Five API Gateway Authentication Strategies

API gateway authentication helps to ensure that only authorized clients are able to access the microservices behind the API gateway. This can help to protect sensitive data and resources from unauthorized access. Here are 5 strategies to consider:

01

Basic API Authentication

Basic authentication is a straightforward method in the HTTP protocol when a client sends an HTTP request with a base64-encoded username and password. The API gateway usually verifies these credentials against a predefined list.

02

Key-Based Authentication

API key authentication is when a client includes a unique key in the request, validated by the API gateway. Keys can be managed by the API provider or an external system, making this method ideal for HTTP APIs.

03

LDAP Authentication

LDAP (Lightweight Directory Access Protocol) authenticates clients by validating credentials against a central LDAP server, commonly used for existing corporate user directories.

04

OAuth Authentication

OAuth 2.0 allows clients to delegate resource access via an access token obtained from an authorization server, used in API gateway requests for verifying access levels. It is effective for restricting access to third-party apps and operates exclusively with HTTPS.

05

OIDC Authentication

OpenID Connect (OIDC) builds on OAuth 2.0, simplifying client authentication and user information retrieval in one request. Clients obtain both an ID token and an access token from an authorization server, allowing authentication and access to user information.

Find out how Gloo Gateway can work for you:

https://www.solo.io/products/gloo-gateway/

solo.io