It’s important for organizations to have a good understanding of the layers of defense for a network, for example allowing SSH connections or blocking the connections to the firewall. In my Cybersecurity boot camp, we created a Project that’s identical but I did allow authorized SSH connections for testing. In the initial project, I only allowed only my jumpbox to be accessed through my personal IP address and the other VM’s were not accessible per my NetworkSecurity Group(NSG) rules. When I tried to SSH to the other VM’s through my jumpbox, I received a connection refused error because the port is closed or blocked by a firewall.

If there was a VM allowing access through SSH keys, the first place to check is the NSG. Secondly, check the inbound access rules because this is where you define rules for incoming and outgoing traffic. Once the rules have been defined, then go test connections to verify the port is blocked from SSH.

To implement this go into Azure’s Network Security Group and check the incoming port rules. Next, review the ports protocol to see what connection’s being allowed, or which port is being accessed and make sure the priority is set high. To make sure this fix is effective, I would attempt to SSH from my personal IP address to my jump box which has access to the VM’s, but blocked by my Network Security Group rules.

Making changes to Network Security Group, does not immune all unauthorized access, however, you can strengthen your monitoring control by having detection/monitoring control to detect any suspicious authentication attempt like checkmk.