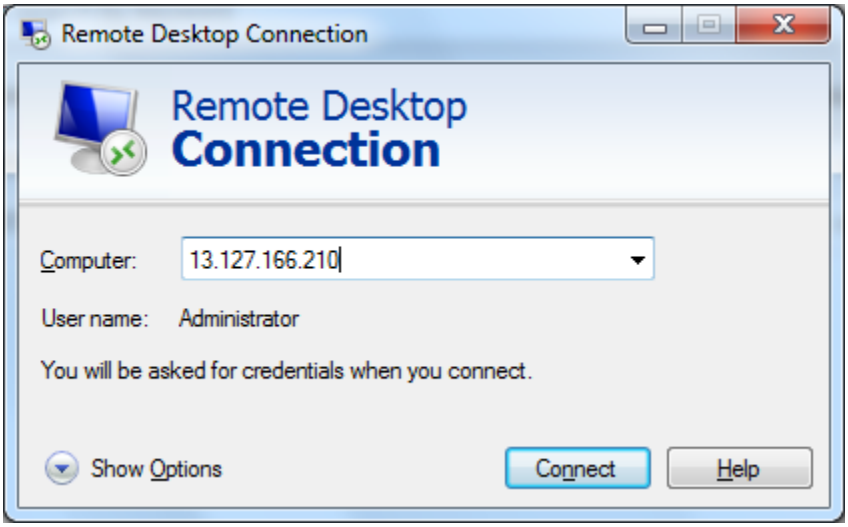
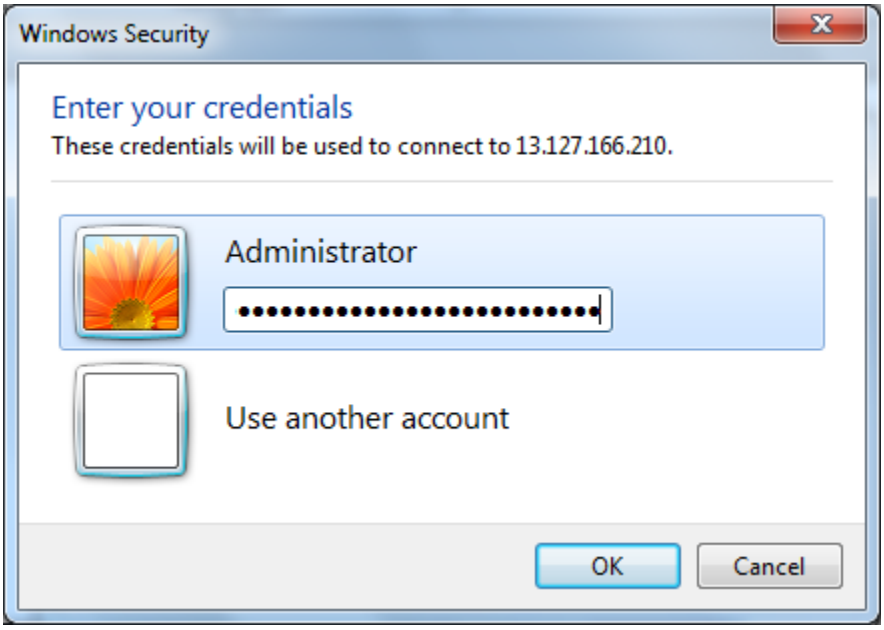
Stateful and Stateless firewall

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

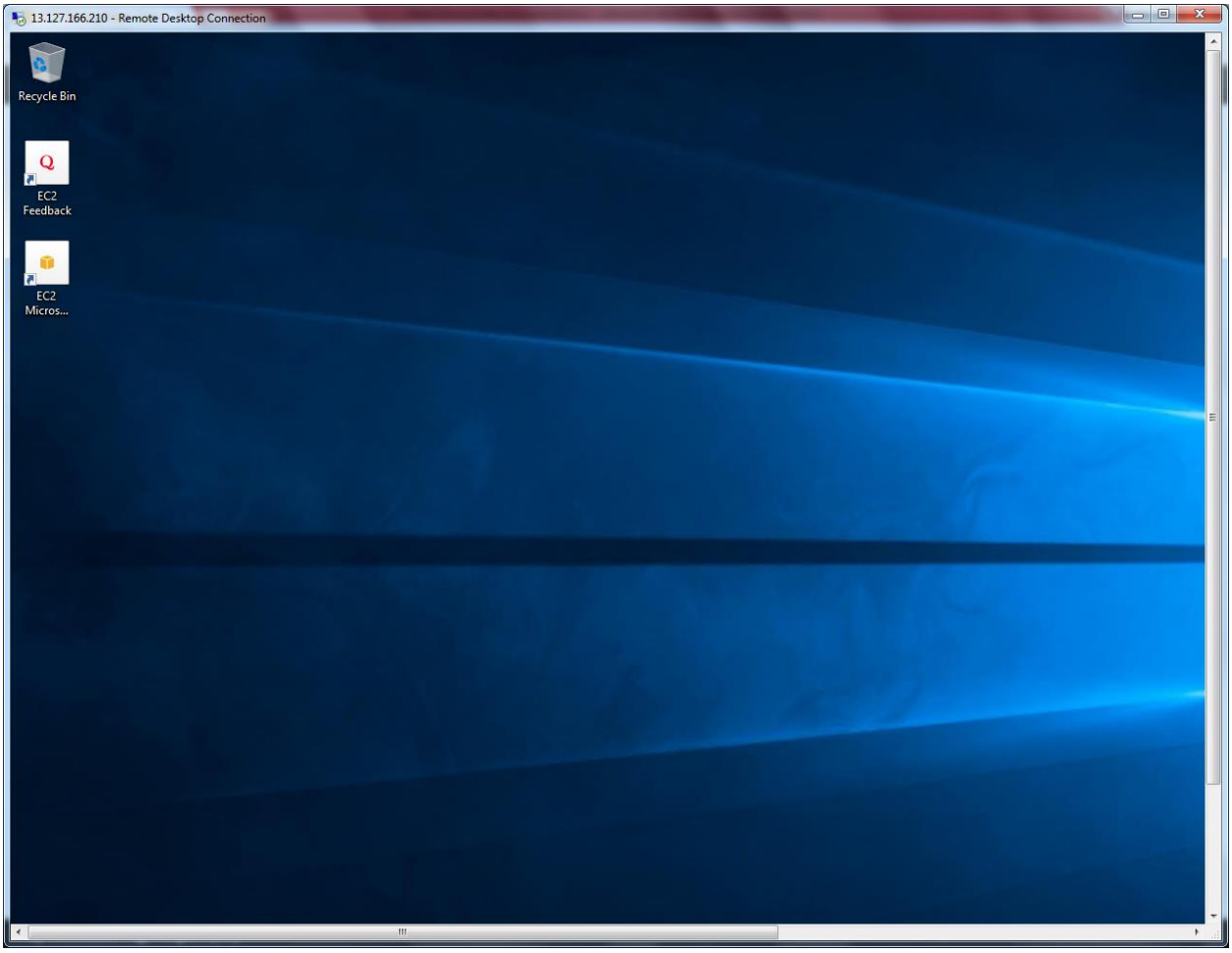
a) Stateful firewall

Type the public server IP in mstsc

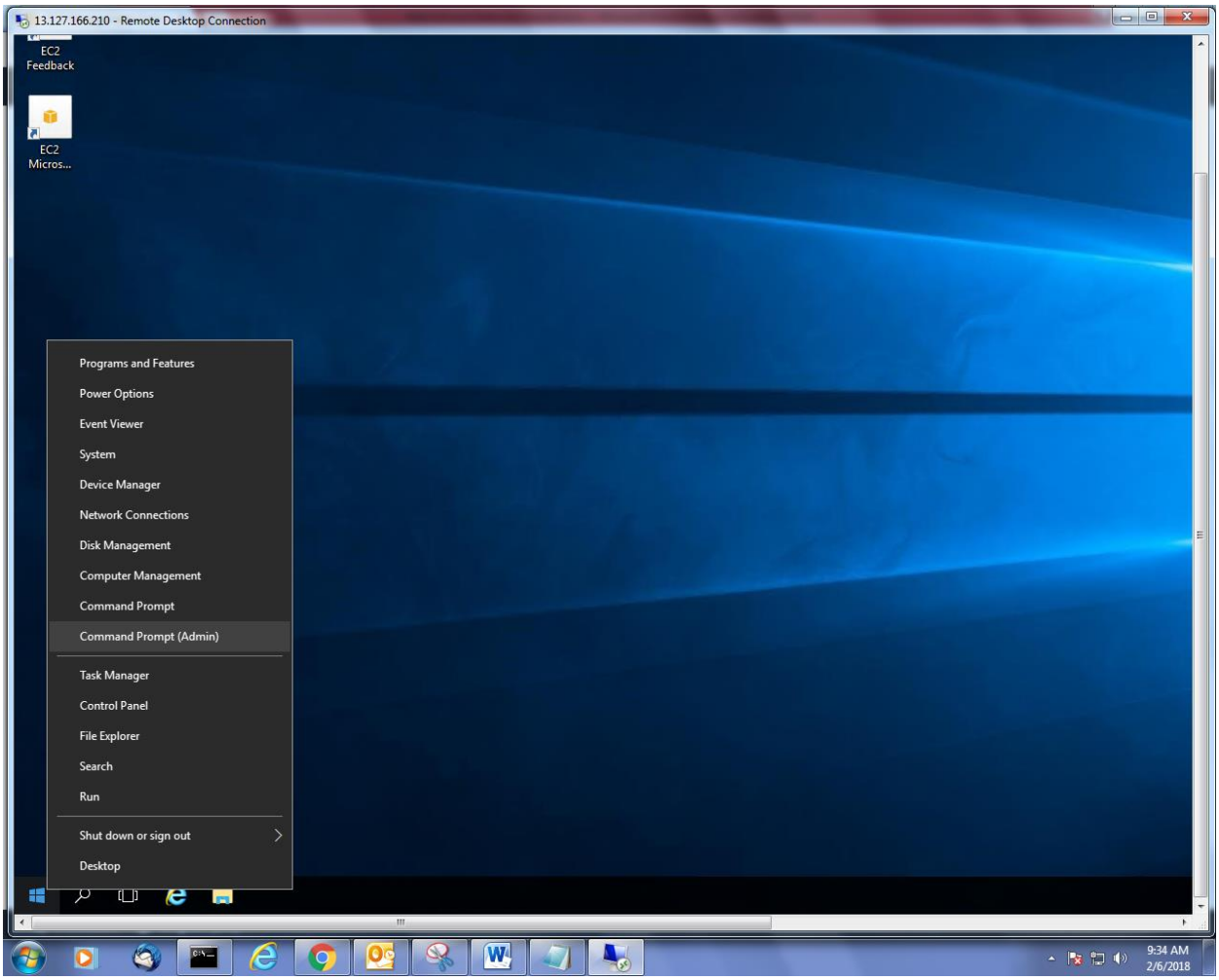



Windows Security
Enter your credentials
These credentials will be used to connect to 13.127.166.210.
Administrator
Use another account
OK
Cancel

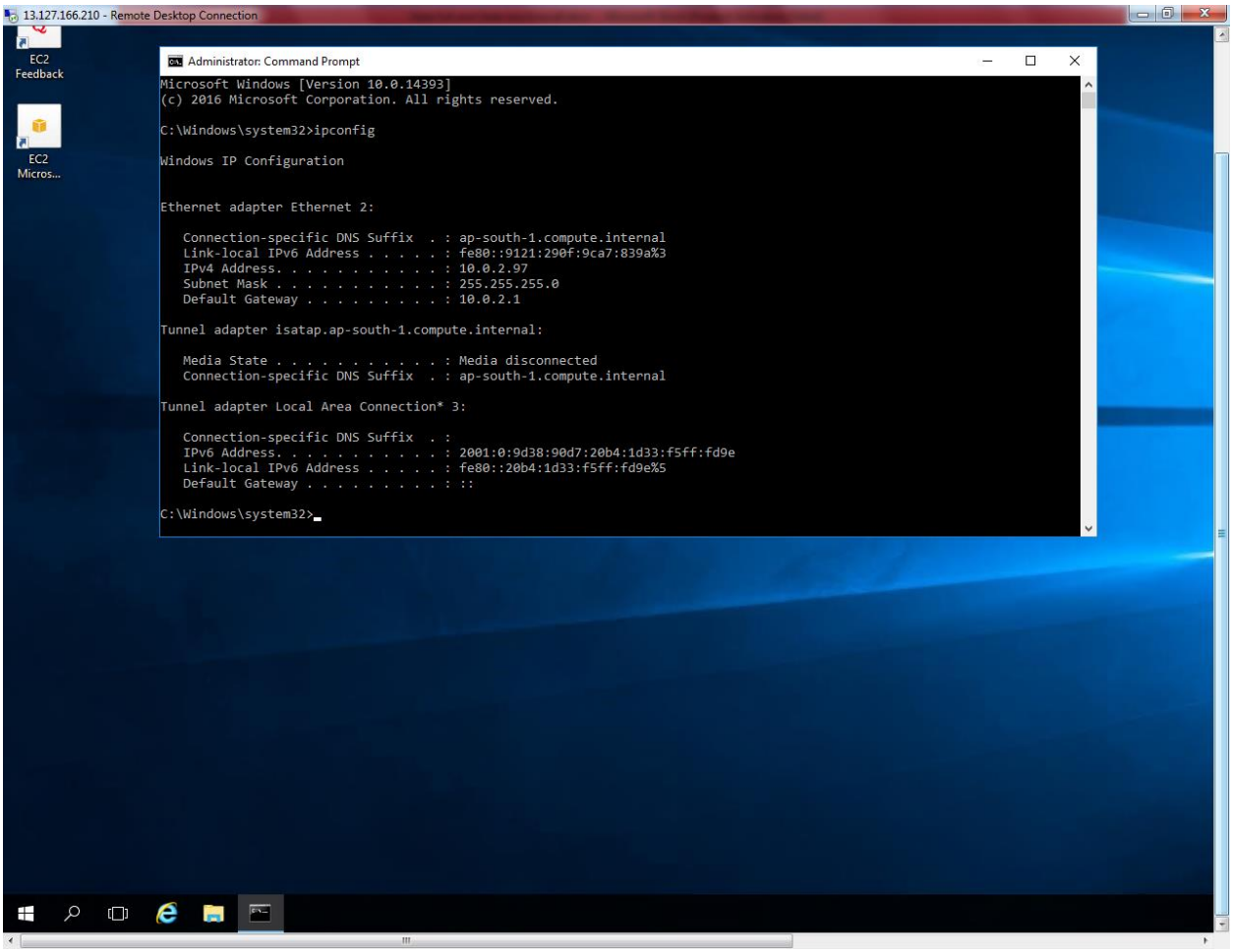
Logged into the Public Server successfully.



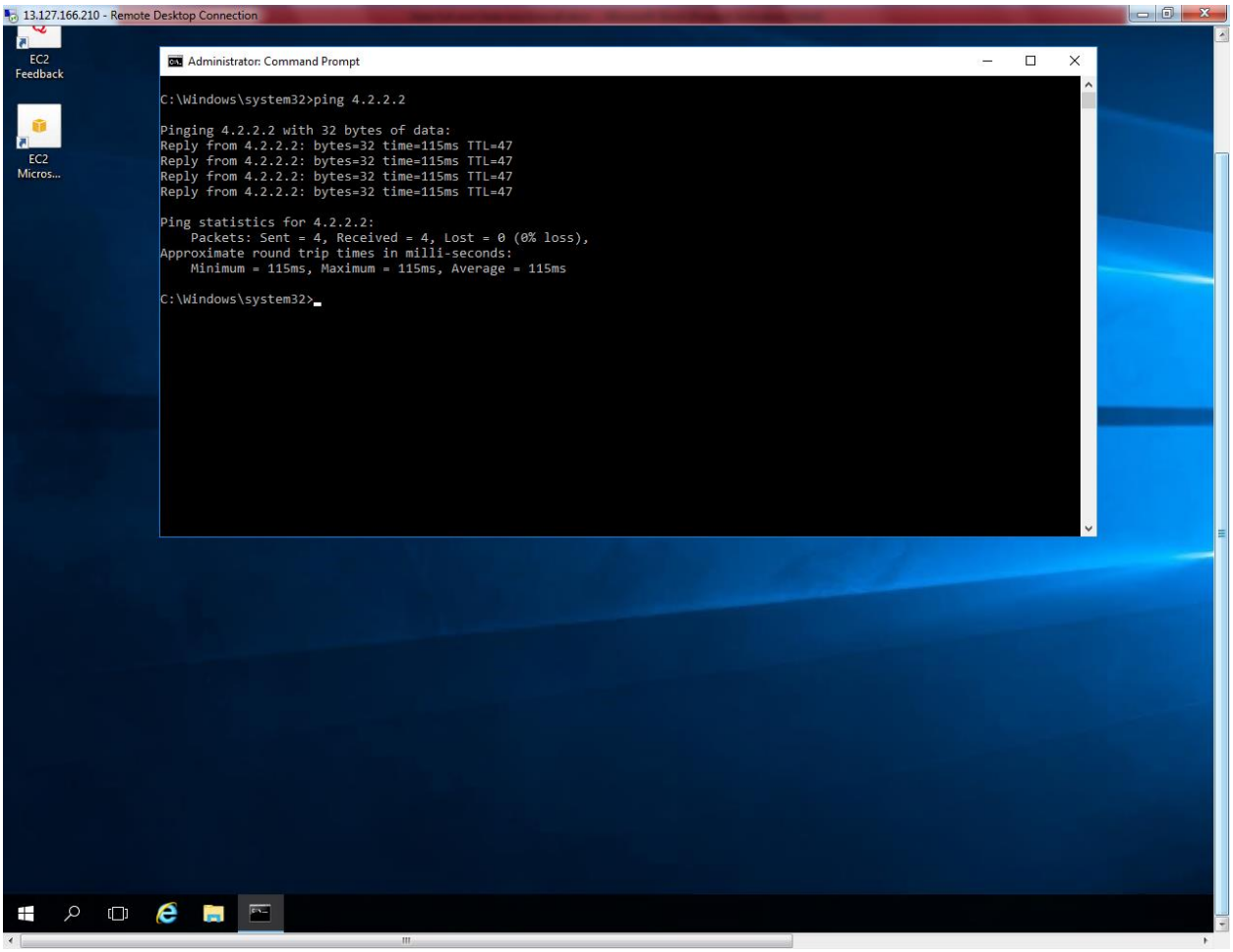
Right click of start menu and click “Command prompt (Admin).



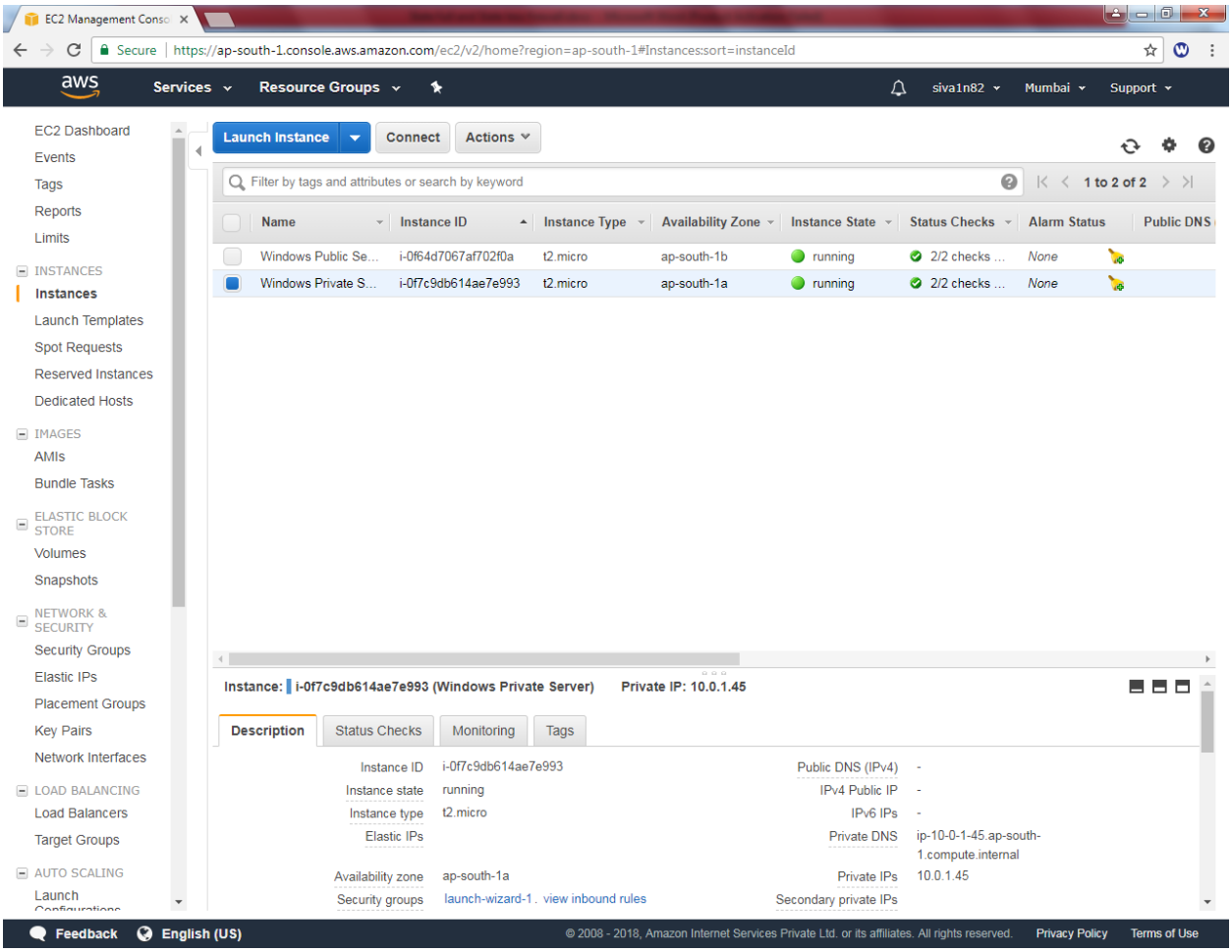
Type “ipconfig” to get the ip address.



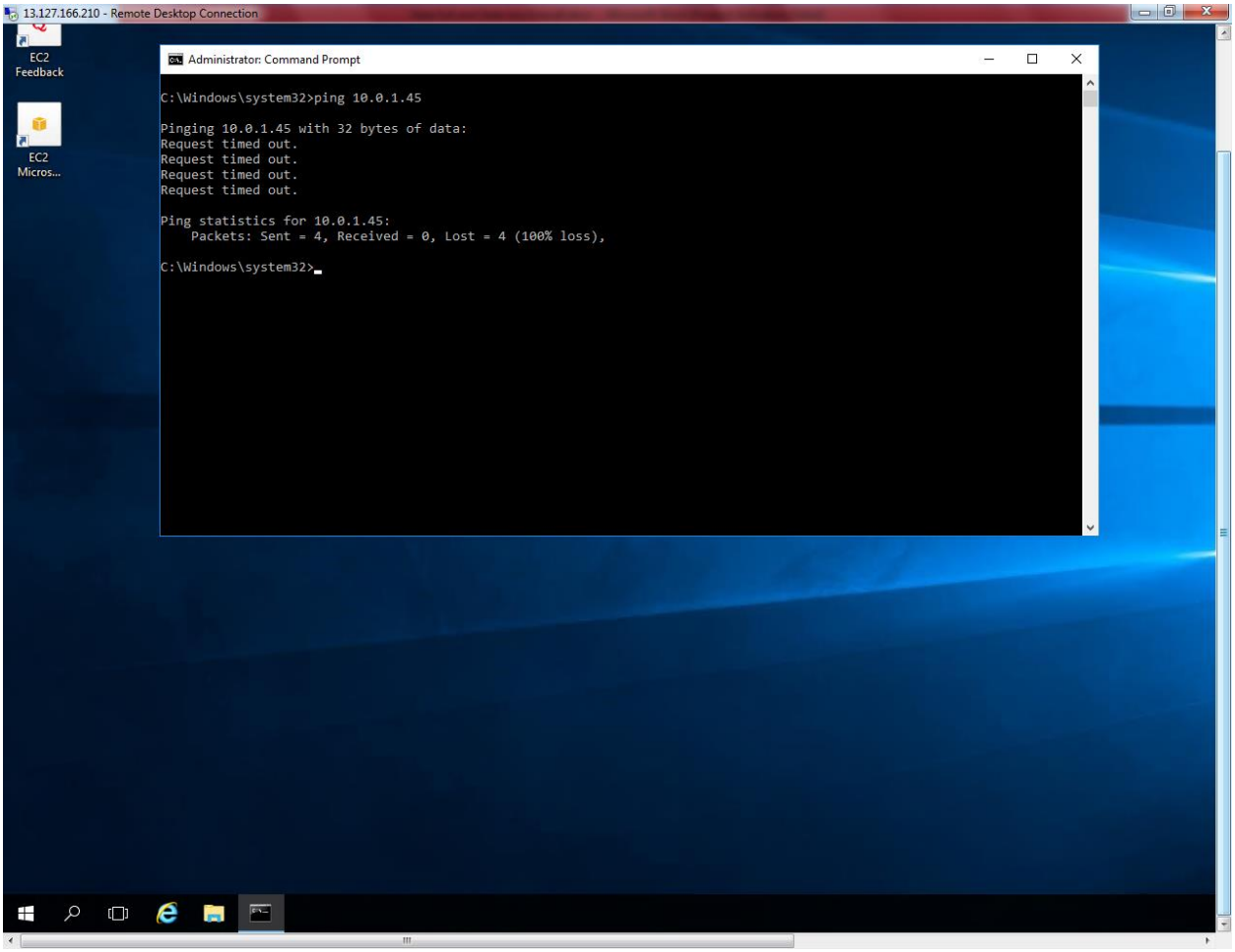
You can able to access public network from public subnet.



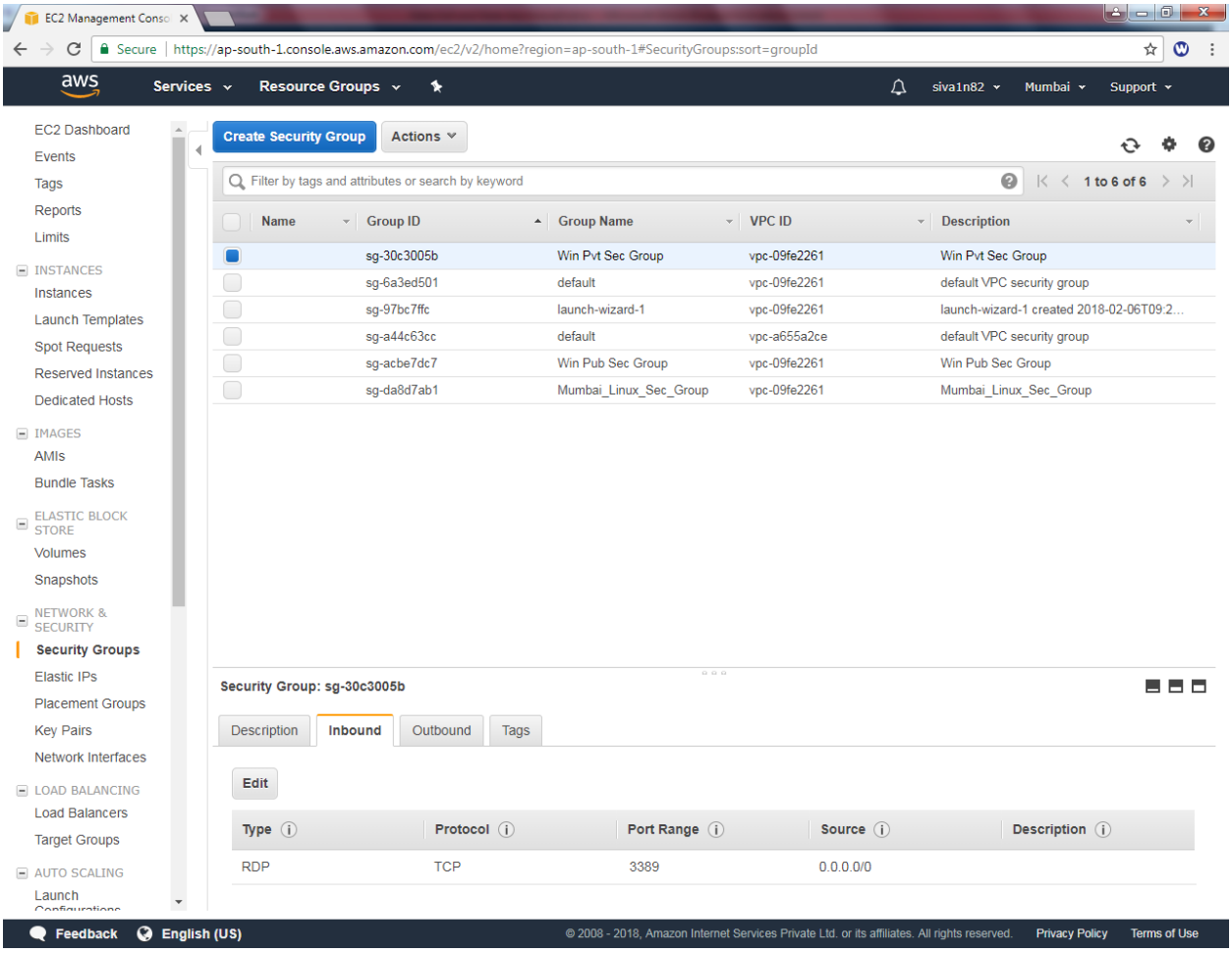
Get the private IP address of Private subnet 10.0.1.45



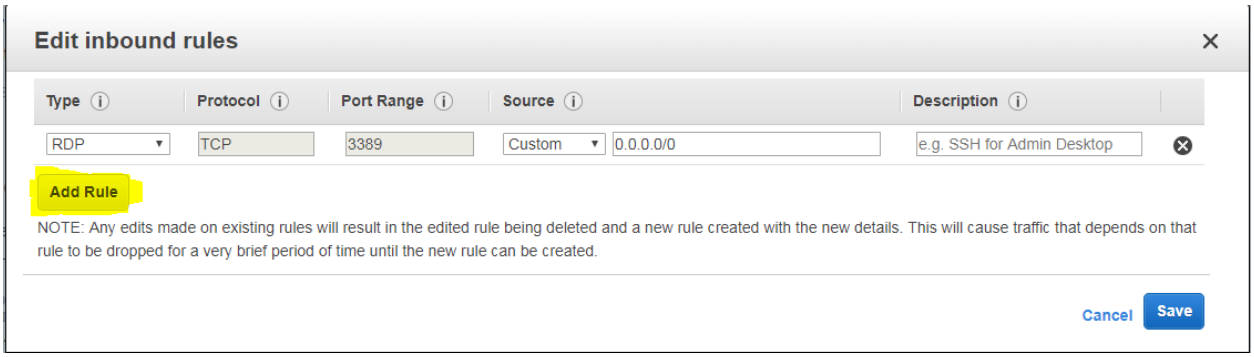
Try to Ping 10.0.1.45, but getting request timed out. Because In security group of Private subnet allowed only RDP Port (3389) in inbound rules.



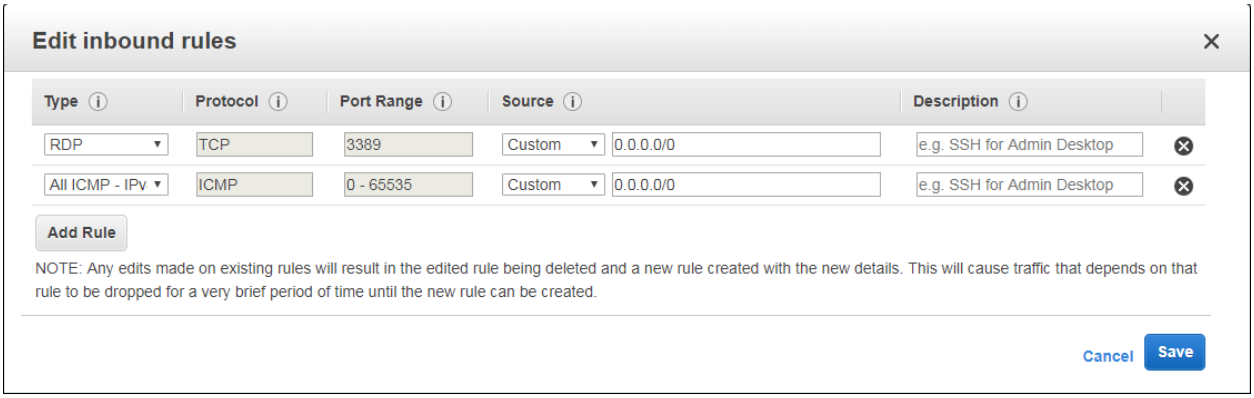
Go to security group and select “Win Pvt Sec Group”.



Click “Add Rule”.

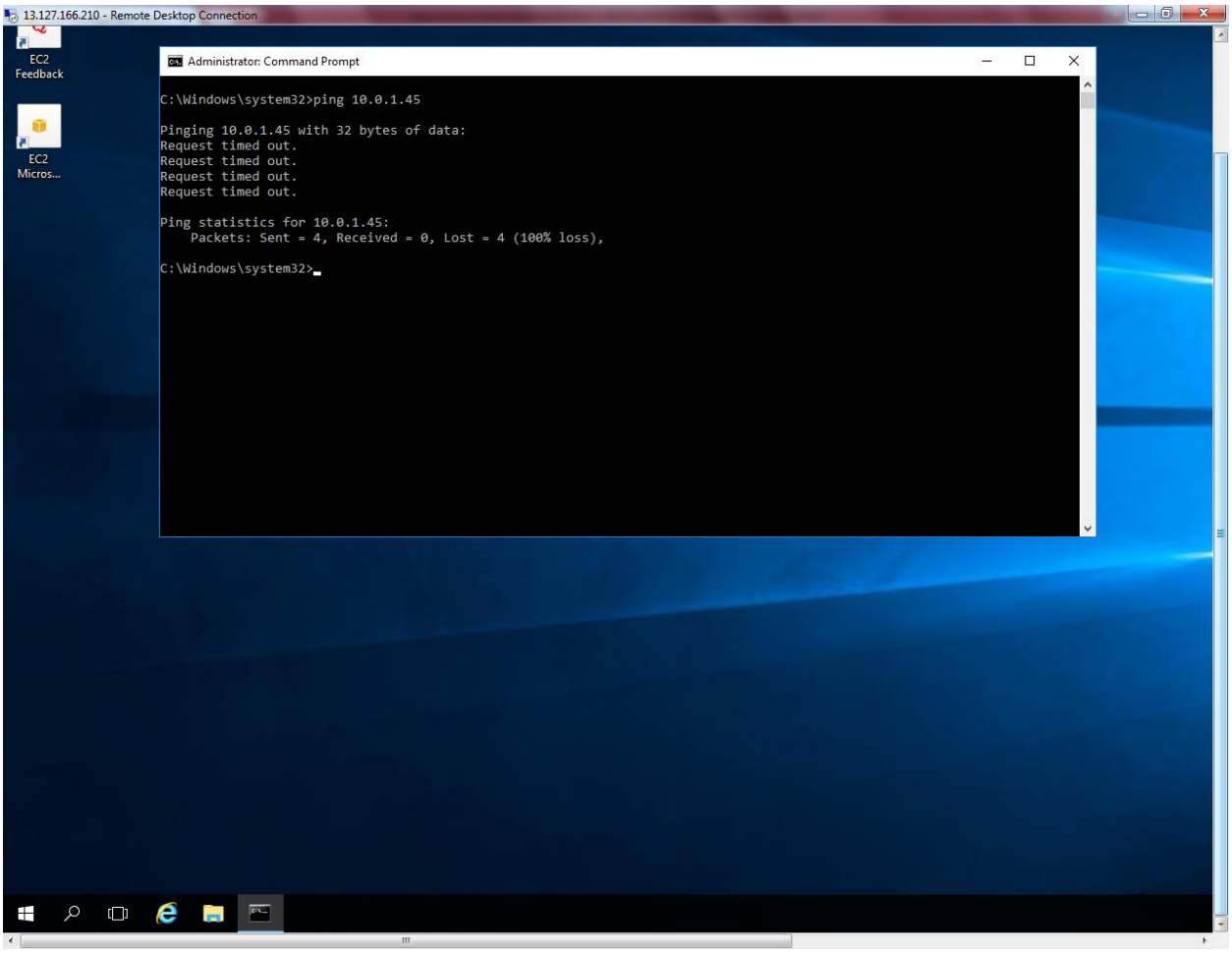


Select “All ICMP “ traffic and source as 0.0.0.0/0

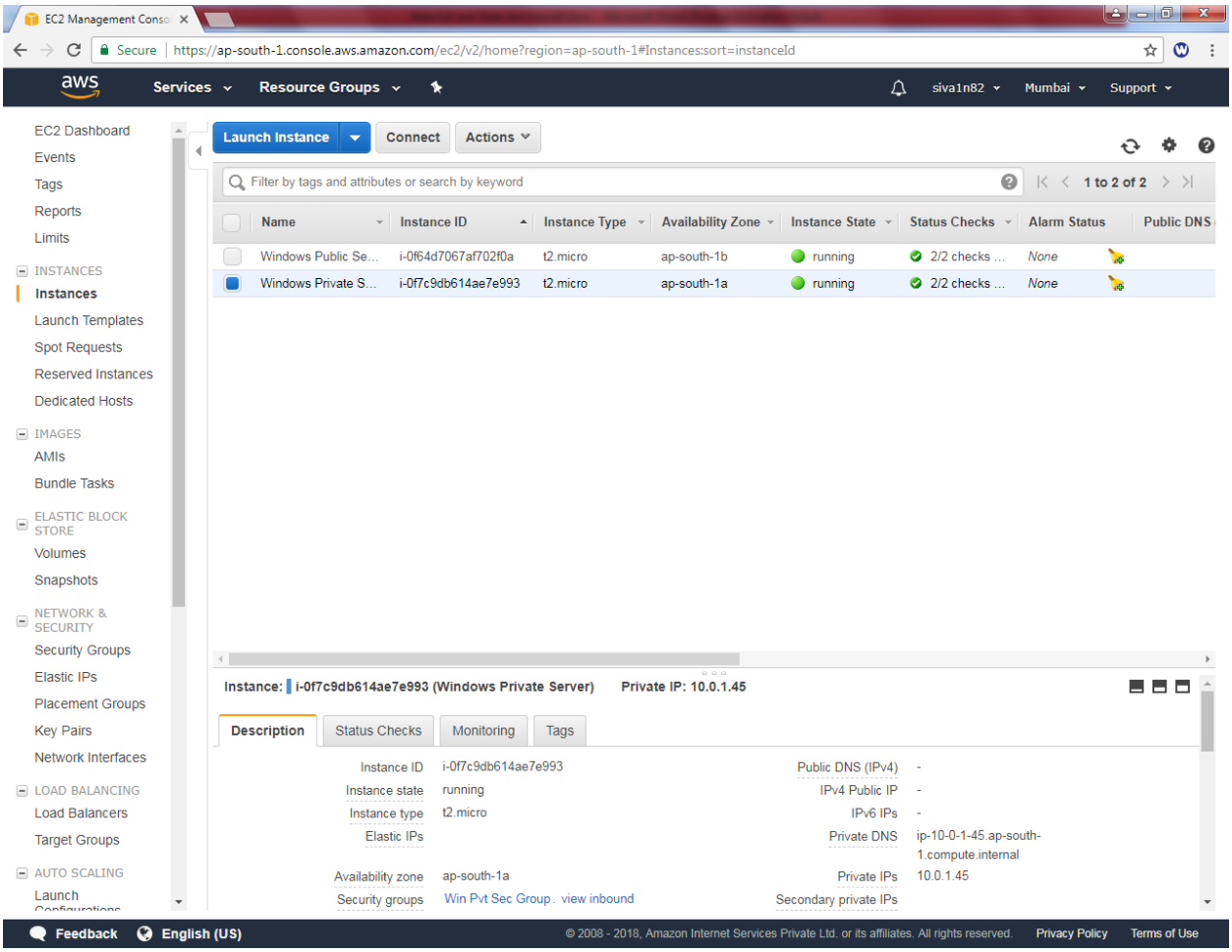


Click “Save”.

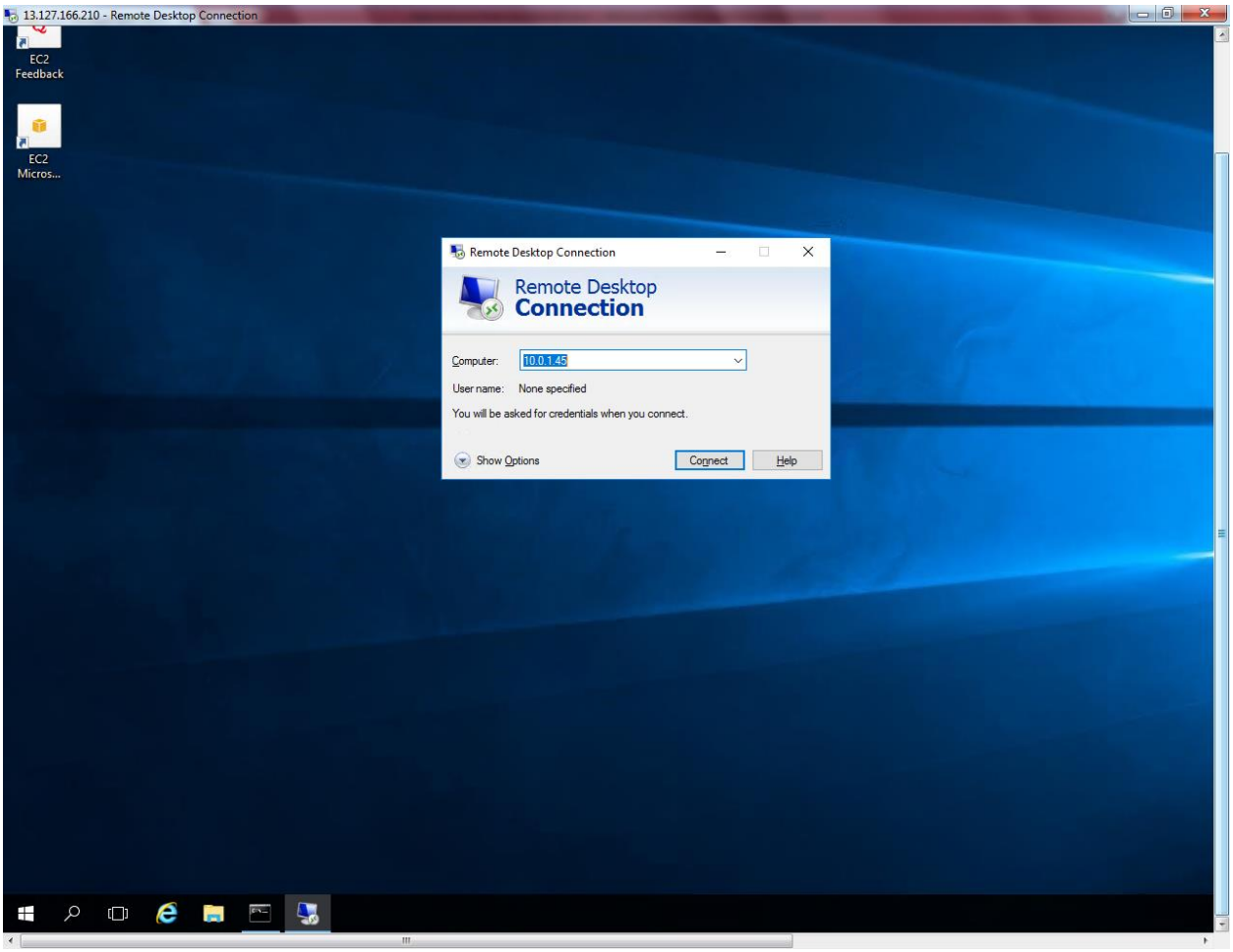
Again try to ping 10.0.1.45 we are unable to ping because windows firewall on private subnet server need to be turned off.

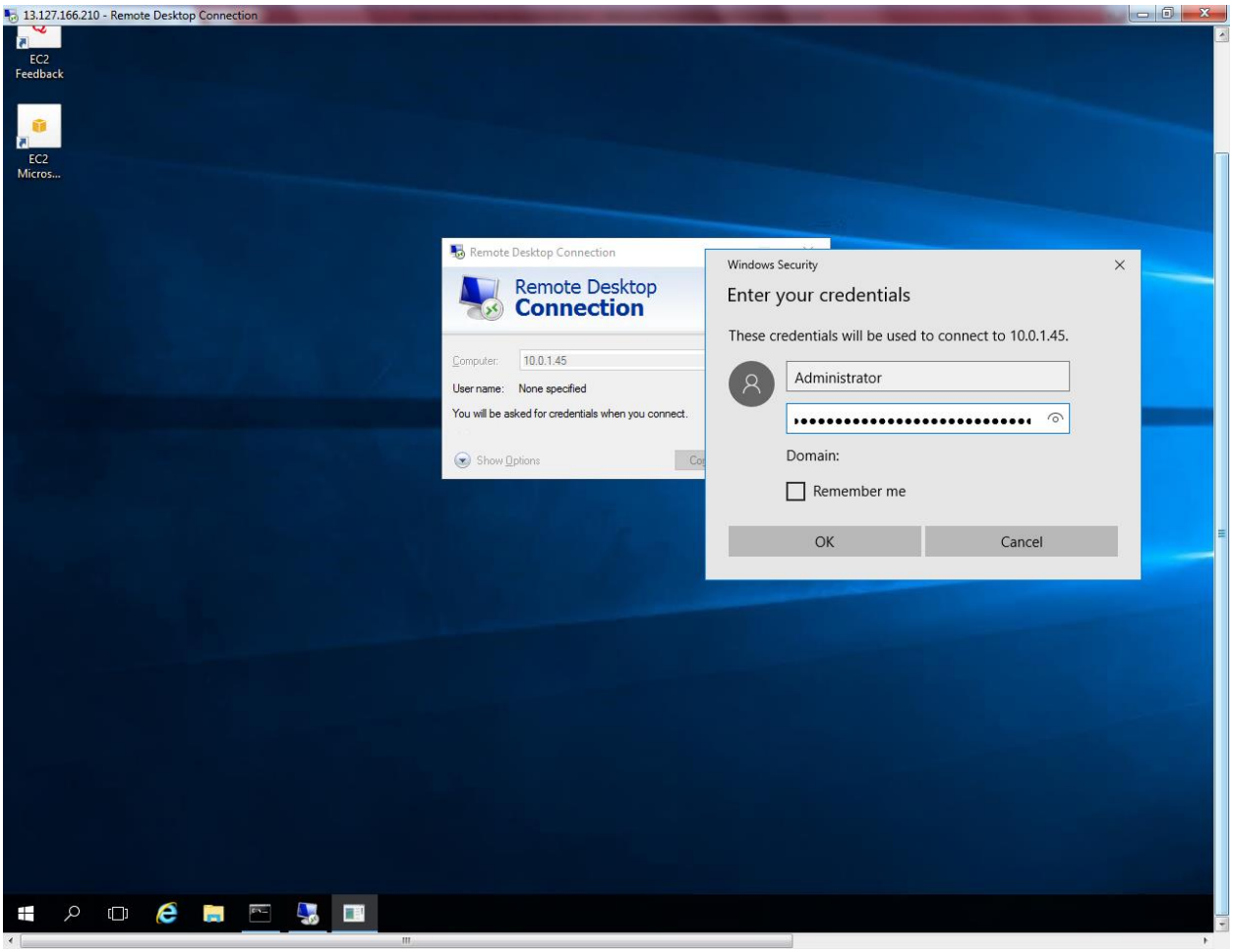


Get the IP address of private server from AWS management console.

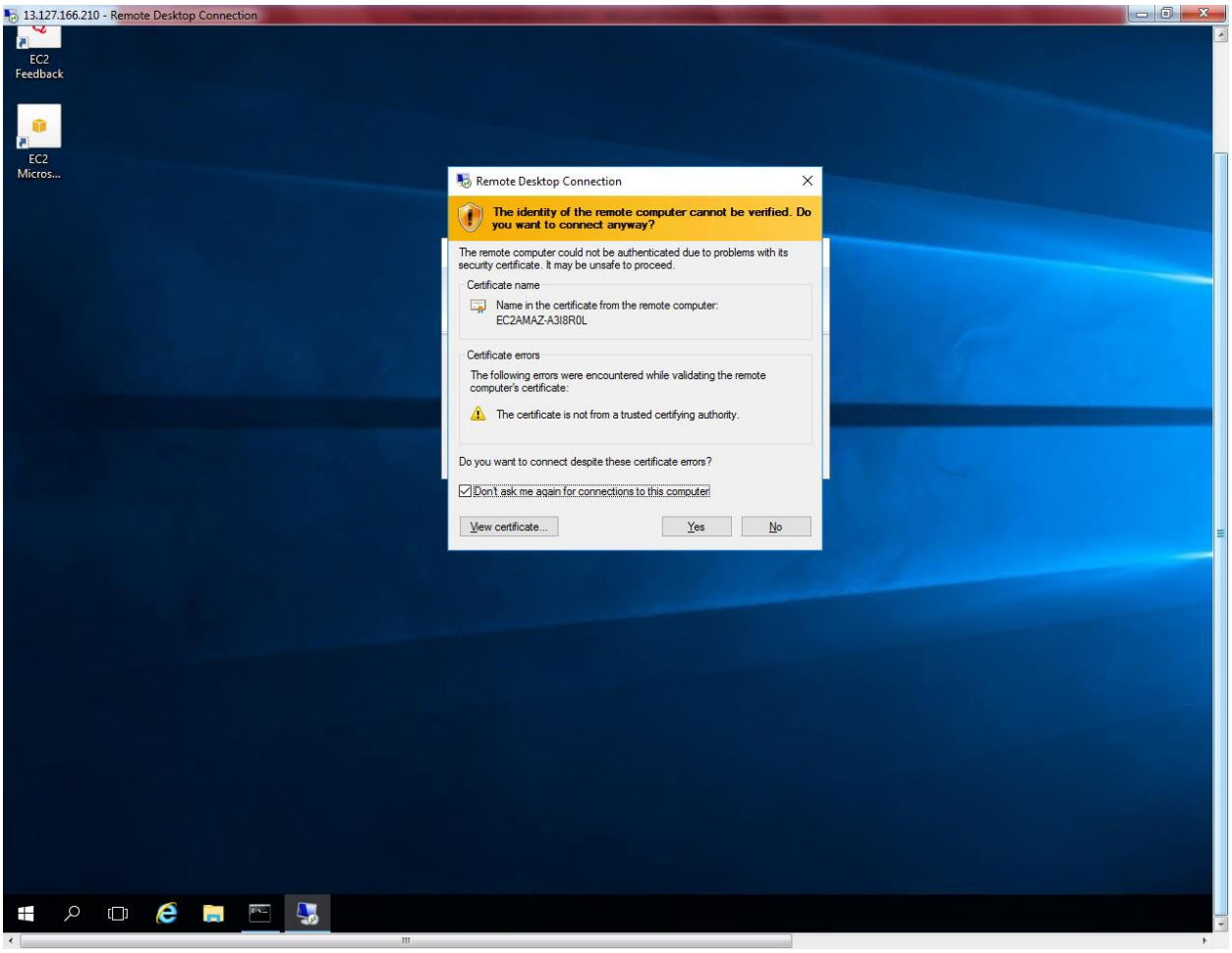


Try to connect private subnet server from public subnet server (10.0.1.45).

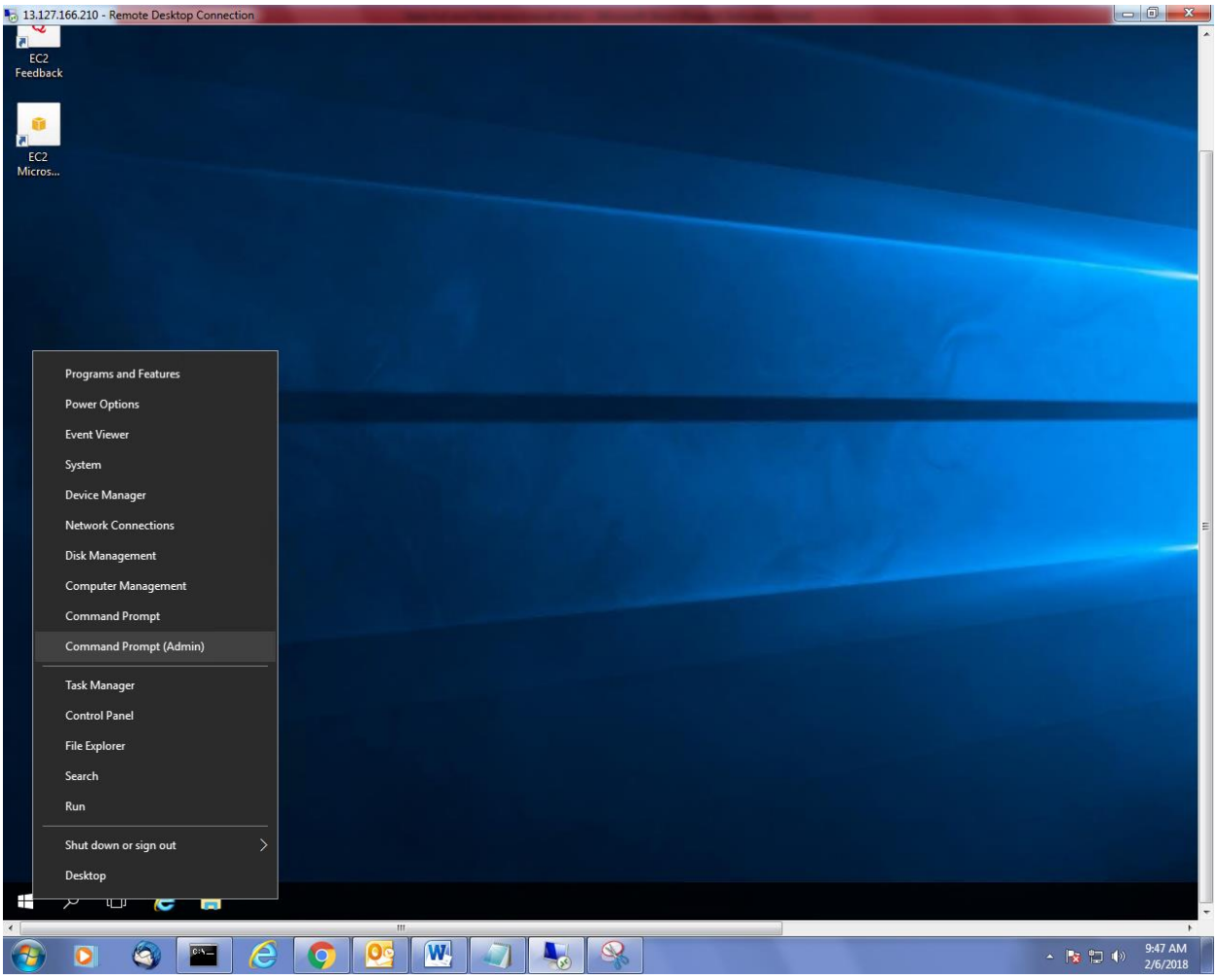



13.127.166.210 - Remote Desktop Connection
EC2 Feedback
EC2 Micros...
Remote Desktop Connection
Remote Desktop Connection
Computer: 10.0.1.45
User name: None specified
You will be asked for credentials when you connect.
Show Options
Windows Security
Enter your credentials
These credentials will be used to connect to 10.0.1.45.
Administrator
Domain:
Remember me
OK
Cancel

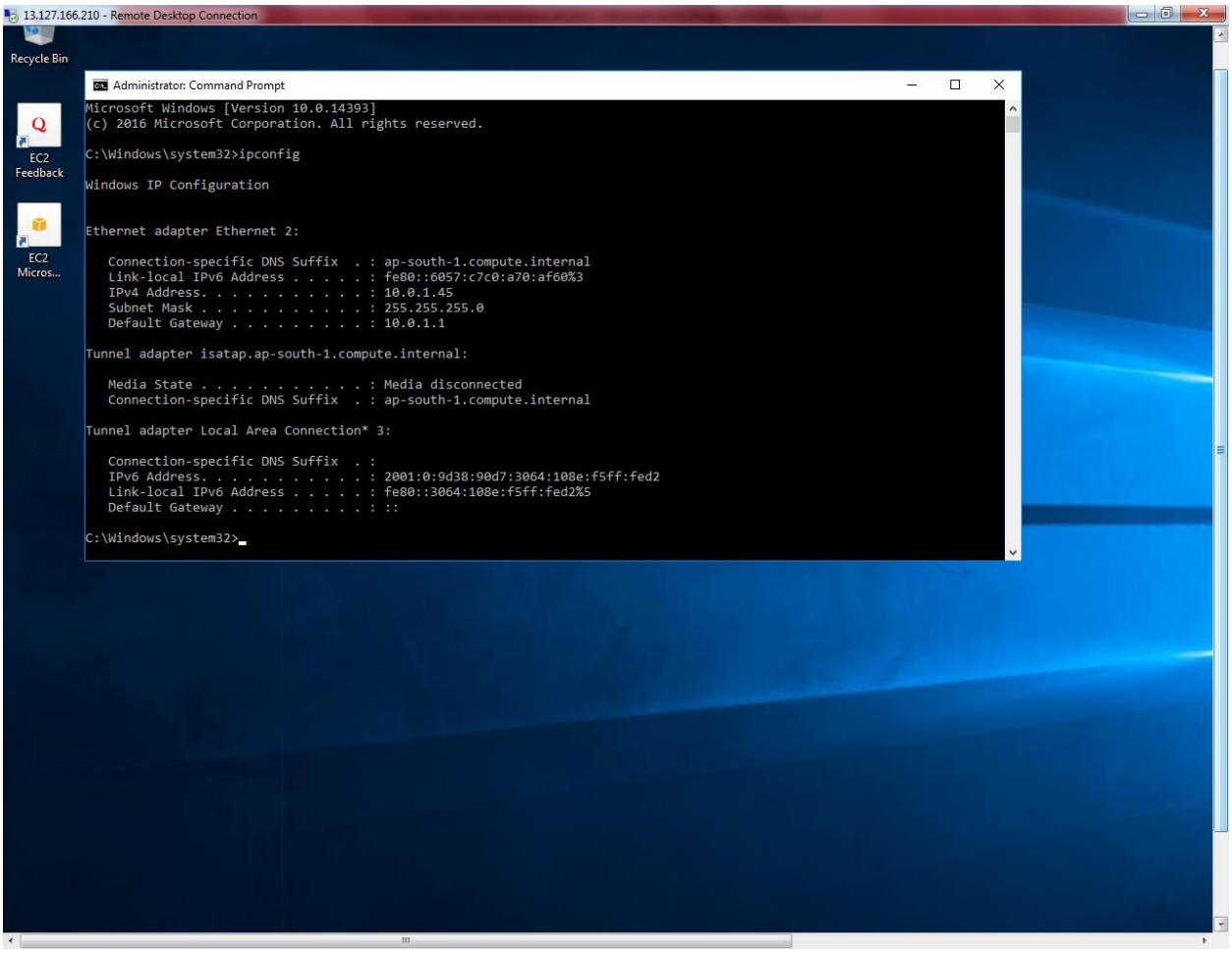
Click "Yes" to continue.



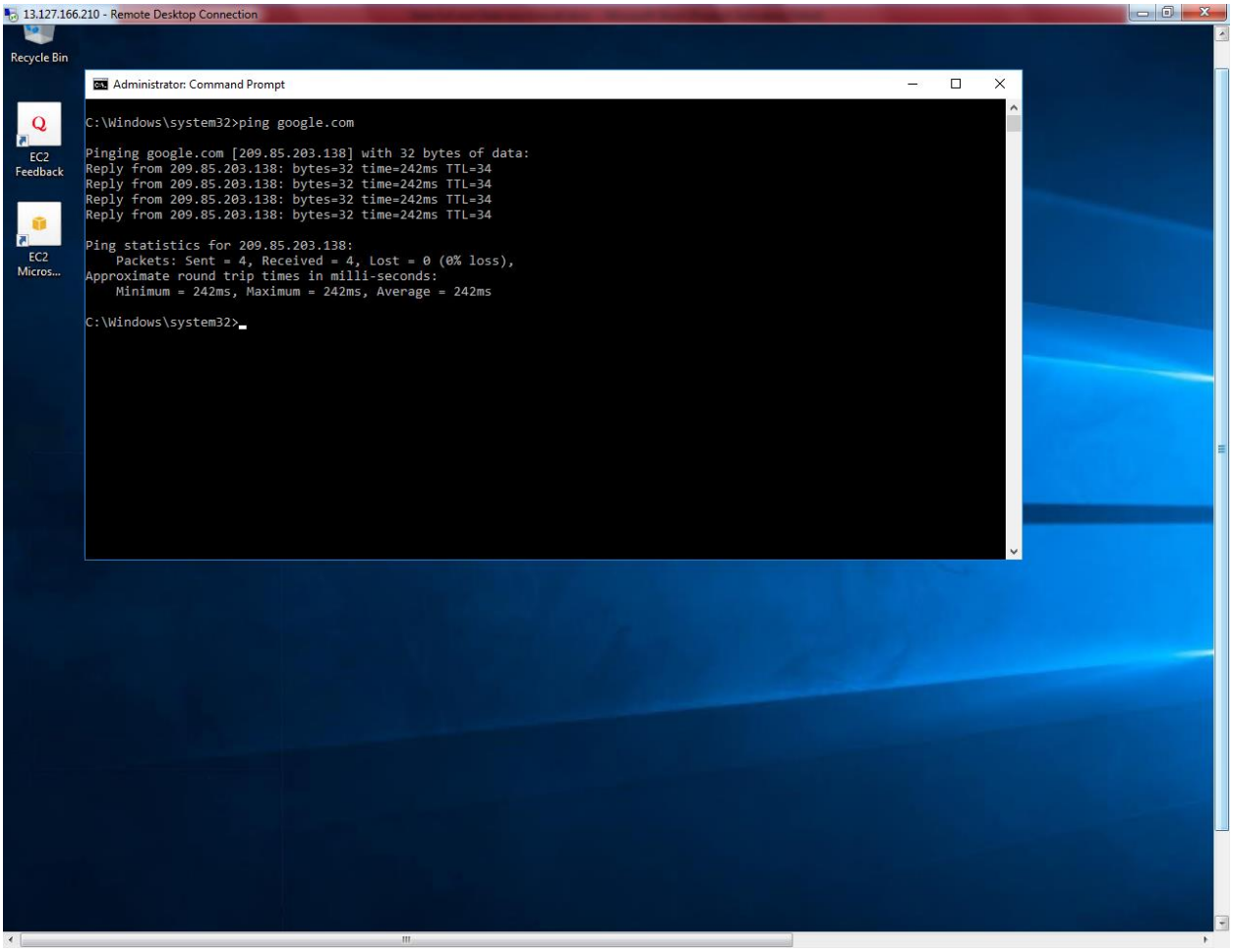
Right click start menu and click "Command prompt (Admin)"



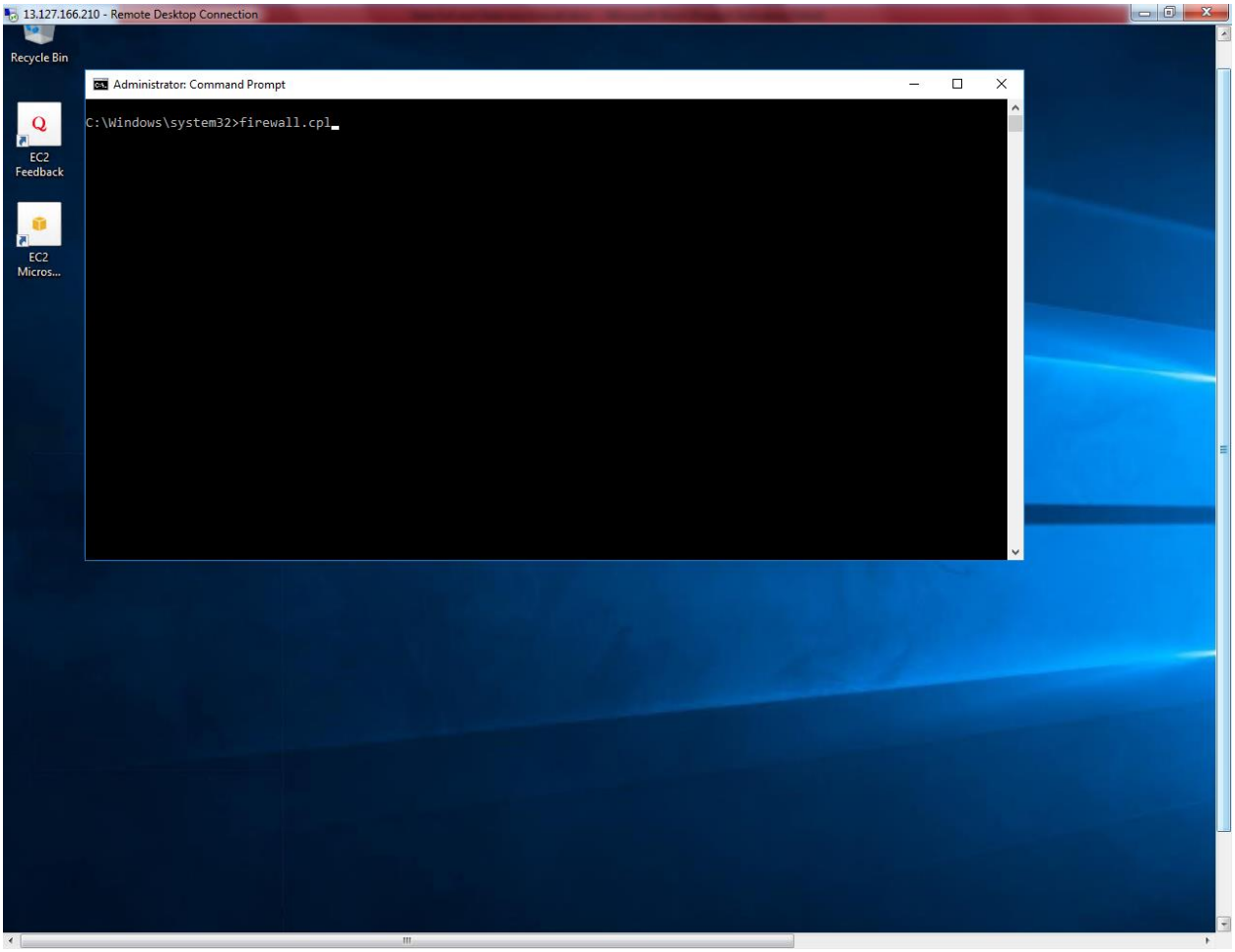
Type ipconfig in Private server.



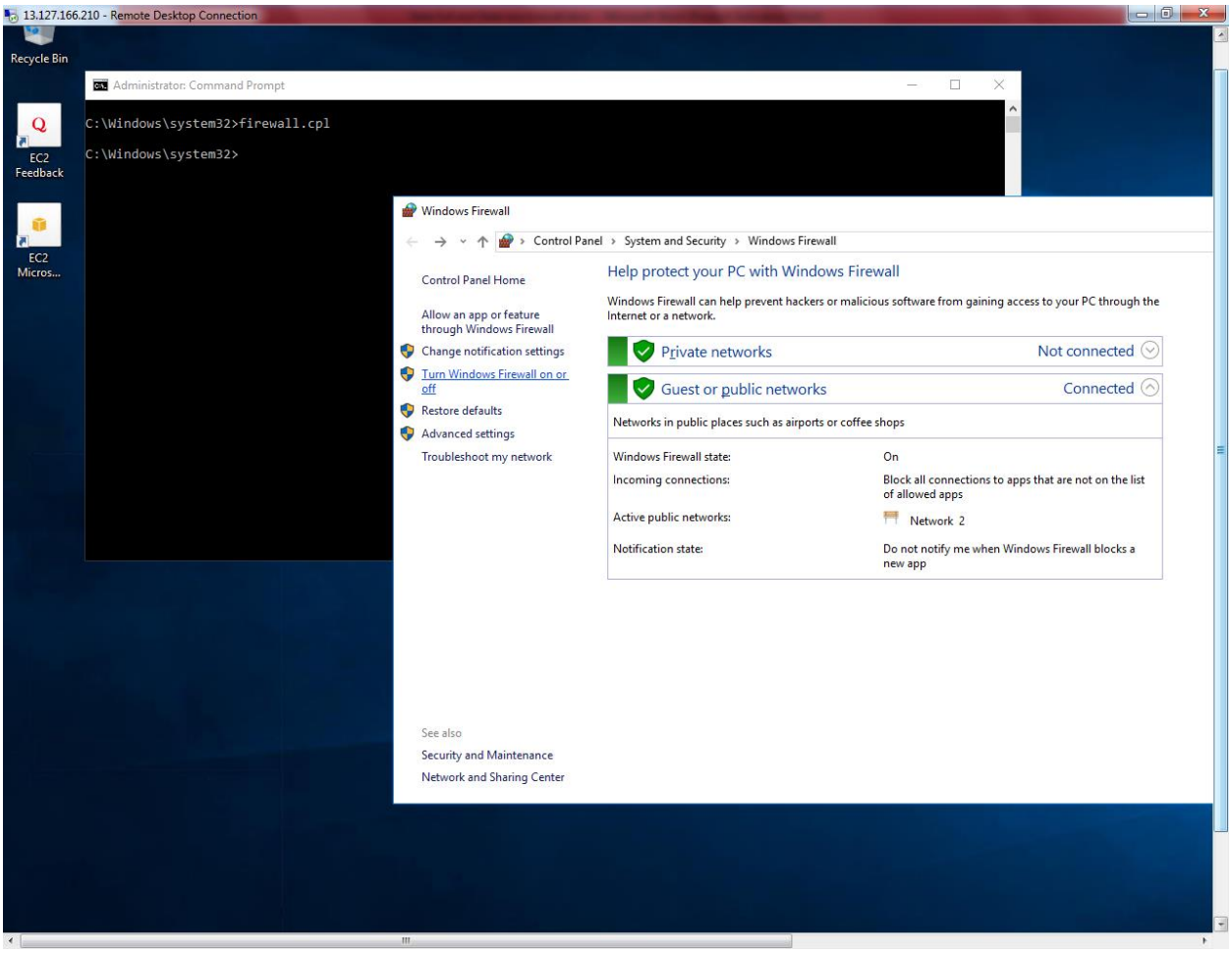
Type google.com in private subnet server. We are able to connect internet from private subnet by using NAT gateway.



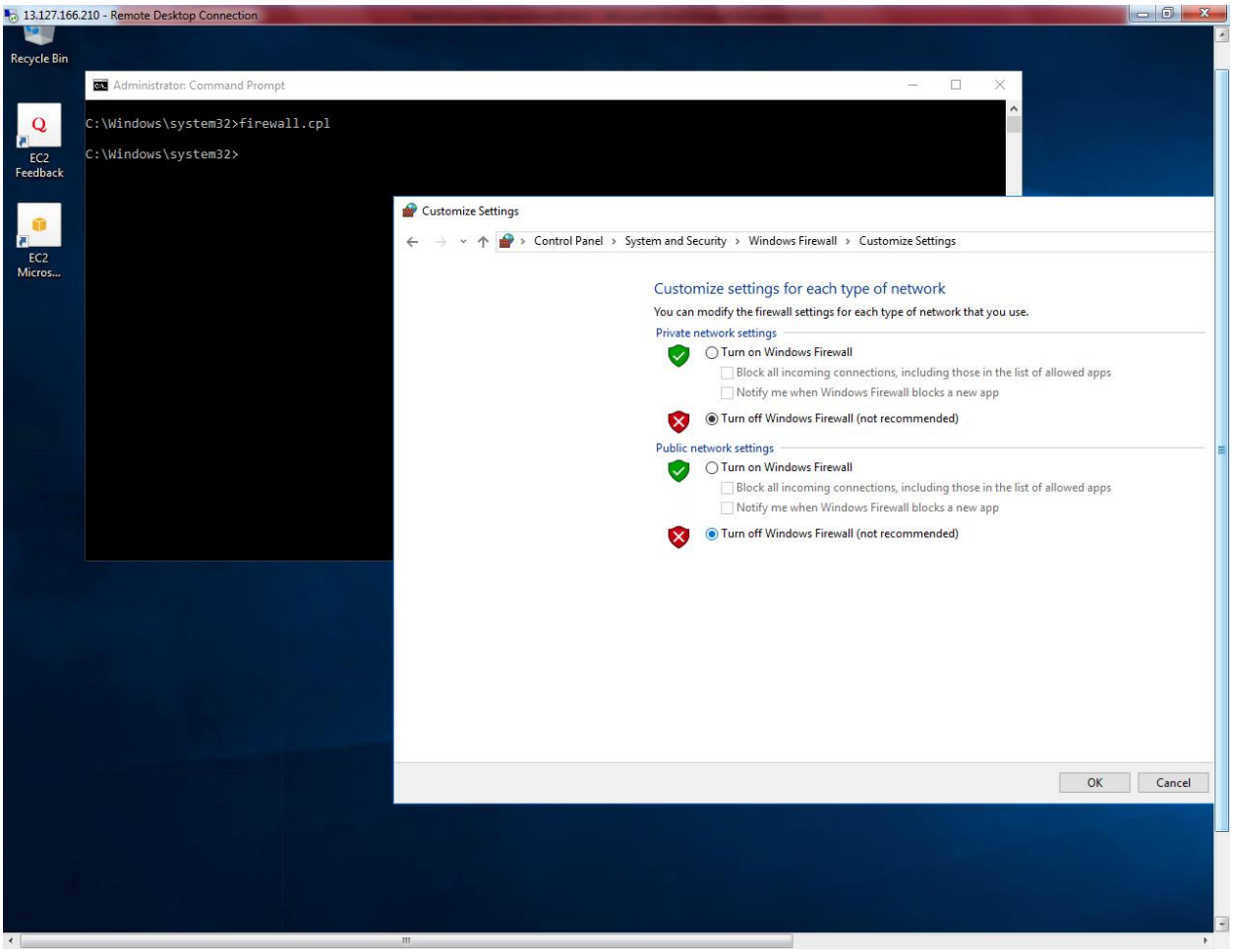
Type Firewall.cpl



Click "Turn Windows Firewall on or Off".

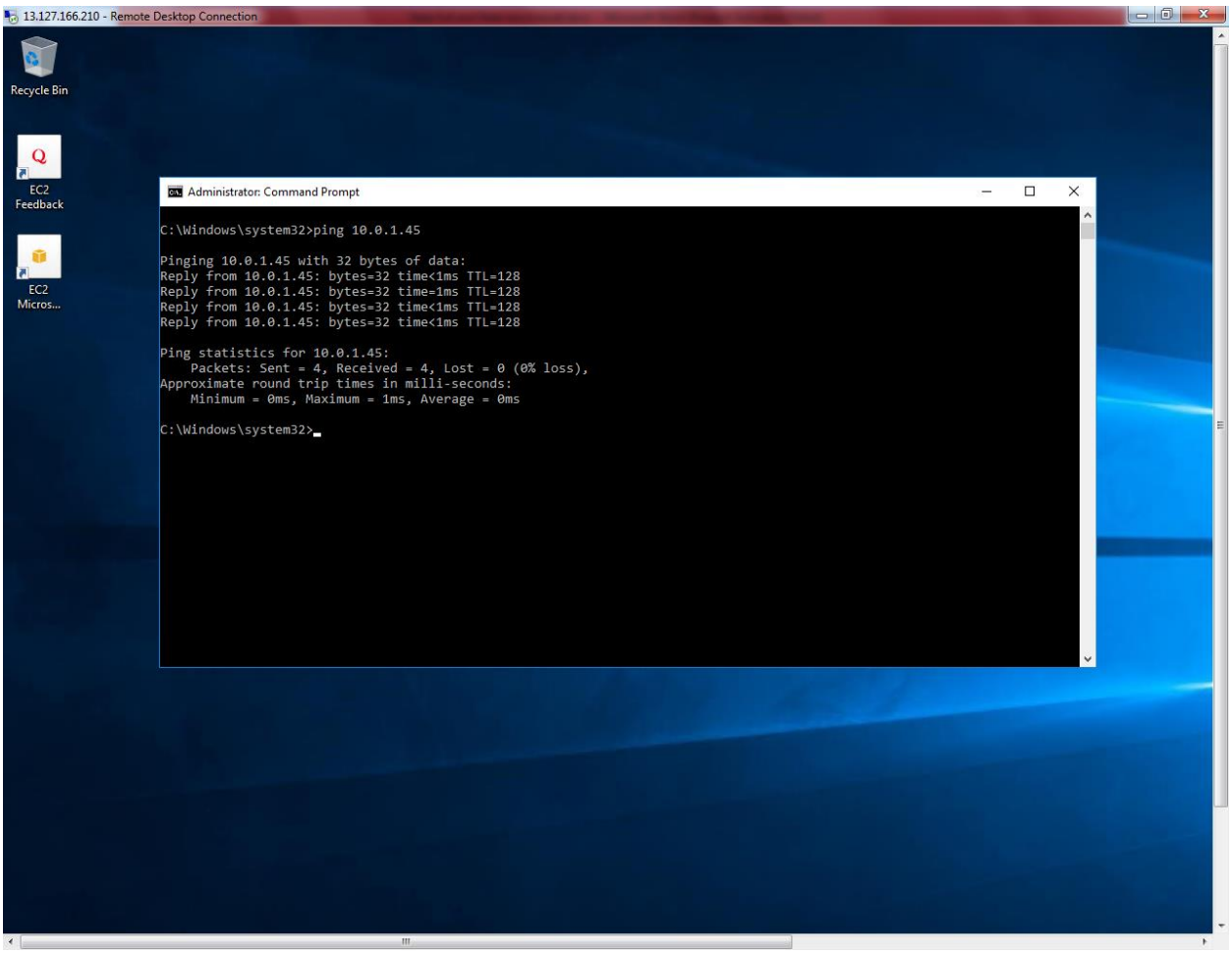


Turn off windows firewall.



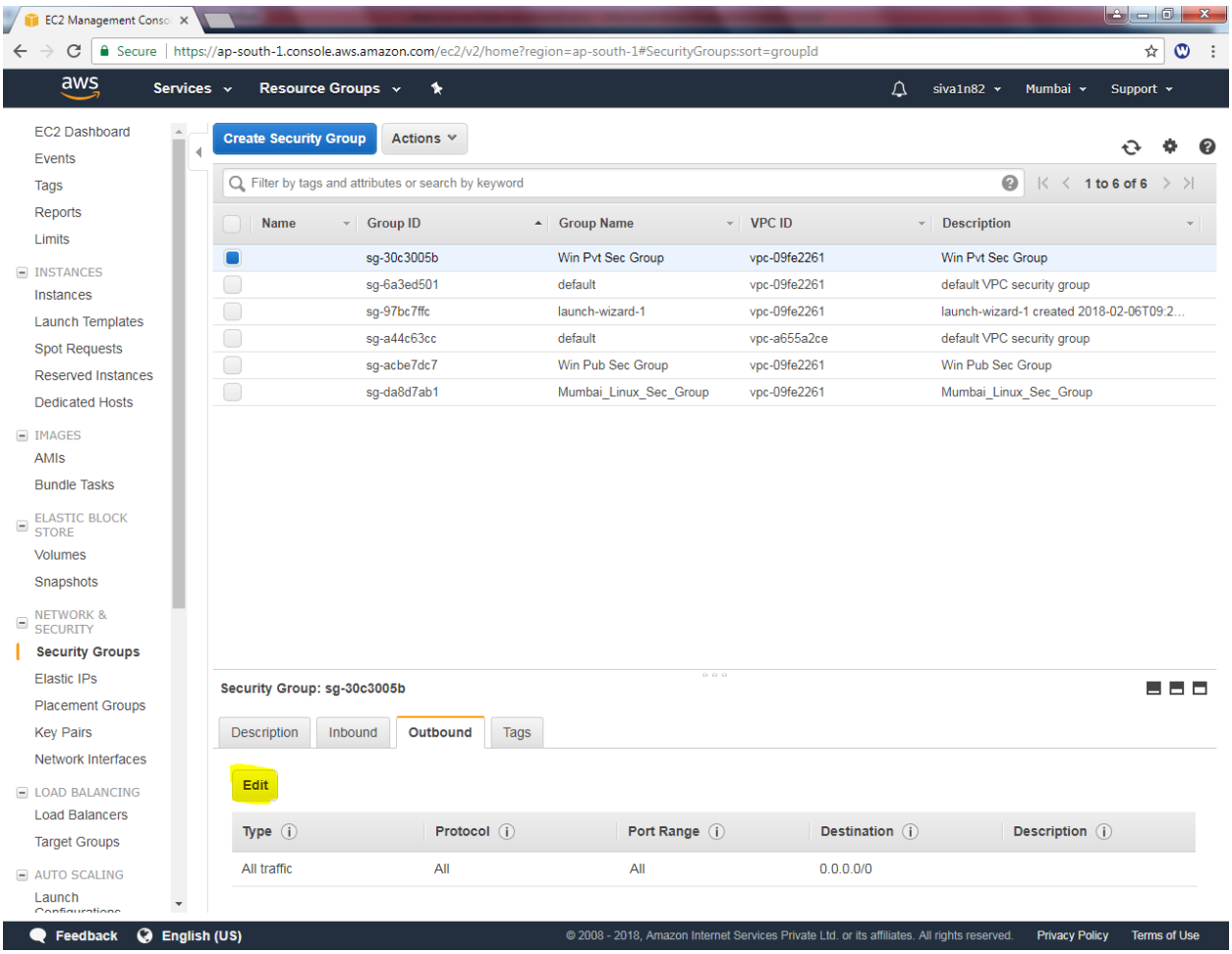
Click "Ok".

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.

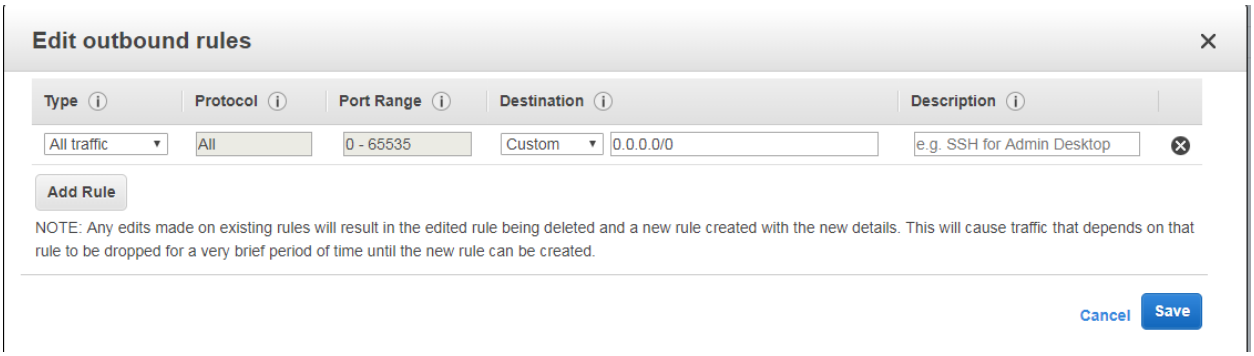


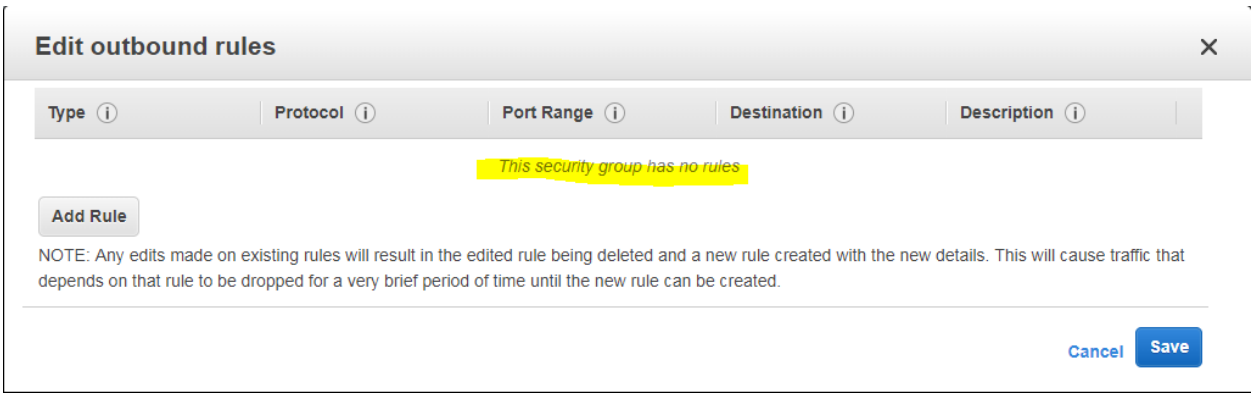
Now I am going to remove out bound rule from Win Pvt Sub Server security group.

Click "Edit".



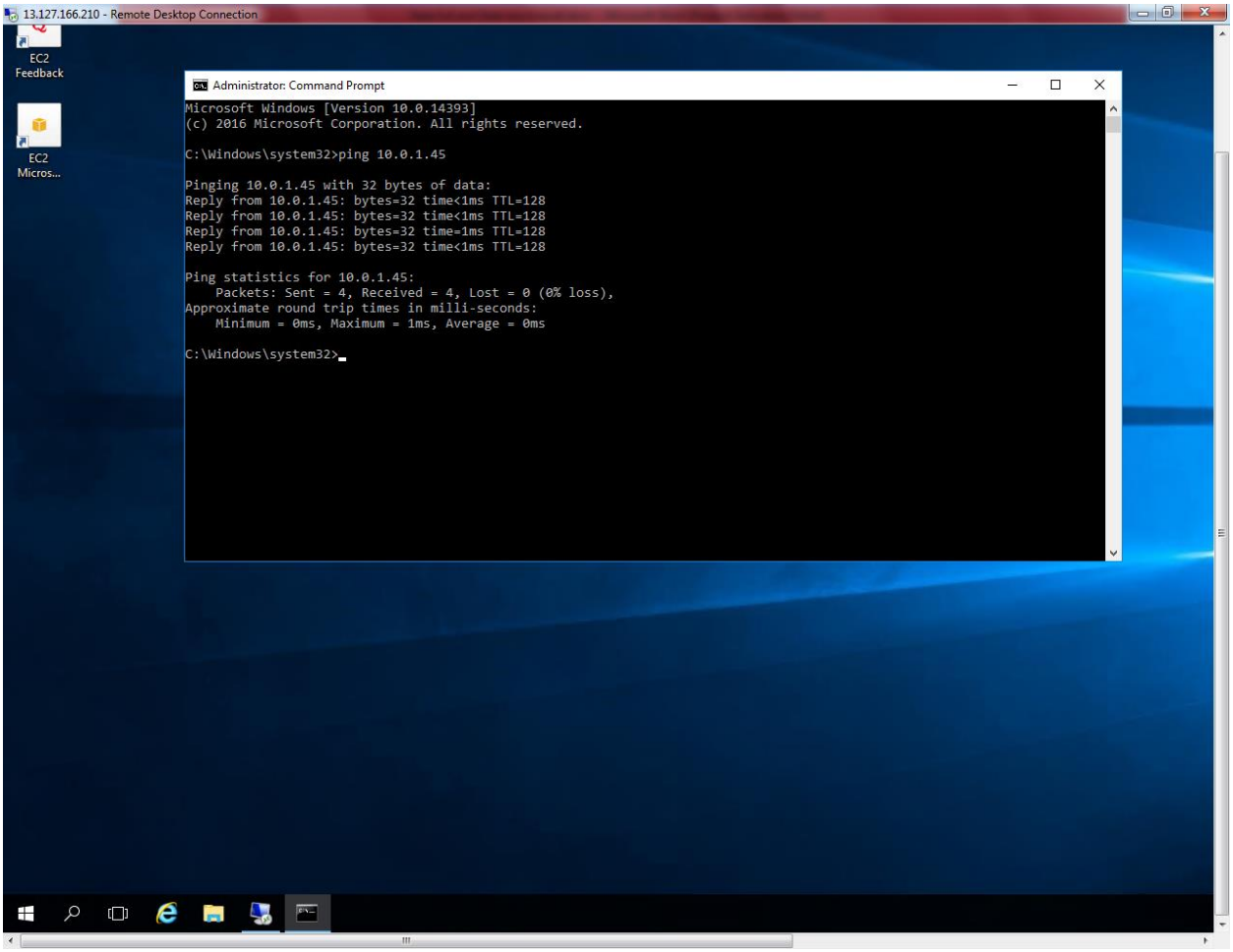
Click "X" mark to remove.





Click Save.

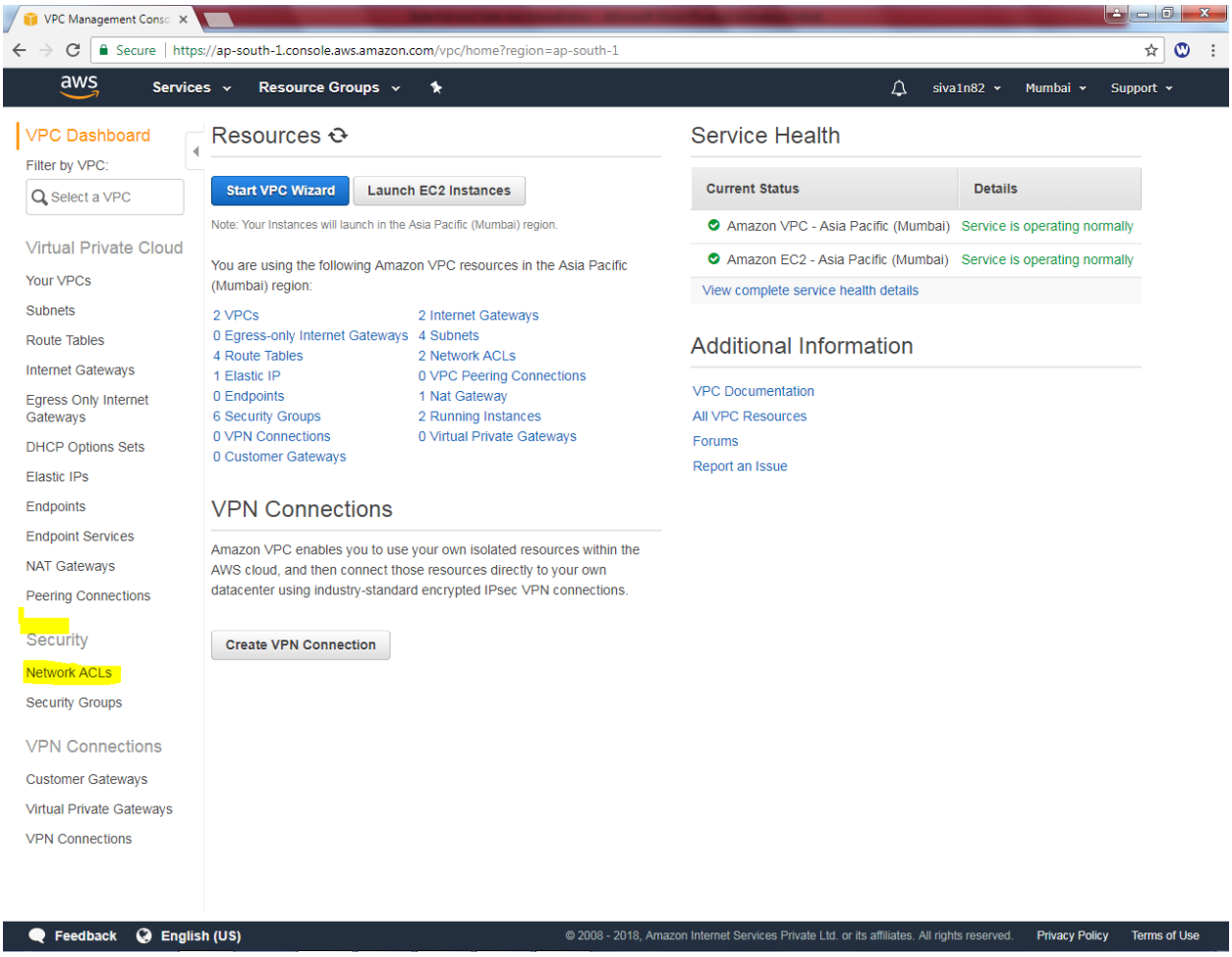
Now we are able ping 10.0.1.45 because security group is stateful firewall. While we permit ICMP rule in inbound that will allow the same traffic / ICMP in outbound also. It does not require any permission in outbound rule. Hence, we can able to ping 10.0.1.45 from public subnet.



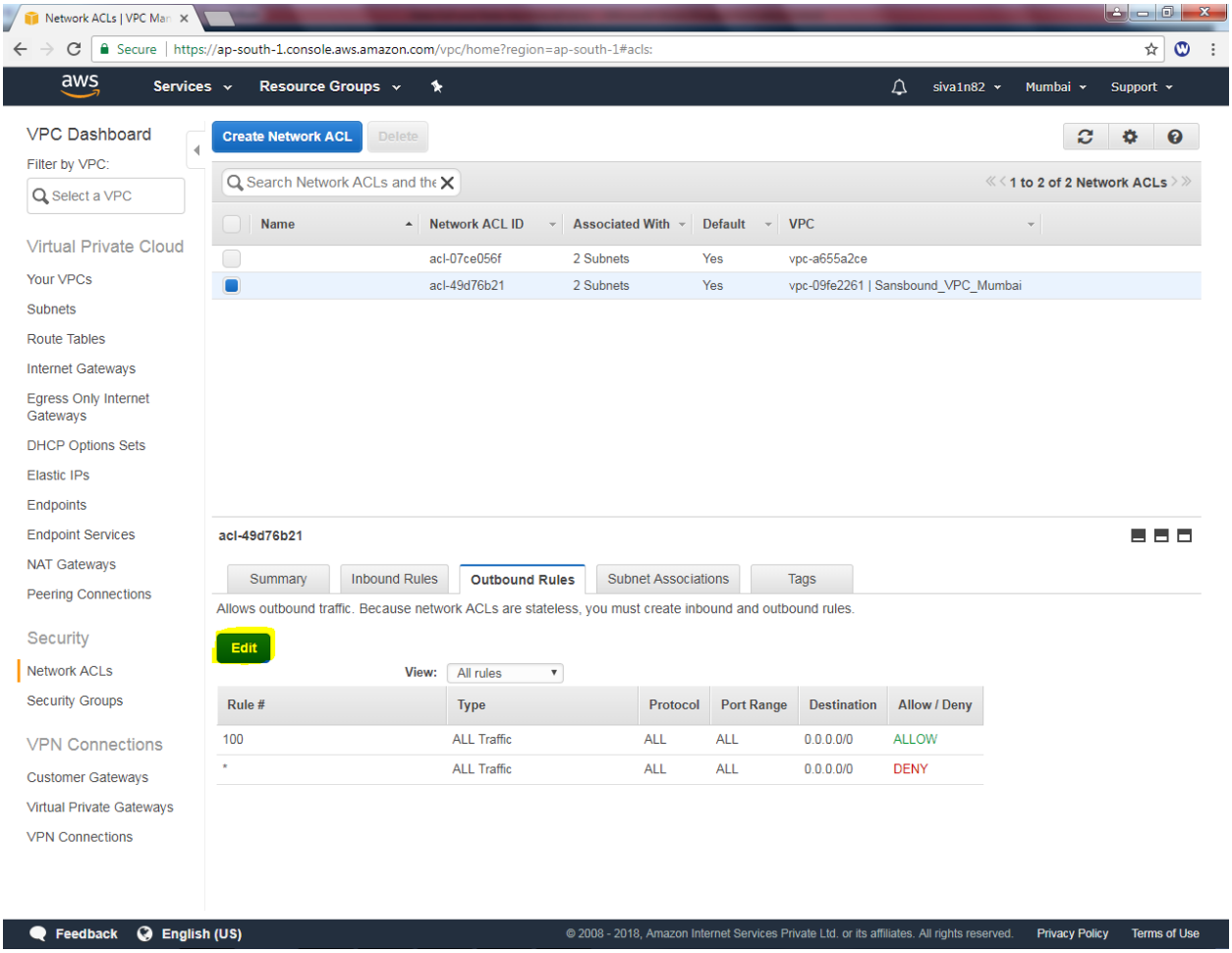
Then restore the outbound rule as default.

b) Stateless Firewall

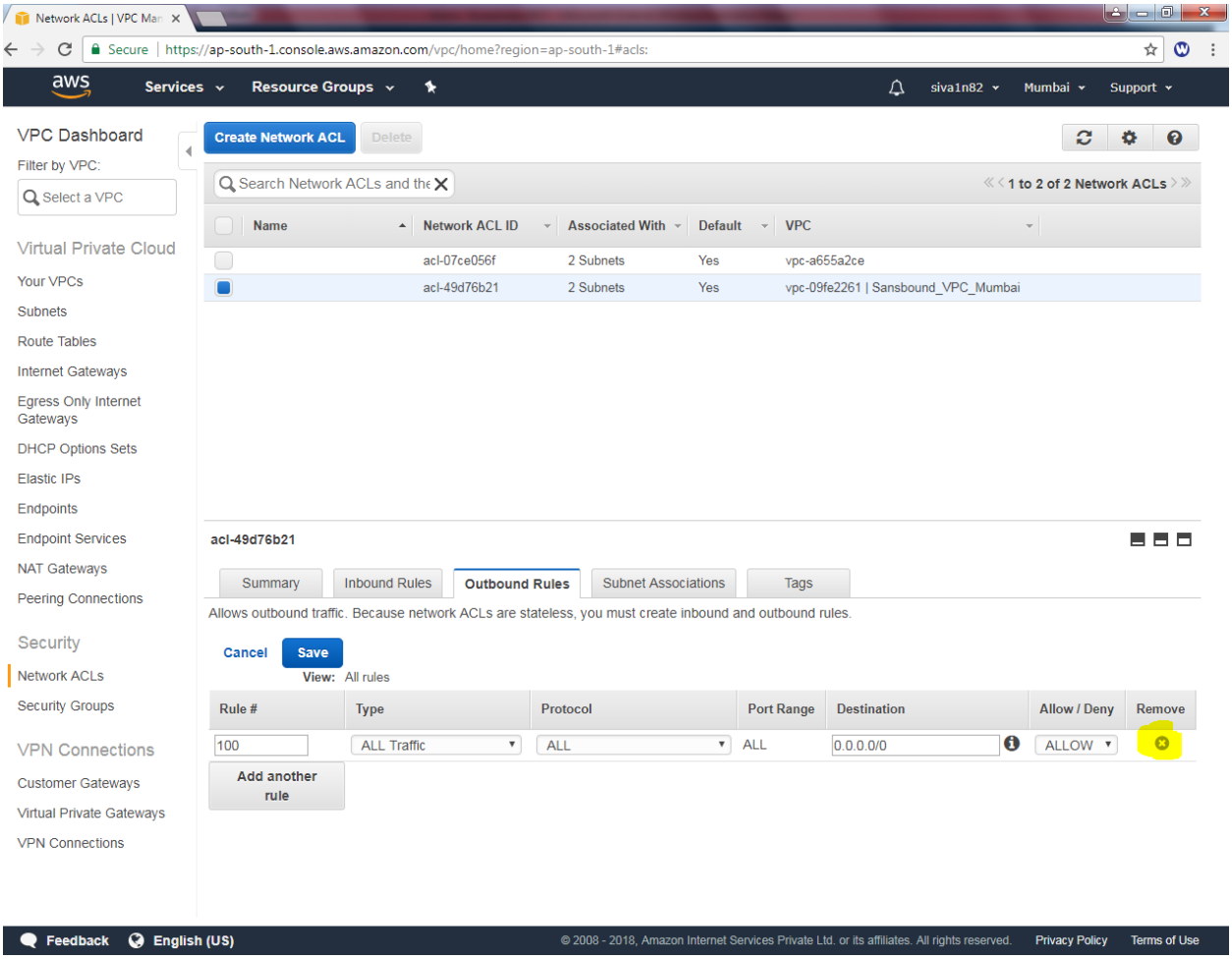
Goto “VPC” click Network ACLs.



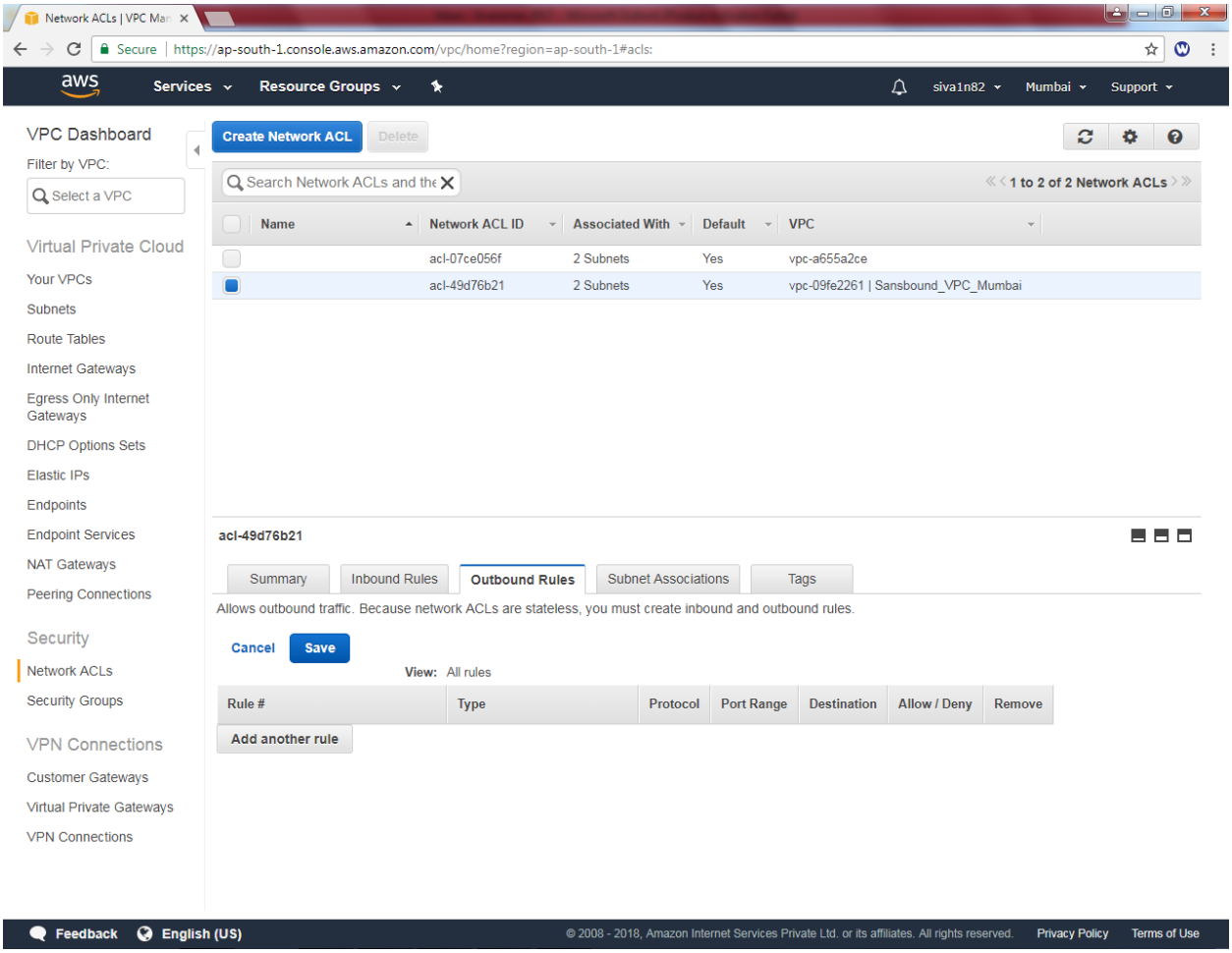
Click “Edit”.


Network ACLs | VPC Man
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
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
100
ALL Traffic
ALL
ALL
0.0.0.0/0
ALLOW
*
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

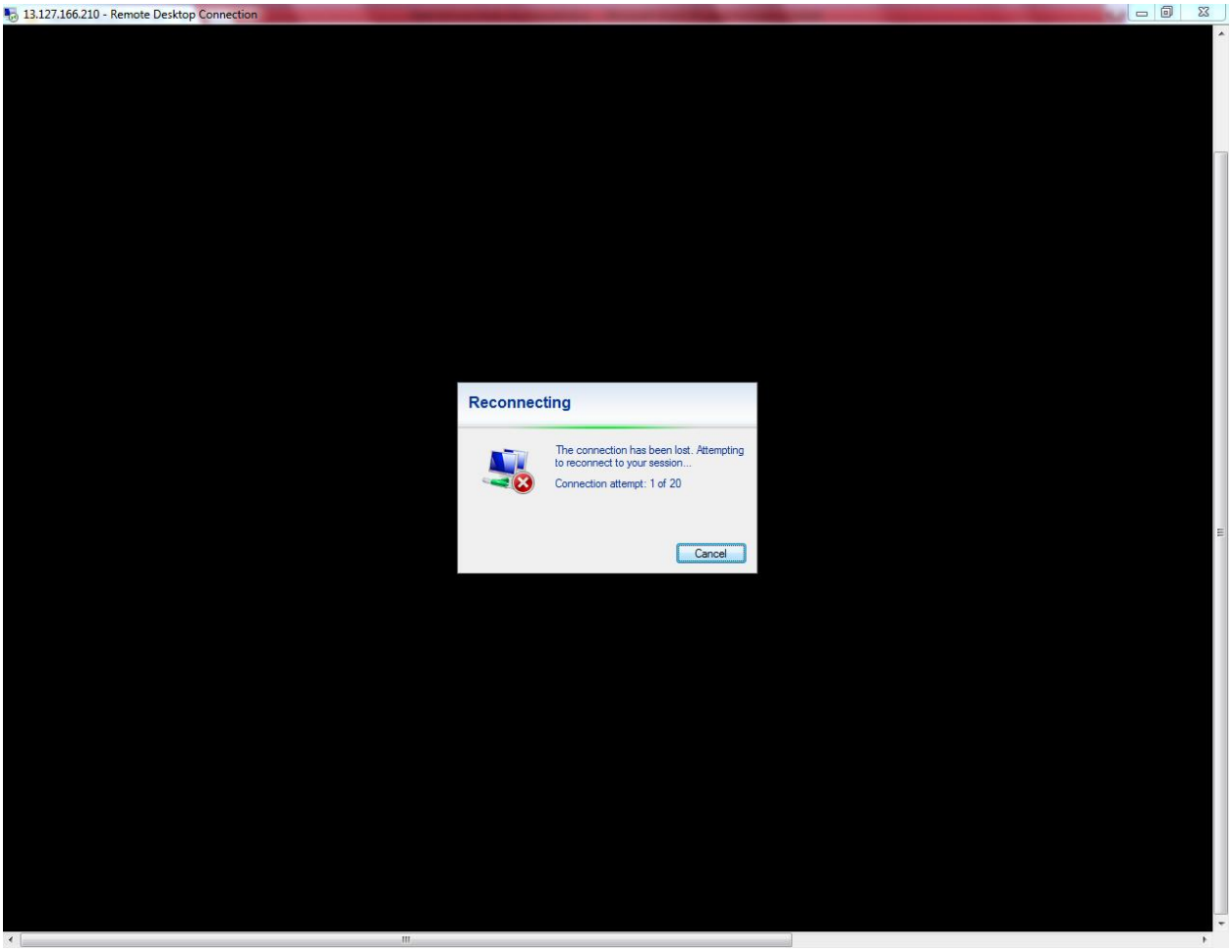
Click “highlighted area” to remove ACL.



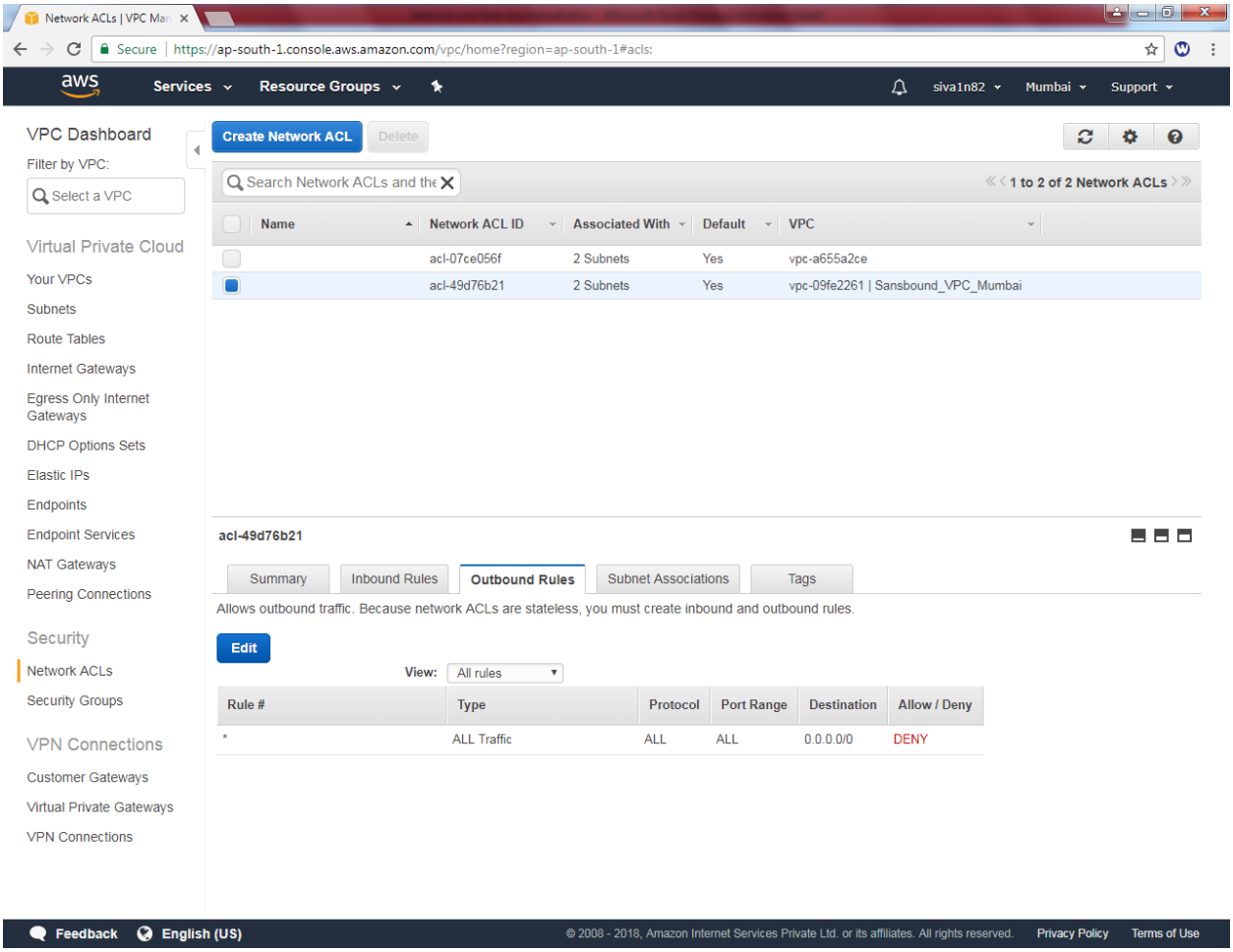
Click “save’.


Network ACLs | VPC Man
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
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

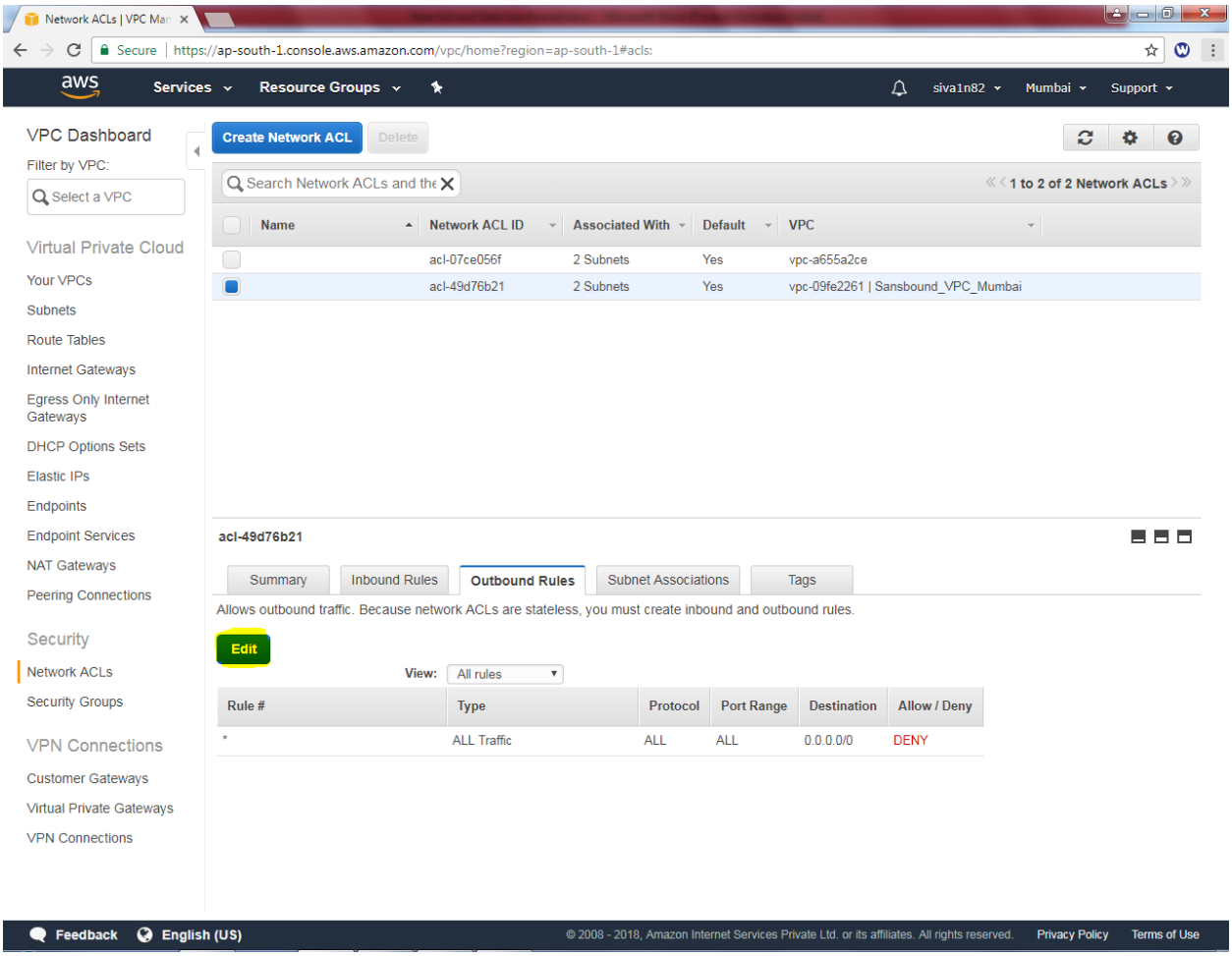
My remote desktop connection on public server has been disconnected. Because Network ACL was stateless firewall. We have permitted RDP (3389) TCP port in inbound rule. But, we have removed All traffic from outbound rule. Hence our remote connection has been removed. We need to provide outbound rule with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



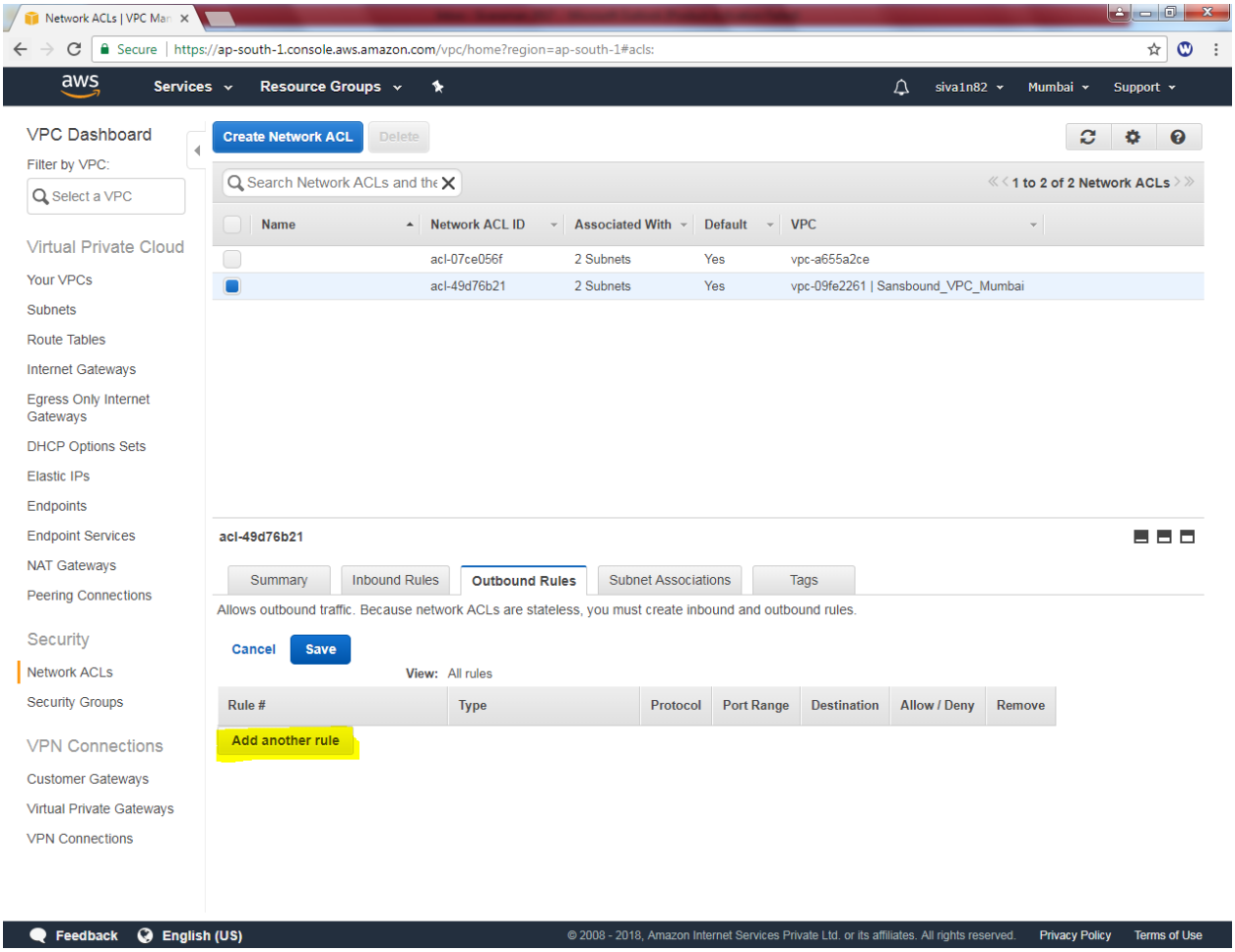
We could not able able to remove * rule / deny from Network ACL.



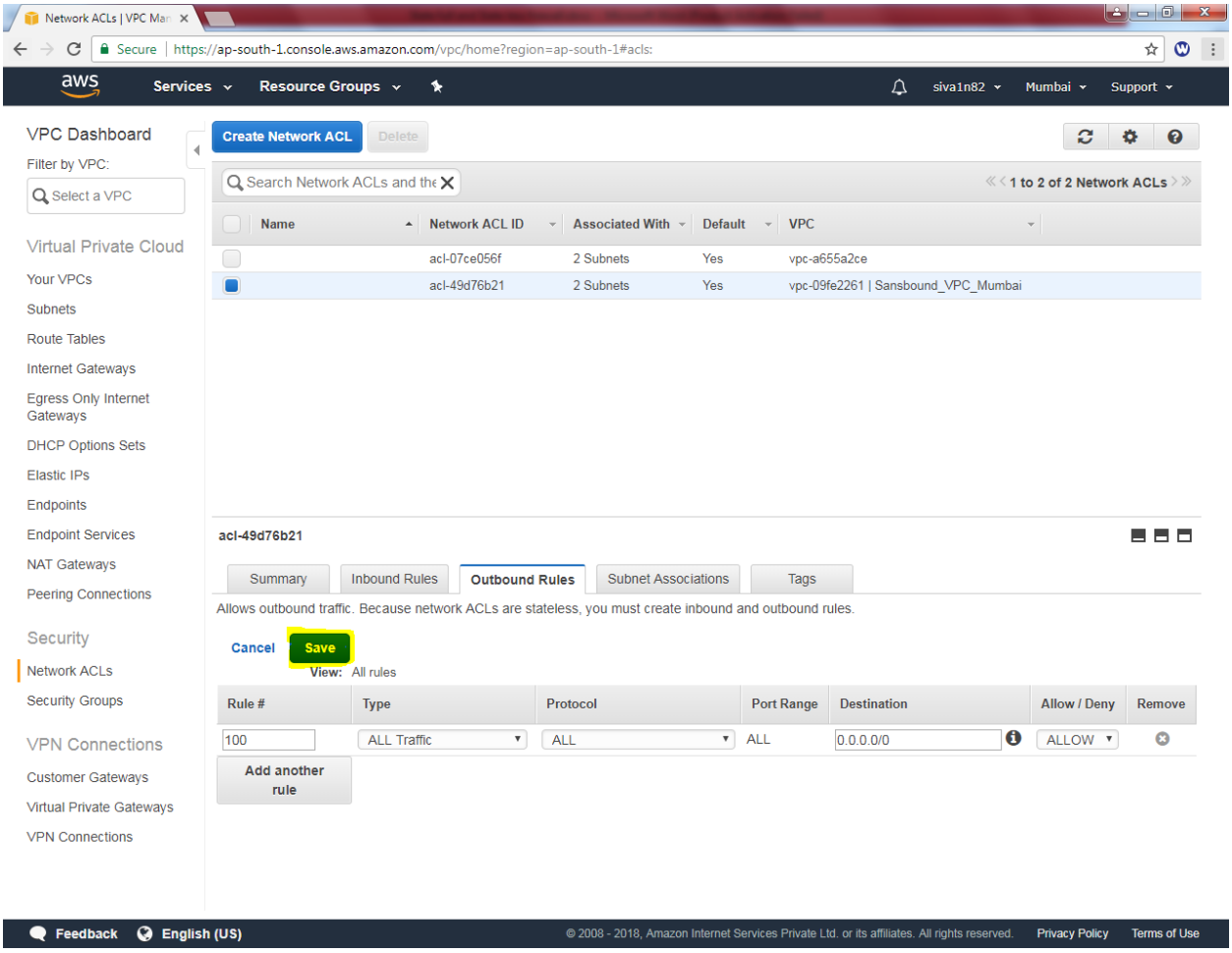
Click “Edit”.


Network ACLs | VPC Man
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
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”.



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



Now we can able to get RDP for public server.