Domain: Cloud Security
Cloud Access Control

When controlling access to the cloud network I would implement access controls that can only be accessed by approved users such administrators or engineers, while blocking access from all other users that did not have permission to access to the environment.

In Project 1, I deployed a cloud network that contained multiple virtual machines on Azure. I configured access controls to ensure that only my IP address had access to prevent any outsiders from gaining access to my virtual networks and virtual machines inside the network. I created firewalls, ssh keys, a jump box, a load balancer, and inbound security rules to gain access into the virtual machines while blocking all other inbound traffic.These controls were necessary to keep other users from gaining access to my virtual network without my permission. I created separate network security groups for my Azure virtual network and for my ELK virtual network. I set these firewalls up to only allow specific traffic to have access to the jump box, the load balancer, and the ELK server. The load balancer rules allow the authorized users to gain access to the DVWA containers through the public key, through port 80, while distributing the workload to the multiple containers. The jump box rules only allow users with access to the private ssh key into the DVWA containers, through the private IP address and to the ELK server via port 22. The DVWA containers can access the ELK server through the public ssh key through ports 5601 and 9200. These rules were established through Kibana, filebeat, and metricbeat. The NSG that protects the ELK server only allows traffic from port 5601. Each access control made it so there were restrictions in place to prevent unwanted access from outside sources to both of my virtual networks. This preventive action ensures that my servers can not be accessed without my permission to ensure that my data is kept secure. These restrictions were necessary for the project to show that I understand how to implement security rules and how to set up appropriate access controls to protect the virtual network and the virtual machines inside the network.

The advantages of the jump box is it is a secure computer that can only be accessed by users with the ssh key. It forces the user to prove its credentials to prevent unauthorized users from gaining access to privileged information within the network. The jumpbox in my project was scalable because I only have four virtual machines within my network that only I have access to. If I were to allow multiple users to gain access through the jumpbox it could potentially slow down production time for the users. The jumpbox is a single server, if there was a successful breach the attacker would be able to access all of the virtual machines within the network, gaining access to all the secure data. If I were setting up the infrastructure for a larger network I would also use a VPN. The VPN allows the users to sign in from a private network disguising their true network information by using the VPN's server information instead of their own. The VPN allows employees to access secure data while preventing access from unwanted parties. The disadvantages of the are VPN's can be complicated to set up and if improperly configured can cause leaks showing that you are trying to hide protected information. The VPN's connection hides your browser information, if it is suddenly lost you could be at risk for violating ISP terms of service and your ISP could shut you down immediately. The VPN can also slow down your internet connection and could potentially be blocked completely by VPN blocking software.