To achieve your request, we’ll break it into **key components** and show you how to implement them. Here's a **complete plan** including **subnet creation, VM deployment, network rules**, and **server configuration**.

## Requirements Summary

| **Tier** | **VM Count** | **Access Rules** | **Internet Access** | **Server** |
| --- | --- | --- | --- | --- |
| Web Tier | 2 (Linux + Windows) | Can access App Tier only | Allowed | Apache (Linux), IIS (Windows) |
| App Tier | 2 (Linux + Windows) | Can access Web + DB Tier | No | Apache (Linux), IIS (Windows) |
| DB Tier | 2 (Linux + Windows) | No access to Web/App Tier (Inbound only) | No | Apache (Linux), IIS (Windows) |

## Infrastructure Steps (Assuming Azure or AWS, similar applies)

You can specify which cloud platform you're using (AWS, Azure, GCP) and I’ll give you exact CLI or Console steps. Below is a generic infrastructure-agnostic setup using high-level concepts.

### Step 1: Create Network and Subnets

**VNet / VPC CIDR block**: 10.0.0.0/16

| **Tier** | **Subnet Range** |
| --- | --- |
| Web Tier | 10.0.1.0/24 |
| App Tier | 10.0.2.0/24 |
| DB Tier | 10.0.3.0/24 |

### Step 2: Create NSGs (Network Security Groups)

| **NSG** | **Rules** |
| --- | --- |
| Web NSG | Allow inbound from Internet (HTTP/HTTPS), outbound to App subnet |
| App NSG | Allow inbound from Web subnet, outbound to DB subnet |
| DB NSG | Allow inbound from App subnet only, **deny all outbound** |

**Important Notes:**

* Attach each NSG to its subnet.
* Use security rules to restrict access:
  + Web NSG: Allow HTTP/HTTPS (ports 80, 443) from Internet
  + App NSG: Allow access on port 80/443 from Web subnet
  + DB NSG: Allow only internal access from App subnet (e.g., MySQL/MSSQL)

### Step 3: Deploy VMs in Each Subnet

| **Tier** | **OS** | **Hostname** | **Notes** |
| --- | --- | --- | --- |
| Web Tier | Linux | web-linux | Apache installed |
|  | Windows | web-win | IIS installed |
| App Tier | Linux | app-linux | Apache installed |
|  | Windows | app-win | IIS installed |
| DB Tier | Linux | db-linux | Apache installed (or DB Server) |
|  | Windows | db-win | IIS installed (or DB Server) |

Ensure these VMs are deployed **in their respective subnets**.

### Step 4: Configure Internet Access

* Create **NAT Gateway / Internet Gateway** and associate it **only with Web Tier subnet**
* App and DB tiers should **not have** internet route.

### Step 5: Install Web Servers

#### Linux VM (Apache)

bash

CopyEdit

# Ubuntu/Debian

sudo apt update

sudo apt install apache2 -y

sudo systemctl enable apache2

sudo systemctl start apache2

# RHEL/CentOS

sudo yum install httpd -y

sudo systemctl enable httpd

sudo systemctl start httpd

#### Windows VM (IIS)

Use PowerShell as Administrator:

powershell

CopyEdit

Install-WindowsFeature -name Web-Server -IncludeManagementTools

Test by opening the IP in a browser.

### Step 6: Test Access

* From Internet: Only Web Tier should be accessible
* Web Linux/Windows: Should access App Linux/Windows (via internal IP)
* App Tier: Should access DB Tier (port 3306, 1433, etc.