Domain - Cloud Security

Question 1: Cloud Access Control

When you create or deploy a cloud network, it is beneficial to control the access to the network or the virtual machines to improve security. This is accomplished by incorporating inbound rules to the network security group, we did this in project 1 in the Red-Team Network Security group. In the Red-Team Resource Group we have the Red-Team VNET and subnet, this VNET is composed of the load balancer, four virtual machines and the firewall.
We configured the rule to allow HTTP connection through my home network's IP address, once we allowed access to port 80 through our home network we are now able to access the virtual network through the Jump-Box VM.

The Jump-Box virtual machine is the only VM in Azure that we have given connectivity through the internet and gives us access to the other virtual machines through dynamic IP. In order to restrict this access we configured the inbound rule for the Jump-Box VM to allow SSH or SecureShell connection from the public IP of the Jump-Box VM. By doing this, we are able to access the Jump-Box through the command line i.e. ssh azureuser@(public IP of Jump-Box VM). We can access the other three virtual machines through the Jump-Box VM after we configured the rule for the security group to allow SSH connections through port 22. So using the private IP of each VM, we can access that particular VM i.e. "ssh azureuser@(Private IP of VM)". Other rules that were configured was to allow inbound traffic from the load balancer for the three web VM's and also communication with the virtual network.

We created a separate network security group for the ELK stack VM that was also created. Similar to the Red-Team Security group, the ELK network security group had inbound rules implemented to restrict access. This network is able to communicate with the Red-Team Network through connect peering. Inbound rules were created for the ELK VM through the ELK VNET that allowed SSH connections and allowed the connection to port 5601 through the internet.

The Red-Team Network Security Group that was deployed in project 1 restricts the IP addresses to communicate with the Jump-Box VM. The restrictions set on the other VM's through the Jump-Box or jump server prevents any exposure to the public which we would not want.

As the application or service provided from the cloud network grows or scales, the system within the network expands as well. Increasing the bandwidth would mitigate any queuing delays or packet loss. At the time of this presentation, Microsoft had announced a secure remote desktop solution. The creation of Azure Bastion extends using virtual machine connectivity using Remote Desktop Protocol(RDP) and SecureShell(SSH) inside your web browser. Thus eliminating the worry of managing network policies.

To reiterate, it is beneficial to control the access to the cloud network and virtual machines to improve security.