**Domain: Cloud Security**

**Question 1: Cloud Access Control**

How would you control access to a cloud network?

1. Restate the Problem.

Controlled access to a cloud network is a constantly occurring situation faced by all companies. Since it has resources that only the IT dept should be able to access, it’s therefore crucial that a company controls access to it. The overlying principle to go on is least privilege, where only the required IT engineers can access it but others cannot.

1. Provide a Concrete Example Scenario
   * In Project 1, did you deploy an on-premises or cloud network?

As one of our Cybersecurity course projects, we configured and deployed an Azure Cloud Network. This virtual network contained VM’s to Azure which only we and our own team were configured to access. Our approach was based on how an organisation would limit cloud access to the required engineers. We implemented remote access control therefore limiting access to only a select few of authorized people.

Although very restrictive these controls were necessary in order to reduce the security risk of making these vm’s more vulnerable to being breached.

What kinds of access controls did you configure, and why were they necessary?

* + How do these details relate to the interview question?
  + Therefore, these access control which were limited by only authorised parties with authorised IP addresses and ports followed the least privilege mantra were go whenever considering our approach to network access.

1. Explain the Solution Requirements

Once I had configured and deployed the virtual network, I then had setup a network security group around the whole subnet. This was to block traffic from all IP addresses except for mine and my team members. This network security group enabled inbound access to only one computer on the internal network which was the VM that was dedicated as the jump box. The network was also secured with all external access coming through the firewall first.

The next step was to configure additional NSG’s on the VM’s within the subnet. This setup was what allowed connections only between the jump box and the local IP addresses.

I then enforced the requirement of SSH keys to eliminate vulnerability to password brute-force attempts.

All these above steps were necessary actions required harden the security of the network when being accessed remotely.

1. Explain the Solution Details

The outcome of all these actions worked well as it achieved the goal of ensuring only the required people had access. While this gave us a very secure system, this would be difficult however to maintain and execute on larger scale as it requires updating the NSG every time a new user requires access to the network. The use of using SSH keys securely on a long-term basis also comes into question. To address these scenarios, we look at implementing a VPN gateway to the private network, where we could manage and monitor more users in a safer manner.

* + Which rules do you set for each NSG in the network?
  + How does access to the jump box work?
  + How does access from the jump box to the web servers work?

1. Identify Advantages/Disadvantages of the Solution
   * Does your solution scale?
   * Is there a better solution than a jump box?
   * What are the disadvantages of implementing a VPN that kept you from doing it this time?
   * What are the advantages of a VPN?
   * When is it appropriate to use a VPN?