Security Group & Network Access Control List

AWS provides a robust set of security features to protect your infrastructure, data, and applications. Security in AWS operates on a **shared responsibility model**, where AWS is responsible for securing the underlying cloud infrastructure, while you (the customer) are responsible for securing the applications, data, and configurations running on the cloud.

Security Group

A **Security Group** acts as a virtual firewall at the **instance level** in AWS. It controls inbound and outbound traffic for **EC2 instances**.

Key Features of Security Groups:

1. **Stateful**:
   - If you allow an inbound request, the response is automatically allowed (and vice versa).
2. **Instance-Level Control**:
   - Security groups are associated with specific EC2 instances.
3. **Rules**:
   - You define rules to allow traffic on specific **ports**, **protocols**, and **IP ranges** (e.g., allow SSH on port 22).
4. **No Deny Rules**:
   - You can only add **allow rules**; all traffic not explicitly allowed is denied by default.

Network Access Control List (NACL)

Key Features of NACLs:

1. **Stateless**:
   - Inbound and outbound rules are evaluated separately; you must explicitly allow return traffic.
2. **Subnet-Level Control**:
   - NACLs are applied to entire subnets, impacting all resources within them.

3. **Rules**:
    - You can define both **allow** and **deny** rules for traffic based on **port**, **protocol**, and **CIDR block**.
4. **Rule Evaluation**:
    - Rules are evaluated in order based on their **rule number** (lowest number first).

Comparison: Security Group vs. NACL

Feature	Security Group	NACL
Level of Operation	Instance level	Subnet level
State	Stateful	Stateless
Allow/Deny Rules	Only allows rules	Allows both allow and deny rules
Evaluation Order	All rules are evaluated	Rules are evaluated in number order
Default Behavior	Deny all traffic unless allowed	Allow all inbound/outbound by default for custom NACLs
Use Case	Fine-grained control for instances	Broader control for subnets

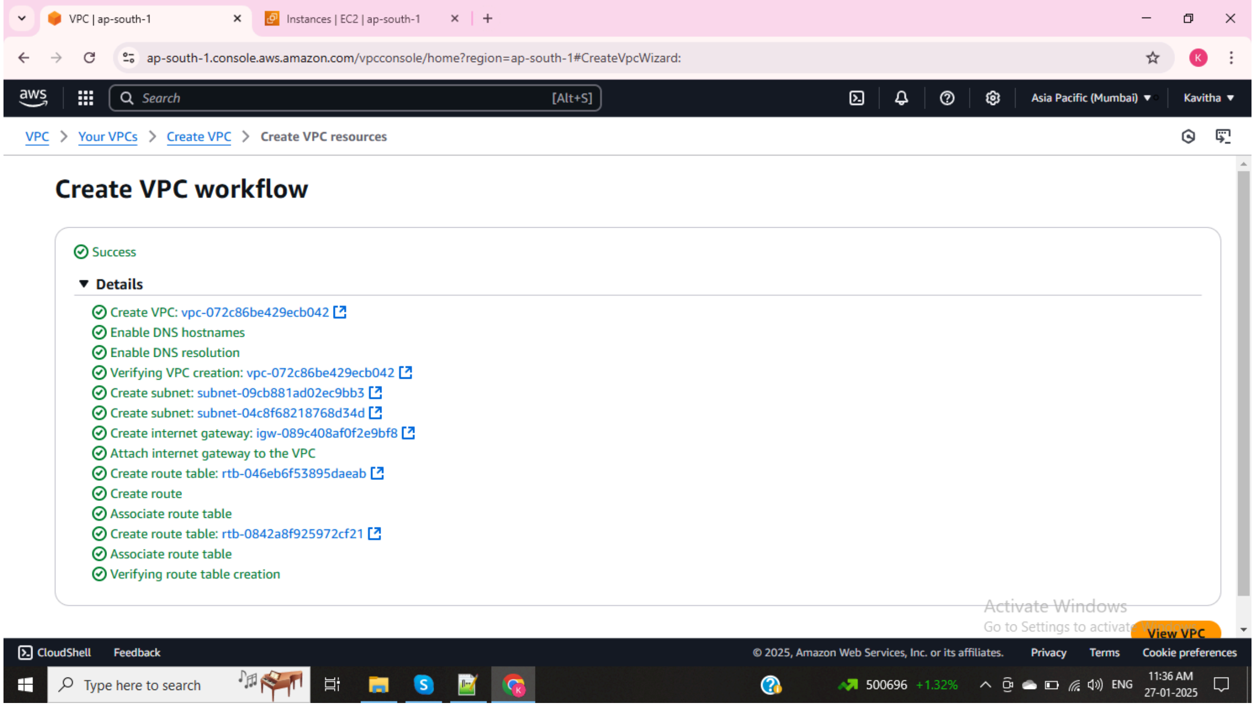
Outbound rules in a **Network Access Control List (NACL)** define the traffic that is **allowed or denied** to leave a subnet in an **AWS Virtual Private Cloud (VPC)**. These rules control the egress (outbound) traffic from resources (such as EC2 instances) within the subnet associated with the NACL.

Rule numbers must be between **1** and **32766 inbound IPv4 traffic.**.

Lower numbers are evaluated first, and higher numbers are evaluated later.

No default inbound rules are present except for rule **32767** (implicit deny all).

Creating a VPC - KAVI VPC



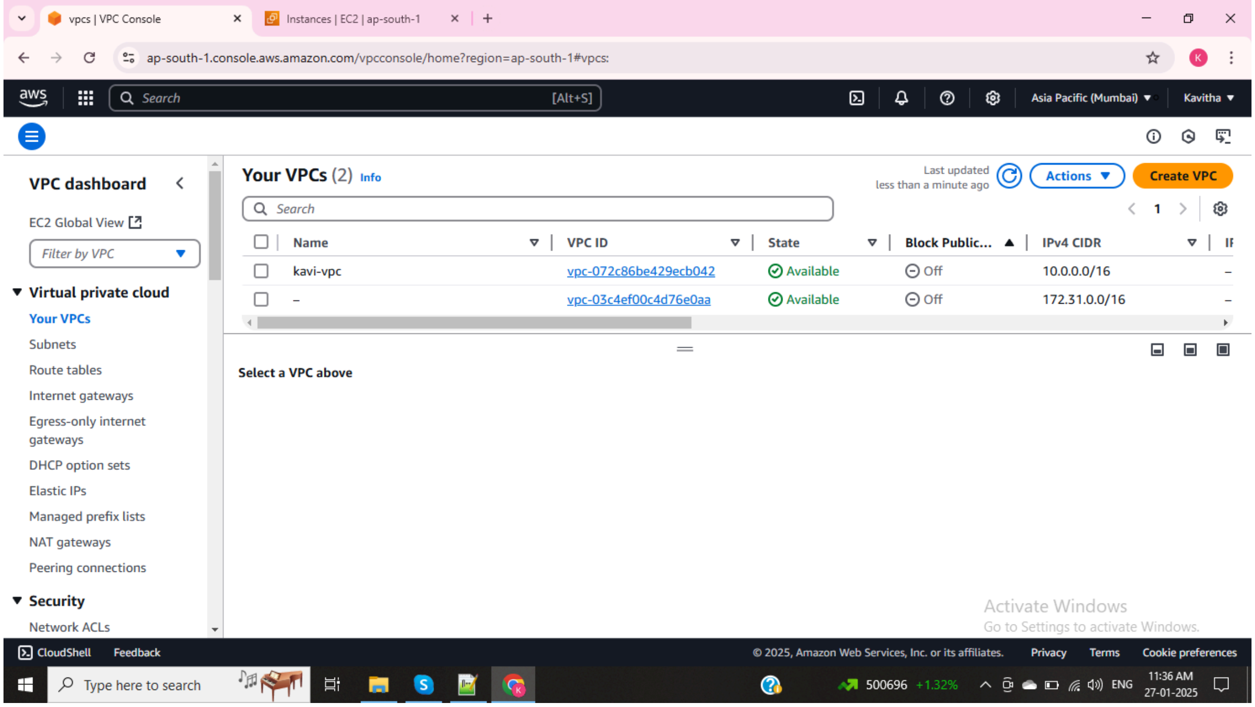
VPC | ap-south-1
Instances | EC2 | ap-south-1
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpcWizard:
Search
[Alt+S]
Asia Pacific (Mumbai)
Kavitha
VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow

✓ Success

▼ **Details**

- ✓ Create VPC: vpc-072c86be429ecb042
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-072c86be429ecb042
- ✓ Create subnet: subnet-09cb881ad02ec9bb3
- ✓ Create subnet: subnet-04c8f68218768d34d
- ✓ Create internet gateway: igw-089c408af0f2e9bf8
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-046eb6f53895daeab
- ✓ Create route
- ✓ Associate route table
- ✓ Create route table: rtb-0842a8f925972cf21
- ✓ Associate route table
- ✓ Verifying route table creation



Your VPCs (2) Info

Last updated less than a minute ago

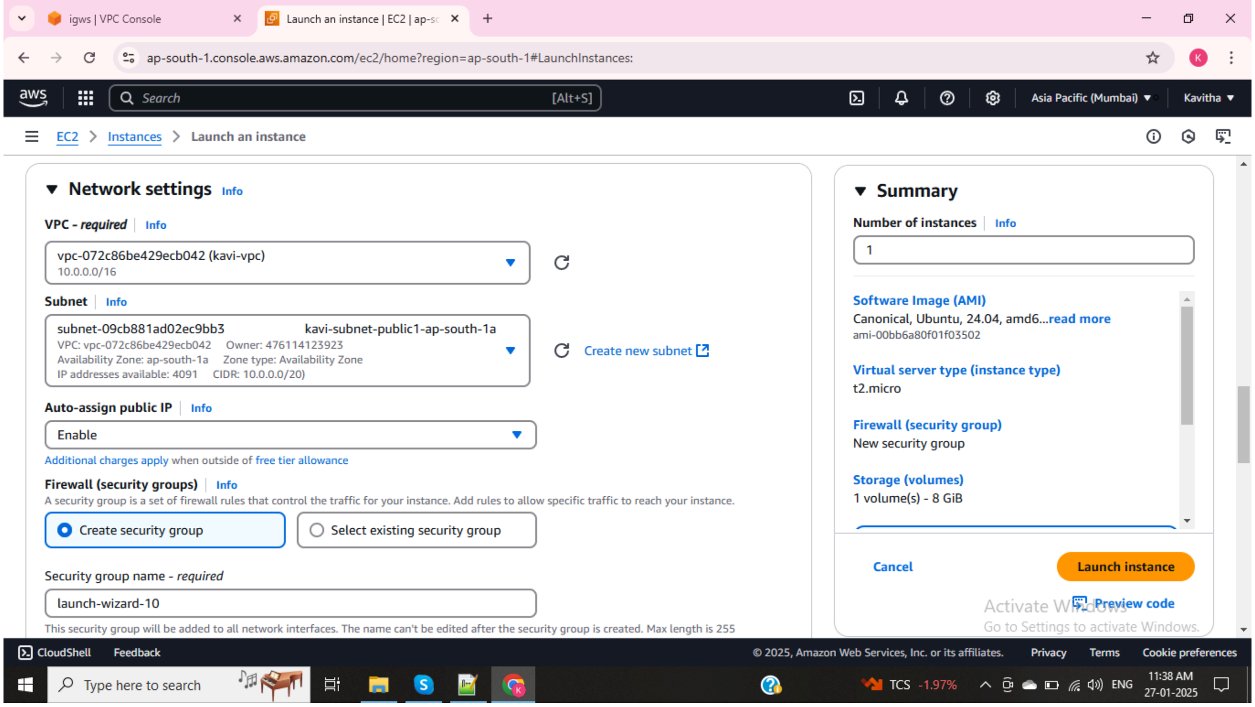
Actions ▼ | Create VPC

Search

□	Name	VPC ID	State	Block Public...	IPv4 CIDR	IF
□	kavi-vpc	vpc-072c86be429ecb042	✓ Available	⊖ Off	10.0.0.0/16	–
□	–	vpc-03c4ef00c4d76e0aa	✓ Available	⊖ Off	172.31.0.0/16	–

Select a VPC above

Created an EC2 instance and in Network settings selected created VPC



▼ Network settings Info

VPC - *required* Info

vpc-072c86be429ecb042 (kavi-vpc)
10.0.0.0/16

Subnet Info

subnet-09cb881ad02ec9bb3 kavi-subnet-public1-ap-south-1a
VPC: vpc-072c86be429ecb042 Owner: 476114123923
Availability Zone: ap-south-1a Zone type: Availability Zone
IP addresses available: 4091 CIDR: 10.0.0.0/20)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

launch-wizard-10

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255

▼ Summary

Number of instances Info

1

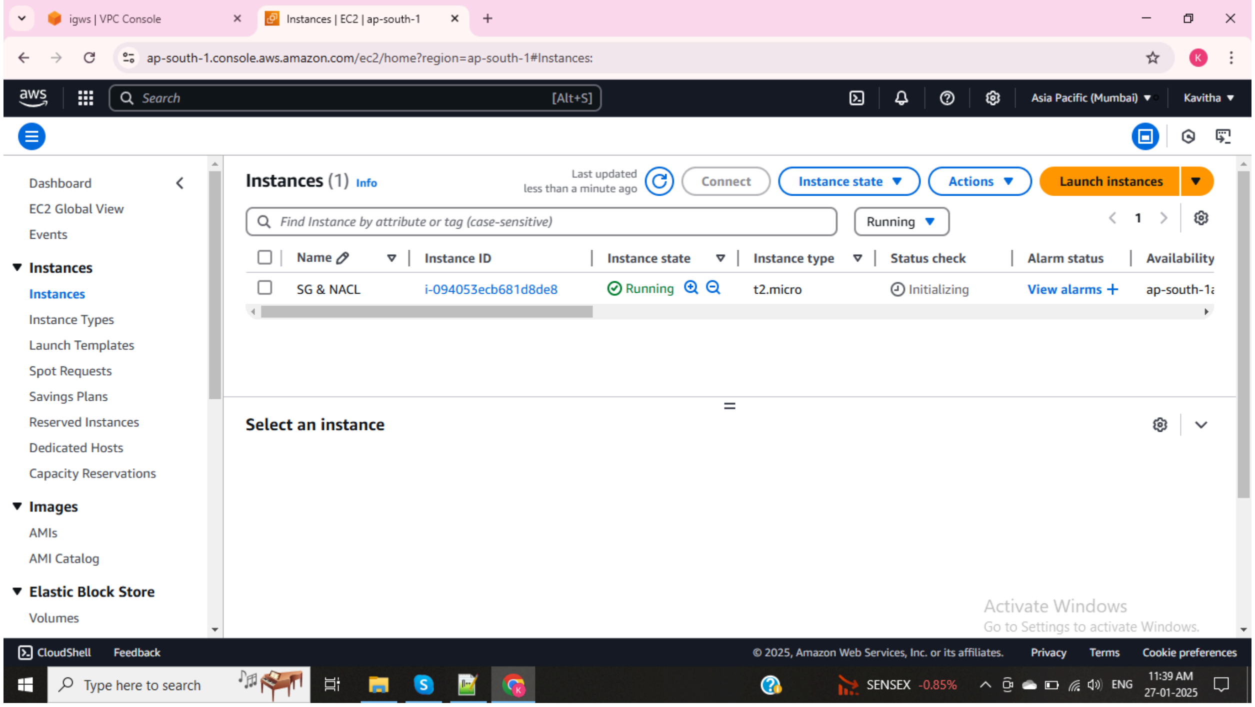
Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-00bb6a80f01f03502

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

EC2 instance for access SG AND NACL



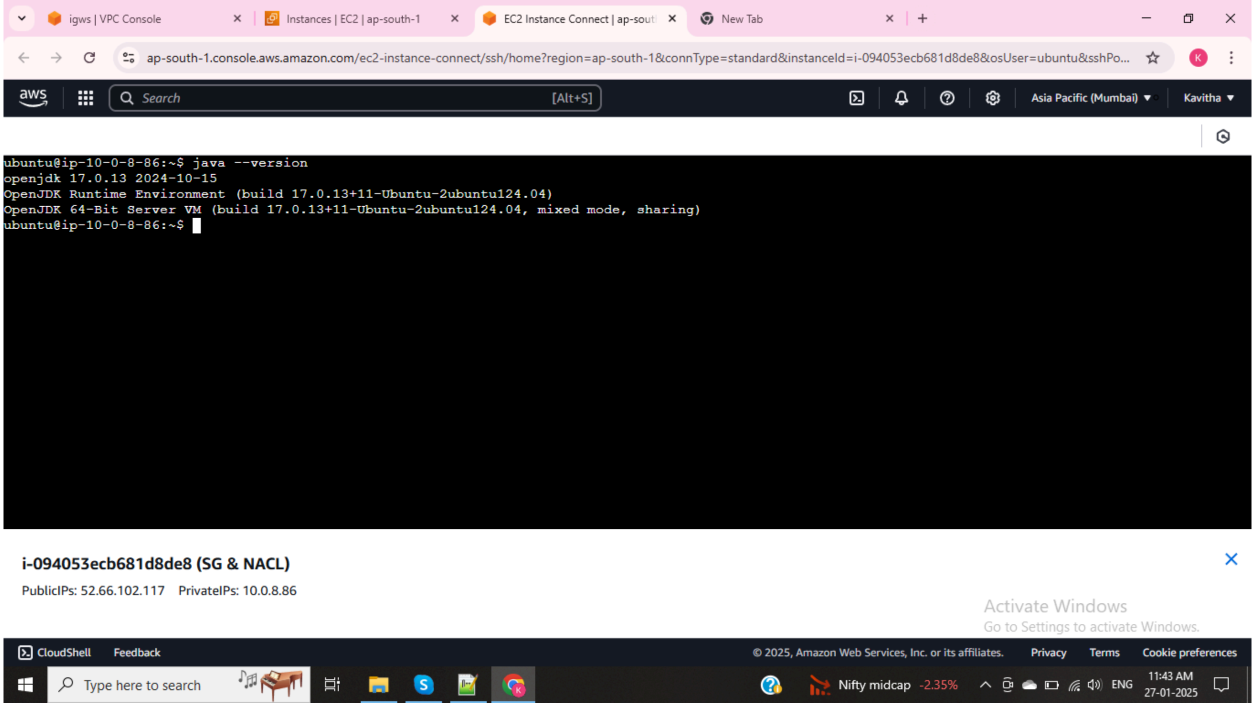
Instances (1) Info

Last updated less than a minute ago

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
□	SG & NACL	i-094053ecb681d8de8	✓ Running	t2.micro	Initializing	View alarms +	ap-south-1ε

Select an instance

Instance Connected --> update instance --> installed java

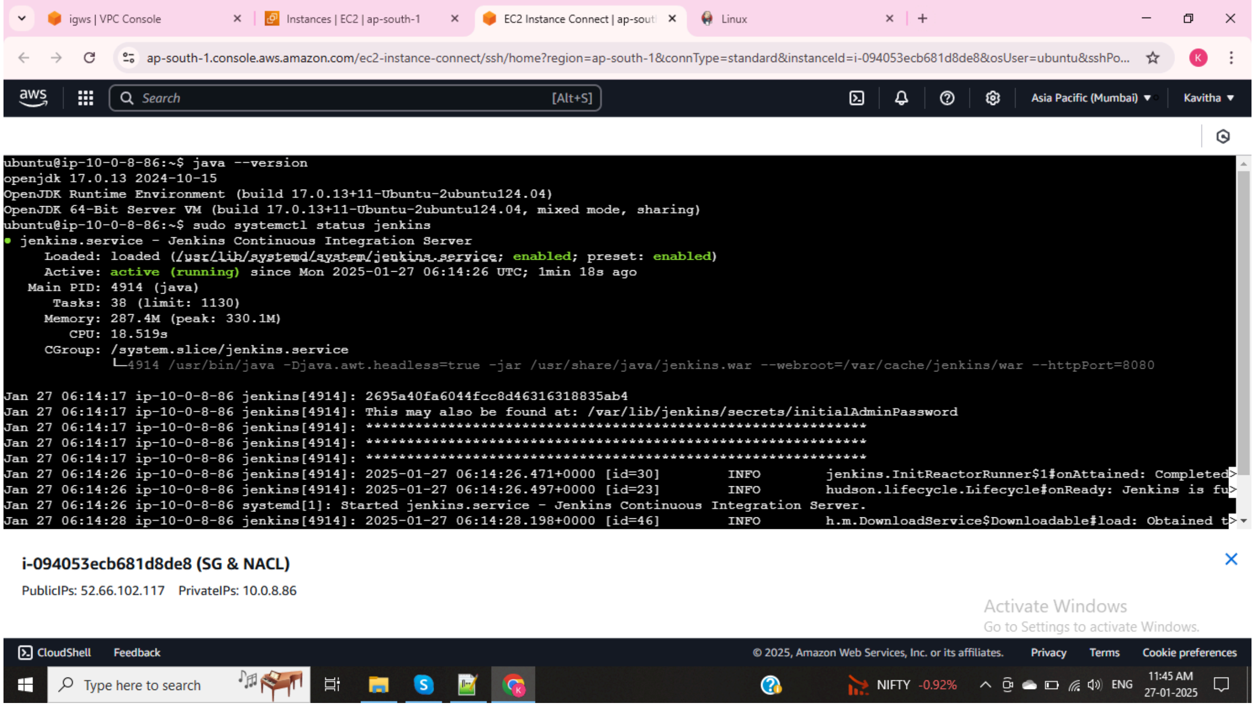

igws | VPC Console
Instances | EC2 | ap-south-1
EC2 Instance Connect | ap-sout
New Tab
ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh/home?region=ap-south-1&connType=standard&instanceId=i-094053ecb681d8de8&osUser=ubuntu&sshPo...
aws
Search
[Alt+S]
Asia Pacific (Mumbai)
Kavitha
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Activate Windows
Go to Settings to activate Windows.
Type here to search
Nifty midcap -2.35%
ENG
11:43 AM
27-01-2025

```
ubuntu@ip-10-0-8-86:~$ java --version
openjdk 17.0.13 2024-10-15
OpenJDK Runtime Environment (build 17.0.13+11-Ubuntu-2ubuntu124.04)
OpenJDK 64-Bit Server VM (build 17.0.13+11-Ubuntu-2ubuntu124.04, mixed mode, sharing)
ubuntu@ip-10-0-8-86:~$
```

i-094053ecb681d8de8 (SG & NACL)

PublicIPs: 52.66.102.117 PrivateIPs: 10.0.8.86

Installed Jenkins and status of Jenkins


igws | VPC Console
Instances | EC2 | ap-south-1
EC2 Instance Connect | ap-sout
Linux
ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh/home?region=ap-south-1&connType=standard&instanceId=i-094053ecb681d8de8&osUser=ubuntu&sshPo...
aws
Search
[Alt+S]
Asia Pacific (Mumbai)
Kavitha
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Activate Windows
Go to Settings to activate Windows.
Type here to search
NIFTY -0.92%
ENG
11:45 AM
27-01-2025

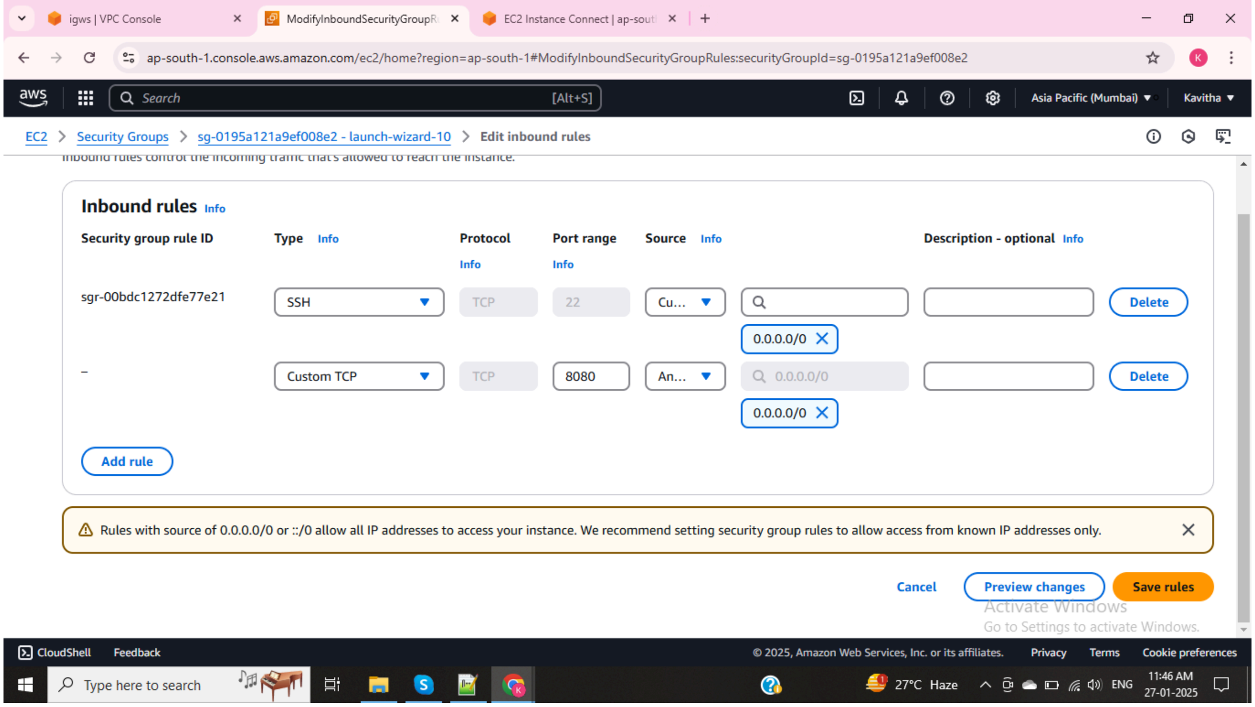
```
ubuntu@ip-10-0-8-86:~$ java --version
openjdk 17.0.13 2024-10-15
OpenJDK Runtime Environment (build 17.0.13+11-Ubuntu-2ubuntu124.04)
OpenJDK 64-Bit Server VM (build 17.0.13+11-Ubuntu-2ubuntu124.04, mixed mode, sharing)
ubuntu@ip-10-0-8-86:~$ sudo systemctl status jenkins
● jenkins.service - Jenkins Continuous Integration Server
     Loaded: loaded (/usr/lib/systemd/system/jenkins.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-01-27 06:14:26 UTC; 1min 18s ago
   Main PID: 4914 (java)
      Tasks: 38 (limit: 1130)
     Memory: 287.4M (peak: 330.1M)
        CPU: 18.519s
     CGroup: /system.slice/jenkins.service
             └─4914 /usr/bin/java -Djava.awt.headless=true -jar /usr/share/java/jenkins.war --webroot=/var/cache/jenkins/war --httpPort=8080

Jan 27 06:14:17 ip-10-0-8-86 jenkins[4914]: 2695a40fa6044fcc8d46316318835ab4
Jan 27 06:14:17 ip-10-0-8-86 jenkins[4914]: This may also be found at: /var/lib/jenkins/secrets/initialAdminPassword
Jan 27 06:14:17 ip-10-0-8-86 jenkins[4914]: *************************************************************
Jan 27 06:14:17 ip-10-0-8-86 jenkins[4914]: *************************************************************
Jan 27 06:14:17 ip-10-0-8-86 jenkins[4914]: *************************************************************
Jan 27 06:14:26 ip-10-0-8-86 jenkins[4914]: 2025-01-27 06:14:26.471+0000 [id=30]        INFO        jenkins.InitReactorRunner$1#onAttained: Completed>
Jan 27 06:14:26 ip-10-0-8-86 jenkins[4914]: 2025-01-27 06:14:26.497+0000 [id=23]        INFO        hudson.lifecycle.Lifecycle#onReady: Jenkins is fu>
Jan 27 06:14:26 ip-10-0-8-86 systemd[1]: Started jenkins.service - Jenkins Continuous Integration Server.
Jan 27 06:14:28 ip-10-0-8-86 jenkins[4914]: 2025-01-27 06:14:28.198+0000 [id=46]        INFO        h.m.DownloadService$Downloadable#load: Obtained t>
```

i-094053ecb681d8de8 (SG & NACL)

PublicIPs: 52.66.102.117 PrivateIPs: 10.0.8.86

Allowing default port of Jenkins - port 8080 to access the Jenkins application



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-0195a121a9ef008e2

EC2 > Security Groups > sg-0195a121a9ef008e2 - launch-wizard-10 > Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

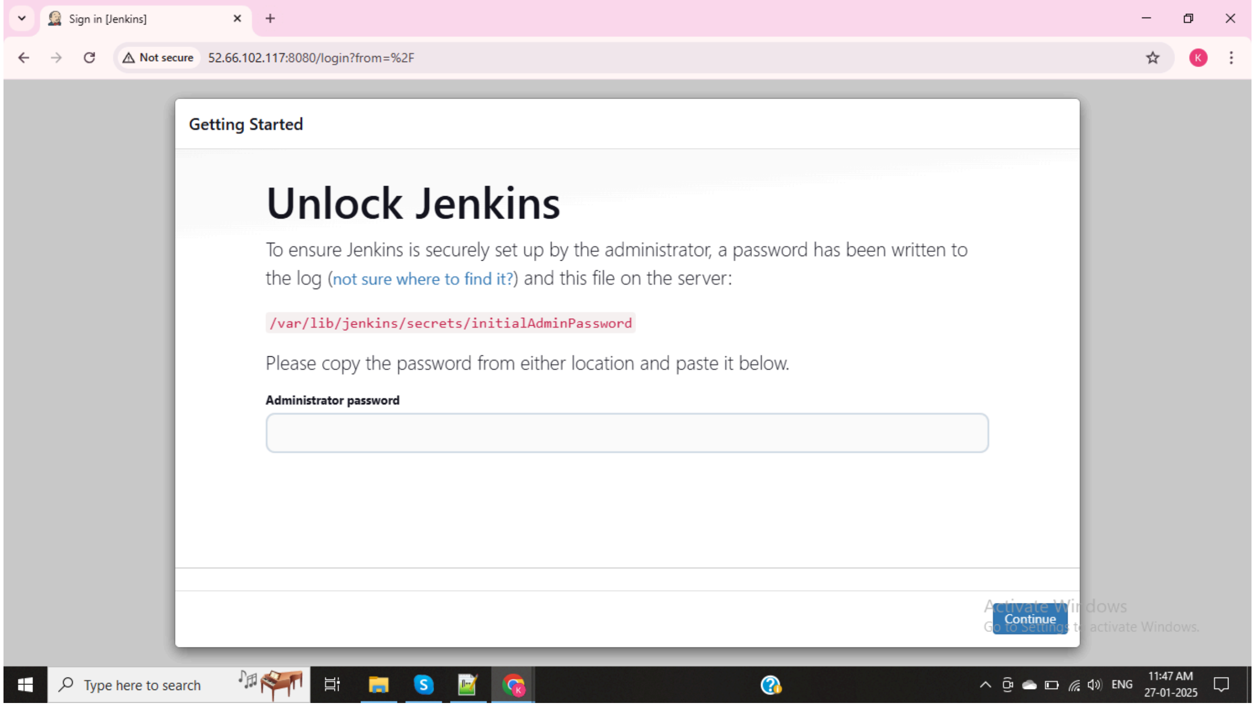
Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info
sgr-00bdc1272dfe77e21	SSH	TCP	22	Cu...	0.0.0.0/0	
–	Custom TCP	TCP	8080	An...	0.0.0.0/0	

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

OUTPUT



52.66.102.117:8080/login?from=%2F

Getting Started

Unlock Jenkins

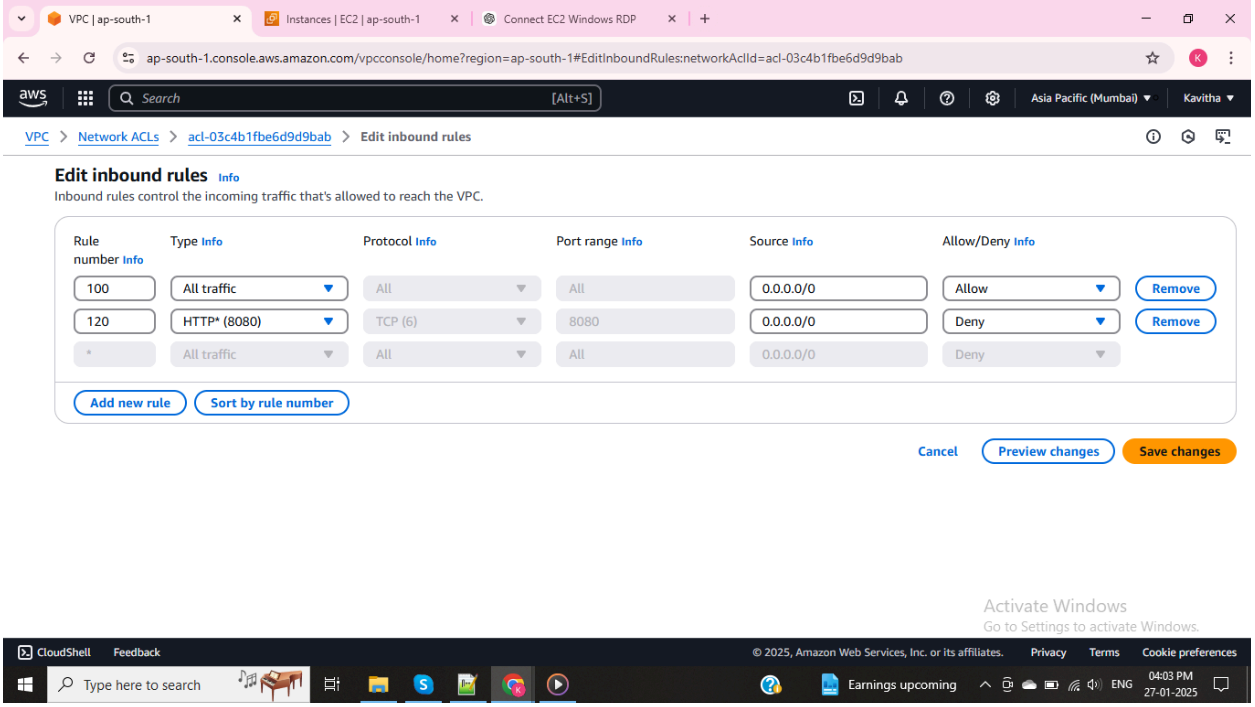
To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:

/var/lib/jenkins/secrets/initialAdminPassword

Please copy the password from either location and paste it below.

Administrator password

VPC --> NACL --> Edited Inbound rules in NACL --> 100 allow all traffic & 120 deny 8080


VPC | ap-south-1
Instances | EC2 | ap-south-1
Connect EC2 Windows RDP
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditInboundRules:networkAclId=acl-03c4b1fbe6d9d9bab
Search
[Alt+S]
Asia Pacific (Mumbai) ▾
Kavitha ▾
VPC > Network ACLs > acl-03c4b1fbe6d9d9bab > Edit inbound rules
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Activate Windows
Go to Settings to activate Windows.
Type here to search
Earnings upcoming
ENG
04:03 PM
27-01-2025

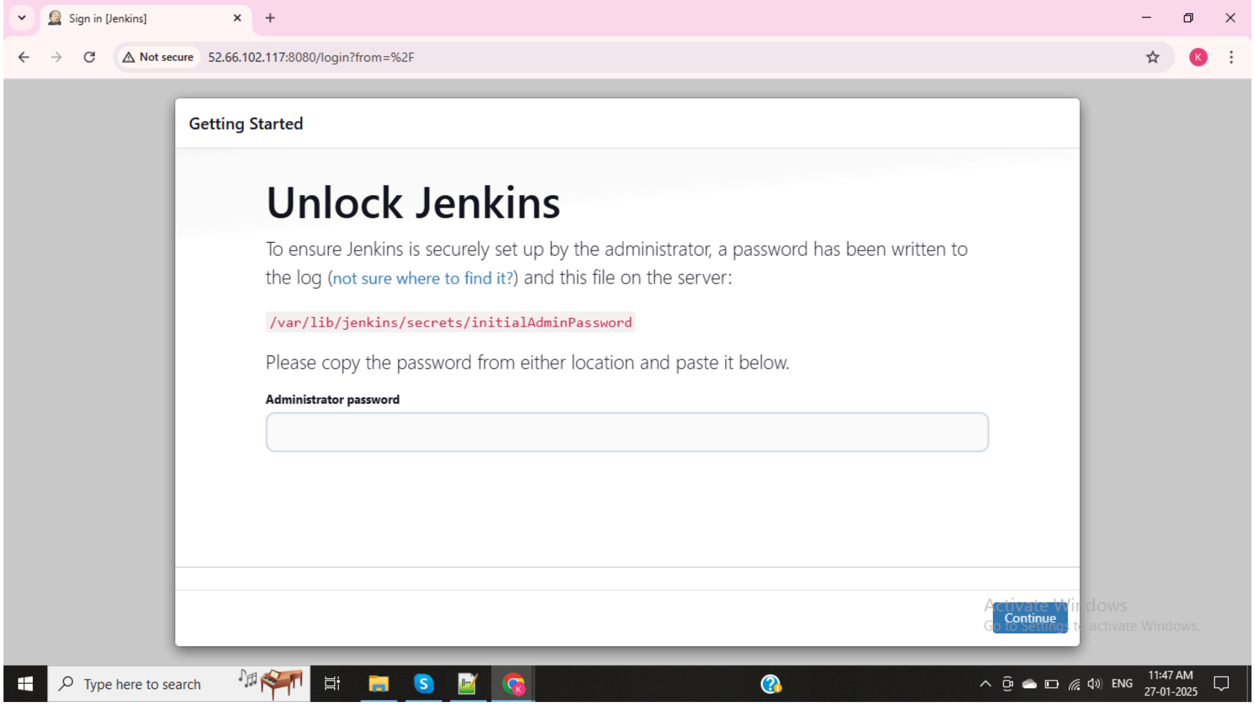
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
100	All traffic	All	All	0.0.0.0/0	Allow	Remove
120	HTTP* (8080)	TCP (6)	8080	0.0.0.0/0	Deny	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

Add new rule
Sort by rule number
Cancel
Preview changes
Save changes

In subnet level deny 8080 port in second rule and in Security group 8080 port open but the application is working because NACL taking ascending order rule numbers.



Unlock Jenkins

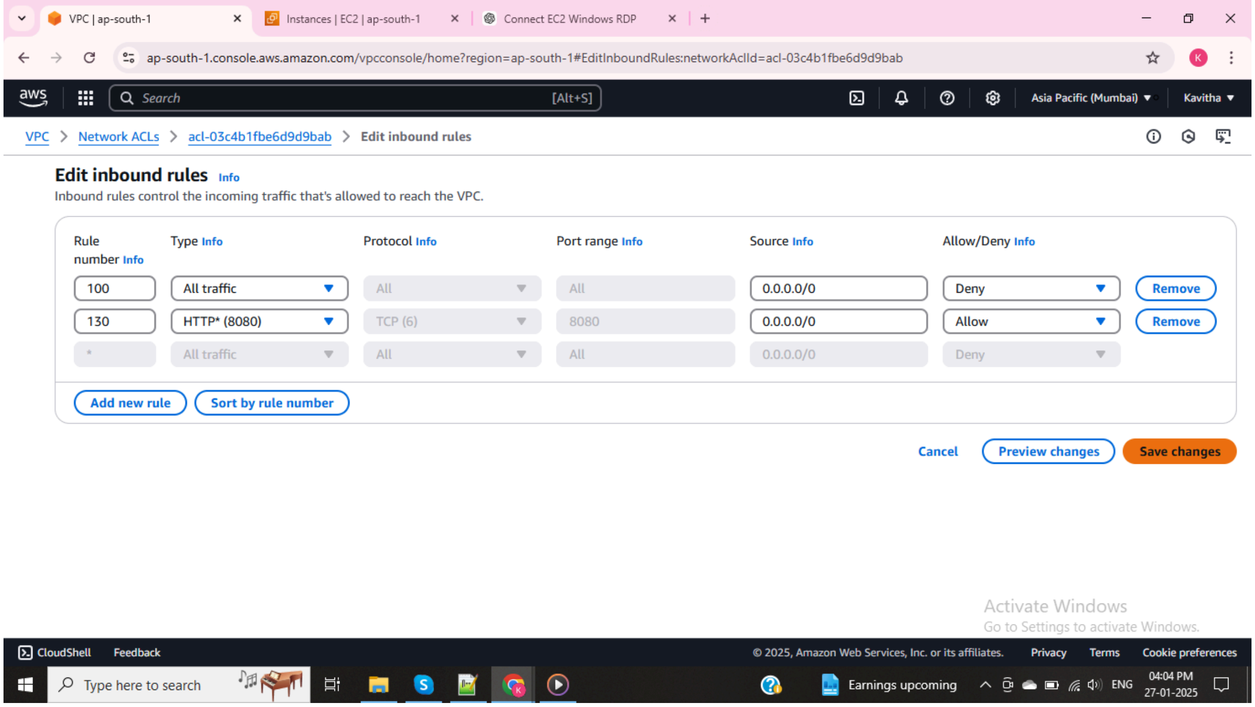
To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:

`/var/lib/jenkins/secrets/initialAdminPassword`

Please copy the password from either location and paste it below.

Administrator password

Now editing the inbound rules as 100 all traffic deny & 130 allow 8080 port and save changes


VPC | ap-south-1
Instances | EC2 | ap-south-1
Connect EC2 Windows RDP
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditInboundRules:networkAclId=acl-03c4b1fbe6d9d9bab
Search
[Alt+S]
Asia Pacific (Mumbai)
Kavitha
VPC > Network ACLs > acl-03c4b1fbe6d9d9bab > Edit inbound rules

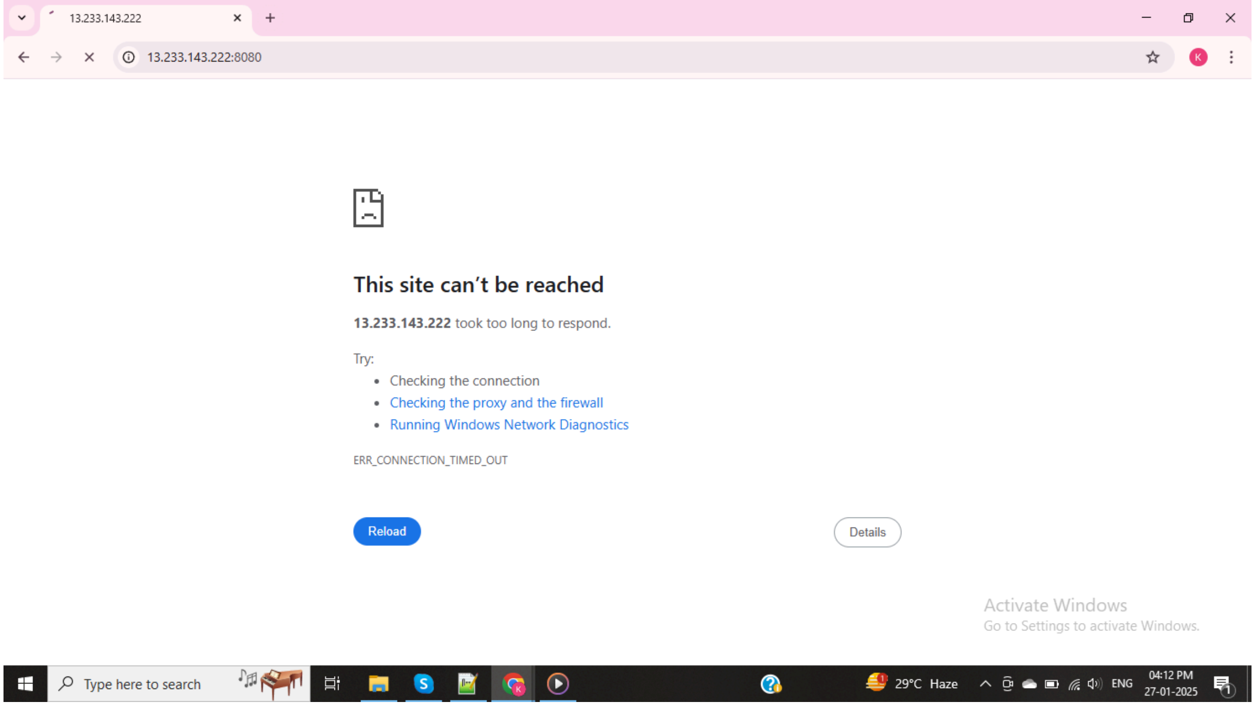
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
100	All traffic	All	All	0.0.0.0/0	Deny	Remove
130	HTTP* (8080)	TCP (6)	8080	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

Add new rule
Sort by rule number
Cancel
Preview changes
Save changes
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Earnings upcoming
ENG
04:04 PM
27-01-2025

In subnet level security is blocked and in instance level port 8080 is open if one level of security blocked means application is not worked and output



This site can't be reached

13.233.143.222 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT