Working with Azure has really been eye opening for me. If I am being completely honest, I did not grasp everything in the two networking weeks. I struggled to understand everything from a conceptual standpoint and felt nervous going into Azure but seeing all this working from a bird's eye point of view really made it all click. I have gone from dreading networking to looking into network security jobs. It has all been a long, long puzzle that has felt great to finally figure out.

The question is, what have I learned? To fully answer that, I must start off by saying that I have come to understand that just because you go from on premise to the cloud, you are not any safer from a security standpoint. Any flaws you have in your network are not magically solved because you have moved your operations to the cloud. Moving to the cloud only changes the location of your network, not the attack surface of it.

It seems to me that the biggest key to this project and my main takeaway is the importance and nuances of setting up Network Security Group rules. Every wall I hit in working on the project was solely an NSG issue that required me to really dig in and figure out the issue. A lot of the times, my key to success was just reading error messages and using that as a starting point to figure out where to go next. In the past I have only messed around with firewalls and ports to get things like my Xbox to connect so that I could get to playing some games. I have now, through painstaking trial and error, become comfortable working with NSGs, and thus, firewalls in general. Nick Strong once brought up the concept of thinking about the traffic as a semi-truck and trailer, and I extended that analogy into the firewall rules. From my time as a driver as well, I know that to leave a facility with a load, you need permission to leave the premises and part of that is a clear destination. Well, when you arrive at the destination, they also need to know where you came from, confirmation that you can enter their premises, and which dock you are unloading the trailer. This works just like in the NSG rules; you need a source and destination port rule set for all the NSGs you are going to. If you are moving traffic from inside one NSG to the other, you need rules in place on both NSGs to allow that connection to be successful.

Through the project I have also had some practice using containers and Docker and reading into the student guides for Week 12 on the subjects has given me a semi-strong understanding of the application of these powerful little machines. I can see their use and love their ability to be destroyed and rebuilt at a moment's notice. I also realize the security benefit they provide through this ability - if one container becomes compromised, it is as easy as deleting and rebuilding on the fly. This, of course, also means that we must properly set these containers up to be as stateless as possible; if data is on one container that no other instance has, we cannot simply delete and rebuild without losing that data. We must move that data to a central location and extract the data as much as possible.

In the future, I really hope to work with Azure again. If I could build/maintain a network on Azure using Linux machines, then go in and work on them using the command line/bash, I could die a happy man.