**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

The firewall is supposed to block SSH connections but it is misconfigured and is allowing SSH connections.

1. Provide a Concrete Example Scenario  
     
   * In Project 1, did you allow SSH traffic to all of the VMs on your network?
     1. No, I did not allow all SSH traffic to the VM’s.
   * Which VMs did accept SSH connections?
     1. I only allowed SSH connection from the internet to the JumpBox-Provisioner VM. I also allowed the JumpBox to SSH to the web server VM’s.
   * What happens if you try to connect to a VM that does not accept SSH connections?
     1. The connection is refused since the SSH key is not accepted.
2. Explain the Solution Requirements  
     
   * If one of your Project 1 VMs accepted SSH connections, what would you assume the source of the error is?
     1. I would assume the problem would be in the configuration of the firewall.
   * Which general configurations would you double-check?
     1. I would double check the inbound security rules to make sure that they are blocking SSH.
   * What actions would you take to test that your new configurations are effective?
     1. I would try to connect with SSH from a device that is not on the permitted list.
3. Explain the Solution Details  
     
   * Which specific panes in the Azure UI would you look at to investigate the problem?
     1. I would check the network security group for the devices in question.
   * Which specific configurations and controls would you check?
     1. I would make sure that there is a rule preventing SSH from all sources except the allowed devices.
   * What would you look for, specifically?
     1. I would look at the rules pertaining to port 22 since that in the well known port for SSH.
   * How would you attempt to connect to your VMs to test that your fix is effective?
     1. I would use a device that is not on that IP address.
4. Identify Advantages/Disadvantages of the Solution  
     
   * Does your solution guarantee that the Project 1 network is now "immune" to all unauthorized access?
     1. I would say yes it would be, but there might be a zero day threat that we don’t know about.
   * What monitoring controls might you add to ensure that you identify any suspicious authentication attempts?​
     1. I would set an alert for IP addresses that try and or gain access that are not on the allowed list.