Domain: Cloud Security

Question 1: Cloud Access Control

A cloud network without access controls is open externally for anyone to access its web servers, which makes it vulnerable to malicious activity.

1. Provide a Concrete Example Scenario

    - In Project 1, I deployed a Cloud network.
    - I had to configure access controls to this network to control how the network could be accessed.
    - I provided key based authentication to restrict access to my Source IP address only. I generated private and public key pairing to ensure that only my gateway was able to connect to the vulnerable Web VMs.
    - By implementing these access controls, I was able to control who was able to access my network. If the machine trying to connect to my network was not on my local network with my Source IP address, it would not be able to access my network, thus providing a barrier to entry from outsiders.

2. Explain the Solution Requirements

    - NSGs were created around the vNet to block external traffic from the internet from getting into the cloud network unless SSH was used from my Source IP address on my local network.
    - The TCP Protocol was implemented to allow only SSH traffic on Port 22. The TCP Protocol was also implemented so that the DVWA could only be accessed via port 80.
    - Each access control was put in place to ensure the data was only available to an authorized user.

3. Explain the Solution Details

    - I set inbound port rules on my Network to restrict access. I set an AllowSSH rule to only allow traffic from Port 22 from my local machine's IP address. I also set another rule to Allow the Jump Box to SSH into my vulnerable web virtual machines on Port 22. Additionally, I set up an inbound security rule to allow DVWA Access on Port 80 from my local machine's IP Address.
    - In order to access the Jumpbox, I have to use an SSH command with my username into the box while on my local network. For example,

ssh azadmin@jumpboxpublicipaddress.

- In order to access the web servers from my jumpbox, I have to use an SSH command with my username and the web server's local ip address. For example, ssh azadmin@webserverlocalipaddress.
- One advantage of this solution is privacy. I was able to ensure that I was the only one able to access my jumpbox and my web servers because it could only be accessed from my local home network and to get onto the web servers it required key pairing with my jump box. However, this also posed a disadvantage because it could be inconvenient if I was not on my local home network and wanted to access my jumpbox. Then, I would have to go in and manually change my inbound security rules to allow access from another public IP address.
- This solution can scale because my Virtual Network allows for multiple web VMs to be created.
- I prefer my jump box as the gateway solution to prevent outsiders from accessing my vulnerable web VMs. If I didn't have a jump box, I would have potentially exposed my web VMs to access by a bad actor from an external network.
- Connecting a VPN would have been difficult because it would have changed my public IP address to the IP address of the VPN host.
- Using a VPN would hide my real IP address and encrypt my internet connection.
- It is appropriate to use a VPN if I want to keep my browsing history private, change my online location, and/or keep my internet activities anonymous.