Domain Cloud Security
Question 1: Cloud Access Control

How would you control access to a cloud network?

How would I control access to a cloud network? I would control access to a cloud network by implementing network security group inbound rules. I actually deployed a cloud network on azure for a project I called OffSec Virtual Network (OffSecVNet). I created 5 virtual machines on the network which included a jump box with ansible, three web server machines, and an elk machine I would use to monitor the logs and data from the other machines with. I had to configure access controls to only allow the people who needed access at the time to it. Through the setup process of the network I was the only one who needed access so I implemented and attached a basic firewall which is called a network security group (NSG) to the OffSecVNet. I created an inbound security rule that would only allow ssh through port 22 from my public home network IP address which is the source and destination being the virtual network with the action of allow through the TCP protocol with the priority being 100. This rule was necessary to stop anyone from accessing the network unless they have my source IP that I only allowed access to. I also implemented an Allow jump box ssh inbound rule that would allow the jump box to ssh into web containers by using the private IP as the source. Which was necessary for me to use the jumpbox to jump to the other web computers on the network by recognizing that private IP. These inbound security rules would restrict the access of the network from anyone who is not using my local machine with my IP address. By placing the basic firewall also known as the network security group around the virtual network I was protecting every device that was connected to the virtual network with the inbound rules. The implemented access control achieved the goal of making and keeping the network secure from anyone not on the allowed list to use any service to access the network. I also implemented the basic network security group for the elk monitoring machine to allow the tcp traffic over port 5601 from the public IP address. Access to the jump box works by configuring the jump box to instead of taking a password but using the public part of the key pair you generated on your local machine. By configuring the machines to use the public key since your private key is stored on your local machine when running the command of ssh username at the IP address on the command line the machines will recognize that the keys are a pair and will automatically logged you into the jumpbox to gain access without having to put in a password which makes it harder for a person to be able to hack into your machines on the network by using a brute force attack or any other type of attack. Once access to the jump box is achieved you will proceed to download a docker ansible container. I would run the command apt-get update command first to make sure everything is updated to the latest update. Then I would proceed to install docker with the sudo apt install docker.io command then I would check to ensure the docker service is running. Once I confirmed it is running I proceeded to download a container image. Once I download and configure the ansible host file of the image with the IP addresses of the web servers I would be able to jump directly from the container to each of the web servers. The jump box would be the best solution to use to access other web servers since you can implement it with a key instead of a password it would be safe to use. The disadvantages of a VPN that kept me from doing it would be that with an VPN your IP addresses is always being changed around so I would have to keep going in and changing the rules every time i'm on my local machine would could become tiring after a while when I would want to jump on one of the machines or need to access the jump box in a hurry. The advantages of having a VPN are being able to encrypt all network traffic between the current network or device and the remote network. Once connected to an VPN you have full access to all resources on the remote network the same as if you were locally connected. Since the VPN creates a direct connection between your local network and a remote network It would be appropriate for remote workers to use a VPN when accessing computers and servers that are otherwise only accessible from the local network.