**Question**: How would you control access to a cloud network?

A cloud network is a vital tool in modern organizations. As such, access should be controlled to limit data and resources to only those that require it. The implications of not having proper access controls in place lead to unwanted users getting access to resources and can allow malicious attackers to take control of the entirety of the network.

In my first project of my cybersecurity bootcamp, we faced a similar problem. We had to deploy an Azure cloud environment consisting of 2 virtual networks, and 4 virtual machines (VM). To implement best practices, we had to set access controls to limit access to only the environment engineers.   
As I solved this in our project, I started with a top-down approach. Starting with the network and subnet, I configured a network security group to set up network policies. The first policy was set to block traffic from all IP addresses except from my workstation. The next policy allowed access from my workstation to only one VM on the network, the jump box. The next set of policies allowed the remaining VMs to be connected from the jump box. Lastly, SSH keys were set up for all connections.

This solution works best for small-scale networks. Although the network was cut off from public access, the NSG configuration is tedious to scale. A new rule or change to an existing policy needs to occur for each new user or additional user to the network. A possible alternative to scale this solution would be implement a VPN gateway rather than a virtual jump box gateway.

The access controls were first configured by allowing Port 22 on the jump box to be open to the workstation IP. Then for the jump box IP to establish SSH connections on Port 22 to the remaining VMs. This allowed for communication to occur only within the virtual subnet. An ELK container was also configured on the fourth VM, using Port 5601 to view the Kibana dashboard. As such, a rule was implemented to allow only the workstation IP to connect to the fourth VM’s container only on Port 5601. The SSH key to connect to the jump box was stored on the workstation and the remaining SSH keys to connect to the virtual machines were stored on the jump box. All of these configurations were set in Azure.