Domain: Cloud Security

Question 1: Cloud Access Control

What is the best way to control access to a cloud network? Having a secure and robust network is vital to any business. There can be several ways to implement security within a network. One such way to do this would be to create a network security group that can control access to the servers and systems. The first step would be to determine what type of traffic you want allowed into your network. Generally you do not want to allow all traffic on any port through. To give you an example, for my first project in the cybersecurity bootcamp, I was tasked with creating a stand alone network with 4 vms. One would be the jump box, two would be web servers and the fourth would be the ELK server. Two network security groups were created, one for the jump box and web servers, the other for the ELK server.

Access was needed for each vm and http access needed to be granted for the web servers. The jump box was created as a single access point for the entire network. I created a few inbound rules that allowed traffic from specific ports to specific IPs. The rules that were created were to allow inbound traffic over port 22 and port 80 from only my public IP address and to allow inbound traffic over port 22 from the private IP of my jump box. This allows the admin to ssh in from only one IP. This ensures a high level of security.

Since there were network security groups, this was used as the firewall for the vms. Each vm is headless, so port 22 needed to be open. To minimize the risk of attack, access was only granted to one public IP address. Port 80 was open because the web servers required it. Port 5601 was open because Kibana required it.

The jump box acts as the administrative access point for both networks. It is the admin computer for setting up and configuring each vm. From the jump box the admin is allowed to ssh into any vm. A public key was created as a password for the jump box and each vm.

The disadvantages to this setup are the use of a public key, enabling port 80 instead of port 443, and allowing access from just one IP. To make this more secure, a couple of things can be implemented. One would be to allow access via VPN. This would allow control to the server at the user level and not by a single machine. This would also help keep track of who and when a user logs into the server. The downside to using VPN is that you would have to also create an Active Directory/LDAP network to allow access. Another option would be to enable multi-factor authentication. This can take additional time and resources to configure. Disabling the use of a public key and letting users access via Active Directory would be much more secure. Finally, disabling port 80 and enabling port 443 to access the web servers is much more secure because it encrypts the traffic.

The advantages of this configuration are that it is relatively quick and easy to set up. The network is scalable, so being able to add to this and implementing the above suggestions should not be a problem.