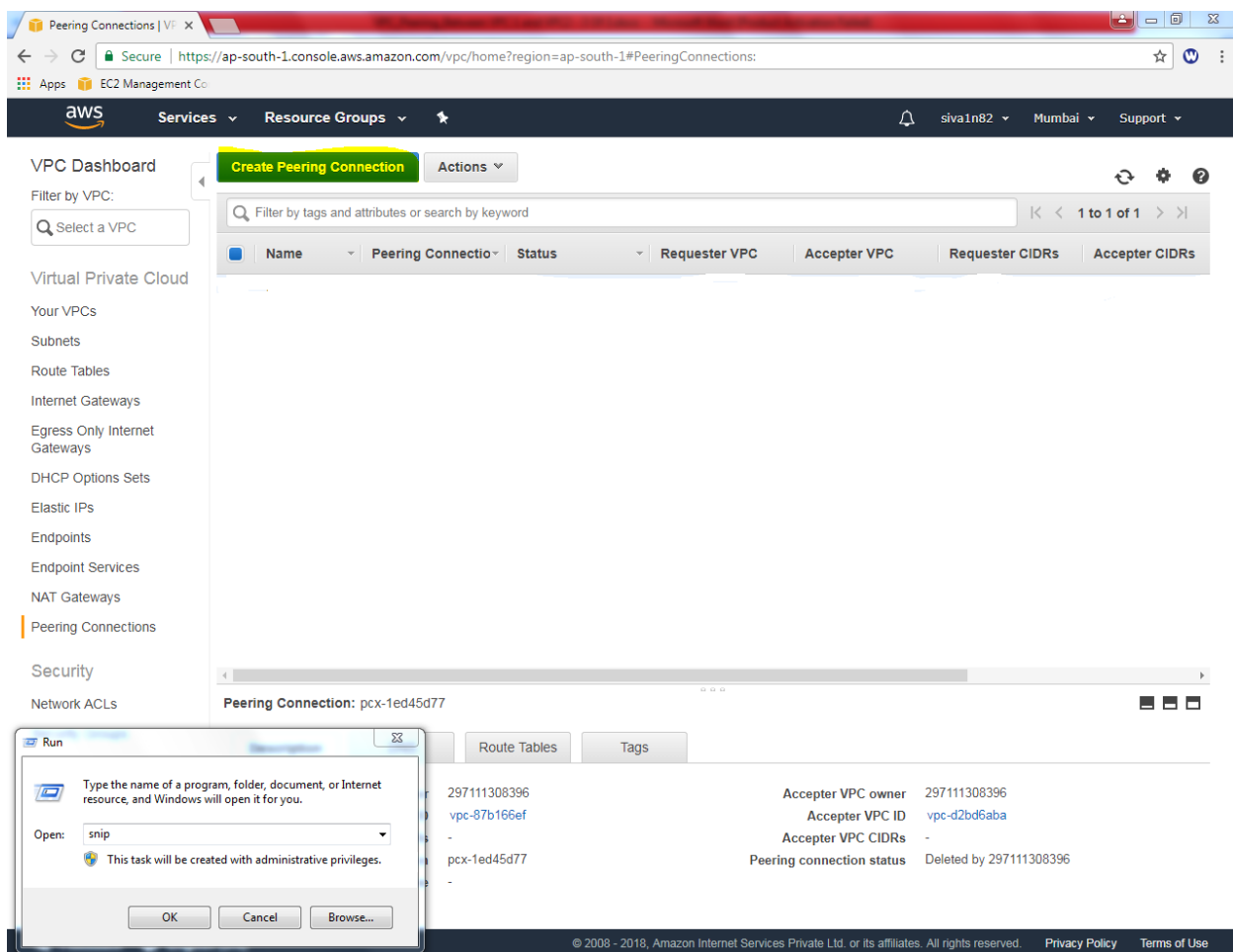


Lab 13

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

In VPC Dashboard,

Go to Peering Connections.



The screenshot shows the AWS VPC Dashboard with the 'Peering Connections' page selected. The 'Create Peering Connection' button is highlighted in green. A 'Run' dialog box is open in the foreground, showing the command 'snip' entered. The background shows the VPC Dashboard interface with a table of peering connections.

Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
pcx-1ed45d77						

Peering Connection: pcx-1ed45d77

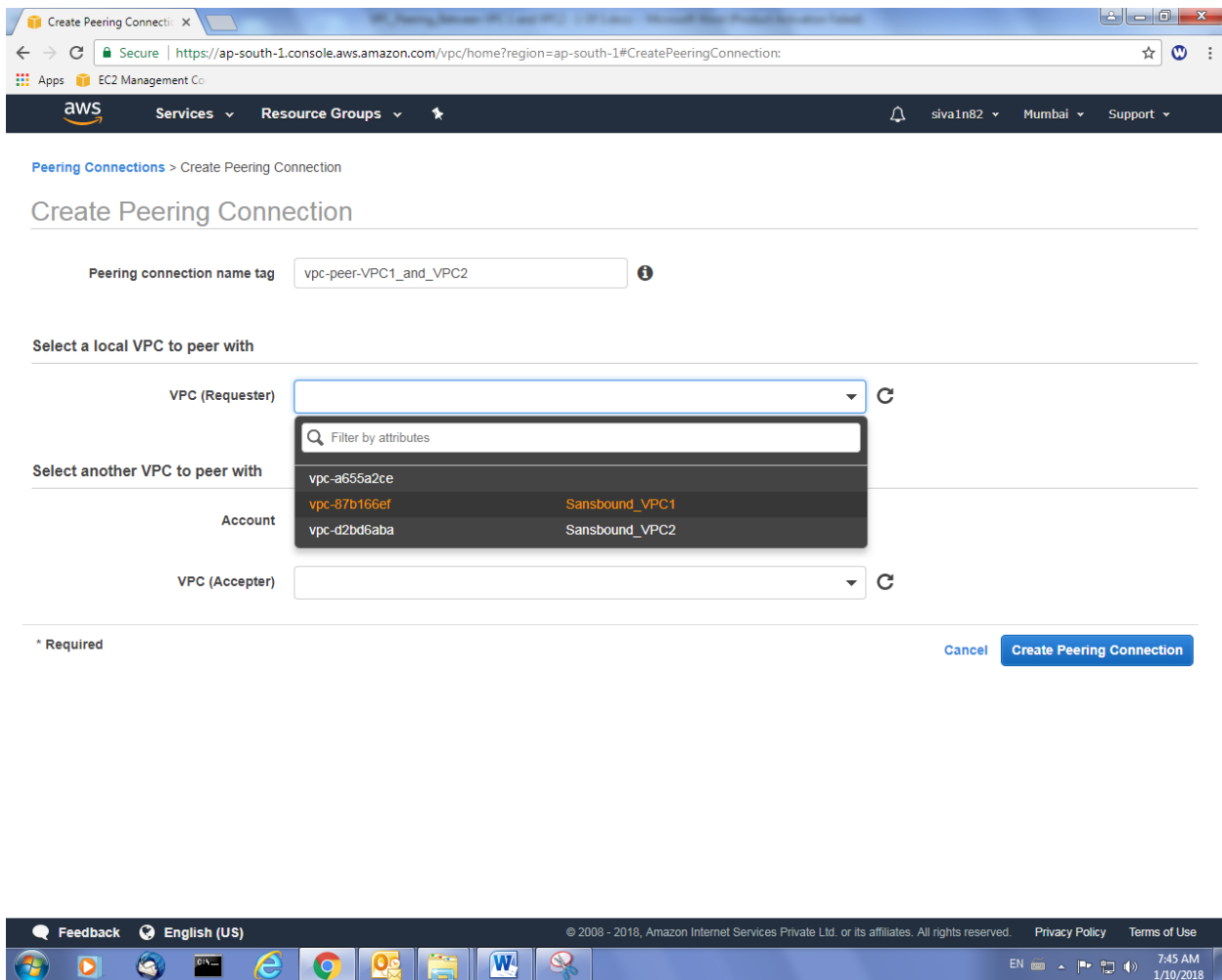
297111308396
vpc-87b166ef
pcx-1ed45d77

Accepter VPC owner: 297111308396
Accepter VPC ID: vpc-d2bd6aba
Accepter VPC CIDRs: -
Peering connection status: Deleted by 297111308396

In Peering connection,

Peering Connection Name tag: vpc-peer-VPC1_and_VPC2

VPC Requestor (Select – VPC1)



Create Peering Connection

Peering connection name tag

Select a local VPC to peer with

VPC (Requester)

Select another VPC to peer with

Account

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

VPC (Acceptor)

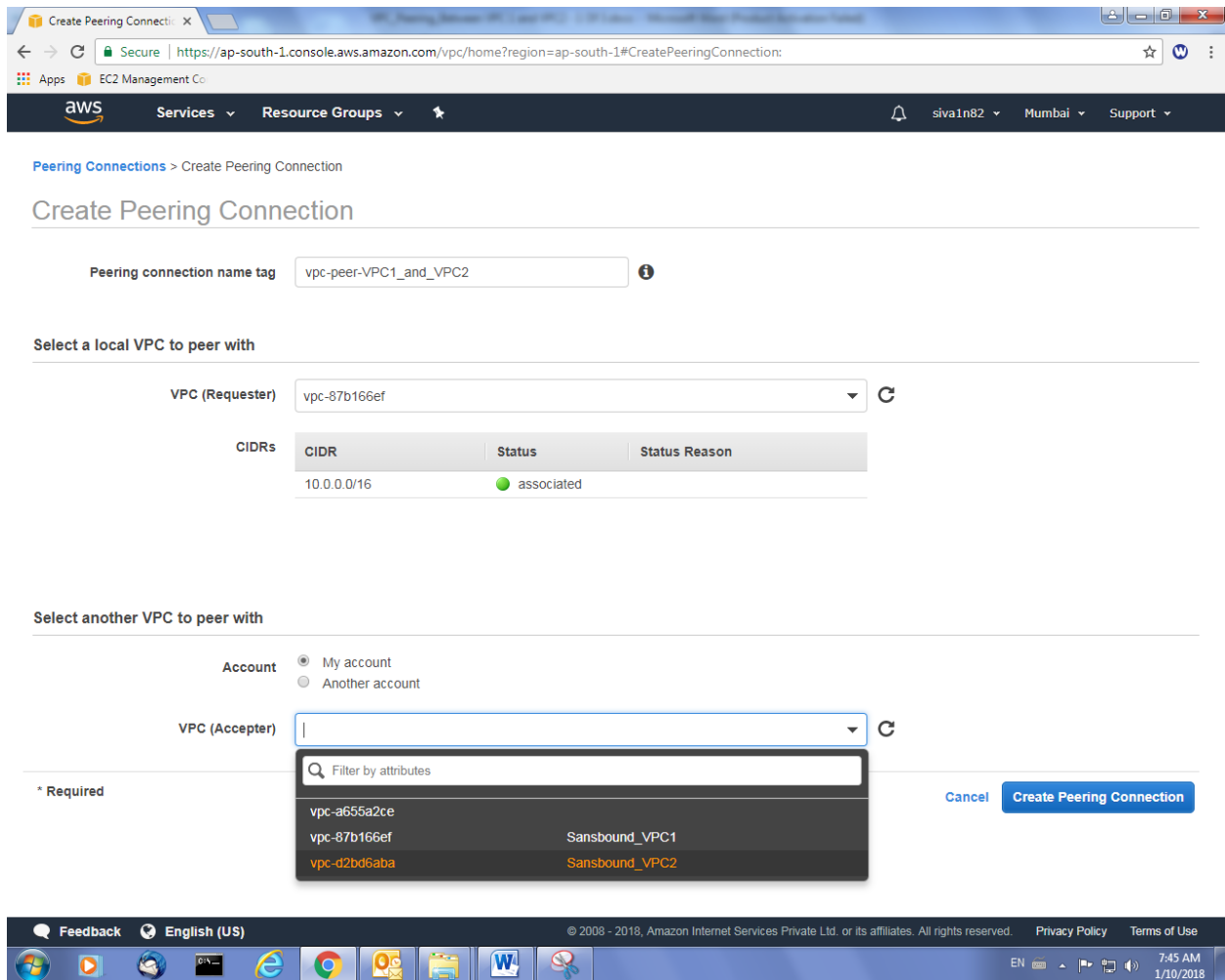
* Required

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

7:45 AM 1/10/2018

VPC Acceptor "Select VPC2"



Create Peering Connection

Peering connection name tag

Select a local VPC to peer with

VPC (Requester)

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Select another VPC to peer with

Account ☒ My account ☐ Another account

VPC (Acceptor)

* Required

Cancel Create Peering Connection

Create Peering Connection

Peering connection name tag

Select a local VPC to peer with

VPC (Requester)

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Select another VPC to peer with

Account ☒ My account ☐ Another account

VPC (Accepter)

CIDR	Status	Status Reason
192.168.0.0/16	associated	

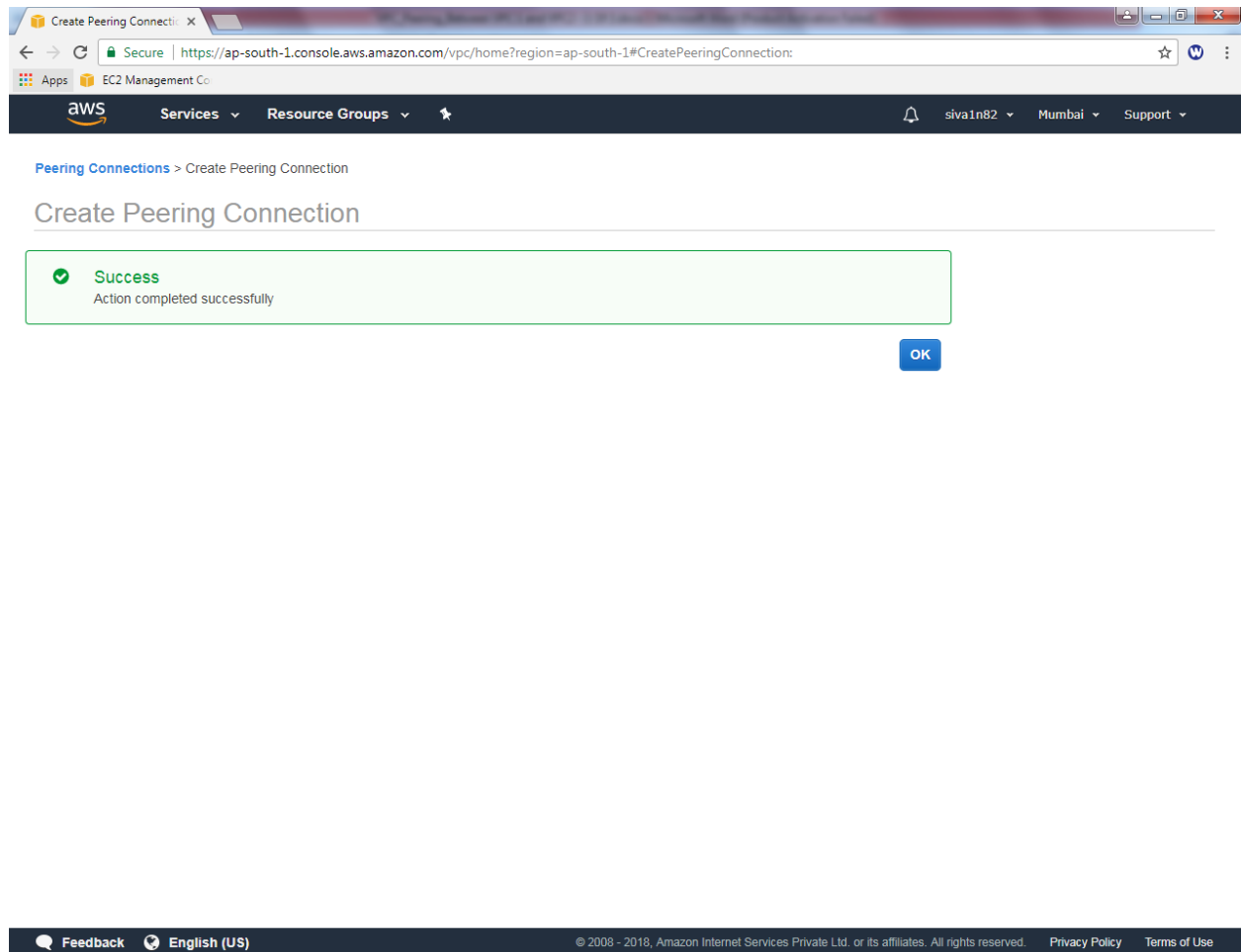
* Required

[Cancel](#) [Create Peering Connection](#)

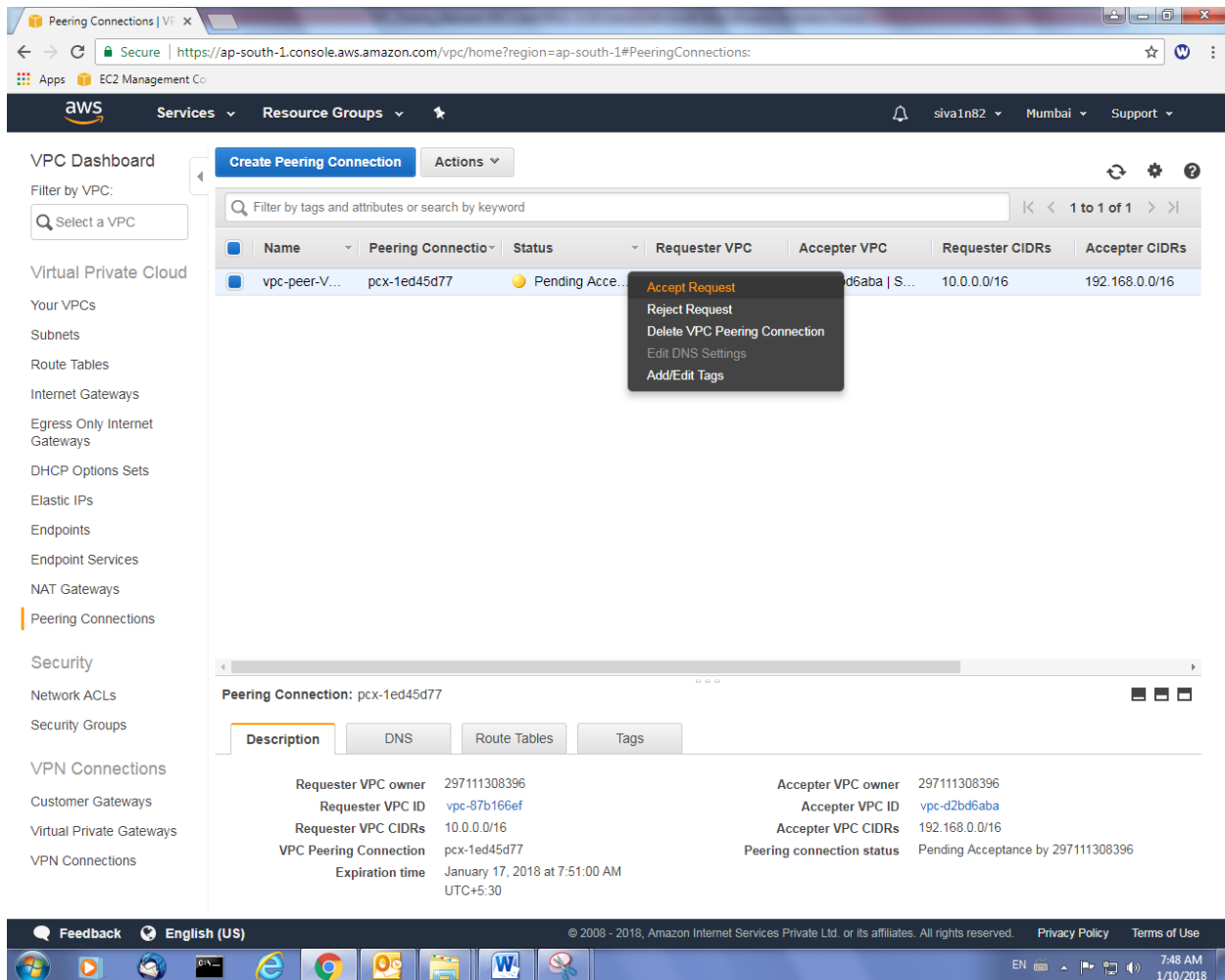
Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click “Creat peering Connection”.

VPC Peer configured successfully.



Goto Mumbai, peering connection, “Click Accept”



VPC Dashboard

Filter by 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 Peering Connection **Actions**

Filter by tags and attributes or search by keyword

Name	Peering Connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
vpc-peer-V...	pcx-1ed45d77	Pending Acceptance	vpc-87b166ef	vpc-d2bd6aba S...	10.0.0.0/16	192.168.0.0/16

Peering Connection: pcx-1ed45d77

Description **DNS** **Route Tables** **Tags**

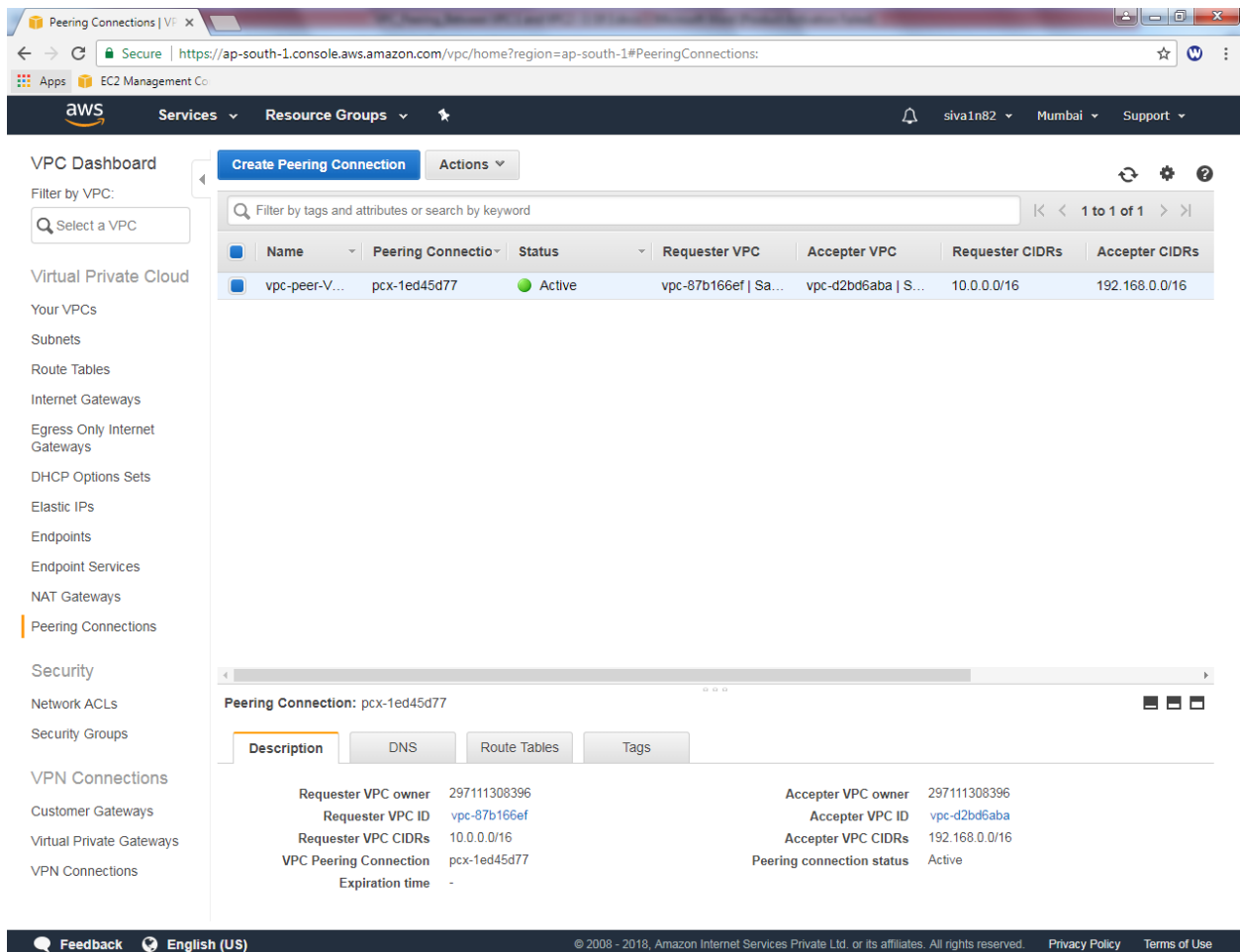
Requester VPC owner	297111308396	Accepter VPC owner	297111308396
Requester VPC ID	vpc-87b166ef	Accepter VPC ID	vpc-d2bd6aba
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	192.168.0.0/16
VPC Peering Connection	pcx-1ed45d77	Peering connection status	Pending Acceptance by 297111308396
Expiration time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

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

7:48 AM 1/10/2018

Then Click “Yes, Accept”.

Now VPC peer is active.



The screenshot shows the AWS Management Console interface for VPC Peering Connections. The left sidebar contains navigation links for VPC Dashboard, 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 (highlighted), Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays a table of Peering Connections. One connection is listed with the ID 'pcx-1ed45d77', status 'Active', and requester/accepter VPCs 'vpc-87b166ef' and 'vpc-d2bd6aba'. Below the table, the details for the selected connection 'pcx-1ed45d77' are shown, including tabs for Description, DNS, Route Tables, and Tags. The Description tab is active, showing details for the requester and acceptor VPCs and the peering connection status.

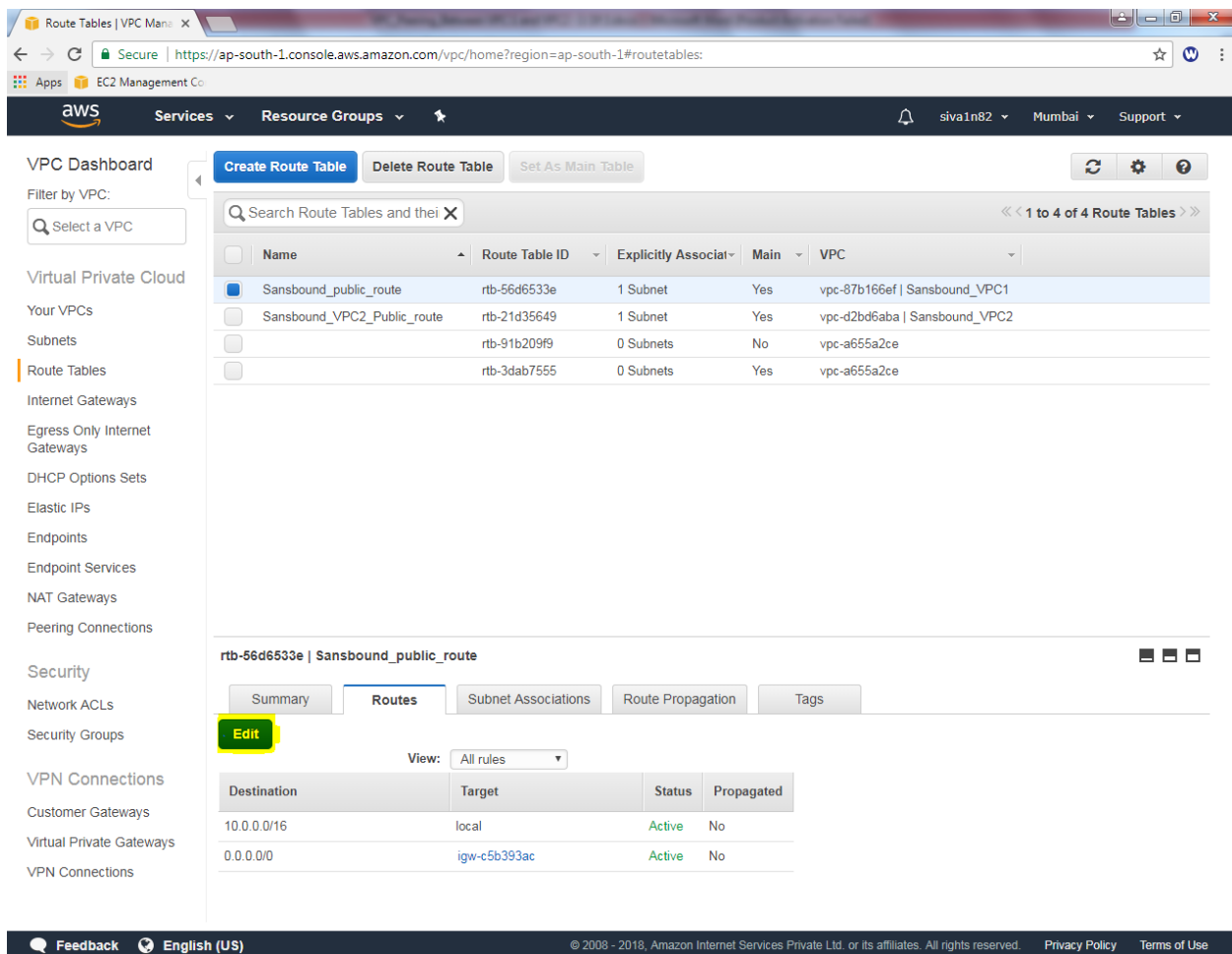
Name	Peering Connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
vpc-peer-V...	pcx-1ed45d77	Active	vpc-87b166ef Sa...	vpc-d2bd6aba S...	10.0.0.0/16	192.168.0.0/16

Peering Connection: pcx-1ed45d77

Requester VPC		Accepter VPC	
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”.

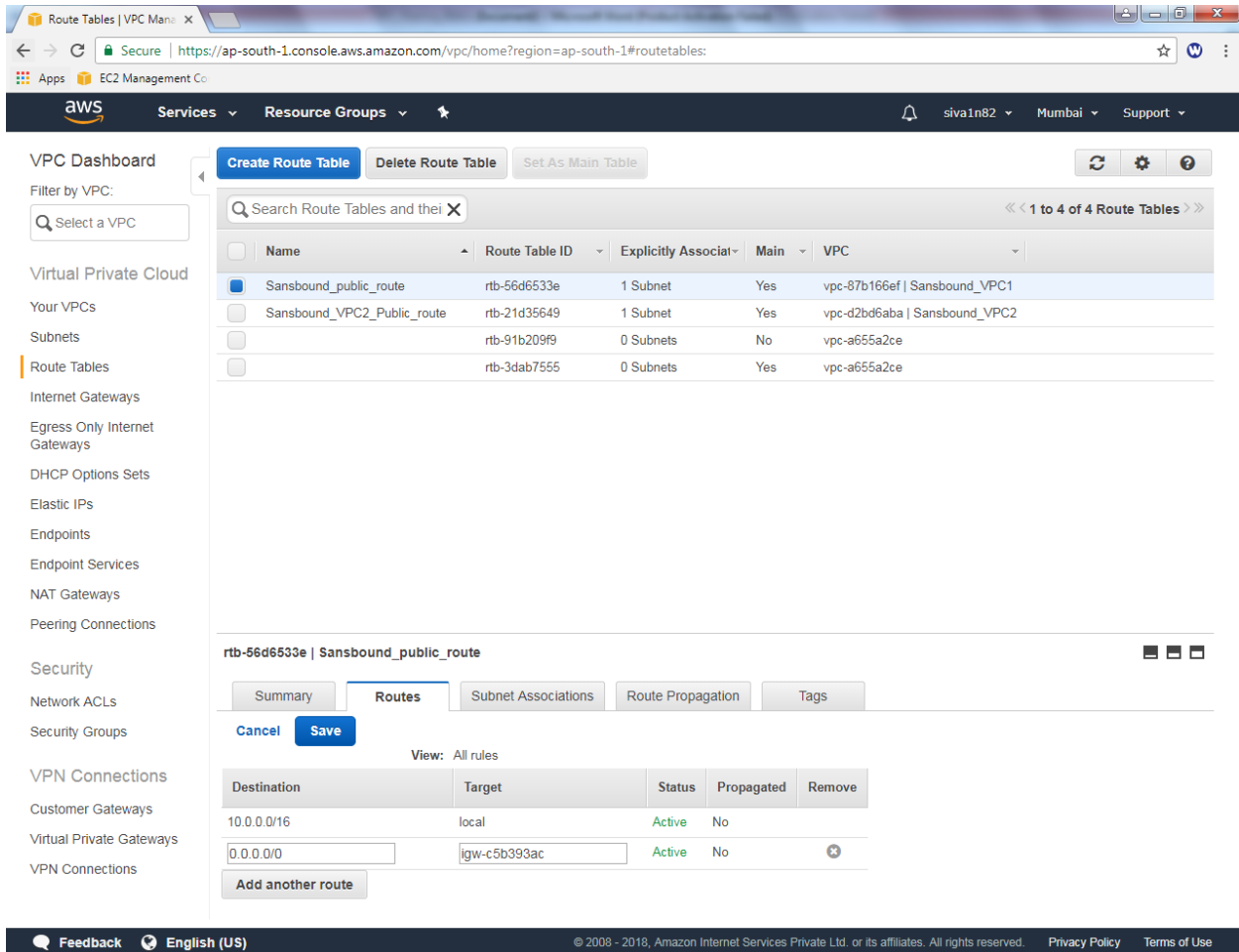


The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and navigation links for Services, Resource Groups, and a user profile. The left sidebar contains a navigation menu with categories like Virtual Private Cloud, Security, and VPN Connections. The main content area displays the VPC Dashboard for 'Sansbound_VPC1'. A table lists four route tables, with 'Sansbound_public_route' (rtb-56d6533e) selected. Below the table, the 'Routes' tab is active, showing a list of routes. The 'Edit' button is highlighted in yellow.

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
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-c5b393ac	Active	No

Click “Add another route”.



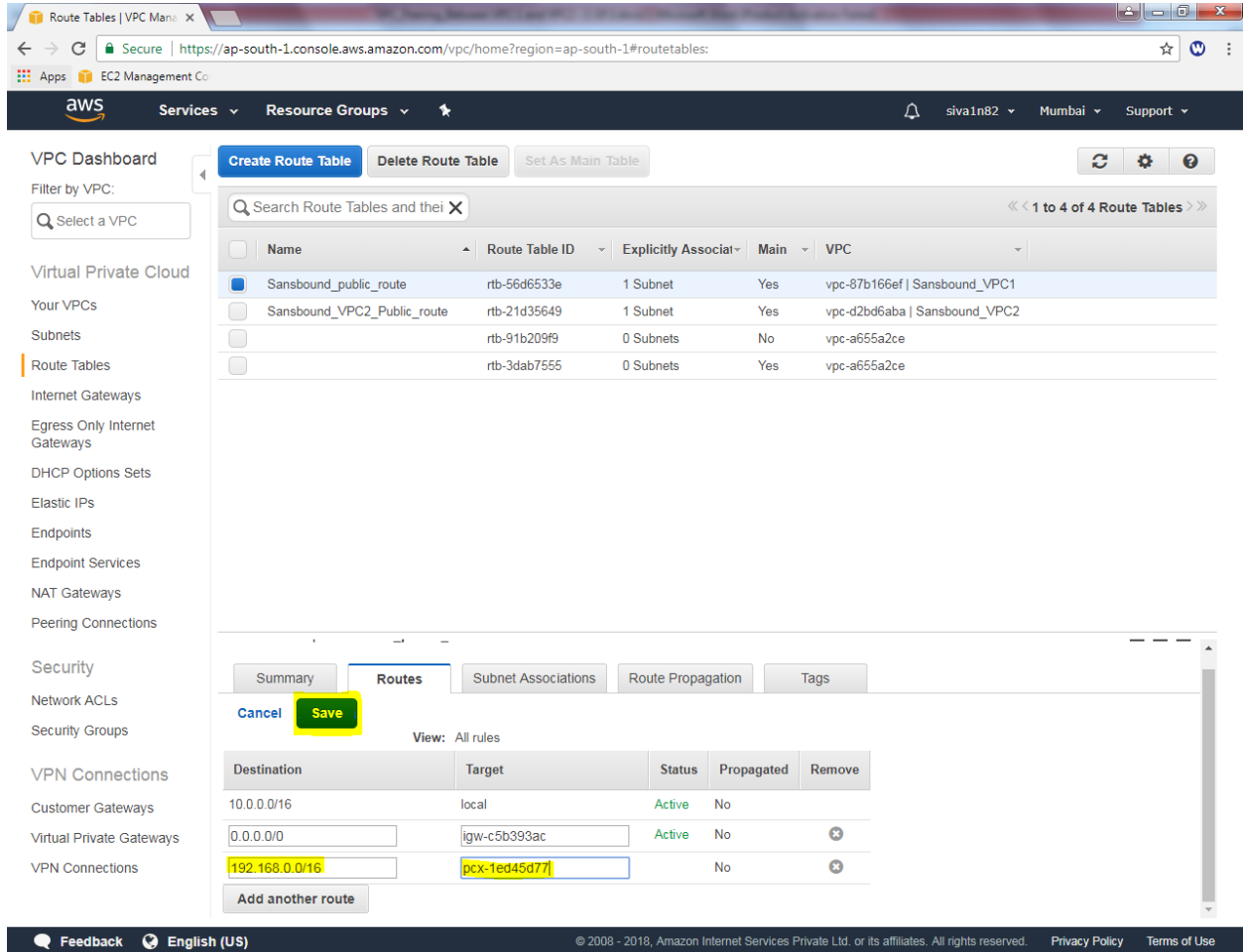
The screenshot shows the AWS Management Console interface for VPC Route Tables. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and various network services. The main content area displays a list of route tables. The 'Sansbound_public_route' is selected, and the 'Routes' tab is active, showing a table with two routes. The 'Add another route' button is visible at the bottom of the route table.

Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/> Sansbound_public_route	rtb-56d6533e	1 Subnet	Yes	vpc-87b166ef Sansbound_VPC1
<input type="checkbox"/> Sansbound_VPC2_Public_route	rtb-21d35649	1 Subnet	Yes	vpc-d2bd6aba Sansbound_VPC2
<input type="checkbox"/>	rtb-91b209f9	0 Subnets	No	vpc-a655a2ce
<input type="checkbox"/>	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	

Add another route

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

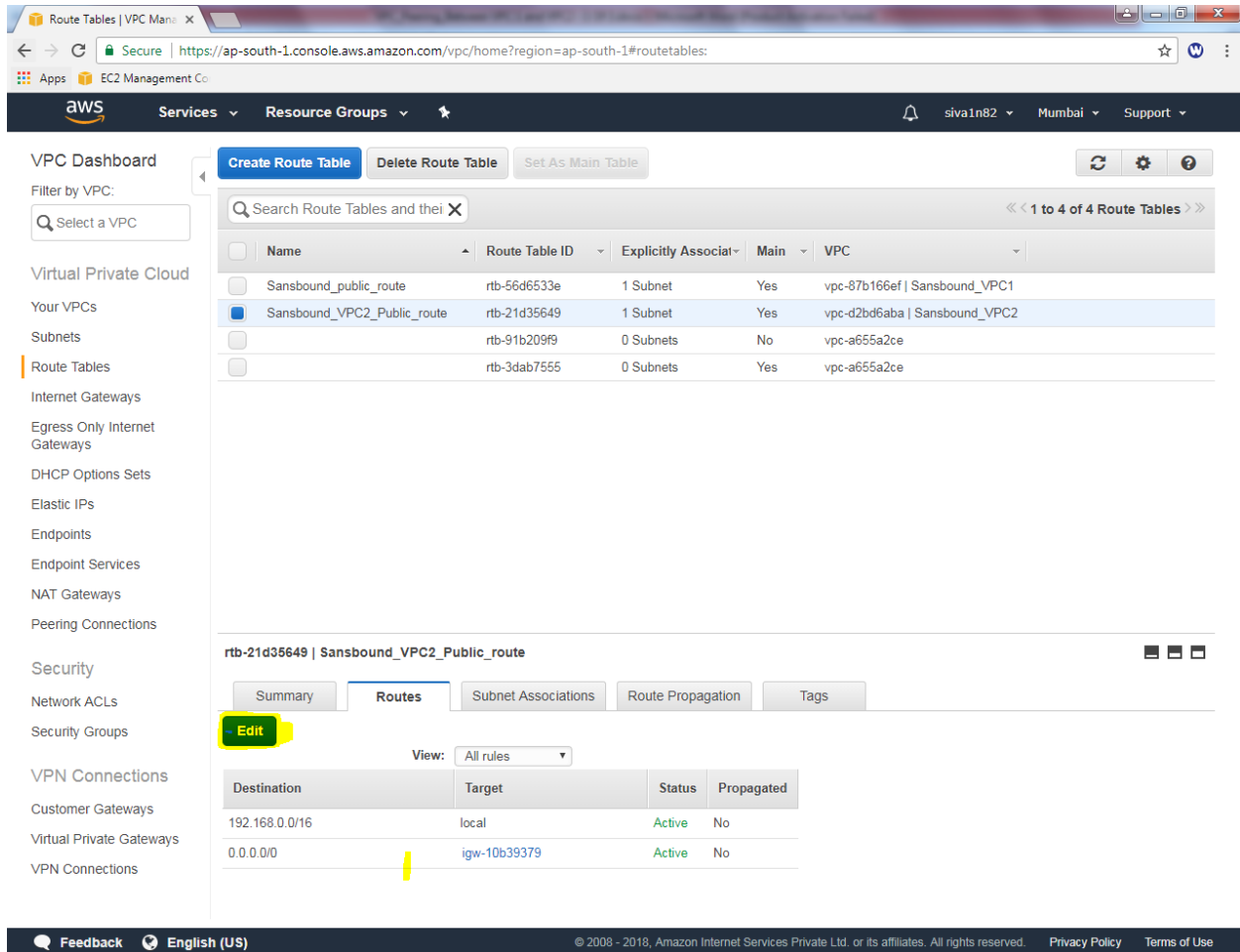


The screenshot shows the AWS Management Console interface for the 'Route Tables' section. The 'Routes' tab is selected, and a route is being edited. The 'Destination' field is set to '192.168.0.0/16' and the 'Target' is set to 'pcx-1ed45d771'. The 'Save' button is highlighted in yellow.

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-1ed45d771	No	No	✖

Click “Save”.

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



The screenshot shows the AWS Management Console interface for the VPC Dashboard. The left sidebar contains a navigation menu with categories like Virtual Private Cloud, Security, and VPN Connections. The main content area displays a list of route tables. The table 'Sansbound_VPC2_Public_route' is selected, and the 'Routes' tab is active. Below the tabs, there is a table of routes with columns for Destination, Target, Status, and Propagated. The route for destination 0.0.0.0/0 is highlighted.

VPC Dashboard

Filter by 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

Route Tables

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their associated subnets

Name	Route Table ID	Explicitly Associated Subnets	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

Summary Routes Subnet Associations Route Propagation Tags

Edit

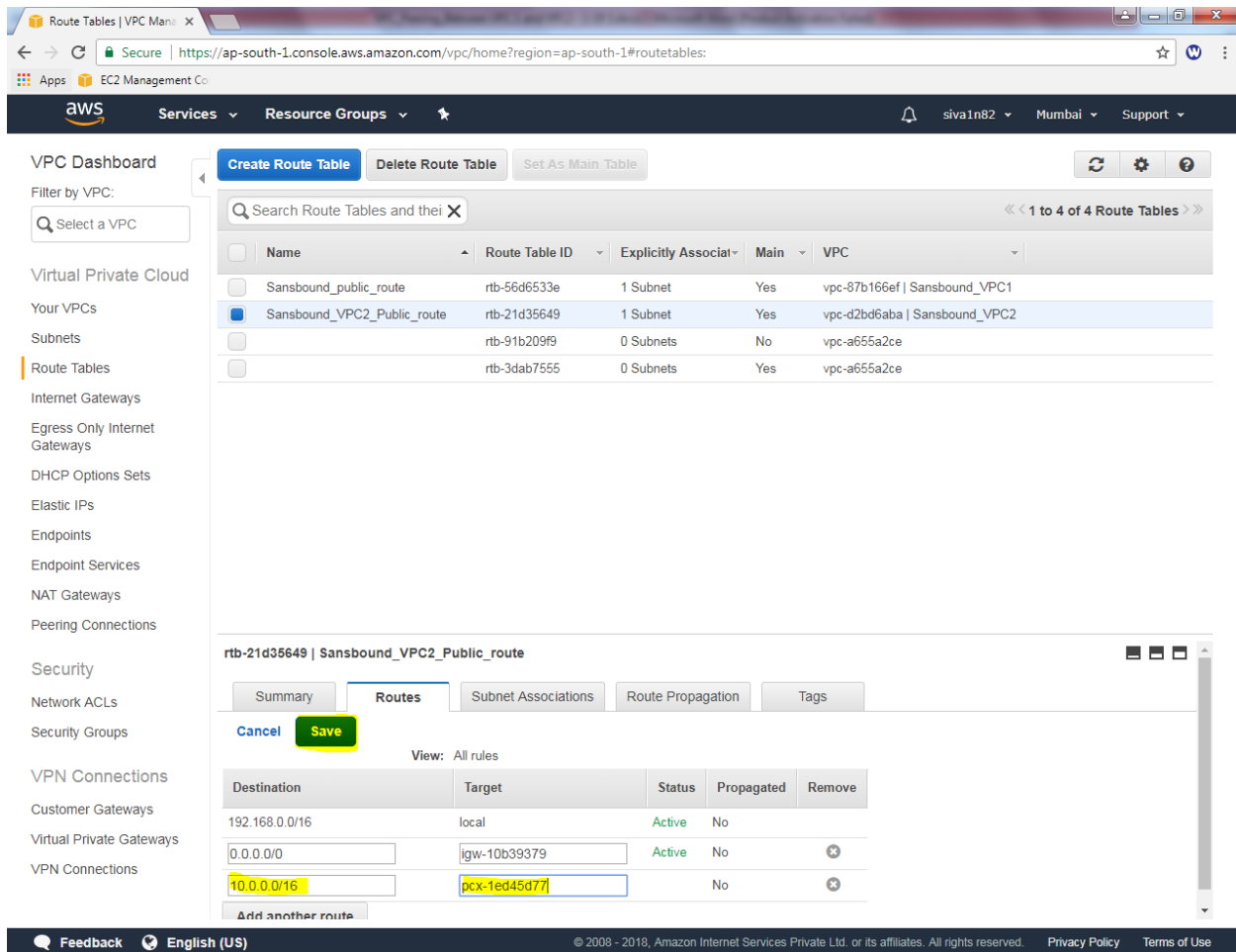
View: All rules

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

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

Click “add another route”

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



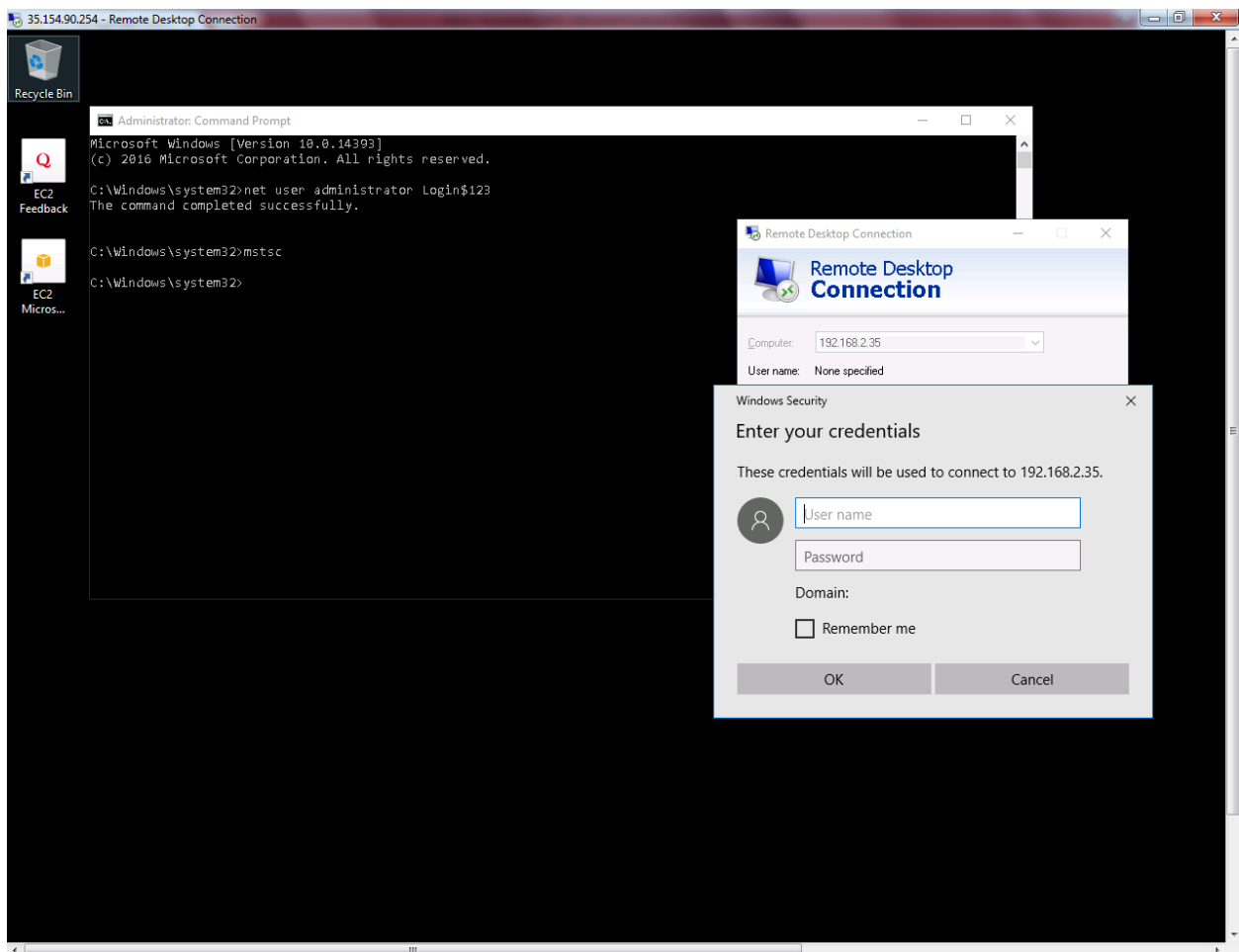
The screenshot shows the AWS Management Console interface. On the left is the navigation menu with categories like Virtual Private Cloud, Security, and VPN Connections. The main area displays the 'Route Tables | VPC Management' page. A table lists route tables, with 'Sansbound_VPC2_Public_route' (rtb-21d35649) selected. Below the table, the 'Routes' tab is active, showing a list of routes. The 'Destination' column contains '10.0.0.0/16', and the 'Target' column contains 'pcx-1ed45d7f'. The 'Status' is 'Active' and 'Propagated' is 'No'. At the bottom of the route list, there is a button labeled '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

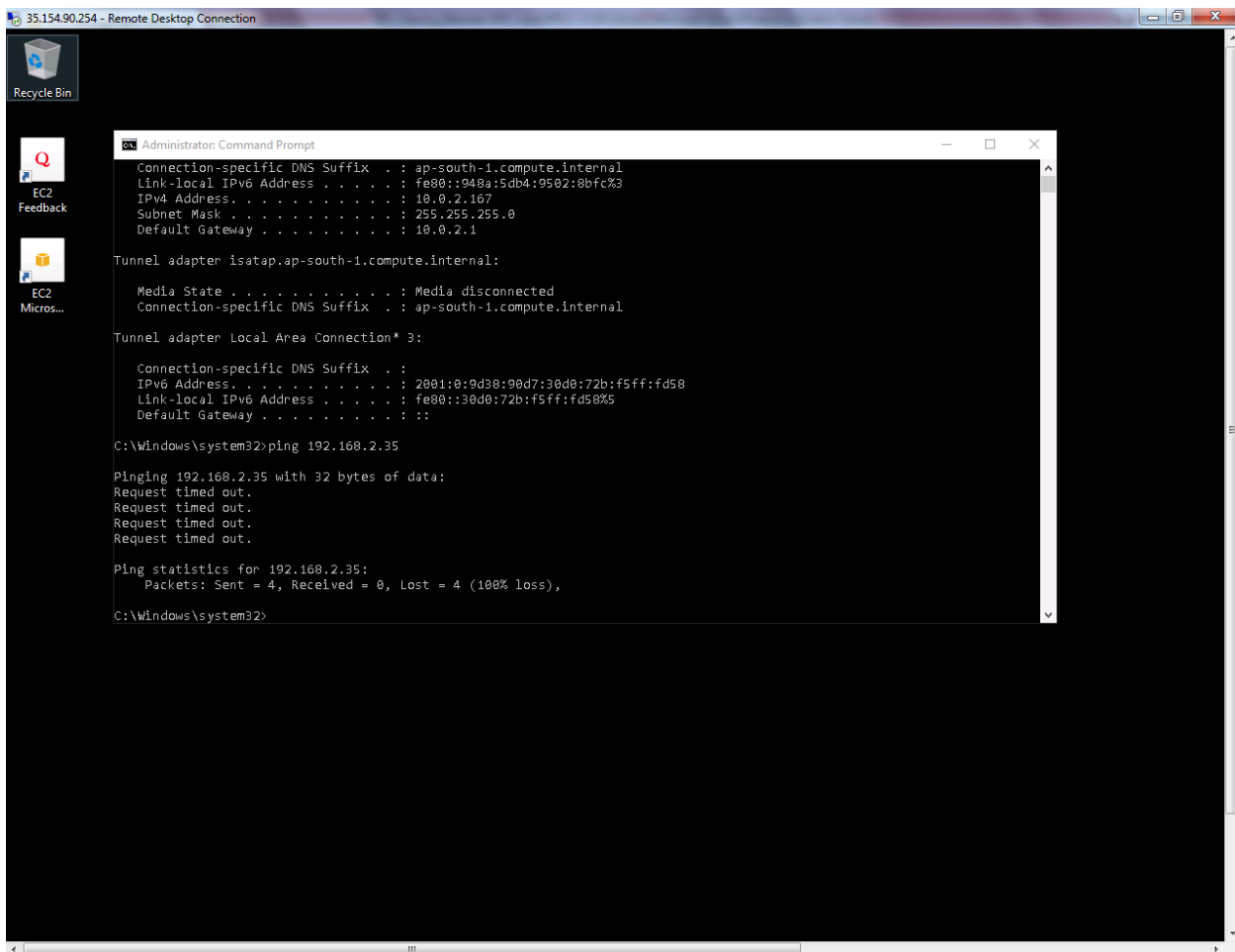
Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-10b39379	Active	No	✕
10.0.0.0/16	pcx-1ed45d7f	No	No	✕

Then click “save”.

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



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 Microservices

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

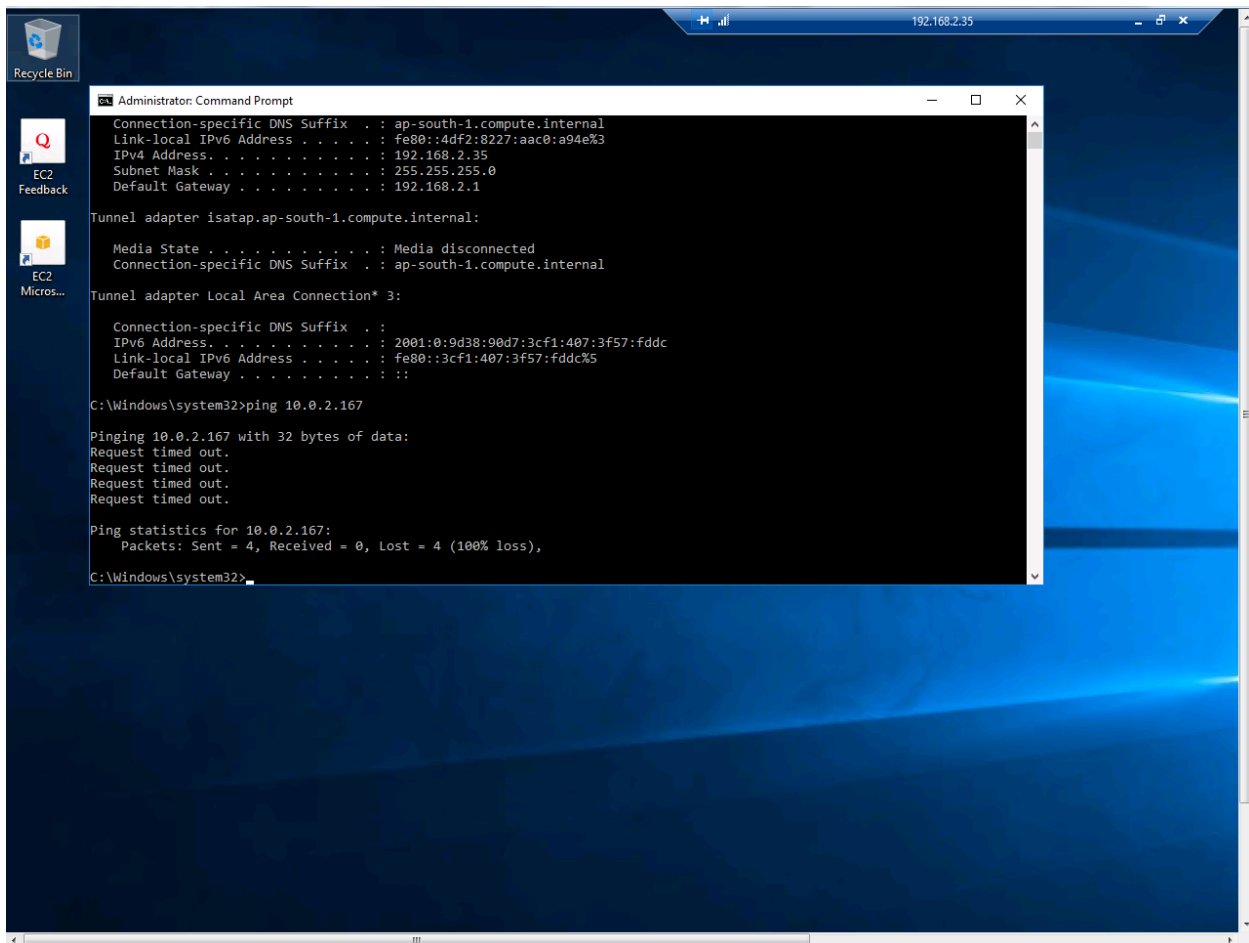
C:\Windows\system32>ping 192.168.2.35

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.



```
Administrator: Command Prompt
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:fdcd
Link-local IPv6 Address . . . . . : fe80::3cf1:407:3f57:fdcd%5
Default Gateway . . . . . :

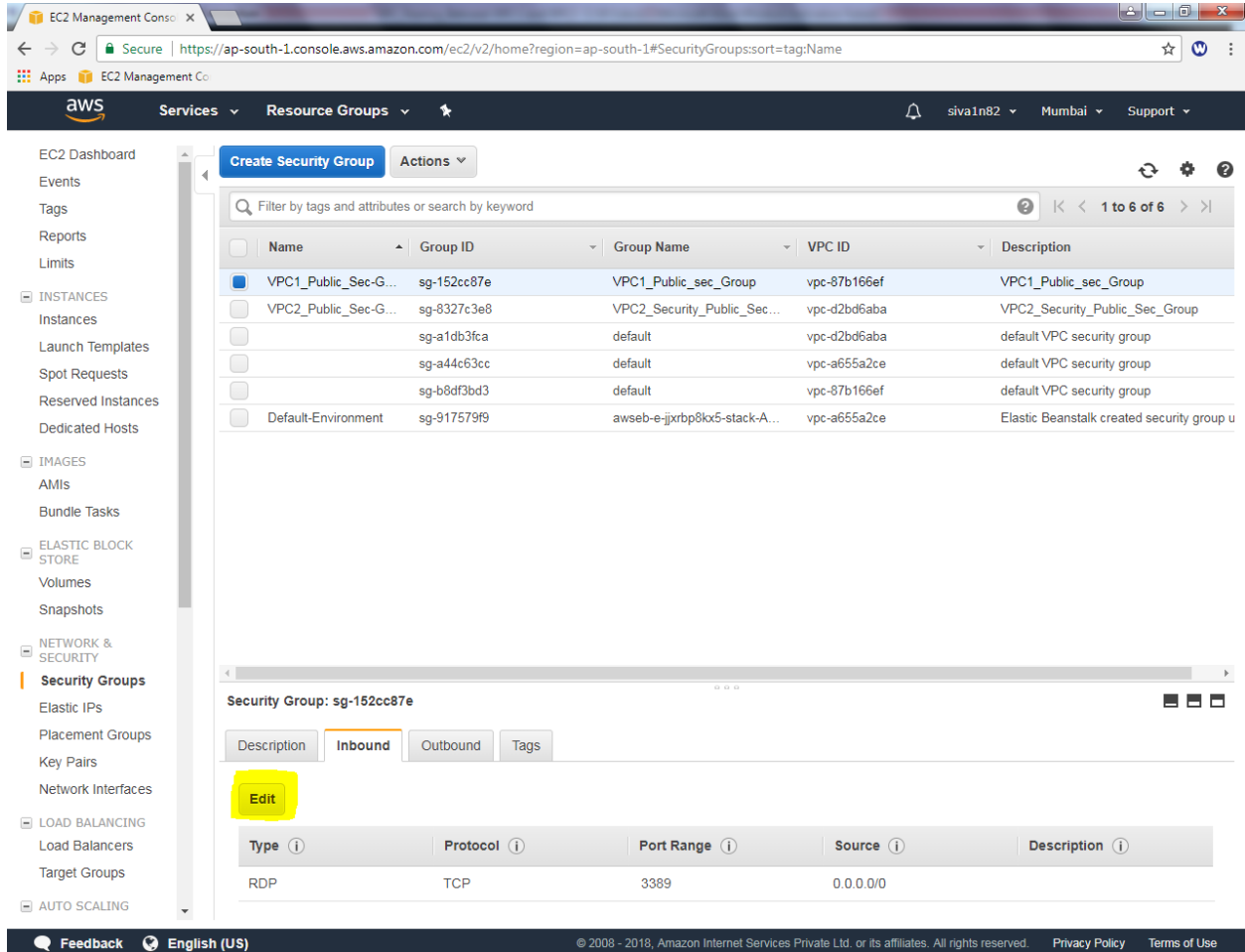
C:\Windows\system32>ping 10.0.2.167

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”.



The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The 'Security Groups' link under NETWORK & SECURITY is selected. The main content area displays a list of security groups. The first group, 'VPC1_Public_Sec-G...', is selected. Below the list, the 'Security Group: sg-152cc87e' details are shown. The 'Inbound' tab is active, and the 'Edit' button is highlighted in yellow. The inbound rules table shows a single rule for RDP on TCP port 3389 from source 0.0.0.0/0.

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

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	×

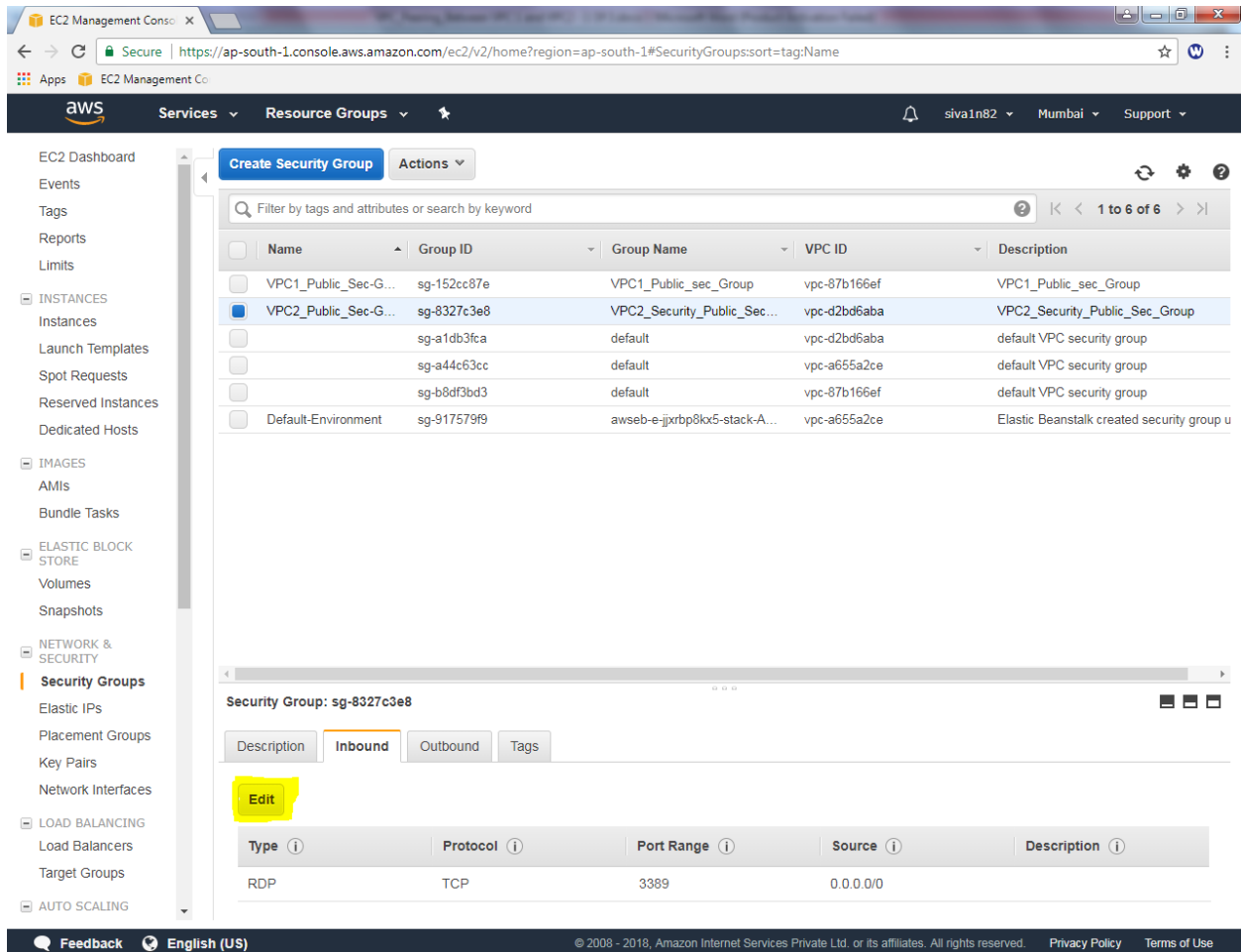
Add Rule

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

Then click “save” .

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



The screenshot shows the AWS Management Console interface. On the left, the navigation pane lists various services, with 'Security Groups' under 'NETWORK & SECURITY' highlighted. The main content area displays a list of security groups. The group 'VPC2_Public_Sec-G...' with ID 'sg-8327c3e8' is selected. Below the list, the 'Security Group: sg-8327c3e8' section is visible, with the 'Inbound' tab selected. An 'Edit' button is highlighted with a yellow box. Below the tabs, a table shows the existing inbound rule for RDP on port 3389.

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 ✕

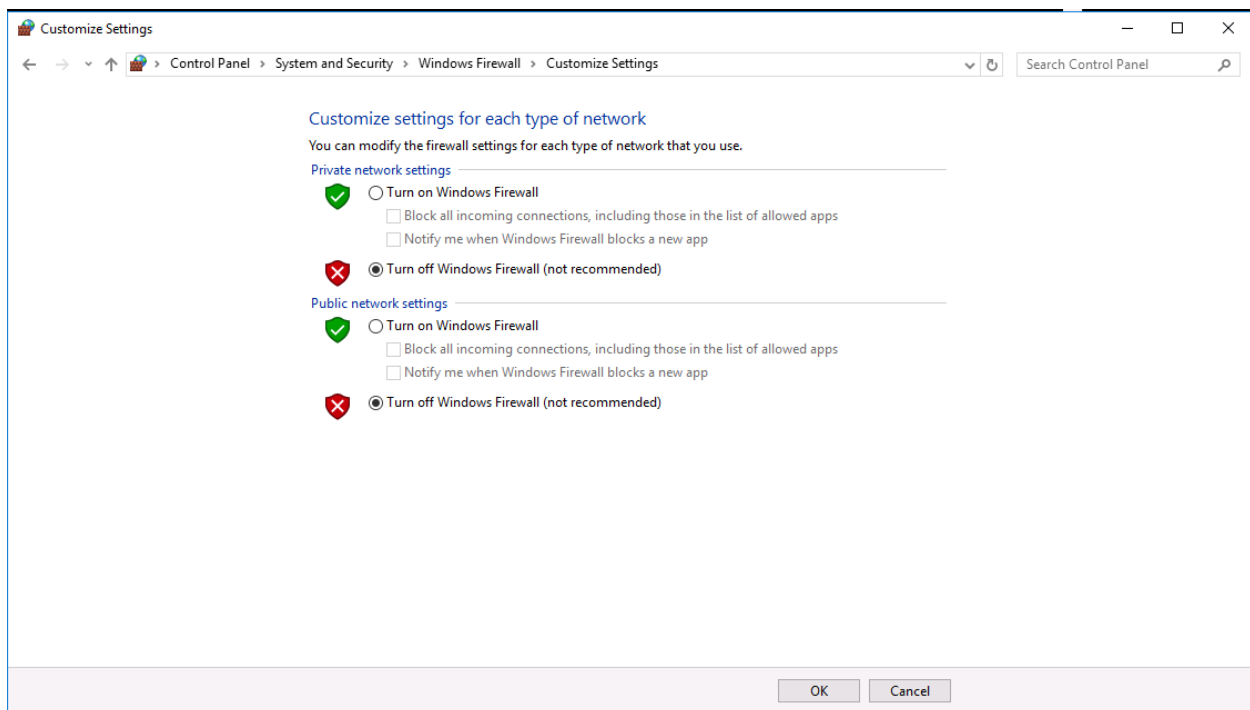
Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	Description <small>i</small>	
RDP ▾	TCP	3389	Custom ▾ 0.0.0.0/0	e.g. SSH for Admin Desktop	✕
Custom ICMP ▾	Echo Reque ▾	N/A	Custom ▾ 0.0.0.0/0	e.g. SSH for Admin Desktop	✕

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.

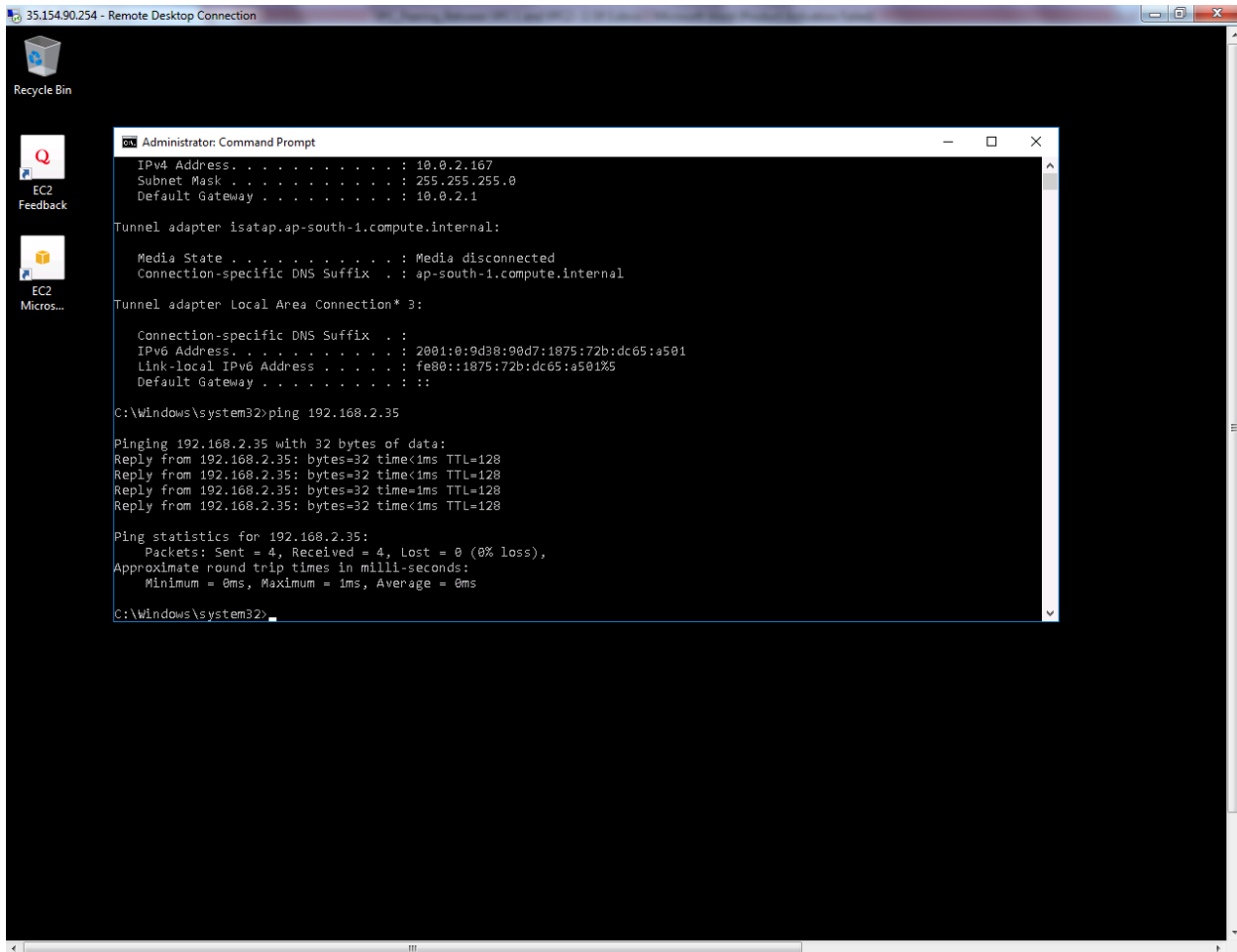
Cancel
Save

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



The screenshot shows the 'Customize Settings' window for Windows Firewall. The breadcrumb path is 'Control Panel > System and Security > Windows Firewall > Customize Settings'. The window title is 'Customize Settings'. Below the title bar, there is a search bar labeled 'Search Control Panel'. The main content area is titled 'Customize settings for each type of network' and includes the instruction: 'You can modify the firewall settings for each type of network that you use.' There are two sections: 'Private network settings' and 'Public network settings'. Each section has a green checkmark icon and two radio button options: 'Turn on Windows Firewall' (which is unchecked) and 'Turn off Windows Firewall (not recommended)' (which is selected). Under 'Turn on Windows Firewall', there are two checkboxes: 'Block all incoming connections, including those in the list of allowed apps' and 'Notify me when Windows Firewall blocks a new app'. At the bottom of the window, there are 'OK' and 'Cancel' buttons.

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



```
35.154.90.254 - Remote Desktop Connection

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 . . . . . : ::

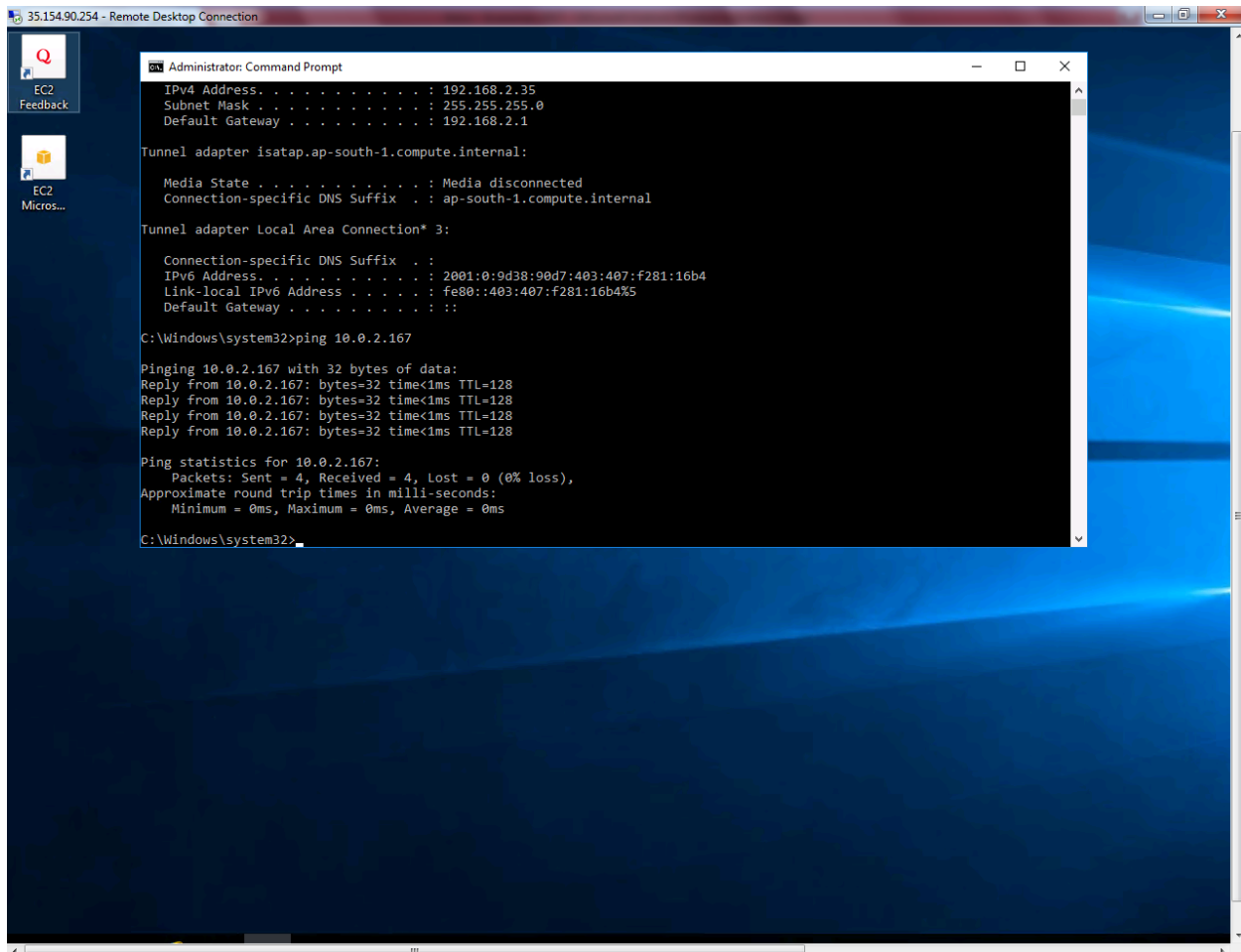
C:\Windows\system32>ping 192.168.2.35

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

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>
```