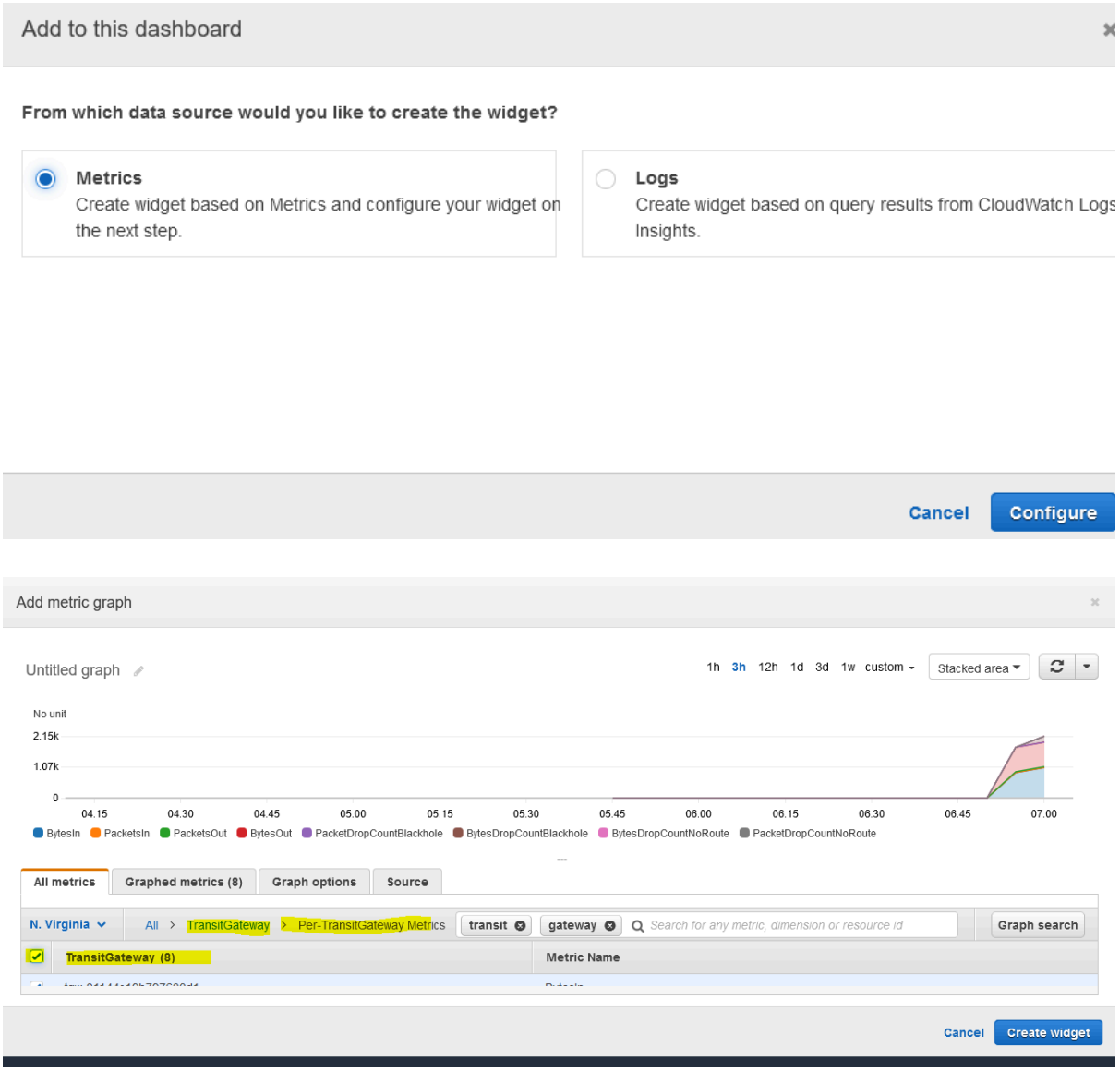
Now when you will ping VPC_2 instance from VPC-1 instance it will show timeout error so we through doing blackhole VPC_1 instance is not able to communicate VPC-2.

Create a CloudWatch Dashboard to monitor your Transit Gateway packets metrics.

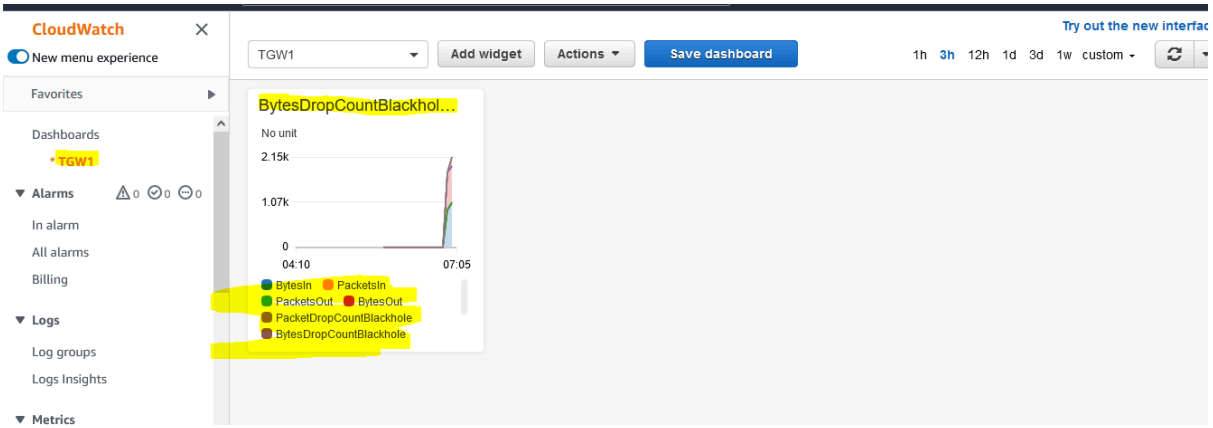



Create new dashboard
Dashboard name:
TGW1
Cancel
Create dashboard


Add to this dashboard
Select a widget type to configure
Line
Compare metrics over time
Stacked area
Compare the total over time
Number
Instantly see the latest value for a metric
Bar
Compare categories of data
Pie
Show percentage or proportional data
Custom widget
Code widgets using Lambda and more
Text
Free text with markdown formatting
Logs table
Explore results from Logs Insights


Add to this dashboard
From which data source would you like to create the widget?
Metrics
Create widget based on Metrics and configure your widget on the next step.
Logs
Create widget based on query results from CloudWatch Logs Insights.
Cancel
Configure

Add metric graph
Untitled graph
1h 3h 12h 1d 3d 1w custom
Stacked area
No unit
2.15k
1.07k
0
04:15 04:30 04:45 05:00 05:15 05:30 05:45 06:00 06:15 06:30 06:45 07:00
BytesIn PacketsIn PacketsOut BytesOut PacketDropCountBlackhole BytesDropCountBlackhole BytesDropCountNoRoute PacketDropCountNoRoute
All metrics
Graphed metrics (8)
Graph options
Source
N. Virginia
All > TransitGateway > Per-TransitGateway Metrics
transit
gateway
Search for any metric, dimension or resource id
Graph search
TransitGateway (8)
Metric Name
Cancel
Create widget


CloudWatch
New menu experience
Favorites
Dashboards
TGW1
Alarms
In alarm
All alarms
Billing
Logs
Log groups
Logs Insights
Metrics
TGW1
Add widget
Actions
Save dashboard
1h 3h 12h 1d 3d 1w custom
BytesDropCountBlackhol...
No unit
2.15k
1.07k
0
04:10 07:05
BytesIn PacketsIn
PacketsOut BytesOut
PacketDropCountBlackhole
BytesDropCountBlackhole