



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

Step – 1 : Creating VPC .

- 1- Go to Amazon Management Console.
- 2 – Search For VPC Service.
- 3 – Click on Your VPCs in the left panel.
- 4 – Click on create VPC.
- 5 – In VPC Settings , Select VPC only in Resource to create.
- 6 – Name Your VPC.
- 7 – Select IPv4 CIDR manual input option .
- 8 – Give 10.0.0.0/16 as IPv4 CIDR .
- 9 – Select No IPv4 CIDR block option .

- 10 – Click on Create VPC .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC console interface. A success message at the top says "You successfully created vpc-099d02eb13cb1cff5 / my-vpc-ccsa-1121". The main panel displays the details of the newly created VPC, including its ID (vpc-099d02eb13cb1cff5), state (Available), and various network settings like CIDR blocks and route tables. Below the details, there's a "Resource map" section showing the VPC, Subnets, Route tables, and Network connections. The left sidebar lists other VPC-related options like Subnets, Route tables, and Internet gateways.

11 – Go to subnets in the left hand panel , click on it.

12 – Click on create Subnet .

13 – In VPC ID , select the VPC created above from dropdown .

14 – In Subnet settings , Name the subnet .

15 – Select Availability Zone as per choice .

16 – Select IPv4 VPC CIDR block as 10.0.0.0/16 .

17 – Set IPv4 subnet CIDR block as 10.0.0.0/24 .

18 – Click on create subnet .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the 'Create subnet' wizard in the AWS VPC console. In the 'VPC' section, the VPC ID is selected as 'vpc-099d02eb13cb1cff5 (my-vpc-ccsa-1121)'. Under 'Associated VPC CDRs', the IPv4 CIDR is set to '10.0.0.0/16'. The 'Subnet settings' section contains the following details:

- Subnet name:** my-subnet-09
- Availability Zone:** Asia Pacific (Mumbai) / ap-south-1b
- IPv4 VPC CIDR block:** 10.0.0.0/16
- IPv4 subnet CIDR block:** 10.0.0.0/24 (256 IPs)

At the bottom, there are 'CloudShell' and 'Feedback' buttons, and a status bar indicating the date and time.

This screenshot shows the same 'Create subnet' wizard with more detailed configurations. In addition to the basic settings, it includes:

- Tags - optional:** A tag named 'Name' is added with the value 'my-subnet-09'.
- IPv4 subnet CIDR block:** 10.0.0.0/24 (256 IPs)
- Create subnet** button at the bottom right.

The interface and status bar are identical to the first screenshot.



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

A screenshot of the AWS VPC Console. The main window shows a table titled "Subnets (1) Info" with one entry: "my-subnet-09". The table includes columns for Name, Subnet ID, State, VPC, IPv4 CIDR, and IPv6 CIDR. The Subnet ID is highlighted. The left sidebar shows navigation options like "Virtual private cloud", "Security", and "Network Firewall". The bottom status bar indicates the session is from "ap-south-1.console.aws.amazon.com" and shows system icons.

19 – Go to Internet Gateway in the left panel and click on it .

20 – Click on create internet gateway .

21 – Name the internet gateway .

22 – Click on create in internet gateway .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot displays two windows from the AWS VPC console.

The top window is titled "Create internet gateway | VPC". It shows the "Internet gateway settings" section. A "Name tag" field contains "my-ig-1121". Below it, a "Tags - optional" section shows a single tag "Name" with value "my-ig-1121". At the bottom right is a yellow "Create internet gateway" button.

The bottom window is titled "InternetGateway | VPC Console". It shows the "Details" tab for the created internet gateway. The "Internet gateway ID" is "igw-09f02328069122278" and the "Name" is "my-ig-1121". The "State" is "Detached". The "Owner" is listed as "891577273585". The "Actions" dropdown menu includes "Attach to a VPC".

23 – Select the internet gateway you created .

PRN: 20220801121



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

24 – Go to Action at top right corner and click on it .

25 – Click on Attach to VPC .

The screenshot shows the AWS VPC Console with the 'Internet gateways' section selected. There are two entries: 'demo-gateway' (Attached to VPC ID 'vpc-08fffe06795a9ec200') and 'my-ig-1121' (Detached). The 'Actions' menu is open over the 'my-ig-1121' entry, with 'Attach to VPC' highlighted in orange. The 'Details' tab is selected for 'my-ig-1121', showing its configuration.

26 – Select the VPC you created above .

27 – Click on Attach internet gateway .



School of Computer Science, Engineering and Applications(SCSEA) B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma PRN: 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the 'Attach to VPC' dialog box. It has a search bar containing 'vpc-099d02eb13cb1cff5'. Below the search bar, there is a note: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the Internet. Specify the VPC to attach below.' A list of available VPCs is shown, with one item selected: 'vpc-099d02eb13cb1cff5'. At the bottom right of the dialog box is a yellow 'Attach internet gateway' button.

The screenshot shows a confirmation message: 'Internet gateway igw-09f02328069122278 successfully attached to vpc-099d02eb13cb1cff5'. The message is preceded by a green circular icon with a checkmark. The background shows the AWS VPC dashboard with the 'Internet gateways' section expanded, showing the attached gateway.

28 – Go to route table at the left panel , click on it .

PRN: 20220801121



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

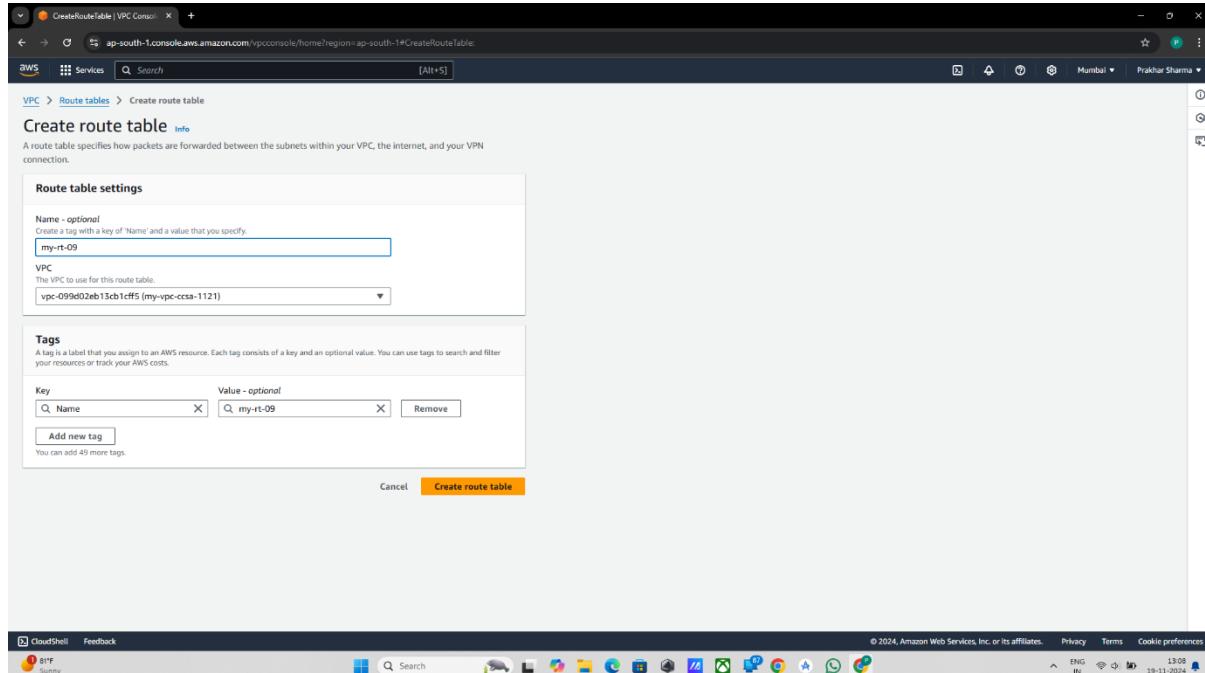
Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

29 – Name the Route table .

30 – Select the VPC you created from the dropdown .

31 – Click on route table .





School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Route Table Details page. The route table 'rtb-01e1e074b8be8978a / my-rt-09' has been created successfully. The 'Details' tab is selected, showing the route table ID, Main status (No), Owner ID (891377273858), and VPC (vpc-099d02eb13cb1cff5 | my-vpc-ccsa-1121). The 'Routes' tab displays one route entry: Destination 10.0.0.0/16, Target local, Status Active, and Propagated No.

32 – Click on the route table you created .

33 – At the bottom , Go to Subnet Association .

34 – Click on edit subnet association .

35 – Select the subnet and click on save association .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

PRN: 20220801121

1
0



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

36 – Now Go to routes tab at the bottom .

37 – Click on edit route .

38 – Click on add rule .

39 – Select Destination as 0.0.0.0/0 .

40 – In target, Select internet gateway and select the internet gateway created above .

41 – Click on save changes .

The screenshot shows the AWS VPC Edit Routes interface. A new route is being added to a route table. The destination is set to 10.0.0.0/16, the target is set to 'local', and the status is 'Active'. The target dropdown also shows 'Internet Gateway' and 'igw-09f02328069122278' selected. The 'Save changes' button is highlighted.



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Route Table Details page. A green banner at the top indicates that routes were updated successfully. The main section displays the details of a route table named 'rtb-01e1e074b8be8978a / my-rt-09'. It lists two routes: one to an internet gateway (igw-09f02328069122278) and one to a local subnet. The interface includes tabs for Routes, Subnet associations, Edge associations, Route propagation, and Tags.

42 – Search for EC2 service .

43 – Click on EC2 .

44 – Click on Launch Instance .

45 – Name the instance .

46 – Select AMI as Windows 2022 Base (Free Tier Eligible) .

47 – Select instance type as t2 micro .

48 – Create key pair .



School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma PRN: 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The user has selected the 't2.micro' instance type, Microsoft Windows Server 2022 AMI, and 1 volume (30 GB). A 'Free tier' callout indicates that the first year includes 750 hours of t2.micro usage in the US East (N. Virginia) Region. The 'Launch Instance' button is visible at the bottom right.

The screenshot shows the 'Instance type' selection screen. The user has chosen the 't2.micro' instance type. A modal window titled 'Create key pair' is open, prompting the user to enter a key pair name ('vpc-1121') and select a key pair type (RSA). The 'Create key pair' button is highlighted.

PRN: 20220801121

1
3



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS EC2 'Launch an instance' wizard. In the 'Instance type' section, a t2.micro instance is selected. In the 'Key pair (login)' section, 'vpc-1121' is chosen. Under 'Network settings', the network 'vpc-05ffe06795a9ec200' and subnet 'No preference' are selected. The 'Launch Instance' button is highlighted in orange at the bottom right.

49 – In Network Settings , click on edit .

50 – Select the VPC created above .

51 – Select the subnet .

52 – Enable auto assign public ip .

53 – Select create Security group .

PRN: 20220801121



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS EC2 console interface for launching a new instance. In the 'Network settings' section, a VPC named 'vpc-099d02eb13cb1cff5 (my-vpc-ccsa-1121)' is selected. A subnet named 'my-subnet-09' is chosen. Under 'Auto-assign public IP', 'Enable' is selected. In the 'Firewall (security groups)' section, a new security group named 'launch-wizard-2' is being created. The 'Inbound Security Group Rules' section shows a single rule: Type 'rdp', Protocol 'TCP', Port range '3389', and Source type 'Anywhere'. A tooltip for the 'Free tier' is visible, stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GiB of bandwidth to the internet.' At the bottom right, there are 'Cancel', 'Launch Instance', and 'Preview code' buttons.

54 - Add security group rule .

55 – Type : All traffic , Source type : Anywhere .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS EC2 Launch Instance wizard. On the left, under 'Inbound Security Group Rules', two rules are defined:

- Security group rule 1 (TCP: 3389, 0.0.0.0/0):** Type: rdp, Protocol: TCP, Port range: 3389. Source type: Anywhere.
- Security group rule 2 (All, All, 0.0.0.0/0):** Type: All traffic, Protocol: All, Port range: All. Source type: Anywhere.

A tooltip for the second rule states: "Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only." On the right, the 'Summary' section shows 1 instance being launched with the following details:

- Software Image (AMI): Microsoft Windows Server 2022
- Virtual server type (instance type): t2.micro
- Storage (volume): 1 volume(s) - 30 GB

At the bottom right of the summary section is a prominent orange 'Launch Instance' button.

56 – Click on launch Instance .

PRN: 20220801121



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with links like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing. The main content area displays a table titled 'Instances (1) Info'. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4, and Elastic IP. One row is shown, corresponding to the instance 'ec2-vpc-1121' with the ID 'i-0c46ec64383b5fd87'. The instance is 'Running', of type 't2.micro', and has passed 2/2 checks. It is located in the 'ap-south-1b' availability zone with the public IP '13.201.100.174'. Below the table, a modal window titled 'Select an instance' is open, showing the same instance 'ec2-vpc-1121'. At the bottom of the page, there's a standard Windows taskbar with icons for File Explorer, Task View, Taskbar settings, and system status.

57 – Select the instance and click on connect .

58 – Download the remote desktop file .

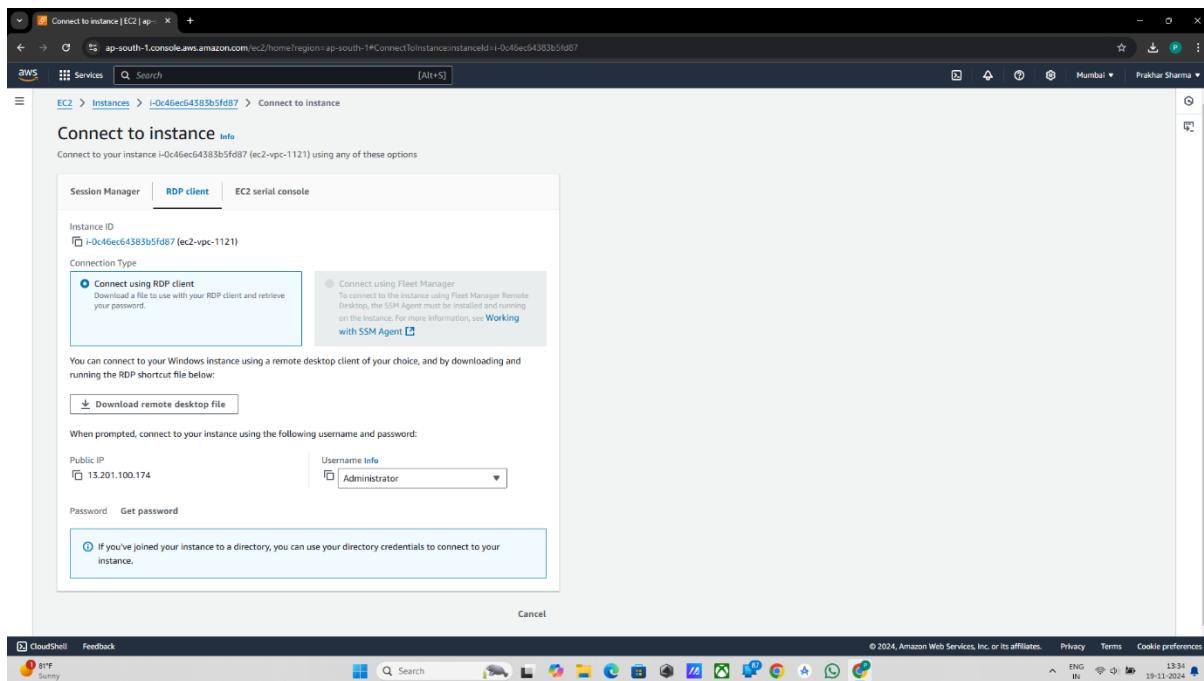
59 – Click on get password .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)



60 – Upload the private key pair file .

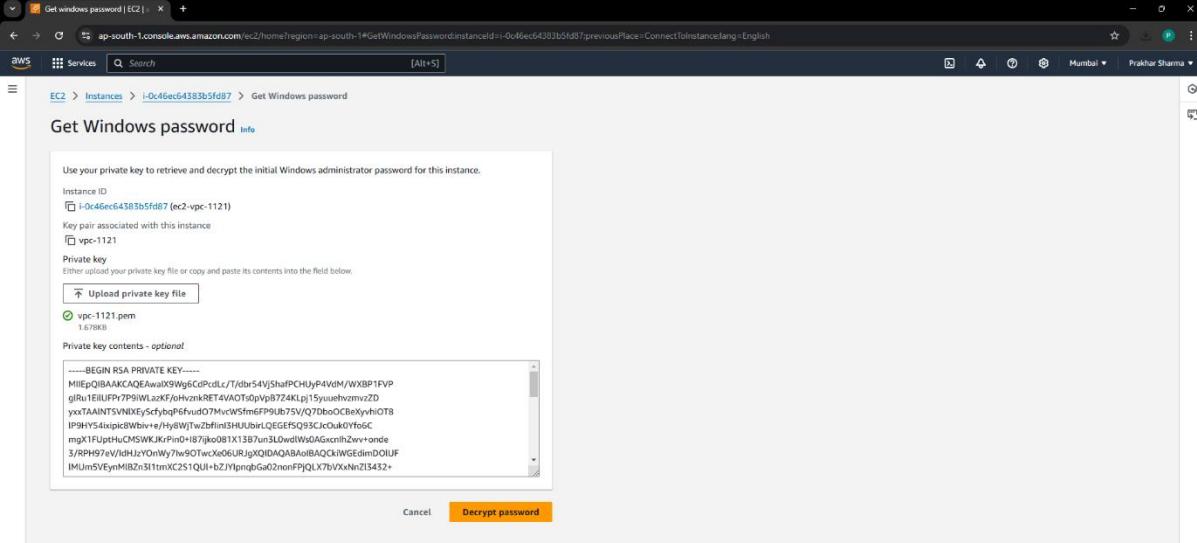
61 – Click on decrypt password .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)



The screenshot shows the AWS EC2 Instances page with a specific instance selected. A modal dialog box is open titled "Get Windows password". It contains instructions to use a private key to retrieve the initial Windows administrator password. It shows a "Private key" section with a file named "vpc-1121.pem" selected. Below it is a "Private key contents - optional" text area containing a long RSA PRIVATE KEY string. At the bottom of the dialog are "Cancel" and "Decrypt password" buttons.



The screenshot shows a Windows desktop with a taskbar at the bottom. The taskbar includes icons for CloudShell, Feedback, and several other system and application icons. The status bar at the bottom right shows the date and time as 13:35 on 19-11-2024.

Copy the password and paste it on notepad .

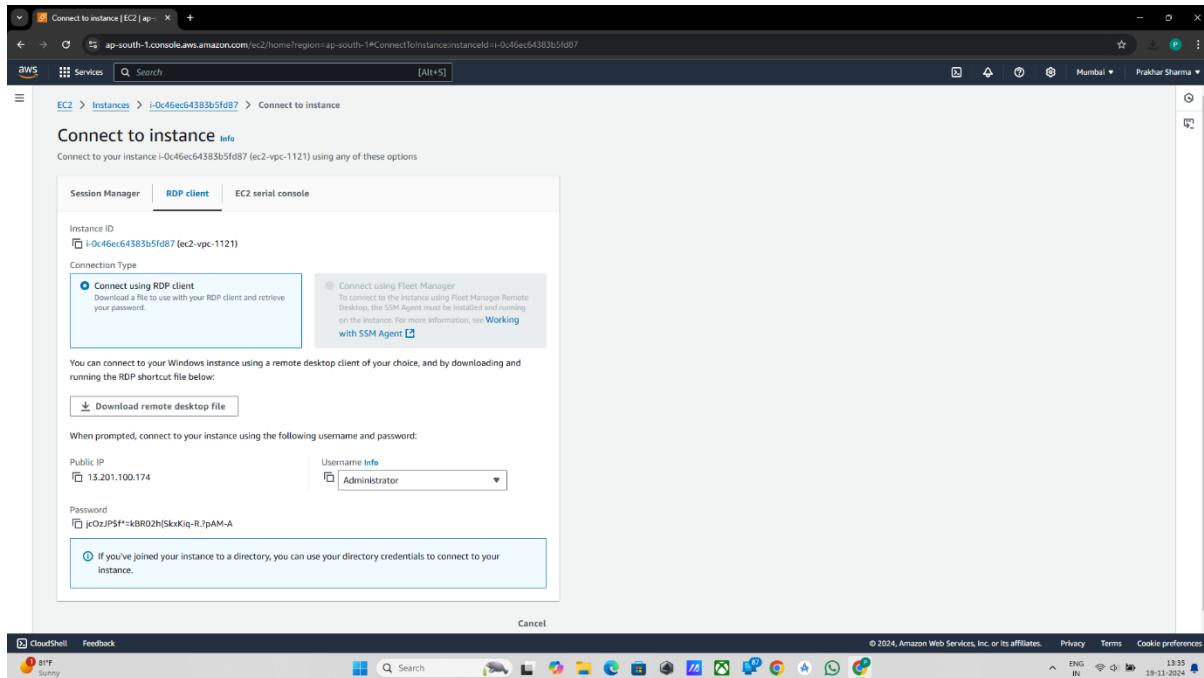
PRN: 20220801121



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)



62 – Open the remote desktop file .

63 – Paste the password .

64 – Click on ok .

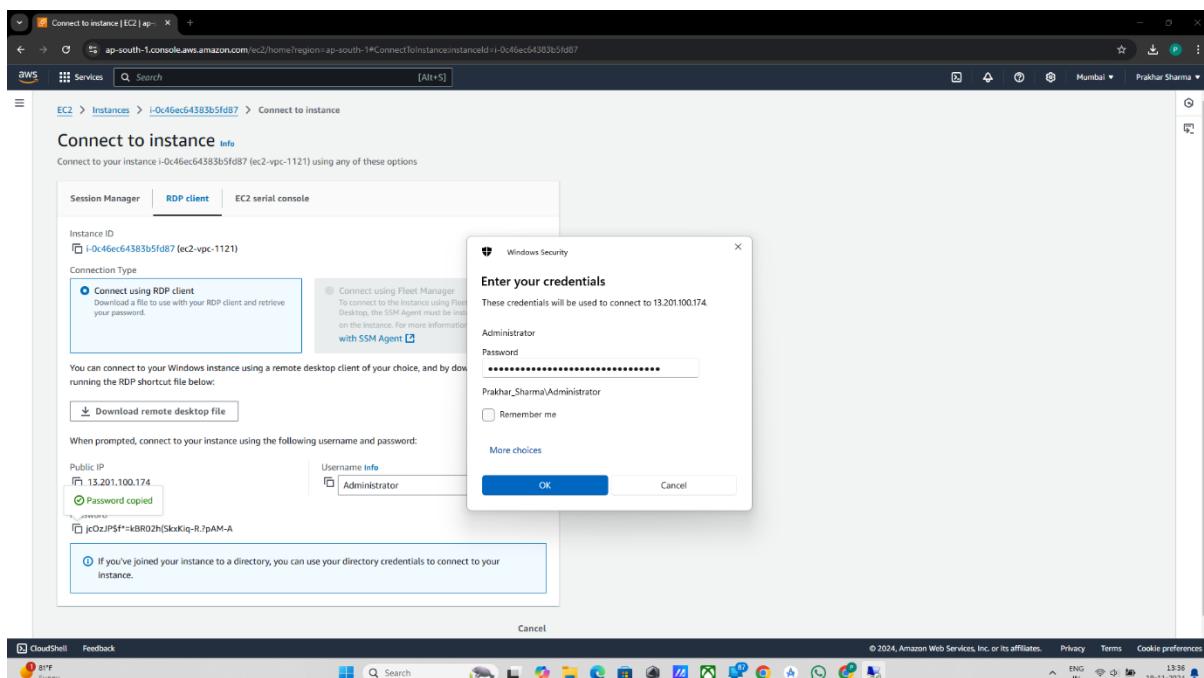
65 – Click on Connect .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)



A new window will open after successful connection .

66 – Now Go to VPC and search Network ACLs in the left hand panel.

67 – Click on it .

68 – Click on Create Network ACLs .

69 – Name the NACL .

70 – Select the VPC from dropdown .

71 – Click on create Network ACL .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Network ACL creation interface. In the 'Network ACL settings' section, a 'Name - optional' field contains 'my-NACL-1121'. A 'VPC' dropdown is set to 'vpc-0eddb86913fb04dc58 (my-vpc-ccsa-1121)'. Under 'Tags', there is a single tag 'Name: my-NACL-1121'. At the bottom right is a yellow 'Create network ACL' button.

The screenshot shows the AWS VPC dashboard with the 'Network ACLs' section selected. A success message 'You successfully created acl-0309b536c494337cd / my-NACL-1121.' is displayed. The table lists three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
acl-04ee9c95ffcc6c369	2 Subnets	-	Yes	vpc-0ffe06795a9e200	2 Inbound rules	2 Outbound rules
acl-04089c0428284cd7	subnet-07ae2a52334ef860 / my-subnet-09	-	Yes	vpc-0eddb86913fb04dc58 / my-vpc-ccsa-1121	2 Inbound rules	2 Outbound rules
my-NACL-1121	acl-0309b536c494337cd	-	No	vpc-0eddb86913fb04dc58 / my-vpc-ccsa-1121	1 Inbound rule	1 Outbound rule

PRN: 20220801121

2
2



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

72 – Select the NACL .

73 – Go to Subnet Association .

74 – Click on edit association .

75 – Select the subnet and click on save changes .

A screenshot of the AWS VPC Network ACL Subnet Associations page. The URL is ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditNetworkAclSubnetAssociations:networkAclId=acl-0309b536c494337cd. The page shows a table of available subnets and a selected subnet. The table has columns: Name, Subnet ID, Associated with, Availability Zone, IPv4 CIDR, and IPv6 CIDR. One row is selected: my-subnet-09, subnet-07ae2a523334ef860, acl-04089c0428284cde7, ap-south-1b, 10.0.0.0/24, and -. Below the table, a section titled "Selected subnets" shows the same subnet entry. At the bottom right are "Cancel" and "Save changes" buttons. The status bar at the bottom indicates it's 24-11-2024, LS 32, ENG IN.

PRN: 20220801121



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Network ACLs page. A success message at the top states: "You have successfully updated subnet associations for acl-0309b536c494337cd / my-NACL-1121". The main table lists three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
acl-04ee9c95fc6e369	acl-04ee9c95fc6e369	2 Subnets	Yes	vpc-08ffe06795a9ec200	2 Inbound rules	2 Outbound rules
acl-04089c0428284cd7	-	-	Yes	vpc-0e6d86913fb04dc58 / my-vpc-ccsa...	2 Inbound rules	2 Outbound rules
my-NACL-1121	acl-0309b536c494337cd	subnet-07ae2a523334ef860 / my-subnet-09	No	vpc-0e6d86913fb04dc58 / my-vpc-ccsa...	1 Inbound rule	1 Outbound rule

Below the table, a specific Network ACL row is expanded:

Network ACL ID ad-0309b536c494337cd	Associated with subnet-07ae2a523334ef860 / my-subnet-09	Default No	VPC ID vpc-0e6d86913fb04dc58 / my-vpc-ccsa-1121
Owner 891377273858			

76 – Go to inbound rule

The inbound rule deny the traffic .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Network ACLs page. A success message at the top states: "You have successfully updated subnet associations for acl-0309b536c494337cd / my-NACL-1121". The main table lists three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
acl-04ee9c95fc6e369	2 Subnets	-	Yes	vpc-08ffe06795a9ec200	2 Inbound rules	2 Outbound rules
acl-04089c0428284cd7	-	-	Yes	vpc-0e6d86913fb04dc58 / my-vpc-ccsa...	2 Inbound rules	2 Outbound rules
my-NACL-1121	acl-0309b536c494337cd	subnet-07aae2a523334ef860 / my-subnet-09	No	vpc-0e6d86913fb04dc58 / my-vpc-ccsa...	1 Inbound rule	1 Outbound rule

The "Inbound rules" tab is selected, showing one rule:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

77 – Go to outbound rule .

The outbound rule deny the traffic .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Network ACL configuration page. A success message at the top states: "You have successfully updated subnet associations for acl-0309b536c494337cd / my-NACL-1121". Below this, the "Details" section displays the "Network ACLs (1/3) Info" table:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
acl-04ee9c95fc6e369	2 Subnets	Yes	vpc-08ffe06795a9ec200	2 Inbound rules	2 Outbound rules	
acl-04089c0428284cd7	-	Yes	vpc-0e6d86913fb04dc58 / my-vpc-ccsa...	2 Inbound rules	2 Outbound rules	
my-NACL-1121	acl-0309b536c494337cd	subnet-07aae2a523334ef860 / my-subnet-09	No	vpc-0e6d86913fb04dc58 / my-vpc-ccsa...	1 Inbound rule	1 Outbound rule

The "Outbound rules (1)" section shows a single rule:

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

We are not able to connect- because we have created custom NACL where everything is denied

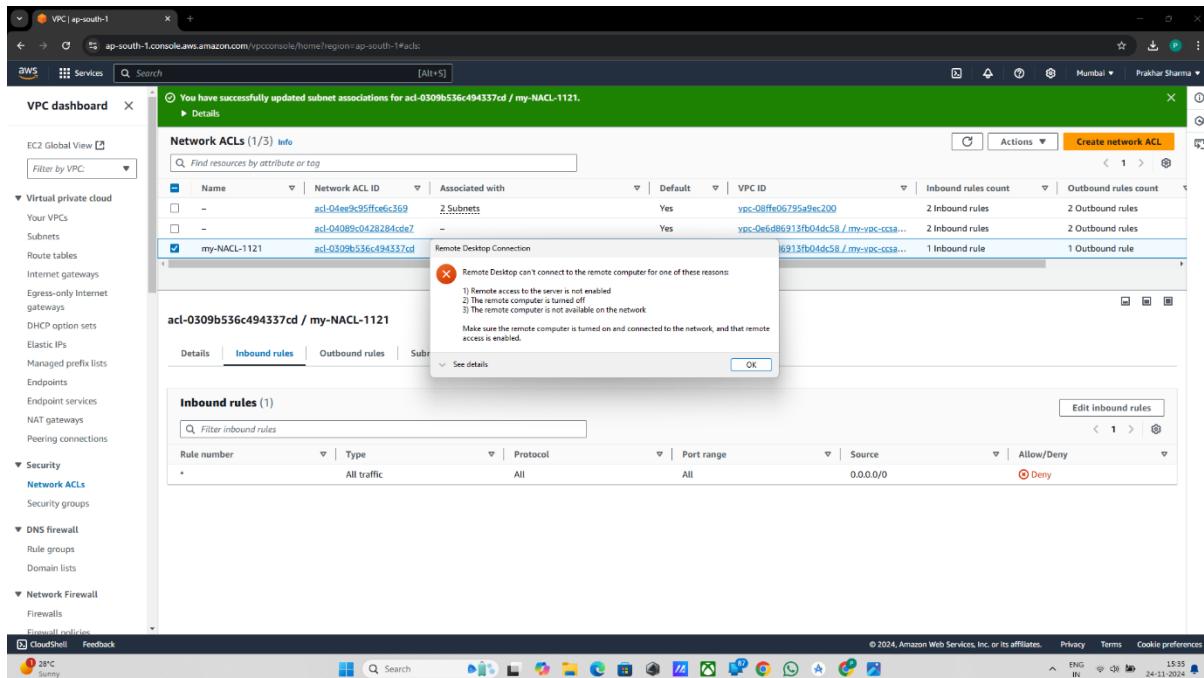


School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

inbound as well as outbound



78 - Go to outbound rule and click on edit outbound rules.

79 – Add two rules

- 1st – Rule no.100 , type – RDP , Destination no - 0.0.0.0/0 , Allow/Deny – Allow .
- 2nd – Rule no.150 , type – Custom TCP , Port Range – 1024-65535 , Destination no - 0.0.0.0/0 , Allow/Deny – Allow .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

80 – Click on Save Changes .

A screenshot of the AWS VPC Network ACLs interface. The URL is ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#EditOutboundRules:networkAclId=ad-0309b536c494337cd. The page shows two outbound rules: Rule 100 (RDP (3389)) allowing port 3389 to 0.0.0.0/0 with Allow action, and Rule 150 (Custom TCP) allowing port 1024-65535 to 0.0.0.0/0 with Allow action. There is also a third row for "All traffic" with All protocol and All port range. Buttons at the bottom include "Cancel", "Preview changes", and a prominent orange "Save changes" button.

81 - Go to inbound rule and click on edit inbound rules.

82 – Add two rules .

- 1st – Rule no.100 , type – Custom TCP , Port Range – 1024-65535 , Destination no - 0.0.0.0/0 , Allow/Deny – Allow .

- 2nd– Rule no.10 , type – RDP , Destination no - 0.0.0.0/0 , Allow/Deny – Allow .

83 – Click on Save Changes .



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Network ACL inbound rules configuration page. It displays two rules:

Rule number	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info
150	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Allow
100	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Buttons at the bottom include 'Add new rule', 'Sort by rule number', 'Cancel', 'Preview changes', and 'Save changes'.

Inbound rule allowed here



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Network ACL configuration page. The main table lists three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
acl-04ee9c95ffce6x309	acl-04ee9c95ffce6x309	2 Subnets	Yes	vpc-08ffe06795a9e200	2 Inbound rules	2 Outbound rules
acl-04089c0428284cd0e7	acl-04089c0428284cd0e7	-	Yes	vpc-0e6d86913fb0fd858 / my-vpc-ccsa...	2 Inbound rules	2 Outbound rules
my-NACL-1121	acl-0309b536c494337cd	subnet-07ae2a523334ef860 / my-subnet-09	No	vpc-0e6d86913fb0fd858 / my-vpc-ccsa...	3 Inbound rules	3 Outbound rules

The details for 'my-NACL-1121' are shown, specifically the 'Inbound rules' section:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
150	RDP (3589)	TCP (6)	3589	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Outbound rule allowed here



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

The screenshot shows the AWS VPC Network ACL configuration page. The main title is "Network ACLs (1/3) Info". It displays a table of Network ACLs with columns: Name, Network ACL ID, Associated with, Default, VPC ID, Inbound rules count, and Outbound rules count. One row is selected: "my-NACL-1121" (acl-0309b536c494337cd). Below this, the specific configuration for "my-NACL-1121" is shown under "Outbound rules [3]". The table has columns: Rule number, Type, Protocol, Port range, Destination, and Allow/Deny. The rules are:

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	RDP (5389)	TCP (6)	3389	0.0.0.0/0	Allow
150	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Now go for remote access

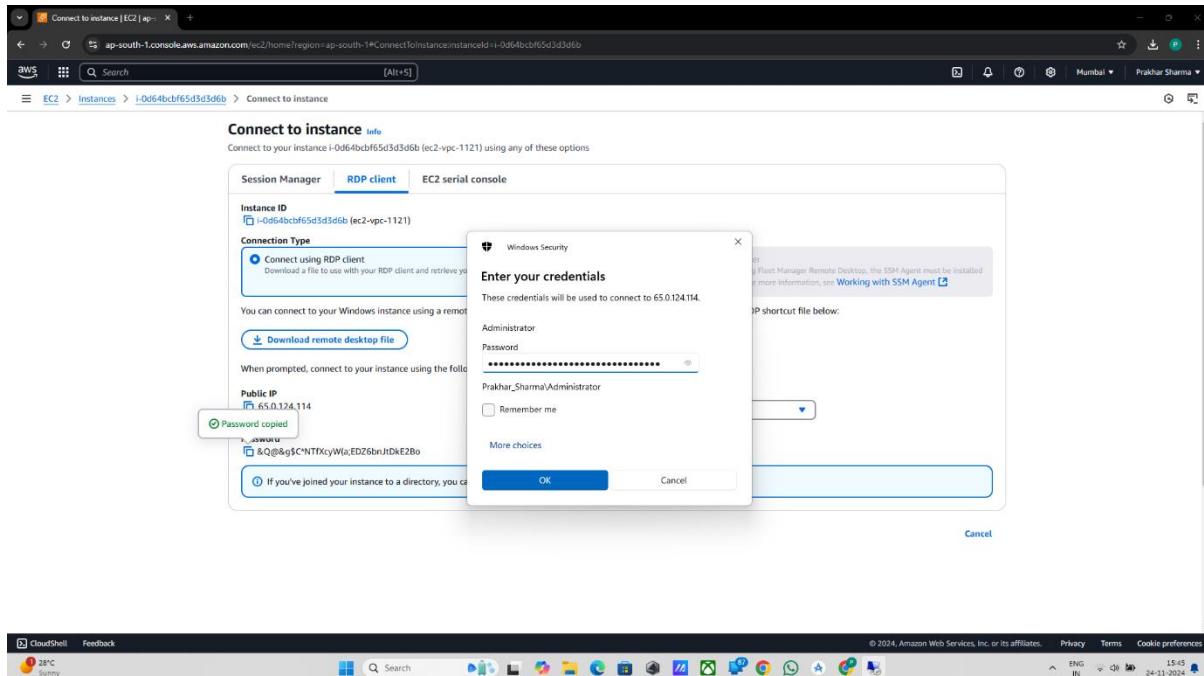
Now you can able to connect



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)



Now NACL is permitting the RDP also, now we have the double level of security, first we have the NACL permission if we removed it from security group again we are not able to connect RDs to this machine But from both end it is permitted now.so we are able to connect to EC2 instance



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma **PRN:** 20220801121

Title of Practical: Configuring Layered Security in an AWS VPC(NACL)

