**How would you control access to a cloud network?**

That's an excellent question; how would I control access to a cloud network?

It's very interesting you ask that question, because in my first project for my cybersecurity bootcamp class we created a virtual network in the cloud. And as I was creating one of the virtual machines, I found that I couldn't access it nor was the that the machine wasn't working correctly.

I found that as I tried to reconfigure the virtual machine, I couldn’t get it to work. I couldn't reconfigure it. So, what I ended up doing was destroying that virtual machine and creating a new one. in doing so I needed to create security controls so that only I or the VMs I indicated would be able to connect to that machine that VM.

What I did was I created a load balancer that would act as a security barrier and a component that would balance the traffic between all virtual machines; therefore, if one of the virtual machines went down the other VM's would be able to pick up the slack. I also created several security groups for each virtual machine so that only certain ports would be open and access only on specific IP addresses, the internal public IP addresses, as well as the internal private IP addresses for each VM.

I started by creating a firewall and behind that firewall I had the load balancer and a jump box. Both the jump box and Load balancer had specific security groups and those NSGs were inherited by the three Web VMs I connected using a Docker container. The jump box was running in an ansible container. I limited access to only three ports, namely ports 80, 22, and 443. Also, I only allowed my desktop to access the virtual network using SSH.

These restrictions were needed to protect the network form outside “bad elements” that could possibly take over the network or worse yet glean data form the servers.

Later, I added an ELK Stack and loaded Kibana on the VM Web servers to monitor the health of the machines and to log traffic and possible DDoS attacks.

Using SSSH to the jump box and load balancer can be seen as a poor man’s VPN for a small company’s network. The possibility to scale this setup is available, but it’s not practical in most cases. Using a VPN would be more practical, but it doesn’t fit needs of small companies or home offices. In that case I would suggest using a cloud services like Azure or Amazon for security needs of small to medium companies and a VPN.

Using a VPN doesn’t exclude basic security measures like load balancers and jump boxes or using a firewall.