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. Go to Azure Portal > Azure Active Directory.  
2. Click Users > Multi-Factor Authentication.  
3. Select a user and click Enable.  
4. Login to that user’s account in private browser.  
5. Set up MFA.

# 2. Use Role-Based Access Control (RBAC)

Why it matters: Limits user access based on their role (least privilege).

Steps:  
1. Go to Azure Portal > Subscriptions.  
2. Click your subscription.  
3. Go to Access Control (IAM).  
4. Add role assignment (e.g., Reader) to a user.

# 3. Set Up Azure Firewall or NSGs

Why it matters: Blocks unwanted traffic at the network level.

Steps (NSG):  
1. Go to VM > Networking.  
2. Click Network Interface > NSG.  
3. Add Inbound Rule to deny port 3389.  
4. Set Priority: 100, Name: Deny-RDP.

# 4. Enable Microsoft Defender for Cloud

Why it matters: Provides threat detection and security posture management.

Steps:  
1. Go to Microsoft Defender for Cloud.  
2. Enable Defender Plan.  
3. Check Recommendations.  
4. Follow a recommendation (e.g., enable disk encryption).

# 5. Enable Logging and Alerts

Why it matters: Allows visibility into changes and attacks.

Steps:  
1. Go to Monitor > Activity Log.  
2. Export Activity Logs.  
3. Create Diagnostic Setting.  
4. Create Alert Rule (e.g., email when VM is deleted).

# Summary Table

1. MFA - Blocks stolen credentials  
2. RBAC - Enforces least privilege  
3. NSG/Azure Firewall - Blocks unauthorized access  
4. Defender - Posture management  
5. Logs/Alerts - Detects suspicious actions

# Worksheet

1. What does MFA protect against? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
2. What role lets a user only view reports? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
3. What port to block to disable RDP? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
4. What alerts did you configure? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_