**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 does not appear to be actively blocking out SSH connections. Instead, it lets connections on this port, 22, to be allowed into the network
2. Provide a Concrete Example Scenario
   * Only the Jump Box was allowed SSH access to connect to it. All the other virtual machines, Web Servers and the ELK Server, were closed off.
   * This was done so that none of the web servers could be connected to straight from the internet. The only way to access any of these servers would be to connect to them from the Jump Box.
   * Attempting to connect to any of the web servers would simply offer a request denied message. This indicates that they could not be connected to from that port number.
3. Explain the Solution Requirements
   * If one of the Virtual Machines was accepting SSH connections that could mean that the rule I created was not working correctly. It should be checked again to confirm that it was denying traffic based on port 22.
   * Then it would be safe to check that the virtual machine was not configured with a public IP address. While potentially not the cause, it’s still worthwhile to restrict having a public IP to keep ease of mind.
   * After confirming the details of the rule to restrict access, its important to test to ensure the rule is working as intended. This can be done but attempting to connect via SSH from any command line/terminal.
4. Explain the Solution Details
   * The primary location to check for this behavior would be under ‘Inbound Rules’ in the Network Security Group. These rules dictate what is allowed or denied for incoming connections to VMs on the Network Security Group.
   * Check to ensure that attempting to connect to any of the web server VMs from anywhere that isn’t the Jump Box gets denied. Attempting to connect via SSH should result in a denied connection.
   * It’s critical to have a rule that allows only the Jump Box to connect to the VMs via SSH. A rule should be in place where the source is the Jump Box IP address and the destination is the virtual network on port 22. Then to test this rule you must first connect to the Jump Box via SSH. Then from this VM you can attempt to connect to the web server VMs.
5. Identify Advantages/Disadvantages of the Solution
   * This solution should guarantee that the VMs cannot be accessed via SSH from anywhere except for the Jump Box. This does not guarantee denial from all ports unless new rules were created to include all other ports. This ensures that the only way to access the web server VMs is through SSH specifically from the Jump Box
   * Logs can then be configured to record all attempts to access any of the VMs. This would help to diagnosis who and where might people be trying to access the VMs.