Interview Question

Domain: Network Security

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

1. So this is problem with a configured firewall that is nonetheless allowing SSH traffic even though it is supposed to be blocked according to policy and there are firewall rules already established.
2. In the ELK stack project, a network was created using Azure cloud. The network security group was created and it had default security rules established by Microsoft. These rules have lower priorities but if your create a rule to allow SSH, for example, with a higher priority then SSH traffic can occur. In the cloud project, SSH connections were permitted from the public IP (mine) to the jumpbox VM internal IP address (not the public one) and then from the jumpbox to the internal virtual machines. Attempting to connect to a machine that is not configured to accept SSH will result in an error message such as “connection refused”.

The solution to unblocked SSH, when using the cloud, is to configure the security group to only accept SSH traffic from your network. In order to debug this problem, first look at the network security rules and verify the existence and priority of the rule to block or restrict access to and from SSH. Azure cloud has a numbering scheme for security rules inwhich the lower the number the higher priority. A second look at security rules should verify that a higher priority rule isn’t allowing SSH while a lower priority rule blocks. Also, you should verify that the IP addresses are corrected if limited SSH traffic is permitted.