🔐 Azure Network Security Architecture (AZ-500)

📌 Project Overview

This project demonstrates the design and implementation of a secure Azure network architecture using hub-spoke topology, network segmentation, Network Security Groups (NSGs), and secure administrative access.

The goal is to eliminate public exposure, restrict lateral movement, and enforce least-privilege network access, aligned with AZ-500: Azure Security Engineer Associate objectives.

🎯 Objectives

- Design an enterprise-style hub–spoke network architecture
- Implement network segmentation using subnets
- Enforce least-privilege traffic control using NSGs
- Remove public exposure from workloads
- Enable secure administrative access using Azure Bastion

🏗️ Architecture Overview

High-level components:

- Hub Virtual Network (shared security services)
- Spoke Virtual Network (application workloads)
- Azure Bastion for secure VM access
- Network Security Groups for traffic control
- VNet peering for controlled connectivity

Traffic Flow:

- Internet → Web Subnet
- Web Subnet → App Subnet

- App Subnet → Database Subnet
- Administrative access → Azure Bastion only

📌 (Architecture diagram available in /architecture folder)

🧱 Network Design

Virtual Networks

VNet	Address Space	Purpose
vnet-hub	10.0.0.0/16	Centralized security services
vnet-spoke	10.1.0.0/16	Application workloads

Subnet Layout (Spoke VNet)

Subnet	CIDR	Purpose
web-subnet	10.1.1.0/24	Frontend tier
app-subnet	10.1.2.0/24	Application tier
db-subnet	10.1.3.0/24	Database tier

🔐 Security Controls Implemented

1️⃣ Network Segmentation

- Tiered subnet design prevents lateral movement
- Separate NSGs applied at subnet level

2️⃣ Network Security Groups (NSGs)

Subnet	Allowed Traffic
Web	HTTP/HTTPS from Internet
App	Traffic only from Web subnet
DB	Traffic only from App subnet

- Default deny-all rule enforced
- Explicit allow rules for required ports only

3️⃣ Secure Administrative Access

- Virtual Machine deployed without a public IP
- SSH/RDP access enabled only via Azure Bastion
- No inbound management ports exposed to the internet

4️⃣ Hub–Spoke Connectivity

- VNet peering configured between hub and spoke
- Enables centralized security services without flattening the network

🛠️ Technologies Used

- Azure Virtual Networks
- Network Security Groups (NSGs)
- Azure Bastion
- Azure Virtual Machines
- VNet Peering