

**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”**

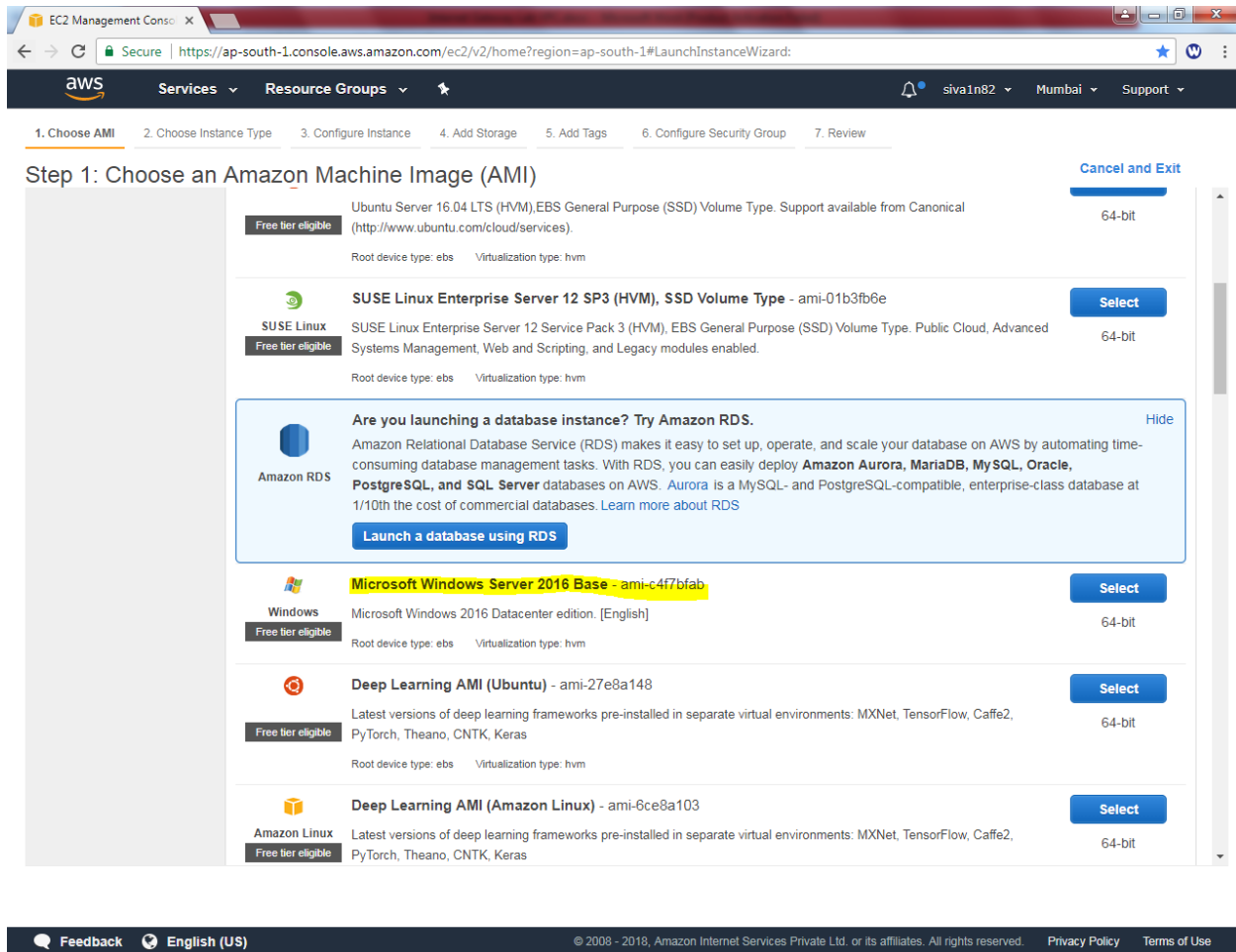
The screenshot shows the AWS Management Console for the EC2 service. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area displays a table of instances with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS (IPv4). A single instance is listed: 'Public Instance' with ID 'i-0ca4dab8e2e09aa1c', type 't2.micro', in 'ap-south-1b' zone, state 'running', and public IP '13.127.108.90'. Below the table, the details for this instance are shown, including its description, status checks, monitoring, and tags. The instance is a 'Public Instance' with a public IP of 13.127.108.90. The details section shows the instance ID, state (running), type (t2.micro), availability zone (ap-south-1b), security groups (Siva\_Public\_Sec\_Group), and public DNS (IPv4) information.

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	13.127.108.90

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

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

In AMI, select “Microsoft windows server 2016-Base”



In Configure instance, Select “Siva\_VPC” in network, “Siva\_Private\_Subnet” in Subnet and “Disable” option in Auto-assign Public IP.

The screenshot shows the 'Step 3: Configure Instance Details' page in the AWS Management Console. The page is for launching an EC2 instance in the 'ap-south-1' region. The navigation bar at the top shows the steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (active), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The user is logged in as 'siva1n82' in the 'Mumbai' region.

**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	<a href="#">Add IP</a>	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

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

Click "Next".

Leave the settings as default

The screenshot shows the AWS Management Console interface for the 'Add Storage' step of the EC2 Launch Wizard. The breadcrumb navigation at the top includes: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (highlighted), 5. Add Tags, 6. Configure Security Group, and 7. Review.

### 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	<input checked="" type="checkbox"/>	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.

Navigation buttons: [Cancel](#), [Previous](#), [Review and Launch](#), [Next: Add Tags](#)

Footer: 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”.

The screenshot shows the AWS Management Console interface for the 'Launch Instance Wizard'. The breadcrumb navigation at the top indicates the current step is '5. Add Tags'. The main heading is 'Step 5: Add Tags', followed by explanatory text: '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 <i>i</i>	Volumes <i>i</i>
Name	Private Instance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Below the table is a button 'Add another tag' with the text '(Up to 50 tags maximum)'.

At the bottom of the wizard, there are four buttons: 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Configure Security Group'.

The footer of the console shows 'Feedback', 'English (US)', and copyright information: '© 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”.

EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:>

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### 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
<input type="checkbox"/> sg-901708f8	default	default VPC security group	<a href="#">Copy to new</a>
<input checked="" type="checkbox"/> sg-410d1229	Siva_Public_Sec_Group	Siva_Public_Sec_Group	<a href="#">Copy to new</a>

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.

Cancel

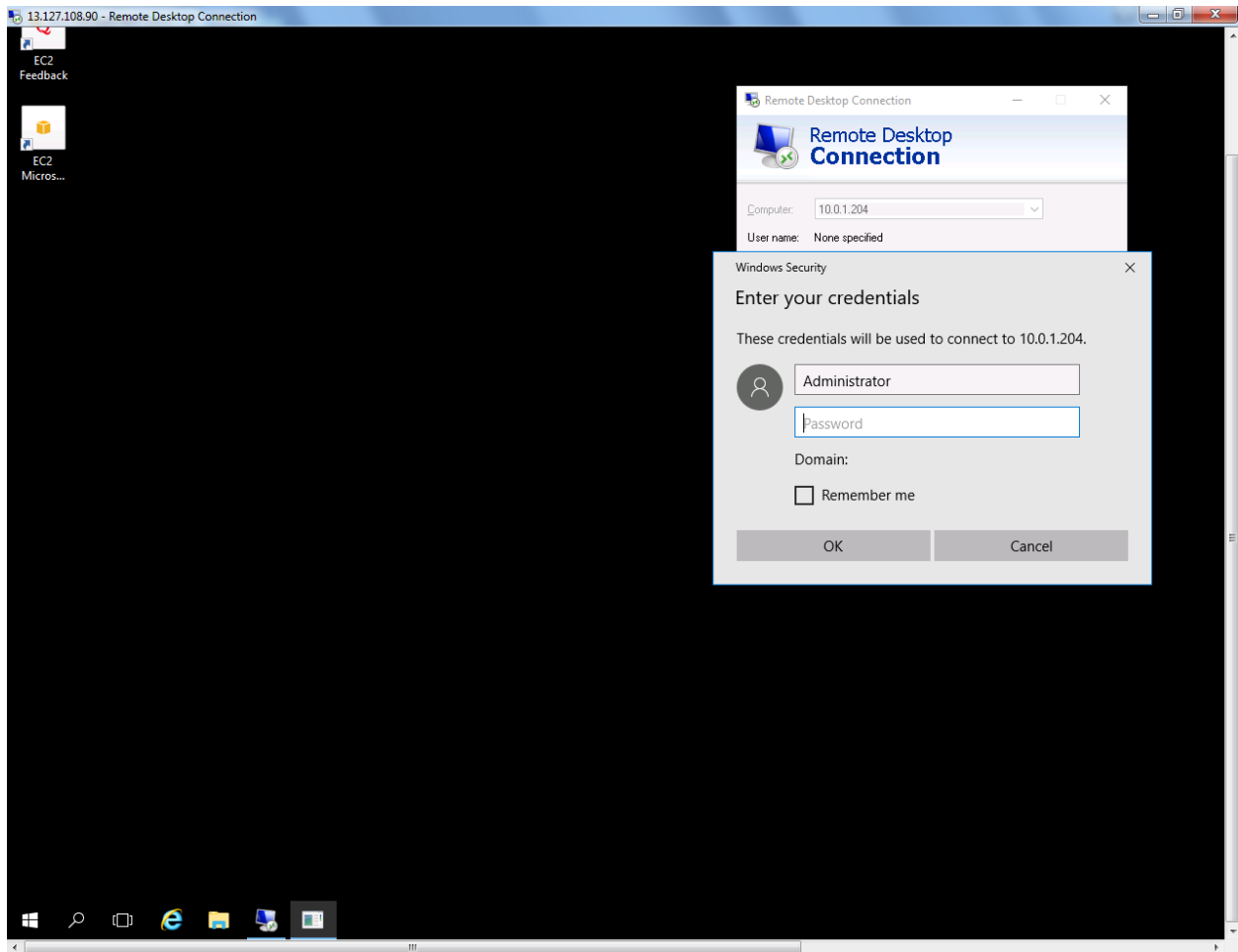
Launch Instances

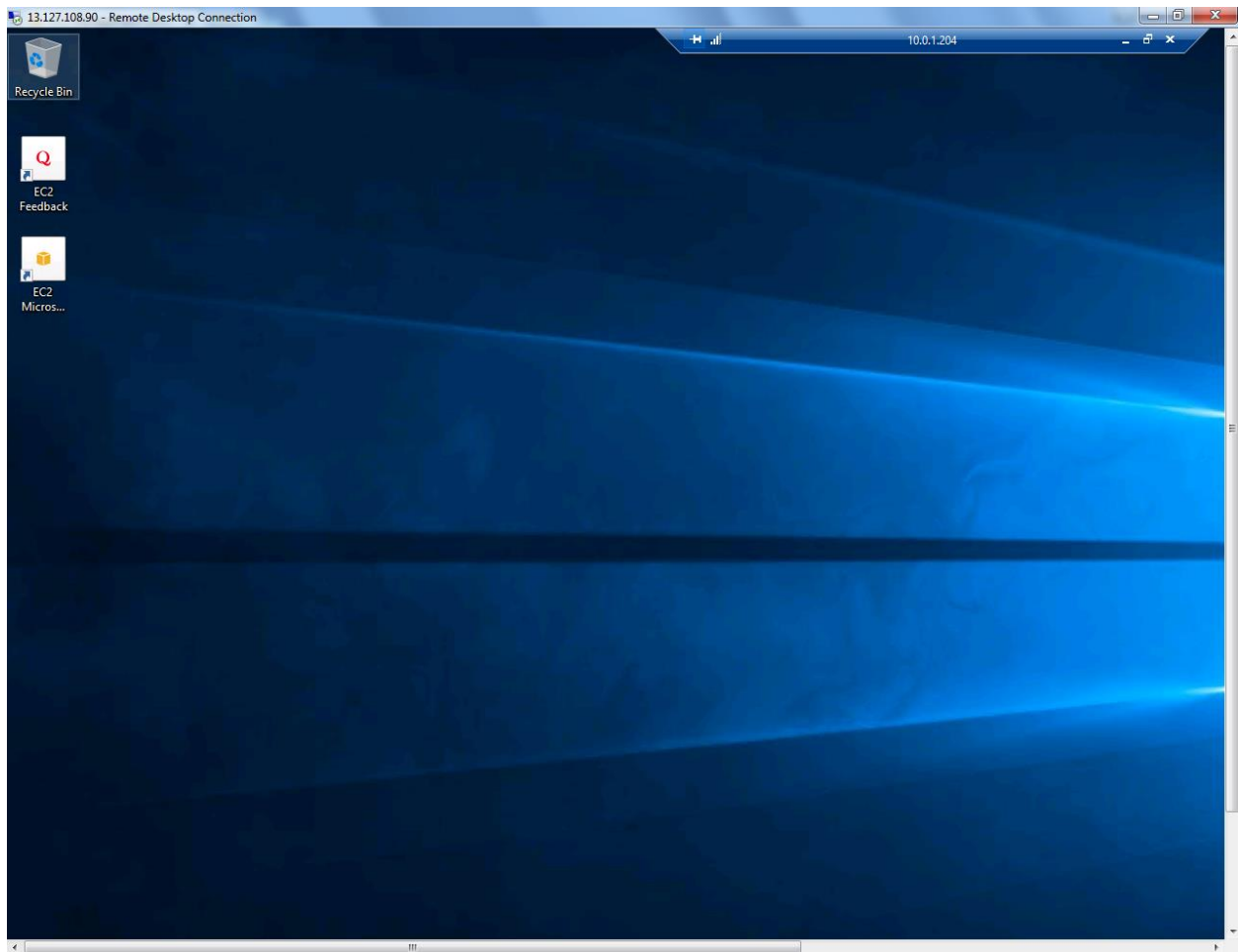
Then click “Launch Instance”.

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

Page 8 of 31

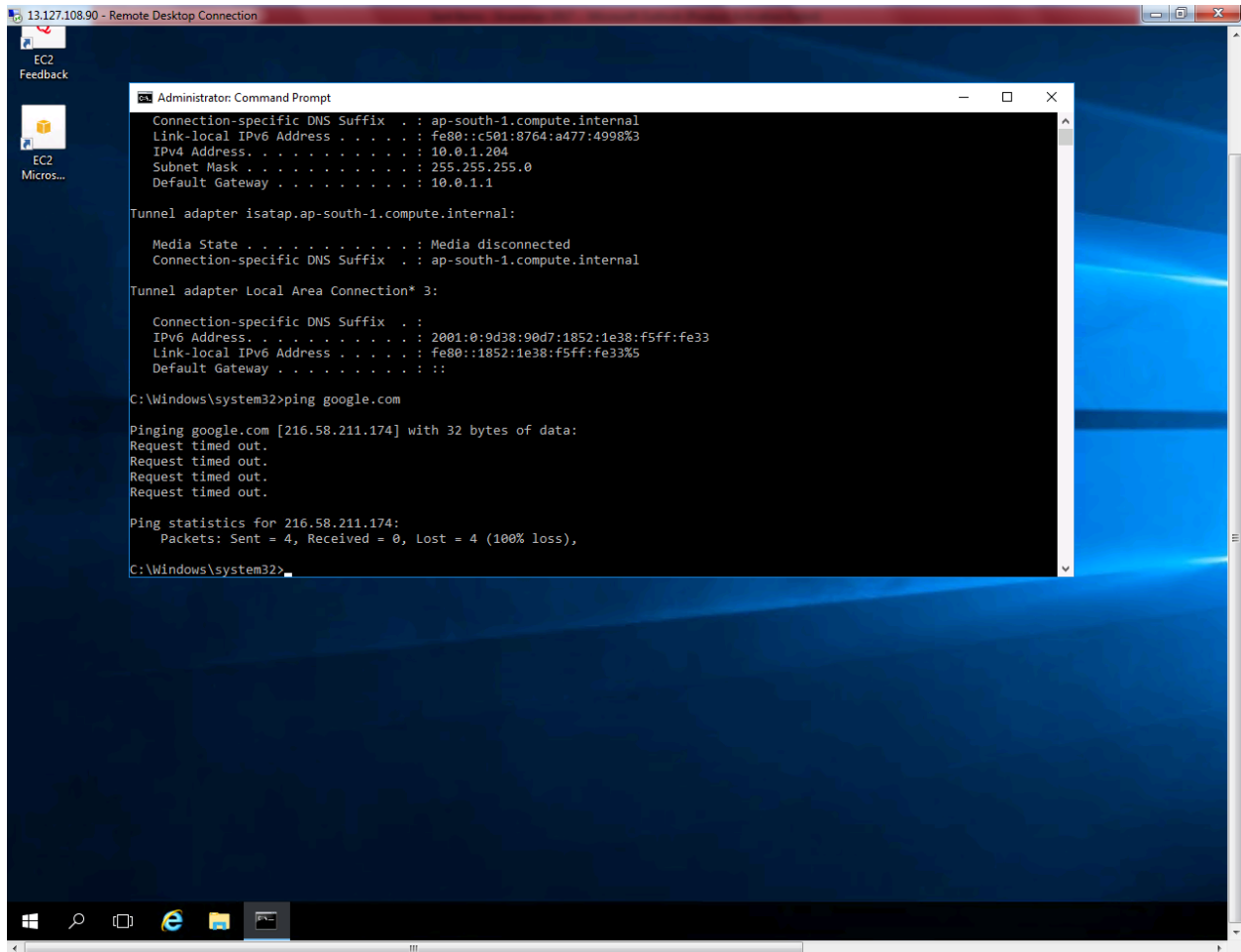




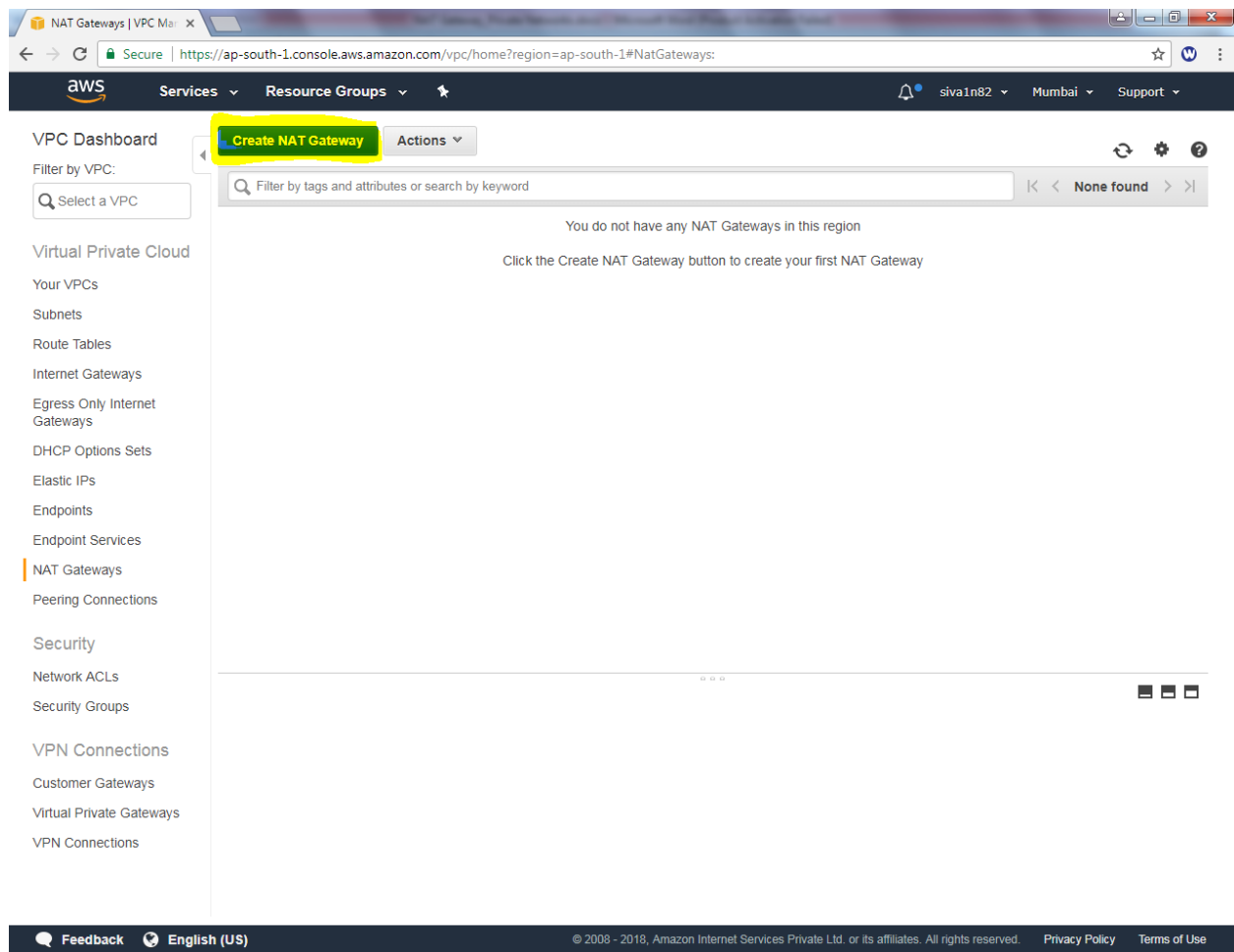


Kindly try to connect internet from 10.0.1.204 machine.

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

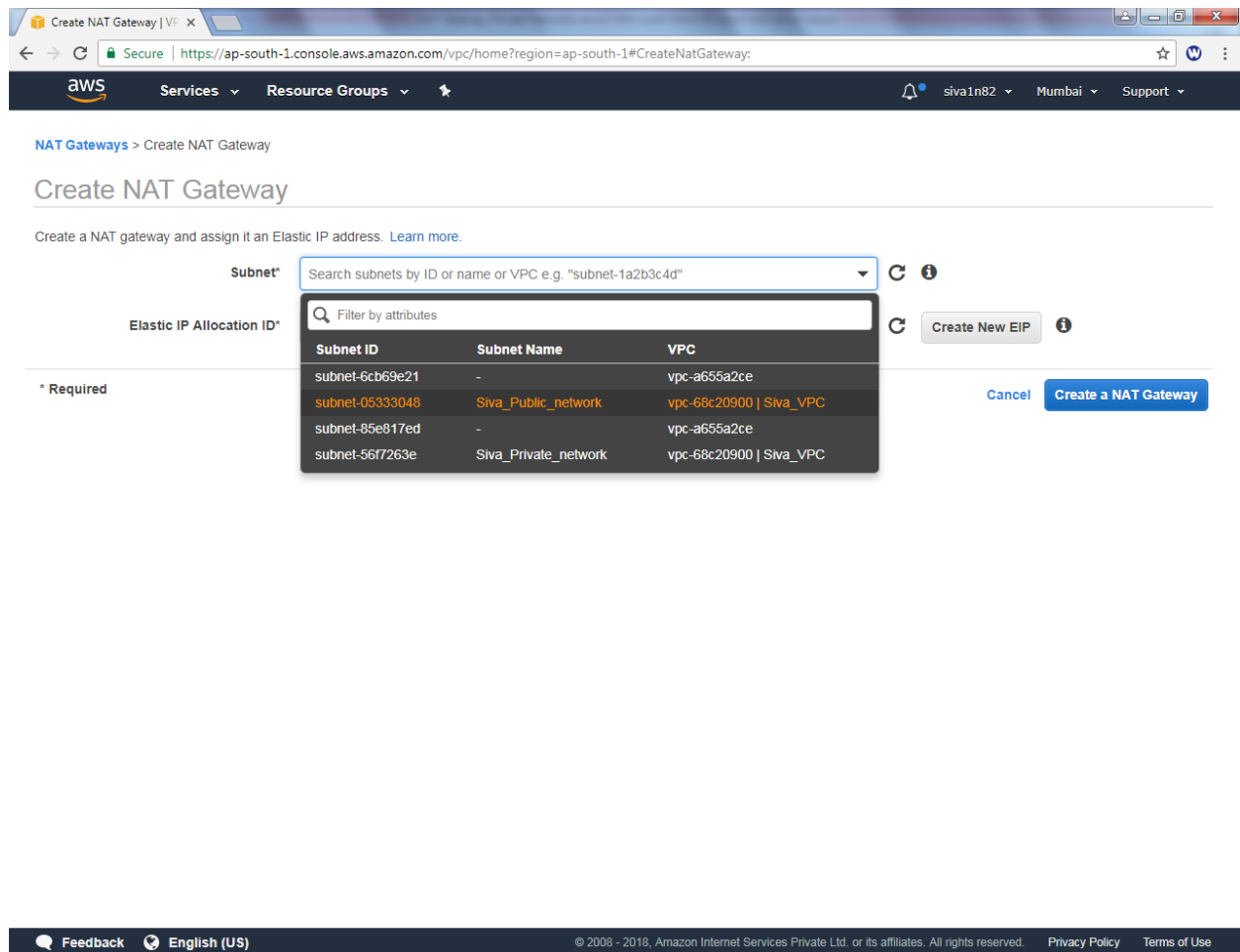


Go to, VPC Dashboard, Select "Nat Gateways"



Click “Create NAT Gateway”.

While creating NAT Gateway, select **“Siva\_Public\_network”**



**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

**\* Required**

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

[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 EIP”

Create NAT Gateway | VPC

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

Create New EIP

New EIP (35.154.116.27) creation successful.

\* Required

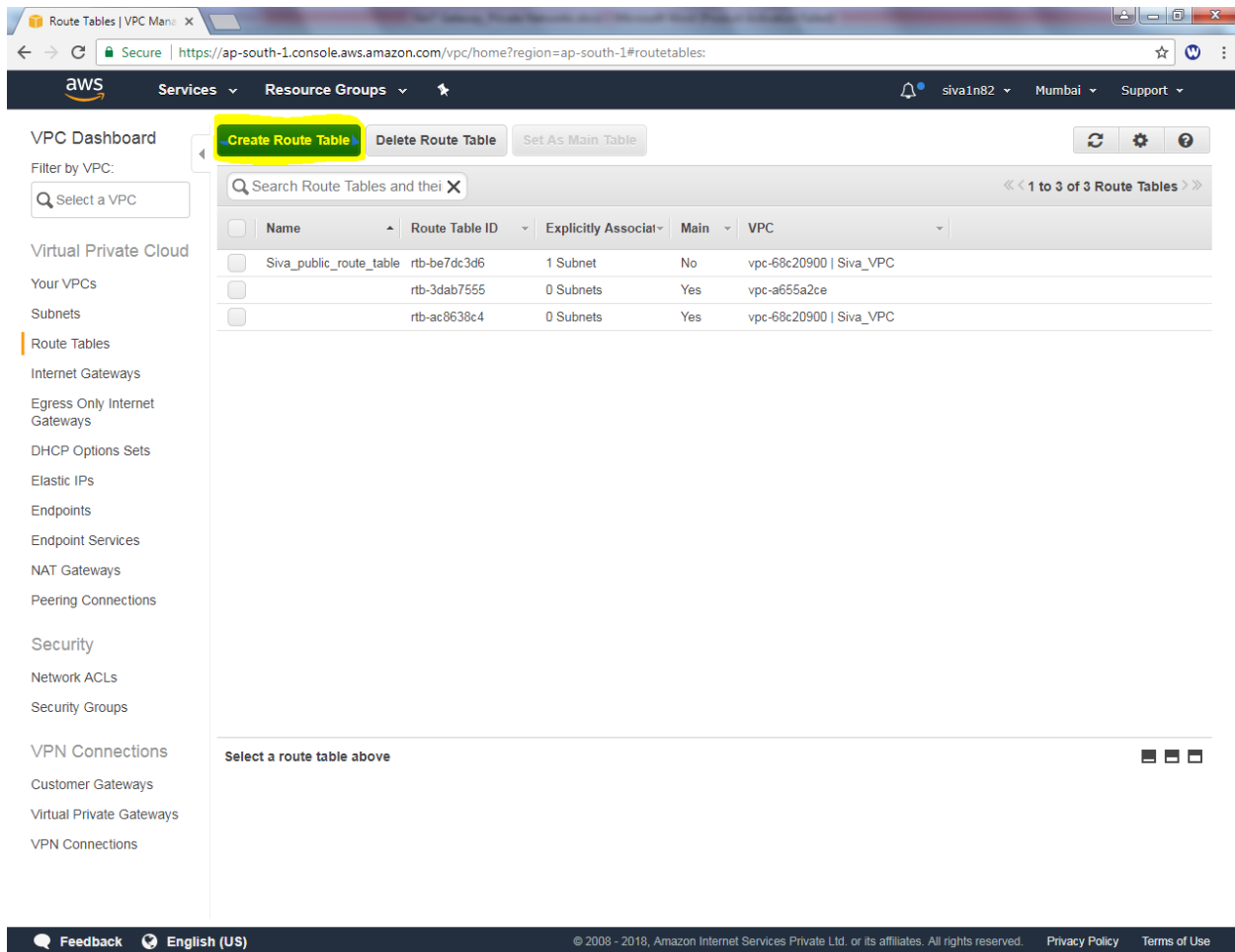
Cancel Create a NAT Gateway

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.



The screenshot shows the AWS VPC console interface. The left sidebar contains a navigation menu with categories like Virtual Private Cloud, Security, and VPN Connections. The main content area displays the 'Route Tables' page for the 'Siva\_VPC'. At the top, there are buttons for 'Create Route Table' (highlighted), 'Delete Route Table', and 'Set As Main Table'. Below these is a search bar and a table listing the route tables. The table has columns for Name, Route Table ID, Explicitly Associated, Main, and VPC. There are three entries in the table, all associated with 'Siva\_VPC'.

Name	Route Table ID	Explicitly Associated	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

Cancel

Yes, Create

Then Click **“Yes create”**.

In Route Table, click edit button.



The screenshot shows the AWS Management Console interface for Route Tables. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and various network services. The main content area displays a list of Route Tables and a detailed view of the selected route.

**Route Tables List:**

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

**Route Details (Routes tab):**

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

In Edit option, click “Add another route”

The screenshot displays the AWS Management Console interface for Route Tables. The left sidebar shows the navigation menu with categories like VPC Dashboard, Virtual Private Cloud, Security, and VPN Connections. The main content area shows a list of route tables. The 'Siva\_Private\_route\_table' is selected, and the 'Routes' tab is active. Below the tab, a table shows the existing route with destination 10.0.0.0/16 and target 'local'. An 'Add another route' button is located at the bottom of the route list.

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

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	

[Add another route](#)

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

Route Tables | VPC Manager

Secure | <https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#routetables>

aws Services Resource Groups

siva1n82 Mumbai Support

VPC Dashboard

Filter by VPC: Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their VPCs

<< 1 to 4 of 4 Route Tables >>

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

Cancel Save

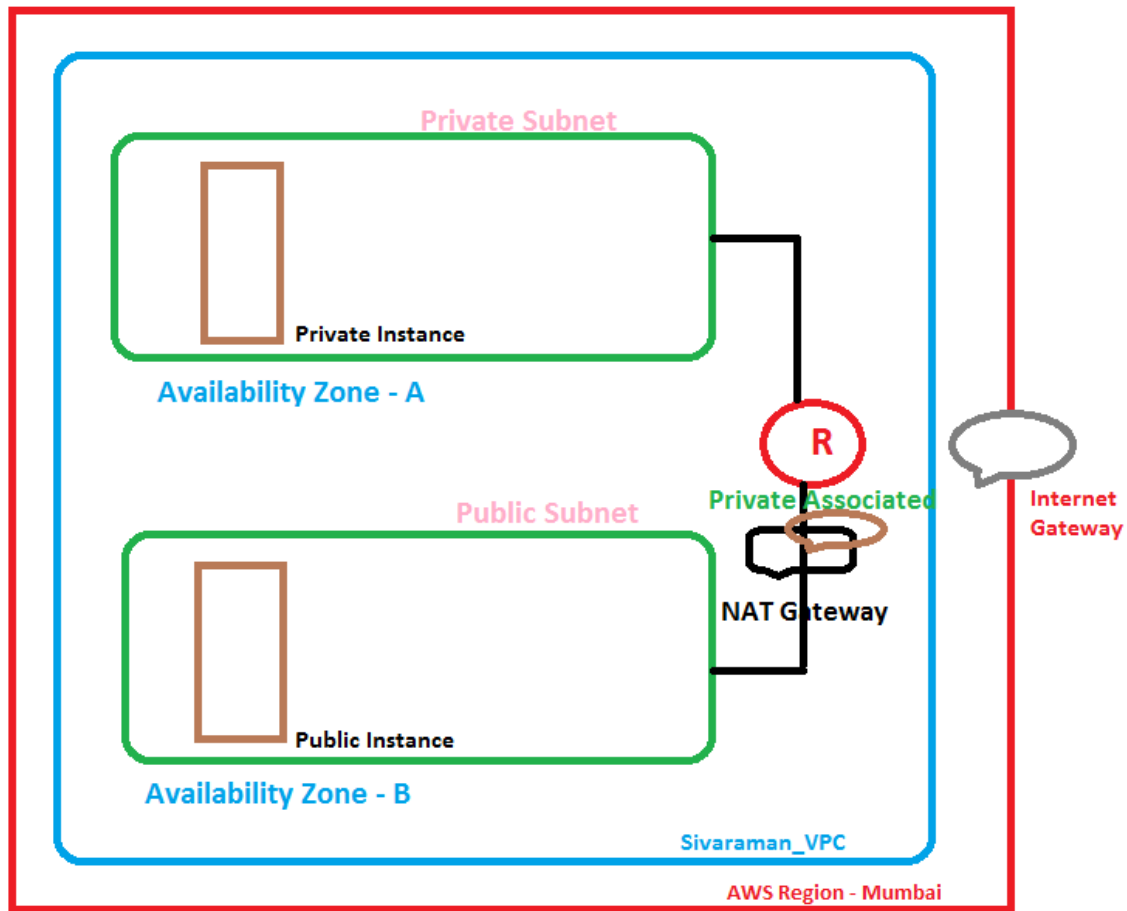
View: All rules

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

Feedback English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click "save".



In Subnet associations., click "Edit" options

The screenshot shows the AWS Management Console interface for Route Tables. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and various network services. The main content area displays a list of route tables. The 'Siva\_Private\_route\_table' is selected, and the 'Subnet Associations' tab is active. The message 'You do not have any subnet associations.' is displayed.

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

rtb-4573cd2d | Siva\_Private\_route\_table

Summary Routes **Subnet Associations** Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations.		

In Subnet associations, select “Siva\_private\_subnet” then click save.

The screenshot displays the AWS Management Console interface for the 'Route Tables' section. The left-hand navigation pane lists various VPC services, with 'Route Tables' currently selected. The main content area shows a list of route tables. The 'Siva\_Private\_route\_tabl' is selected, and the 'Subnet Associations' tab is active. Below this, a table lists the subnets associated with the selected route table.

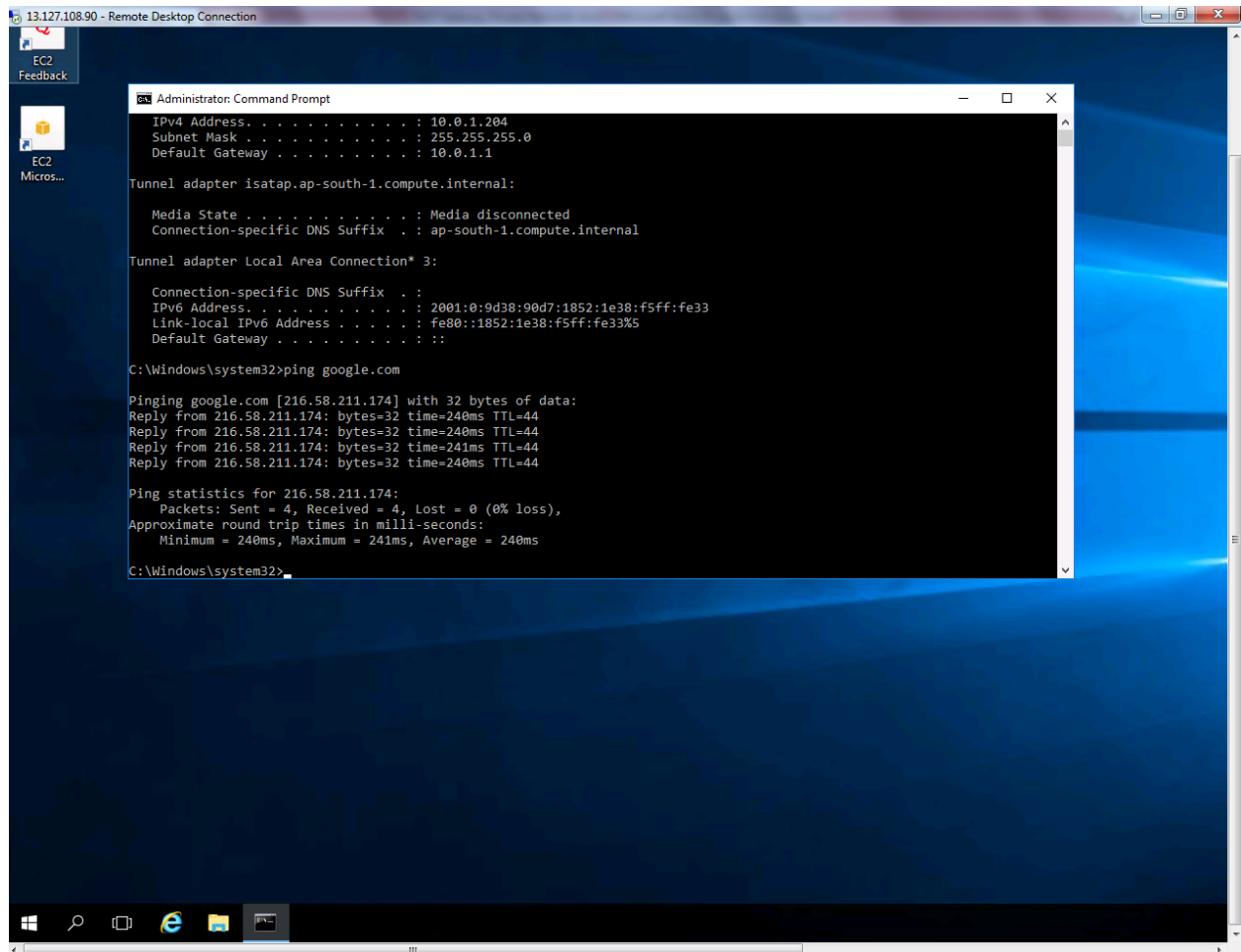
**Route Tables List:**

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

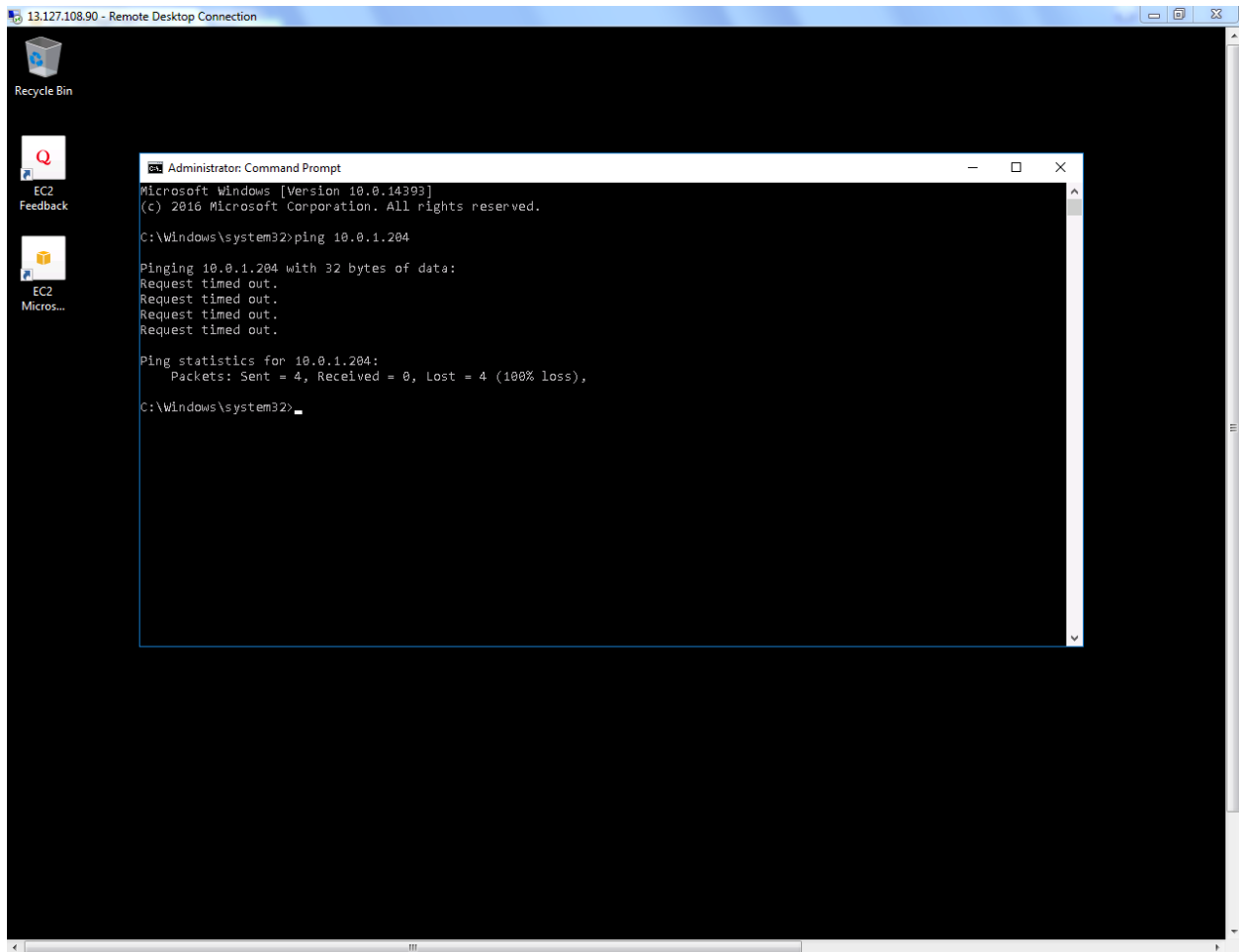
**Subnet Associations Table:**

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-56f7263e   Siva_Private_network	10.0.1.0/24	-	Main
<input type="checkbox"/>	subnet-05333048   Siva_Public_network	10.0.2.0/24	-	rtb-be7dc3d6   Siva_public_route_table

Now we are able to connect internet.



Now try to ping private subnet 10.0.1.204 from 10.0.2.14



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.



The screenshot displays the AWS Management Console interface for the 'Security Groups' section. The left-hand navigation pane shows various AWS services, with 'Security Groups' highlighted under the 'NETWORK & SECURITY' category. The main content area shows a list of security groups. The 'Public Sec Group' (sg-410d1229) is selected. Below the list, the details for this security group are shown, including the 'Inbound' tab which lists a single rule for RDP access over TCP on port 3389 from 0.0.0.0/0. The 'Edit' button is highlighted in yellow.

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-jxrbp8kx5-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

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

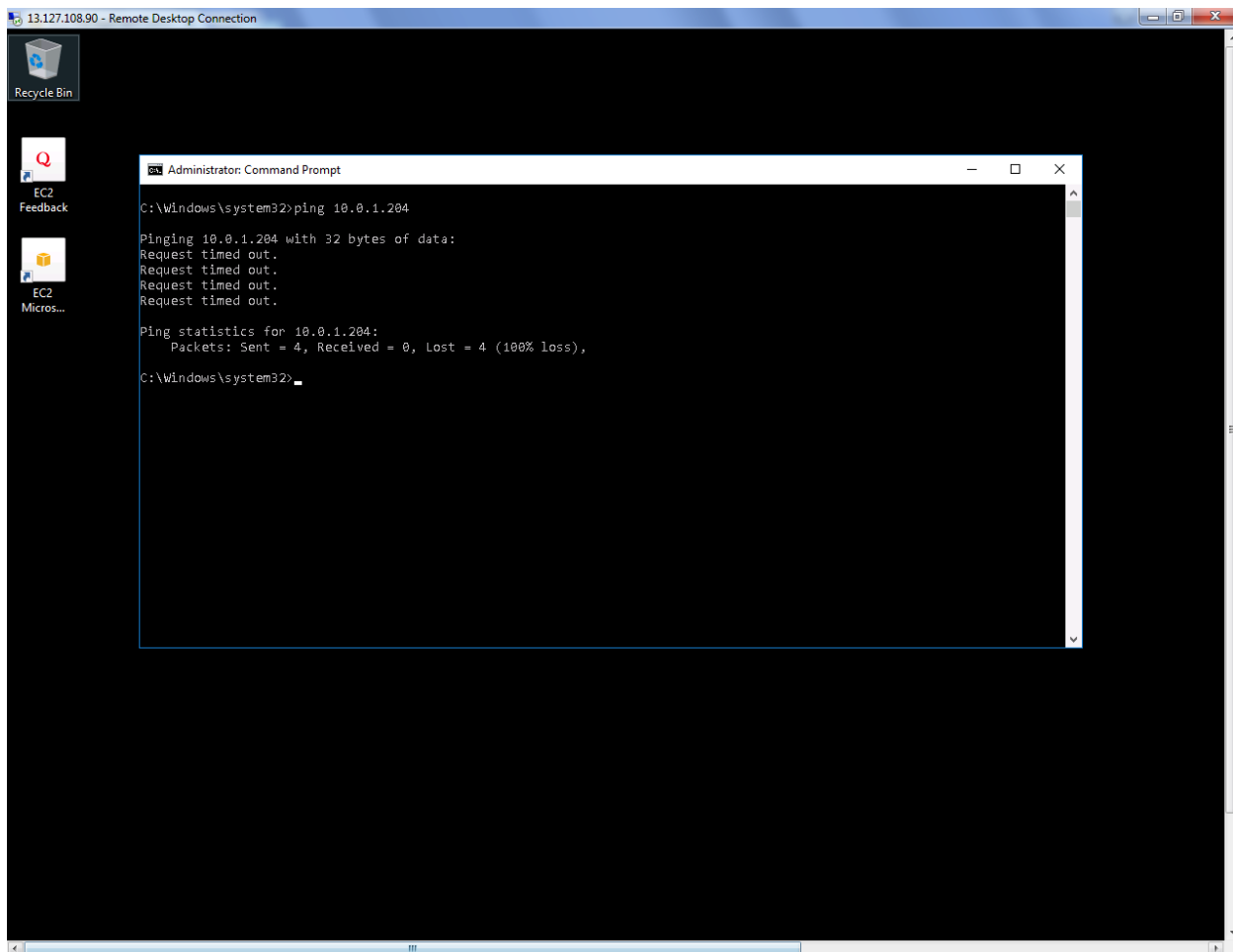
Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
Custom ICMP	All	N/A	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

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.

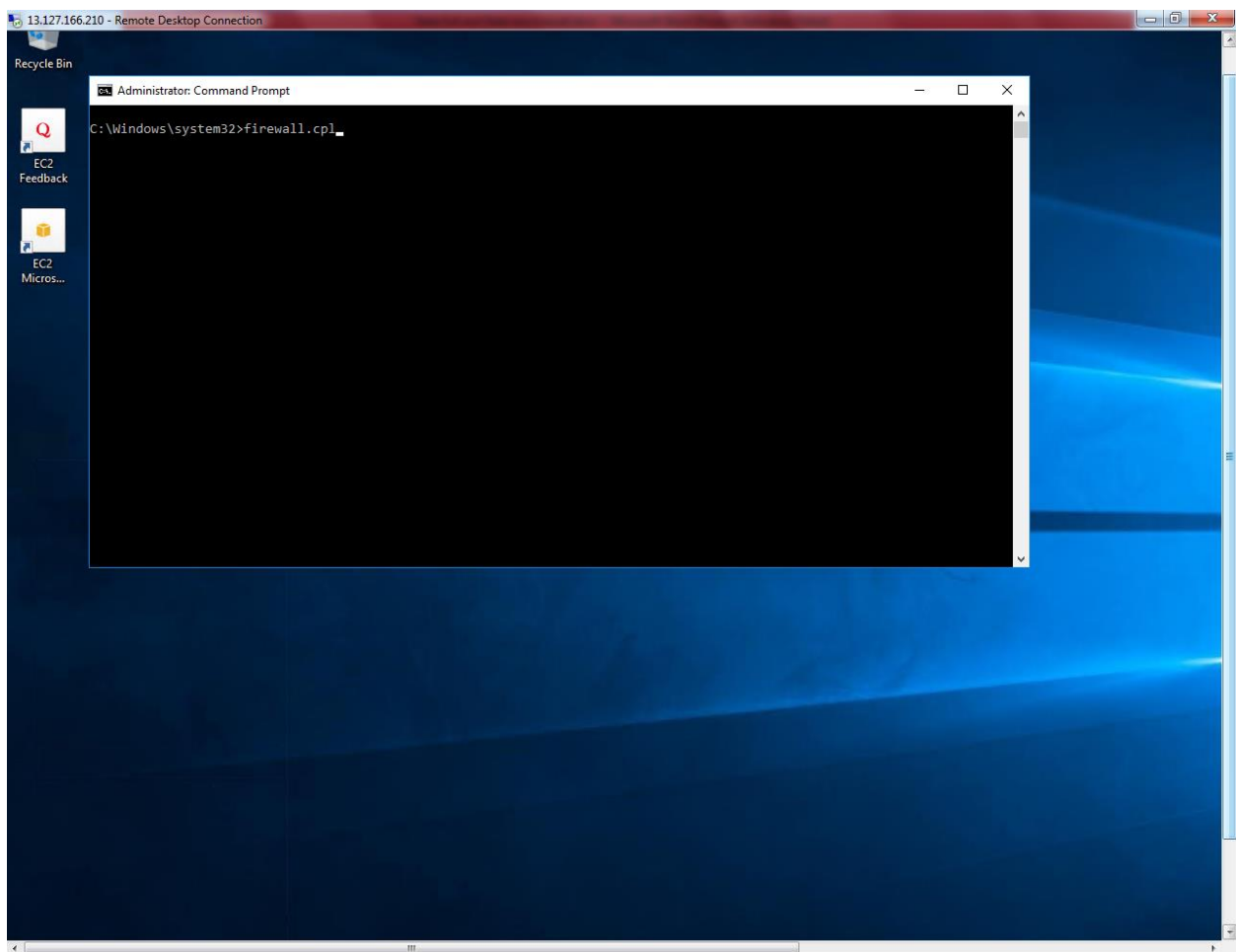
Cancel Save

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.

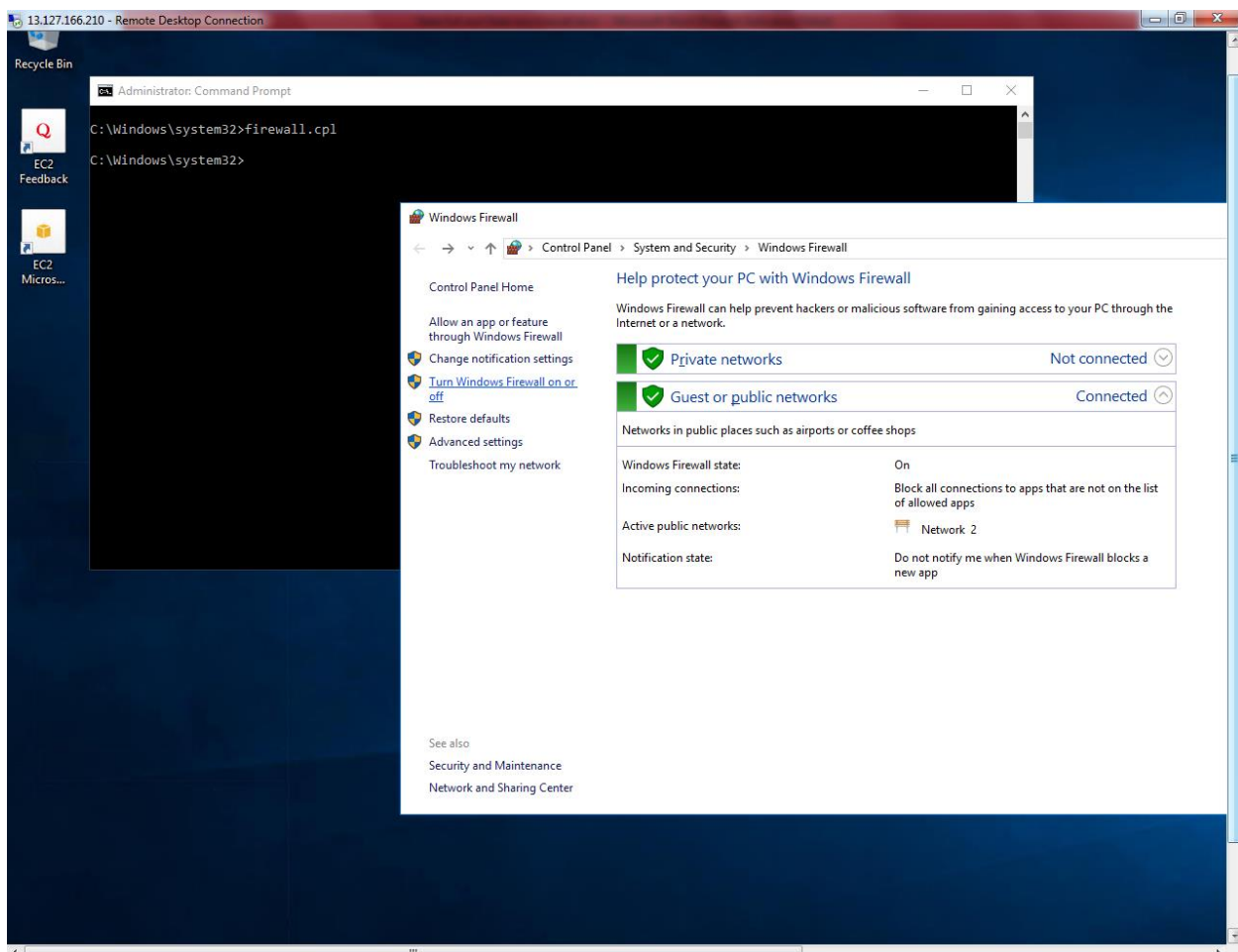


Hence, we need to turn off the windows firewall in both servers.

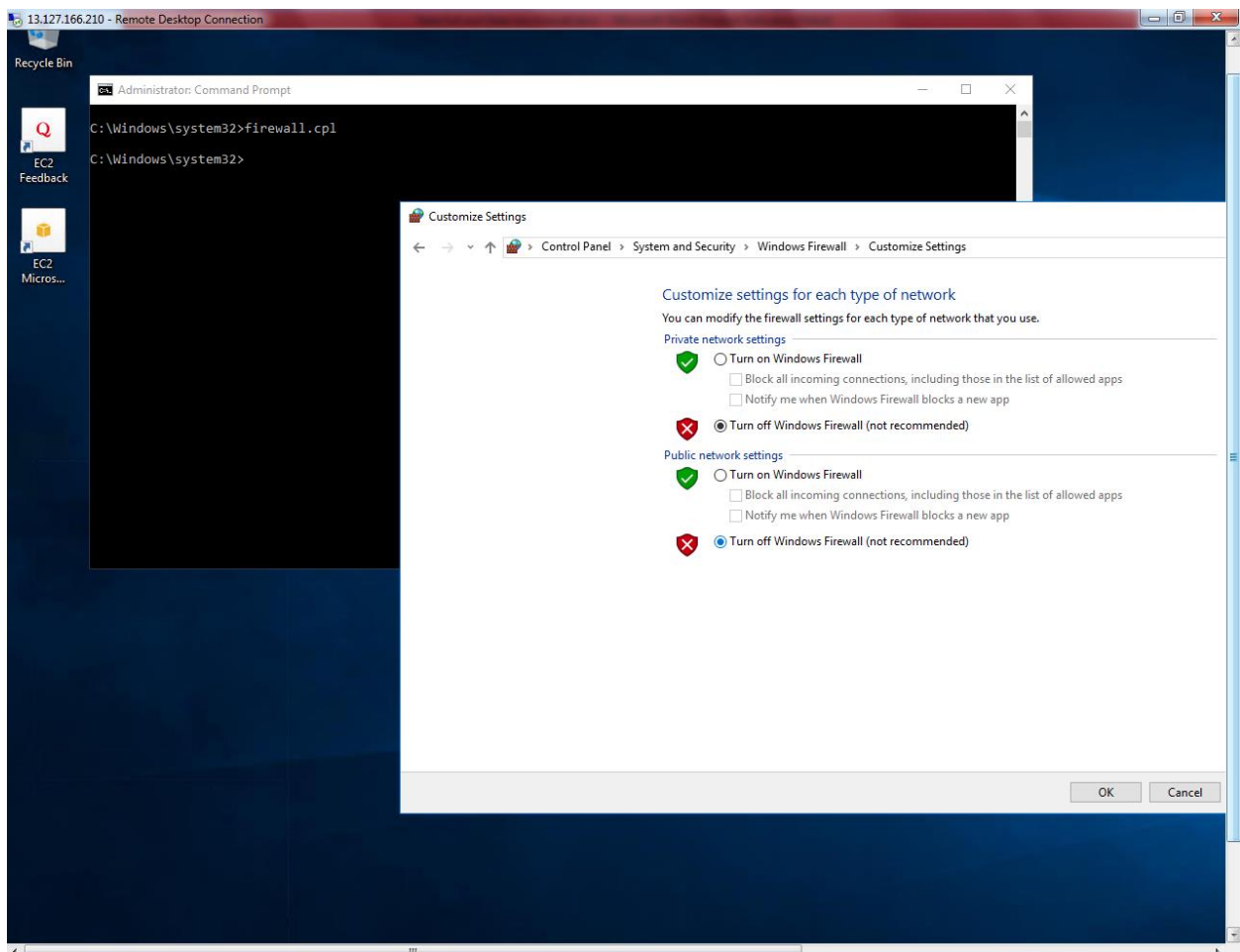
### Type Firewall.cpl



Click “Turn Windows Firewall on or Off”.

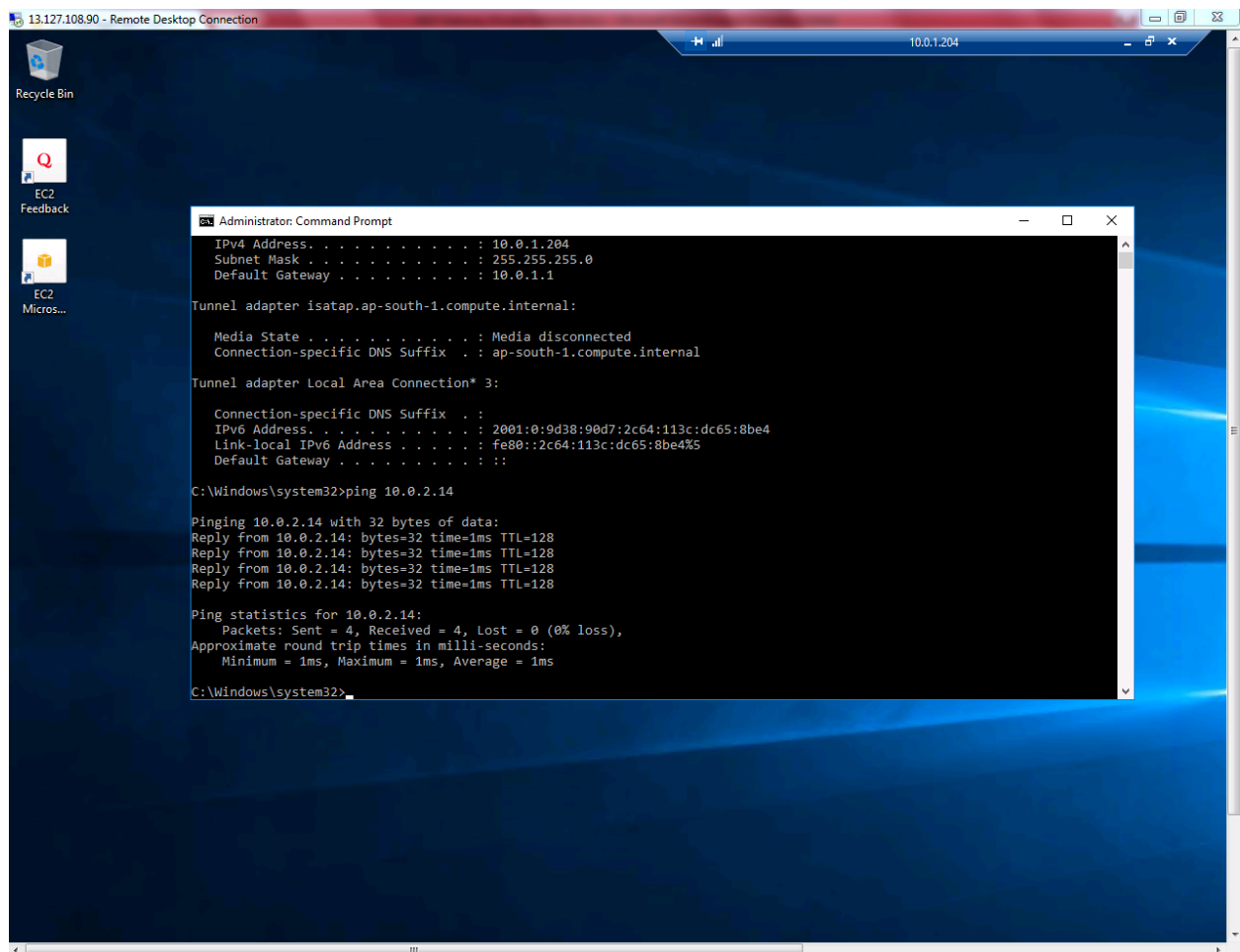


### Turn off windows firewall.



Click "Ok".

We can able to connect 10.0.2.14 host from 10.0.1.204.



We can able ping 10.0.1.204 host from 10.0.2.14 host.

