Security+ Lab Guide: Top 5 Ways to Protect Azure Cloud

Objective:

Help students understand and implement 5 essential security best practices in Azure.

Requirements:

- Azure subscription
- Admin access to Azure Portal
- A deployed Virtual Machine

1. Enable Multi-Factor Authentication (MFA)

Why it matters: Protects Azure identities from credential theft and brute-force attacks.

Steps:

1. Azure Portal > Azure Active Directory
2. Users > MFA
3. Enable for user
4. Login & set up MFA

2. Use Role-Based Access Control (RBAC)

Why it matters: Enforces least privilege.

Steps:

1. Azure Portal > Subscriptions > IAM
2. Add role (e.g., Reader)

3. Set Up Azure Firewall or NSGs

Why it matters: Blocks unwanted traffic.

Steps:

1. VM > Networking > NSG

2. Deny RDP (port 3389)

4. Enable Microsoft Defender for Cloud

Why it matters: Security posture & recommendations.

Steps:

1. Defender for Cloud > Enable Plan

2. Follow recommendations

5. Enable Logging and Alerts

Why it matters: Visibility into changes/attacks.

Steps:

1. Monitor > Activity Logs

2. Export Logs

3. Alert Rules

Summary Table:

1. MFA - Block stolen creds

2. RBAC - Least privilege

3. NSG/Firewall - Access control

4. Defender - Security posture

5. Logs - Monitoring

Worksheet:

1. MFA protects against? _____

2. Role for view-only? _____

3. Port to block RDP? _____

4. Alerts configured? _____