Domain: Cloud Security

Question 1: Cloud Access Control

How would you control access to a cloud network?

Controlling access to a cloud network is a crucial component of ensuring a secure network is in place. A lack of access control can severely impact the confidentiality, availability and integrity of the network and its data or components. An unsecure network could result in denial of service (DoS) attacks, or allow unauthorized personnel to corrupt data or view confidential information. Implementing secure access controls can mitigate the risks of an unsecure virtual network.

The virtual cloud network I created, RedTeamNet, consists of a jump box VM that is used to access three web servers. All of these VMs were placed behind a Network Security Group called RedSecurity, which acts as a firewall to block or allow traffic to and within the network. These three web servers are then monitored by an ELK Stack VM, which is shielded by its own security group called the ELK-VM-SG. Security Groups or firewalls are necessary to protect these servers from unwanted or unauthorized access.

To properly secure this network, I created several rules on the RedSecurity Group, each with its own purpose.

- Allowing only inbound SSH connection from my personal device only, ensuring that no other device could have access to the Jump Box without the SSH key (see below).
- Allowing SSH connection from the jump box to the web servers and not giving the web servers a public IP address. This ensures that connection to these servers only can occur within the network from the Jump Box, using a unique SSH key (see below).
- For the ELK Stack VM, allow TCP traffic over port 5601 from my personal device IP address. This allows you to access the web servers via Kibana, but prevents other devices from doing so and manipulating the logs for example.

Additional access controls I implemented included generating a SSH key pair that was used to allow access to the jump box only from my personal device. Further, a second SSH key was generated from the jump box that each Web server uses to allow SSH login from only the Jump Box. Therefore, no device or server without the key can access these web servers.

Also, I created a load balancer that was placed in front of the web servers, that is accessible to the public. The Web Server VMs are not publicly accessible, so all web traffic must filter through the load balancer. THe load balancer can help ensure availability as if one server goes down, the other can pick up the load.

Security groups are resources that can be created independent of a virtual network and attached to them later. You can create the security group resource, its rules, and then attach

them to the specific VMs you want later. This would allow for security engineers to create security groups for different traffic protocols, and be replicated to your entire VNET.

A higher level version of jump box is available from Azure called Azure Bastion. It allows for RDP and SSH connections directly from a web browser and eliminates the need for a public IP address as it is not required.

A VPN is another way of ensuring a secure network. A Virtual Private Network or VPN connects directly between your local network and a remote network. It can encrypt all traffic between your current network, or device and your remote network.Once connected to the VPN, full access to all resources on the remote network is available. VPNs are appropriate for remote works because it allows workers who work from home to access their computers and servers otherwise only accessible in person on the Local Area Network.

VPN's however block or mask your true IP address. This would create an issue later on fro investigators if a suspect's IP address was masked and unable to be traced.