



CELEBAL TECHNOLOGY INTERNSHIP (CSI)

Name: Harsh Tongariya

College: Arya College of Engineering Information
Technology

Domain: Cloud Infra & Security

Student ID: CT_CSI_CI_1160

Research & Implementation Document

Title: Implementation of Secure Three-Tier Architecture in Azure

1. Introduction

This document provides a comprehensive R&D guide to implement a secure three-tier architecture in Microsoft Azure, following the n-tier architectural style. The deployment consists of three logically separated subnets: Web Tier, Application (App) Tier, and Database (DB) Tier. Each subnet will host two Virtual Machines (VMs): one running Linux (Apache) and another running Windows (IIS) to demonstrate cross-platform deployment.

The architecture enforces strict network isolation policies to follow zero-trust principles:

- Web Tier → Internet (Allowed)
- Web Tier → App Tier (Allowed)
- App Tier → DB Tier (Allowed)
- DB Tier → Any Other Tier (Denied)

2. Goal Recap

Create:

- 3 Subnets: Web, App, and DB
- Deploy 6 VMs: 2 per subnet (1 Linux + 1 Windows)
- Configure:
 - Apache on Linux VMs
 - IIS on Windows VMs
- Setup Network Security Groups (NSGs) to control access as follows:
 - Web Tier: Only talks to App Tier, and can go to Internet
 - App Tier: Talks to DB and Web Tiers

- DB Tier: No communication with Web or App Tier

3. Step-by-Step Deployment

Step 1: Create Resource Group

1. Go to [Azure Portal](#)
2. Search “Resource groups”
3. Click Create
4. Name: three-tier-rg
5. Region: Central India
6. Click Review + Create

The screenshot shows the Microsoft Azure Resource Groups page. At the top, there's a header bar with the Azure logo, a search bar, and various navigation icons. Below the header, the main title is "Resource groups". A message at the top says, "You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience." There are filter options for "Subscription equals all" and "Location equals all". The table below lists the resource groups:

Name	Subscription	Location
NetworkWatcherRG	Azure for Students	Central India
three-tier-rg	Azure for Students	Central India

At the bottom of the page, there's a footer with system status (31°C Haze), a taskbar with various application icons, and a system tray showing the date and time (29-06-2025).

Step 2: Create Virtual Network + Subnets

1. Go to “Virtual Networks” > Create
2. Name: three-tier-vnet

3. Resource Group: three-tier-rg

4. Address space: 10.0.0.0/16

The screenshot shows the Microsoft Azure portal interface. A deployment named "three-tier-vnet-1751204722755" is shown as complete. Deployment details include:

- Deployment name: three-tier-vnet-1751204722755
- Subscription: Azure for Students
- Resource group: three-tier-rg

Timestamp: Start time: 6/29/2025, 7:15:57 PM; Correlation ID: 95a9bd98-553e-4a12-a175-458537a1ecf4. The portal also features a sidebar with links for Cost management, Microsoft Defender for Cloud, Free Microsoft tutorials, and Work with an expert.

Now add 3 subnets:

- WebSubnet → 10.0.1.0/24
- AppSubnet → 10.0.2.0/24
- DBSubnet → 10.0.3.0/24

5. Click Review + Create

Step 3: Create Network Security Groups (NSGs)

You'll create 3 NSGs, one per subnet.

3.1 Create NSG for Web Tier:

1. Go to "Network Security Groups" > Create
2. Name: web-nsg
3. Add Inbound Rule:

- Allow HTTP (Port 80) from Internet
- Source: Any | Destination: Any | Port: 80 | Action: Allow

4. Outbound Rule:

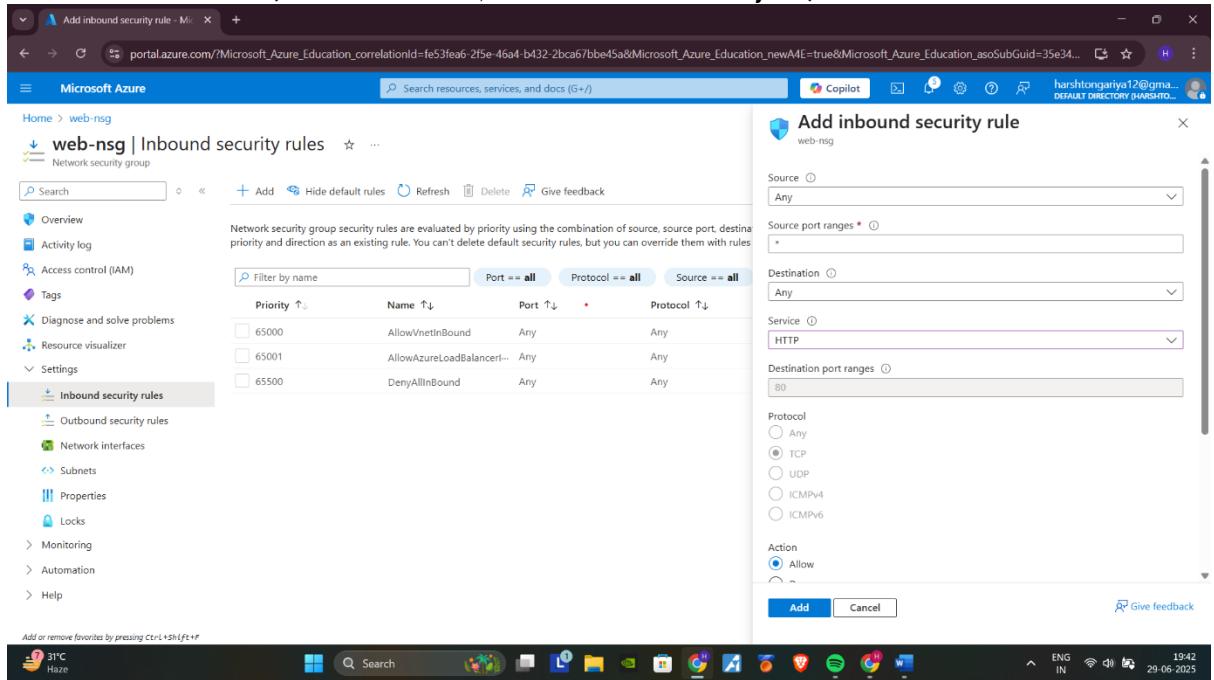
- Allow to AppSubnet 10.0.2.0/24 on required ports

3.2 NSG for App Tier:

- Inbound: Allow from WebSubnet 10.0.1.0/24
- Outbound: Allow to DBSubnet 10.0.3.0/24

3.3 NSG for DB Tier:

- Inbound: Only allow from AppSubnet 10.0.2.0/24
- Outbound: Block all (Default is allow, so add a rule to deny all)



Add outbound security rule

web-nsg

10.0.2.0/24

Service: Custom

Destination port ranges: 1

Protocol: Any

Action: Allow

Priority: 100

Name: Allow-Outbound-to-AppSubnet

Outbound security rules

Priority	Name	Port	Protocol
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

app-nsg | Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-Outbound-to-D...	Any	Any	Any	10.0.3.0/24	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Step 4: Associate NSGs to Subnets

1. Go to your Virtual Network → Subnets
2. Click each subnet → Associate the right NSG:
 - o WebSubnet → web-nsg
 - o AppSubnet → app-nsg

- DBSubnet → db-nsg

Edit subnet

Include an IPv6 address space This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access)

Security

Simplify Internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Network security group web-nsg

Route table None

Service Endpoints

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Select a service endpoint

Save **Cancel** [Give feedback](#)

Edit subnet

NAT gateway None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Network security group db-nsg

Route table None

Service Endpoints

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Select a service endpoint

Subnet Delegation

Delegate subnet to a service None

Network Policy for Private Endpoints

The network policy affects the types of network policies that control traffic going to the private endpoints in this subnet. [Learn more](#)

Private endpoint network policy Disabled

Save **Cancel** [Give feedback](#)

Step 5: Create Virtual Machines (6 Total)

Repeat below steps 6 times (2 per subnet; 1 Linux + 1 Windows)

For Linux VM (Apache):

1. Go to Virtual Machines > Create VM

2. Name: web-linux, app-linux, db-linux
3. Image: Ubuntu LTS
4. Size: B1s (free tier)
5. Username: azureuser
6. Subnet: Select the right subnet (Web/App/DB)
7. Public IP:
 - o Web Tier: Yes
 - o App & DB Tiers: No

8. Custom data (scroll to Advanced tab → Custom data):

Paste this (auto installs Apache):

- bash

```
sudo apt update
```

```
sudo apt install apache2 -y
```

```
sudo systemctl start apache2
```

```
sudo systemctl enable apache2
```

9. Click Review + Create

For Windows VM (IIS):

1. Same as above but choose Windows Server 2019/2022
2. Subnet: Same logic
3. Public IP:
 - o Only Web Tier VMs should have Public IP
4. After login (via RDP):
 - o Open PowerShell:

`Install-WindowsFeature -name Web-Server -IncludeManagementTools`

`Start-Service W3SVC`

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and a Copilot button. The main area displays a 'Create a virtual machine' wizard step, indicating 'Validation passed'. Below this, the 'Basics' section shows configuration details: Subscription (Azure for Students), Resource group (three-tier-rg), Virtual machine name (web-linux-vm-01), Region (Central India), Availability options (Availability zone), Zone options (Self-selected zone), Availability zone (1), Security type (Standard), Image (Ubuntu Server 22.04 LTS - Gen2), VM architecture (x64), Size (Standard_B1s (1 vcpu, 1 GiB memory)), Enable Hibernation (No), Authentication type (Password), Username (azureuser), and Public Inbound ports (SSH, HTTP). Buttons for 'Previous', 'Next >', and 'Create' are at the bottom. A note at the bottom right says 'Download a template for automation' and 'Give feedback'.

Below this, the 'Compute infrastructure | Virtual machines' page is shown. It has a sidebar with 'Overview', 'All resources', and 'Infrastructure' sections, with 'Virtual machines' selected. The main area shows a table of virtual machines:

Name	Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address	Disk
web-linux-vm-01	Azure for Students	three-tier-rg	Central India	Running	Linux	Standard_B1s	40.81.224.136	1
web-windows-vm-01	Azure for Students	three-tier-rg	Central India	Running	Windows	Standard_B1s	20.193.128.113	1

At the bottom, a note says 'Showing 1 - 2 of 2. Display count: 10' and 'Give feedback'.

Step 6: Test Network Connectivity

- Use ping/curl from:

- Web → App:

- App → DB:
- DB → Any:
- Web → DB:
- Web → Internet:
- App → Internet:

4. Conclusion

The described architecture follows Microsoft's recommended n-tier design pattern, enabling:

- Security isolation between functional layers.
- Cross-platform application support (Linux + Windows).
- Scalable deployment of services.
- Tight access controls using NSGs and routing.

This structure is ideal for production-grade applications requiring modularity, maintainability, and robust security.