Suppose you find a server running HTTP on port 80, despite compliance guidelines requiring encryption in motion. What do you do? ​​

1. Restate the Problem

The issue we are running into in this specific scenario is traffic running through port 80 from a unprotected server HTTP. Compliance guidelines require us to have encryption in motion. My first action would be to stop all traffic through port 80 for the time being until some updated inbound rules can be created. I know this because I’ve had a similar scenario in a recent ELK stack project I had created. HTTP traffic was allowed through port 80 but I made the inbound IP static and had it set to only my personal IP. In a real world deployment I would use a more encrypted access for the jumpbox to limit who can gain access.

As discussed earlier HTTP on port 80 needs to be strictly monitored and only allows certain IP addresses to access it. For my previous project I was able to create my own network, jumpbox, and containers using the azure portal. The portal allowed me to set my own ports, IP’s with access, inbound and outbound rules, peering rules and more. Personally I hardened my security by limiting open ports and backend traffic. The advantages of my solution can be simplified to target hardening, more secure traffic, oversight of network access points. The disadvantages to my solution would be user error, if anything is wrong in any scripts or playbook configurations then things may not run due to the limited access.