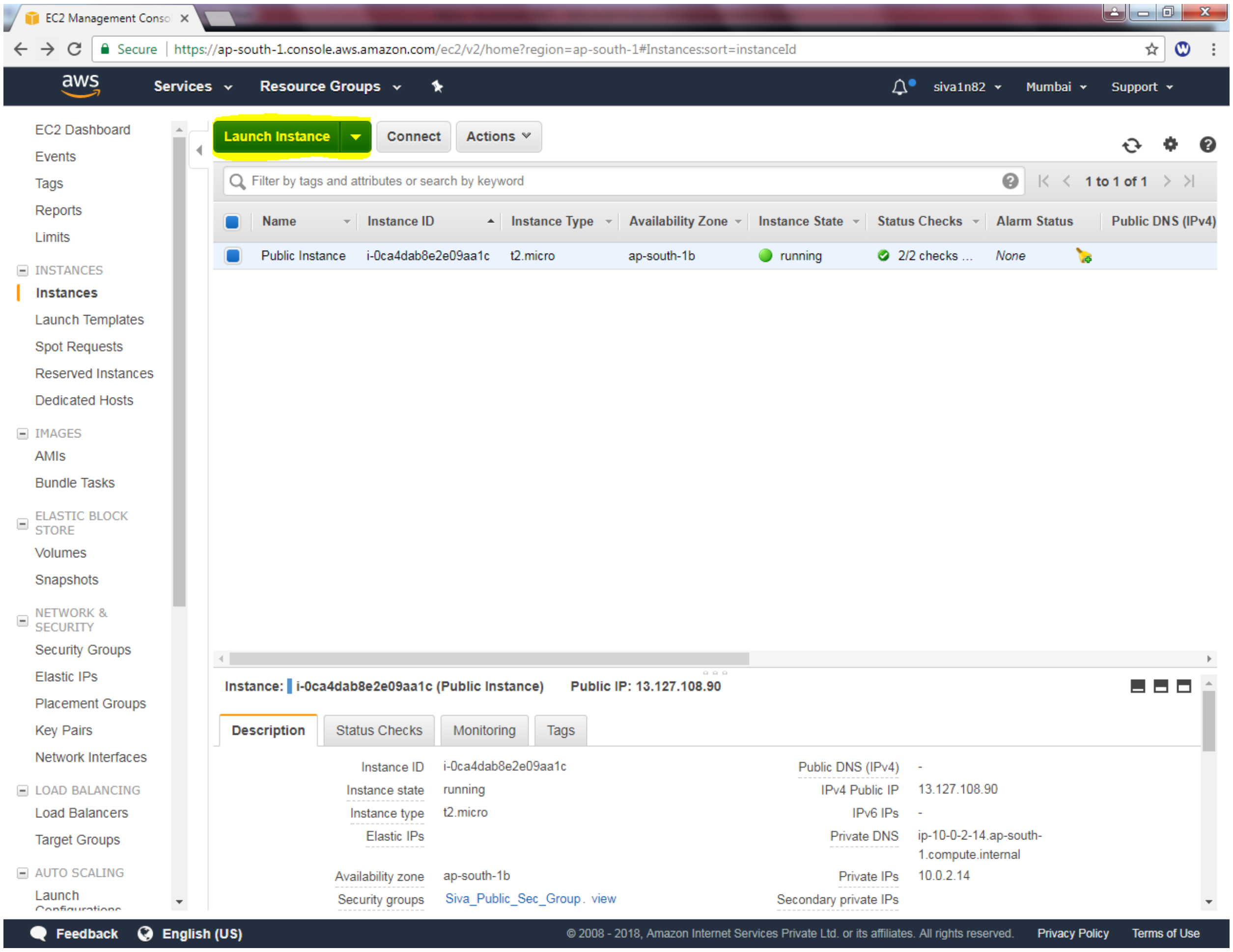
Note: It's continuity of Internet gateway lab, Need to delete the Nat gateway and release the Elastic IP once scenario has been completed. Otherwise charges will be applicable for Elastic IP. If you are facing any challenges please contact our whatsapp group.

Lab: Need to access internet from Private Network.

Goto EC2 Dashboard, select instances and click **"Launch Instance"**

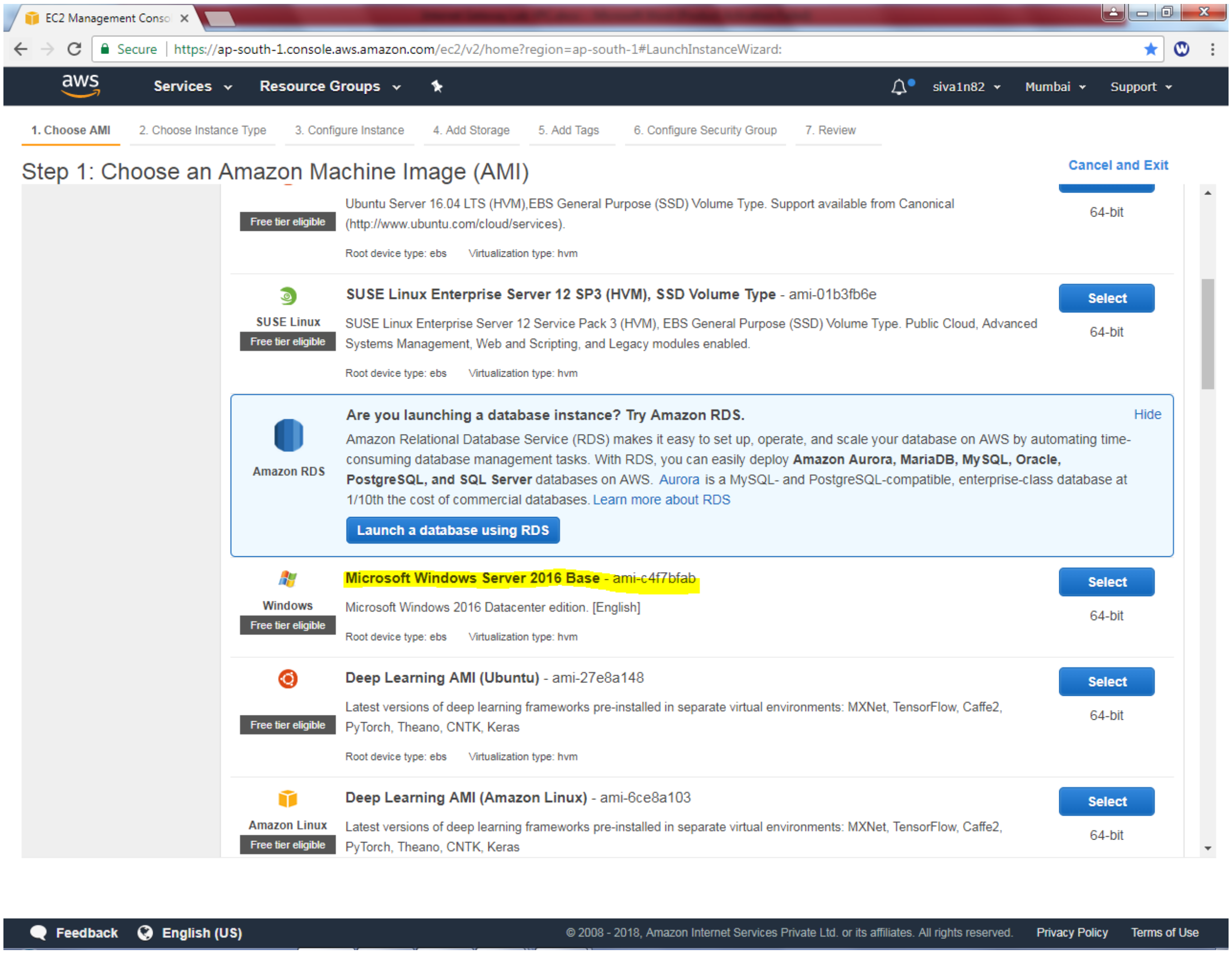


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Public Instance	i-0ca4dab8e2e09aa1c	t2.micro	ap-south-1b	running	2/2 checks ...	None	

Instance: i-0ca4dab8e2e09aa1c (Public Instance)   Public IP: 13.127.108.90

Instance ID	i-0ca4dab8e2e09aa1c	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	13.127.108.90
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-2-14.ap-south-1.compute.internal
Availability zone	ap-south-1b	Private IPs	10.0.2.14
Security groups	Siva_Public_Sec_Group. view	Secondary private IPs	

In AMI, select "Microsoft windows server 2016-Base"



Step 1: Choose an Amazon Machine Image (AMI)

Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Root device type: ebs Virtualization type: hvm

64-bit

SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-01b3fb6e

SUSE Linux Enterprise Server 12 Service Pack 3 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.

Root device type: ebs Virtualization type: hvm

64-bit

Are you launching a database instance? Try Amazon RDS.

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora, MariaDB, MySQL, Oracle, PostgreSQL, and SQL Server** databases on AWS. Aurora is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. Learn more about RDS

Microsoft Windows Server 2016 Base - ami-c4f7bfab

Microsoft Windows 2016 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm

64-bit

Deep Learning AMI (Ubuntu) - ami-27e8a148

Latest versions of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe2, PyTorch, Theano, CNTK, Keras

Root device type: ebs Virtualization type: hvm

64-bit

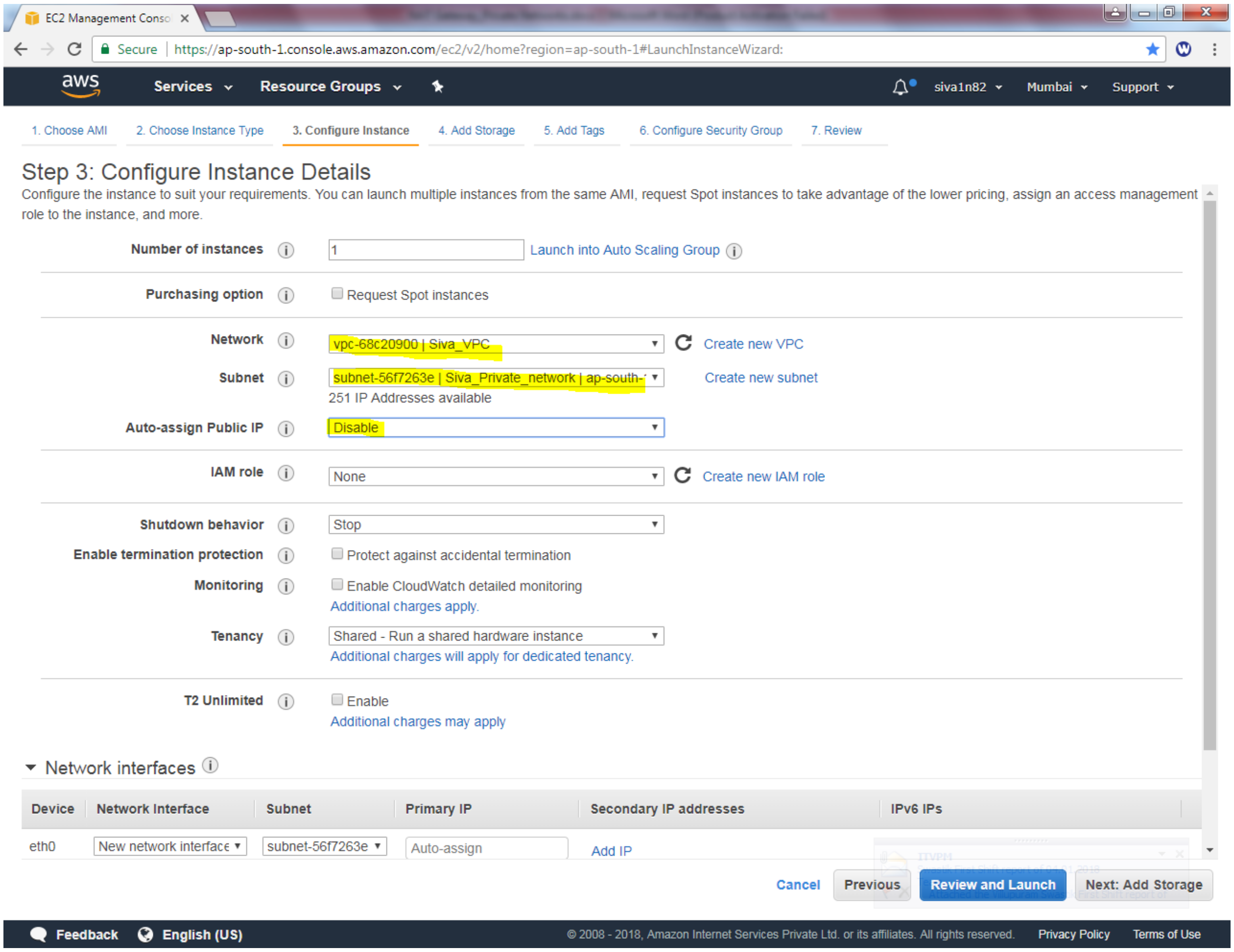
Deep Learning AMI (Amazon Linux) - ami-6ce8a103

Latest versions of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe2, PyTorch, Theano, CNTK, Keras

64-bit

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

In Configure instance, Select **“Siva_VPC”** in network, ”**Siva_Private_Subnet”** in Subnet and “Disable“ option in Auto-assign Public IP.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

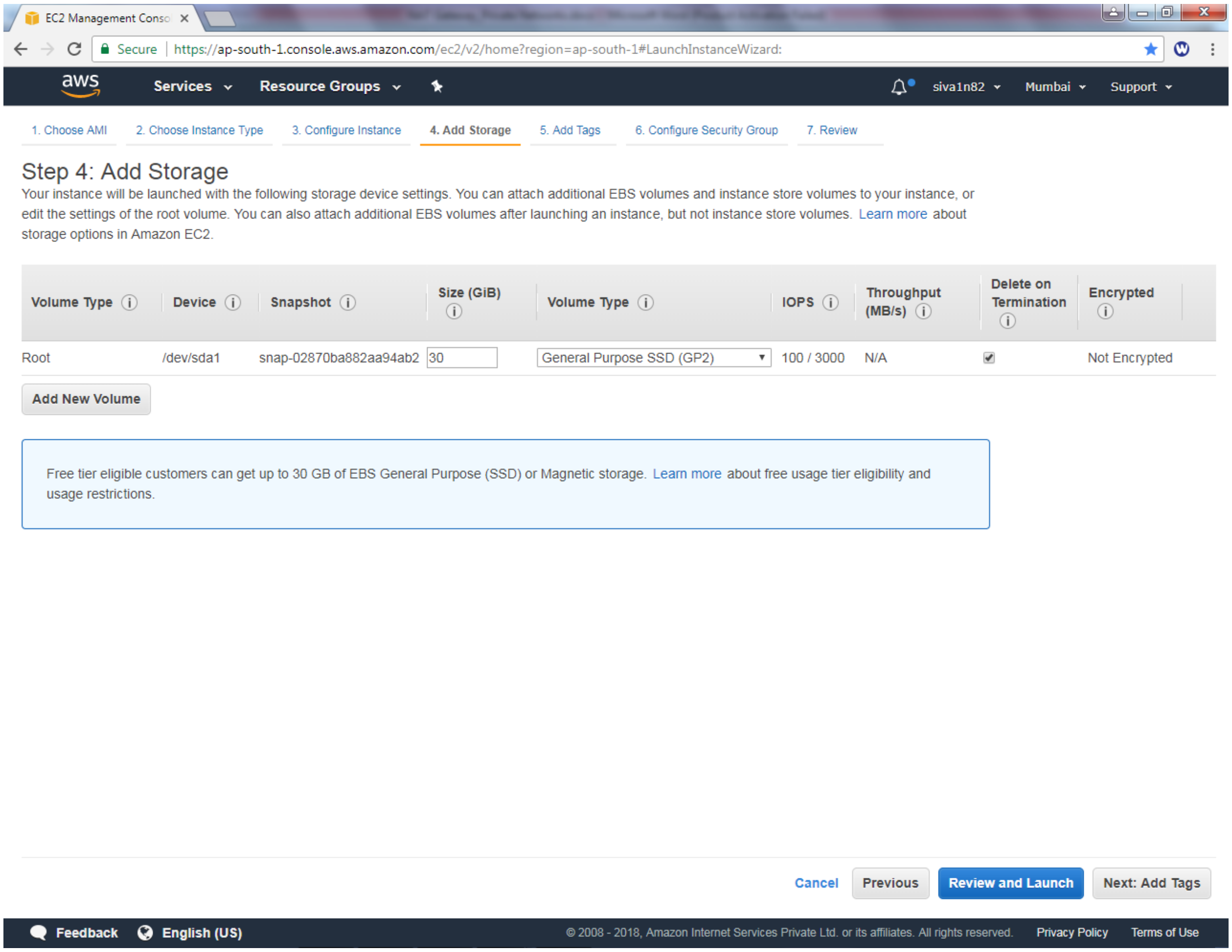
Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-68c20900 | Siva_VPC — Create new VPC
Subnet	subnet-56f7263e | Siva_Private_network | ap-south-1 — Create new subnet 251 IP Addresses available
Auto-assign Public IP	Disable
IAM role	None — Create new IAM role
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
T2 Unlimited	□ Enable Additional charges may apply

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-56f7263e	Auto-assign	Add IP	

Click “Next”.

Leave the settings as default



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-02870ba882aa94ab2	30	General Purpose SSD (GP2)	100 / 3000	N/A	☑	Not Encrypted

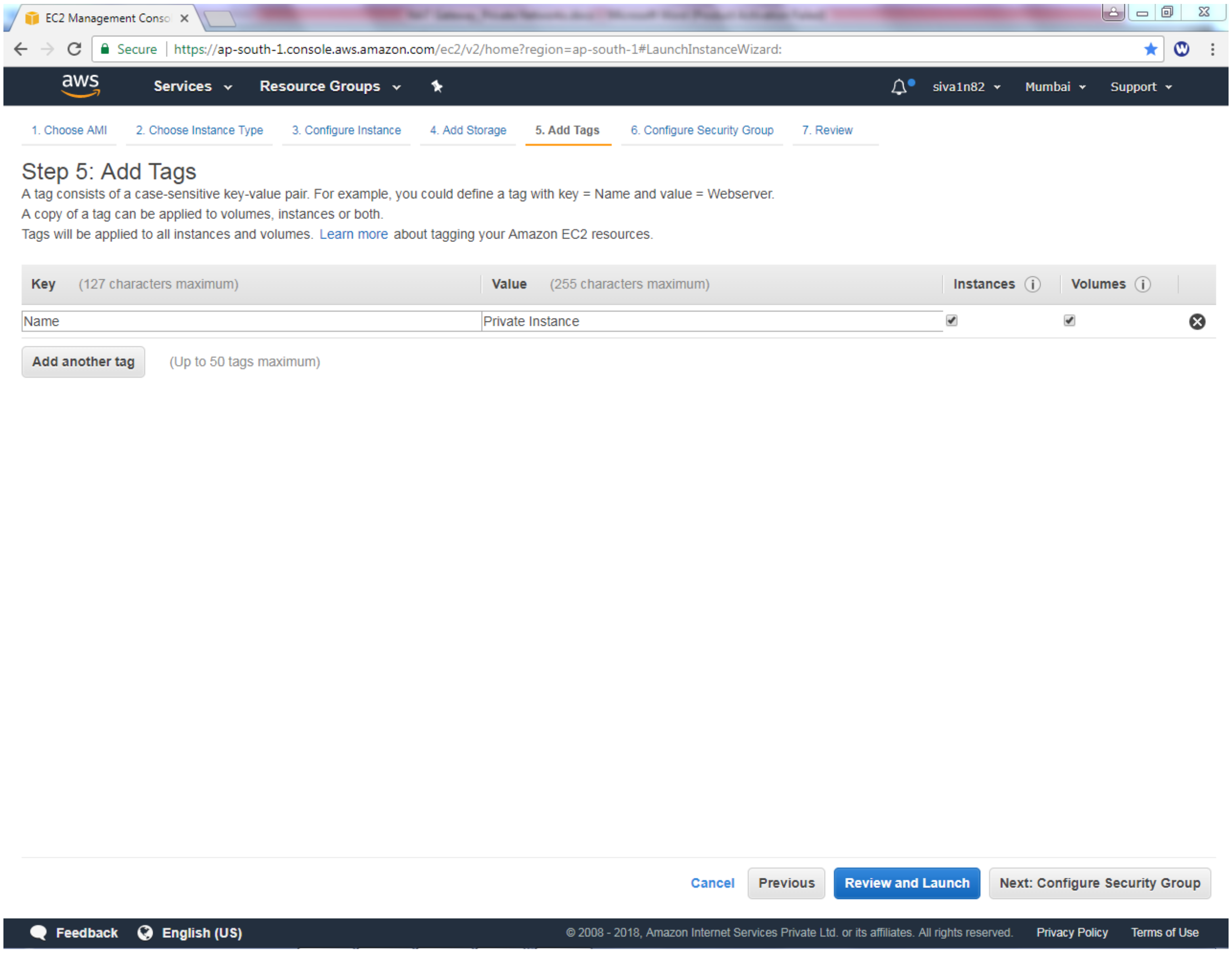
Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Cancel
Previous
Review and Launch
Next: Add Tags
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Click “Next”.

In Add tag, Key value as “Name” and Value as “Private Instance”.



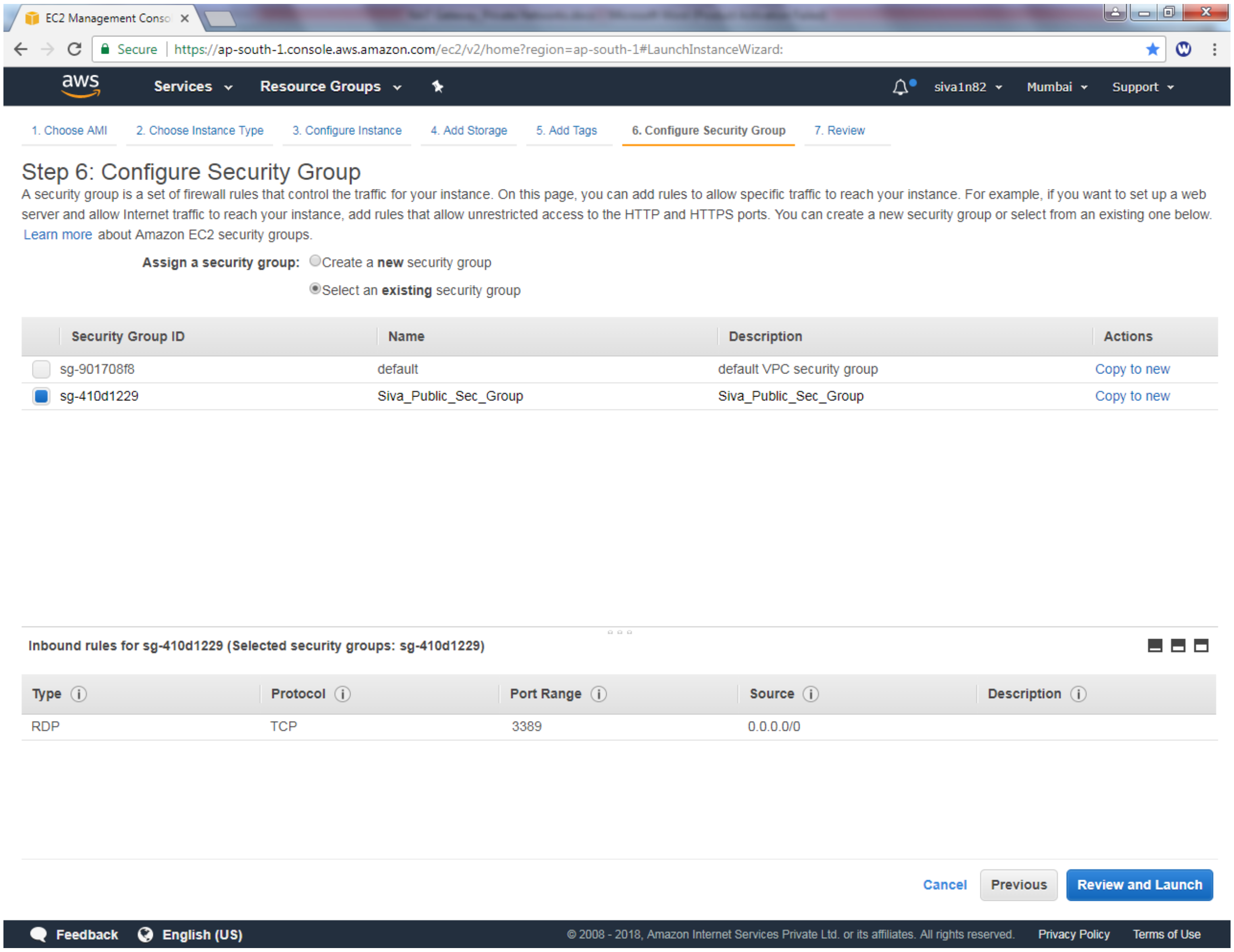
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes
Name	Private Instance	☑	☑

Add another tag
(Up to 50 tags maximum)
Cancel
Previous
Review and Launch
Next: Configure Security Group
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

In Configure security group, select “Siva_Public_Sec_Group”.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description	Actions
□	sg-901708f8	default	default VPC security group	Copy to new
☑	sg-410d1229	Siva_Public_Sec_Group	Siva_Public_Sec_Group	Copy to new

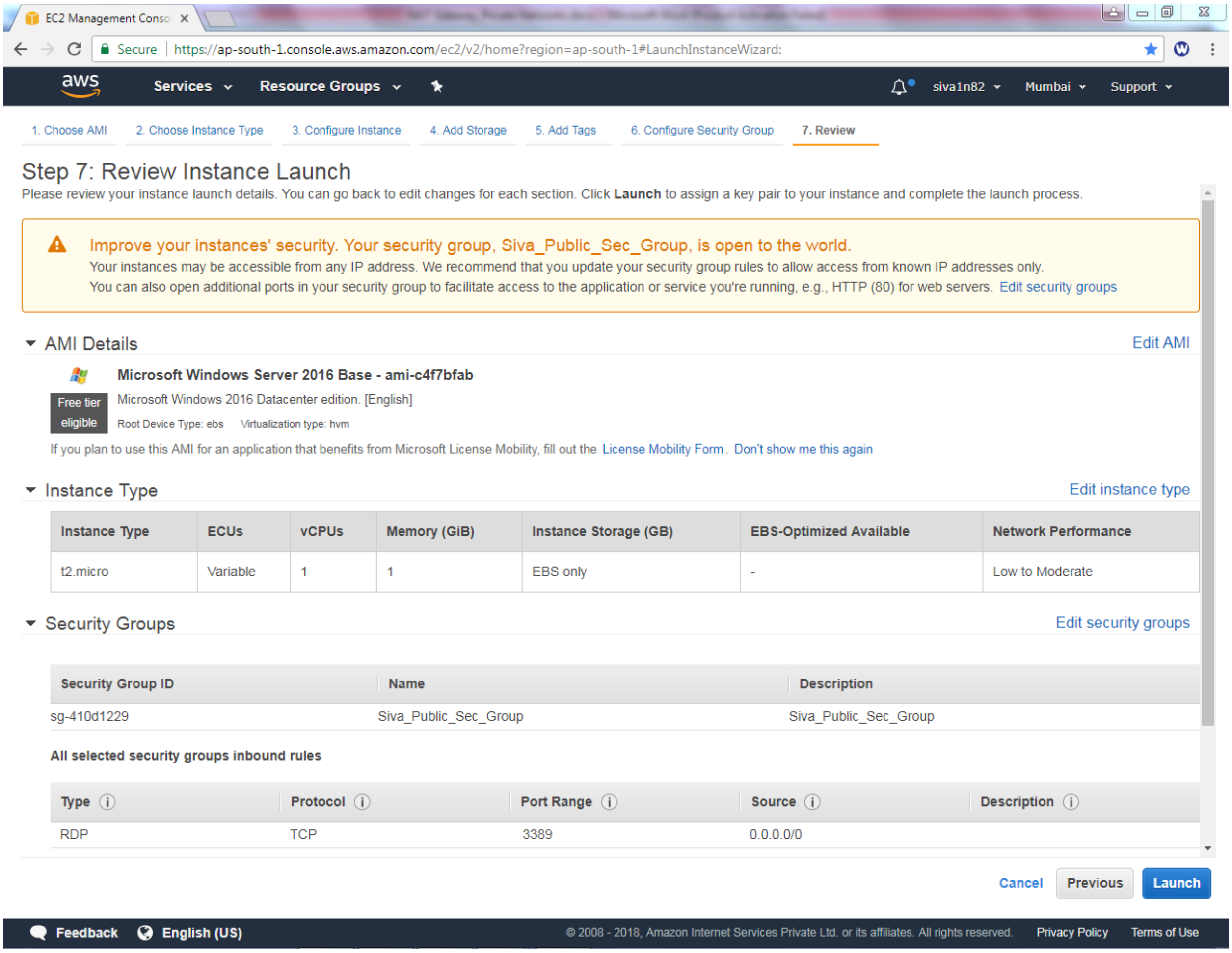
Inbound rules for sg-410d1229 (Selected security groups: sg-410d1229)

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	0.0.0.0/0	

Cancel
Previous
Review and Launch
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Click “Review and Launch”.

Leave the settings as default.



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, Siva_Public_Sec_Group, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details — Edit AMI

Microsoft Windows Server 2016 Base - ami-c4f7bfab
Free tier eligible
Microsoft Windows 2016 Datacenter edition. [English]
Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. Don't show me this again

Instance Type — Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups — Edit security groups

Security Group ID	Name	Description
sg-410d1229	Siva_Public_Sec_Group	Siva_Public_Sec_Group

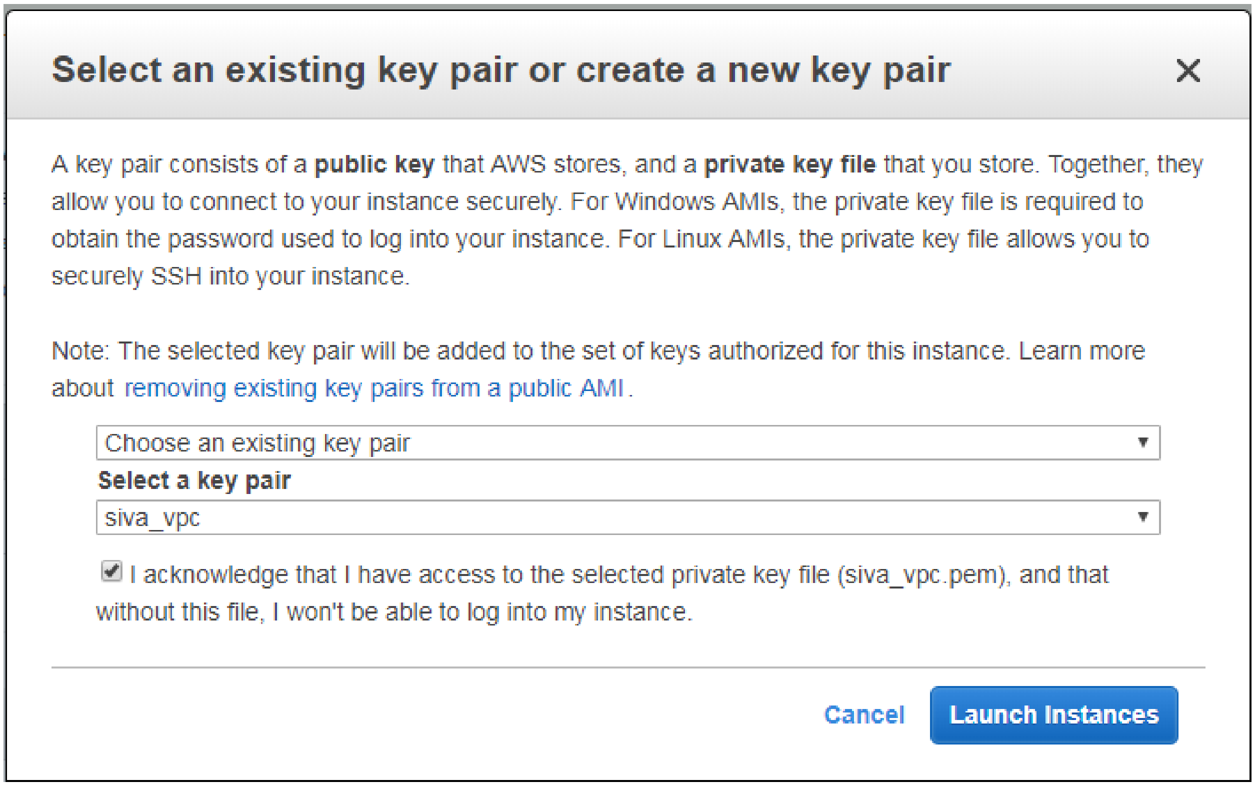
All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	0.0.0.0/0	

Cancel
Previous
Launch
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Click “Launch”.

Select a existing key pair and select the key pair. Acknowledge the access of key.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair ▾

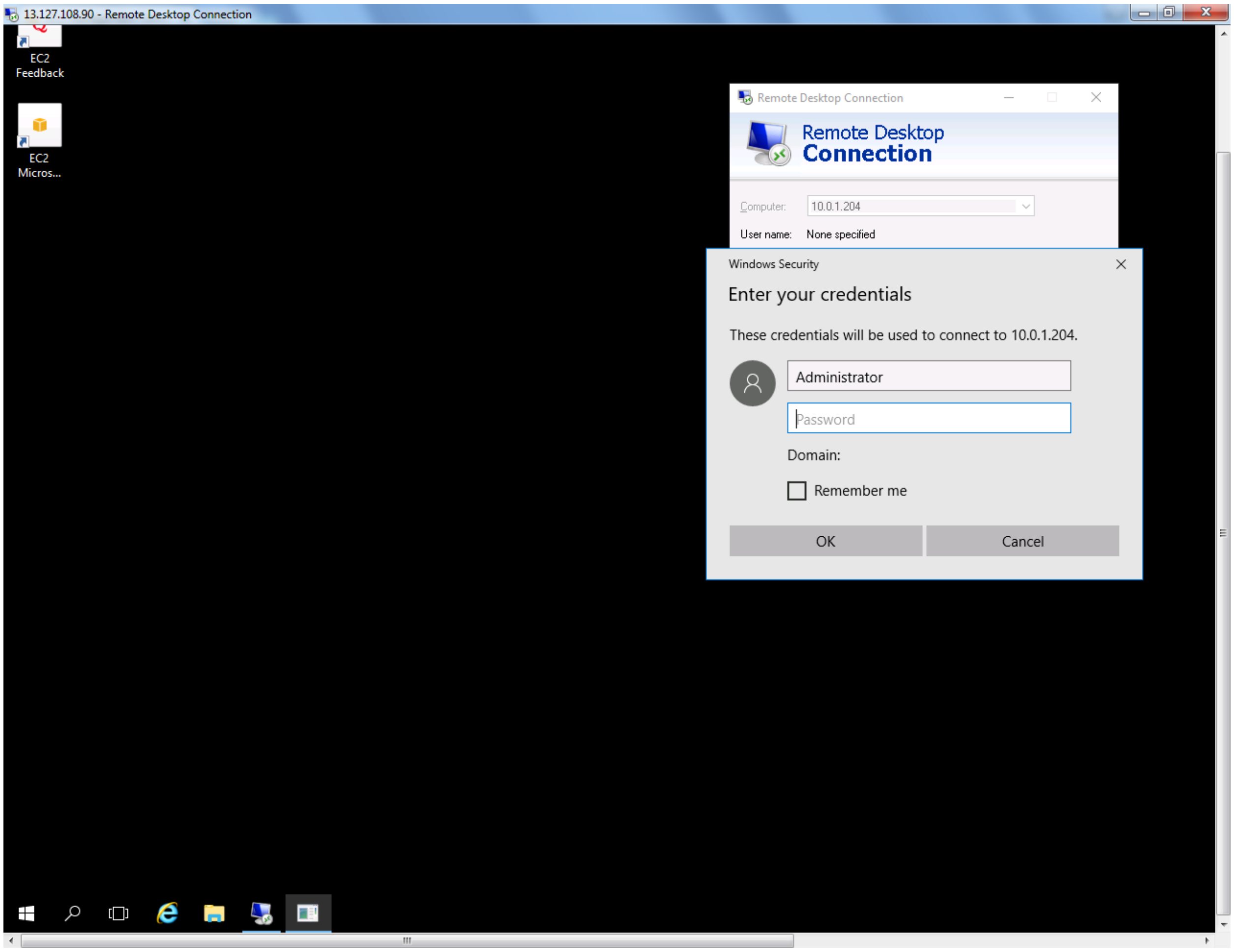
Select a key pair

siva_vpc ▾

☑ I acknowledge that I have access to the selected private key file (siva_vpc.pem), and that without this file, I won't be able to log into my instance.

Then click "Launch Instance".

Try to connect 10.0.1.204 (private subnet host) from Public subnet host.



13.127.108.90 - Remote Desktop Connection

Remote Desktop Connection

Computer: 10.0.1.204

User name: None specified

Windows Security

Enter your credentials

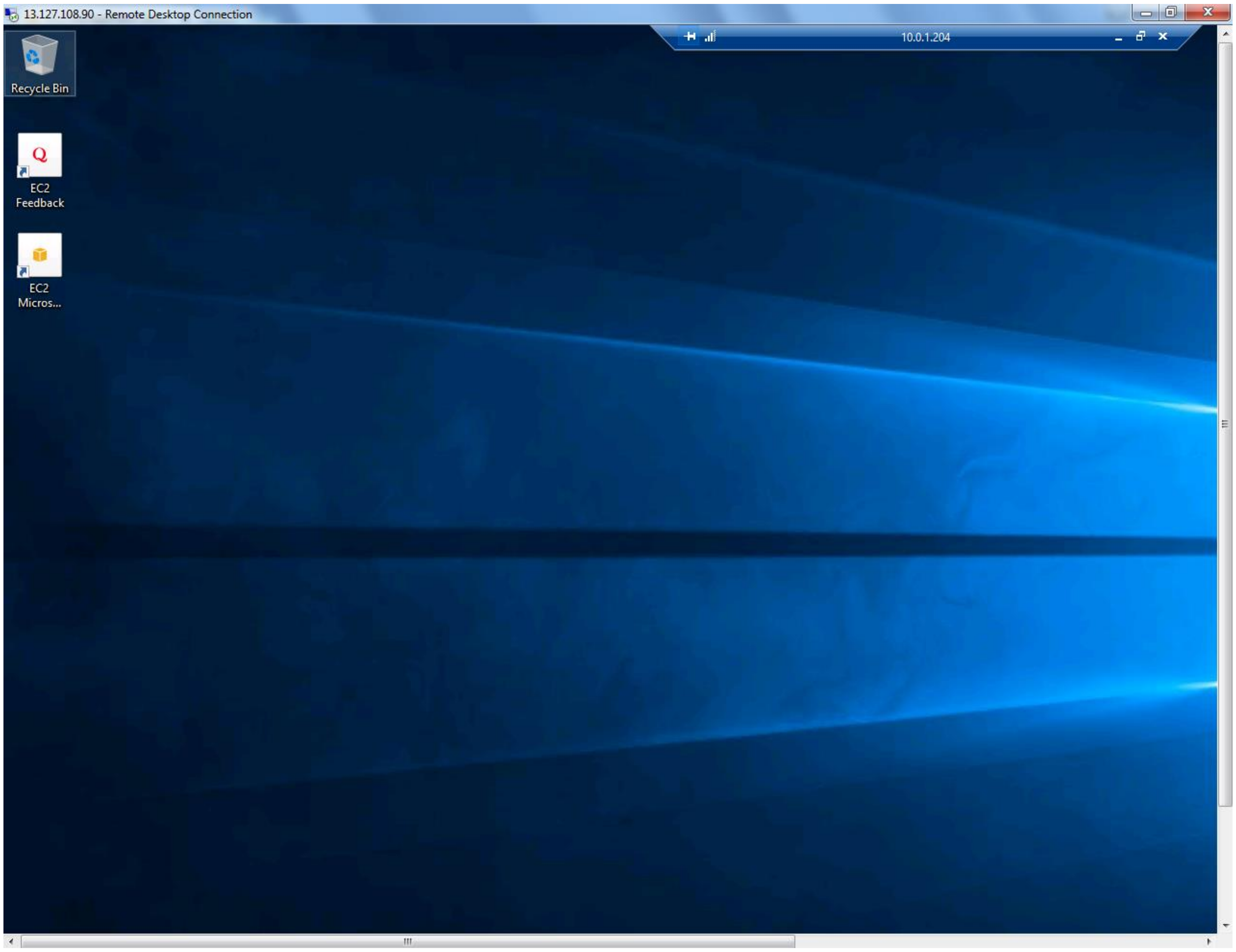
These credentials will be used to connect to 10.0.1.204.

Administrator

Password

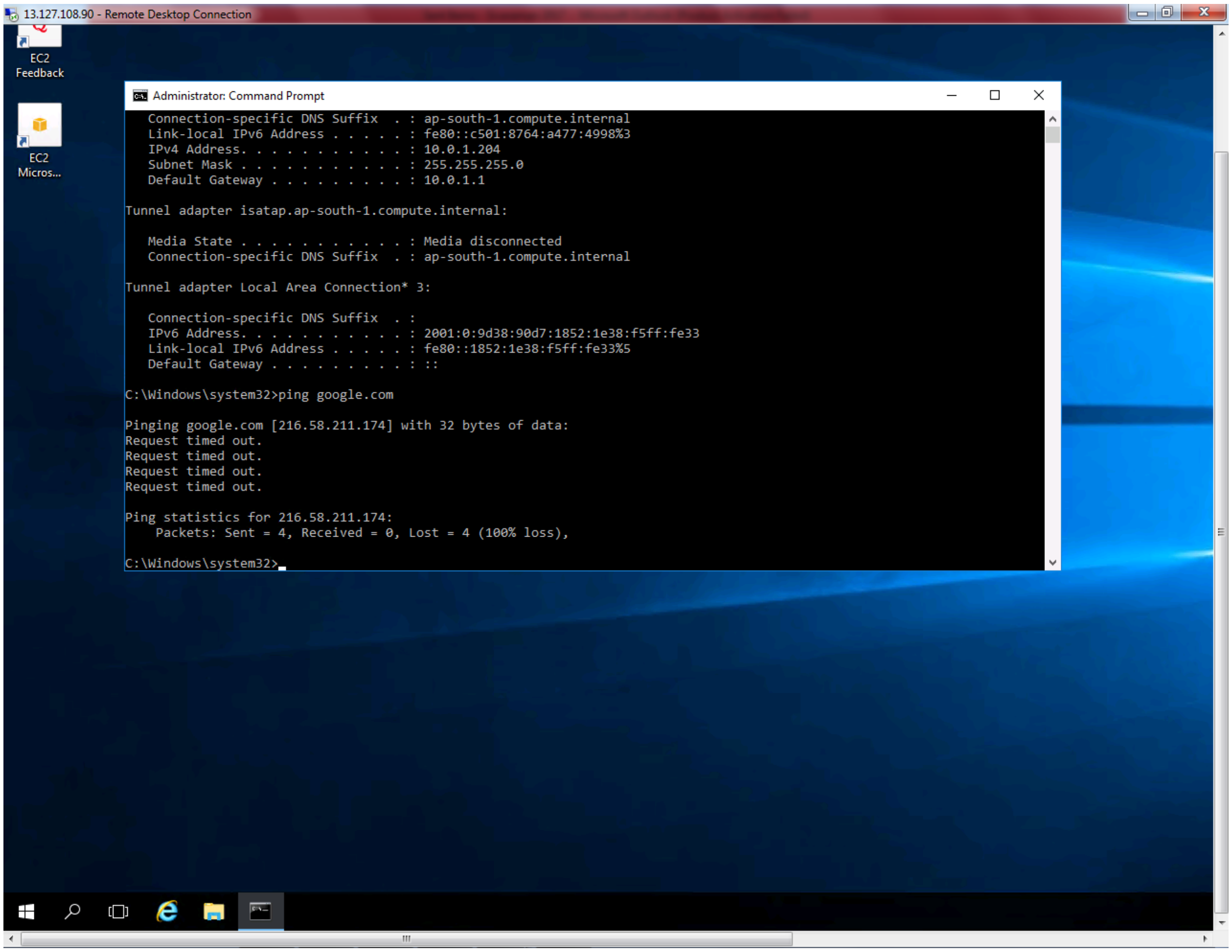
Domain:

□ Remember me



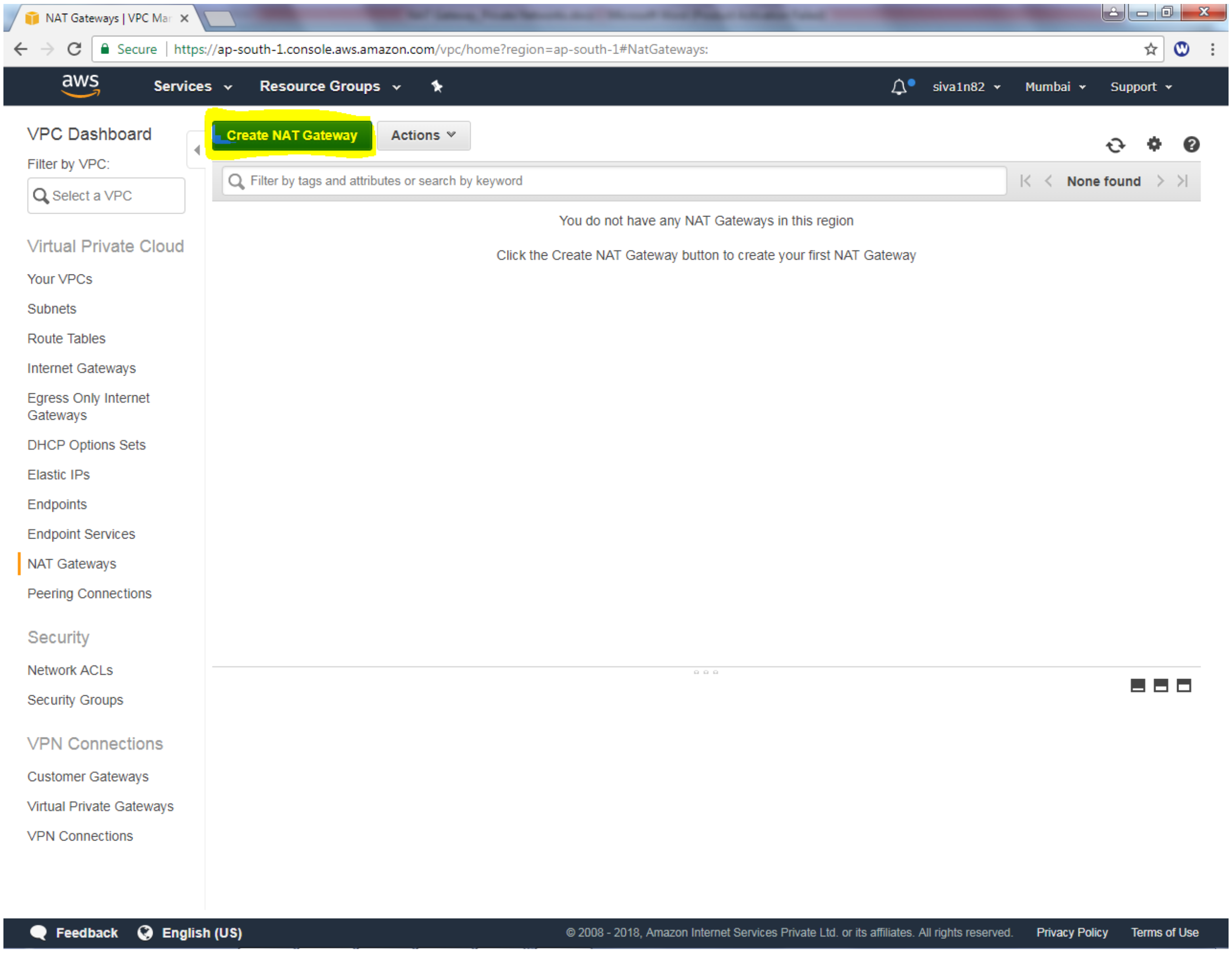
Kindly try to connect internet from 10.0.1.204 machine.

But, you are not able to connect Internet. Because you are in private network, need to configure NAT Gateway in VPC.


13.127.108.90 - Remote Desktop Connection
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt

```
   Connection-specific DNS Suffix  . : ap-south-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::c501:8764:a477:4998%3
   IPv4 Address. . . . . . . . . . . : 10.0.1.204
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1

Tunnel adapter isatap.ap-south-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-south-1.compute.internal

Tunnel adapter Local Area Connection* 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:90d7:1852:1e38:f5ff:fe33
   Link-local IPv6 Address . . . . . : fe80::1852:1e38:f5ff:fe33%5
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>ping google.com

Pinging google.com [216.58.211.174] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 216.58.211.174:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>
```

Go to, VPC Dashboard, Select “Nat Gateways”

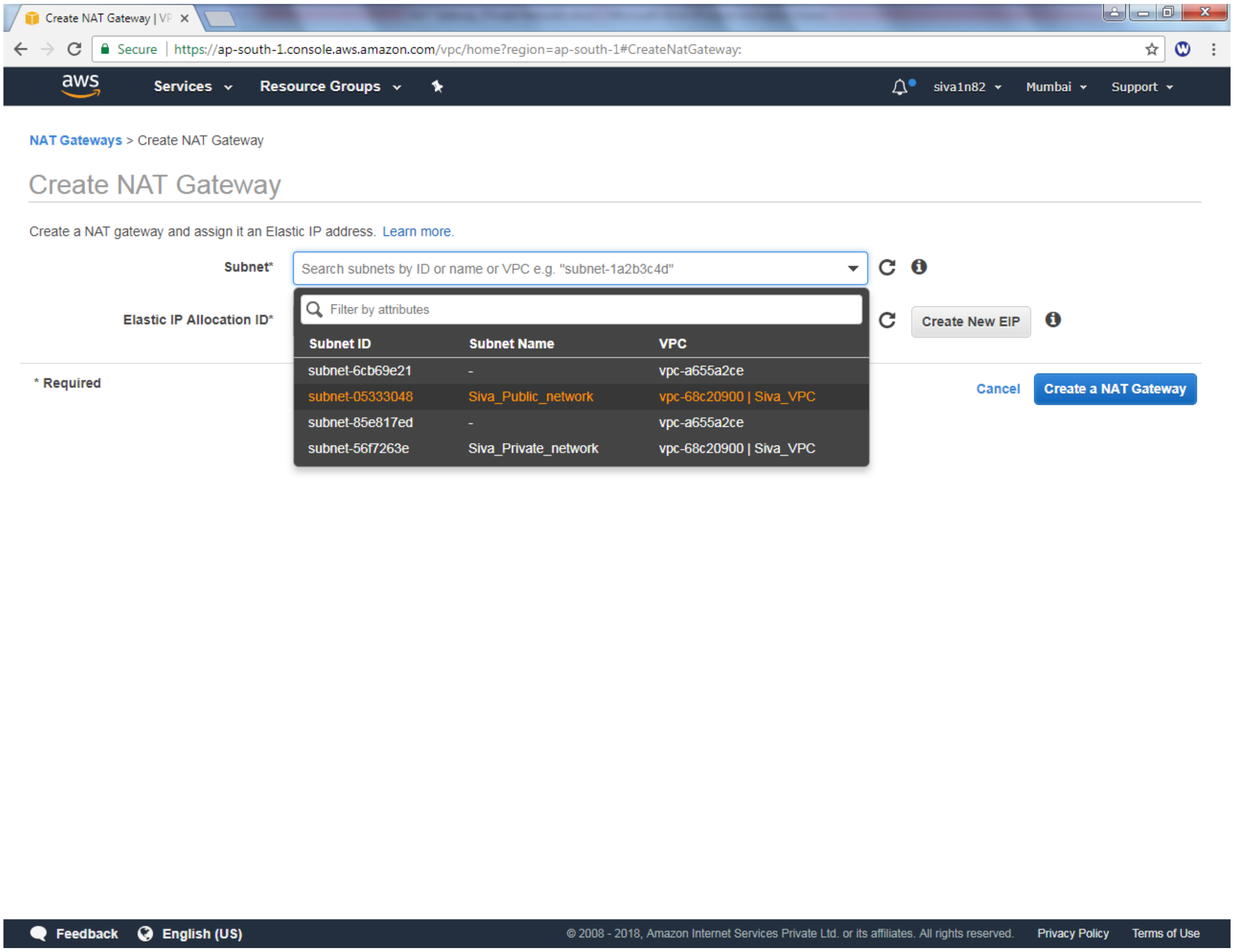


You do not have any NAT Gateways in this region

Click the Create NAT Gateway button to create your first NAT Gateway

Click “Create NAT Gateway”.

While creating NAT Gateway, select **“Siva_Public_network”**



Create NAT Gateway | VF
Secure
https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreateNatGateway:
aws
Services
Resource Groups
siva1n82
Mumbai
Support

NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. Learn more.

Subnet* Search subnets by ID or name or VPC e.g. "subnet-1a2b3c4d"

Elastic IP Allocation ID*

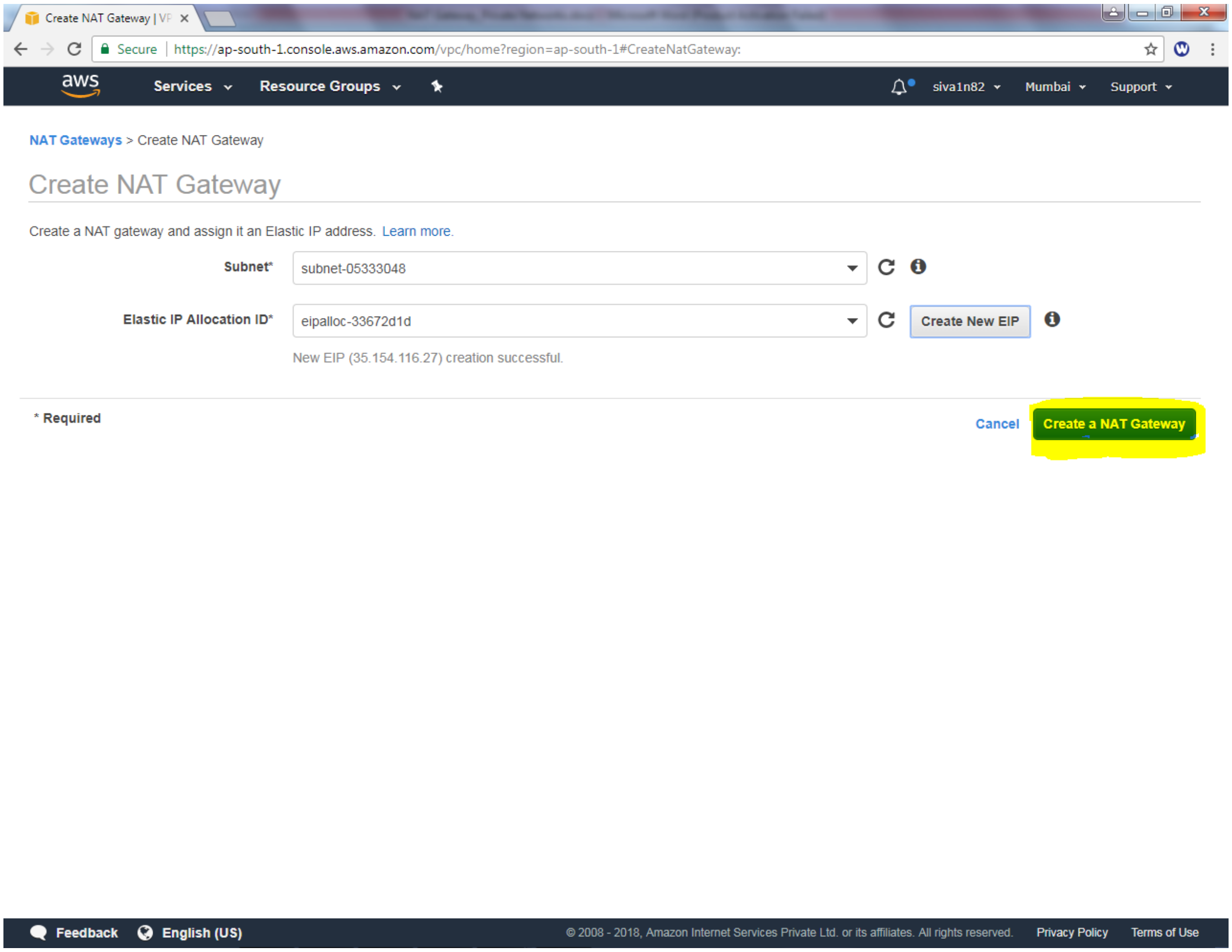
Filter by attributes

Subnet ID	Subnet Name	VPC
subnet-6cb69e21	-	vpc-a655a2ce
subnet-05333048	Siva_Public_network	vpc-68c20900 | Siva_VPC
subnet-85e817ed	-	vpc-a655a2ce
subnet-56f7263e	Siva_Private_network	vpc-68c20900 | Siva_VPC

* Required

Create New EIP
Cancel
Create a NAT Gateway
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

In Elastic IP Allocation ID, click “Create new ËIP”



Create NAT Gateway | VF
Secure https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreateNatGateway:
aws
Services
Resource Groups
siva1n82
Mumbai
Support

NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. Learn more.

Subnet* subnet-05333048

Elastic IP Allocation ID* eipalloc-33672d1d

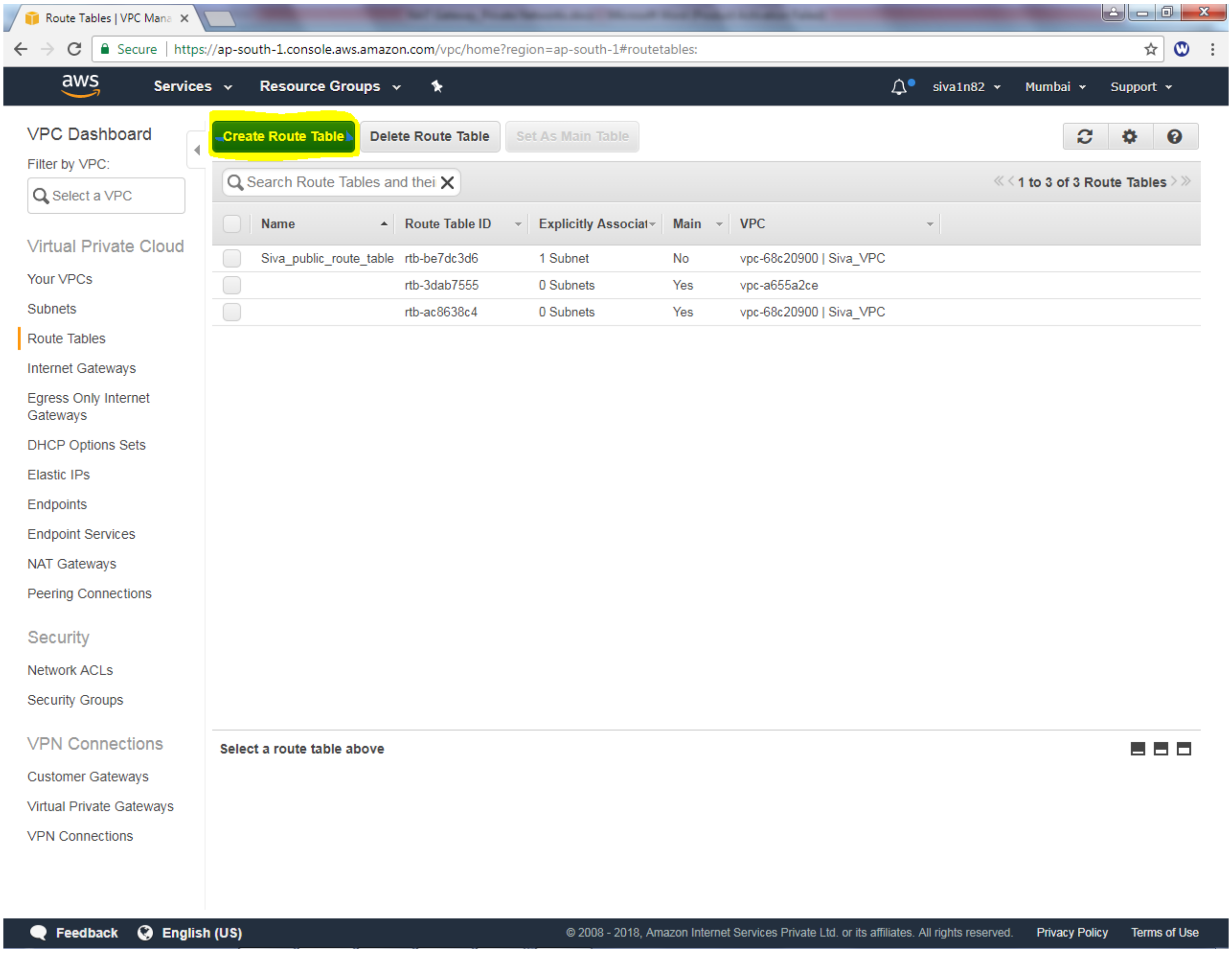
New EIP (35.154.116.27) creation successful.

* Required

Cancel
Create a NAT Gateway
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Then click “Create a NAT Gateway”.

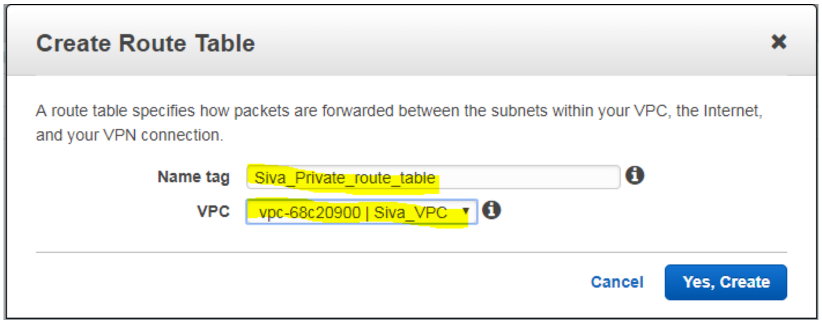
We have required to create an routing table for private network.



Name	Route Table ID	Explicitly Associat	Main	VPC
Siva_public_route_table	rtb-be7dc3d6	1 Subnet	No	vpc-68c20900 | Siva_VPC
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
	rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 | Siva_VPC

Click “Create Route Table”.

In Name tag, Type “siva_private_route_table” and select “Siva_VPC”.



Create Route Table

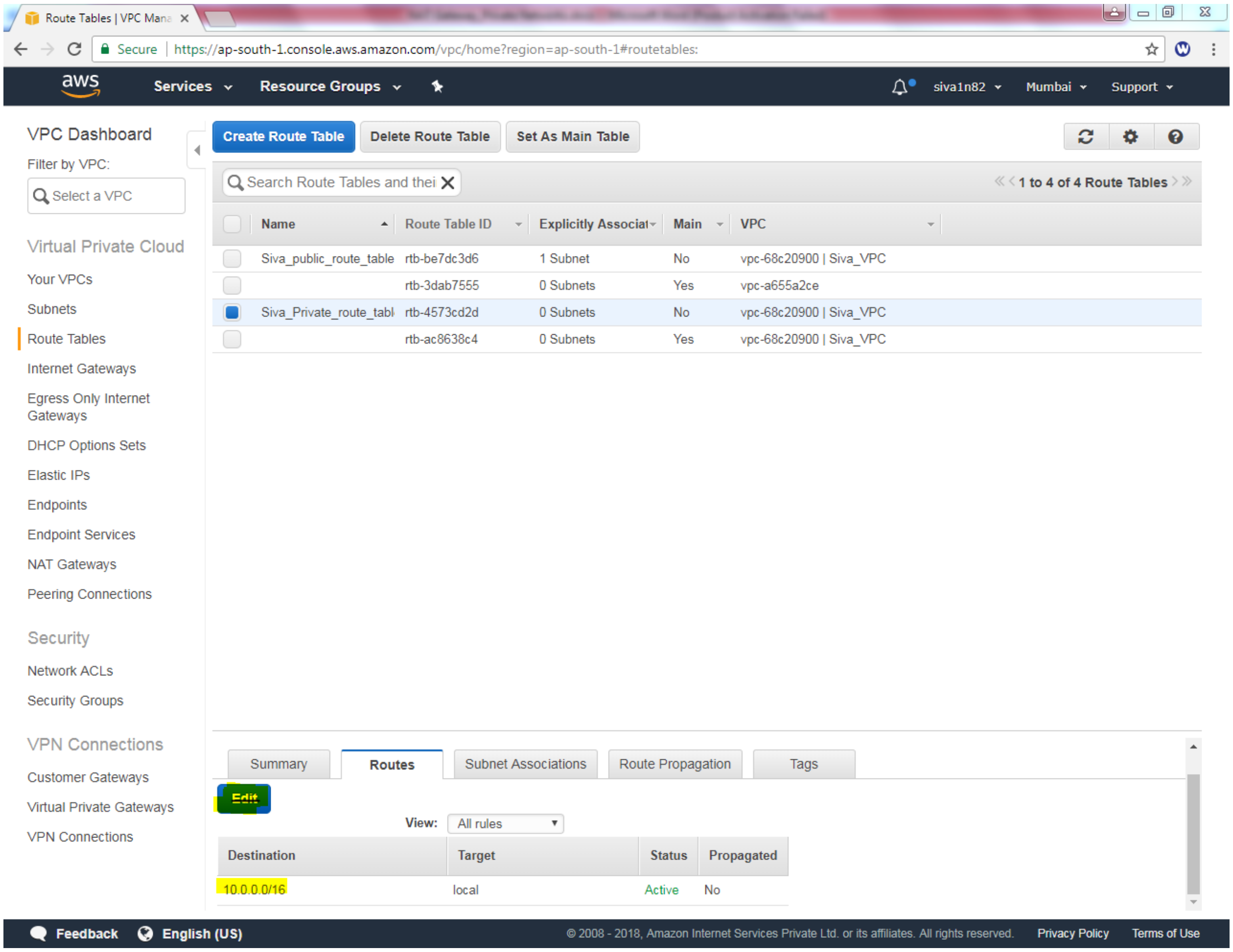
A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag: Siva_Private_route_table

VPC: vpc-68c20900 | Siva_VPC

Then Click “**Yes create”**.

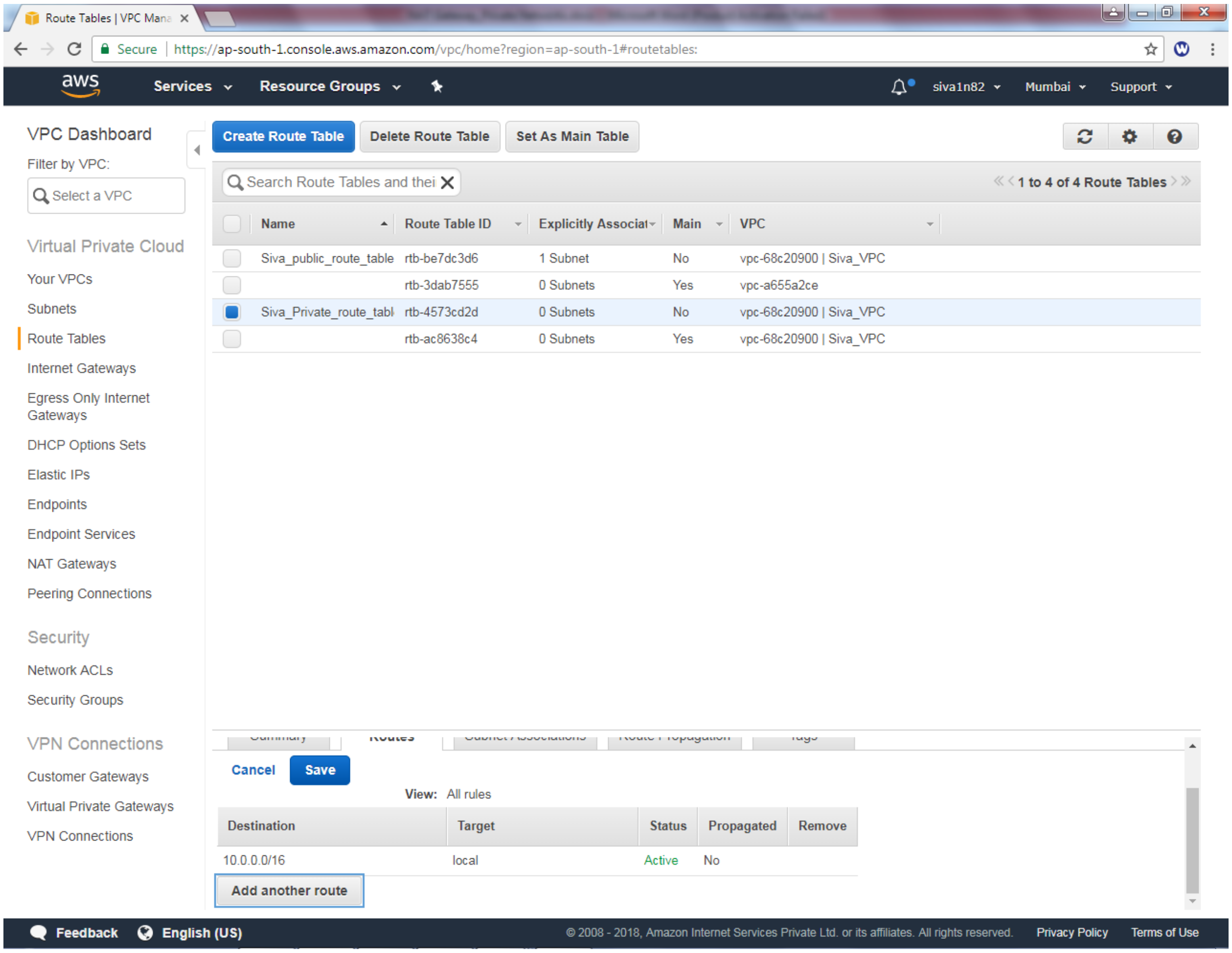
In Route Table, click edit button.



	Name	Route Table ID	Explicitly Associat	Main	VPC
□	Siva_public_route_table	rtb-be7dc3d6	1 Subnet	No	vpc-68c20900 | Siva_VPC
□		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
☑	Siva_Private_route_tabl	rtb-4573cd2d	0 Subnets	No	vpc-68c20900 | Siva_VPC
□		rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 | Siva_VPC

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

In Edit option, click “Add another route”

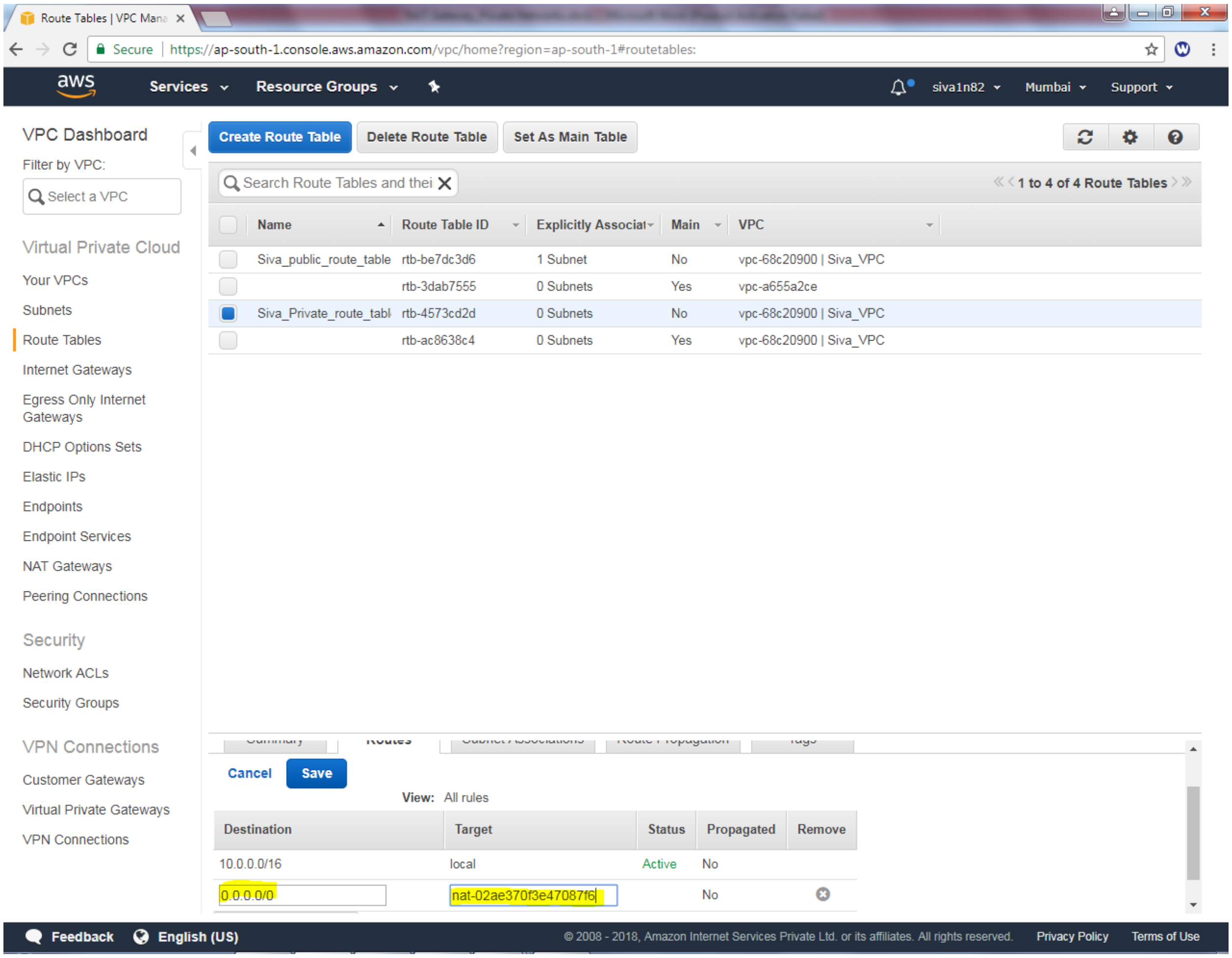


Name	Route Table ID	Explicitly Associat	Main	VPC
Siva_public_route_table	rtb-be7dc3d6	1 Subnet	No	vpc-68c20900 | Siva_VPC
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
Siva_Private_route_tabl	rtb-4573cd2d	0 Subnets	No	vpc-68c20900 | Siva_VPC
	rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 | Siva_VPC

View: All rules

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	

In add another route, enter the default route 0.0.0.0/0 with next hop address as nat-* as target.

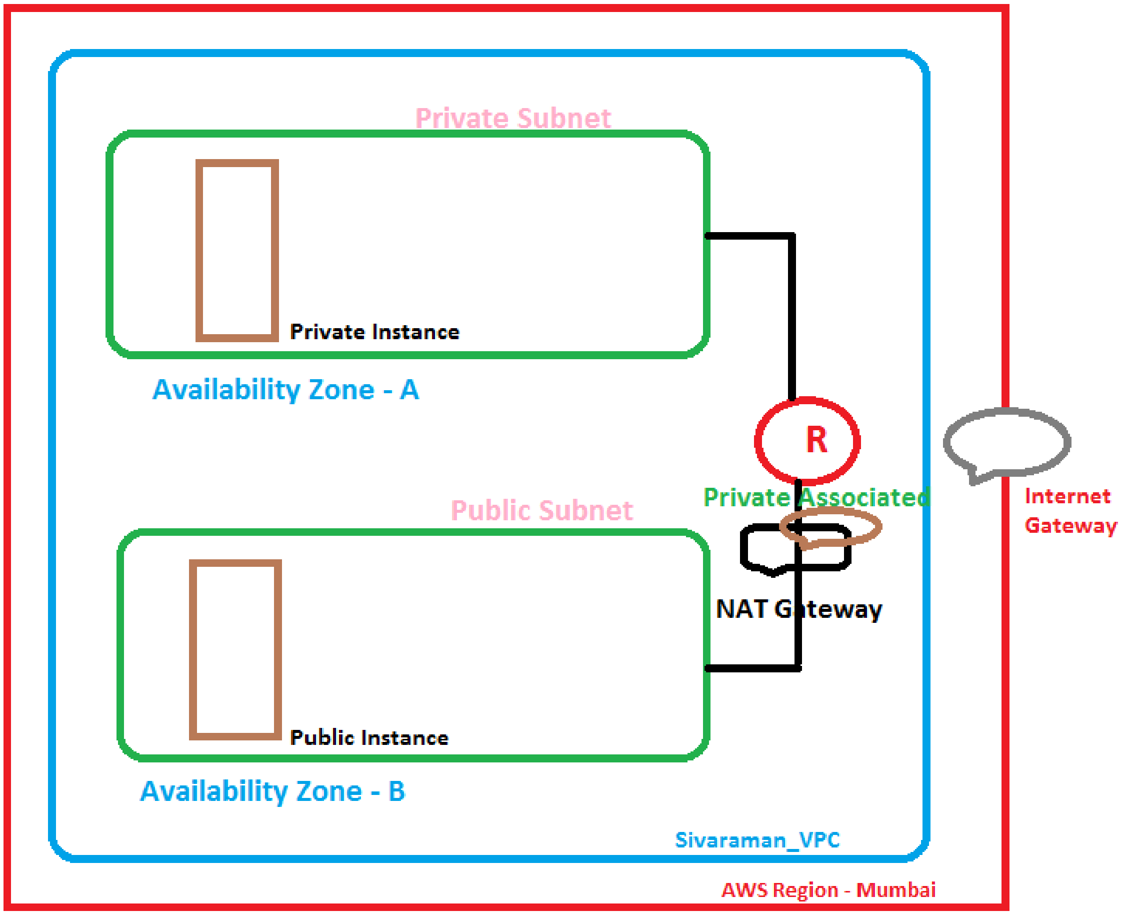


	Name	Route Table ID	Explicitly Associat	Main	VPC
□	Siva_public_route_table	rtb-be7dc3d6	1 Subnet	No	vpc-68c20900 | Siva_VPC
□		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
☑	Siva_Private_route_tabl	rtb-4573cd2d	0 Subnets	No	vpc-68c20900 | Siva_VPC
□		rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 | Siva_VPC

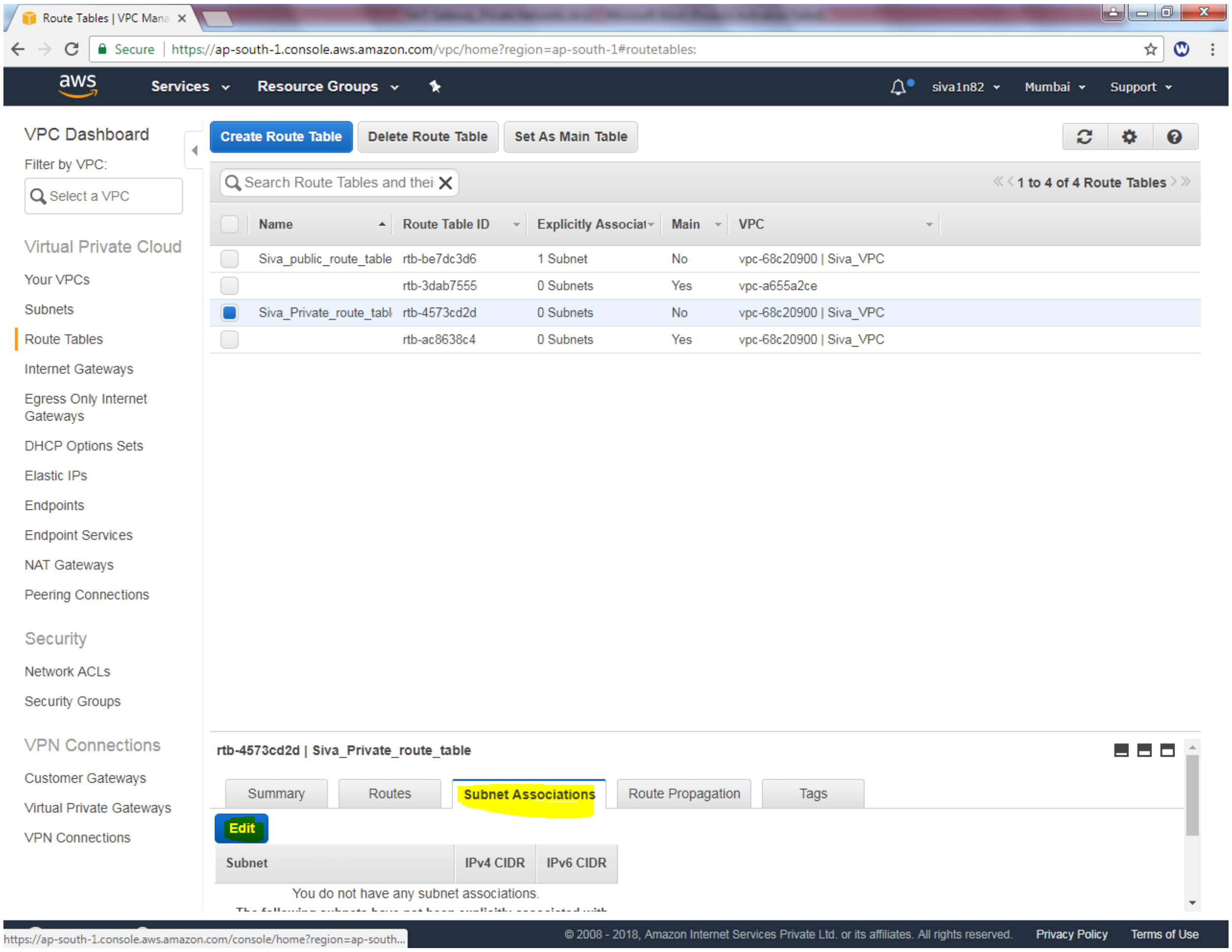
View: All rules

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	nat-02ae370f3e47087f6		No	⊗

Click “save”.


Private Subnet
Private Instance
Availability Zone - A
R
Private Associated
Internet
Gateway
Public Subnet
NAT Gateway
Public Instance
Availability Zone - B
Sivaraman_VPC
AWS Region - Mumbai

In Subnet associations., click “Edit”options



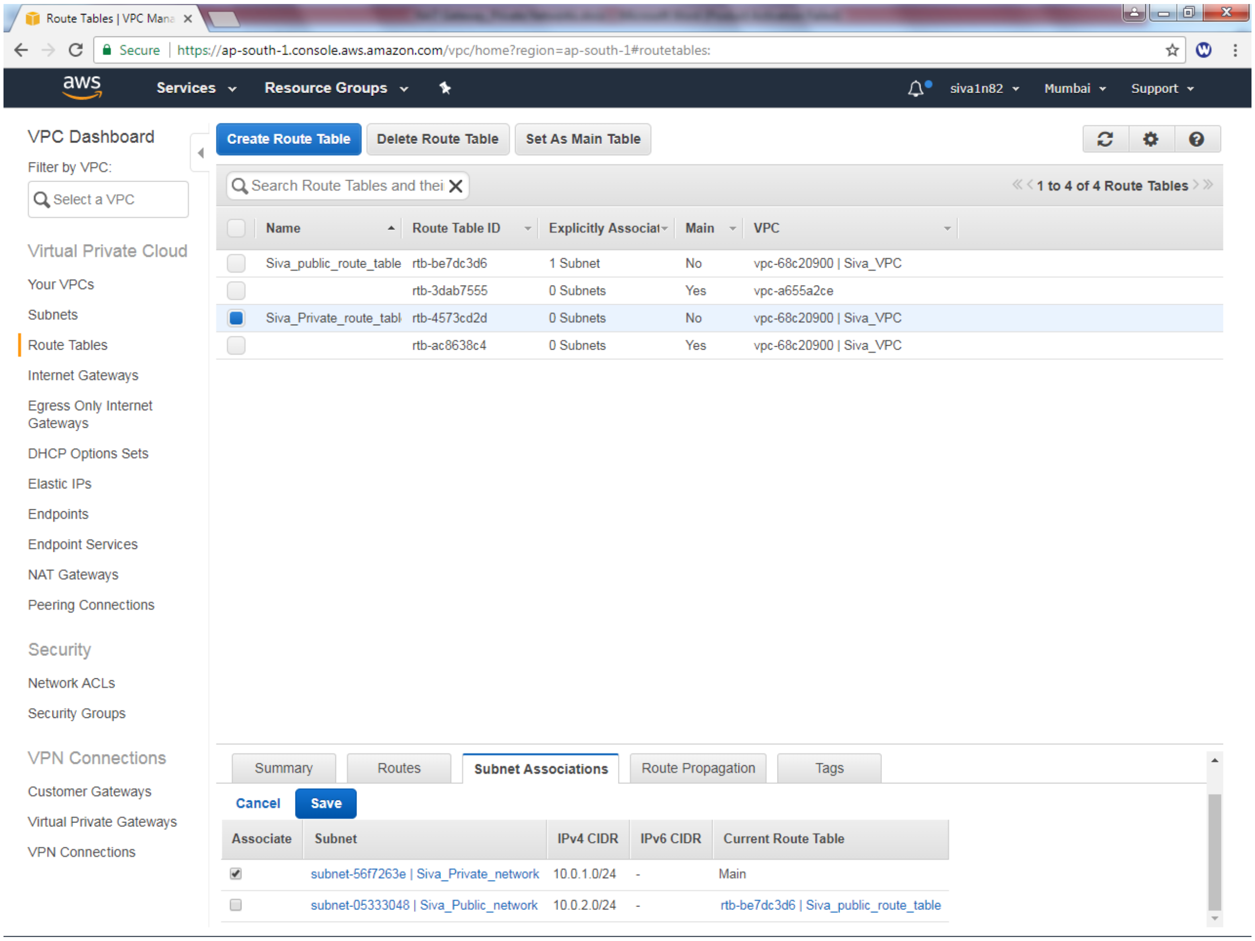
	Name	Route Table ID	Explicitly Associat	Main	VPC
□	Siva_public_route_table	rtb-be7dc3d6	1 Subnet	No	vpc-68c20900 | Siva_VPC
□		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
☑	Siva_Private_route_tabl	rtb-4573cd2d	0 Subnets	No	vpc-68c20900 | Siva_VPC
□		rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 | Siva_VPC

rtb-4573cd2d | Siva_Private_route_table

Subnet	IPv4 CIDR	IPv6 CIDR

You do not have any subnet associations.

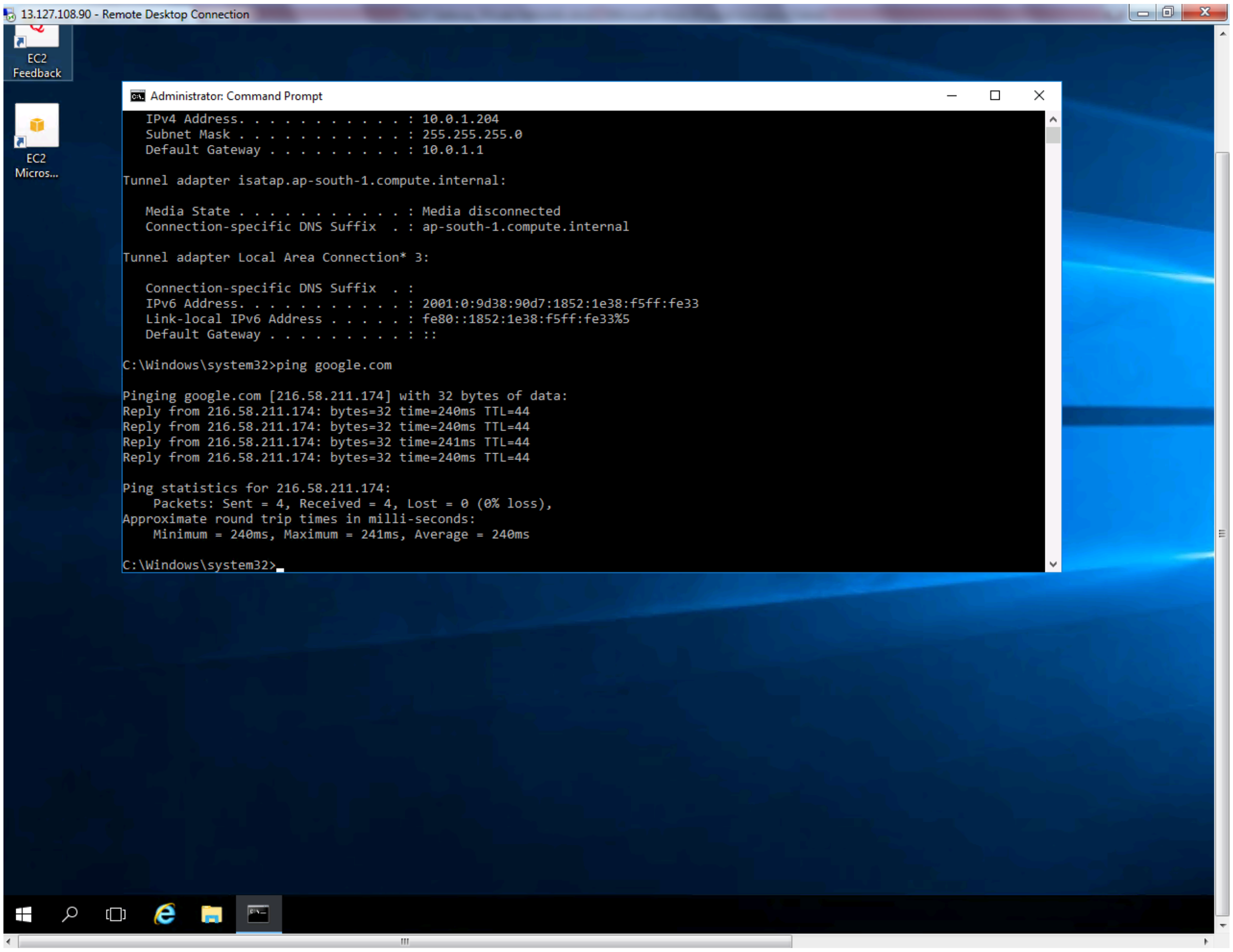
In Subnet associations, select “Siva_private_subnet” then click save.



	Name	Route Table ID	Explicitly Associat	Main	VPC
□	Siva_public_route_table	rtb-be7dc3d6	1 Subnet	No	vpc-68c20900 | Siva_VPC
□		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
☑	Siva_Private_route_tabl	rtb-4573cd2d	0 Subnets	No	vpc-68c20900 | Siva_VPC
□		rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 | Siva_VPC

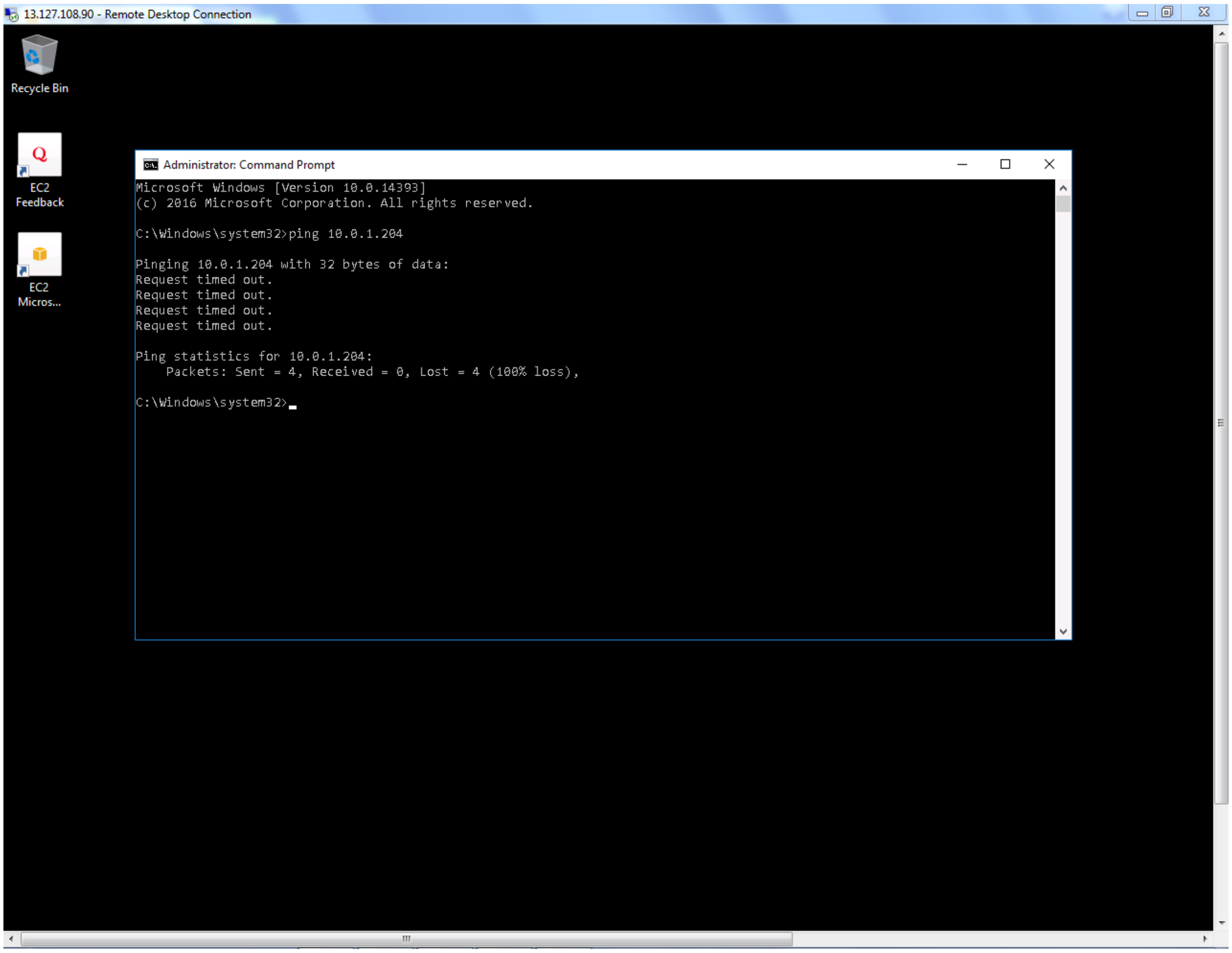
Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
☑	subnet-56f7263e | Siva_Private_network	10.0.1.0/24	-	Main
□	subnet-05333048 | Siva_Public_network	10.0.2.0/24	-	rtb-be7dc3d6 | Siva_public_route_table

Now we are able to connect internet.


13.127.108.90 - Remote Desktop Connection
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt

```
   IPv4 Address. . . . . . . . . . . : 10.0.1.204
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1

Tunnel adapter isatap.ap-south-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-south-1.compute.internal

Tunnel adapter Local Area Connection* 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:90d7:1852:1e38:f5ff:fe33
   Link-local IPv6 Address . . . . . : fe80::1852:1e38:f5ff:fe33%5
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>ping google.com

Pinging google.com [216.58.211.174] with 32 bytes of data:
Reply from 216.58.211.174: bytes=32 time=240ms TTL=44
Reply from 216.58.211.174: bytes=32 time=240ms TTL=44
Reply from 216.58.211.174: bytes=32 time=241ms TTL=44
Reply from 216.58.211.174: bytes=32 time=240ms TTL=44

Ping statistics for 216.58.211.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 240ms, Maximum = 241ms, Average = 240ms

C:\Windows\system32>
```

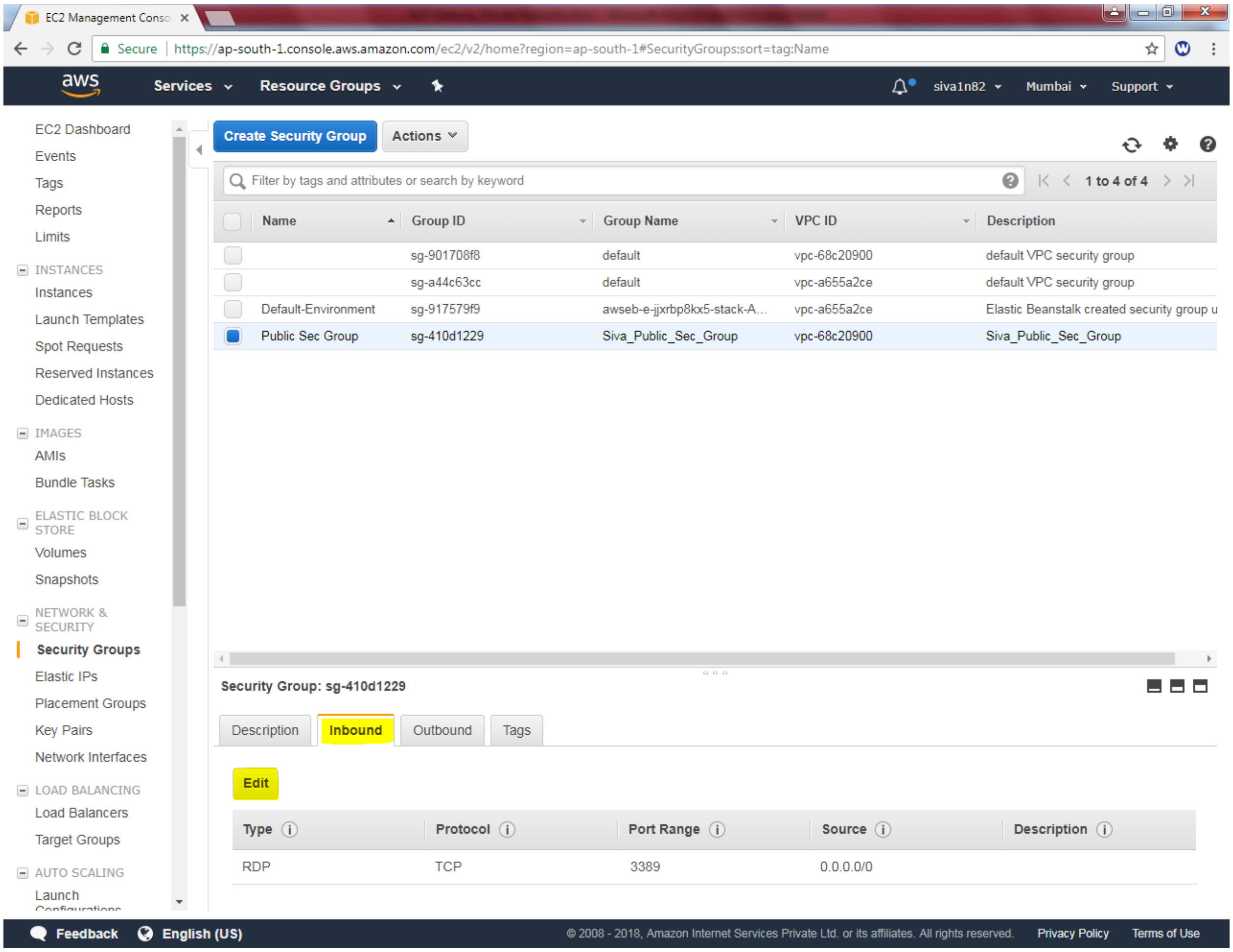
Now try to ping private subnet 10.0.1.204 from 10.0.2.14


13.127.108.90 - Remote Desktop Connection
Recycle Bin
EC2
Feedback
EC2
Micros...
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.0.1.204

Pinging 10.0.1.204 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.1.204:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>
```

But, we are unable to ping what could be reason?

In Siva_Public_Sec_Group we have allowed only RDP port to inside the network. Hence we are unable to ping the private subnet 10.0.1.204 from 10.0.2.14.



	Name	Group ID	Group Name	VPC ID	Description
□		sg-901708f8	default	vpc-68c20900	default VPC security group
□		sg-a44c63cc	default	vpc-a655a2ce	default VPC security group
□	Default-Environment	sg-917579f9	awseb-e-jjxrbp8kx5-stack-A...	vpc-a655a2ce	Elastic Beanstalk created security group u
■	Public Sec Group	sg-410d1229	Siva_Public_Sec_Group	vpc-68c20900	Siva_Public_Sec_Group

Security Group: sg-410d1229

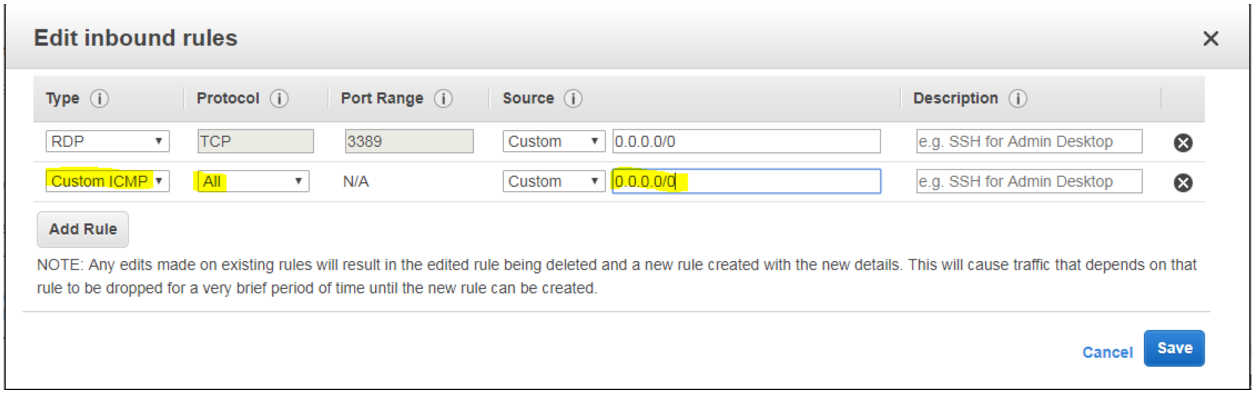
Description | Inbound | Outbound | Tags

Edit

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	0.0.0.0/0	

Click edit .

Then add rule **“Custom ICMP”** **“Protocol – All”** or **ICMP Echo Request** and Source 0.0.0.0/0 (any) network.

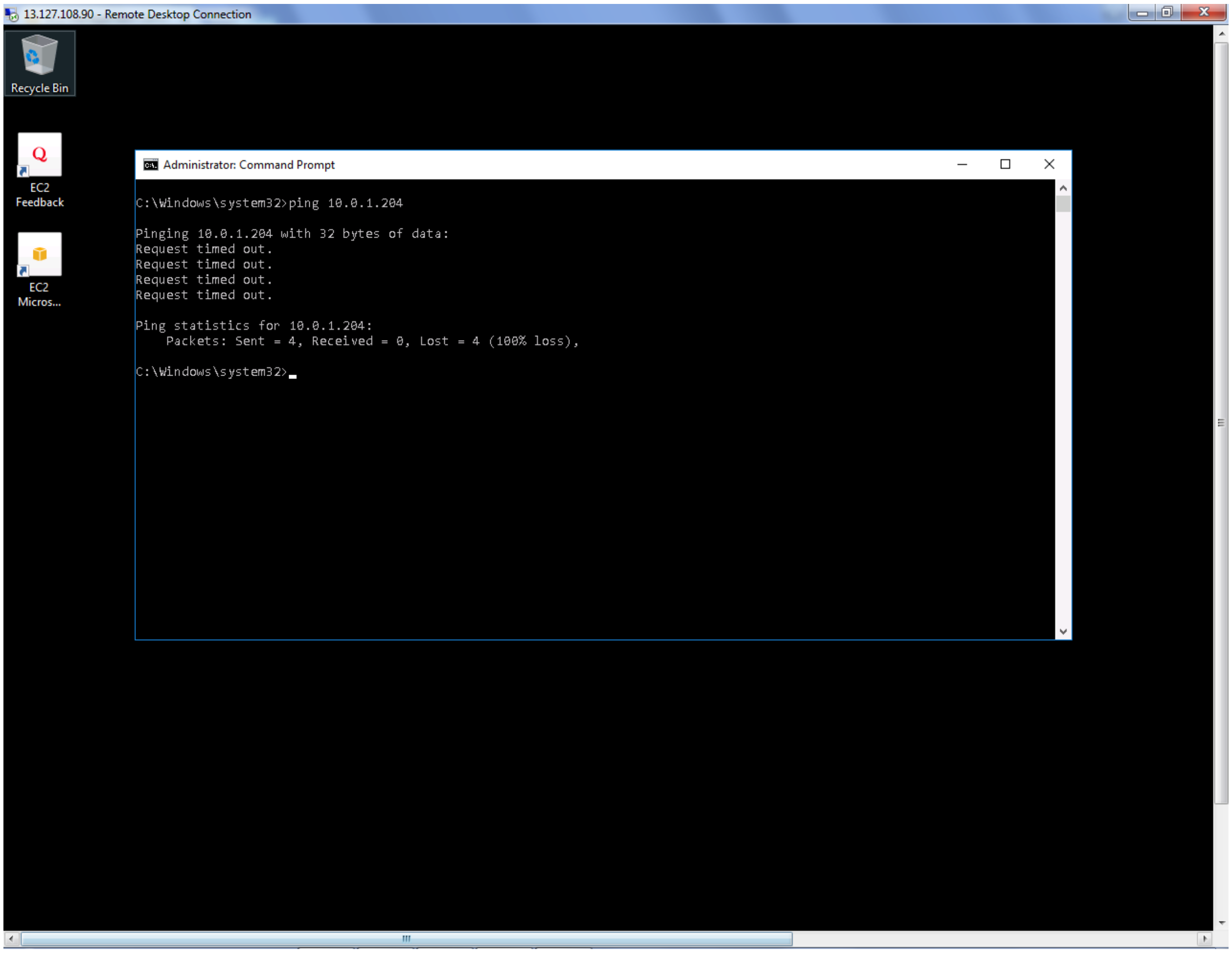


Edit inbound rules

Type	Protocol	Port Range	Source		Description
RDP	TCP	3389	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom ICMP	All	N/A	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

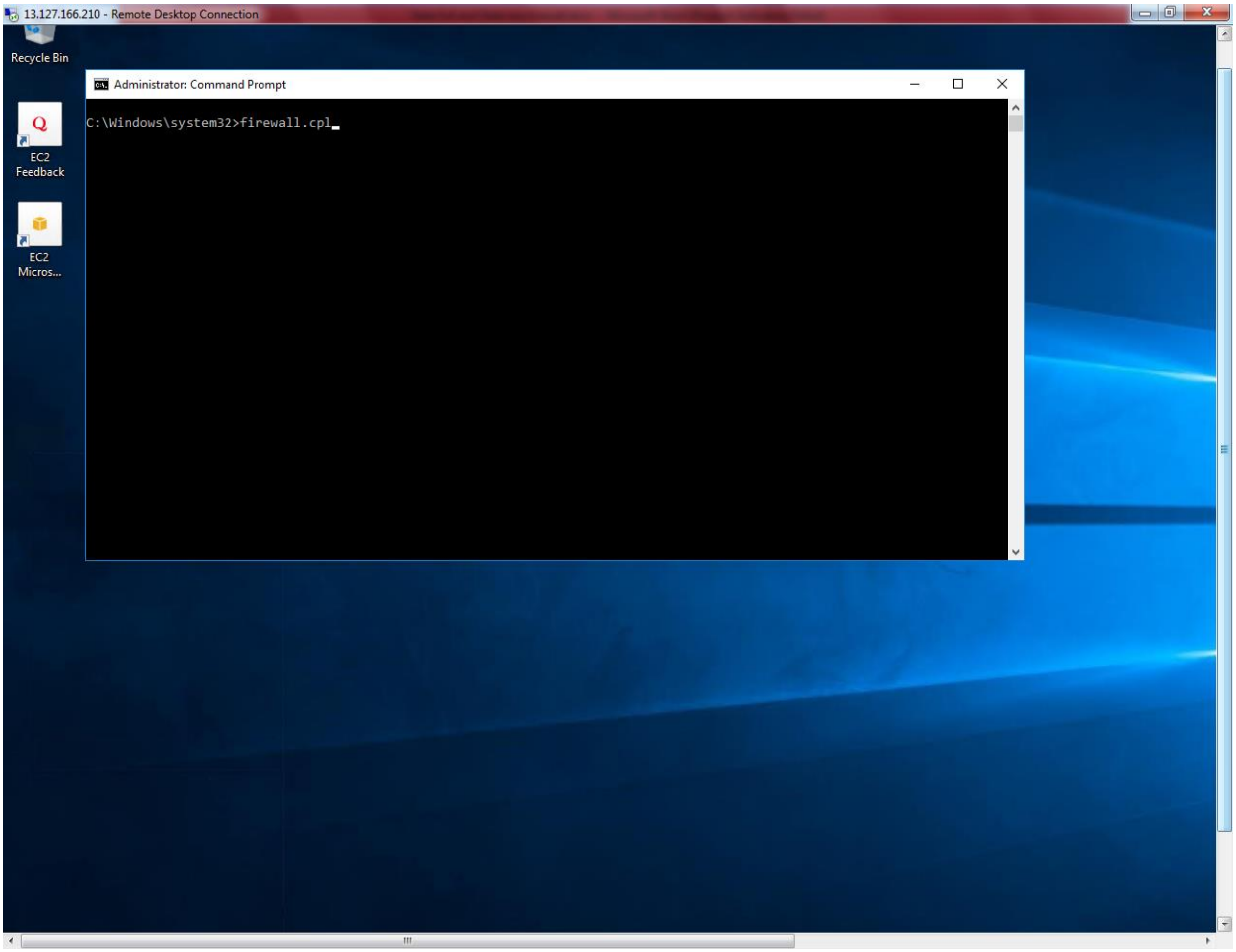
Try to ping 10.0.1.204 from 10.0.2.14 host. What could be the reason. Traffic ICMP has been allowed in Inbound rule. But server’s firewall is on, that is the reason for unable to ping the host.


13.127.108.90 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt

```
C:\Windows\system32>ping 10.0.1.204

Pinging 10.0.1.204 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.1.204:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

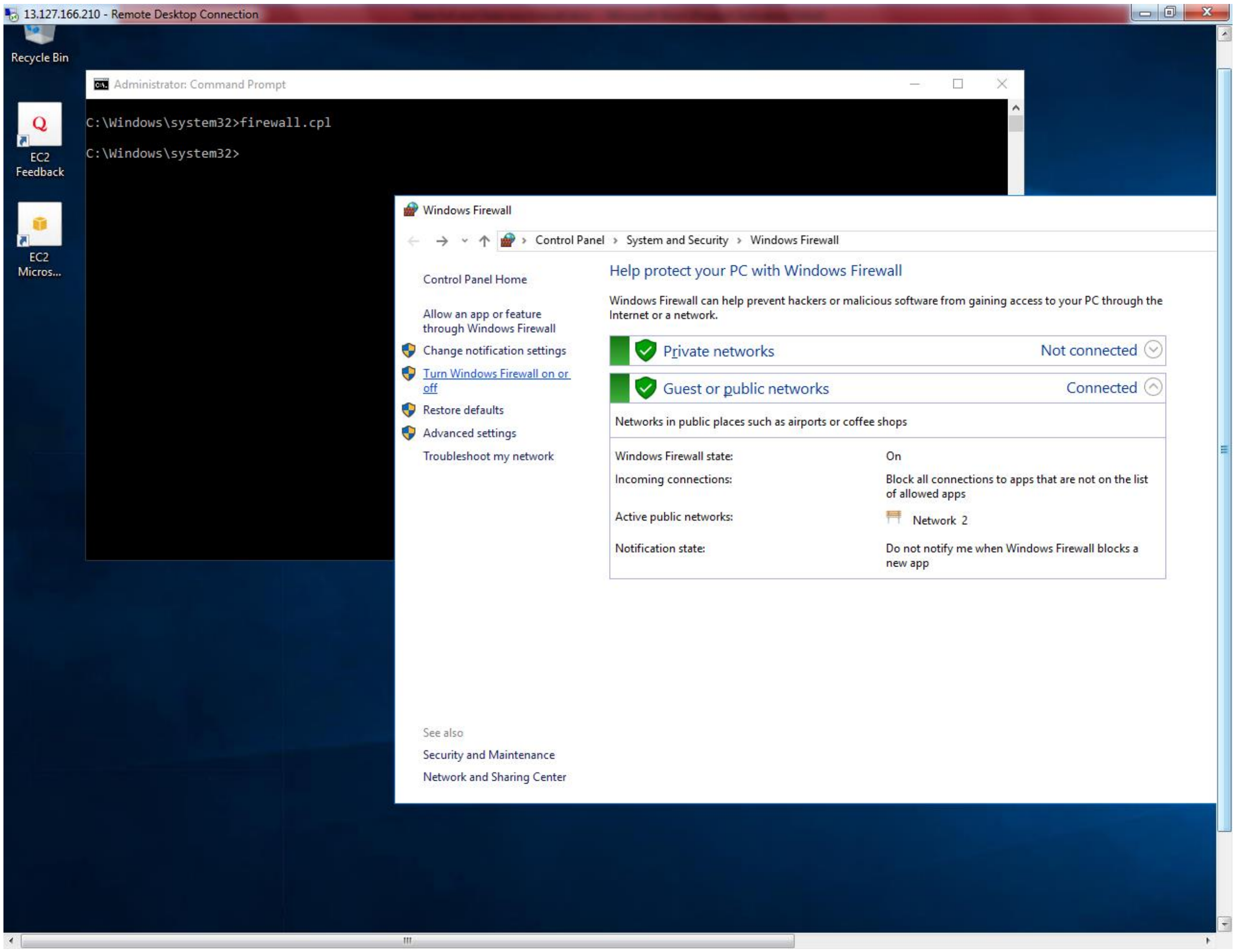
Hence, we need to turn off the windows firewall in both servers.

Type Firewall.cpl


13.127.166.210 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt

```
C:\Windows\system32>firewall.cpl
```

Click "Turn Windows Firewall on or Off".



```
C:\Windows\system32>firewall.cpl

C:\Windows\system32>
```

13.127.166.210 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt
Windows Firewall
Control Panel > System and Security > Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

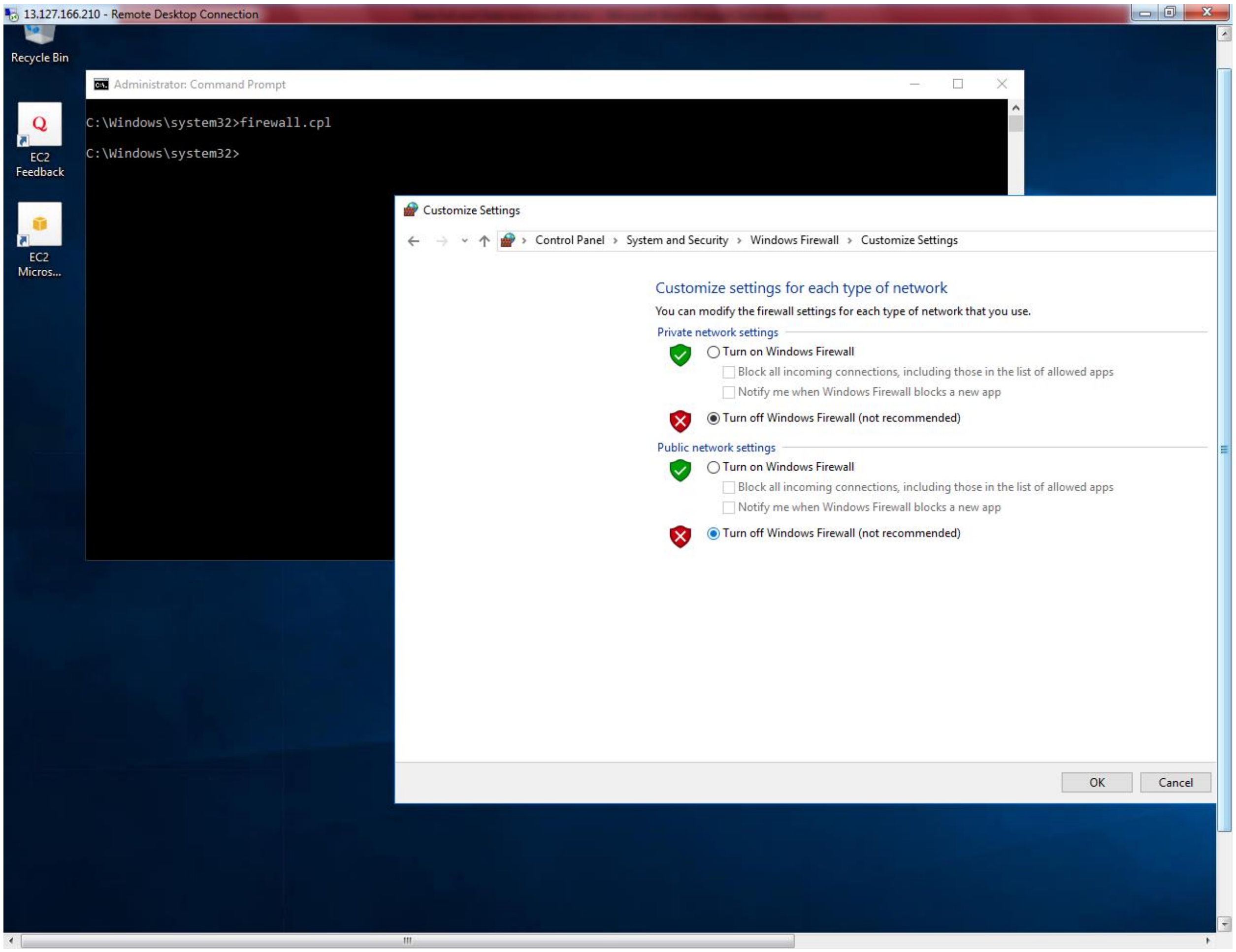
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network 2
Notification state:	Do not notify me when Windows Firewall blocks a new app

Turn off windows firewall.



```
C:\Windows\system32>firewall.cpl

C:\Windows\system32>
```

Control Panel > System and Security > Windows Firewall > Customize Settings

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

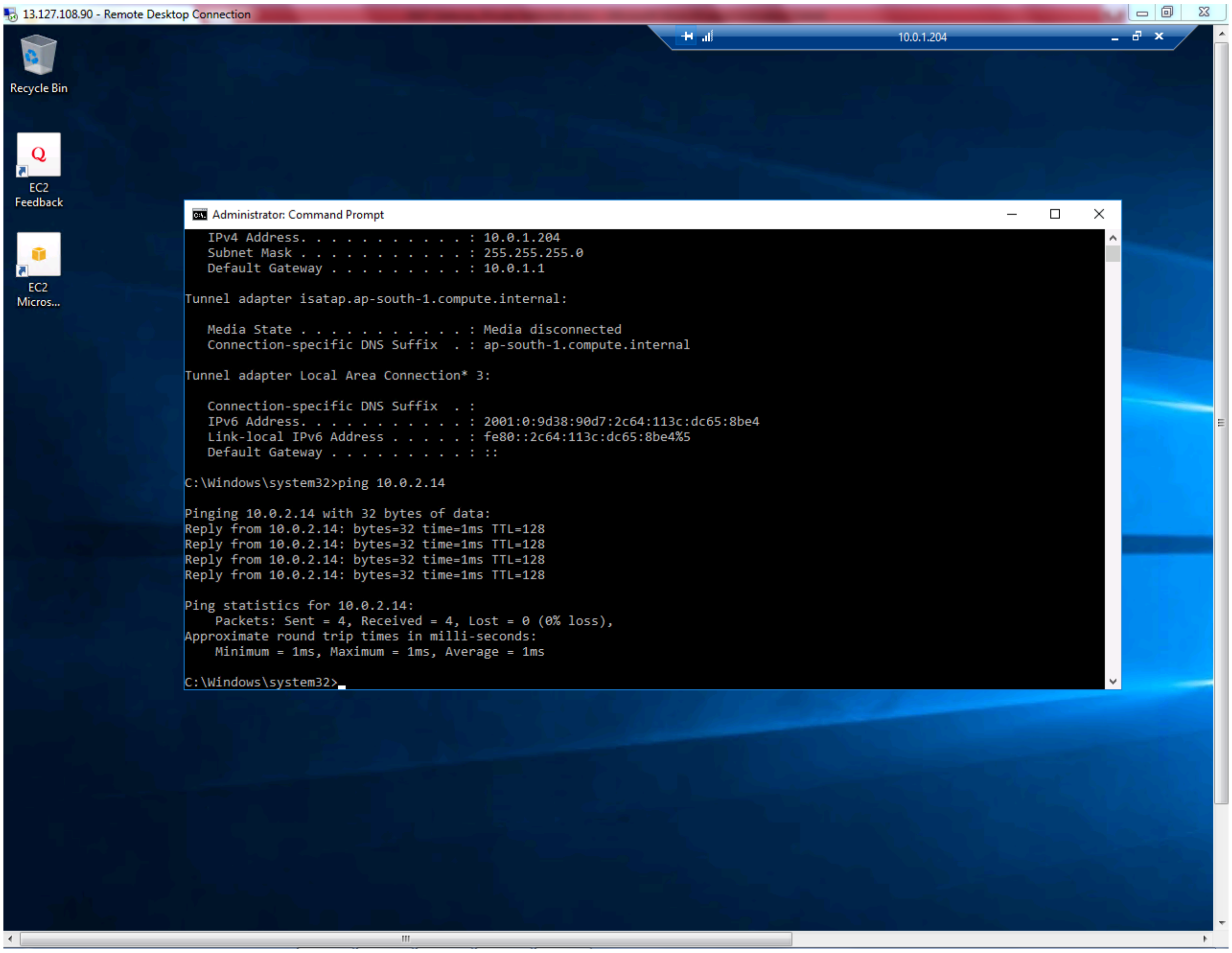
□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

13.127.166.210 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt
Customize Settings
OK
Cancel

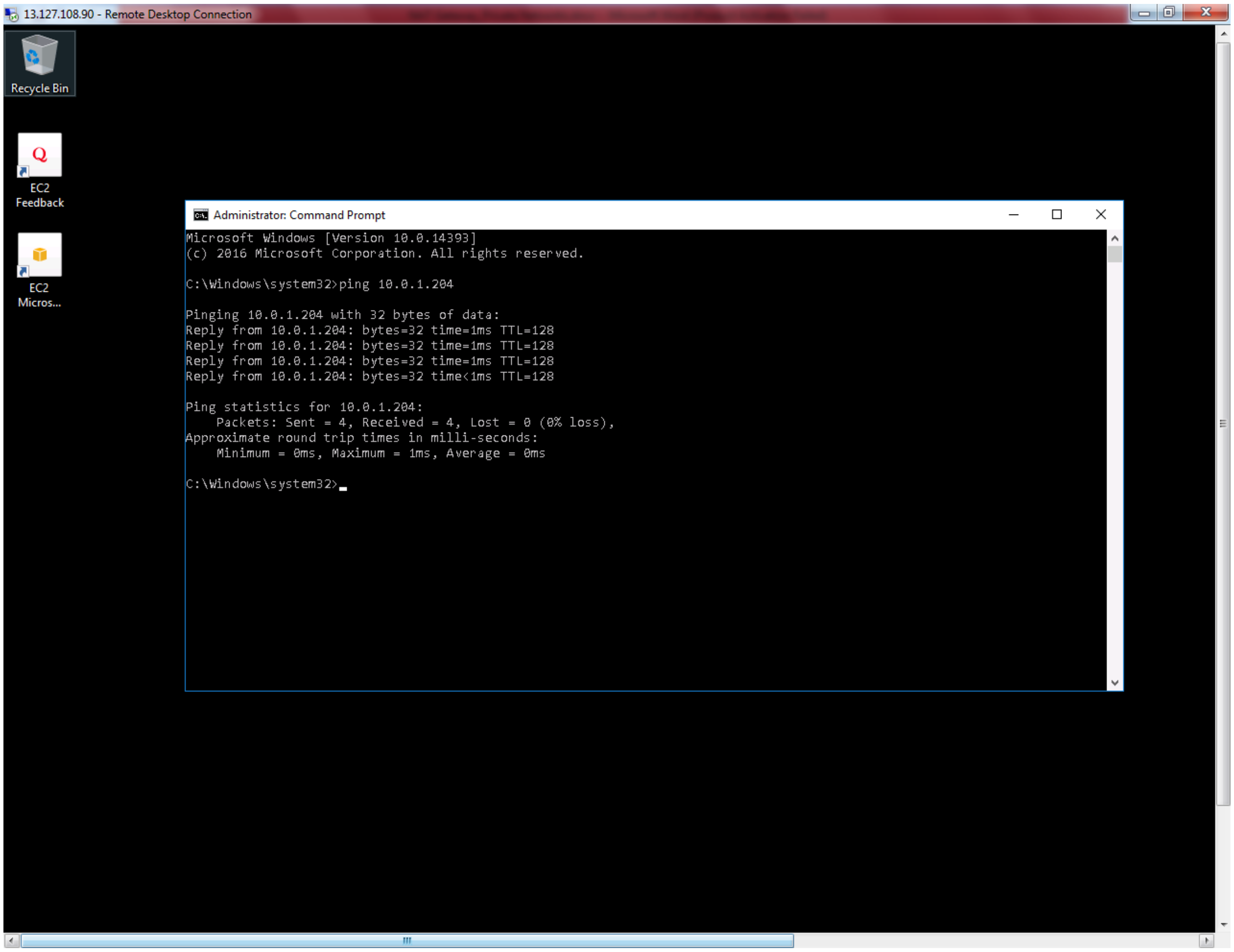
Click ”Ok”.

We can able to connect 10.0.2.14 host from 10.0.1.204.


13.127.108.90 - Remote Desktop Connection
10.0.1.204
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt

```
   IPv4 Address. . . . . . . . . . . : 10.0.1.204
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1

Tunnel adapter isatap.ap-south-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-south-1.compute.internal

Tunnel adapter Local Area Connection* 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:90d7:2c64:113c:dc65:8be4
   Link-local IPv6 Address . . . . . : fe80::2c64:113c:dc65:8be4%5
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>ping 10.0.2.14

Pinging 10.0.2.14 with 32 bytes of data:
Reply from 10.0.2.14: bytes=32 time=1ms TTL=128
Reply from 10.0.2.14: bytes=32 time=1ms TTL=128
Reply from 10.0.2.14: bytes=32 time=1ms TTL=128
Reply from 10.0.2.14: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.2.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Windows\system32>
```

We can able ping 10.0.1.204 host from 10.0.2.14 host.


13.127.108.90 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.0.1.204

Pinging 10.0.1.204 with 32 bytes of data:
Reply from 10.0.1.204: bytes=32 time=1ms TTL=128
Reply from 10.0.1.204: bytes=32 time=1ms TTL=128
Reply from 10.0.1.204: bytes=32 time=1ms TTL=128
Reply from 10.0.1.204: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.1.204:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>_
```