Securing an application in the cloud

Levels of security

Securing an application in the cloud involves a multi-level approach, including:

1 **Network security:** Secure traffic to the application using firewall rules, traffic encryption, avoiding DDos attacks, etc.

2 **Application security:** Secure application or API by allowing/denying traffic based on authentication/authorization of the user and following principle of least-privilege; input validation

3 **Data security:** Involves data encryption at rest and in transit; data access management; data availability

Network Security

- **Implement Strong Firewall Rules**: Develop robust firewall rules to control the traffic coming in and out of the network. Using tools provided by cloud service providers, you can specify the type, source, and destination of traffic that is allowed or disallowed.

- **Apply Traffic Encryption:** Enforce SSL/TLS protocols for network traffic to secure data in transit. For stored data, utilize encryption techniques to protect against unauthorized access.

- **DDoS Mitigation Strategies**: Utilize load balancers to evenly distribute network traffic across multiple servers, reducing the risk of any single point of failure. Use DNS services to route inbound traffic through scrubbing centers, effectively separating malicious traffic from legitimate traffic.

- **Network Segmentation**: Implement network segmentation to isolate different parts of the network. In case of a security breach, this limits the attacker's ability to move across the network.

- **Regular Network Monitoring and Auditing**: Regularly monitor network traffic and promptly investigate any anomalies. This will help in the early detection of potential attacks and vulnerabilities.

- **Establish an Incident Response Plan**: Have a clear plan in place for how to respond when a security incident occurs. This should include steps for identifying and isolating the problem, mitigating damage, and implementing necessary improvements to prevent future incidents.

- **Continuous Security Training**: Keep the team updated on the latest security threats and best practices for network security. Regular training can help to avoid accidental breaches and improve the overall security of the network.

Application Security

- Make sure application has proper authentication and authorization policies defined to allow/deny a user
- Make sure all the artifacts related to the application are properly scanned, e.g., scanning container images for vulnerabilities
- Follow principle of least-privilege to give minimum required access to the user accessing the application or process running the service

Data Security

- Make sure data is encrypted while at rest (i.e., data is stored in the databases or file systems, etc.) and while in transit using secure protocol like HTTPS.
- Make sure that proper IAM policies are in place to access the application data
- Make sure to have a proper vault solution to store keys/secrets/certificates related the application
- Make sure to take regular backups of the data stored in the DB/file systems, etc.