Cloud Network & Access Control Architecture for Internal Applications

Name: Prem S

Roll No: 727823TUI0039

- Course: Cloud / Network Security

1. Problem Statement

An internal application must be accessible only to authorized employees while remaining protected from external threats. Previously, systems were directly exposed to the internet without proper firewall rules, which resulted in security vulnerabilities and unauthorized access.

The organization requires a secure cloud network design that balances accessibility and protection. The solution must ensure restricted administrative access, controlled application exposure, and proper network segregation to protect private servers.

2. Objective

The objective of this project is to design a secure cloud-based network architecture for internal applications by

- Protecting private servers from direct internet exposure
- Restricting SSH access to authorized users only
- Implementing firewall and access control rules
- Allowing application access only through defined ports
- Reducing security risks caused by open ports and unrestricted access

3. Overview

The proposed architecture uses a layered security approach to protect internal servers. The network is divided into public and private sections to control access and isolate sensitive resources.

The design includes:

- A virtual cloud network
- A public access layer with firewall protection
- A private network for internal application servers

- Secure administrative access using SSH
- Firewall rules to control inbound and outbound traffic

4. Architecture Design

The architecture consists of two main network segments:

Public Network

- Acts as the entry point for controlled access
- Protected by firewall rules
- Used only for secure administrative access

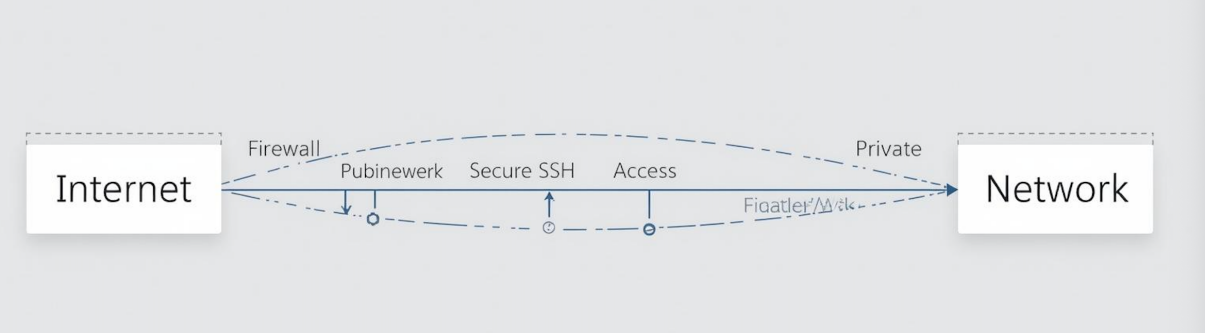
Private Network

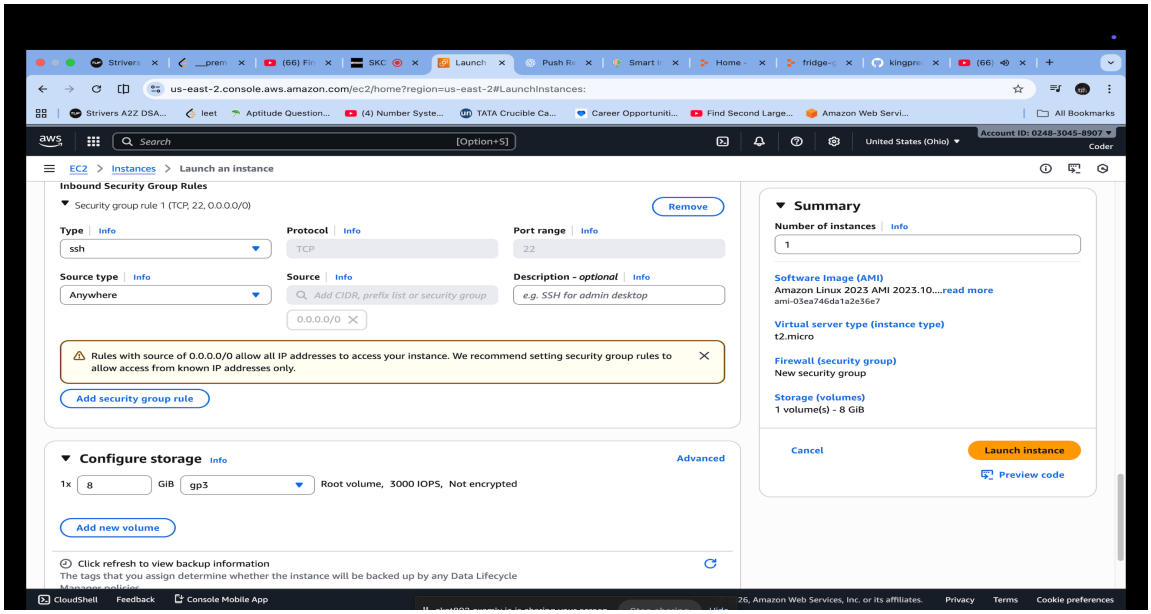
- Hosts the internal application server
- Not directly accessible from the internet
- Protected from unauthorized external access

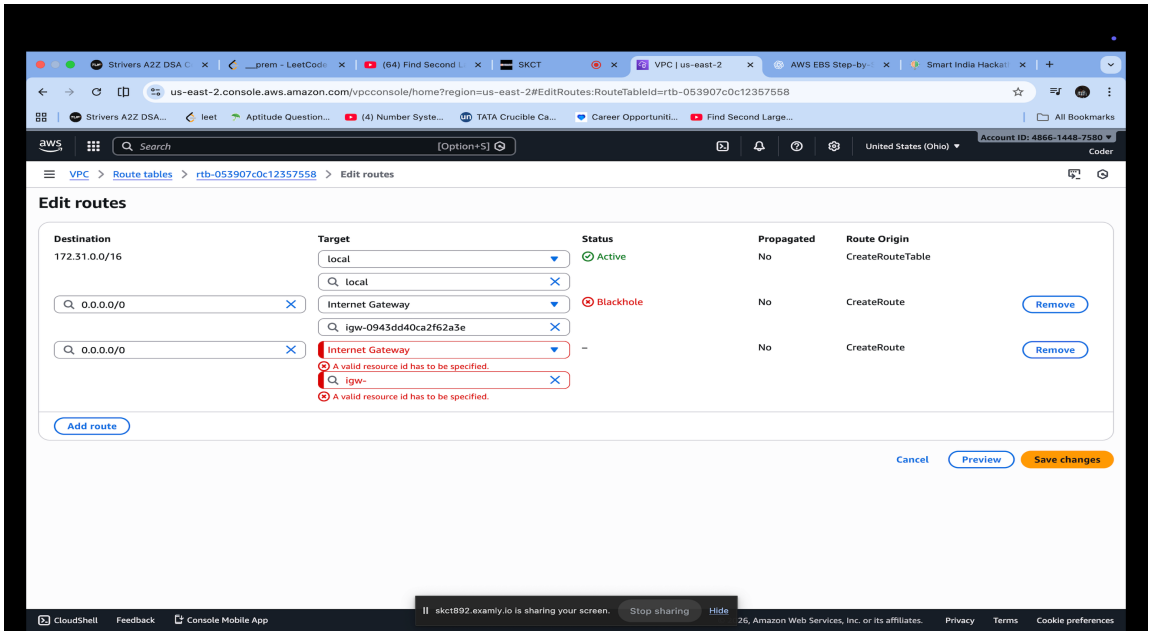
This separation ensures that even if the public layer is compromised, internal servers remain protected.

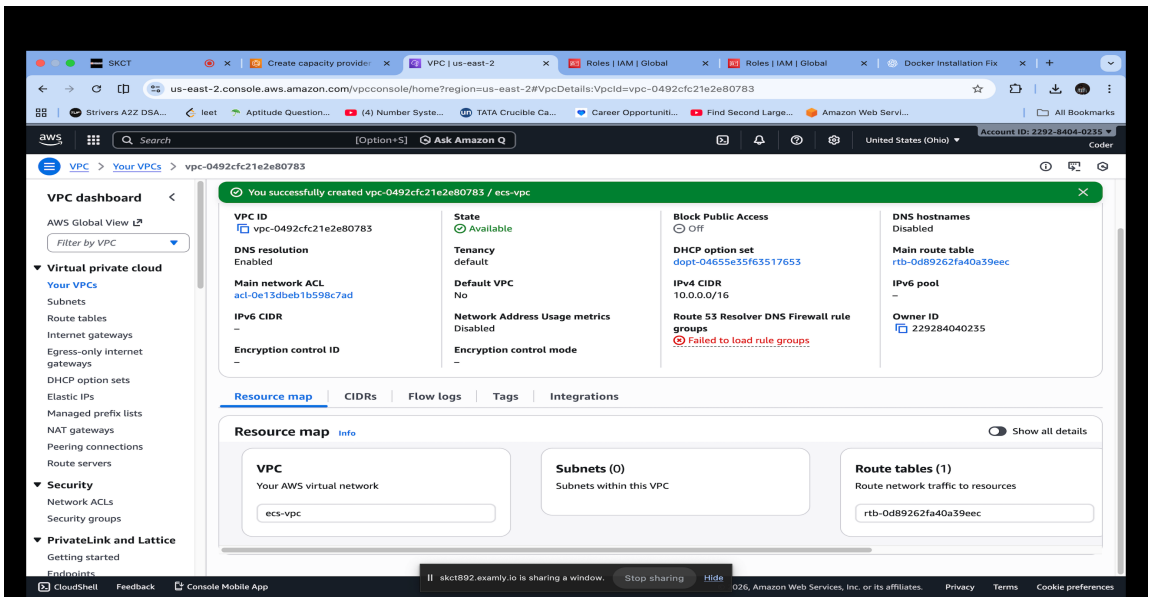
5. Architecture Flow Diagram

```
Internet
   |
Firewall
   |
Public Network
   |
Secure SSH Access
   |
Private Network
   |
Internal Application Server
```




us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#LaunchInstances:
EC2 > Instances > Launch an instance
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type | Info
ssh
Protocol | Info
TCP
Port range | Info
22
Source type | Info
Anywhere
Source | Info
Add CIDR, prefix list or security group
0.0.0.0/0
Description - optional | Info
e.g. SSH for admin desktop
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.
Add security group rule
Configure storage Info
Advanced
1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted
Add new volume
Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle
Summary
Number of instances | Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-03ea746da1a2e36e7
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#EditRoutes:RouteTableId=rtb-053907c0c12357558
VPC > Route tables > rtb-053907c0c12357558 > Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
172.31.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
Internet Gateway
Blackhole
No
CreateRoute
Remove
igw-0943dd40ca2f62a3e
0.0.0.0/0
Internet Gateway
No
CreateRoute
Remove
A valid resource id has to be specified.
igw-
A valid resource id has to be specified.
Add route
Cancel
Preview
Save changes
skct892.examly.io is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#VpcDetails:VpcId=vpc-0492cfc21e2e80783
VPC > Your VPCs > vpc-0492cfc21e2e80783
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started
Endpoints
You successfully created vpc-0492cfc21e2e80783 / ecs-vpc
VPC ID
vpc-0492cfc21e2e80783
State
Available
Block Public Access
Off
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
default
DHCP option set
dopt-04655e35f63517653
Main route table
rtb-0d89262fa40a39eec
Main network ACL
acl-0e13dbeb1b598c7ad
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
IPv6 CIDR
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
Failed to load rule groups
Owner ID
229284040235
Encryption control ID
Encryption control mode
Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
Show all details
VPC
Your AWS virtual network
ecs-vpc
Subnets (0)
Subnets within this VPC
Route tables (1)
Route network traffic to resources
rtb-0d89262fa40a39eec
skct892.examly.io is sharing a window.
Stop sharing
Hide
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

6. Security Design and Access Control

Security is implemented using multiple layers to ensure strong protection:

Firewall Protection

- Only required ports such as SSH (22) and HTTP/HTTPS (80/443) are allowed
- All other ports are blocked by default

SSH Access Control

- Direct SSH access from the internet is not permitted
- Administrative access is restricted and controlled

Private Server Protection

- Internal application servers do not have public access
- Servers are isolated within a private network

7. Access Flow

- Employees access the internal application through permitted ports only
- Administrators use secure SSH access for management
- Unauthorized access attempts are blocked by firewall rules
- Private servers remain isolated from the public internet

8. Common Security Issues and Solutions

Issue 1: Servers exposed directly to the internet

Solution: Servers are placed in a private network

Issue 2: SSH access open to everyone

Solution: SSH access is restricted to authorized users only

Issue 3: All ports open by default

Solution: Only necessary ports are allowed

9. Constraints and Assumptions

- No advanced intrusion detection or prevention systems are used
- Only basic firewall and access control mechanisms are applied
- A single internal application server is assumed
- The project focuses on secure design rather than actual deployment

10. Conclusion

This project presents a secure cloud network architecture designed to protect internal applications. By using private servers, firewall rules, and restricted SSH access, the design significantly reduces security risks while maintaining necessary accessibility. The architecture demonstrates best practices for protecting internal systems in a cloud environment.