Domain: Cloud Security

Question 1: Cloud Access Control

Ensuring the proper network security measures are implemented is important in preventing security breaches within private networks and organizations. Not having an understanding with the architecture and what each layer signifies creates an open invitation for cybercriminals to gain access and steal sensitive data, inject malware, and other cloud-related breaches.

In Project 1, we deployed a cloud network using Azure services. Access controls had to be configured in order to protect our network environment. We ensured that only authorized IP addresses and users had access to the network and blocked unwanted external access attempting to gain access to our cloud data by setting inbound rules in place. We also added additional layers of security by creating a jump server and network security groups.

Network security groups are a set of access control rules that protect virtual networks or a subnet. These rules monitor incoming and outgoing traffic and determine whether to allow or not allow within the network. Within the two network security groups in our cloud network, we created inbound rules. Our Red-TeamSG group allowed ports 80 and 22 from my IP to the cloud network. We also created an inbound rule in our jumpbox to allow SSH connections only from my IP address, which can be connected using GitBash. Our ELK-ServerSG inbound rules allow port 22 and port 5601 access to our cloud network only. These restrictions were set in place to prevent unwanted external traffic to my cloud network. Lastly, we created a rule that allowed our jumpbox complete access to our virtual network.

Our jumpbox serves as a pipeline allowing traffic into our network. We must first log into the jumpbox before establishing a connection, considering its control point. In order to connect to our network and begin initiating tasks, we must first connect to our jumpbox. We do this in GitBash using command line *ssh azadmin@20.228.243.125.* Once connected, we then can access our virtual machines and perform tasks.

Software scalability indicates a system's need for revamping given the amount of workload. A network is measured scalable when there's an increase of users, it has reached the maximum number of activity it can handle, or anything that pushes it to its max capacity handled without having to constantly rebuild it's design. Due to the expansion and growth in the development of software and security (not to mention the quick transition to WFH), I believe there are better ways to enhance cloud security networks. One specific alternative would be using a VPN. VPNs have many advantages such as controlling which users can gain access by required credentials, remote access to your office network, provide end-to-end encryption, etc. However, everything has its disadvantages. VPNs that offer higher security measures also come at higher costs. Another disadvantage is its complexity during the deployment process; this requires the right knowledge and understanding of data encryption, public network security, etc.

VPN servers are also not capable of excessive workload and were intended for smaller-scale, short-use. I believe VPNs should only be used temporarily for remote employees (large-scale or small-scale enterprises), subsequently, leveraging higher security measures.