If I have a fire wall that was inationally suppose to block ssh connections but is instead allowing them in first I will look at my nsg for the network and check what vms im letting in the network and see if I have any rules that are countering each and make any changes for example I would make a rule to block all traffic except a jump box and then make a separate rule that will let my jumpbox into the network. This way I can look at any traffic that was getting in and I will add internal ips to the config file to let me into other vm that way a have a quarantined network. A advantage to this is that it will be well protected but a disadvantage would be adding and removing vm to the net work and the nsg rule smay cause problems to more complex networks.

**Unsecured Web Server**

If I find a server that is running http on port 80 this is what ill do. First it will need to be open because I need traffic from the internet to go thru it to get to my network but I will put safety procations because they can gain access easily thru it or ddos the server itself so first ill install elk to monitor the traffic and log it and prevent any attacks I will as well put in metricbeat to monitor and metrics and statistics this way im getting information from the internet but it will be monitored and checked on just in case and I would as well make a backup webserver just in case if the first one goes down I have a second that can take over while the issue is getting fixed