Domain: Cloud Security

Question 1: Cloud Access Control

How would you control access to a cloud network? During Project 1 we deployed a cloud network using Microsoft Azure and several access controls within and around our created network. We initially set up two VPC's that were governed by a network security group. The first network (Rednet) was created and within that network we created 3 virtual machines, the second network (Elknet) was created to house our virtual machine that would be running our ELK stack. The two networks were connected via peering and both were isolated from the public by only having one access point to the internet via a Jump box. I restricted access to my Jump Box so that only my personal IP address was able to access it keeping the rest of my network secure. I also set security rules for each individual VM denying all traffic except for specific ports that I configured to remain open like port 22 to be able to SSH into each machine.

Defining a Jump Box, A jump box is simply a system, usually a single operating system, that is connected to two networks. The first of these networks is the common network and the second is the sensitive security zone. One of the disadvantages of using a Jump box from a security standpoint is that in theory it would be easier to compromise because it is only one target which will give access to every other system once compromised. However the advantage of a Jump box was mentioned above by only having a single controlled access point to the internet. The scalability of using a jump box is also a factor depending on how many users were trying to access the network. Eventually you would get to a choke point of having too many users trying to access through one server.

There are several alternatives to using a jump box, LDAP or Active Directory infrastructure is one way. These systems have been designed to manage user access and control, but to do that through a centralized directory, not a centralized choke point. LDAP is a path for organizations hosted in the cloud and utilizing a great deal of Linux. For organizations that are controlling compliance or managing their on-premises Windows infrastructure, AD can be an option. Both LDAP and AD can provide detailed logging for auditors and both of these effectively avoid many of the key limitations of a jump server, offering better scalability, reduced overhead, and variable access policies.

To complete the security picture, and really replace a jump box, you really need a VPN in front of your protected network resources. Without it, you turn one exposed bastion host into many exposed bastion hosts, increasing your attack surface. The benefit here is that a VPN, integrated into your firewall, provides another layer of protection on top of your already secured hosts, and it provides for a much better user experience where users have their full toolsets available for use in the protected environment. The VPN must be configured to allow only remote SSH or remote desktop connections through it. Otherwise, a compromised VPN client host would have unfettered access to your protected network resources.