Cloud Network Security

In project 1 I deployed a cloud network

I did have to configure access controls to this network, I restricted the traffic flow going through the server.

The first rule that I made allowed all traffic to flow inside the virtual network. The source and the destination were set to internal network, this allowed all the machines that we created to be able to communicate with each other. The second rule that I made allowed all traffic that was coming from the load balancer in our network. The third rule that I made blocked all traffic from other sources like the internet. Any source in the network that is being protected by the firewall will have the traffic coming from the internet blocked.

These details were important when setting up our cloud network because we had to make sure that it was secure and no incoming traffic from the internet would be allowed through.

I also created an inbound rule for the jump box that allowed SSH access to the jump-box using a public key that we generated through git Bash. The jump-box allows access to the virtual machines that we created only from specific IP addresses. I configured my jump-box to be able to run Docker containers. I then used the ansible container in the jump-box to configure the other virtual machines. The way I accessed the other servers through the jump-box was by SSHing into the jump-box using the command SSH sysadmin@mypublicip. After I was in the jump-box I needed to see what container was the one that I was using so I listed them using the command 'sudo docker container list -a'. After I found my container I started it with the command 'sudo docker start mycontainer' and finally I accessed the container by using the command 'sudo docker attach. Once I was inside the container I could SSH into the other 3 web servers using the command 'ssh sysadmin@webserverip'.

There are alternatives to jump-box and one of them is called Azure Bastion. It is very similar to jump-box in that it is used to securely access resources on a network. It differs from jump-box in that it does not require a public IP address or VPN gateway connectivity to the virtual machines that it will be connected to. Jump-box also tends to be more locked down and hardened compared to Bastion. Some pros of using a VPN is that you can hide your location and also keep internet service providers from tracking your data and lastly a VPN allows you to visit sites that may be georestricted. One con of using a VPN is that it can fail and cause your location to leak or the services may stop working. One of the biggest drawbacks of using jump servers is that they have a single point of failure which can jeopardize your entire network. The choice of which one to use is going to depend on the scale of use and the individual needs.