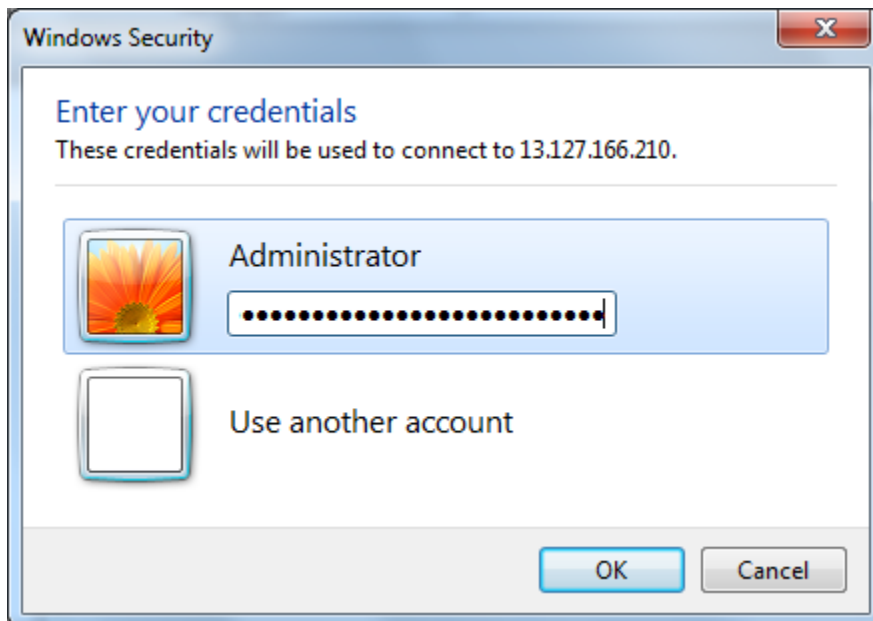
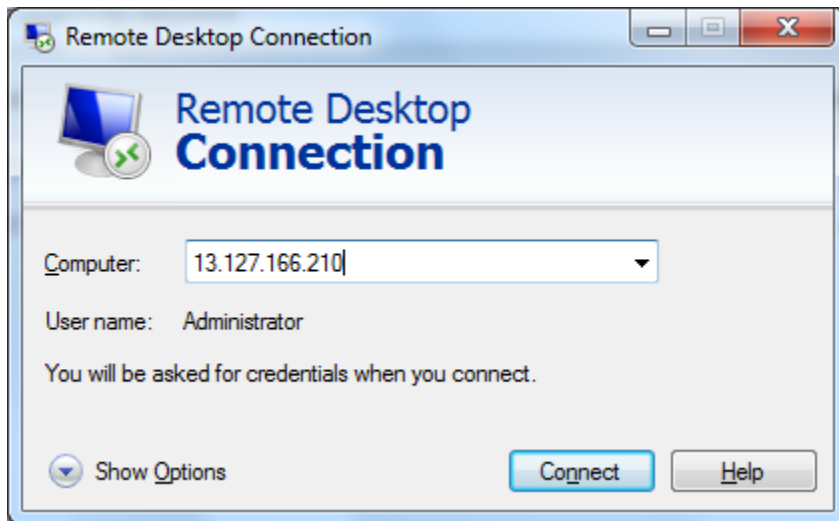


Stateful and Stateless firewall

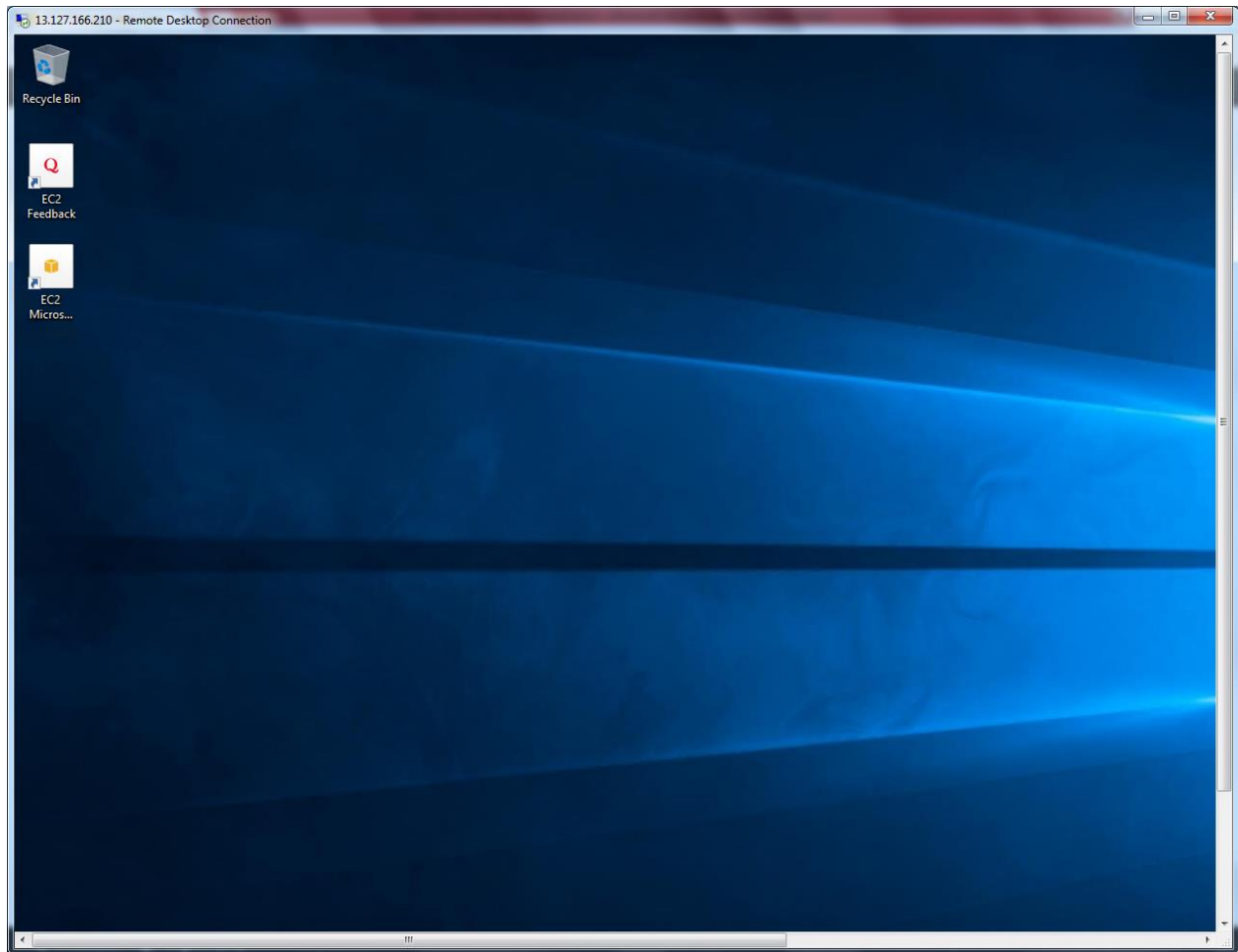
Note: Before Start this scenario, you must be configured VPC, Internet gateway and Nat gateway in your AWS Console. Then only it will work.

a) Stateful firewall

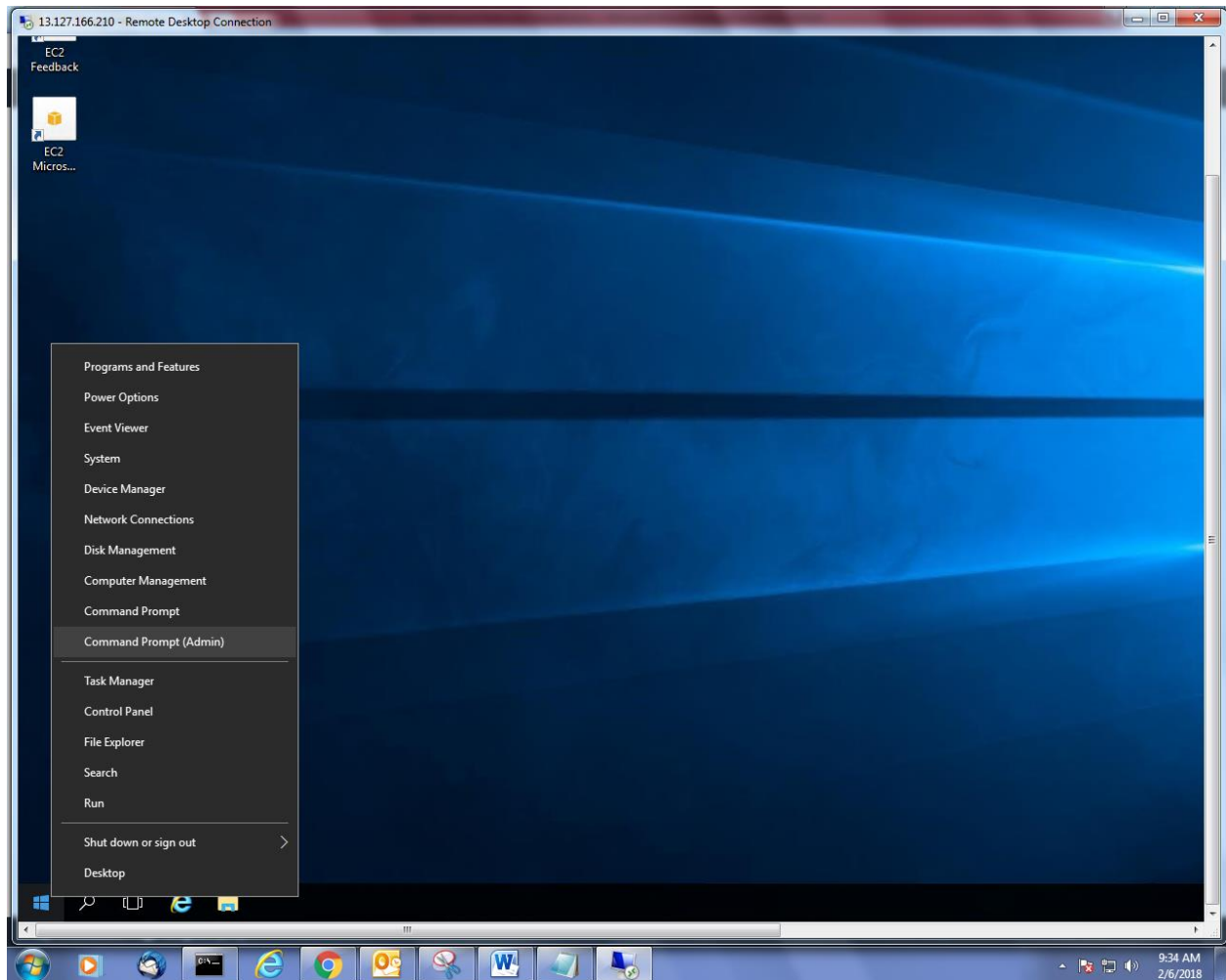
Type the public server IP in mstsc



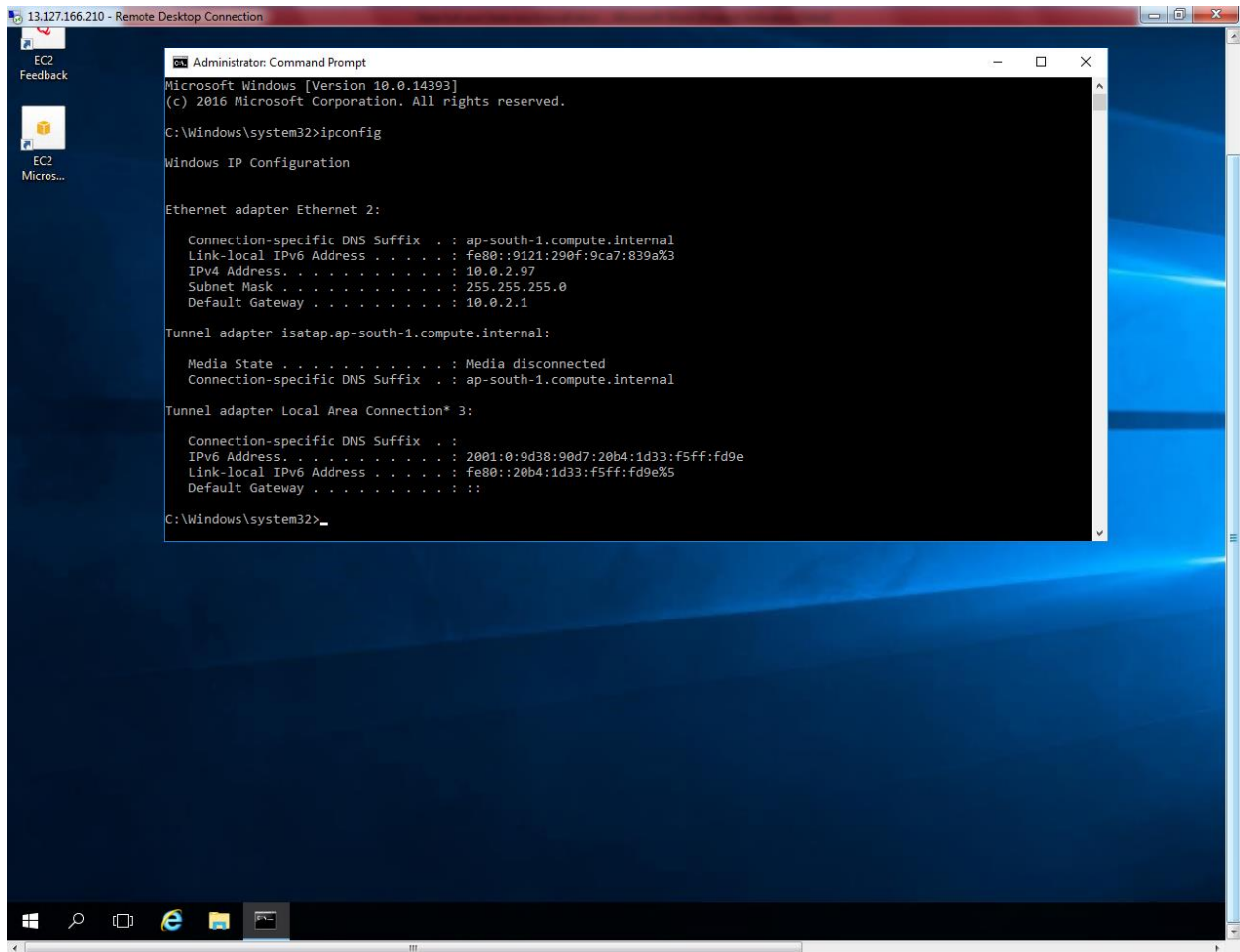
Logged into the Public Server successfully.



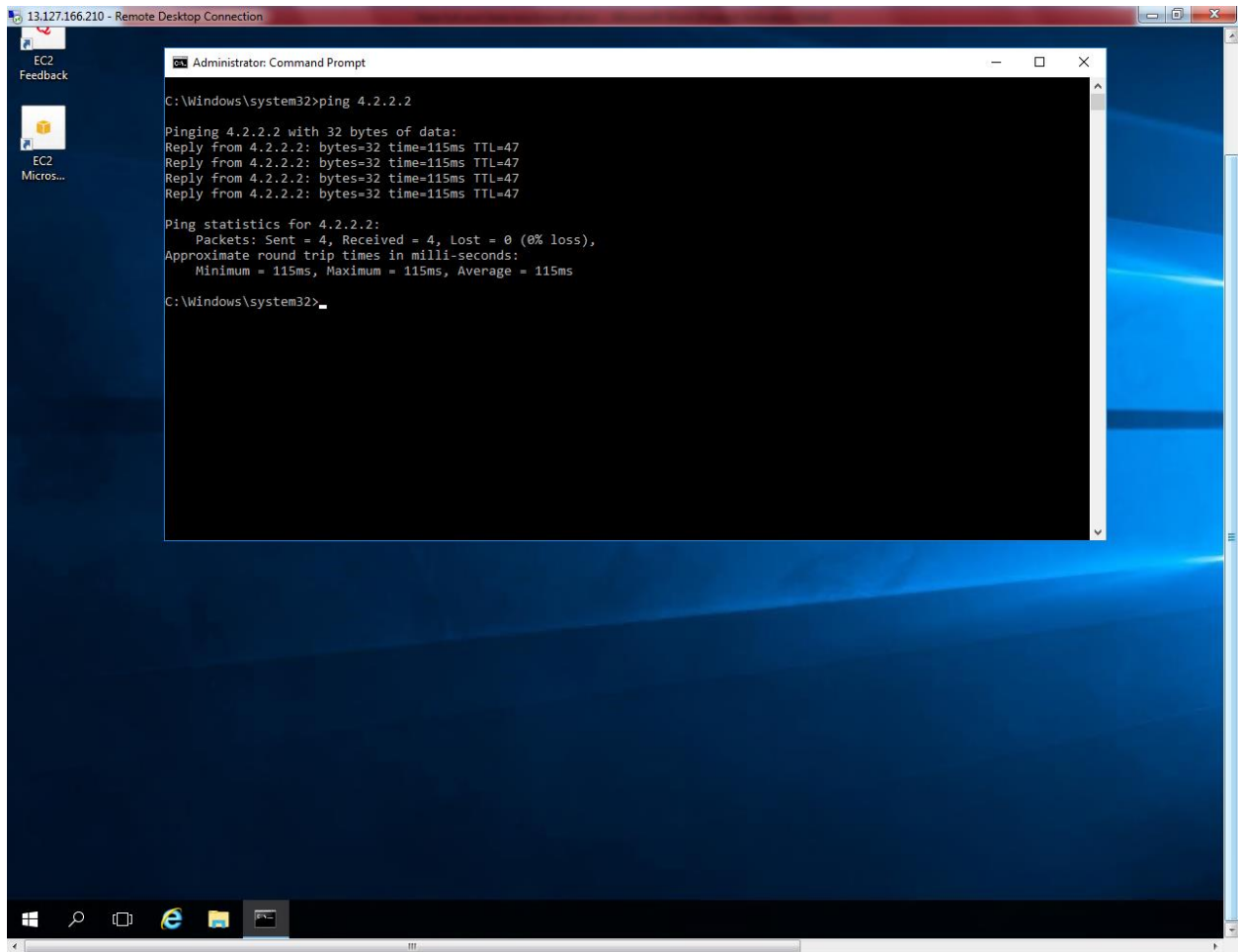
Right click of start menu and click "Command prompt (Admin).



Type “ipconfig” to get the ip address.



You can able to access public network from public subnet.



Get the private IP address of Private subnet 10.0.1.45

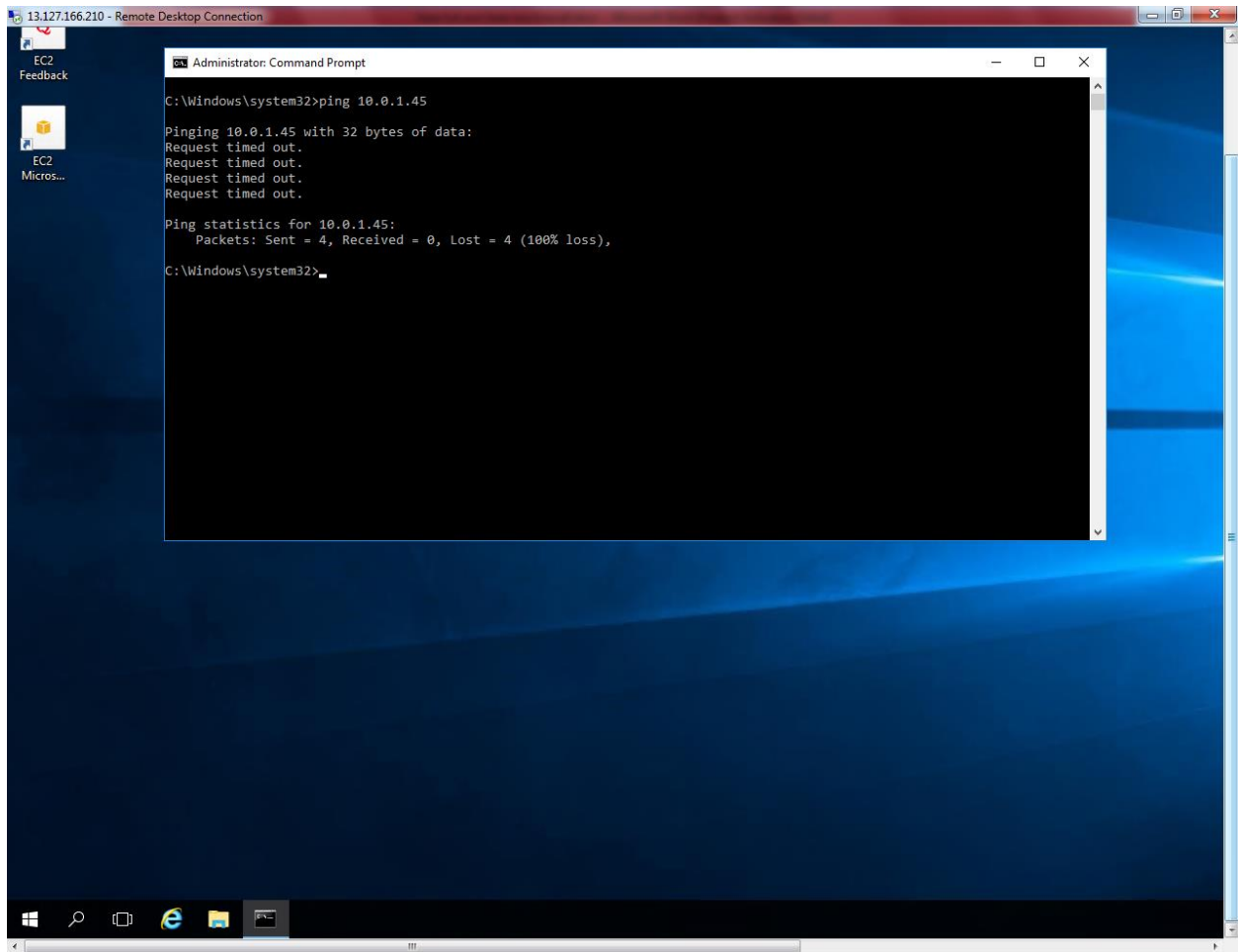
The screenshot shows the AWS Management Console for the 'ap-south-1' region. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area displays the 'Instances' page with a table of running instances. The selected instance, 'Windows Private Server' (ID: i-0f7c9db614ae7e993), is shown in the details pane below. The details pane includes tabs for Description, Status Checks, Monitoring, and Tags. The Description tab is active, showing the instance's state (running), type (t2.micro), and private IP address (10.0.1.45). The console also shows the instance's security groups and network interfaces.

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	
Instance ID	i-0f7c9db614ae7e993
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	ap-south-1a
Security groups	launch-wizard-1, view inbound rules
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 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”.

EC2 Management Console

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

aws Services Resource Groups

EC2 Dashboard
Events
Tags
Reports
Limits

INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts

IMAGES
AMIs
Bundle Tasks

ELASTIC BLOCK STORE
Volumes
Snapshots

NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

LOAD BALANCING
Load Balancers
Target Groups

AUTO SCALING
Launch Configurations

Create Security Group Actions

Filter by tags and attributes or search by keyword

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 VPC security group	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 VPC security group	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

Security Group: sg-30c3005b

Description Inbound Outbound Tags

Edit

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”.

Edit inbound rules [X]

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
RDP ▾	TCP	3389	Custom ▾ 0.0.0.0/0	e.g. SSH for Admin Desktop [X]

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 [X]

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
RDP ▾	TCP	3389	Custom ▾ 0.0.0.0/0	e.g. SSH for Admin Desktop [X]
All ICMP - IPv ▾	ICMP	0 - 65535	Custom ▾ 0.0.0.0/0	e.g. SSH for Admin Desktop [X]

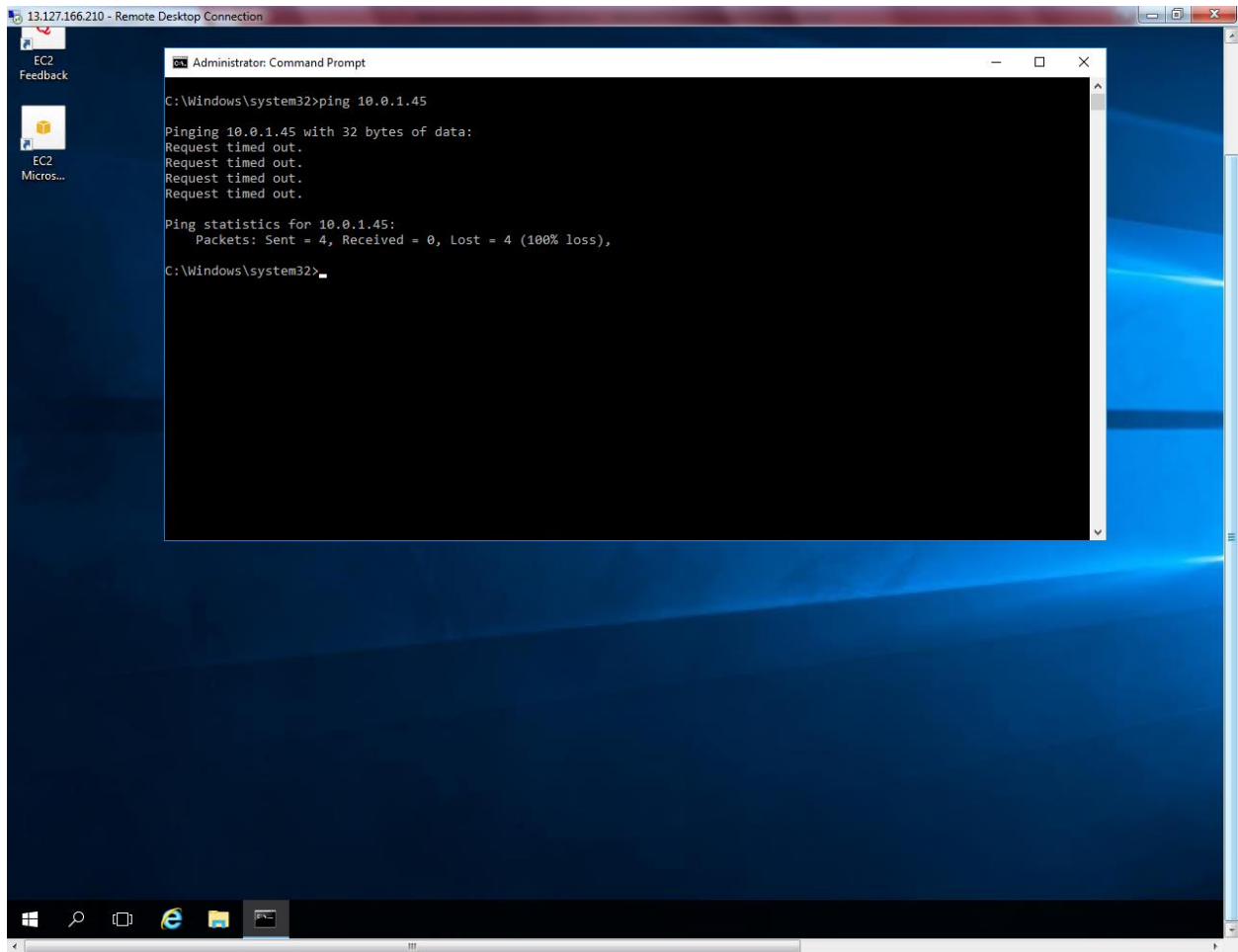
Add Rule

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.

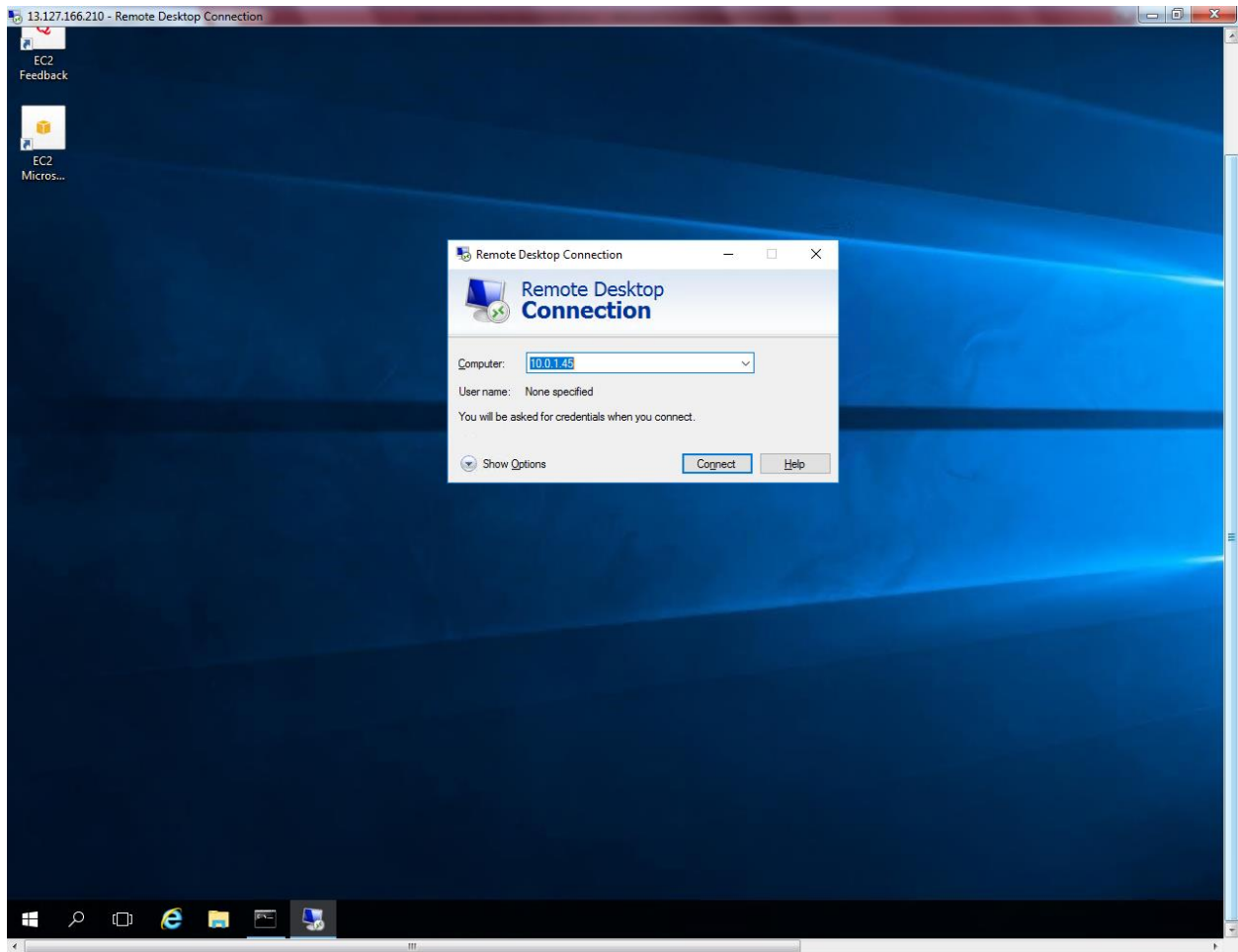
The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar contains navigation links for various AWS services. The main content area displays the 'Instances' page, which includes a table of running EC2 instances. The second instance, 'Windows Private S...', is selected. Below the table, the details for this instance are shown, including its ID, state, type, and private IP address (10.0.1.45).

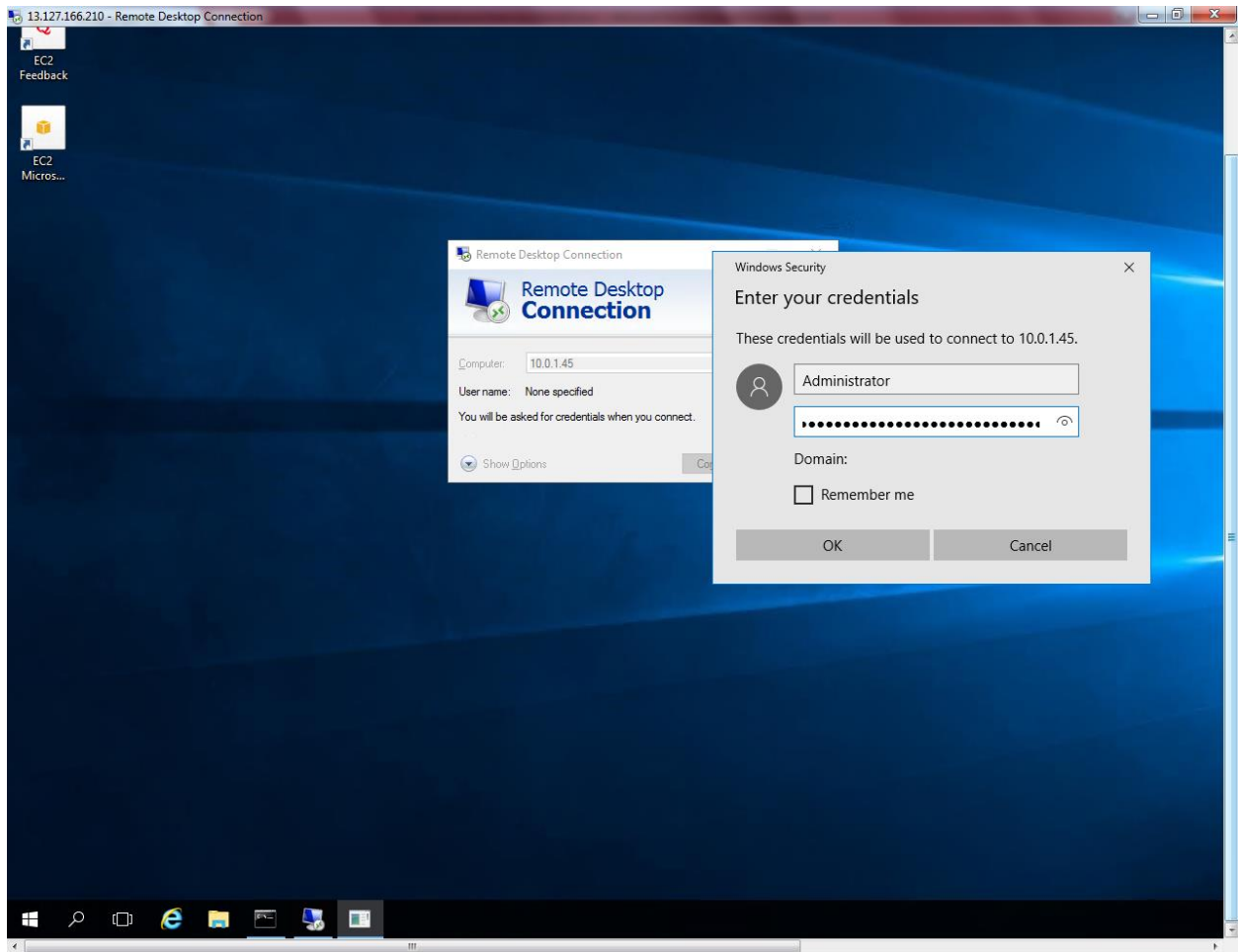
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Windows Public Se...	i-0f64d7067af702f0a	t2.micro	ap-south-1b	running	2/2 checks ...	None	
Windows Private S...	i-0f7c9db614ae7e993	t2.micro	ap-south-1a	running	2/2 checks ...	None	

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

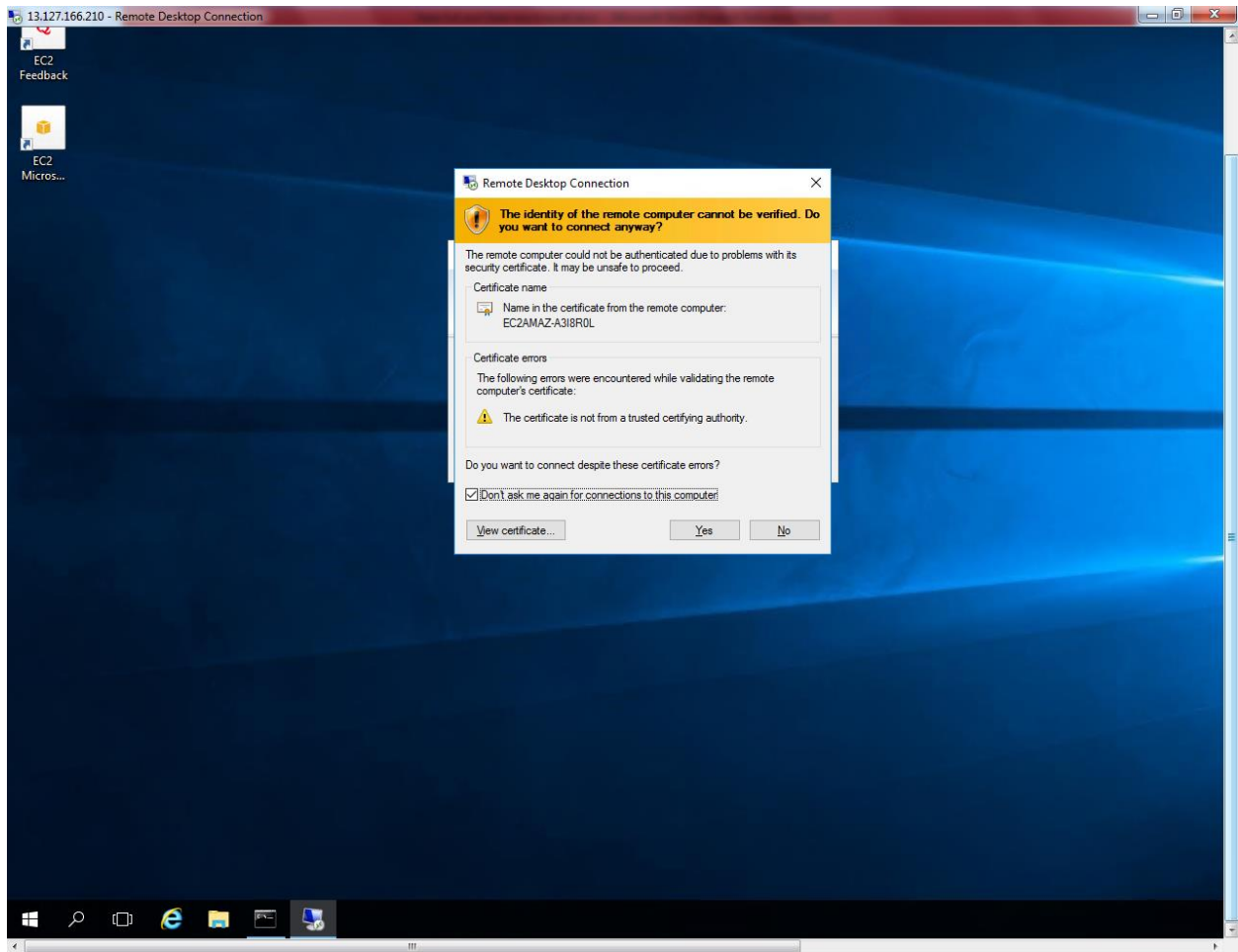
Description	Status Checks	Monitoring	Tags
Instance ID	i-0f7c9db614ae7e993	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-1-45 ap-south-1.compute.internal
Availability zone	ap-south-1a	Private IPs	10.0.1.45
Security groups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

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

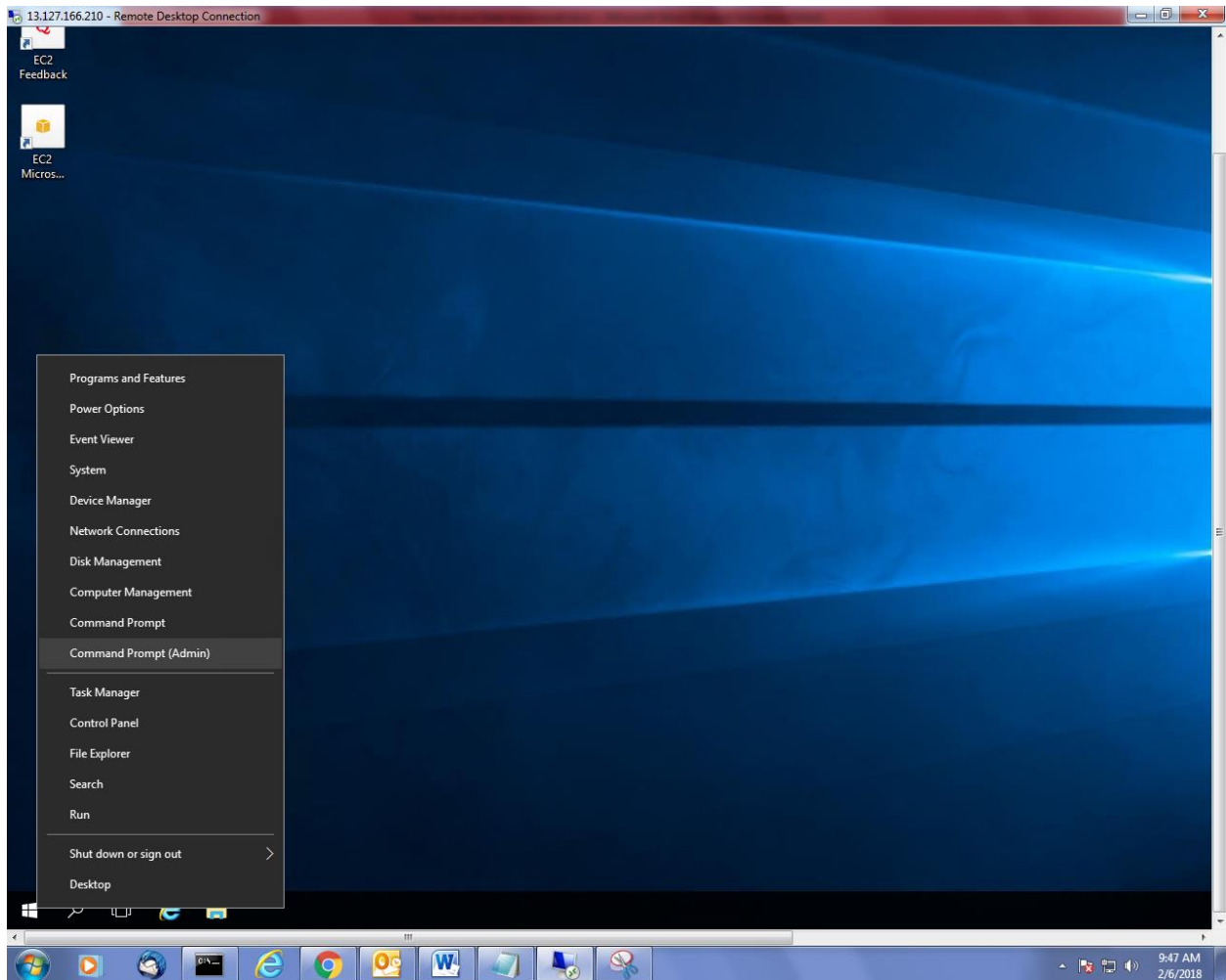




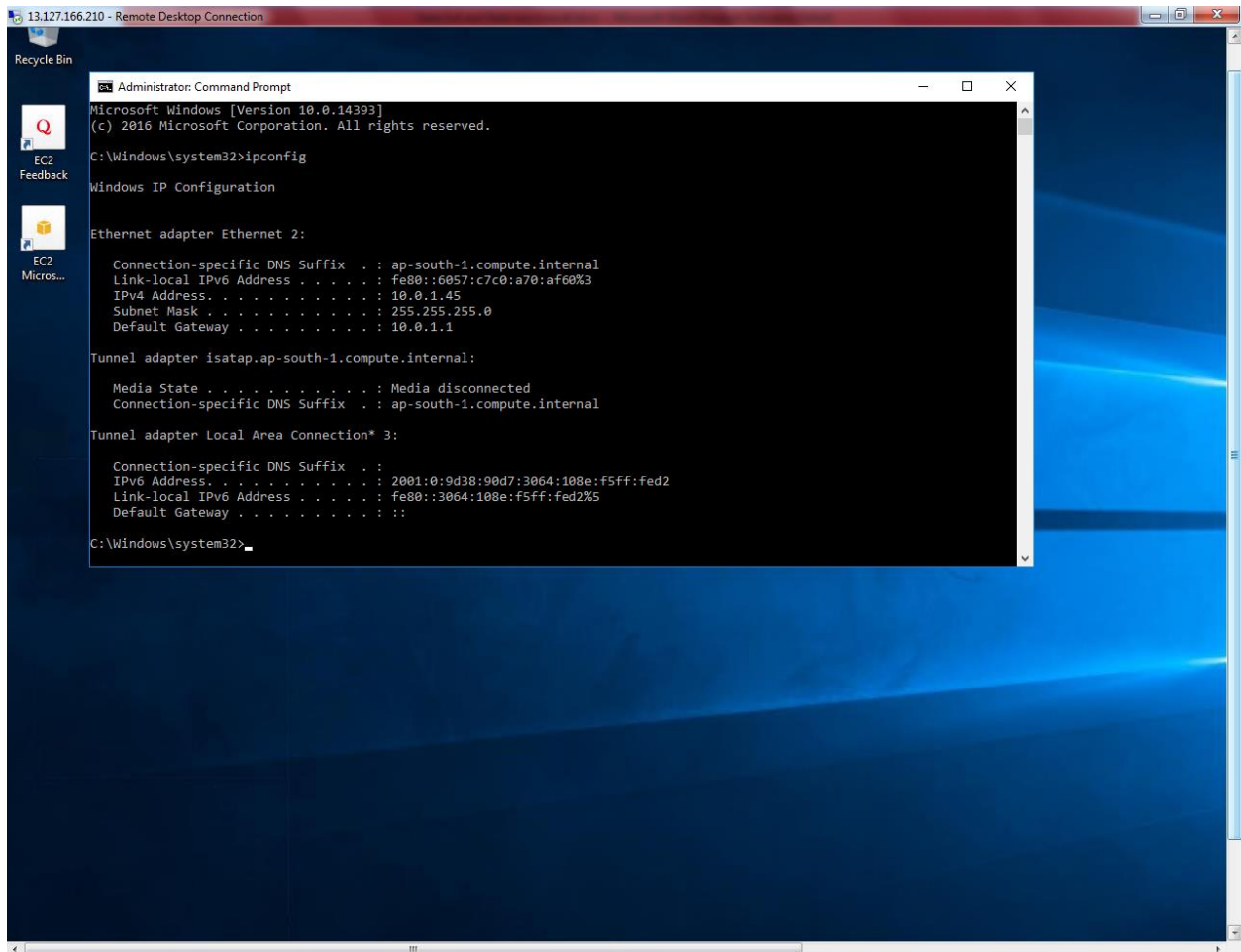
Click "Yes" to continue.



Right click start menu and click "Command prompt (Admin)"



Type ipconfig in Private server.



```
13.127.166.210 - Remote Desktop Connection
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::6057: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:

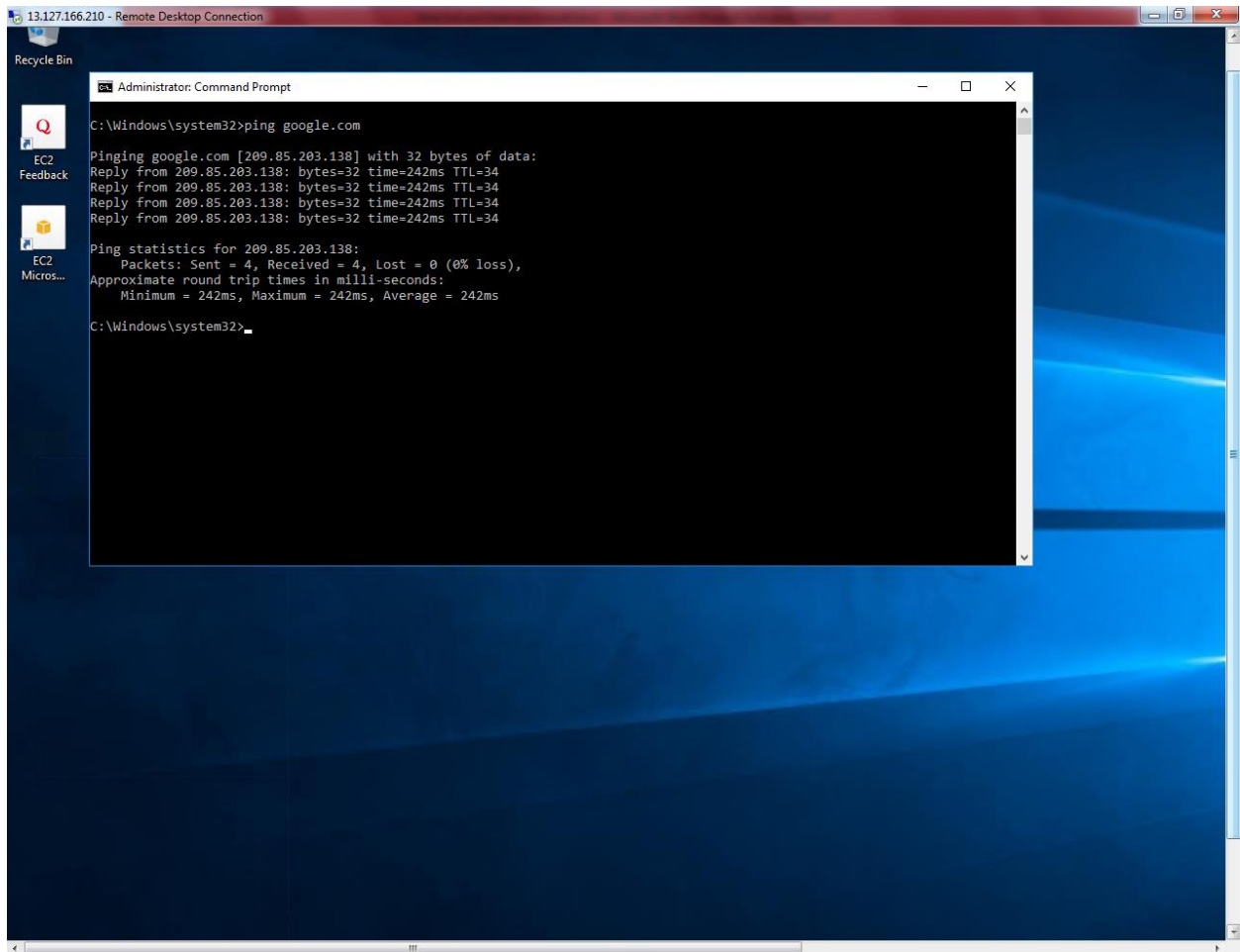
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : ap-south-1.compute.internal

Tunnel adapter Local Area Connection* 3:

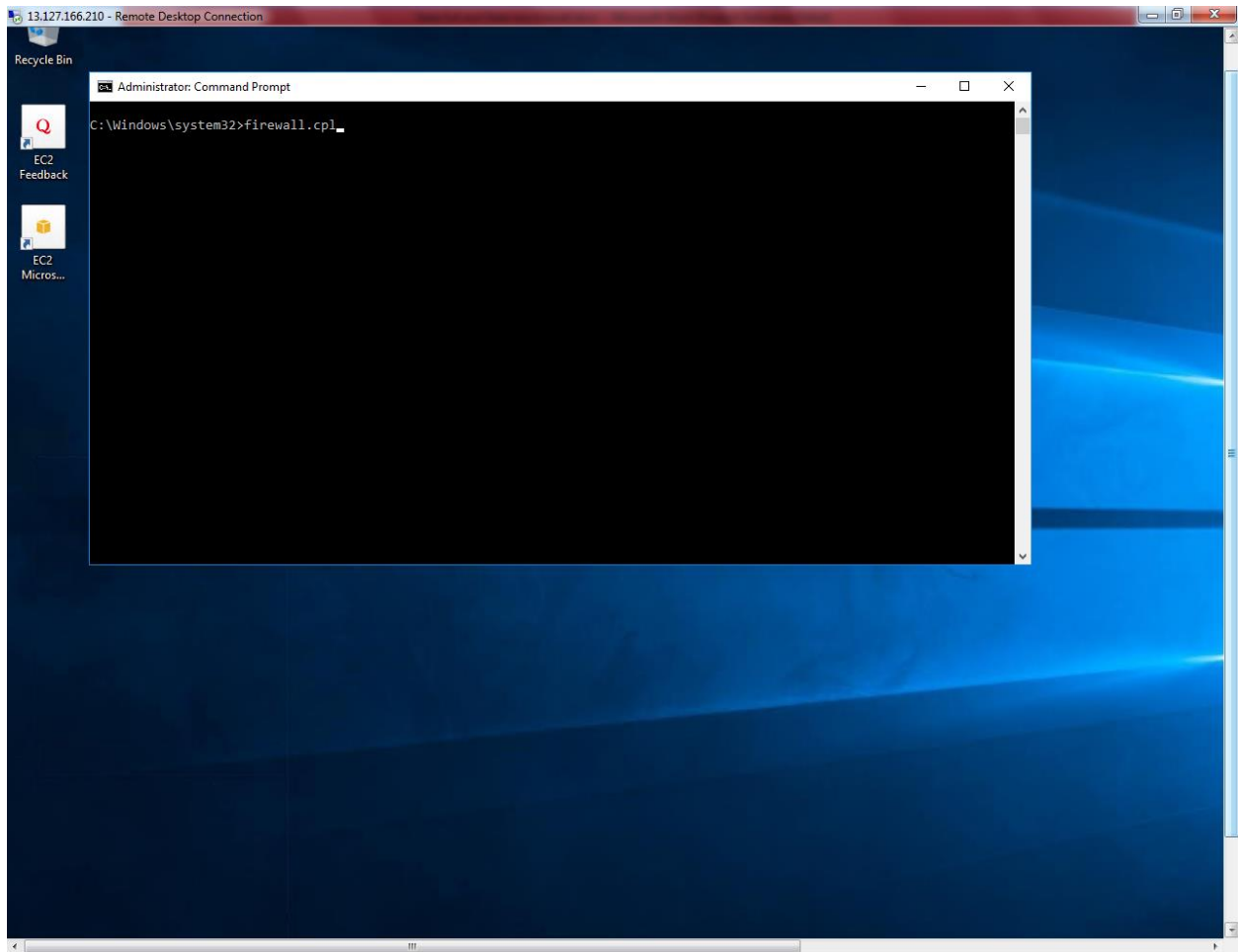
    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:9d38:90d7:3064:108e:f5ff:fed2
    Link-local IPv6 Address . . . . . : fe80::3064:108e:f5ff:fed2%5
    Default Gateway . . . . . :

C:\Windows\system32>
```

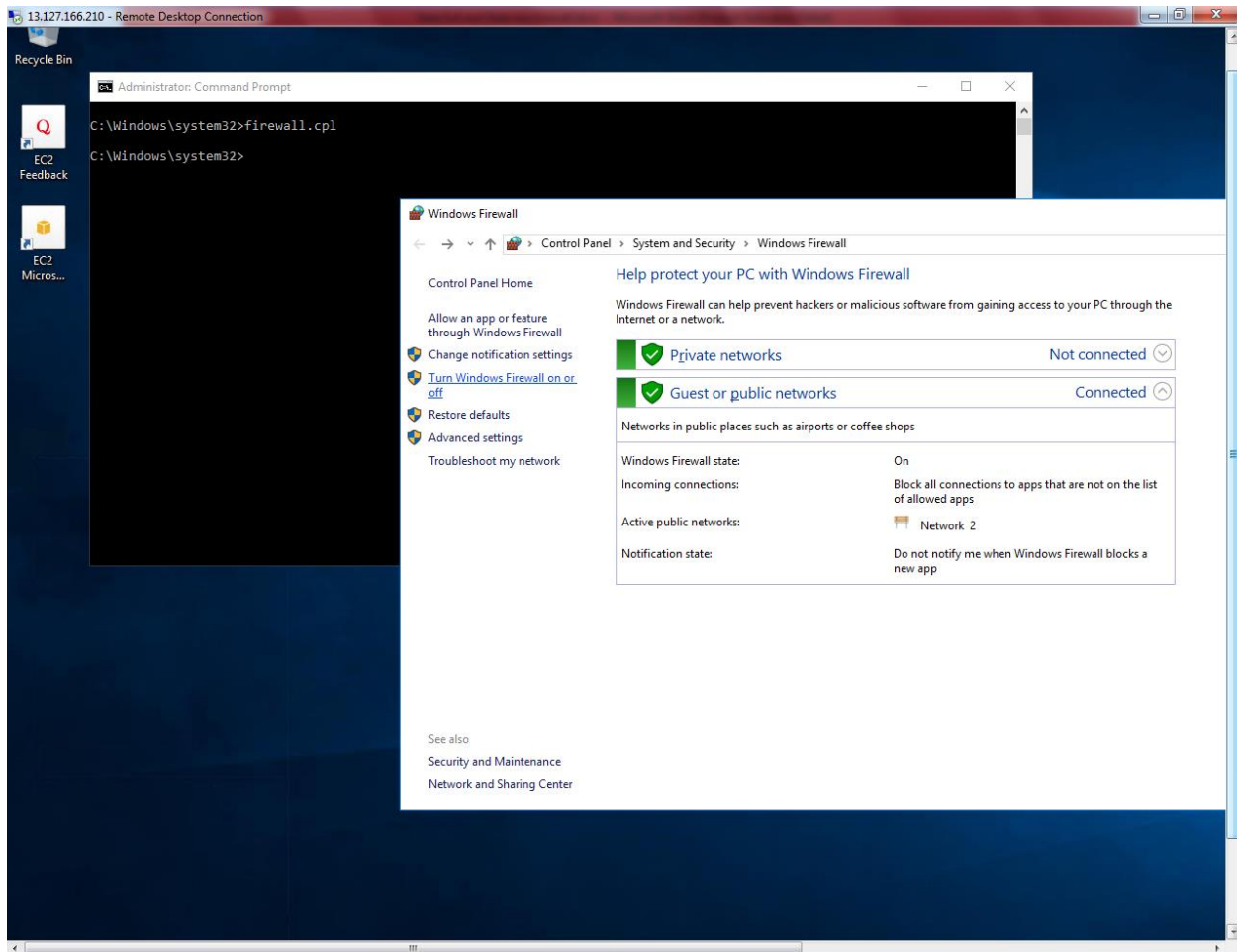
Type google.com in private subnet server. We are able to connect internet from private subnet by using NAT gateway.



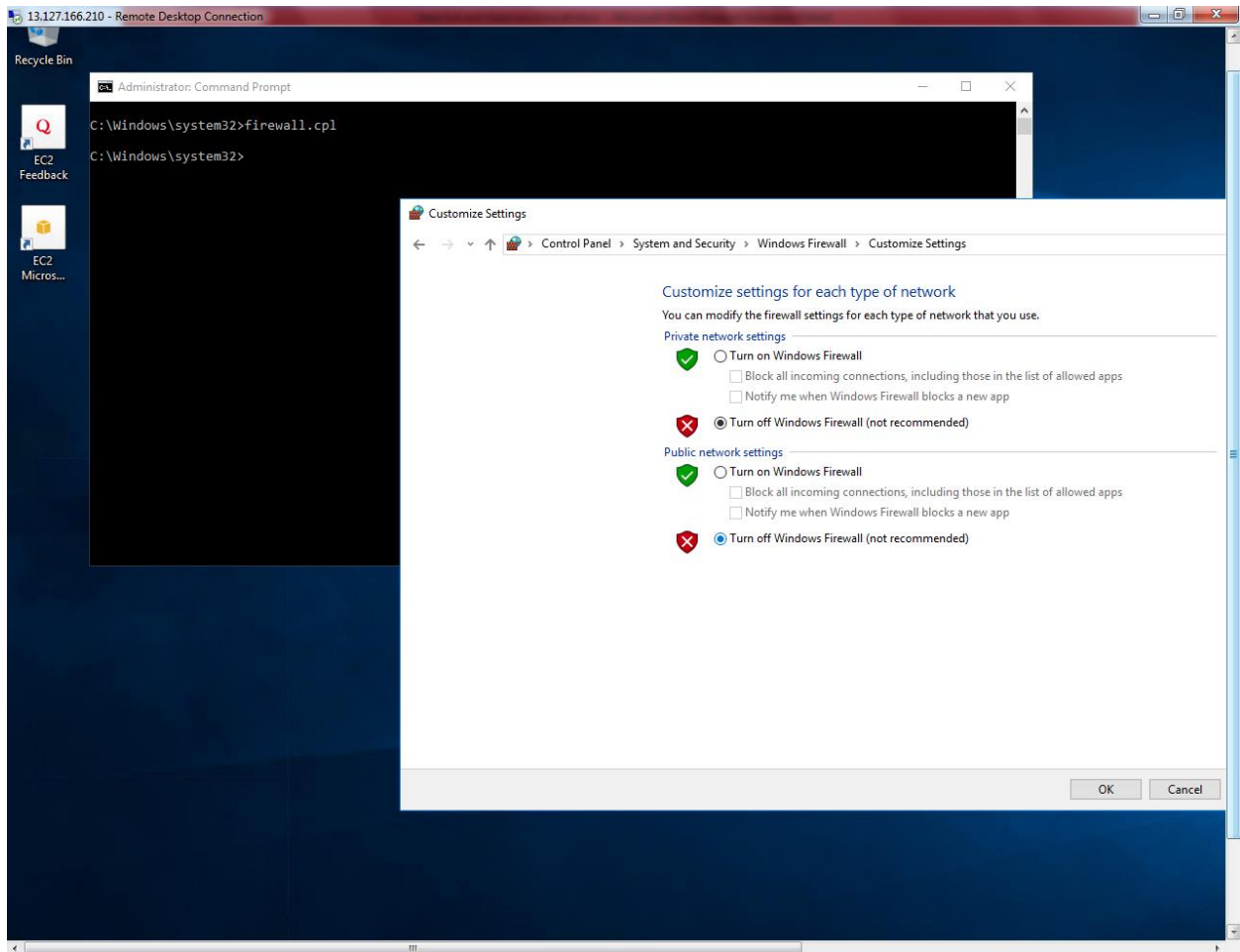
Type Firewall.cpl



Click “Turn Windows Firewall on or Off”.

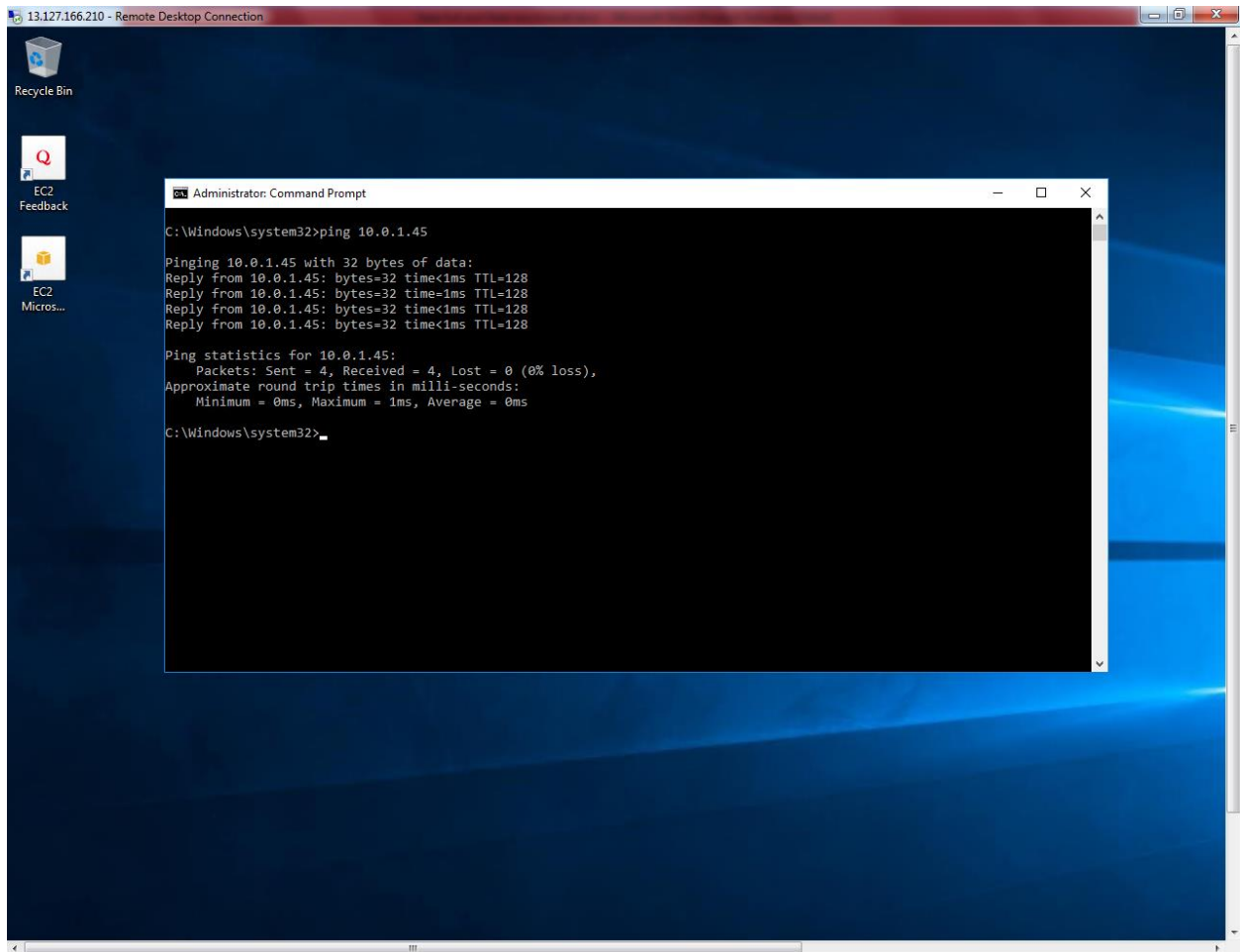


Turn off windows firewall.



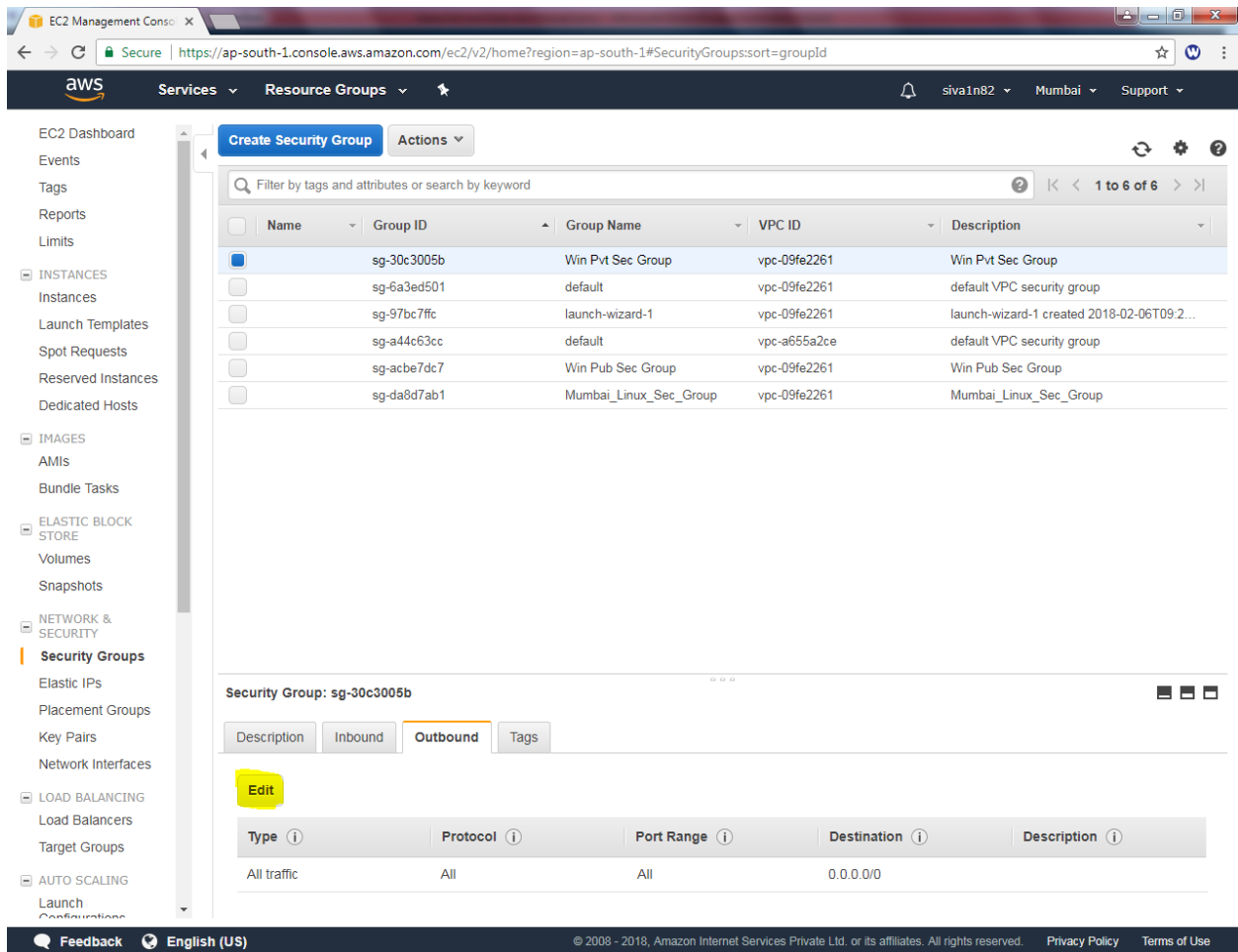
Click "Ok".

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.



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

Click "Edit".



The screenshot displays the AWS Management Console interface for the 'Security Groups' page. The left sidebar contains a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY (highlighted), LOAD BALANCING, and AUTO SCALING. Under NETWORK & SECURITY, 'Security Groups' is selected. The main content area shows a list of security groups with columns for Name, Group ID, Group Name, VPC ID, and Description. The first group, 'sg-30c3005b', is highlighted. Below the list, the detailed view for 'Security Group: sg-30c3005b' is shown, with tabs for Description, Inbound, Outbound, and Tags. The Outbound tab is active, showing a table with columns: Type, Protocol, Port Range, Destination, and Description. The table contains one entry: 'All traffic' with protocol 'All' and port range 'All'.

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	Destination	Description
All traffic	All	All	0.0.0.0/0	

Click "X" mark to remove.

Edit outbound rules

Type ⓘ

Protocol ⓘ

Port Range ⓘ

Destination ⓘ

Description ⓘ

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 ⓘ

Protocol ⓘ

Port Range ⓘ

Destination ⓘ

Description ⓘ

This security group has no rules

Add Rule

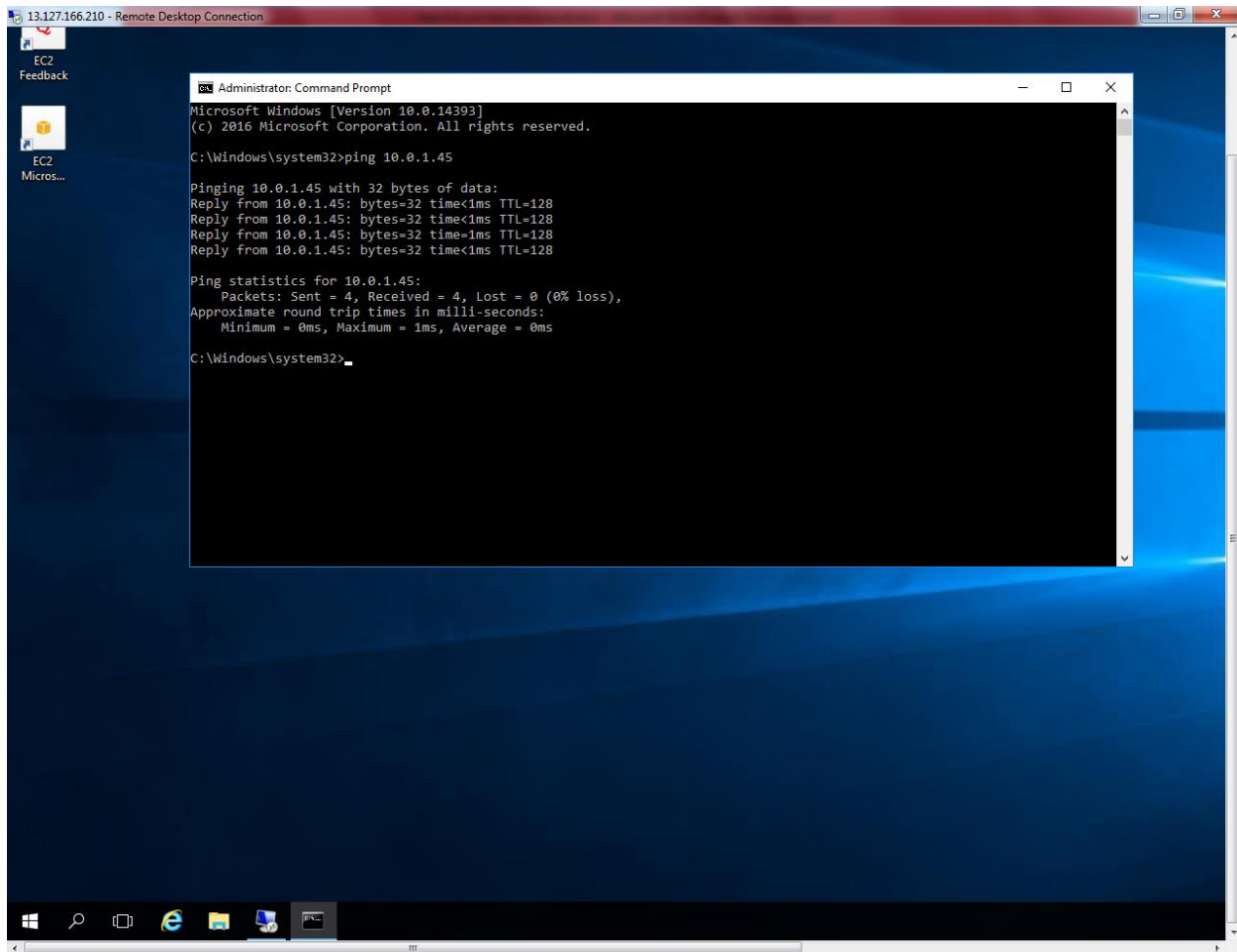
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

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.



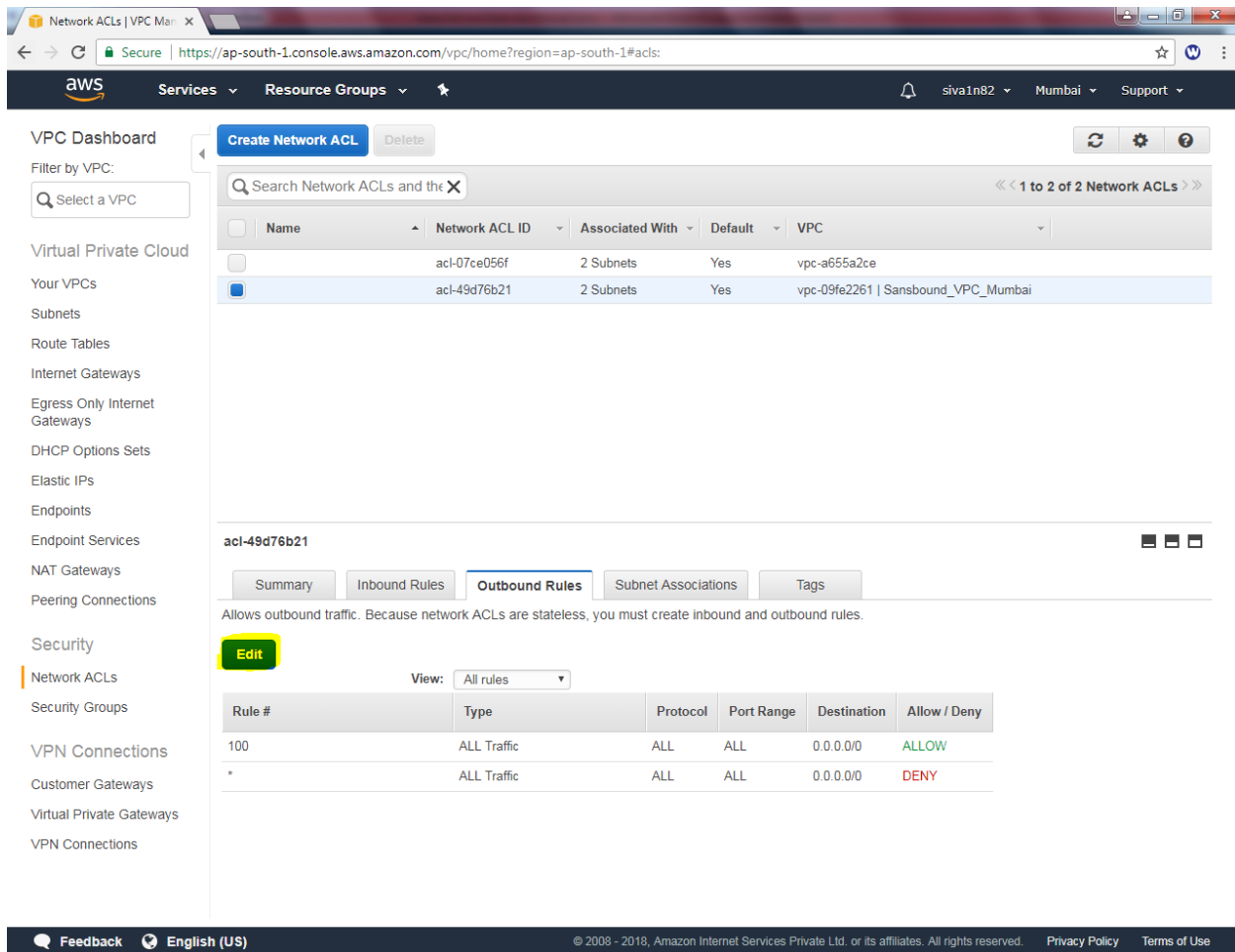
Then restore the outbound rule as default.

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, which includes a 'Start VPC Wizard' button, a 'Launch EC2 Instances' button, and 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 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 bottom of the console features a footer with Feedback, English (US), and copyright information.

Click “Edit”.



The screenshot displays the AWS Management Console interface for Network ACLs. The left sidebar shows the navigation menu with 'Network ACLs' highlighted under the 'Security' section. The main content area shows a list of Network ACLs, with 'acl-49d76b21' selected. Below the list, the 'Outbound Rules' tab is active, showing a table of rules. A yellow box highlights the 'Edit' button. The rules table contains two entries: Rule 100 (ALLOW) and Rule * (DENY).

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

Create Network ACL Delete

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

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
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".

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, and VPN Connections. The main content area displays a list of Network ACLs with columns for Name, Network ACL ID, Associated With, Default, and VPC. The selected Network ACL, acl-49d76b21, is shown in detail, including its Outbound Rules. The Outbound Rules tab is active, showing a table with columns for Rule #, Type, Protocol, Port Range, Destination, Allow / Deny, and Remove. The rule list is currently empty, and the 'Add another rule' button is visible. The console also includes a top navigation bar with the AWS logo, Services, Resource Groups, and user information.

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

Create Network ACL Delete

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

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

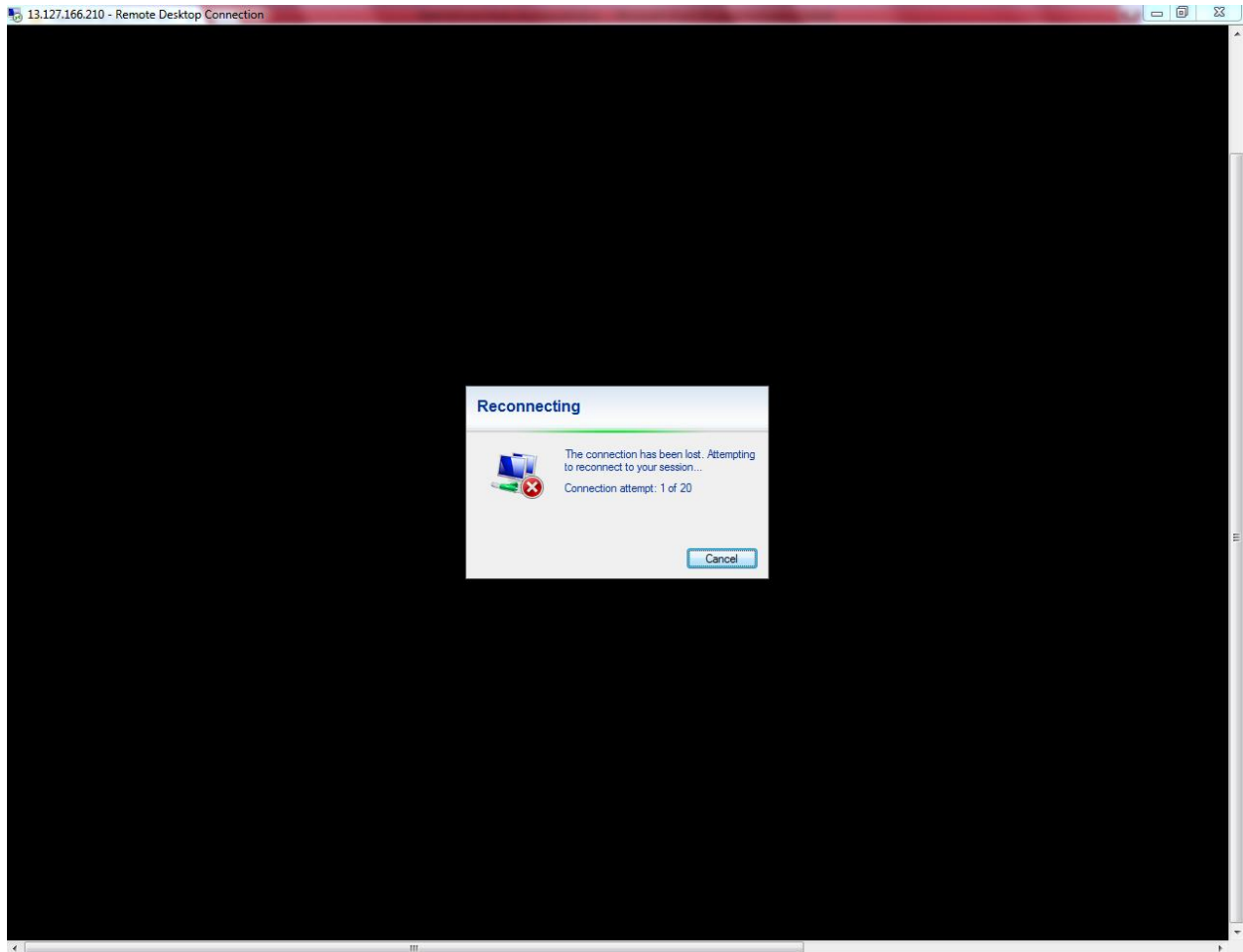
Rule #	Type	Protocol	Port Range	Destination	Allow / Deny	Remove
Add another rule						

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.

The screenshot shows the AWS Management Console interface for Network ACLs. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Security, and VPN Connections. The main content area displays a list of Network ACLs, with 'acl-49d76b21' selected. Below the list, the 'Outbound Rules' tab is active, showing a single rule that denies all traffic.

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

Selected Network ACL: acl-49d76b21

Outbound Rules:

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

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

Click “Edit”.

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
	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 “Add another rule”.

Network ACLs | VPC Main

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.

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

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

Network ACLs | VPC Main

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

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
	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
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

Now we can able to get RDP for public server.

