Domain: Network Security

Question 1: Faulty Firewall

Suppose you have a firewall that's supposed to block SSH connections, but instead lets them through. How would you debug it?

Make sure each section of your response answers the questions laid out below.

1. Restate the Problem

a firewall that's supposed to block SSH connections, but instead lets them through

2. Provide a Concrete Example Scenario

    ○ In Project 1, did you allow SSH traffic to all of the VMs on your network? Yes
    ○ Which VMs did accept SSH connections? Web1 (ippr
    ○ #) and web2(ippr#)
    ○ What happens if you try to connect to a VM that does not accept SSH connections? Connections refuse error Why? The vm port 22 is closed or being blocked

3. Explain the Solution Requirements

    ○ If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is? Error in the network security group
    ○ Which general configurations would you double-check?Inbound security rules
    ○ What actions would you take to test that your new configurations are effective? Try to ssh into VM

4. Explain the Solution Details

    ○ Which specific panes in the Azure UI would you look at to investigate the problem? Network security group -adjust incoming port rules
    ○ Which specific configurations and controls would you check? Action check ports (protocol priority
    ○ What would you look for, specifically? See what connection's being allowed, or which port being access and check the priority of incoming(higher than ssh connect.
    ○ How would you attempt to connect to your VMs to test that your fix is effective?
    ○ Run ssh to VM 's (ippr#)

5. Identify Advantages/Disadvantages of the Solution

    ○ Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?

- What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?Detection/monitoring control to detect any suspicious authentication attempt. I can use a Checkmk, and Languardian. Install security patches, backup data online