Authentication bằng jwt

Quản lý đăng nhập bằng access token và refresh token là một phương pháp phổ biến để xác thực người dùng và duy trì phiên làm việc trên ứng dụng web hoặc di động. Dưới đây là giải thích một cách dễ hiểu về quản lý đăng nhập bằng access token và refresh token:

1. **Đăng nhập**: Người dùng cung cấp thông tin đăng nhập (tên người dùng và mật khẩu) để truy cập vào ứng dụng. Khi thông tin đăng nhập chính xác, máy chủ xác thực người dùng và **tạo ra một cặp access token và refresh token.**
2. **Access Token**: Access token là một chuỗi mã hóa được máy chủ tạo ra và trả về **lưu ở phía người dùng** sau khi đăng nhập thành công. Access token thường có hạn sử dụng ngắn, ví dụ như 15 phút hoặc 1 giờ. Access token được sử dụng **để xác thực các yêu cầu** từ người dùng khi gửi đến máy chủ.
3. **Refresh Token**: Refresh token cũng là một chuỗi mã hóa được máy chủ tạo ra và trả về **lưu ở phía người dùng** sau khi đăng nhập thành công. Refresh token có hạn sử dụng lâu hơn so với access token, ví dụ như vài tuần hoặc vài tháng. **Refresh token được sử dụng để làm mới (refresh) access token khi nó hết hạn**.
4. **Gửi Access Token**: Mỗi lần người dùng gửi request bảo mật đến máy chủ, họ cần gửi access token cùng với yêu cầu. Access token được gửi qua **header "Authorization"**
5. **Xác thực Access Token**: Máy chủ nhận được access token và kiểm tra tính hợp lệ của nó. Nếu access token hợp lệ và chưa hết hạn, máy chủ thực hiện yêu cầu từ người dùng. **Nếu access token không hợp lệ hoặc đã hết hạn, máy chủ yêu cầu người dùng cung cấp refresh token.**
6. **Làm mới Access Token**: Khi máy chủ nhận được refresh token, nó kiểm tra tính hợp lệ của nó. Nếu refresh token hợp lệ, máy chủ tạo ra một cặp access token mới và refresh token mới và trả về cho người dùng. Người dùng sử dụng access token mới để tiếp tục gửi yêu cầu bảo mật.
7. **Quá trình lặp lại**: Quá trình trên được lặp lại trong suốt quá trình sử dụng ứng dụng. Mỗi khi access token hết hạn, người dùng sẽ sử dụng refresh token để làm mới access token và tiếp tục sử dụng ứng dụng mà không cần đăng nhập lại.

Phương pháp này giúp tăng tính bảo mật bằng cách giới hạn thời gian tồn tại của access token và cung cấp cách làm mới an toàn thông qua refresh token. Ngoài ra, việc sử dụng access token và refresh token giúp hạn chế tác động của việc đăng nhập lại đối với trải nghiệm người dùng, đồng thời cung cấp sự linh hoạt trong quản lý phiên làm việc trên nhiều thiết bị và ứng dụng khác nhau.