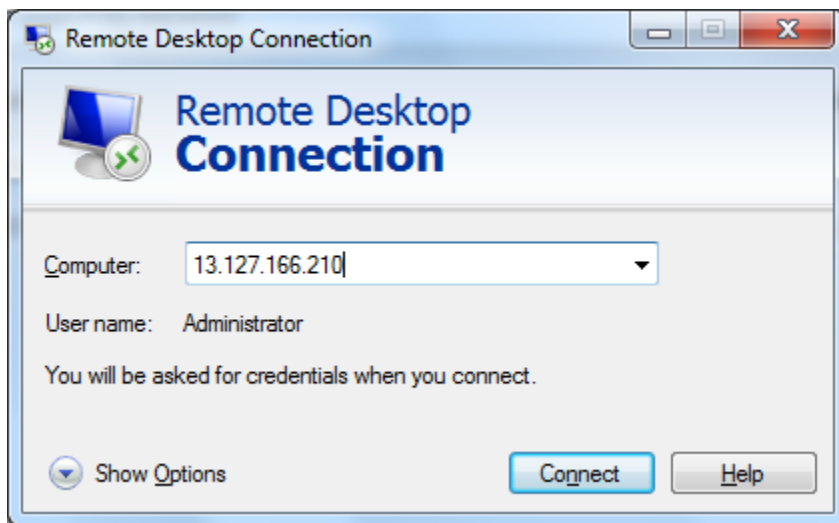


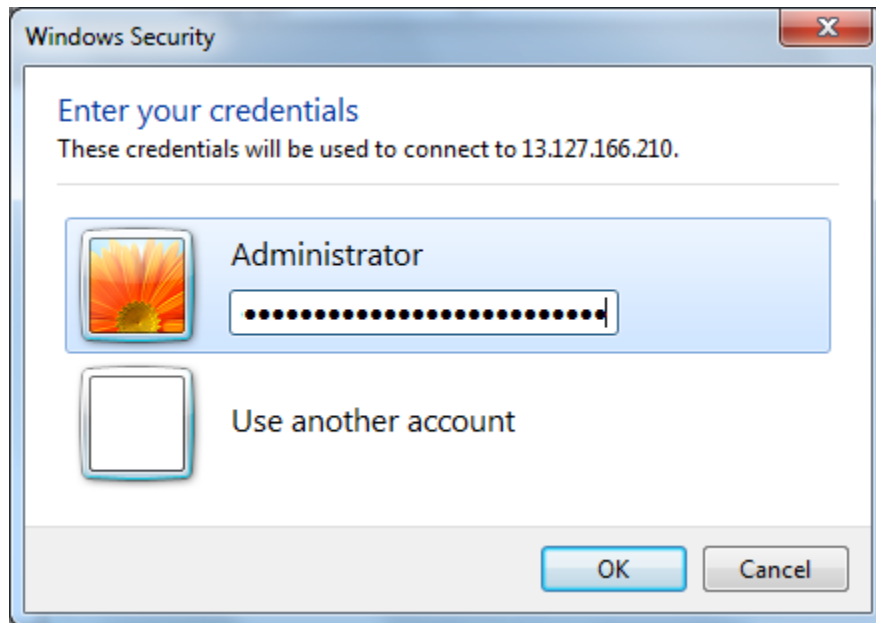
Stateful and Stateless firewall

Note: Before Start this scenario, you must be configured VPC, Internet gateway and Nat gateway in your AWS Console. Then only it will work.

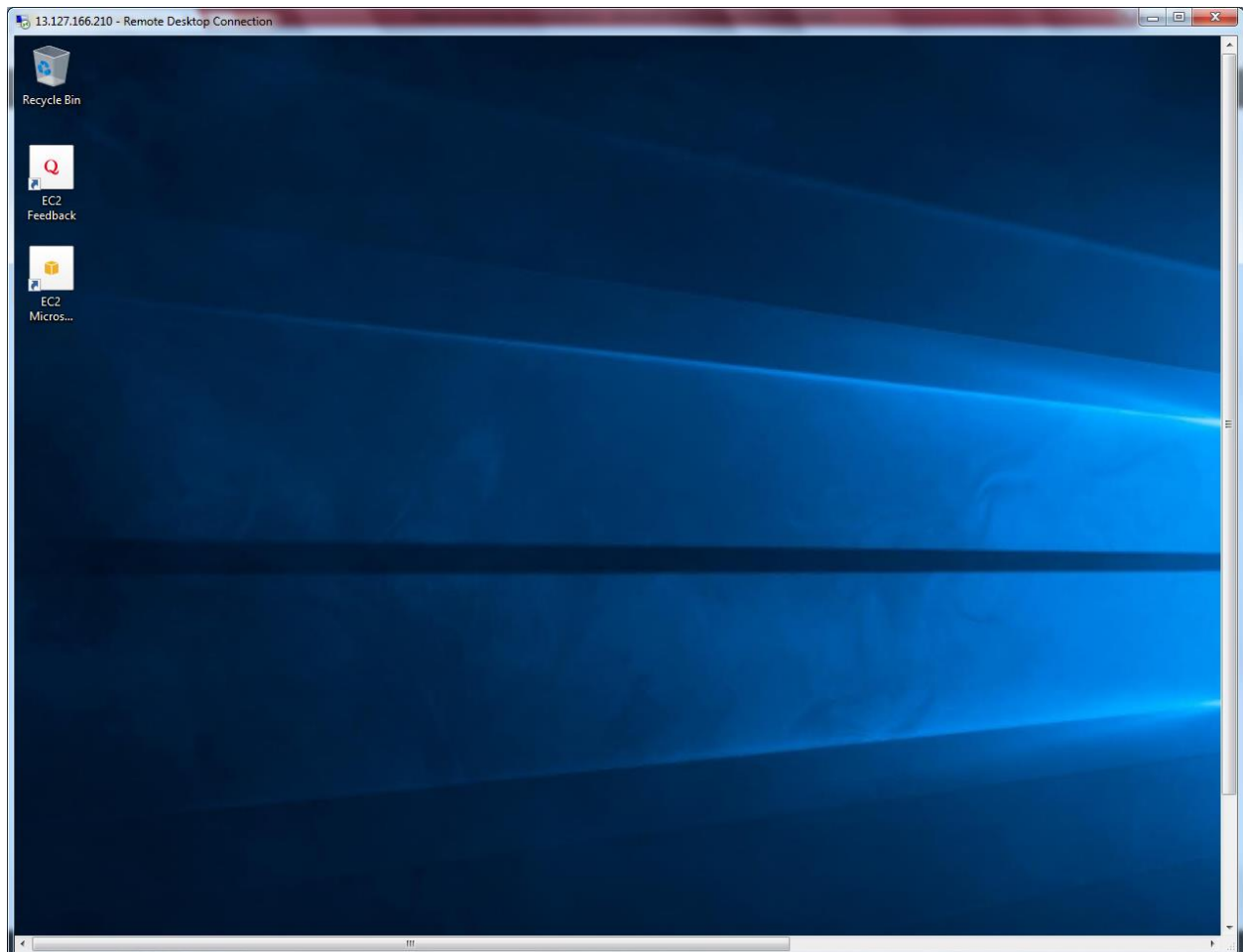
a) Stateful firewall

Type the public server IP in mstsc

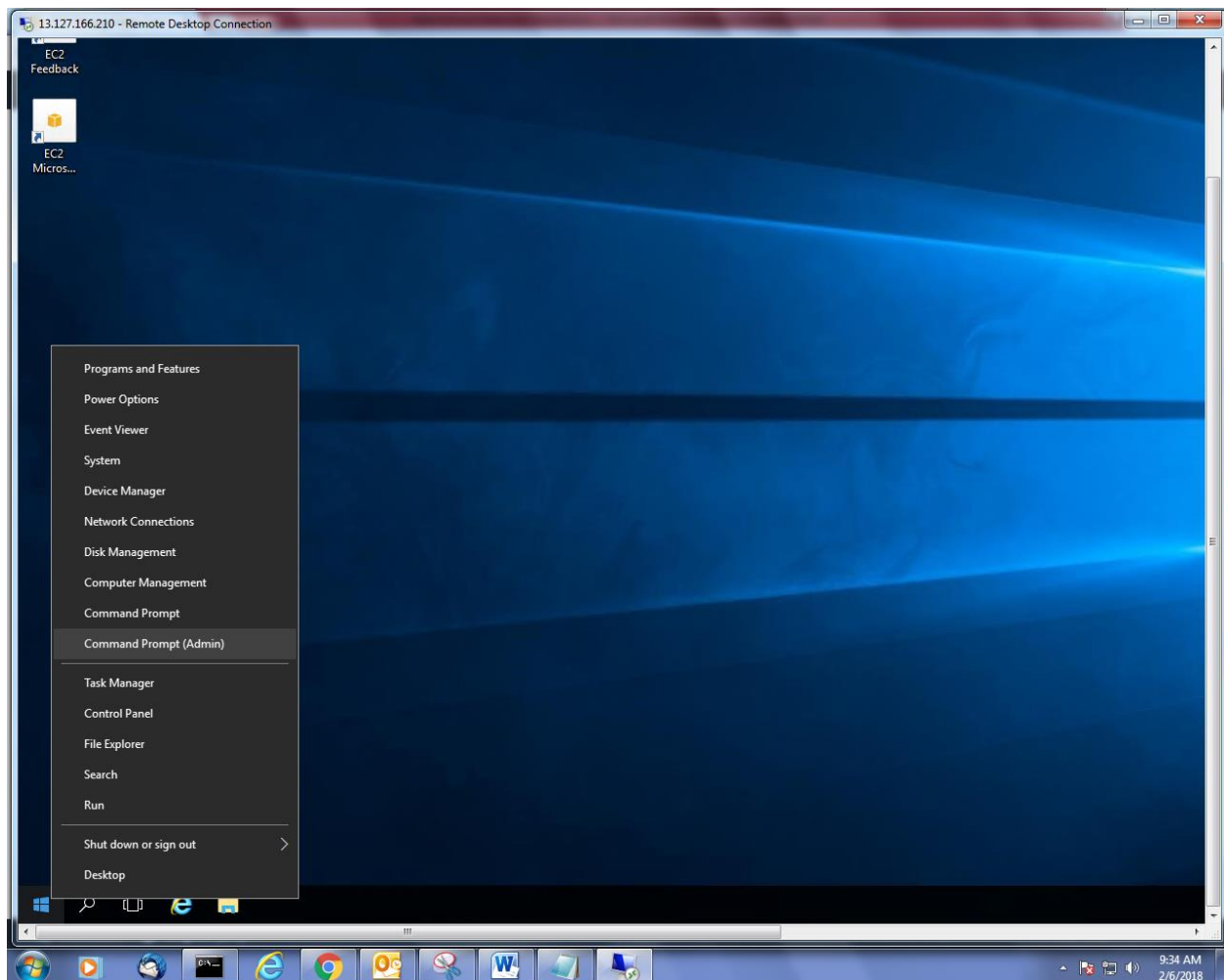




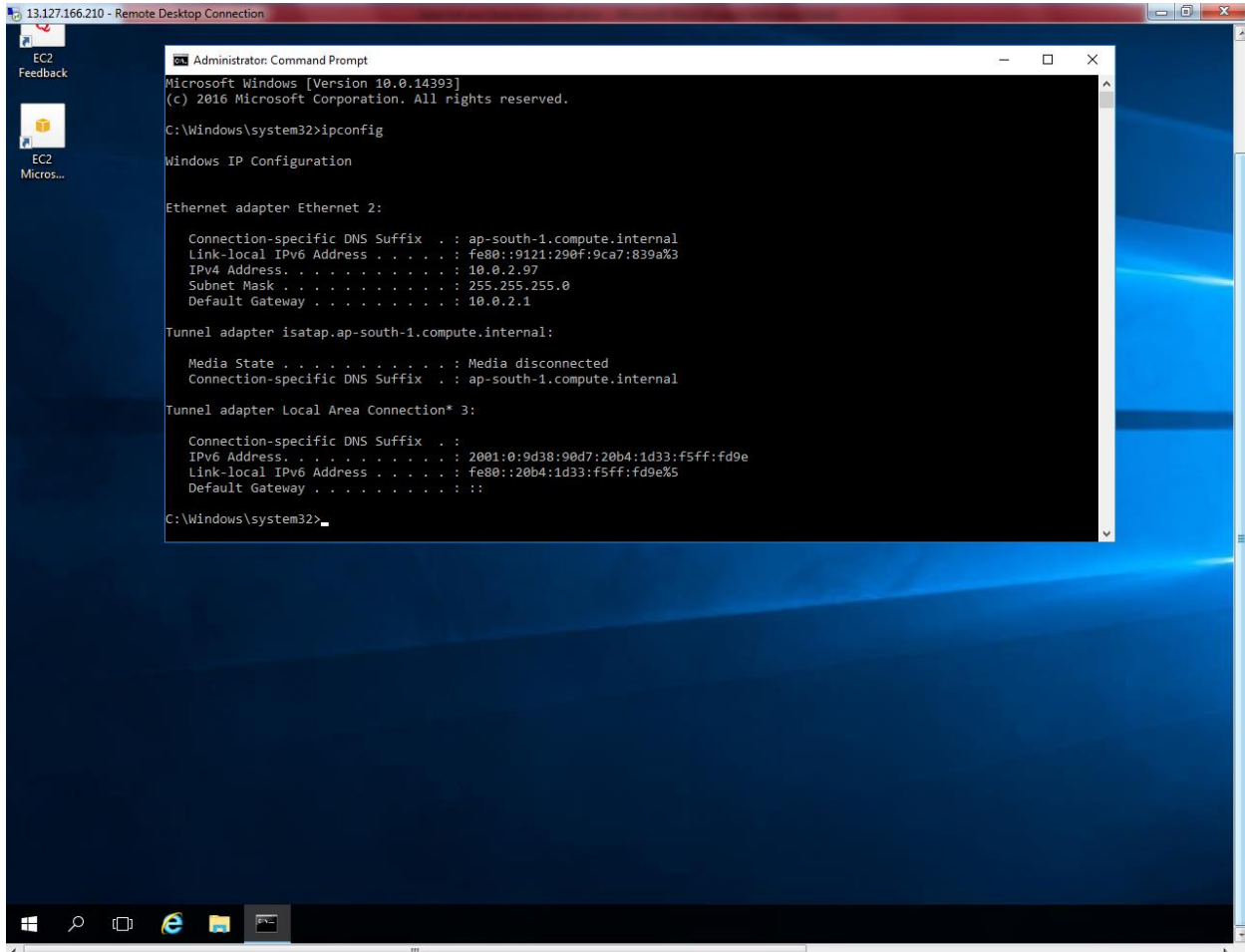
Logged into the Public Server successfully.



Right click of start menu and click “Command prompt (Admin).



Type “ipconfig” to get the ip address.



The screenshot shows a Remote Desktop Connection window titled "13.127.166.210 - Remote Desktop Connection". The desktop background is the standard Windows 10 blue wallpaper. On the left sidebar, there are icons for "EC2 Feedback", "EC2", and "Micros...". A "Command Prompt" window is open, displaying the output of the "ipconfig" command. The output shows the IP configuration for the Ethernet adapter "Ethernet 2" and the Tunnel adapter "isatap.ap-south-1.compute.internal".

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

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : ap-south-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::9121:290f:9ca7:839a%3
    IPv4 Address. . . . . : 10.0.2.97
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

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

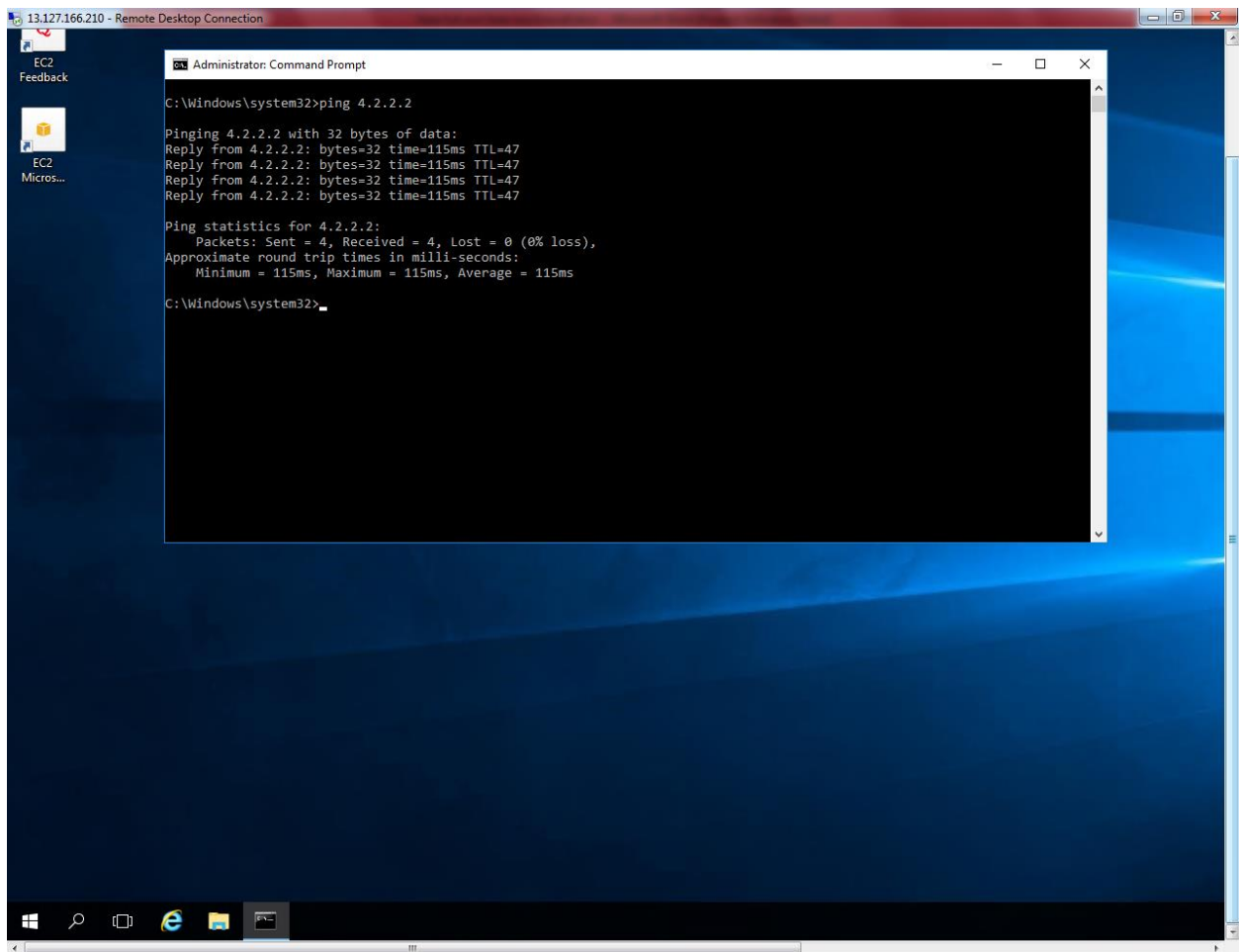
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : ap-south-1.compute.internal

Tunnel adapter Local Area Connection* 3:

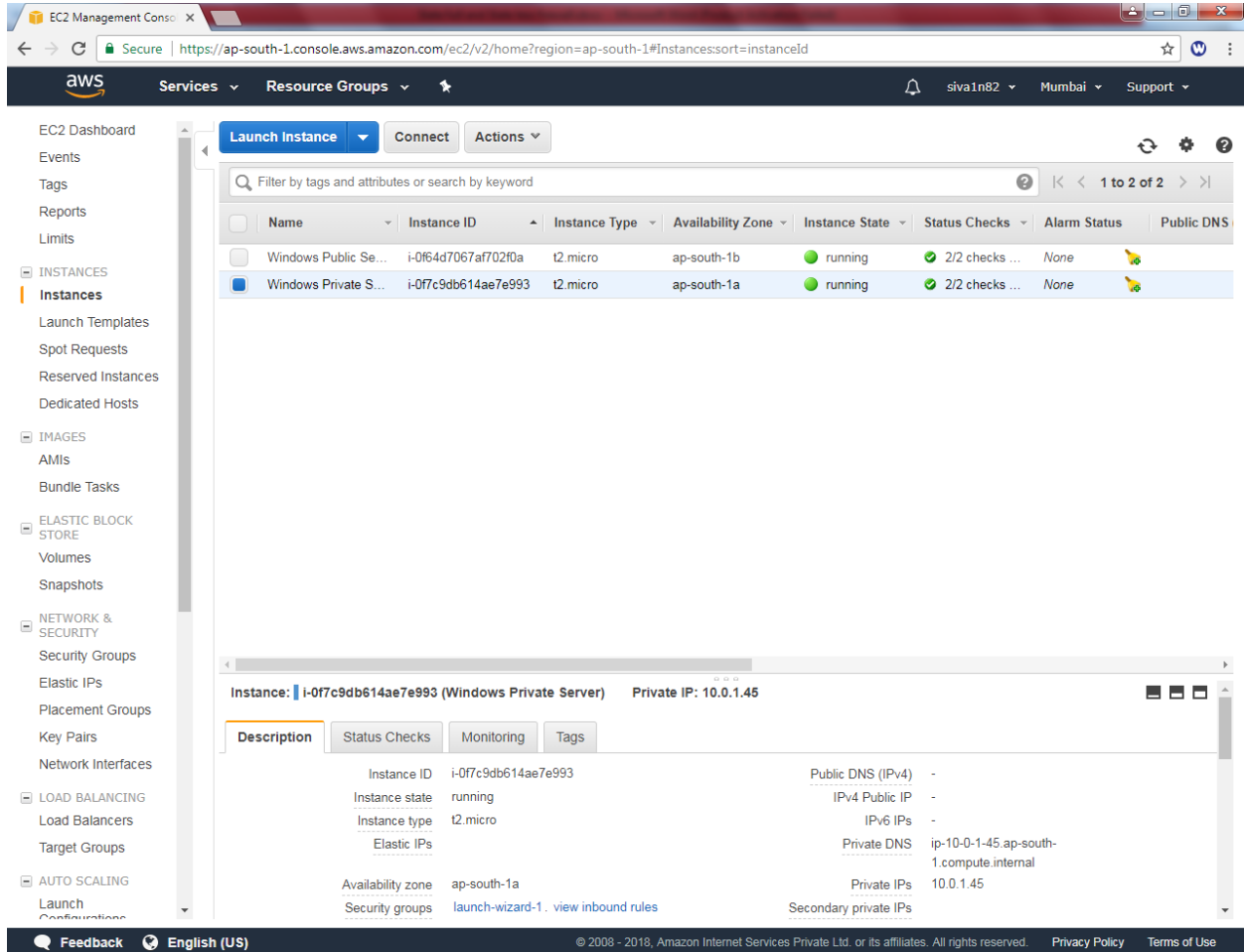
    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:9d38:90d7:20b4:1d33:f5ff:fd9e
    Link-local IPv6 Address . . . . . : fe80::20b4:1d33:f5ff:fd9e%5
    Default Gateway . . . . . :

C:\Windows\system32>
```

You can able to access public network from public subnet.



Get the private IP address of Private subnet 10.0.1.45



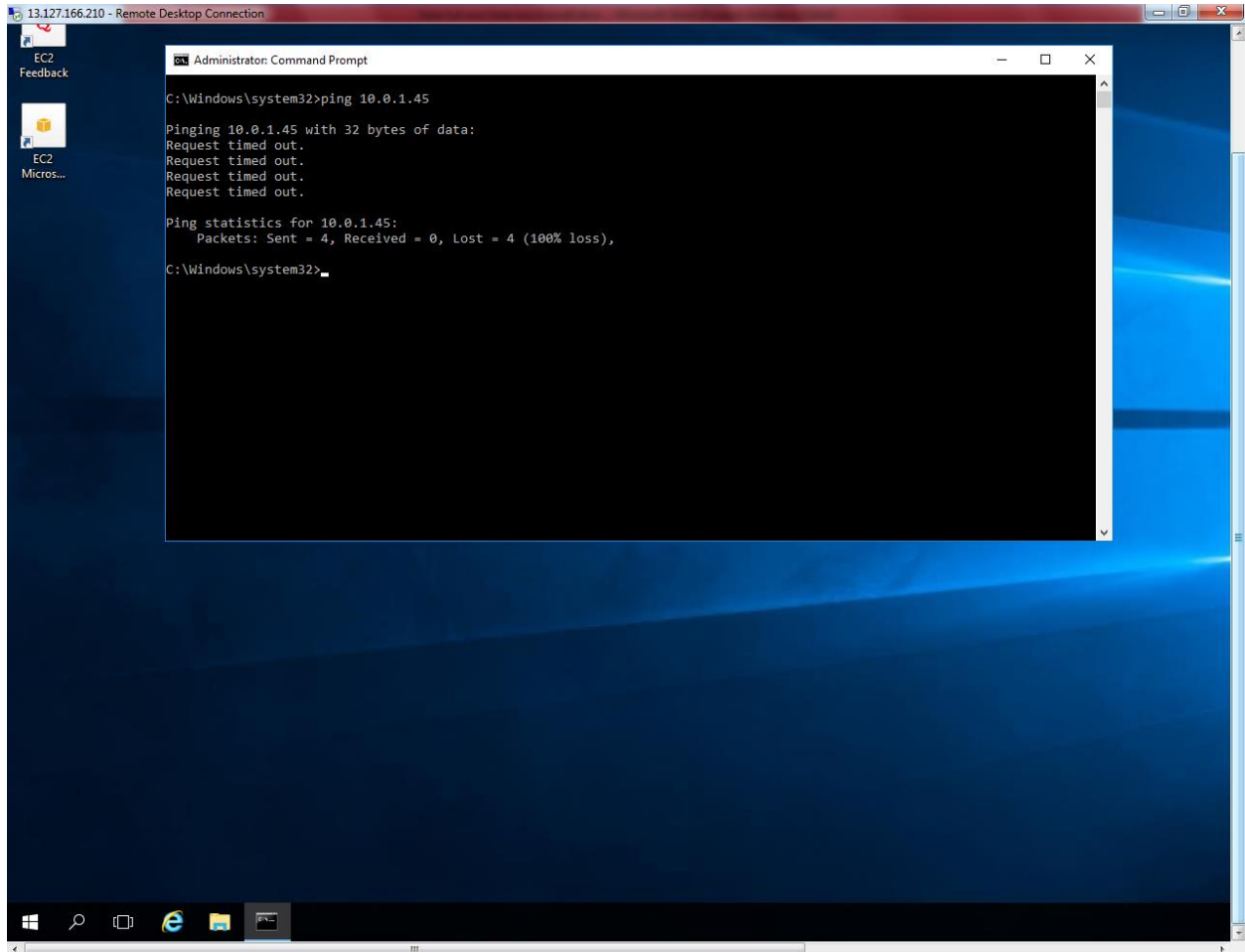
The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area displays a table of EC2 instances. The instance 'Windows Private S...' with ID 'i-0f7c9db614ae7e993' is selected. Below the table, the details for this instance are shown, including its status (running), type (t2.micro), and availability zone (ap-south-1a). The private IP address is listed as 10.0.1.45.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Windows Public Se...	i-0f64d7067af702f0a	t2.micro	ap-south-1b	running	2/2 checks ...	None	
Windows Private S...	i-0f7c9db614ae7e993	t2.micro	ap-south-1a	running	2/2 checks ...	None	

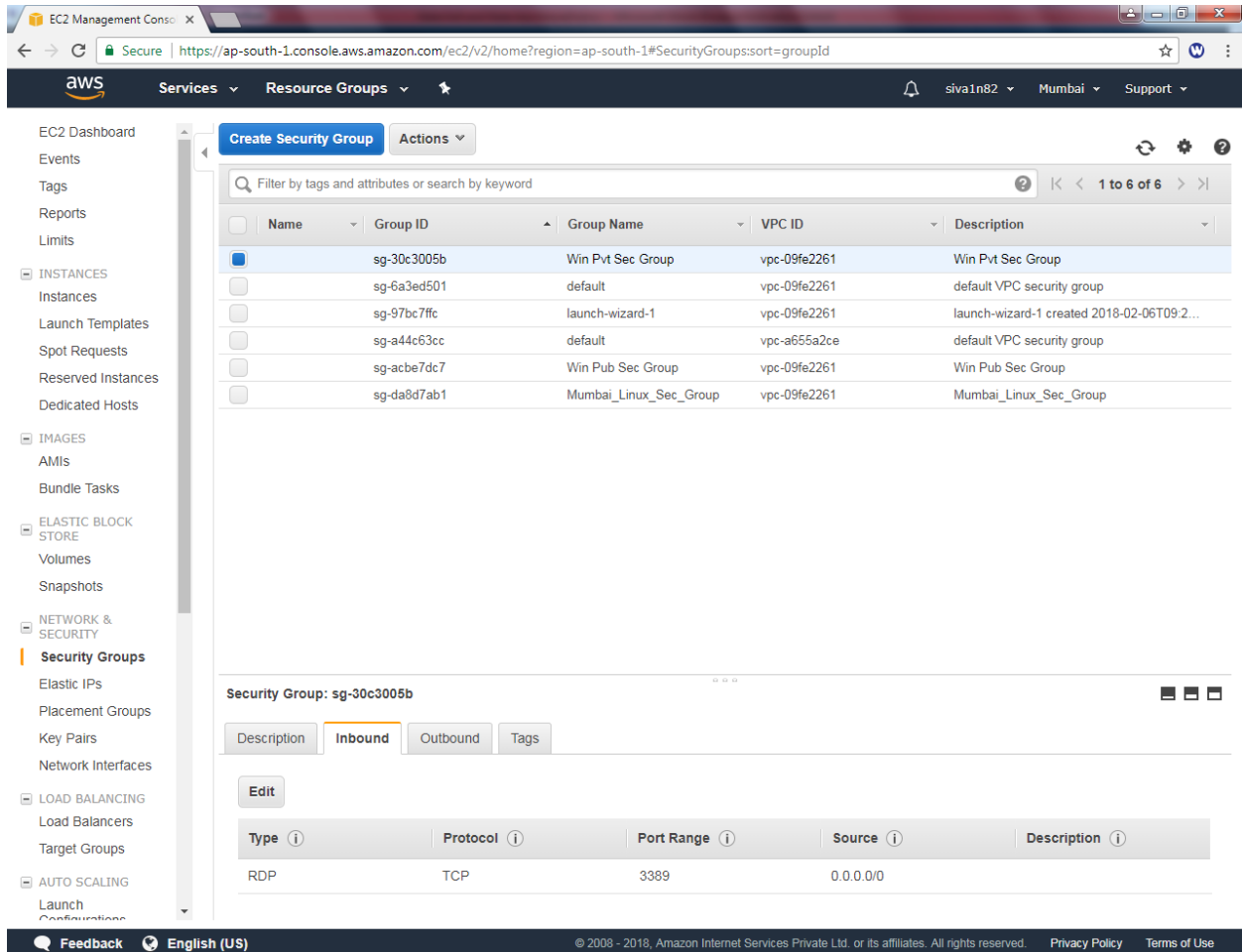
Instance: **i-0f7c9db614ae7e993 (Windows Private Server)** Private IP: 10.0.1.45

Description		Status Checks		Monitoring		Tags	
Instance ID	i-0f7c9db614ae7e993	Public DNS (IPv4)	-				
Instance state	running	IPv4 Public IP	-				
Instance type	t2.micro	IPv6 IPs	-				
Elastic IPs		Private DNS	ip-10-0-1-45.ap-south-1.compute.internal				
Availability zone	ap-south-1a	Private IPs	10.0.1.45				
Security groups	launch-wizard-1. view inbound rules	Secondary private IPs					

Try to Ping 10.0.1.45, but getting request timed out. Because In security group of Private subnet allowed only RDP Port (3389) in inbound rules.



Go to security group and select “Win Pvt Sec Group”.



The screenshot shows the AWS Management Console interface for the 'Security Groups' section. The left-hand navigation pane lists various AWS services, with 'Security Groups' highlighted under the 'NETWORK & SECURITY' category. The main content area displays a table of security groups. The first group, 'Win Pvt Sec Group' (ID: sg-30c3005b), is selected. Below the table, the details for this specific security group are shown, including the 'Inbound' tab and a list of rules.

Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/>	sg-30c3005b	Win Pvt Sec Group	vpc-09fe2261	Win Pvt Sec Group
<input type="checkbox"/>	sg-6a3ed501	default	vpc-09fe2261	default VPC security group
<input type="checkbox"/>	sg-97bc7ffc	launch-wizard-1	vpc-09fe2261	launch-wizard-1 created 2018-02-06T09:2...
<input type="checkbox"/>	sg-a44c63cc	default	vpc-a655a2ce	default VPC security group
<input type="checkbox"/>	sg-acbe7dc7	Win Pub Sec Group	vpc-09fe2261	Win Pub Sec Group
<input type="checkbox"/>	sg-da8d7ab1	Mumbai_Linux_Sec_Group	vpc-09fe2261	Mumbai_Linux_Sec_Group

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

Click “Add Rule”.

Edit inbound rules

Type ⓘ

Protocol ⓘ

Port Range ⓘ

Source ⓘ

Description ⓘ

RDP ▾

TCP

3389

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

Select “All ICMP “ traffic and 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 ✕

All ICMP - IPv ▾

ICMP

0 - 65535

Custom ▾

0.0.0.0/0

e.g. SSH for Admin Desktop ✕

Add Rule

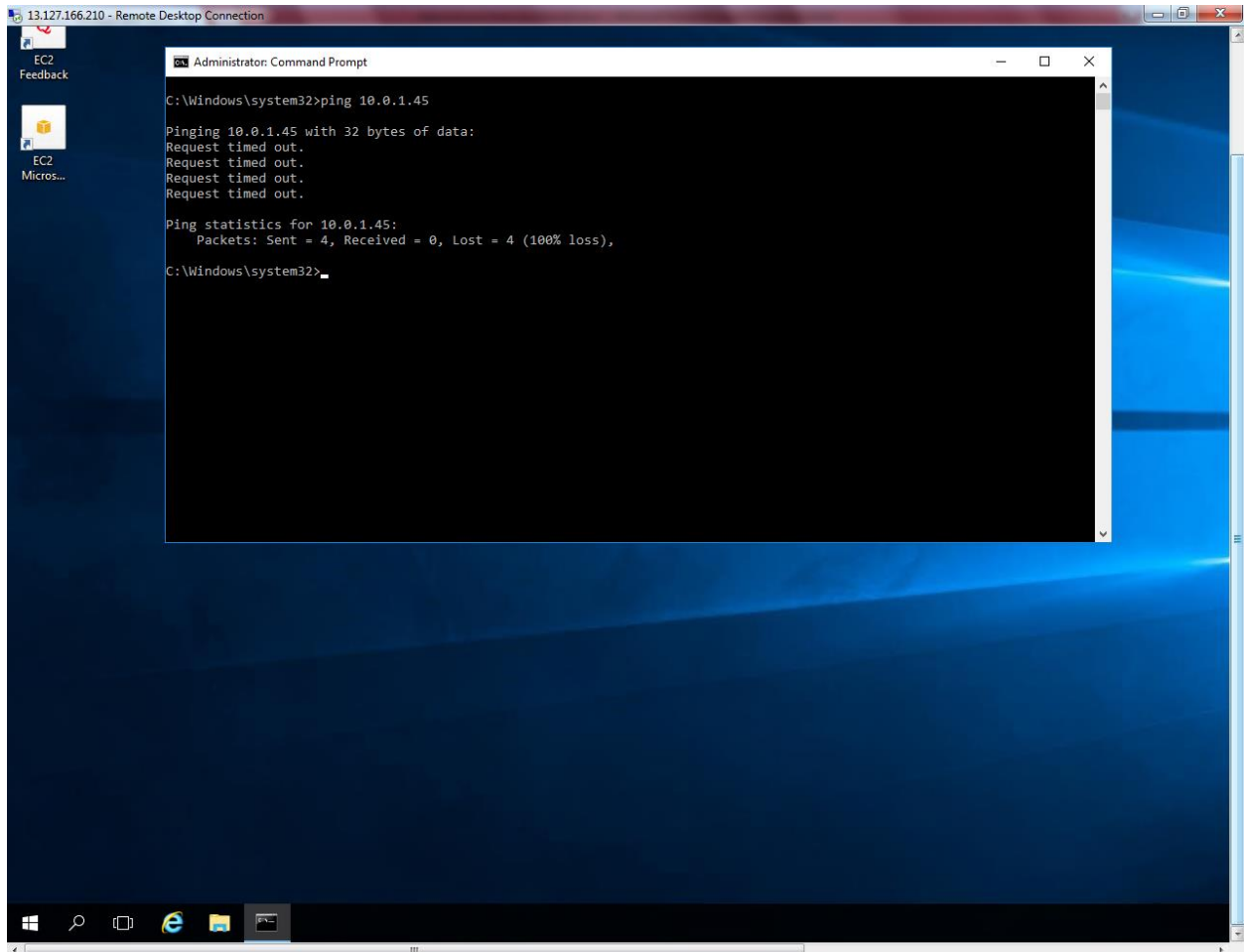
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel

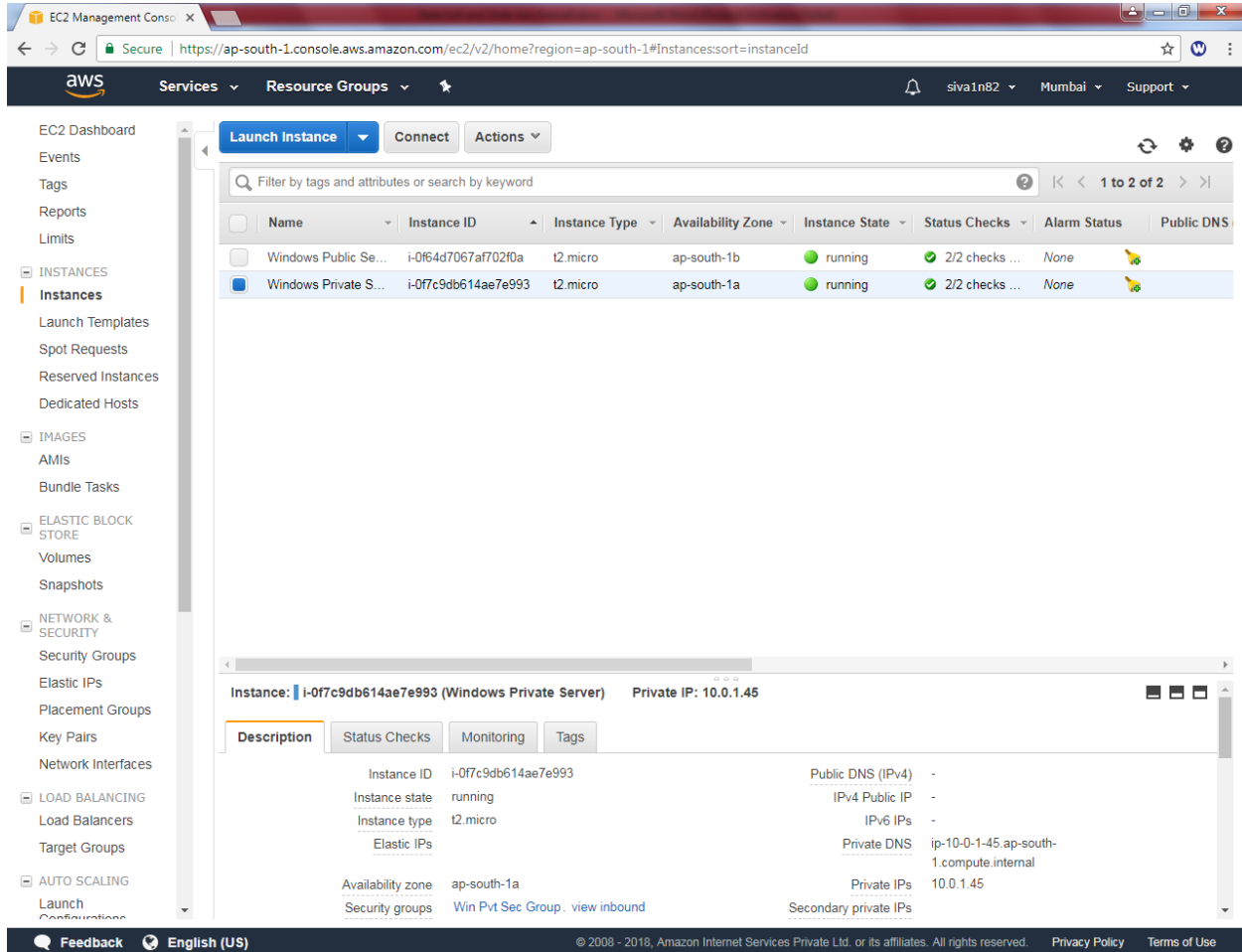
Save

Click “Save”.

Again try to ping 10.0.1.45 we are unable to ping because windows firewall on private subnet server need to be turned off.



Get the IP address of private server from AWS management console.



The screenshot shows the AWS Management Console for the EC2 service. The left sidebar contains navigation links for various AWS services. The main content area displays the 'Instances' page. A table lists two instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Windows Public Se...	i-0f64d7067af702f0a	t2.micro	ap-south-1b	running	2/2 checks ...	None	
Windows Private S...	i-0f7c9db614ae7e993	t2.micro	ap-south-1a	running	2/2 checks ...	None	

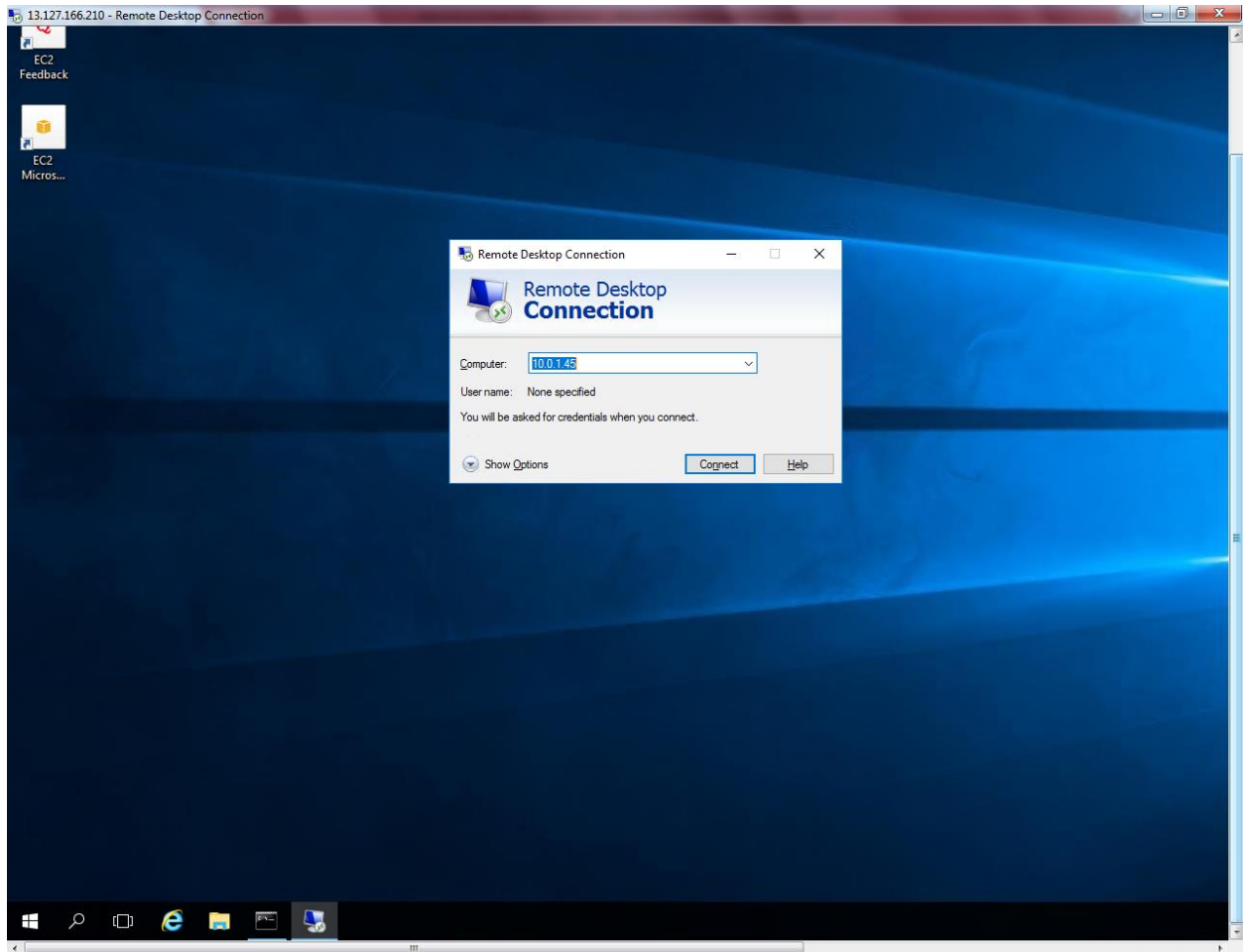
The second instance, 'Windows Private S...', is selected. Below the table, the details for this instance are shown:

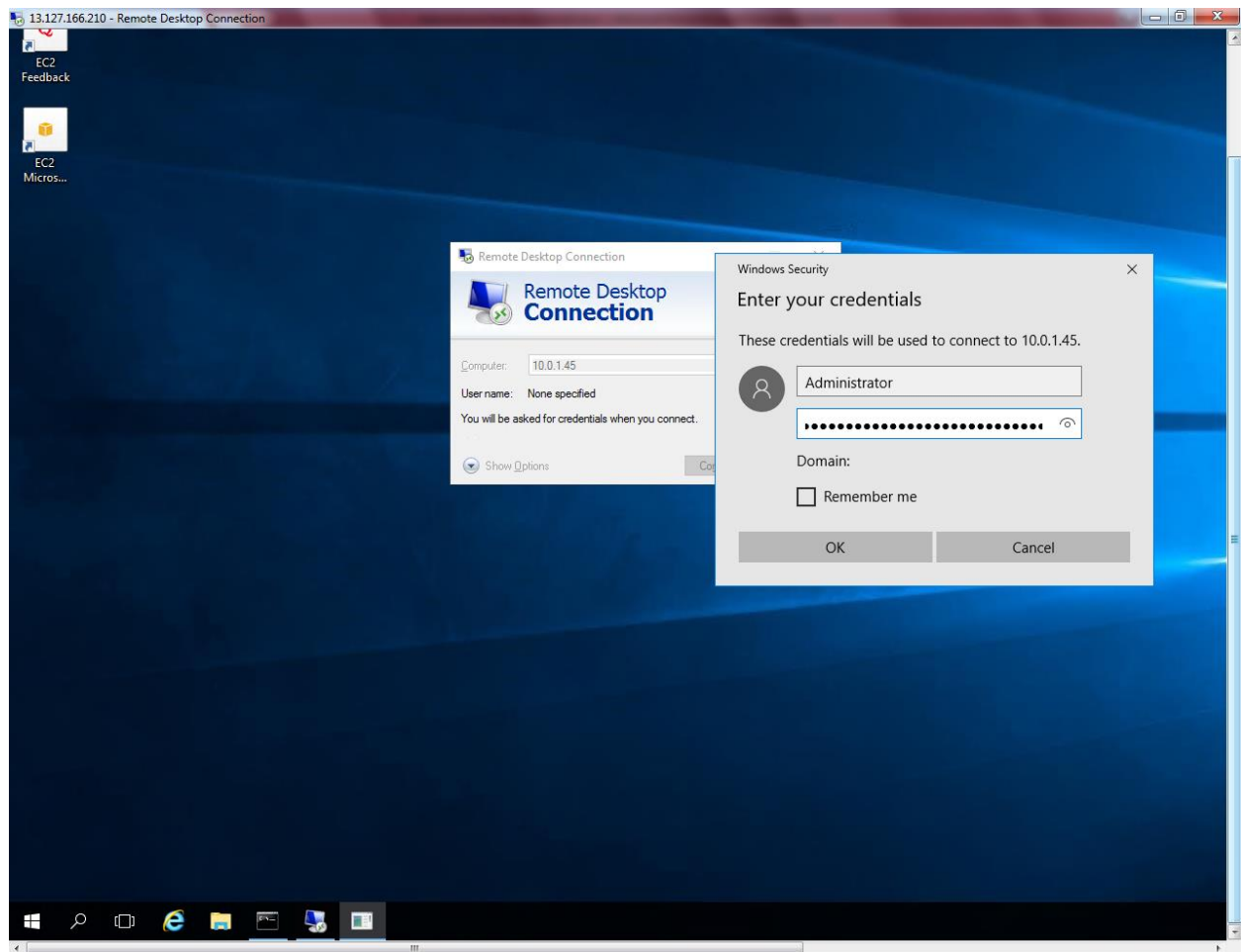
Instance: **i-0f7c9db614ae7e993 (Windows Private Server)** Private IP: 10.0.1.45

The 'Description' tab is active, showing the following details:

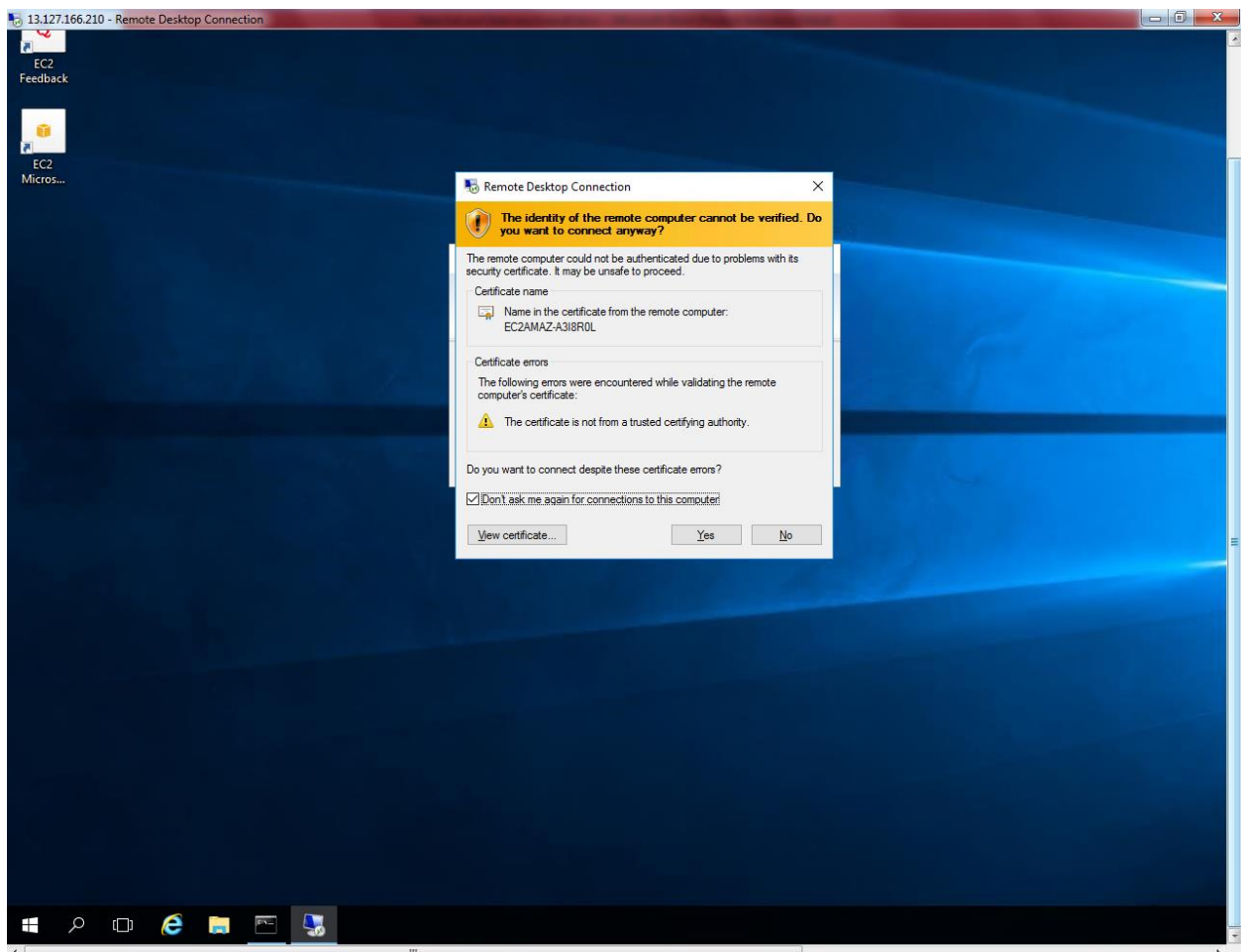
Property	Value
Instance ID	i-0f7c9db614ae7e993
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	ap-south-1a
Security groups	Win Pvt Sec Group, view inbound
Public DNS (IPv4)	-
IPv4 Public IP	-
IPv6 IPs	-
Private DNS	ip-10-0-1-45.ap-south-1.compute.internal
Private IPs	10.0.1.45
Secondary private IPs	

Try to connect private subnet server from public subnet server (10.0.1.45).

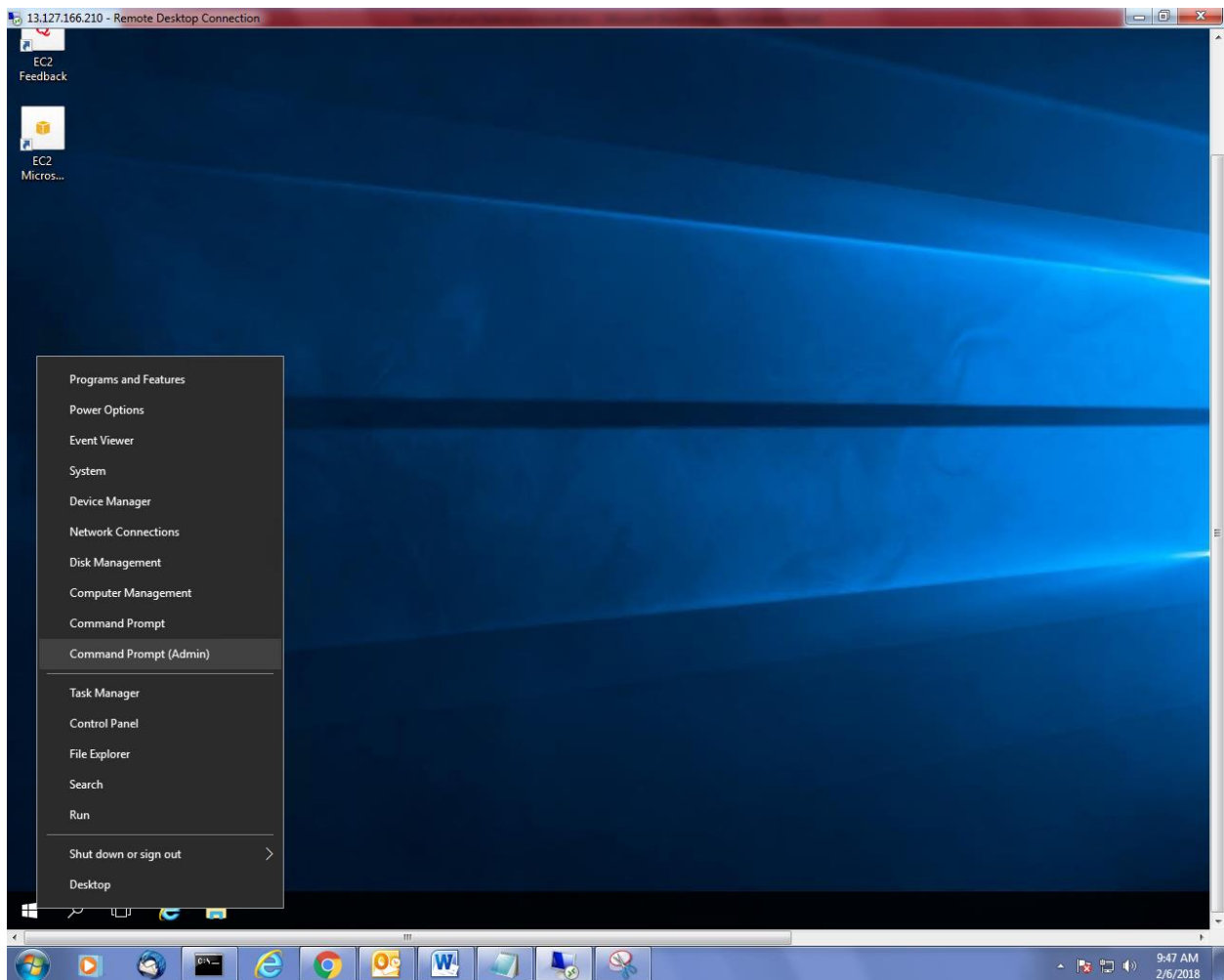




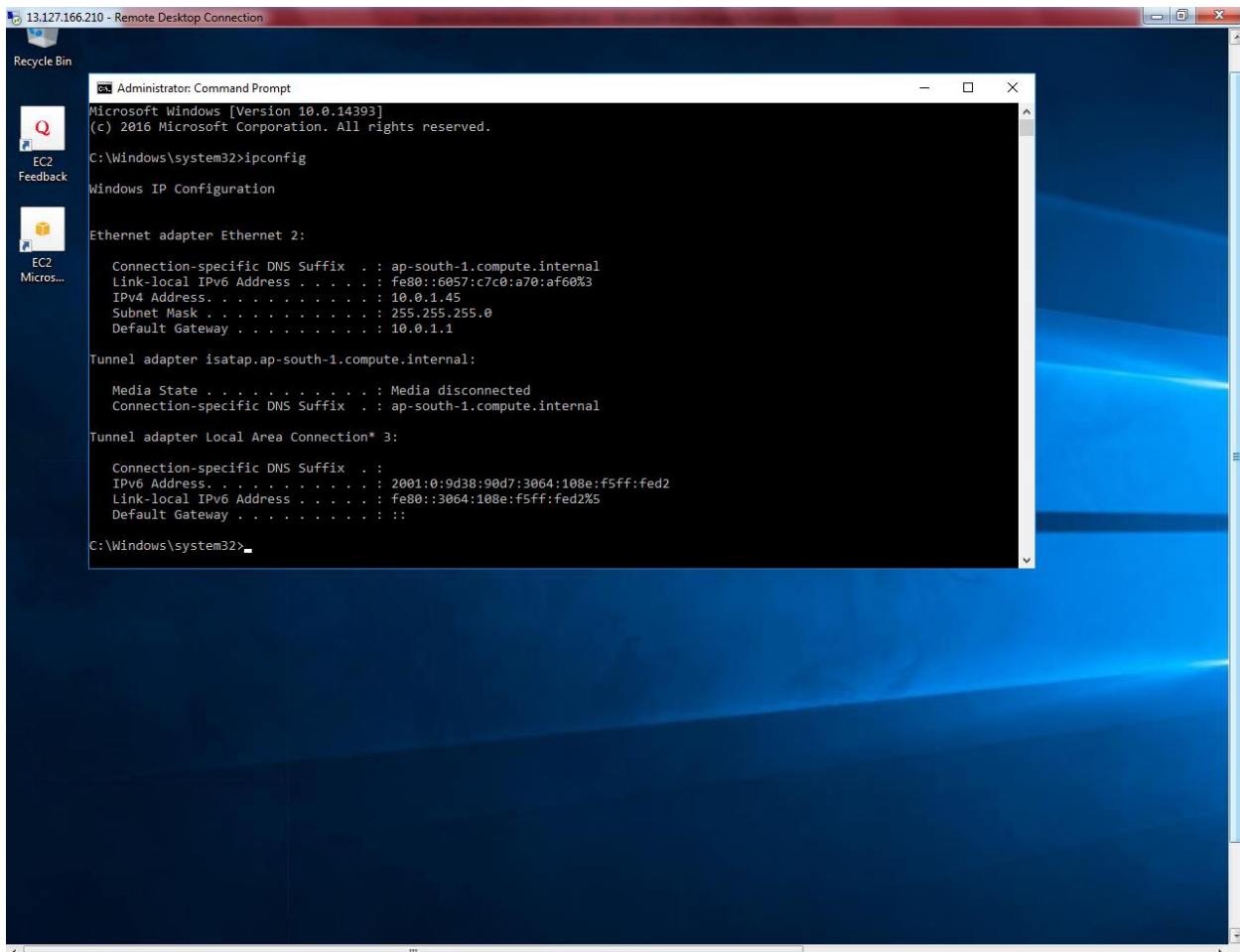
Click “Yes” to continue.



Right click start menu and click “Command prompt (Admin)”



Type ipconfig in Private server.



13.127.166.210 - 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>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : ap-south-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::c7c0:a70:af60%3
    IPv4 Address. . . . . : 10.0.1.45
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.1.1

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

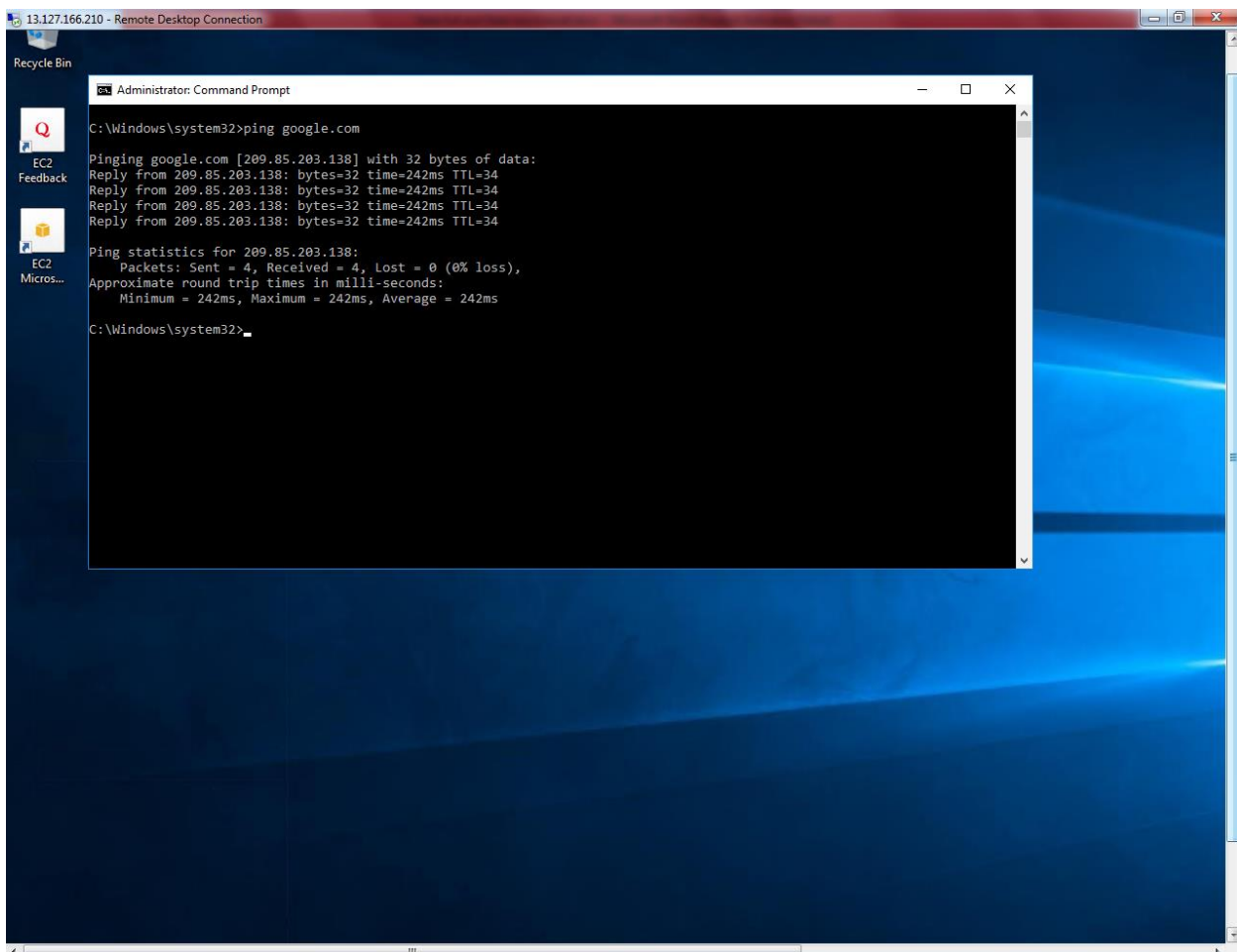
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : ap-south-1.compute.internal

Tunnel adapter Local Area Connection* 3:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:9d38:90d7:3064:108e:f5ff:fed2
    Link-local IPv6 Address . . . . . : fe80::3064:108e:f5ff:fed2%5
    Default Gateway . . . . . : ::
```

C:\Windows\system32>

Type `google.com` in private subnet server. We are able to connect internet from private subnet by using NAT gateway.



13.127.166.210 - Remote Desktop Connection

Recycle Bin

EC2 Feedback

EC2 Micros...

Administrator: Command Prompt

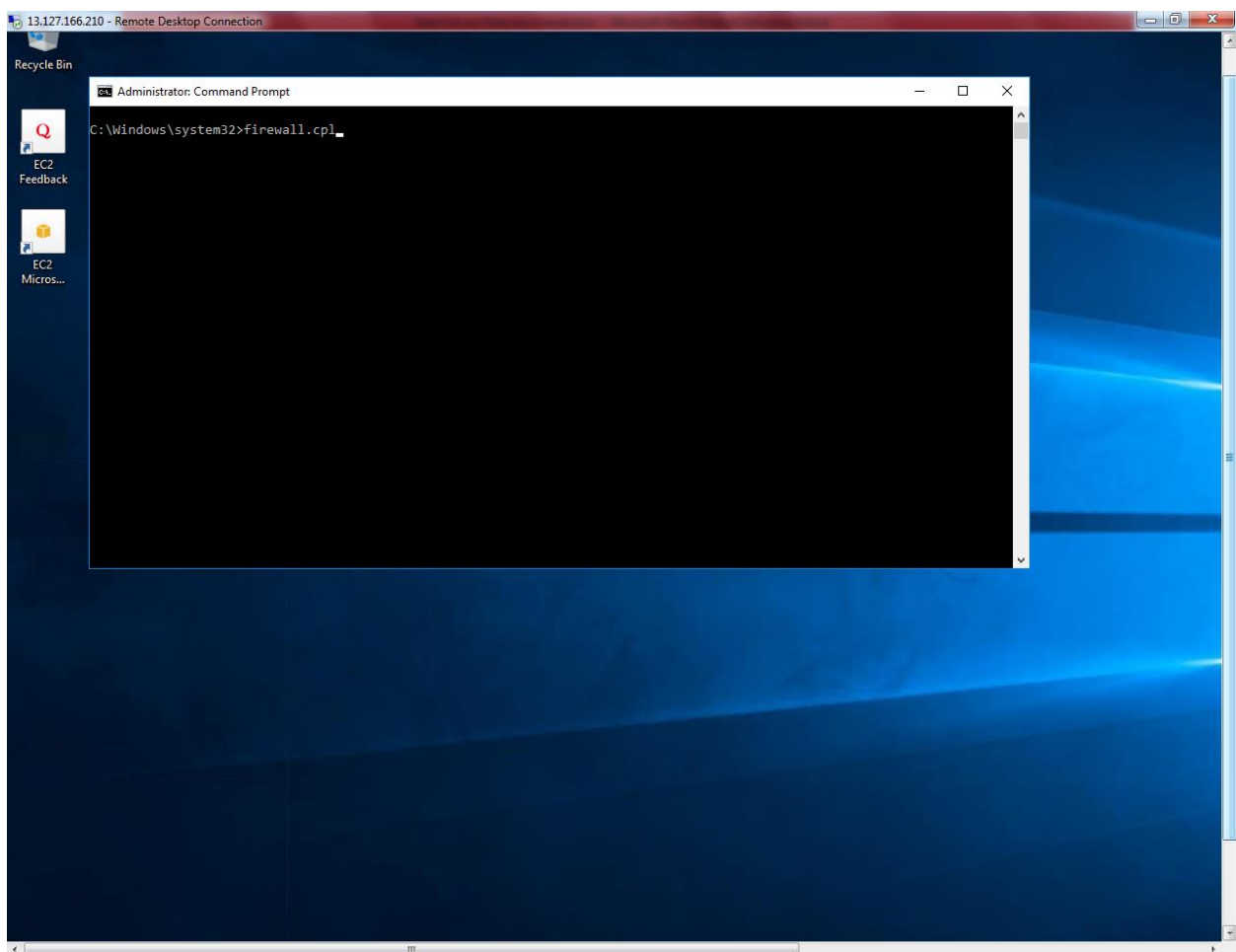
```
C:\Windows\system32>ping google.com

Pinging google.com [209.85.203.138] with 32 bytes of data:
Reply from 209.85.203.138: bytes=32 time=242ms TTL=34
Reply from 209.85.203.138: bytes=32 time=242ms TTL=34
Reply from 209.85.203.138: bytes=32 time=242ms TTL=34
Reply from 209.85.203.138: bytes=32 time=242ms TTL=34

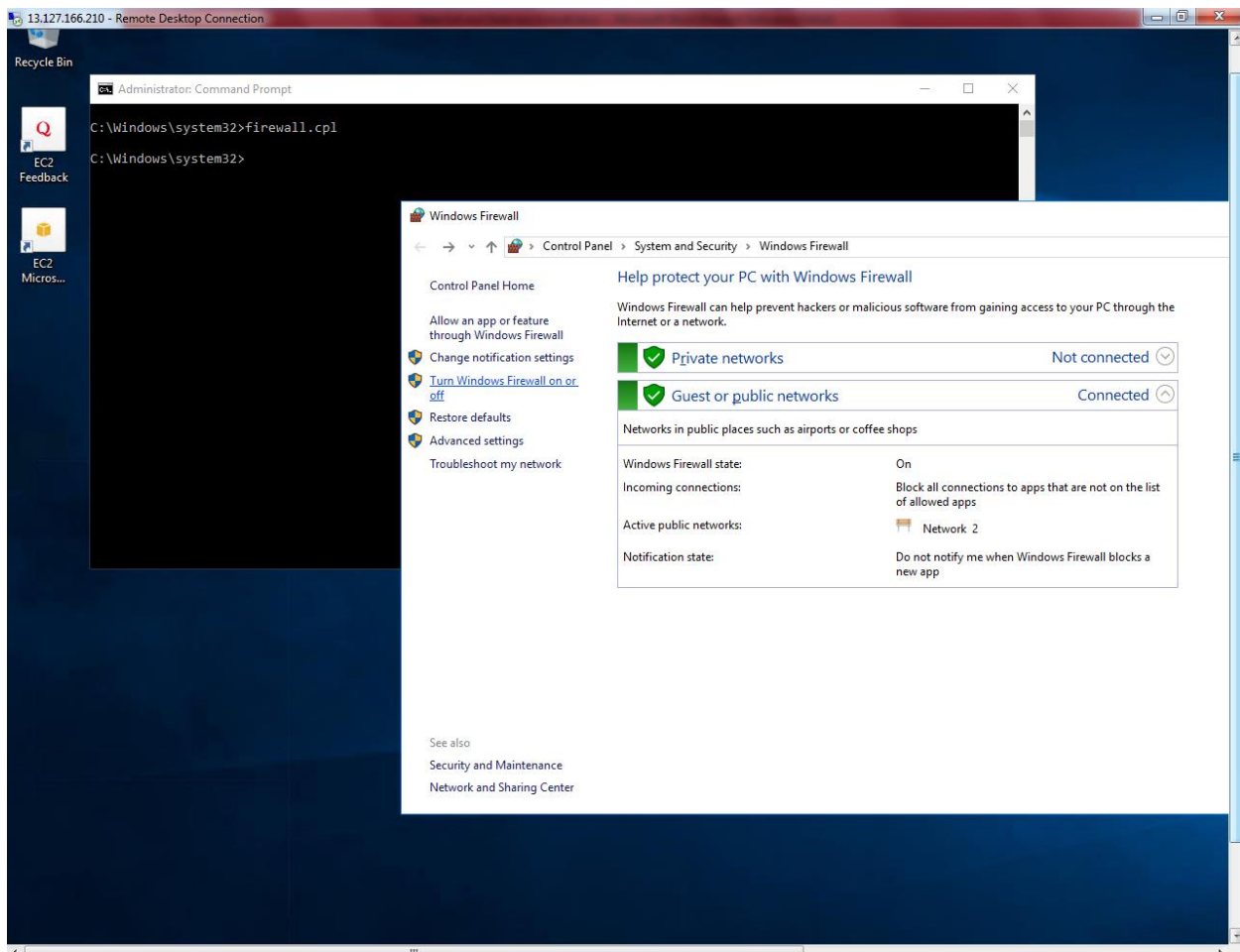
Ping statistics for 209.85.203.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 242ms, Maximum = 242ms, Average = 242ms

C:\Windows\system32>
```

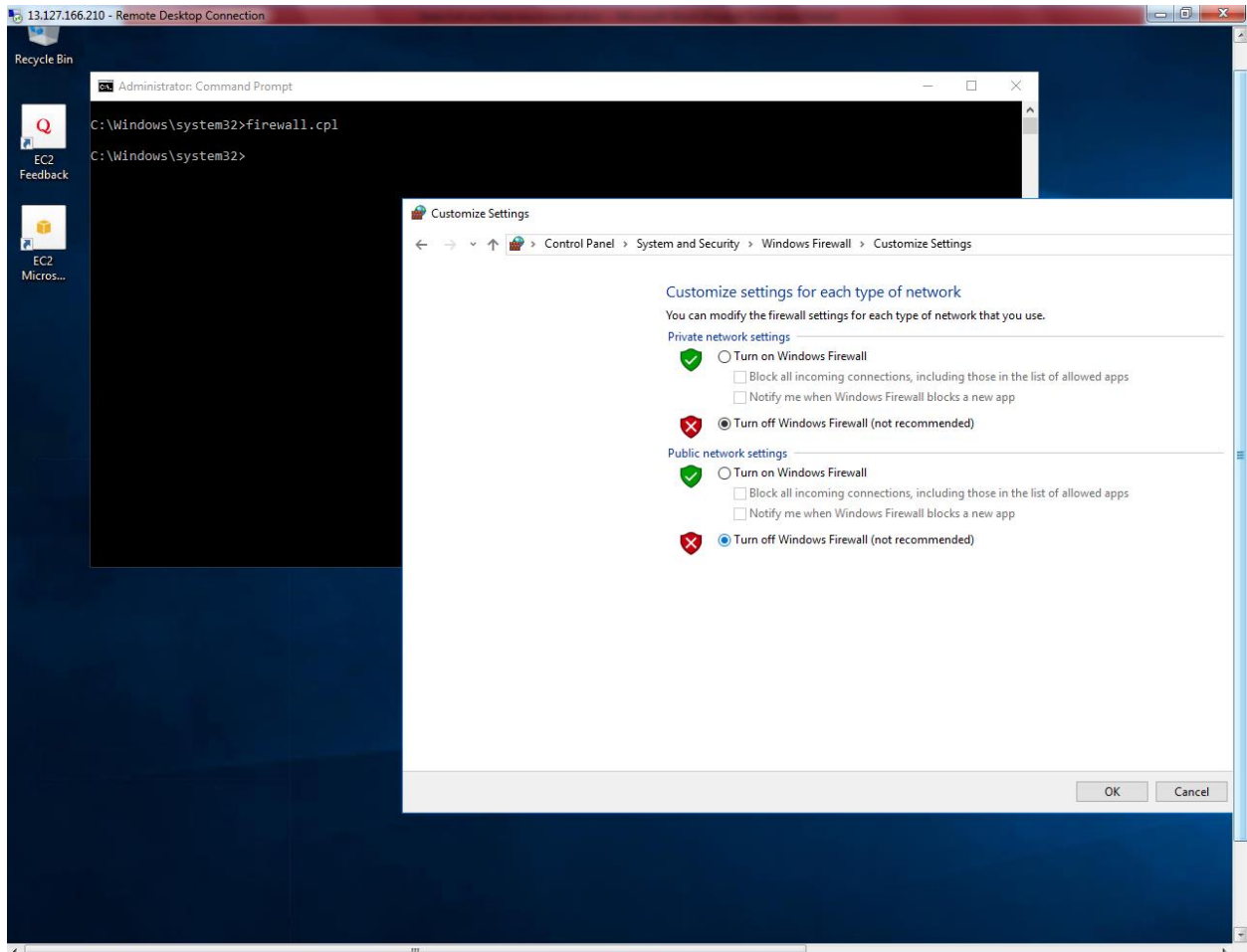
Type Firewall.cpl



Click “Turn Windows Firewall on or Off”.

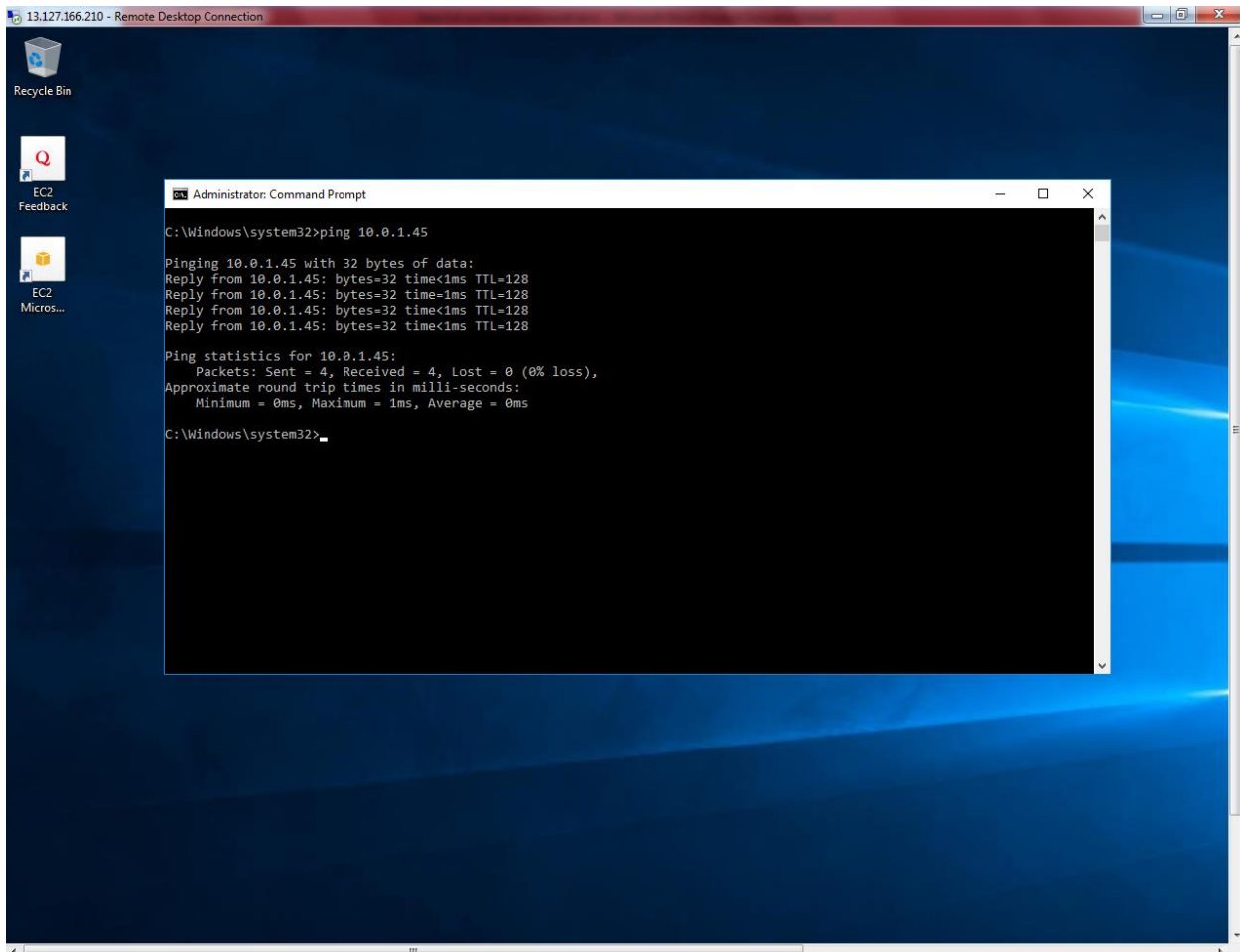


Turn off windows firewall.



Click "Ok".

Now try to ping 10.0.1.45 from Public subnet server. We can able to ping 10.0.1.45 from public subnet server.



13.127.166.210 - Remote Desktop Connection

Recycle Bin

EC2 Feedback

EC2 Micros...

```
C:\Windows\system32>ping 10.0.1.45

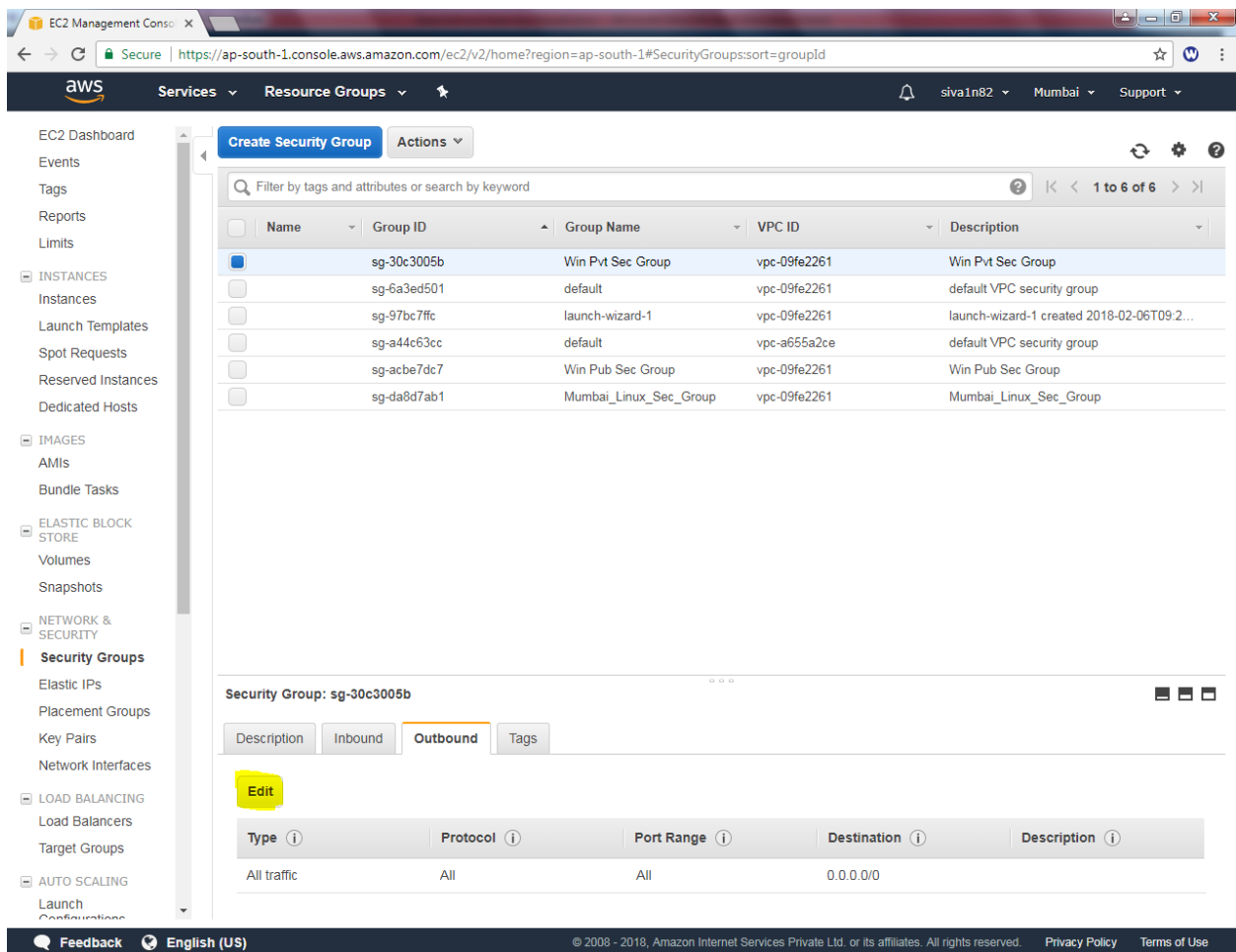
Pinging 10.0.1.45 with 32 bytes of data:
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.1.45:
    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>
```

Now I am going to remove out bound rule from Win Pvt Sub Server security group.

Click “Edit”.



The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and LOAD BALANCING. The 'Security Groups' link under NETWORK & SECURITY is selected. The main content area displays a list of security groups. The first group, 'Win Pvt Sec Group' (sg-30c3005b), is highlighted. Below the list, the details for this group are shown, including tabs for Description, Inbound, Outbound, and Tags. The 'Outbound' tab is active, showing a table with one rule: 'All traffic' to '0.0.0.0/0'. A yellow 'Edit' button is positioned above the table.

Name	Group ID	Group Name	VPC ID	Description
Win Pvt Sec Group	sg-30c3005b	Win Pvt Sec Group	vpc-09fe2261	Win Pvt Sec Group
default	sg-6a3ed501	default	vpc-09fe2261	default VPC security group
launch-wizard-1	sg-97bc7ffc	launch-wizard-1	vpc-09fe2261	launch-wizard-1 created 2018-02-06T09:2...
default	sg-a44c63cc	default	vpc-a655a2ce	default VPC security group
Win Pub Sec Group	sg-acbe7dc7	Win Pub Sec Group	vpc-09fe2261	Win Pub Sec Group
Mumbai_Linux_Sec_Group	sg-da8d7ab1	Mumbai_Linux_Sec_Group	vpc-09fe2261	Mumbai_Linux_Sec_Group

Type	Protocol	Port Range	Destination	Description
All traffic	All	All	0.0.0.0/0	

Click “X” mark to remove.

Edit outbound rules ✕

Type i	Protocol i	Port Range i	Destination i	Description i
All traffic ▼	All	0 - 65535	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

Edit outbound rules ✕

Type i	Protocol i	Port Range i	Destination i	Description i
This security group has no rules				

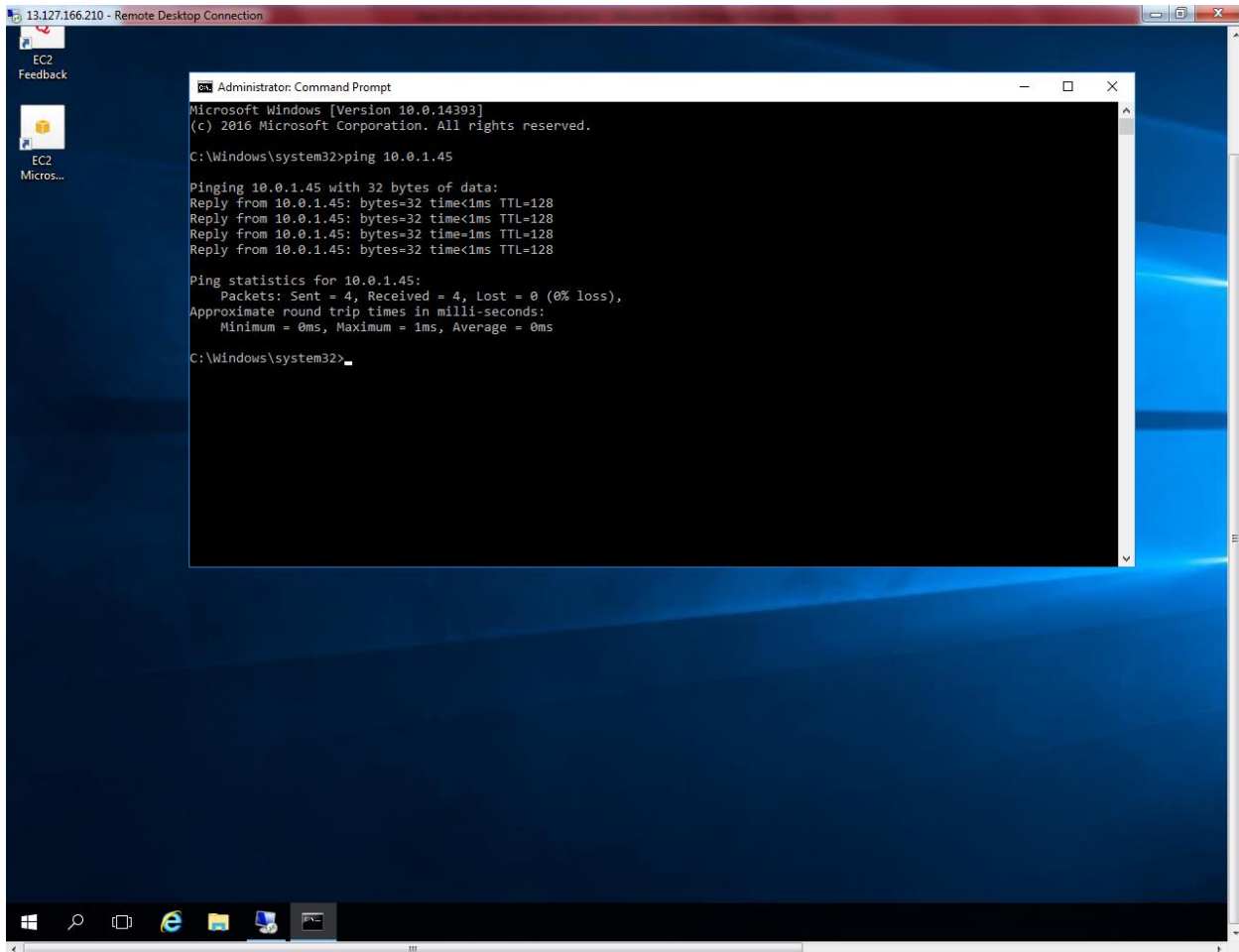
Add Rule

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

Click Save.

Now we are able ping 10.0.1.45 because security group is stateful firewall. While we permit ICMP rule in inbound that will allow the same traffic / ICMP in outbound also. It does not require any permission in outbound rule. Hence, we can able to ping 10.0.1.45 from public subnet.



```
13.127.166.210 - Remote Desktop Connection
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.0.1.45

Pinging 10.0.1.45 with 32 bytes of data:
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128
Reply from 10.0.1.45: bytes=32 time<1ms TTL=128

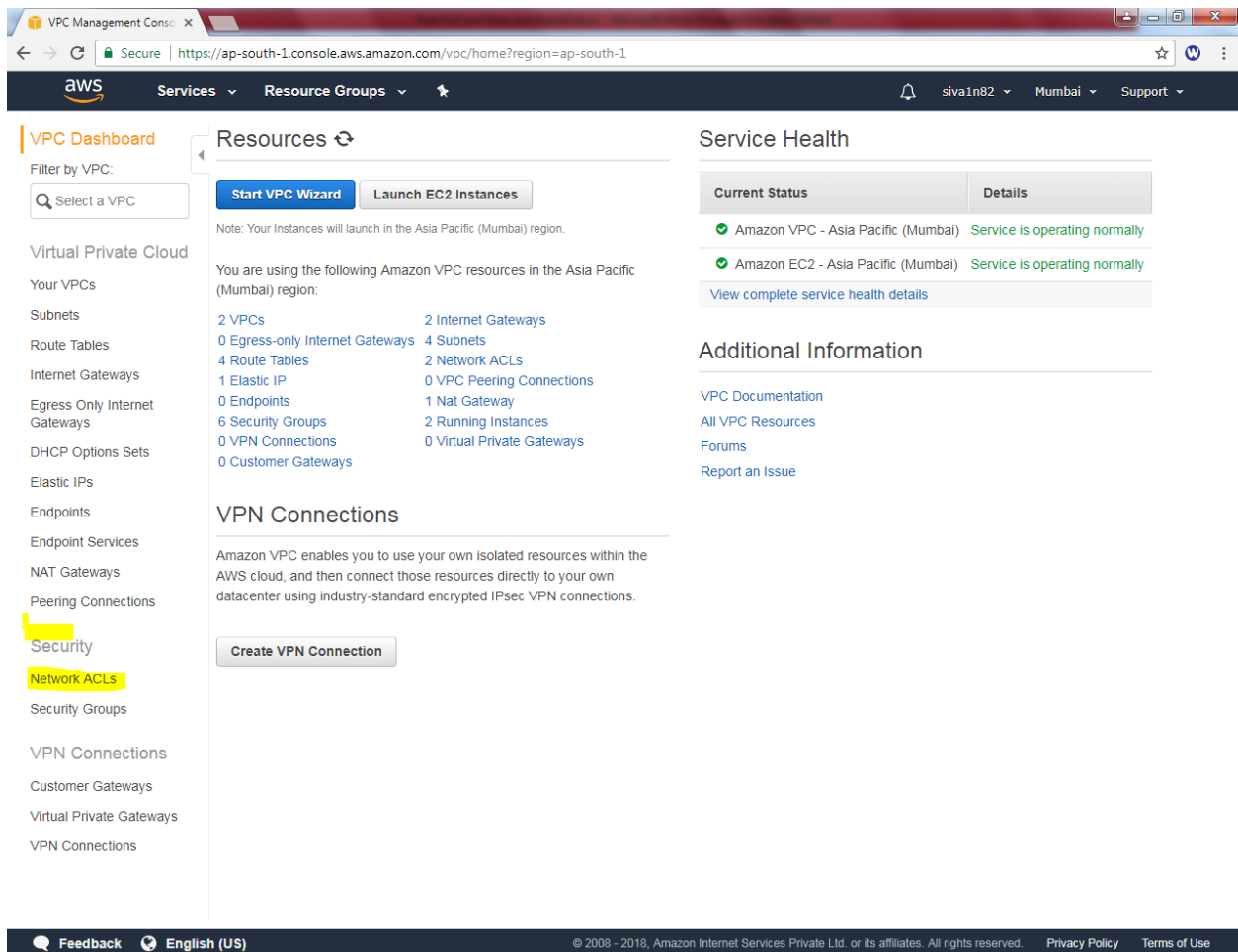
Ping statistics for 10.0.1.45:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>
```

Then restore the outbound rule as default.

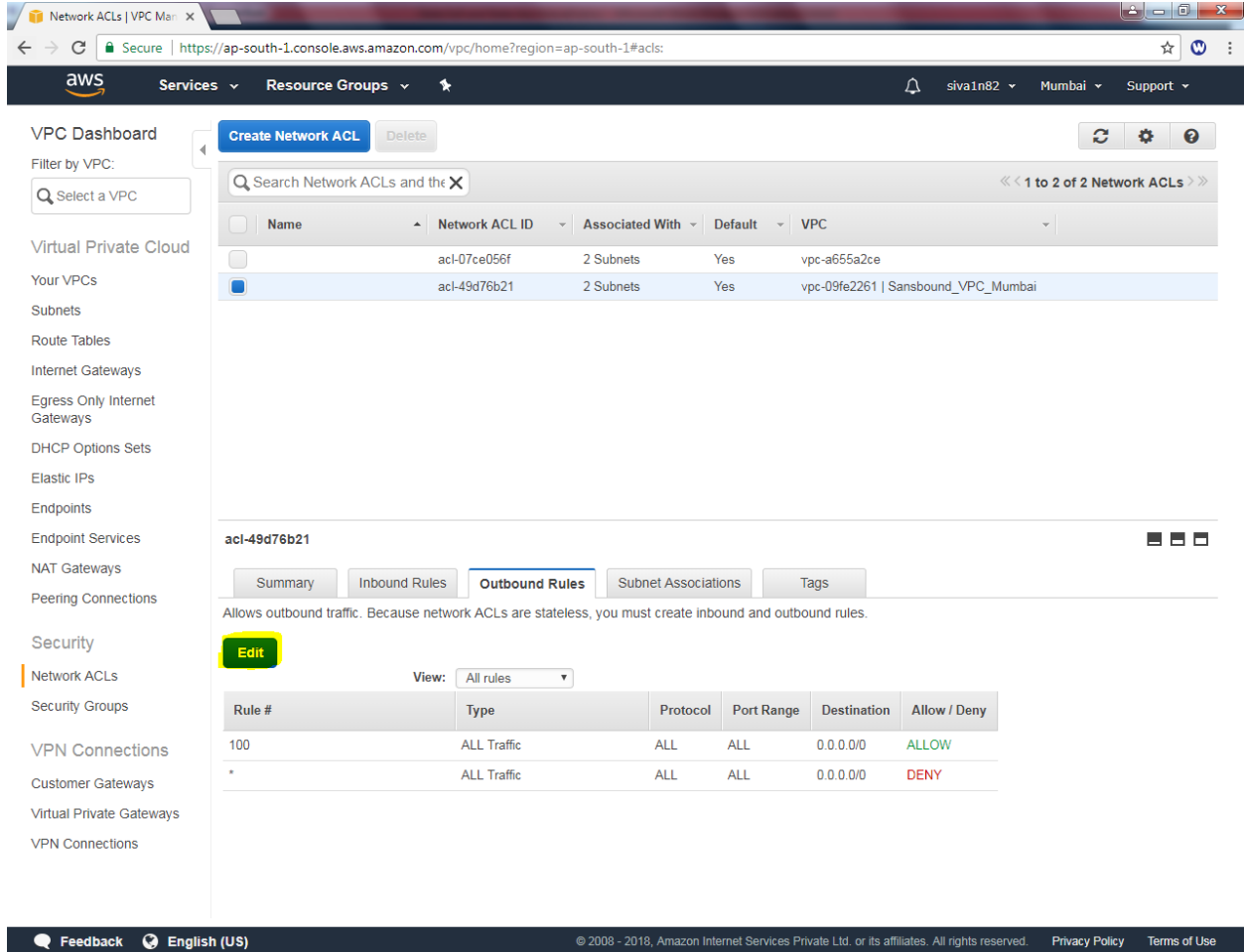
b) Stateless Firewall

Goto “VPC” click Network ACLs.



The screenshot shows the AWS VPC Management Console interface. The left sidebar contains a navigation menu with the following items: 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 (highlighted in yellow), Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays the 'Resources' section for the selected VPC, showing a list of resources in the Asia Pacific (Mumbai) region: 2 VPCs, 0 Egress-only Internet Gateways, 4 Route Tables, 1 Elastic IP, 0 Endpoints, 6 Security Groups, 0 VPN Connections, 0 Customer Gateways, 2 Internet Gateways, 4 Subnets, 2 Network ACLs, 0 VPC Peering Connections, 1 Nat Gateway, 2 Running Instances, and 0 Virtual Private Gateways. The 'Service Health' section on the right shows that both Amazon VPC and Amazon EC2 are operating normally. The 'Additional Information' section provides links to VPC Documentation, All VPC Resources, Forums, and Report an Issue. The footer contains a Feedback button, English (US) language selector, and copyright information for Amazon Internet Services Private Ltd.

Click “Edit”.



The screenshot shows the AWS Management Console interface for Network ACLs. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and Security. The main content area displays a list of Network ACLs. The selected ACL, 'acl-49d76b21', is shown in detail, including its 'Outbound Rules' tab. The 'Edit' button is highlighted in yellow.

Network ACLs List:

Name	Network ACL ID	Associated With	Default	VPC
	acl-07ce056f	2 Subnets	Yes	vpc-a655a2ce
	acl-49d76b21	2 Subnets	Yes	vpc-09fe2261 Sansbound_VPC_Mumbai

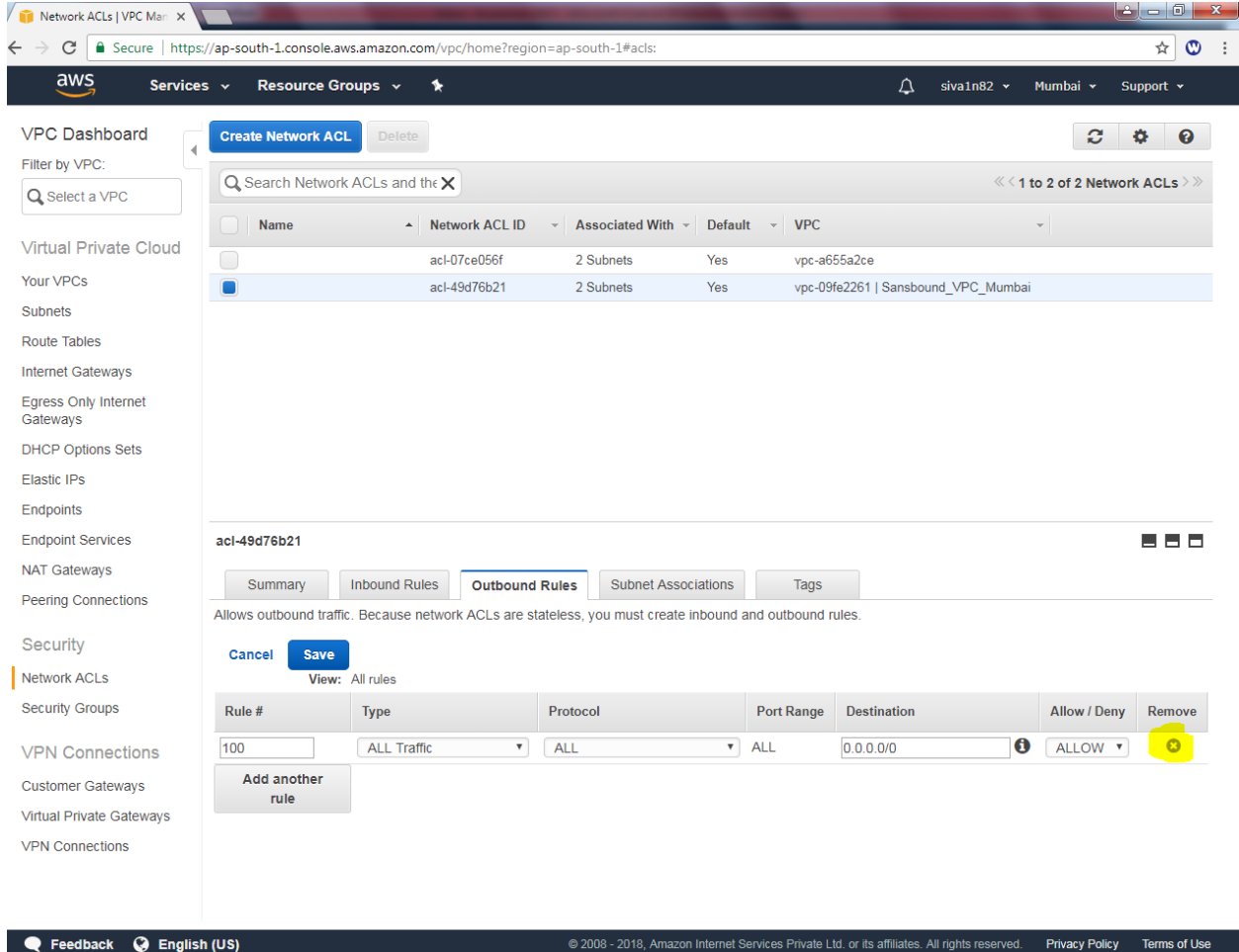
ACL Details: acl-49d76b21

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Outbound Rules:

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Click “highlighted area” to remove ACL.



Network ACLs | VPC Main

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

aws Services Resource Groups

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 Network ACL Delete

Search Network ACLs and the X

<< 1 to 2 of 2 Network ACLs >>

	Name	Network ACL ID	Associated With	Default	VPC
<input type="checkbox"/>		acl-07ce056f	2 Subnets	Yes	vpc-a655a2ce
<input checked="" type="checkbox"/>		acl-49d76b21	2 Subnets	Yes	vpc-09fe2261 Sansbound_VPC_Mumbai


acl-49d76b21

Summary Inbound Rules Outbound Rules Subnet Associations Tags

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Cancel Save

View: All rules

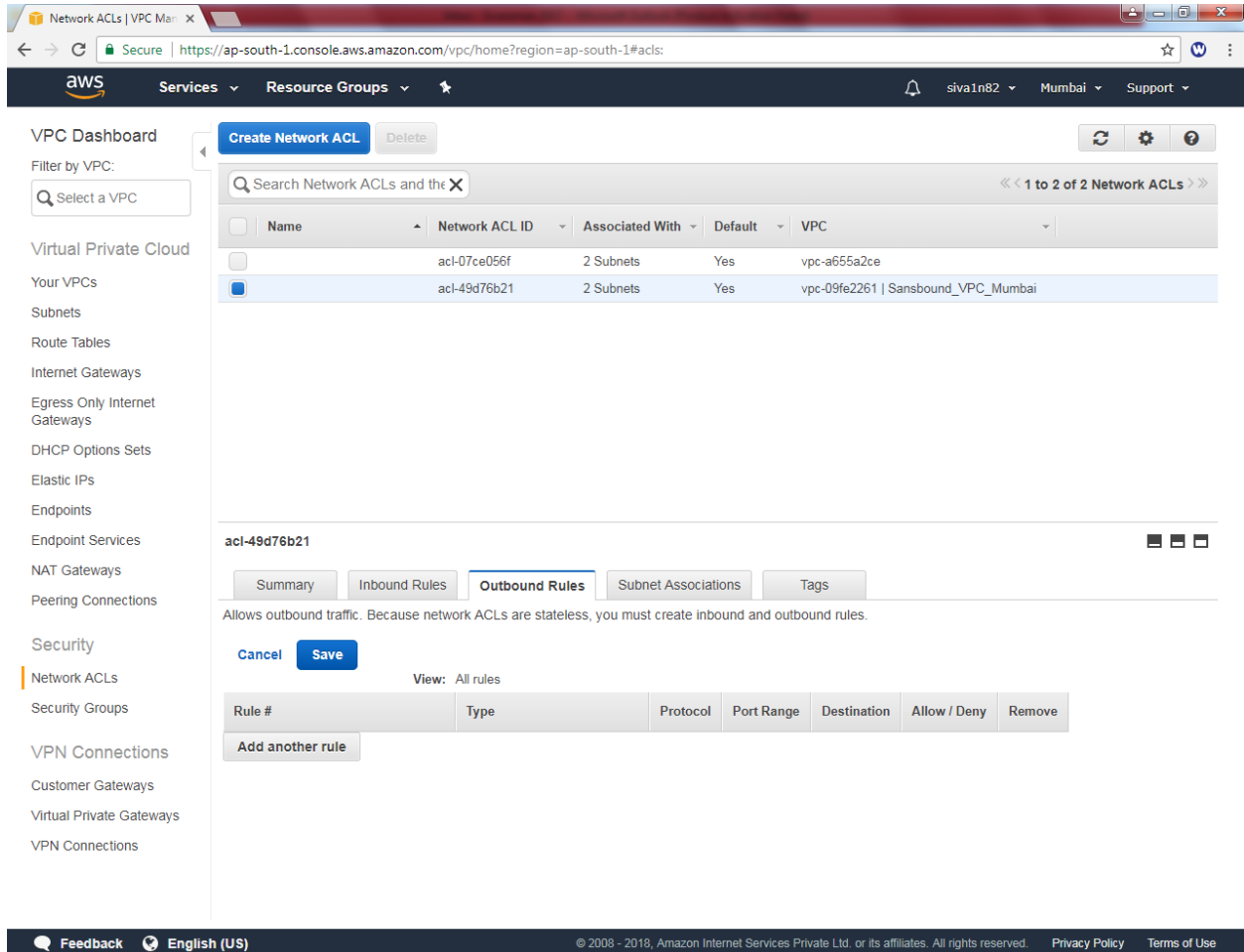
Rule #	Type	Protocol	Port Range	Destination	Allow / Deny	Remove
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW	

Add another rule

Feedback English (US)

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

Click “save”.



Network ACLs | VPC Manager

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 Network ACL Delete

Search Network ACLs and the X

<< 1 to 2 of 2 Network ACLs >>

Name	Network ACL ID	Associated With	Default	VPC
	acl-07ce056f	2 Subnets	Yes	vpc-a655a2ce
	acl-49d76b21	2 Subnets	Yes	vpc-09fe2261 Sansbound_VPC_Mumbai

acl-49d76b21

Summary Inbound Rules **Outbound Rules** Subnet Associations Tags

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Cancel Save

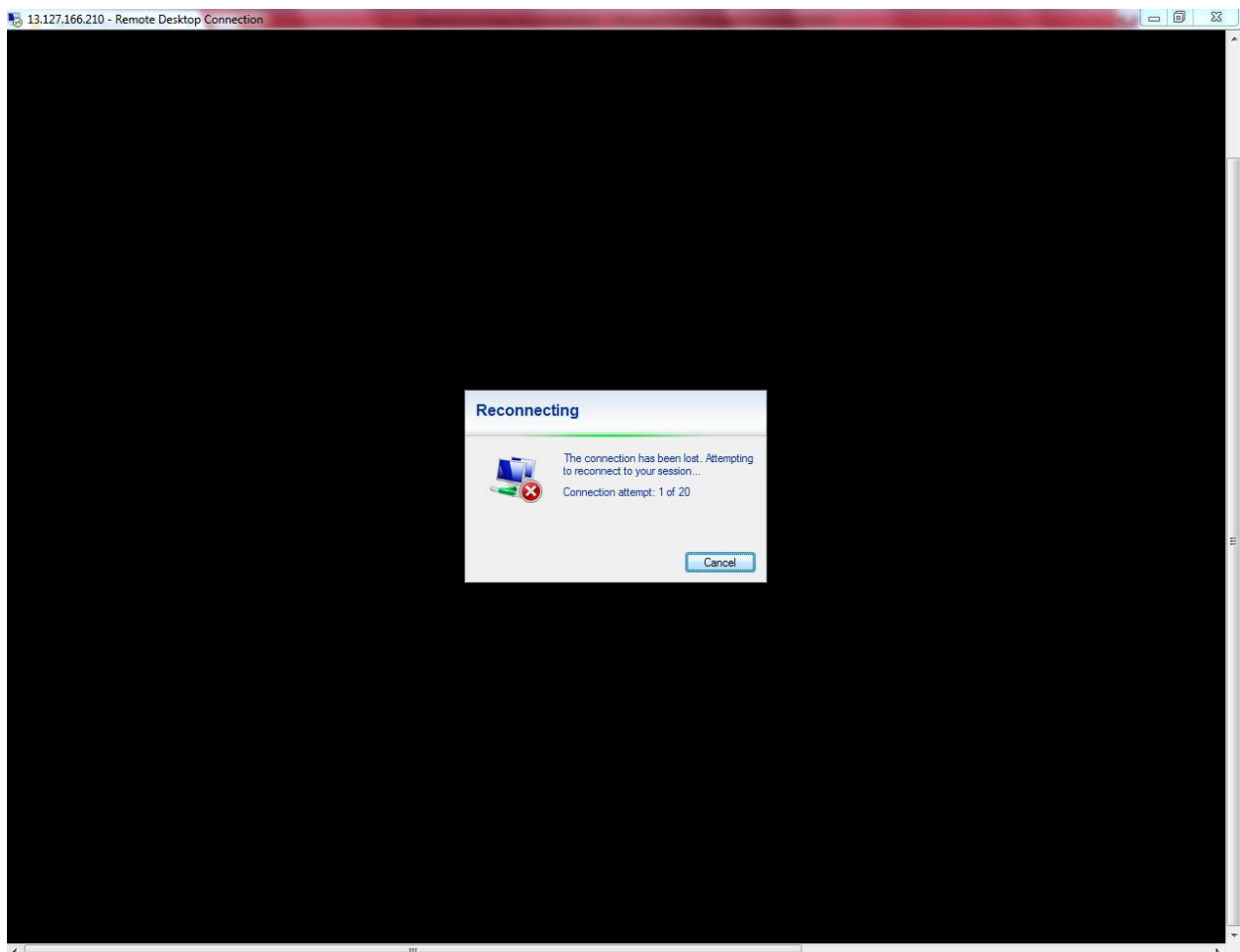
View: All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny	Remove
Add another rule						

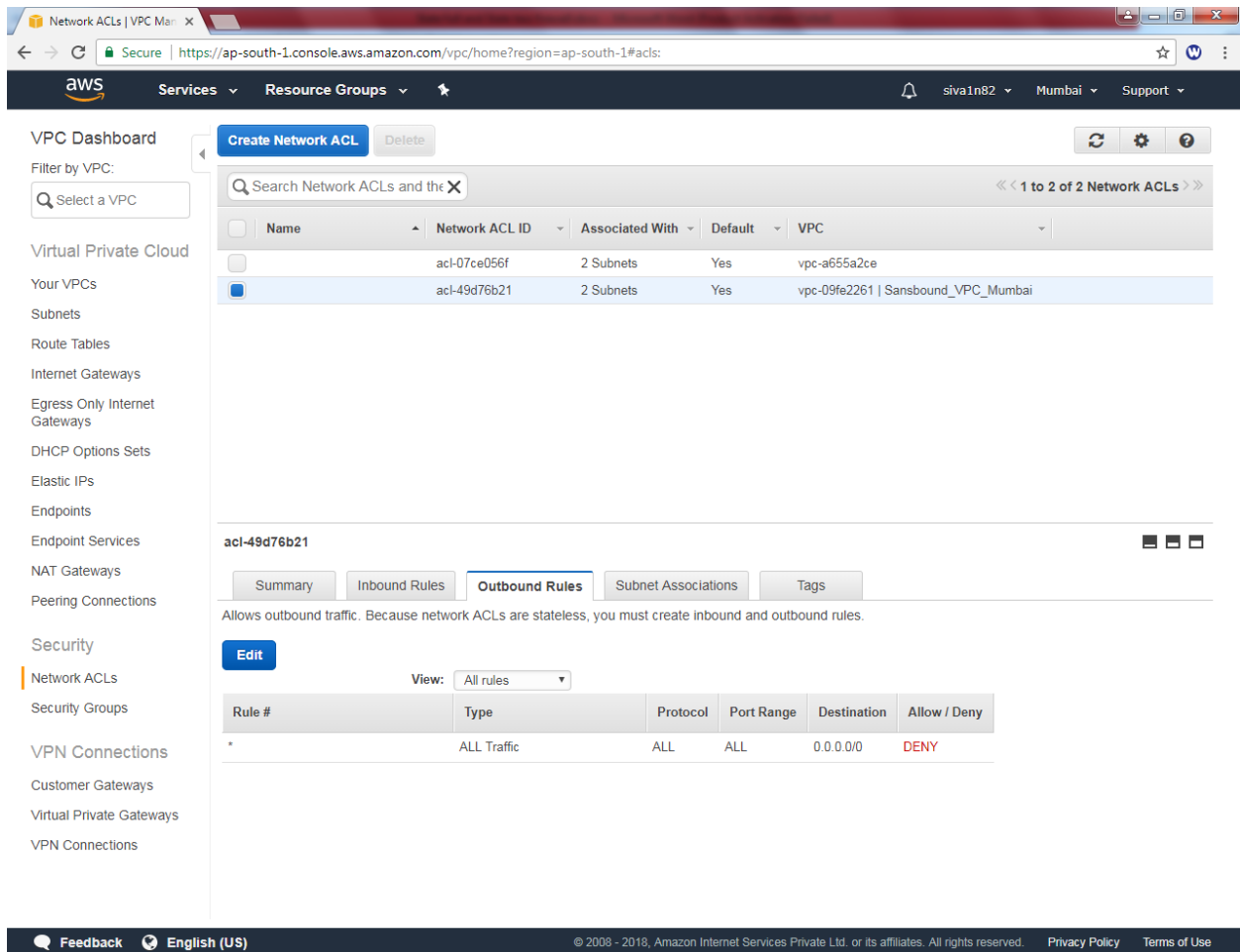
Feedback English (US)

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

My remote desktop connection on public server has been disconnected. Because Network ACL was stateless firewall. We have permitted RDP (3389) TCP port in inbound rule. But, we have removed All traffic from outbound rule. Hence our remote connection has been removed. We need to provide outbound rule with all traffic as allow.



We could not able able to remove * rule / deny from Network ACL.



Network ACLs | VPC Main

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

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 Network ACL Delete

Search Network ACLs and the X << 1 to 2 of 2 Network ACLs >>

Name	Network ACL ID	Associated With	Default	VPC
	acl-07ce056f	2 Subnets	Yes	vpc-a655a2ce
	acl-49d76b21	2 Subnets	Yes	vpc-09fe2261 Sansbound_VPC_Mumbai

acl-49d76b21

Summary Inbound Rules **Outbound Rules** Subnet Associations Tags

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

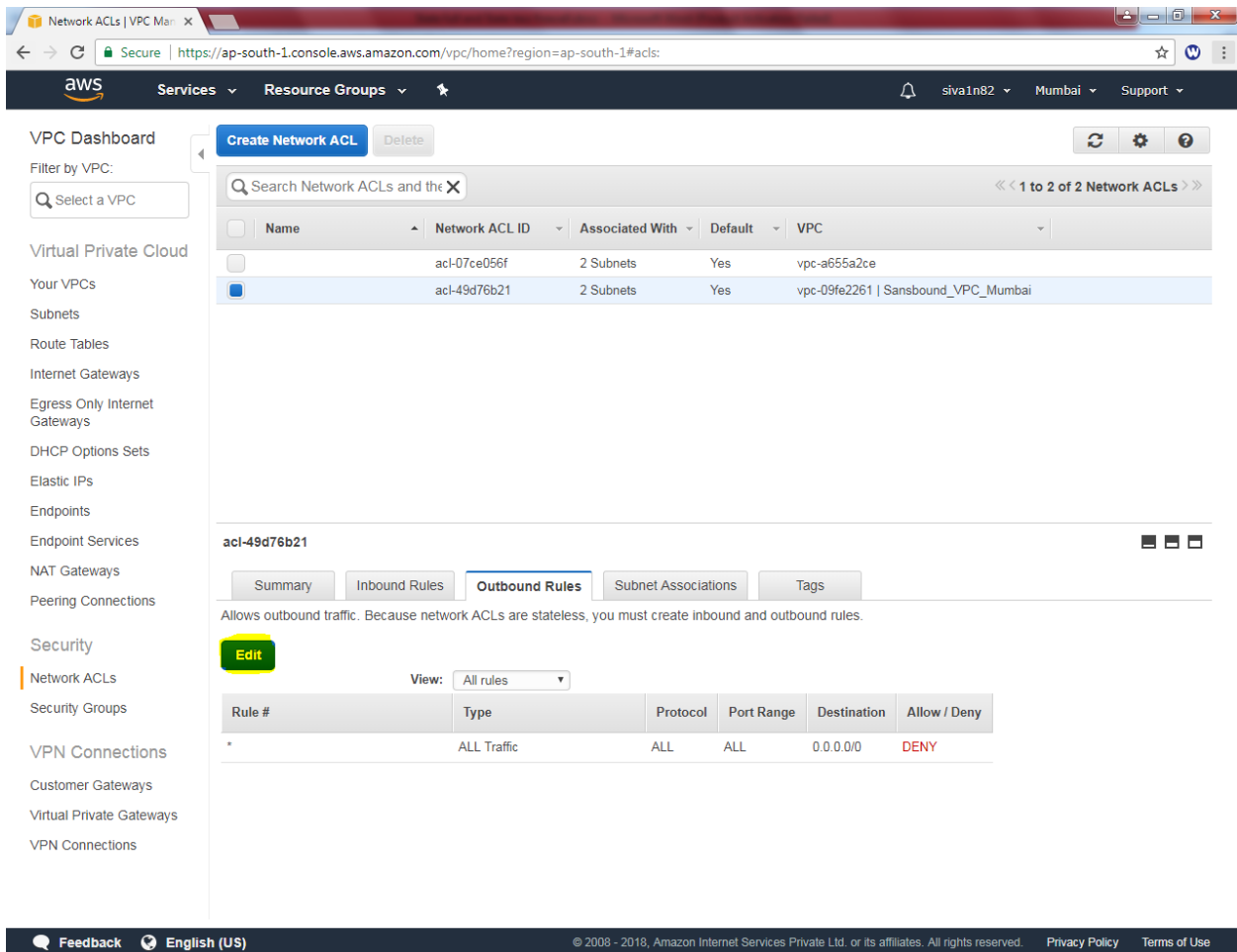
Edit

View: All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

Click “Edit”.



The screenshot shows the AWS Management Console interface for Network ACLs. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and Security. The main content area displays a list of Network ACLs. The selected ACL, 'acl-49d76b21', is shown in detail, including its rules. The 'Edit' button is highlighted in yellow.

Network ACLs List:

Name	Network ACL ID	Associated With	Default	VPC
	acl-07ce056f	2 Subnets	Yes	vpc-a655a2ce
	acl-49d76b21	2 Subnets	Yes	vpc-09fe2261 Sansbound_VPC_Mumbai

ACL Details: acl-49d76b21

Summary | Inbound Rules | **Outbound Rules** | Subnet Associations | Tags

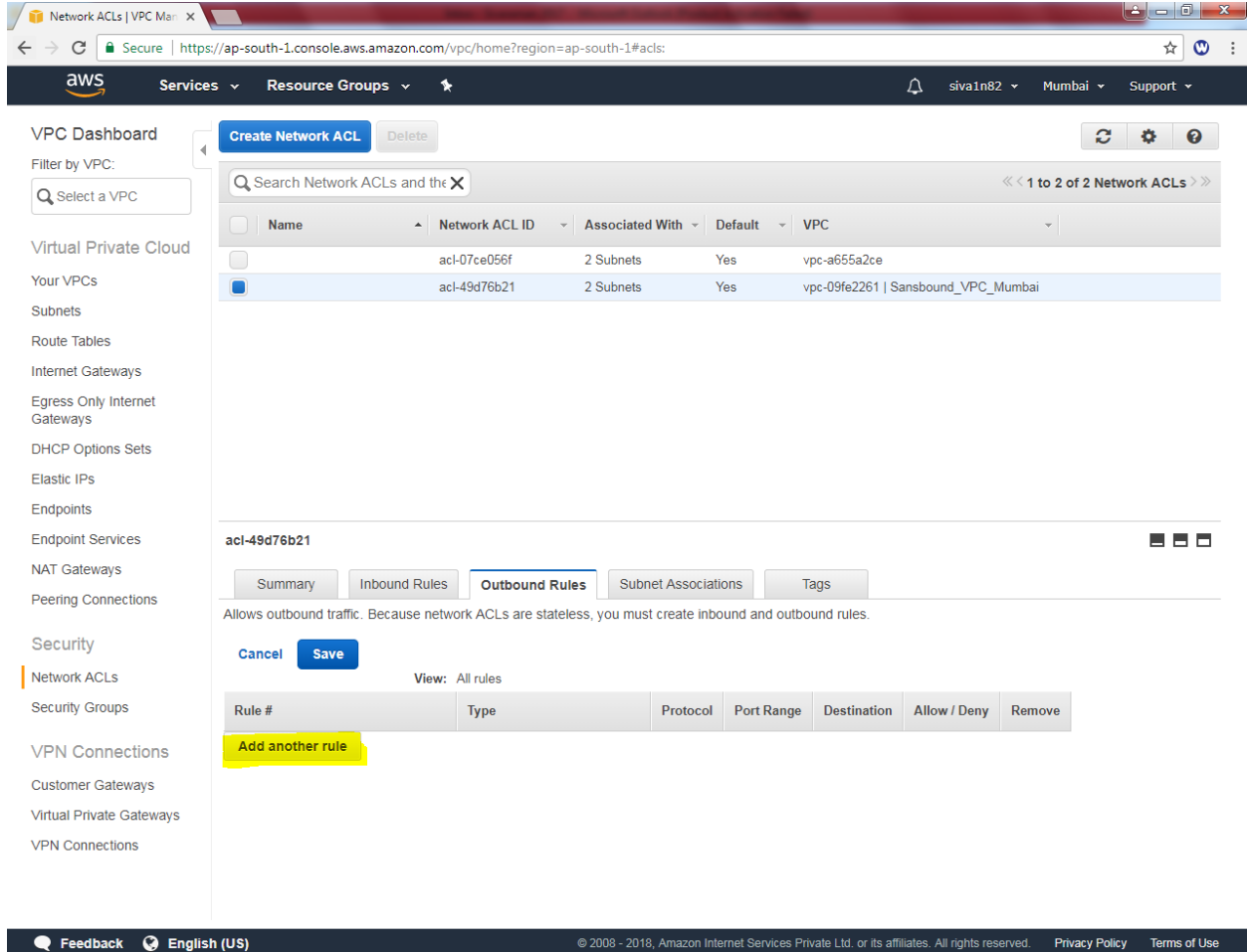
Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Click “Add another rule”.



The screenshot shows the AWS Management Console interface for configuring a Network ACL. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Security, Network ACLs, and VPN Connections. The main content area displays a list of Network ACLs, with the selected ACL (acl-49d76b21) shown in detail. The 'Outbound Rules' tab is active, and the 'Add another rule' button is highlighted in yellow.

Network ACLs List:

Name	Network ACL ID	Associated With	Default	VPC
	acl-07ce056f	2 Subnets	Yes	vpc-a655a2ce
	acl-49d76b21	2 Subnets	Yes	vpc-09fe2261 Sansbound_VPC_Mumbai

ACL Details: acl-49d76b21

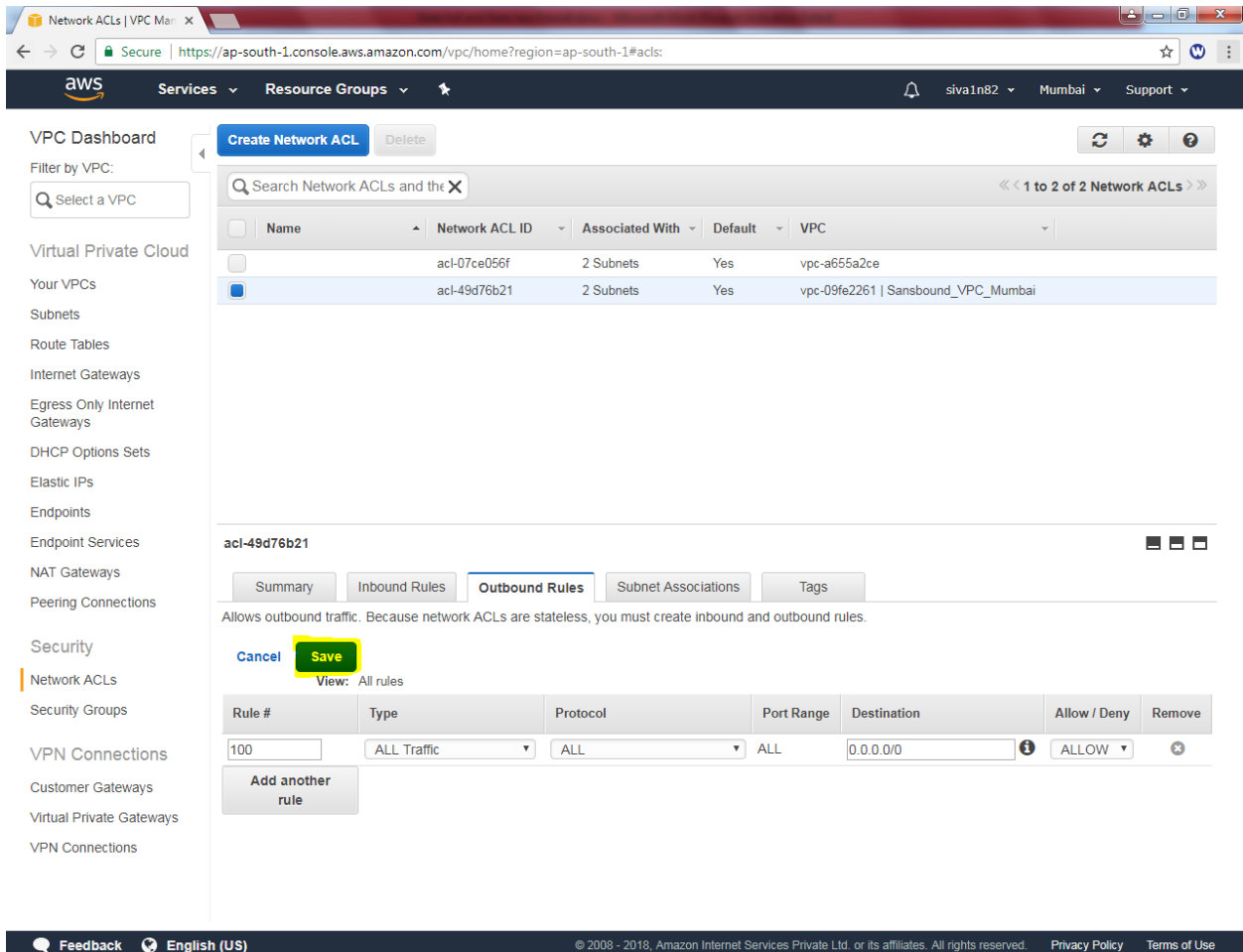
Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Outbound Rules Tab:

View: All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny	Remove
Add another rule						

Type ACL rule as : “100” Select type as “All traffic” destination as 0.0.0.0/0 and allow/ deny as allow.



The screenshot shows the AWS Management Console interface for configuring a Network ACL rule. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and Security. The main content area displays a list of Network ACLs, with the selected rule 'acl-49d76b21' shown in detail. The rule is configured with the following settings:

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny	Remove
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW	X

The rule is currently set to 'ALLOW' and is associated with the VPC 'vpc-09fe2261 | Sansbound_VPC_Mumbai'. The 'Outbound Rules' tab is selected, and the 'Save' button is highlighted in yellow.

Now we can able to get RDP for public server.

