Domain: Cloud Security

Question 1: Cloud Access Control

Cloud provides services such as network, compute and memory on a pay-as-you-go basis by using virtualization software running on servers accessed through internet. Cloud access is a means to control who is authenticated to access these services over the internet and whether they can modify or download any data or configuration.

In project 1, we deployed a cloud network consisting of 3 web servers attached to a load balancer. The web servers were configured to send system logs and processes information to an ELK server. The web servers and ELK server could only be configured using a jumpbox. SSH access was restricted from all other devices. All were connected by private network. Each device access was configurable by using a Network Security Group.

All devices were part of a virtual private network and traffic flow within the network was allowed. The web servers were not configured with a public ip address to prevent access from the Internet. A public ip was assigned to the jumpbox, ELK server to be able to view logs and to the load balancer. SSH access to webservers and Elk server was restricted to the jumpbox though an inbound security rule. The web site hosted on web servers was accessible through the load balancer. The Kibana website on ELK server could be accessed through port 5601 using public ip. SSH access to the jumbox was allowed through public ip.

All these restrictions were configured using inbound traffic rules stating source ip, port and destination ip, port along with protocol. Outbound traffic was mostly unrestricted. This allows web servers to download data from the internet.

We used ansible to configure all the web servers and the ELK server through the jumbox. So if the number of web servers is increased, it would be easy to configure them using ansible. The jumpbox could become a potential bottleneck. Also as the jumpbox contains the ansible hosts file and the config files, access to the jumpbox was restricted to specific ips so that no one else can learn the network configuration. A VPN is complex to implement that’s why it wasn’t implemented this time. However VPN is integrated with firewall, and you can directly access the server, so is more scalable.