**Network Security**

**Question 1: Faulty Firewall**

The problem is that there is a firewall that is supposed to be set up to block SSH connections, but instead is letting them through. In Project 1 we allowed all VMs to accept SSH traffic through port 22. However, the VMs that we wanted to allow SSH to privately did not have public IP addresses. If you tried to SSH into a VM that does not accept SSH connections the connection will time out. Most likely because port 22 is not open, or you need the private IP address so you can set up a key between the machine you’re on and the machine you’re trying to SSH into.

In Project 1 if one of the VMs that I set up to allow SSH connections failed to allow me to SSH to it, I would assume two things. 1, it could be that I did not set up the private key between my machine and the VM. I would need to either **cat** and copy the key from my machine, or make a private key if that hadn’t been done yet. Then I would need to input that key into the settings of the VM and input the username I’m trying to SSH to. In Project 1 this was done in the Azure portal in the VM settings under ‘Reset Password’. 2, I would need to make an inbound security rule to allow SSH from my physical machines IP address over port 22. This can also be done in the Azure portal in the VM settings. Security rules are found under the ‘Networking’ tab. After having checked both of those things I would then attempt to SSH to the VM, it should now work.

Making these changes to the VMs in Project 1 does make it more secure but it does not make it ‘immune’ to all unauthorized access. To make sure you keep your VMs secure and free of unwanted access you can add some monitoring controls to help monitor unwanted access. In Project 1 we set up a Jump Box as the ‘gatekeeper’ to SSH to all of the VMs. The advantage of doing this is that only authorized users can SSH to the VMs. Another thing we did in Project 1 to help monitor our VMs was install an ELK server. Doing this will help you monitor changes to the file systems of the VMs on the network and system metrics. With the ELK server we installed Filebeat, which is used to detect changes to the file systems and collect Apache logs. You can also install Metricbeat with the ELK server. Metricbeat allows you to record system metrics. It also allows you to monitor and detect SSH login attempts, failed sudo escalations, and CPU and RAM usage. Adding these things to your network can help you harden and monitor it to prevent unwanted access.