We live in a time where the world is shifting to cloud-based services. Everything from email, data storage, telecom, etc. At the same time, there is a rise in cybercrimes. No CEO or customer of any company wants to hear the company name on the news followed by the word “breach”. The cloud offers convenience while also providing cybercriminals with a new avenue for their crimes. That’s why it is imperative that businesses take their IT seriously. All businesses need to seek out and hire cybersecurity professionals to protect them from the word “breach”. One good example would be the Marriott International breach in 2018. More than 500,000 of Marriott’s Starwood guest had sensitive personal information exposed. During the investigation of this breach, it was discovered that Marriott’s infrastructure had been compromised in 2014.

During my time in the SMU Cybersecurity program, one of my projects was to build and deploy a cloud-based network. It was a network that allowed secure access into the vm servers while allowing the public to access the vm web servers via a load balancer and public IP address.

The network included a firewall (security group), 4 virtual machines (jump box, 3 web servers, and an ELK server), and a load balancer. Part of the access controls were implemented within the security group. A rule was setup to deny all incoming traffic. Then I opened port 22 to allow an SSH connection from my computers public IP into the jump box’s public IP. To help improve access controls, the jump box was configured with my computer’s public key to allow me access via SSH. The three web servers were configured to be accesses by the Ansible container on the jump box also utilizing my public key and the private IP’s of the web servers. These access controls help increase security to the network while minimizing who had access to the configuration the three web servers and the jump box.

In order to secure the network, a security group (firewall) was setup with the following rules and protocols…

- Rule: allow my home computer access to port 5601
    - Port: 5601
    - Protocol: TCP
- Rule: allow home network the ability to HTTP into the network
    - Port: 80
    - Protocol: TCP
- Rule: SSH access into the jump box
    - Port: 22
    - Protocol: TCP
- Rule: allow SSH from home network
    - Port 22
    - Protocol: TCP

Also, I setup network security groups in the jump box and ELK VM…

- Jump box: SSH access
    - Port: 22:
    - Protocol: TCP
- ELK VM: SSH access
    - Port: 22
    - Protocol: TCP

- ELK VM: home computer access into the ELK VM
    - Port: 5601
    - Protocol: TCP

Each access control rule was necessary to allow my computer (a trusted resource) access to the network and all cloud equipment in order to have administrator capabilities on all equipment in the network. The restrictions were necessary to secure the network from the public and potential cyber criminals.

Overall, this network setup is scalable in the fact that it is cloud based. Memory, CPUs, and storage can be added on the fly for increase demand. On the other hand, with the jump box in place, it could be an obstacle for network growth. Although the jump box is a single point of attack for the network, and once compromised, the entire network is compromised. Another solution would be a VPN. Properly managed, the VPN can provide greater security and scalability to the network. In my opinion, it is best to use a VPN. It allows for secured connection, data privacy, and grants the network administrators the use of all their tools.

Whether the network is in the cloud or your data center, the design of the network is crucial to security and access control. One wrong configuration can be the hole that cyber criminals exploit to do harm to your organization or its customers.