**Domain: Cloud Security**

**Question1: Cloud Security Control**

How would you control access to a cloud network?

In project1, I deployed a cloud network through Microsoft Azure.

I configured access controls for anyone with proper username and public IP for network access.

I implemented access controls by creating the network security group (NSG)

Red-TSG which at the initial stage was blocking all inbound traffic as per “Ground up security”

practice before I created and properly configured other VMs in a secure working environment.

I configured NSGs with whitelist of Source IPs, Ports and Protocols for allowing passing

through the firewall. By implementing these security controls I managed to specify machines and

granted them with permissions for connection to the cloud network.

Implemented access controls - NSGs configured for the virtual networks:

Red-TNet and Green-Team (for elk Vnet)

NSGs had customized inbound security rules for the machines to communicate properly.

Secure SSH connection was established with generated public key from my PC for Jump-Box

connection, and from the Jump-Box for access to VMs through ansible container attached to the

Jump-Box.

With set of inbound security rules I managed authorization for remote user for the VMs access

with a public key.

Access to the VMs were achieved with external machine after proper authentication and authorization. Implementation of these restrictions were necessary for the project to create a secure networking environment.

Access to Jump-Box is implemented with key pairs between my personal PC and Jump-Box (for SSH connection)

Access from Jump-Box to the web servers are implemented by ansible container. From inside the container with another generated key pair and through Azure configured the VMs to only allow connection from that ansible container.

A better solution than a Jump box would have been Bastion hosts (also called “jump servers”) are often used as a best practice for accessing privately accessible hosts within a system environment.

Disadvantages: Specific activities that require high bandwidth, such as gaming, might not be able to function using it, but they are easily enabled and disabled. It impedes to network growth, provides less reliability and unpredictability of performance.

Advantages: allows users to hide their network information and safely browse the web no matter the location. Ensures security, and is less expansive to maintain. The use of a VPN can give us access to company’s internal networks and resources while not on site so it provides additional security and flexibility.

I did not implement VPN on this network, as configured security rules are sufficient enough to provide the required services and also network was not connected to any sensitive databases so it

is not require any additional safety measures to take.

**Security rules sets:**

Rule SSH - Port 22; Protocol TCP; Src my IPv4; Dest VNet;

Jump-Box - Port 22; Protocol TCP; Src Jump-Box Int IP 10.0.0.4; Dest VNet;

Traffic from internet (HTTP) - Port 8080 - Port 80; Protocol any; Src my IPv4; Dest Vnet;

Kibana port 5601 (by default) - Port 5601; Protocol TCP; Src my IPv4; Dest Vnet;