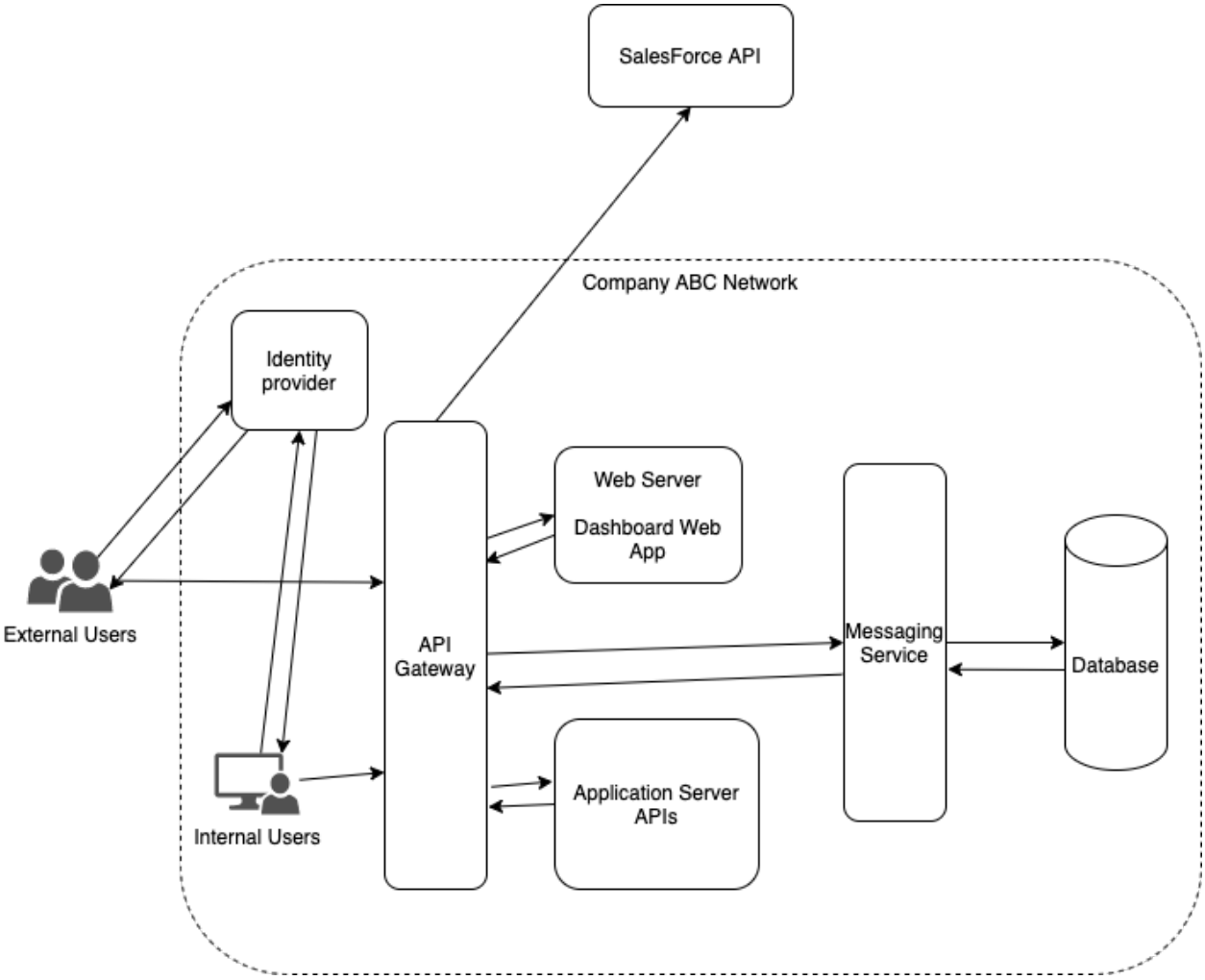
Security Design Architecture

The following is the updated network diagram that includes security and performance improvements. Please review the details below the diagram.



1. All users internal and external should use Identity Provider service to acquire authentication to use the system API.
2. All APIs will be exposed via API Gateway. This can give us authentication centralization for API consumption as well as rate limiting and monitoring/logging capabilities.
3. External users can access Dashboard web app only after authentication.
4. Application Server APIs are only exposed via API Gateway. Neither WebServer or Internal Users can invoke Application Server APIs directly.
5. A messaging service is employed so that users and application do not interact with the Database directly. In addition to improving the security, this also improves overall performance since database CRUD API is generally slow.
6. Data on the database is encrypted.

7. Data in transition is encrypted and all APIs should use secure protocol.
8. SalesForce API is also exposed to the on-prem applications via API Gateway.
9. Firewall rules are in place to only allow outbound traffic to the predetermined SalesForce FQDN/IP.