Secure migration to the cloud

For a model of business like an e-shop is a priority the security of the data that they manage, due to the transactions that are developing into the web page, intending to do a secure migration to the cloud that preserves the data integrity, confidentiality and availability in both of the data states (in repose and in transit) are advised to follow the following strategy.

Like the first step, should deploy the structure of the server (this includes storage, virtual machines, VPN, etc.) throw an admin account that must configure the Multi-Factor Authentication (MFA) at the same time that was created this makes it more difficult for an attacker to enter the system. This structure must configure a firewall that allows web traffic (HTTP/HTTPS) and only open the ports that will be used to configure the server to avoid unnecessary traffic and reduce the possibility of an intrusion.

After that, should create the different user groups that will administrate the web page and the different components of the server, this must follow the least privilege strategy to assign each permission to the respective user group, that consist in assign just the permissions needed for the job that the user develops. This prevents an employee modifies or read secret information or in case of authentication data steal the fake user will have limited access to the system.

At the time of creating the users in the respective group they must use a strong password to authenticate and if the user has high privileges is advisable to use a second factor of authentication. For users that work out of the office center, the access to the system must be done throw a VPN connection and with an encryption protocol like HTTPS or encrypting the information before being sent.

Once the structure of the server is ready the next step is copying the local information to the cloud, this can be done throw a direct connection that allows some cloud computing service providers or throws the internet, regardless of the case this must be done encrypting the data that will be sent this protects critical data from being modified or read while being copied to available cloud storage.

To provide a good service and ensure the availability of this should be used resources like a load balancer to manage the computation resources that are used and avoid a Distributed Denial of Service (DDoS) attack, by last to reach more clients in different countries is a good idea reproduce the configuration in different availability zones. Finally, all communication between the client and the server must be done in an encrypted way using the HTTPS protocol and must have a certification of the identity of the web site.