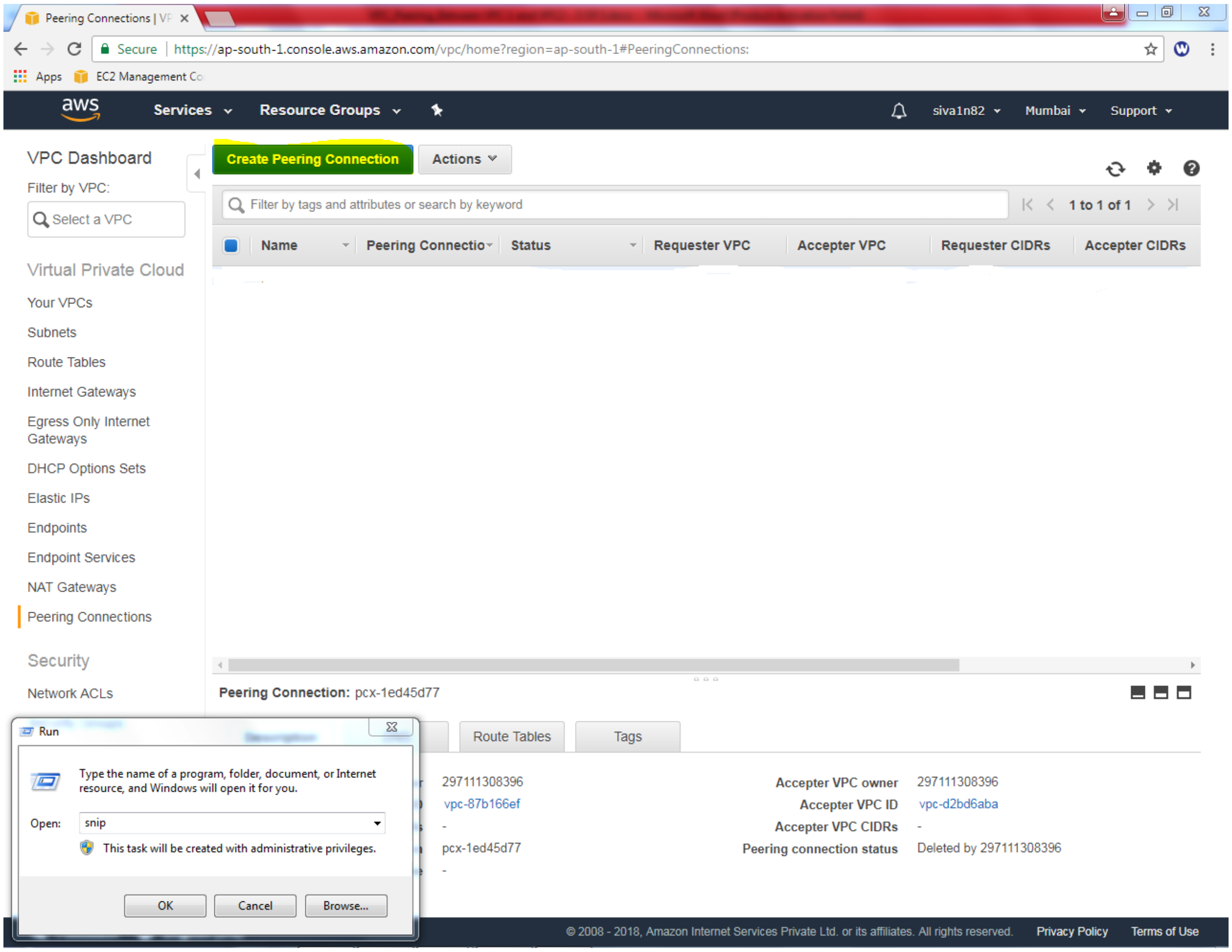
Lab 13

Configure VPC Peering Between two VPC's – 3 of 3

In VPC Dashboard,

Go to Peering Connections.



Peering Connection: pcx-1ed45d77

	297111308396	Accepter VPC owner	297111308396
	vpc-87b166ef	Accepter VPC ID	vpc-d2bd6aba
	-	Accepter VPC CIDRs	-
	pcx-1ed45d77	Peering connection status	Deleted by 297111308396
	-		

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: snip

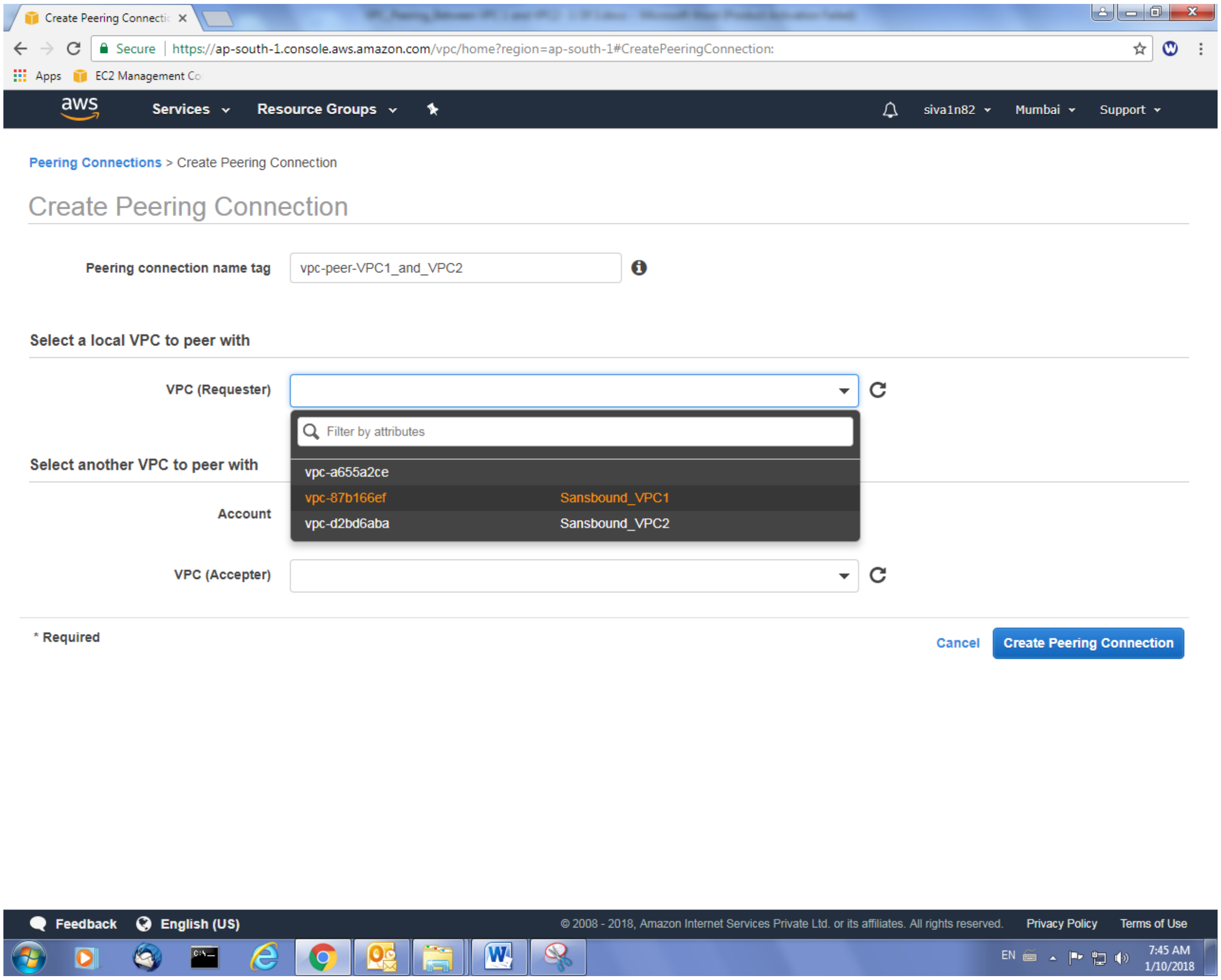
This task will be created with administrative privileges.

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

In Peering connection,

Peering Connection Name tag: vpc-peer-VPC1_and_VPC2

VPC Requestor (Select – VPC1)



Create Peering Connectio
https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreatePeeringConnection:
Apps
EC2 Management Co
aws
Services
Resource Groups
siva1n82
Mumbai
Support

Peering Connections > Create Peering Connection

Create Peering Connection

Peering connection name tag: vpc-peer-VPC1_and_VPC2

Select a local VPC to peer with

VPC (Requester)

Filter by attributes

vpc-a655a2ce	
vpc-87b166ef	Sansbound_VPC1
vpc-d2bd6aba	Sansbound_VPC2

Select another VPC to peer with

Account

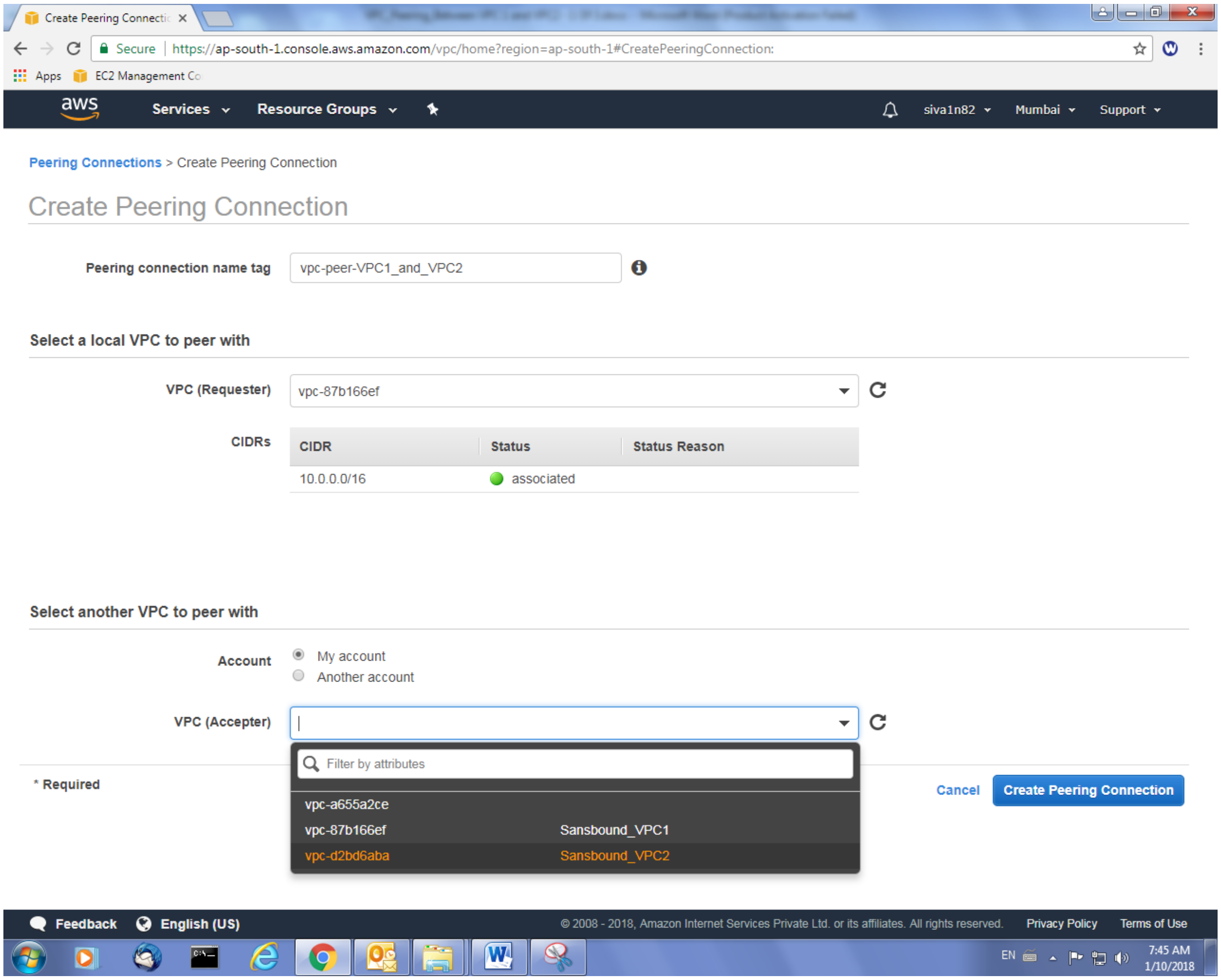
VPC (Accepter)

* Required

Cancel | Create Peering Connection

Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
EN
7:45 AM
1/10/2018

VPC Accepter “Select VPC2”



Create Peering Connectio
Secure
https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreatePeeringConnection:
Apps
EC2 Management Co
aws
Services
Resource Groups
siva1n82
Mumbai
Support
Peering Connections > Create Peering Connection

Create Peering Connection

Peering connection name tag: vpc-peer-VPC1_and_VPC2

Select a local VPC to peer with

VPC (Requester): vpc-87b166ef

CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	● associated	

Select another VPC to peer with

Account
● My account
○ Another account

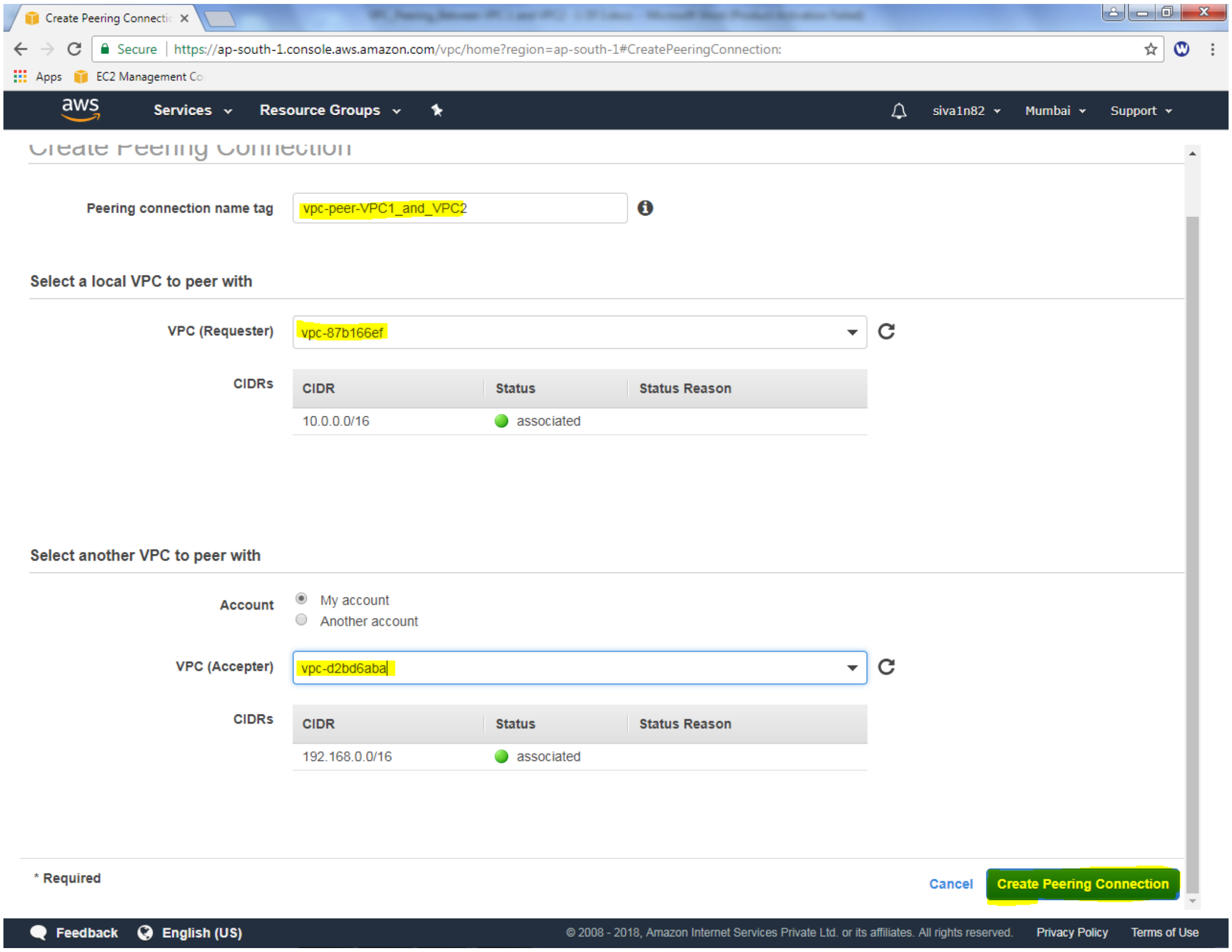
VPC (Accepter):

Filter by attributes

vpc-a655a2ce	
vpc-87b166ef	Sansbound_VPC1
vpc-d2bd6aba	Sansbound_VPC2

* Required

Cancel
Create Peering Connection
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
EN
7:45 AM
1/10/2018



Create Peering Connecti
Secure
https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreatePeeringConnection:
Apps
EC2 Management Co
aws
Services
Resource Groups
siva1n82
Mumbai
Support

Create Peering Connection

Peering connection name tag: vpc-peer-VPC1_and_VPC2

Select a local VPC to peer with

VPC (Requester): vpc-87b166ef

CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	● associated	

Select another VPC to peer with

Account: ● My account ○ Another account

VPC (Accepter): vpc-d2bd6aba

CIDRs

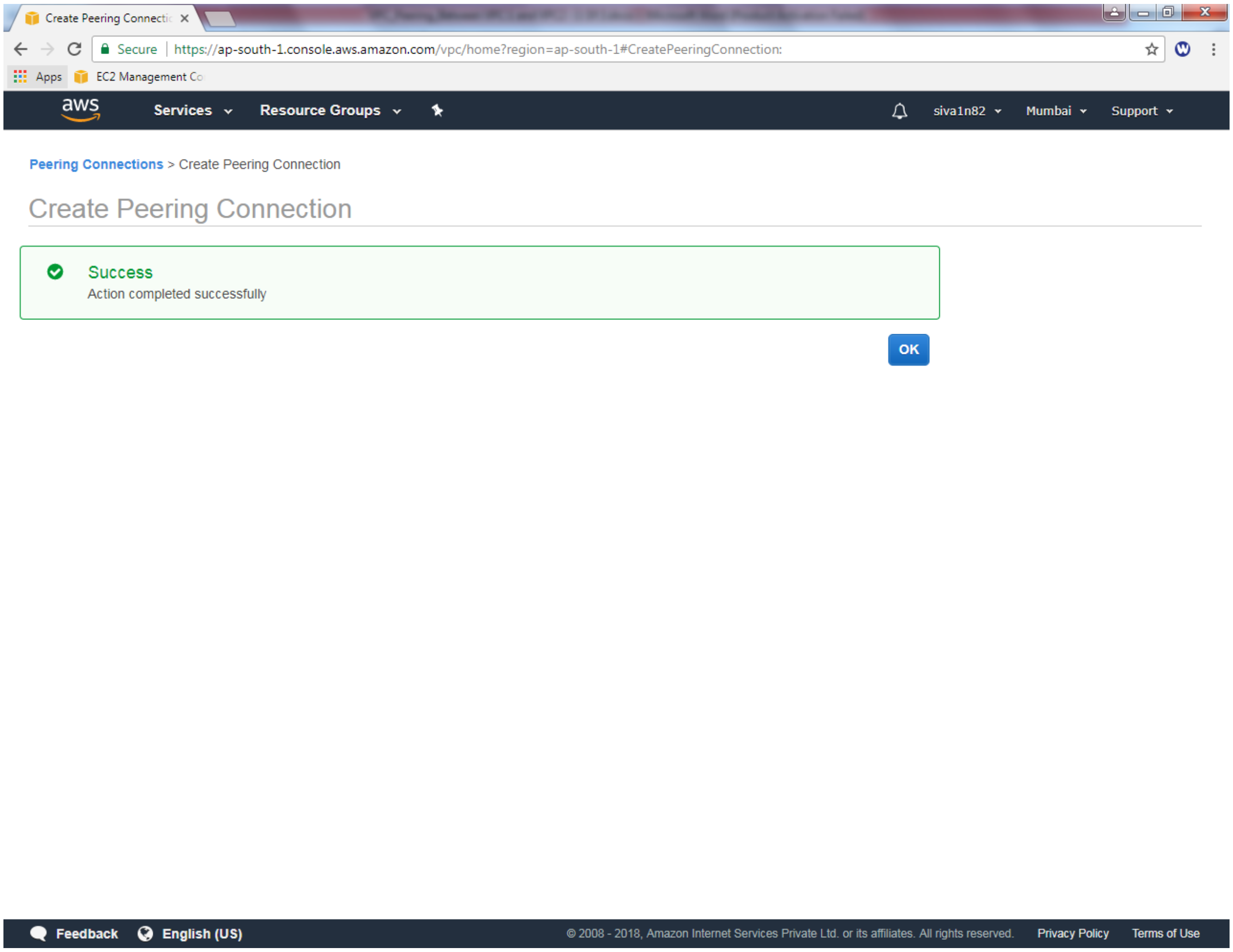
CIDR	Status	Status Reason
192.168.0.0/16	● associated	

* Required

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

Click “Creat peering Connection”.

VPC Peer configured successfully.

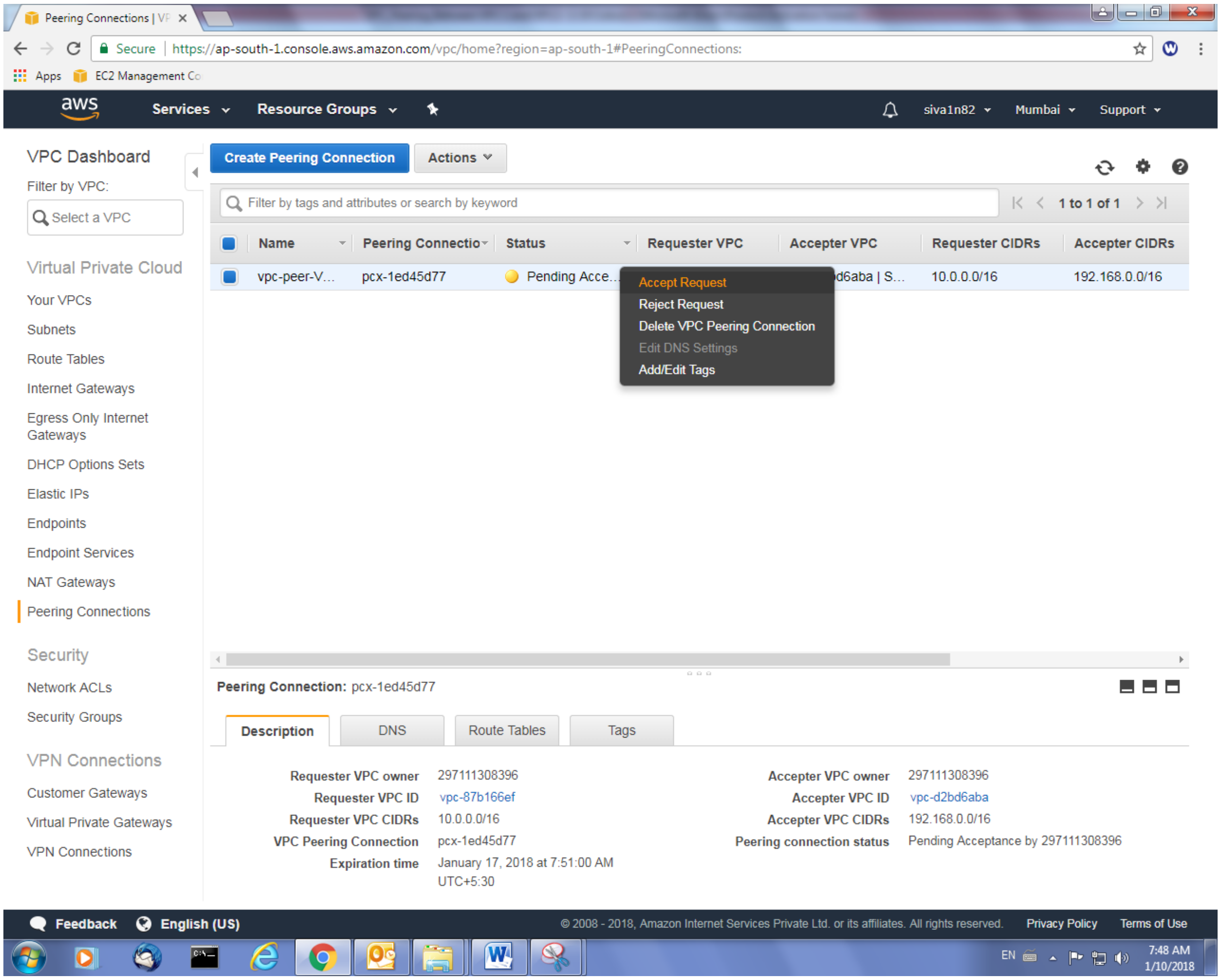

Create Peering Connecti
Secure
https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreatePeeringConnection:
Apps
EC2 Management Co
aws
Services
Resource Groups
siva1n82
Mumbai
Support
Peering Connections > Create Peering Connection

Create Peering Connection

Success
Action completed successfully

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

Goto Mumbai, peering connection, “Click Accept”



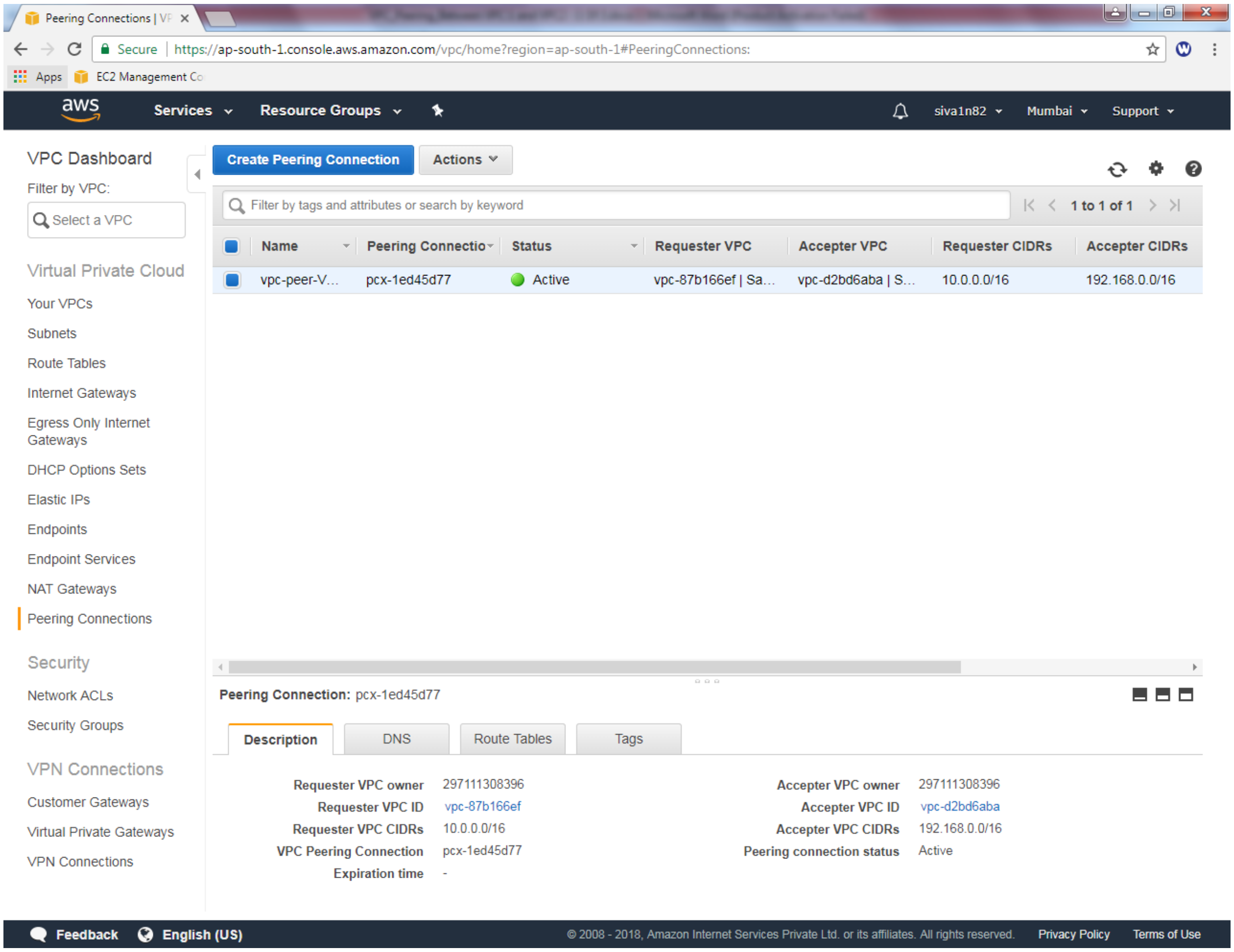
Name	Peering Connectio	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
vpc-peer-V...	pcx-1ed45d77	Pending Acce...		d6aba | S...	10.0.0.0/16	192.168.0.0/16

Peering Connection: pcx-1ed45d77

Requester VPC owner	297111308396	Accepter VPC owner	297111308396
Requester VPC ID	vpc-87b166ef	Accepter VPC ID	vpc-d2bd6aba
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	192.168.0.0/16
VPC Peering Connection Expiration time	pcx-1ed45d77 January 17, 2018 at 7:51:00 AM UTC+5:30	Peering connection status	Pending Acceptance by 297111308396

Then Click “Yes, Accept”.

Now VPC peer is active.



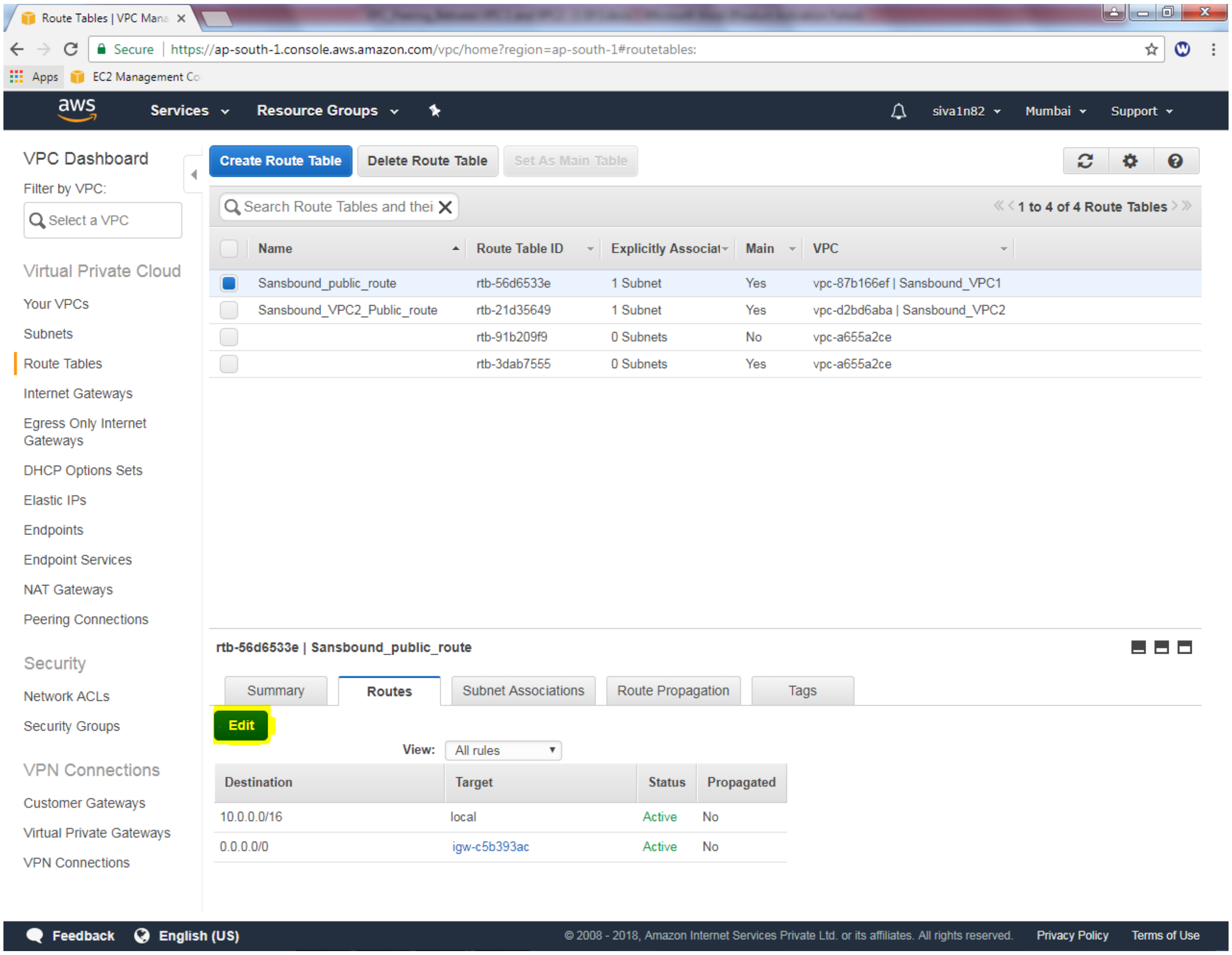
	Name	Peering Connectio	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
■	vpc-peer-V...	pcx-1ed45d77	● Active	vpc-87b166ef | Sa...	vpc-d2bd6aba | S...	10.0.0.0/16	192.168.0.0/16

Peering Connection: pcx-1ed45d77

Requester VPC owner	297111308396	**Accepter VPC owner**	297111308396
Requester VPC ID	vpc-87b166ef	**Accepter VPC ID**	vpc-d2bd6aba
Requester VPC CIDRs	10.0.0.0/16	**Accepter VPC CIDRs**	192.168.0.0/16
VPC Peering Connection	pcx-1ed45d77	**Peering connection status**	Active
Expiration time	-		

Now, you can try RDP for VPC2 subnet from VPC1 subnet. You are not able to get RDP. Because you need to add VPC2 subnet in VPC1 Public route table.

In Route tab, click “Edit”.

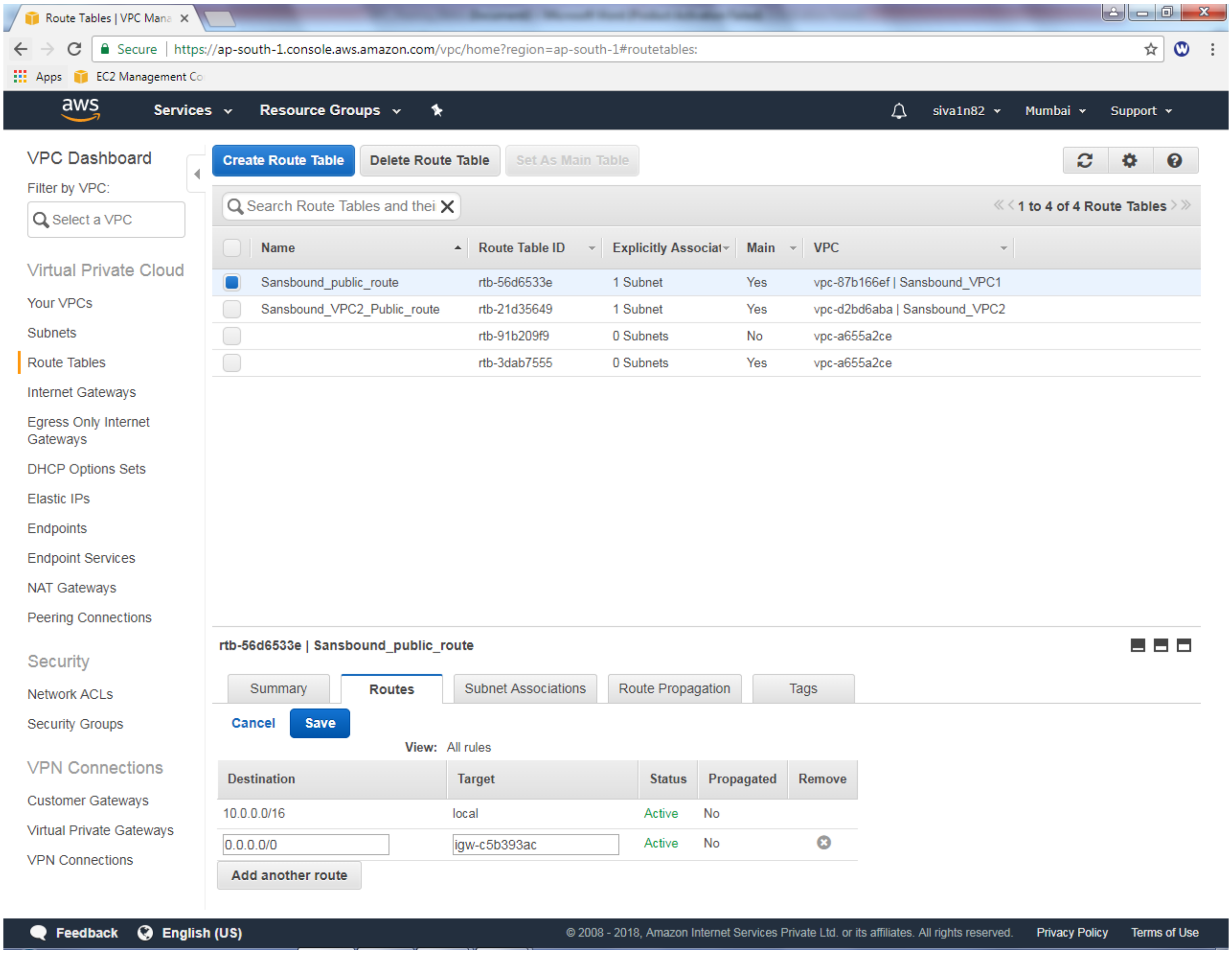


	Name	Route Table ID	Explicitly Associat	Main	VPC
☑	Sansbound_public_route	rtb-56d6533e	1 Subnet	Yes	vpc-87b166ef | Sansbound_VPC1
□	Sansbound_VPC2_Public_route	rtb-21d35649	1 Subnet	Yes	vpc-d2bd6aba | Sansbound_VPC2
□		rtb-91b209f9	0 Subnets	No	vpc-a655a2ce
□		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce

rtb-56d6533e | Sansbound_public_route

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-c5b393ac	Active	No

Click “Add another route”.



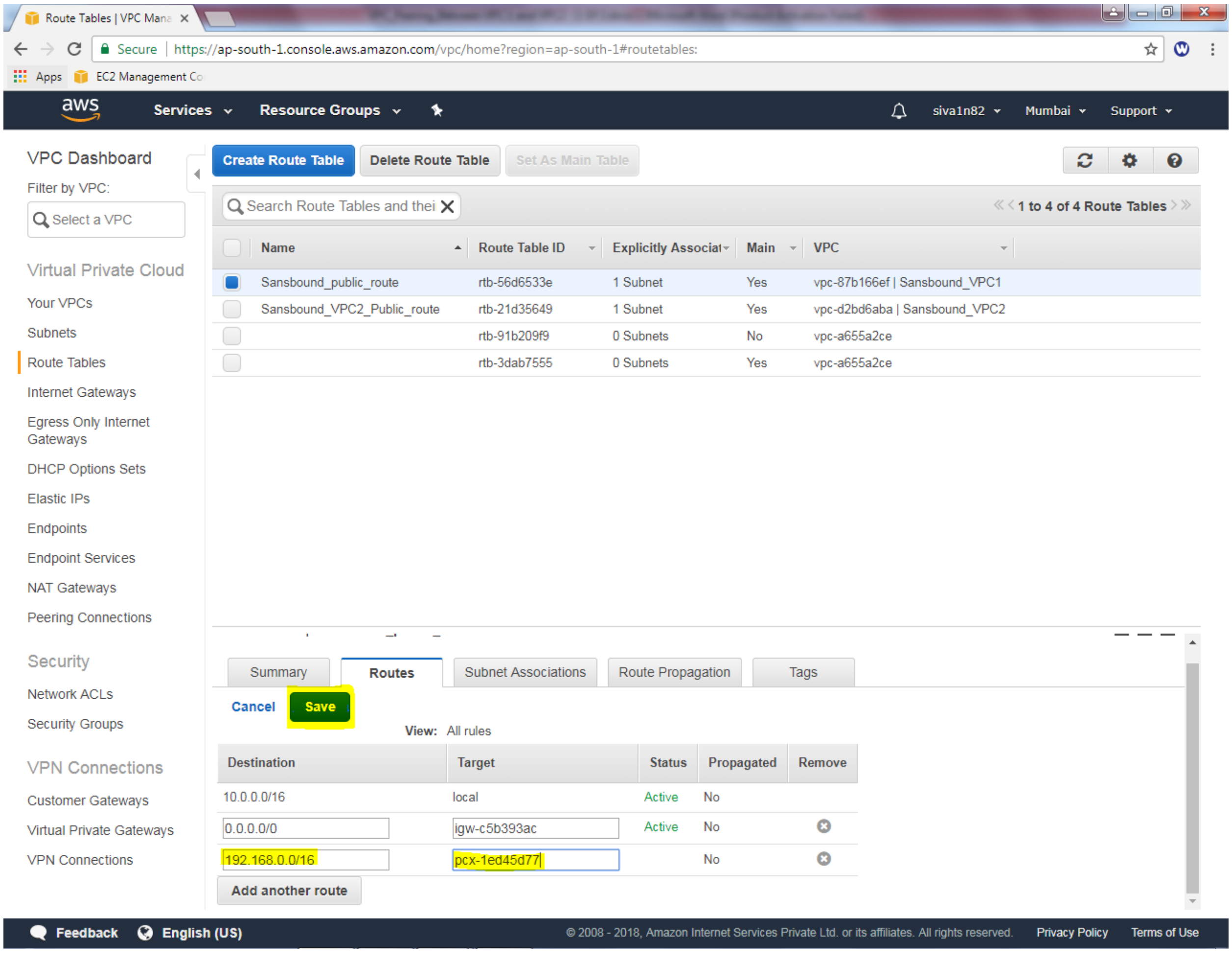
	Name	Route Table ID	Explicitly Associat	Main	VPC
☑	Sansbound_public_route	rtb-56d6533e	1 Subnet	Yes	vpc-87b166ef | Sansbound_VPC1
□	Sansbound_VPC2_Public_route	rtb-21d35649	1 Subnet	Yes	vpc-d2bd6aba | Sansbound_VPC2
□		rtb-91b209f9	0 Subnets	No	vpc-a655a2ce
□		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce

rtb-56d6533e | Sansbound_public_route

View: All rules

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-c5b393ac	Active	No	⊗

In VPC1, public routing table add 192.168.0.0/16 (VPC2) subnet and select **“pcx-*”**

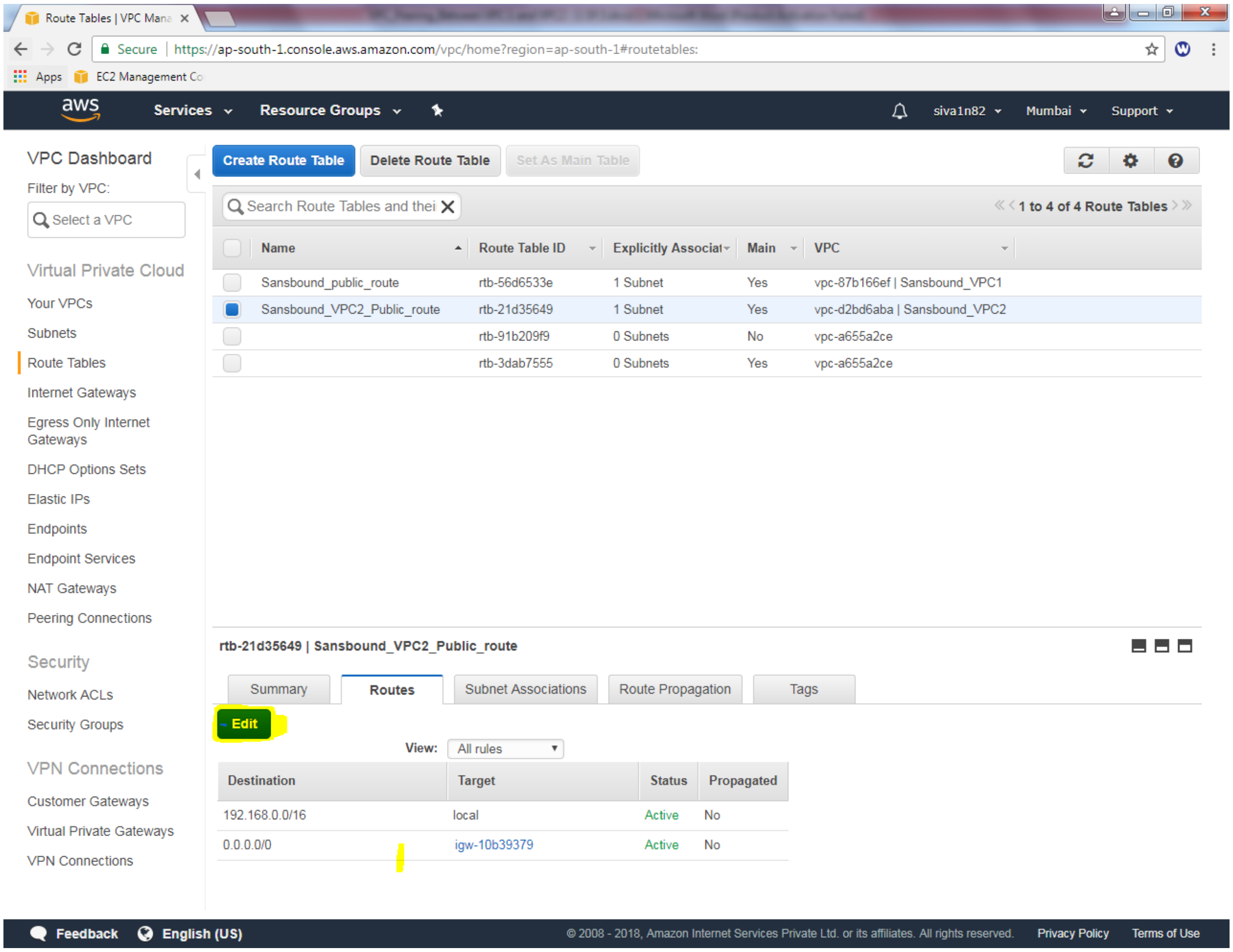


	Name	Route Table ID	Explicitly Associat	Main	VPC
☑	Sansbound_public_route	rtb-56d6533e	1 Subnet	Yes	vpc-87b166ef | Sansbound_VPC1
□	Sansbound_VPC2_Public_route	rtb-21d35649	1 Subnet	Yes	vpc-d2bd6aba | Sansbound_VPC2
□		rtb-91b209f9	0 Subnets	No	vpc-a655a2ce
□		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-c5b393ac	Active	No	⊗
192.168.0.0/16	pcx-1ed45d77		No	⊗

Click “Save”.

Click sansbound_VPC2_public_route table, select “Route “tab and then click “Edit”



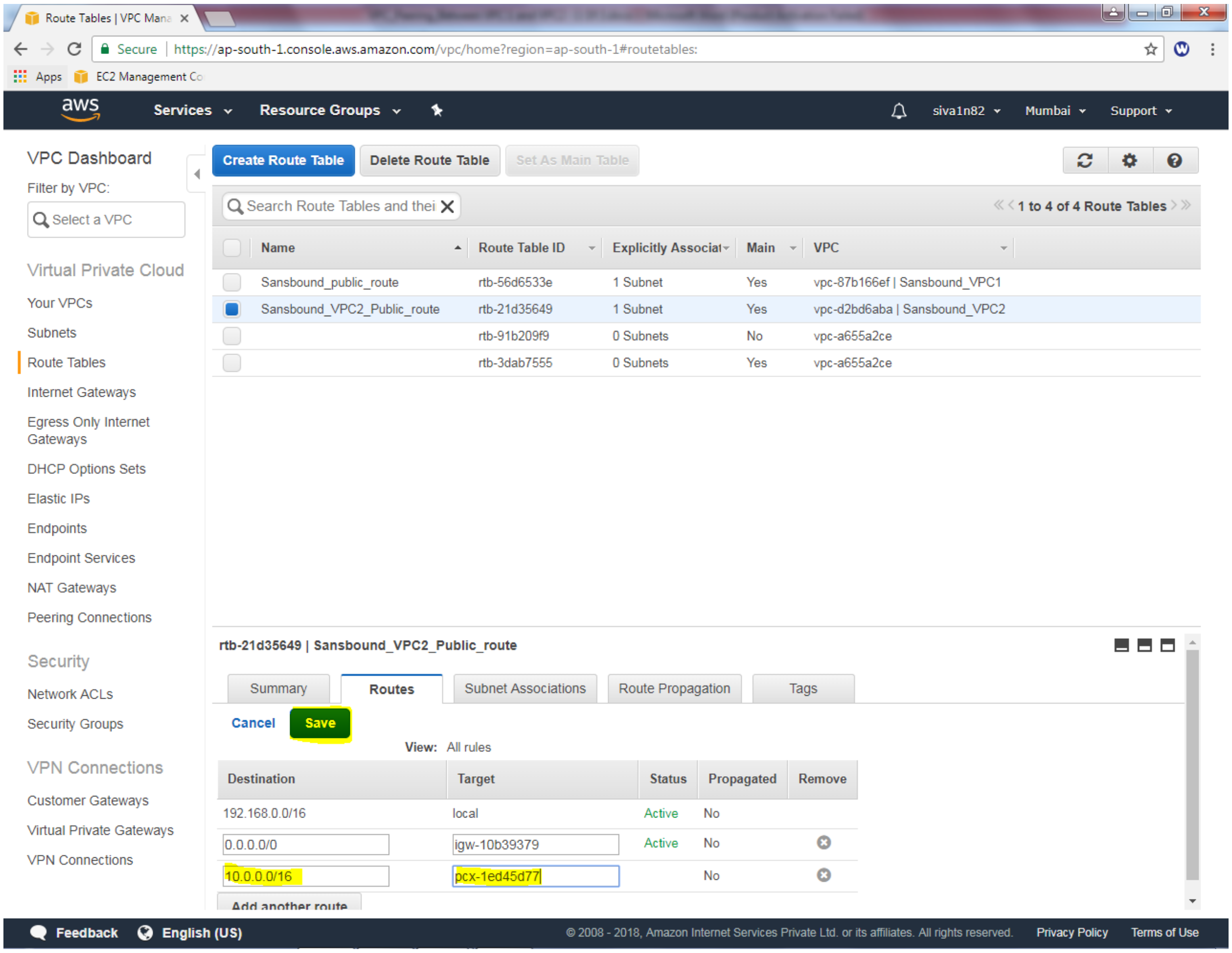
Name	Route Table ID	Explicitly Associat	Main	VPC
Sansbound_public_route	rtb-56d6533e	1 Subnet	Yes	vpc-87b166ef | Sansbound_VPC1
Sansbound_VPC2_Public_route	rtb-21d35649	1 Subnet	Yes	vpc-d2bd6aba | Sansbound_VPC2
	rtb-91b209f9	0 Subnets	No	vpc-a655a2ce
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce

rtb-21d35649 | Sansbound_VPC2_Public_route

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-10b39379	Active	No

Click “add another route”

Then add 10.0.0.0/16 (VPC1) subnet and select “pcx-*”.



Name	Route Table ID	Explicitly Associat	Main	VPC
Sansbound_public_route	rtb-56d6533e	1 Subnet	Yes	vpc-87b166ef | Sansbound_VPC1
Sansbound_VPC2_Public_route	rtb-21d35649	1 Subnet	Yes	vpc-d2bd6aba | Sansbound_VPC2
	rtb-91b209f9	0 Subnets	No	vpc-a655a2ce
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce

rtb-21d35649 | Sansbound_VPC2_Public_route

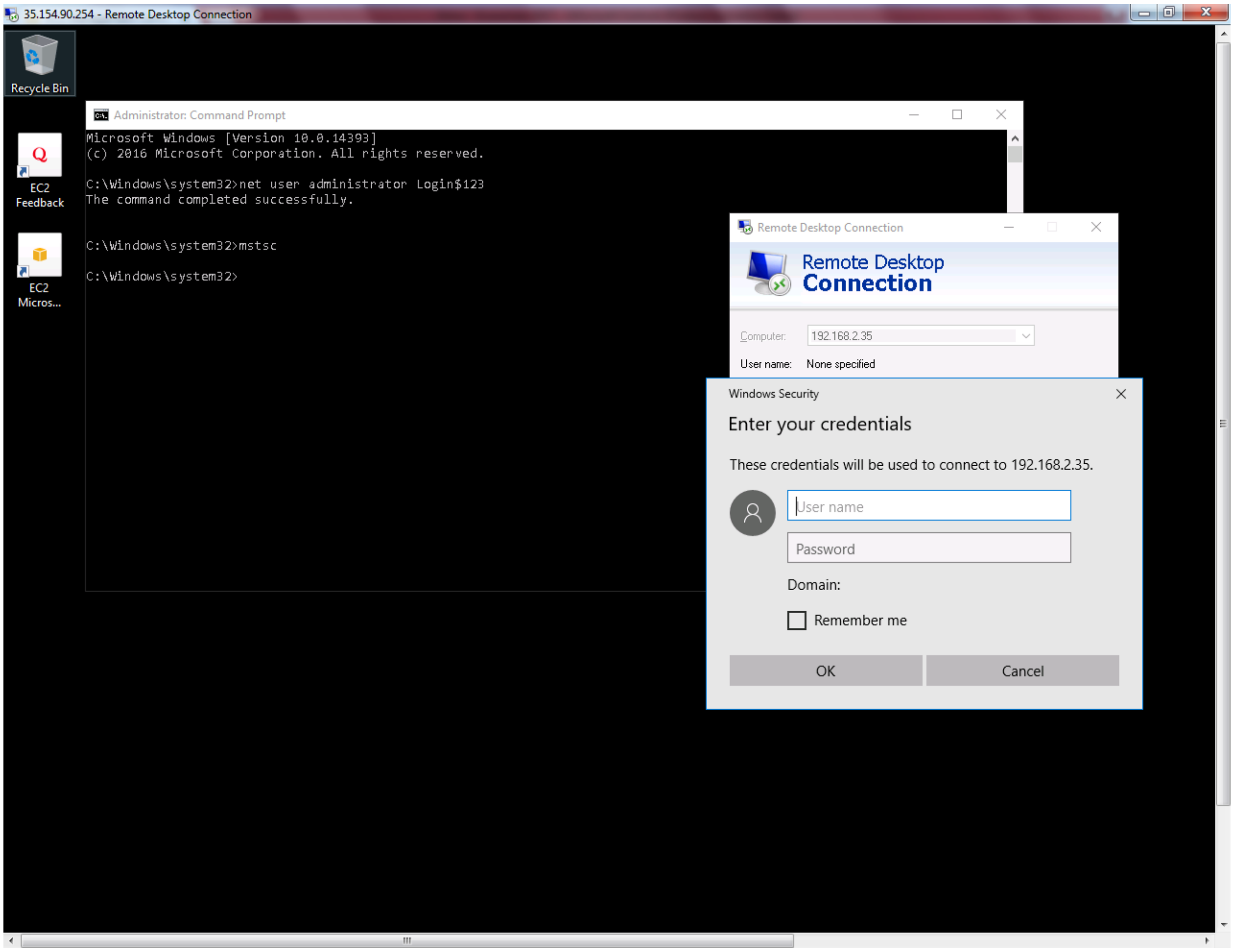
View: All rules

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-10b39379	Active	No	⊗
10.0.0.0/16	pcx-1ed45d77		No	⊗

Add another route

Then click “save”.

Now try to connect VPC2 private subnet from VPC1 private subnet. You will get RDP for VPC2 private subnet.


35.154.90.254 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
Administrator: Command Prompt
Remote Desktop Connection
Remote Desktop Connection
Windows Security
OK
Cancel

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

C:\Windows\system32>net user administrator Login$123
The command completed successfully.


C:\Windows\system32>mstsc

C:\Windows\system32>
```

Computer: 192.168.2.35

User name: None specified

Enter your credentials

These credentials will be used to connect to 192.168.2.35.

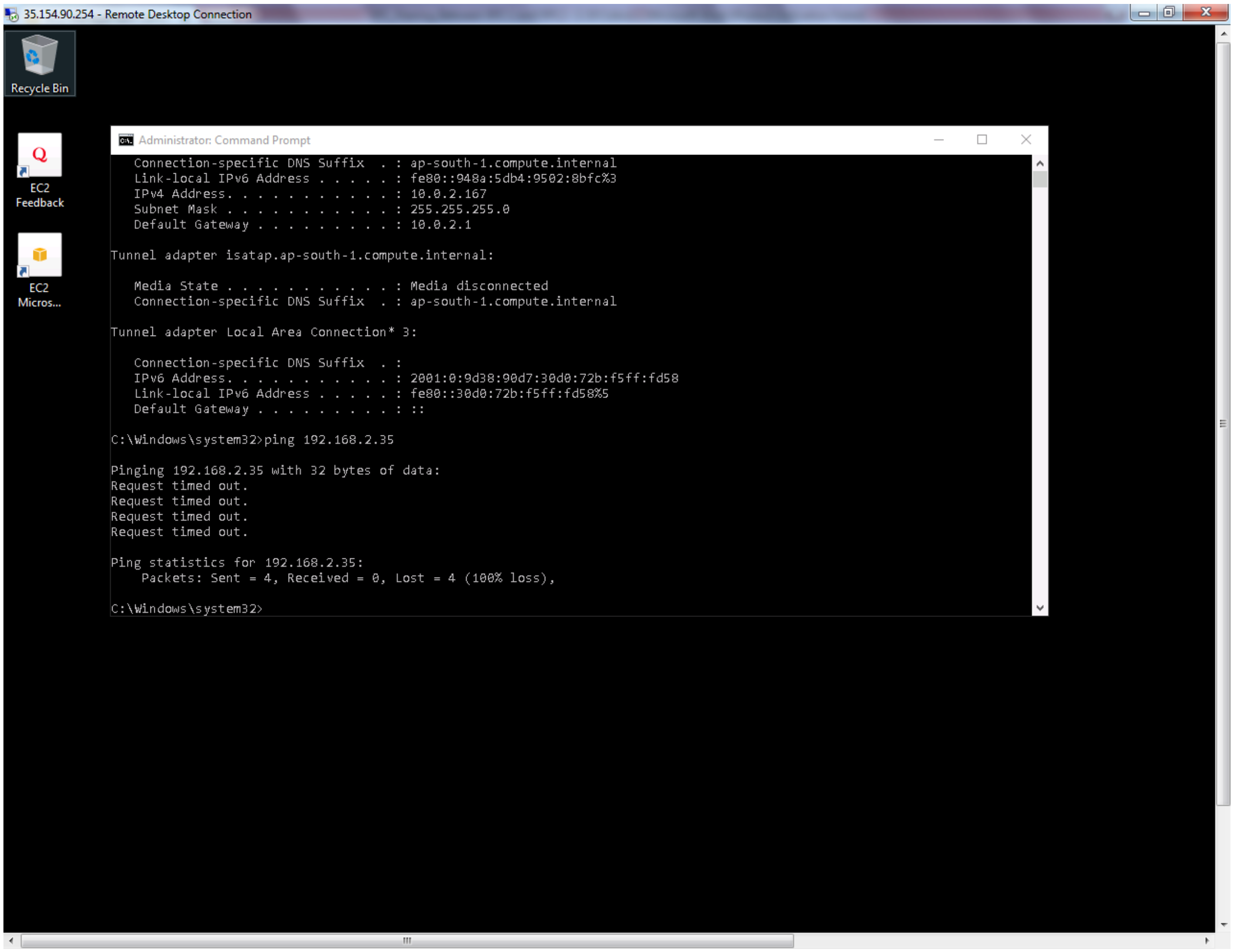
User name

Password

Domain:

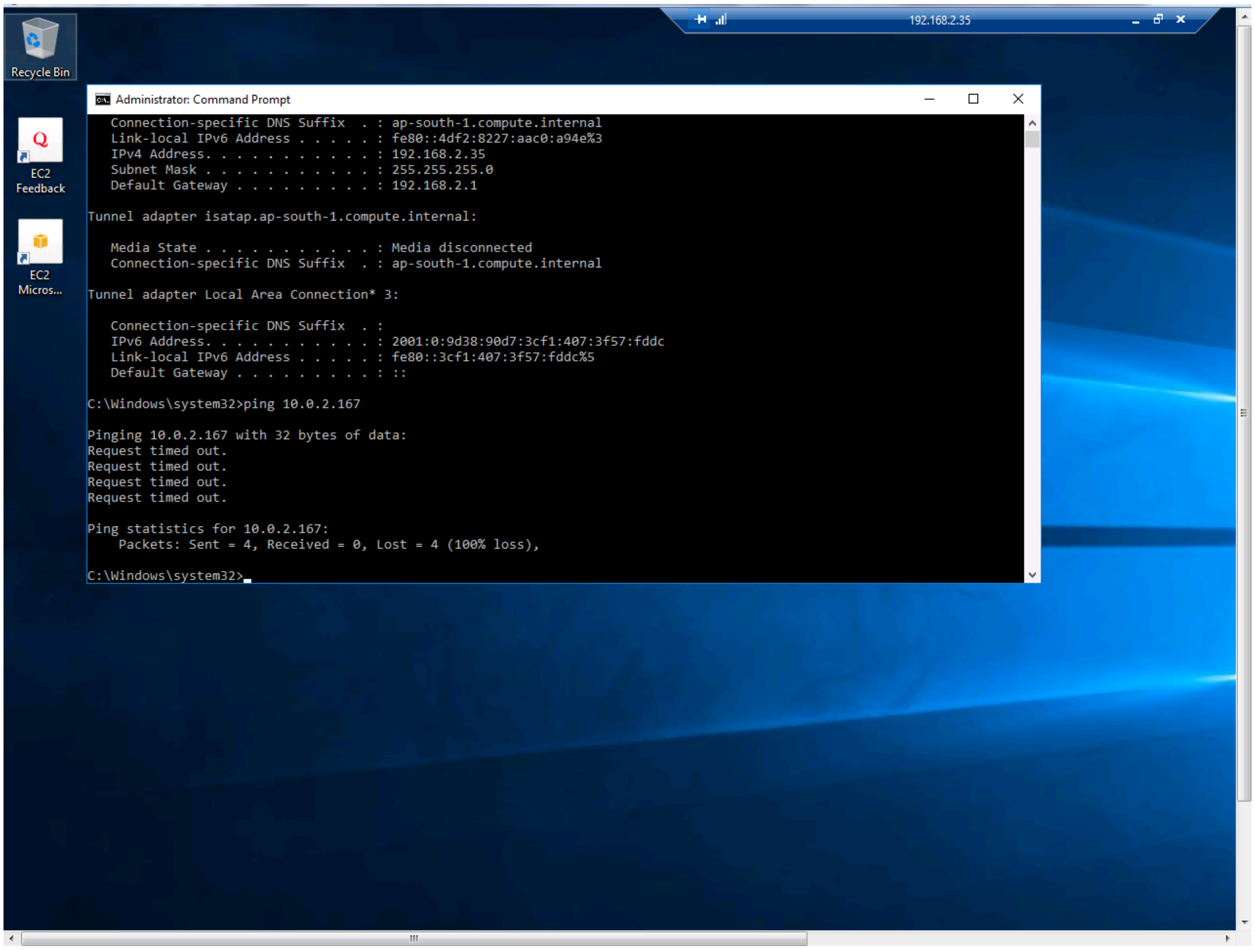
□ Remember me

Now try to ping 192.168.2.23 (VPC2 host IP) from VPC1 Host. You will get request timed out, because ICMP was not permitted on VPC2 Security Group. RDP Port only permitted by default.


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

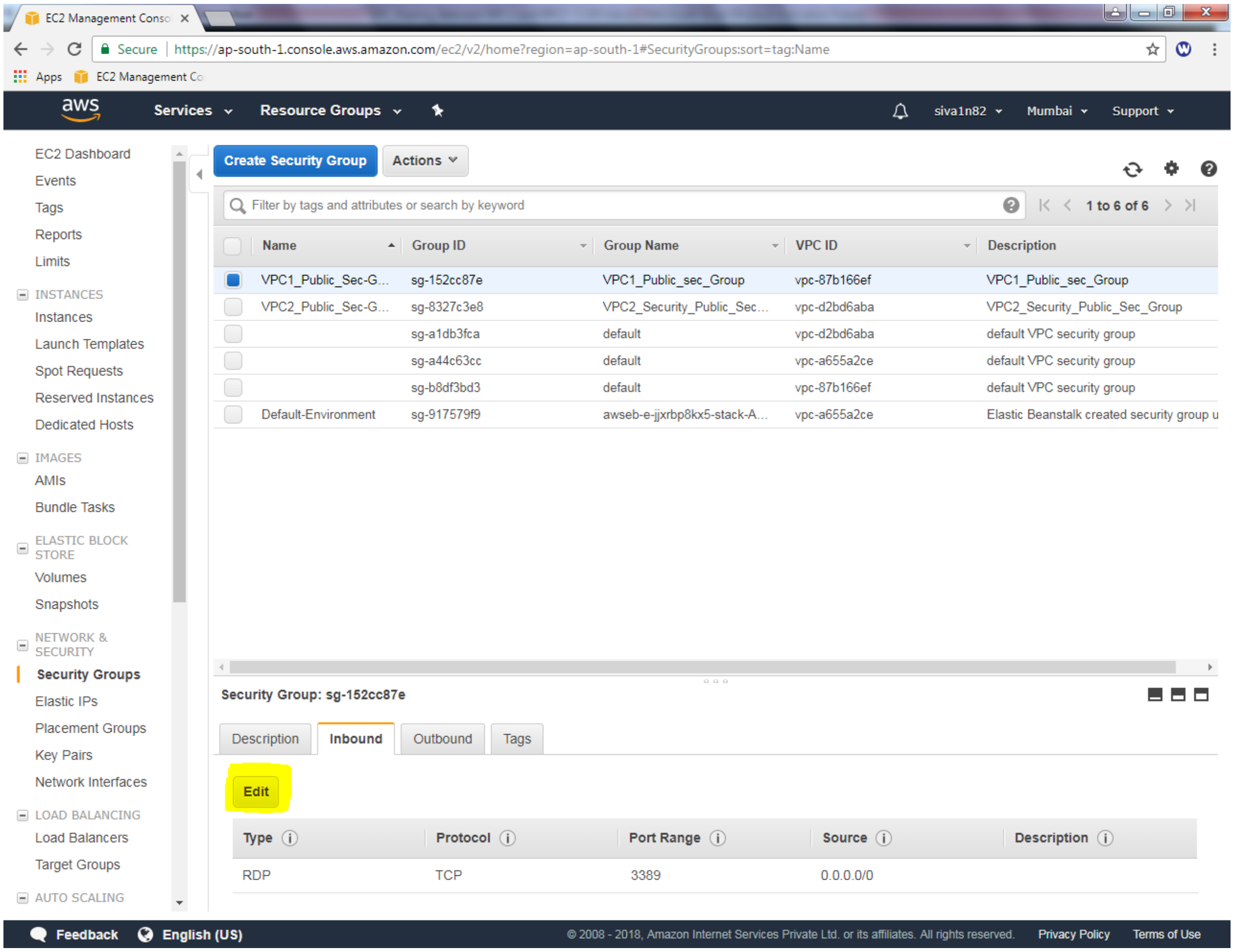
```
   Connection-specific DNS Suffix  . : ap-south-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::948a:5db4:9502:8bfc%3
   IPv4 Address. . . . . . . . . . . : 10.0.2.167
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

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. . . . . . . . . . . : 2001:0:9d38:90d7:30d0:72b:f5ff:fd58
   Link-local IPv6 Address . . . . . : fe80::30d0:72b:f5ff:fd58%5
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>ping 192.168.2.35

Pinging 192.168.2.35 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>
```

Now try to ping 10.0.2.167 (VPC1 host IP) from VPC2 Host. You will get request timed out, because ICMP was not permitted on VPC1 Security Group. RDP Port only permitted by default.



```
   Connection-specific DNS Suffix  . : ap-south-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::4df2:8227:aac0:a94e%3
   IPv4 Address. . . . . . . . . . . : 192.168.2.35
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

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. . . . . . . . . . . : 2001:0:9d38:90d7:3cf1:407:3f57:fddc
   Link-local IPv6 Address . . . . . : fe80::3cf1:407:3f57:fddc%5
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>ping 10.0.2.167

Pinging 10.0.2.167 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.167:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>
```

Go to “VPC1_public_sec-group” in Inbound Tab, click “Edit”.



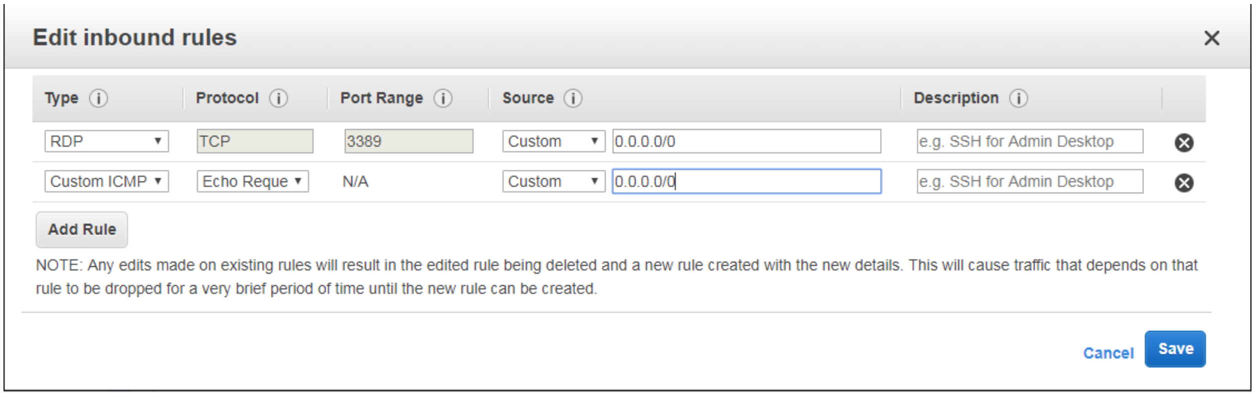
	Name	Group ID	Group Name	VPC ID	Description
■	VPC1_Public_Sec-G...	sg-152cc87e	VPC1_Public_sec_Group	vpc-87b166ef	VPC1_Public_sec_Group
□	VPC2_Public_Sec-G...	sg-8327c3e8	VPC2_Security_Public_Sec...	vpc-d2bd6aba	VPC2_Security_Public_Sec_Group
□		sg-a1db3fca	default	vpc-d2bd6aba	default VPC security group
□		sg-a44c63cc	default	vpc-a655a2ce	default VPC security group
□		sg-b8df3bd3	default	vpc-87b166ef	default VPC security group
□	Default-Environment	sg-917579f9	awseb-e-jjxrbp8kx5-stack-A...	vpc-a655a2ce	Elastic Beanstalk created security group u

Security Group: sg-152cc87e

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

Click “Add rule”

Select “Custom ICMP” and select protocol as “Echo Request” then type source as 0.0.0.0/0



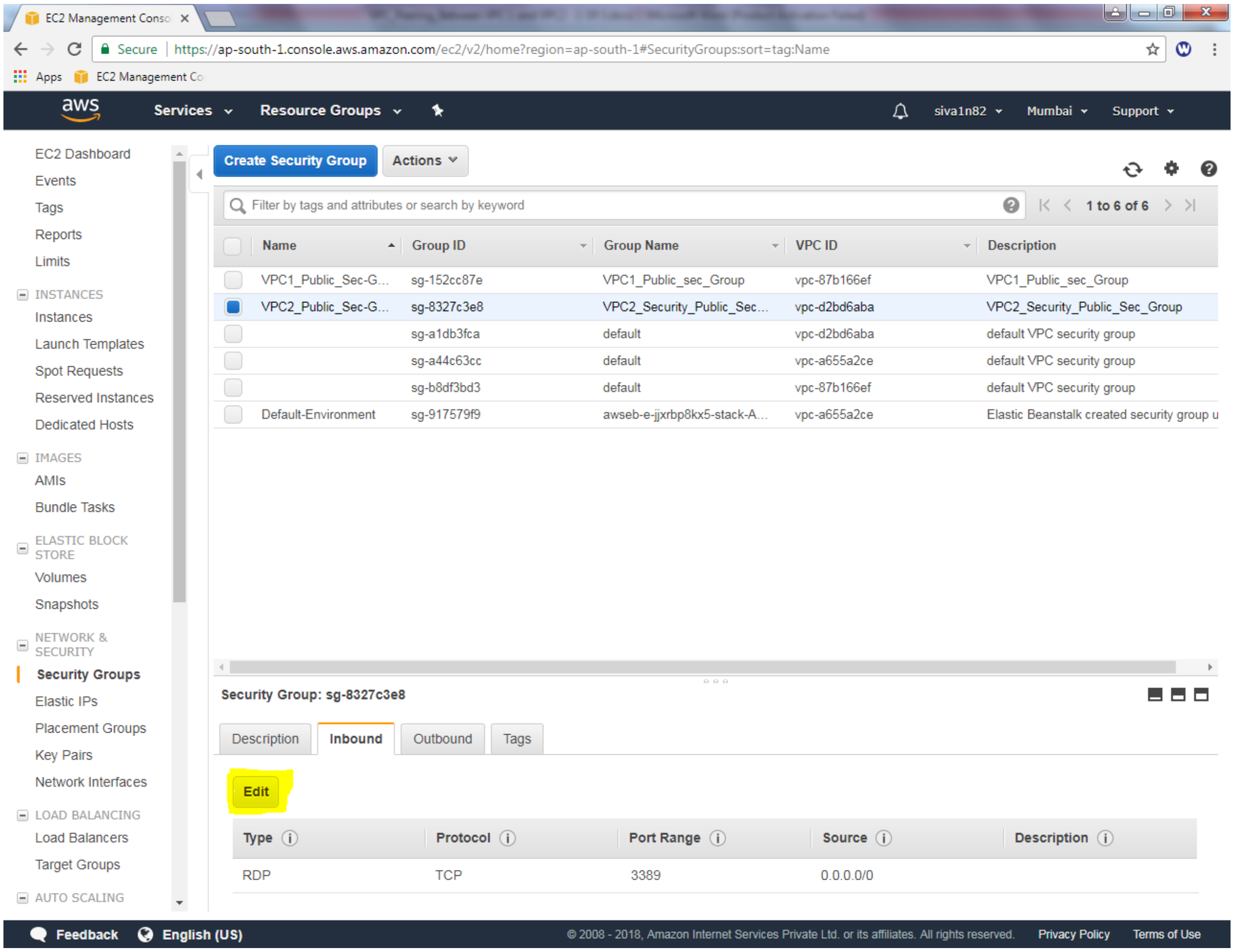
Edit inbound rules

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

Then click “save”.

Go to “VPC2_public_sec-group” in Inbound Tab, click “Edit”.



	Name	Group ID	Group Name	VPC ID	Description
□	VPC1_Public_Sec-G...	sg-152cc87e	VPC1_Public_sec_Group	vpc-87b166ef	VPC1_Public_sec_Group
■	VPC2_Public_Sec-G...	sg-8327c3e8	VPC2_Security_Public_Sec...	vpc-d2bd6aba	VPC2_Security_Public_Sec_Group
□		sg-a1db3fca	default	vpc-d2bd6aba	default VPC security group
□		sg-a44c63cc	default	vpc-a655a2ce	default VPC security group
□		sg-b8df3bd3	default	vpc-87b166ef	default VPC security group
□	Default-Environment	sg-917579f9	awseb-e-jjxrbp8kx5-stack-A...	vpc-a655a2ce	Elastic Beanstalk created security group u

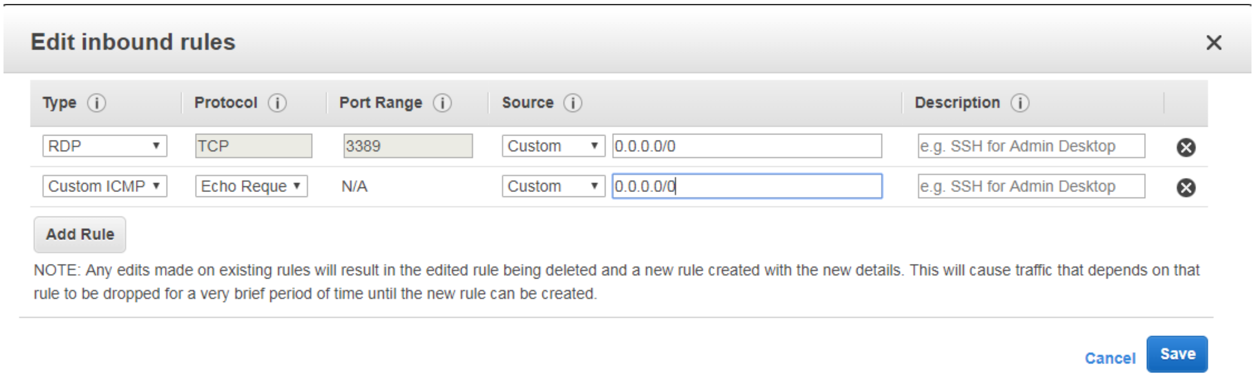
Security Group: sg-8327c3e8

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

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

Click “Add rule”

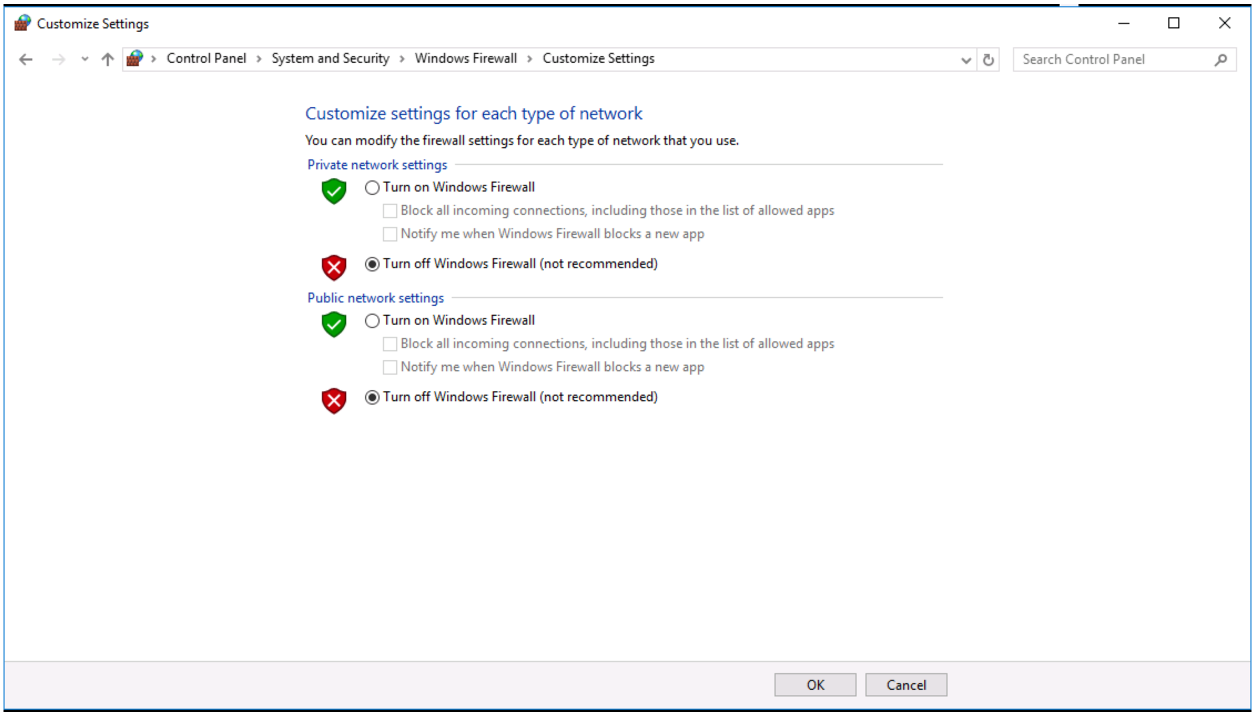
Select “Custom ICMP” and select protocol as “Echo Request” then type source as 0.0.0.0/0


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	Echo Reque	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.

Then we need to turn off windows firewall on both servers on VPC1 and VPC2.


Customize Settings
Control Panel › System and Security › Windows Firewall › Customize Settings
Search Control Panel

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

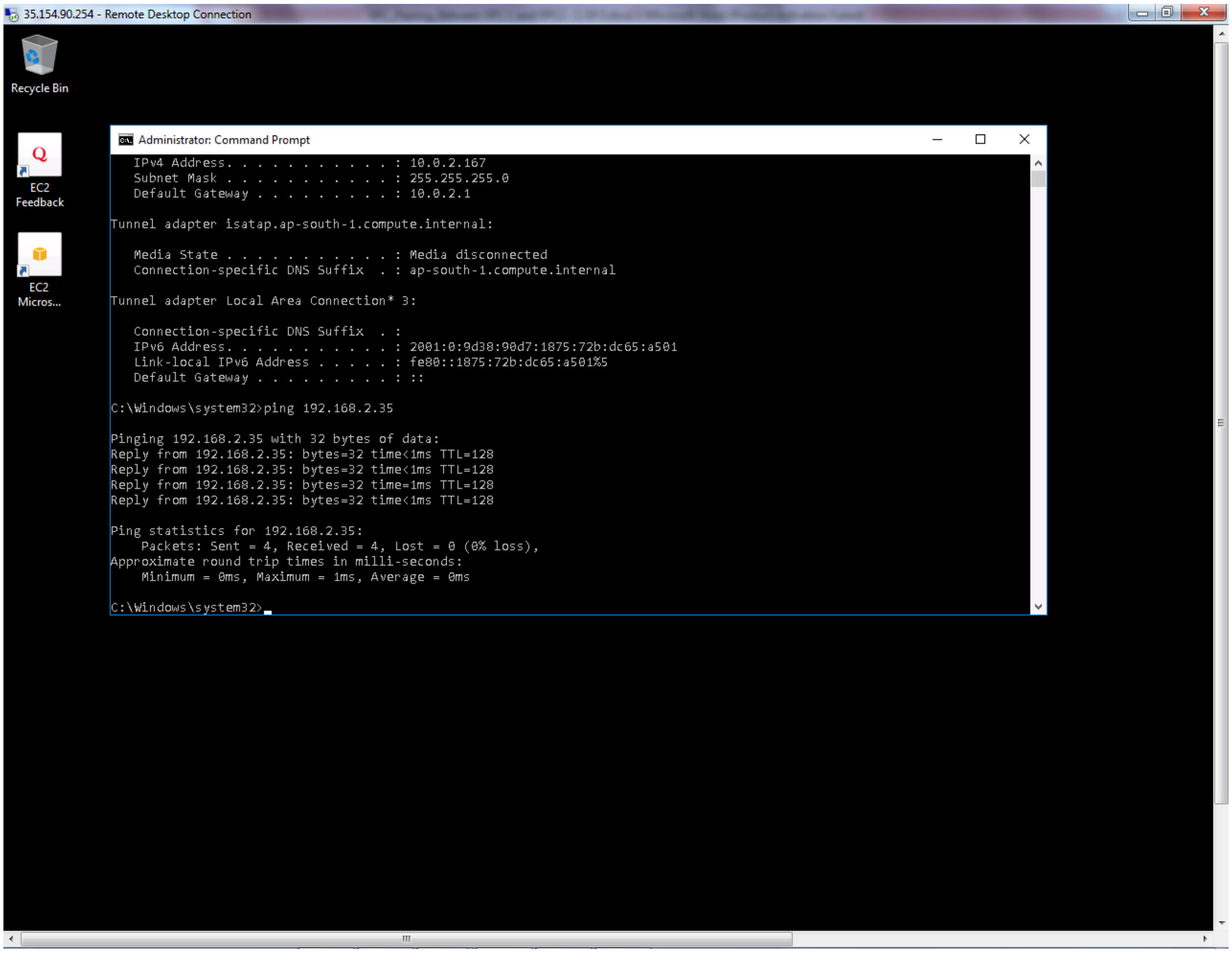
○ Turn on Windows Firewall

□ 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)

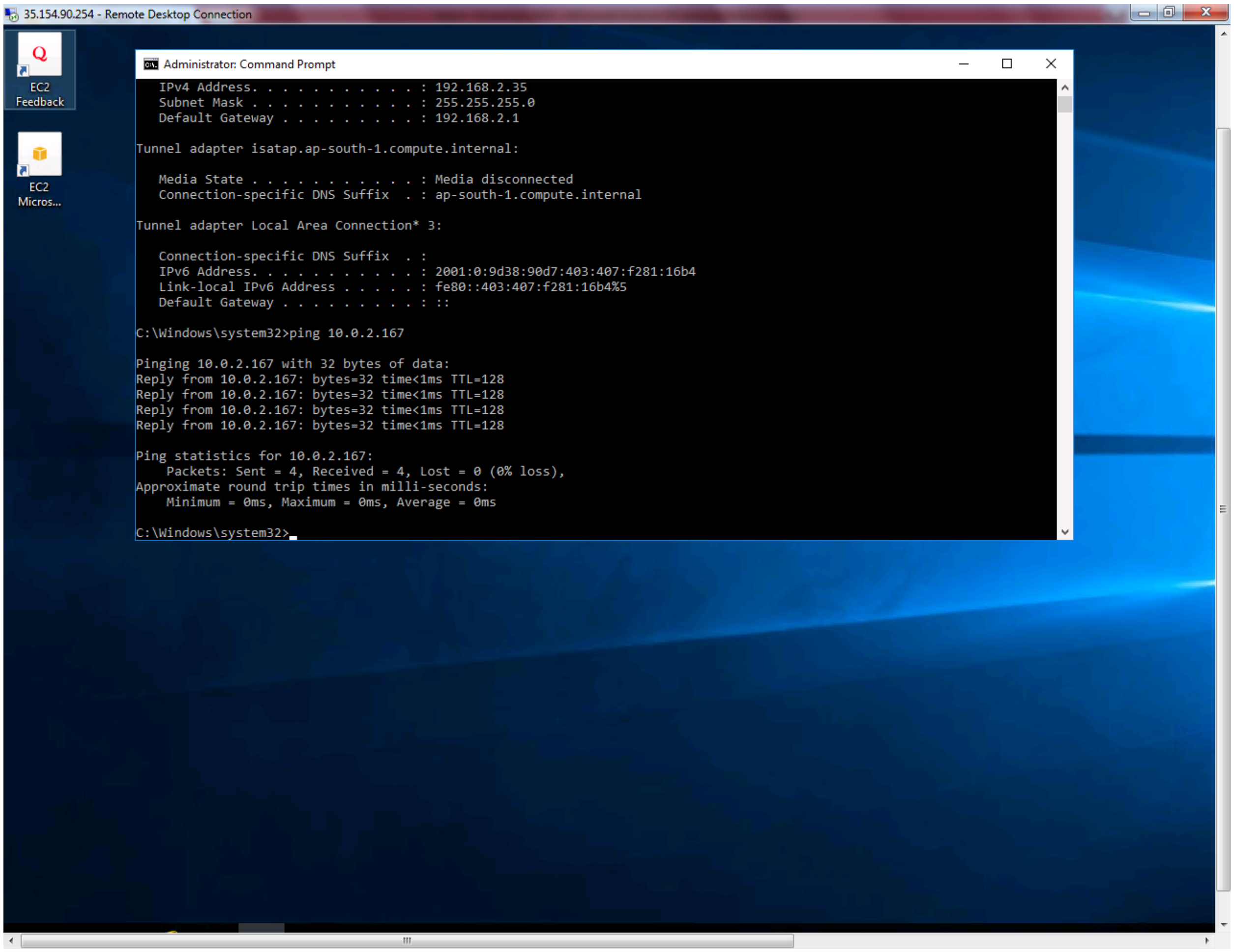
Then try to ping 192.168.2.35 host from 10.0.2.167 with successful reply.



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

```
   IPv4 Address. . . . . . . . . . . : 10.0.2.167
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

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. . . . . . . . . . . : 2001:0:9d38:90d7:1875:72b:dc65:a501
   Link-local IPv6 Address . . . . . : fe80::1875:72b:dc65:a501%5
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>ping 192.168.2.35

Pinging 192.168.2.35 with 32 bytes of data:
Reply from 192.168.2.35: bytes=32 time<1ms TTL=128
Reply from 192.168.2.35: bytes=32 time<1ms TTL=128
Reply from 192.168.2.35: bytes=32 time=1ms TTL=128
Reply from 192.168.2.35: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.35:
    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>
```

Try to ping 10.0.2.167 from 192.168.2.35 host with successful reply.



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

```
   IPv4 Address. . . . . . . . . . . : 192.168.2.35
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

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. . . . . . . . . . . : 2001:0:9d38:90d7:403:407:f281:16b4
   Link-local IPv6 Address . . . . . : fe80::403:407:f281:16b4%5
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>ping 10.0.2.167

Pinging 10.0.2.167 with 32 bytes of data:
Reply from 10.0.2.167: bytes=32 time<1ms TTL=128
Reply from 10.0.2.167: bytes=32 time<1ms TTL=128
Reply from 10.0.2.167: bytes=32 time<1ms TTL=128
Reply from 10.0.2.167: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.167:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```