**Interview Question**

**Domain:** Cloud Security

**Question:** Cloud Access Control

**Answer:** In my Project called “Elk Project”, I deployed a cloud network and controlled access on the network. In which I deployed regulations, monitor permissions, restricting unwanted traffic to the virtual networks (VNs) and between my virtual machines. Secondly, on each VNs, I deployed two firewalls and Network Security Groups (NSG). That NSG plays the role of blocking all the traffic from in and out. Only a public IP address was given authorization to connect to the Network Security Group (NSGs), an IPv4 from the workstation used for this project, with a destination to port 80, protocol.

Moreover, the first VN was given the name of “RedTeamNet”, which carries the JumpBoxProvisioner, an Ansible container that allows access via SSH call port 22, and which allows TCP to the other three exited VMs in the network. Plus, I configured the VMs with SSH key access only. A most secure way to configure remote access. In addition, the second VN is called “RedTeamNet2” and contains an ELK VM with an elk-docker. It has inbound rules, which allow HTTP connection from the workstation ipv4 to ports 5601, 9200 and 5044. The JumpBox from RedTeamNet VN can also access the ELK VM via SSH as well. ELK VM also has two tools installed and configured called Filebeat and Metricbeat. Where Ansible playbooks were created to automatically install Filebeat and Metricbeat to Damn Vulnerable Web Applications (DVWA), allowing for easy access.

For more cloud security control, Jump Box plays the role of a single point for attacks. An alternative to a Jump Box will be to use a Virtual Private Network (VPN) in front of the VNs. As for the security benefits of a Virtual Private Network, it can be integrated into the firewalls by providing additional security as well.