Network Security

Faulty Firewall

If I configured my network to block any SSH from outside my network and someone was able to enter. The first thing I would do would be to check my NSG and make sure that I have only allowed my IP or whichever IP address I allowed. In order for someone to be able to SSH into any of the VMs. The person must first go through the gateway which is the JumpBoxProvisoner VM. If someone tries to SSH from outside of the gateway. They will be denied access due to their lack of a public access key. If someone was able to connect from the outside. The first place I would check is my Inbound Security Ruel which allows SSH from the JumpBox Provisioner VM only. I would check that the correct IOP address was entered and that only my IP address is allowed to SSH as well. In order to make sure that the new configurations work. I would try to SSH from a different IP address outside of the JumpBox VM. If I get a denied response, that means my changes were done correctly. TO go into detail of where I would check these configurations. I head to the Network Security Group section and look in the Inbound Security Rules section. I would make sure to check that the priorities are set in the correct order and that the correct IP addresses are added in. Port 22 is SSH and I would make sure that all my rules that include that are correct. To check that everything is done correctly. I would double-check that no other IP address can enter and attempt SSH outside the gateway. My configuration would have one big flaw and that would be if someone ever had access to my own computer. They can enter due to my IP address being allowed and my public key is registered in the NSG. I would have to make sure to create filebeat and metric beat configurations to monitor my network incase anyone from outside the gateway attempts to enter. If someone does get access to my computer, I would also see times that I wasn’t online and somehow someone was able to SSH successfully using my IP address.