

# **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

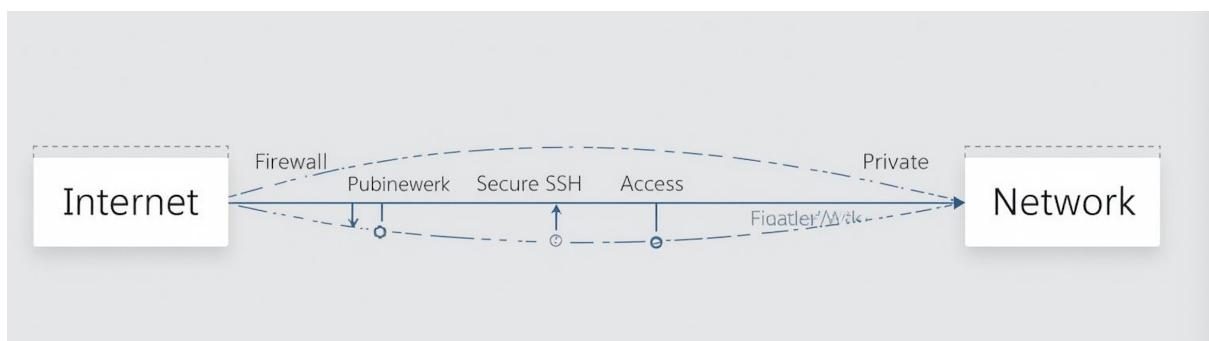
This separation ensures that even if the public layer is compromised, internal servers remain protected.

## 5. Architecture Flow Diagram

```

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

```



## 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.