**Network Engineer**

* **How to migration configuration**

To transfer network configurations to cloud from on premises begin with the process of conducting a detailed audit of the current network configurations, devices Ip address schemes VLANs and security policies. After that, configure the target environment through the development of network requirements, including virtual networks, subnets as well as security rules. Export them and make sure they will work in the cloud environment and import and then, apply the configurations in the new set-up. Carry out thorough testing of connectivity, performances and security to confirm all applications and services within the system to be usable. After all the changes have been made, and everything has been checked for accuracy, traffic should be rerouted to the new environment, and the results should be carefully monitored for potential problems and adjusted for as needed. Last but not the least create all new reports, take the back of all the configurations and a good backup and recovery plan of the new cloud environment.

* **How to Implement Network Security Controls in cloud?**

Network security controls in the cloud refer to measures and means which are put in place to safeguard cloud assets against imitation, unauthorized access and cyber attacks.

* **Design a Secure Network Architecture:** Begin by selecting a structure of a cloud network with Virtual Private Clouds (VPCs) or virtual networks with various subnets for various sorts of resources (for instance, public, private and administration subnets). Least-privilege approach should be applied to reduce the risk exposure as much as possible and divide the workloads according to their level of sensitivity and purpose.
* **Implement Access Controls:** Identity and Access Management should be used to define and implement who should have access to cloud resources and what amount of access each of them should have. Implement secured login procedures such as MFA and follow strict access control measures to give the users the minimum level of access necessary to accomplish their duties.
* **Configure Firewalls and Security Groups:** Use native cloud firewall options at the network and instance levels, for example, Azure NSGs. Define rules that would only permit traffic that is essential and then block all other traffic.
* **Set Up VPNs and Private Connectivity:** The primary method of establishing a secure connection between the servers on premises and servers in the cloud is to utilize VPNs, or dedicated connections, such as Azure ExpressRoute. This makes sure that, the data transfer is done in a secure manner over a dedicated communication link.
* **Implement Security Automation:** Power up the security tasks which include the deployment of configurations, the monitoring process, patching, and incident response through the tools like Azure Functions. This way security is maintained without the need of manual interjection and thus limits human interference.