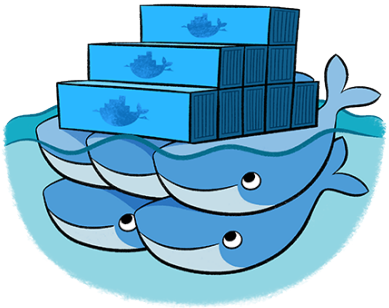
What is Authelia?



Introduction

Authelia is a two-factor authentication (2FA) and single sign-on (SSO) server focused on enhancing the security of applications and users. Acting as an extension of reverse proxies, it provides various authentication-related features, such as:

- Multiple two-factor authentication methods.
- Identity verification for registering second-factor devices.
- Self-service password reset functionality.
- Account banning after excessive failed login attempts (rate limiting).

Features Summary

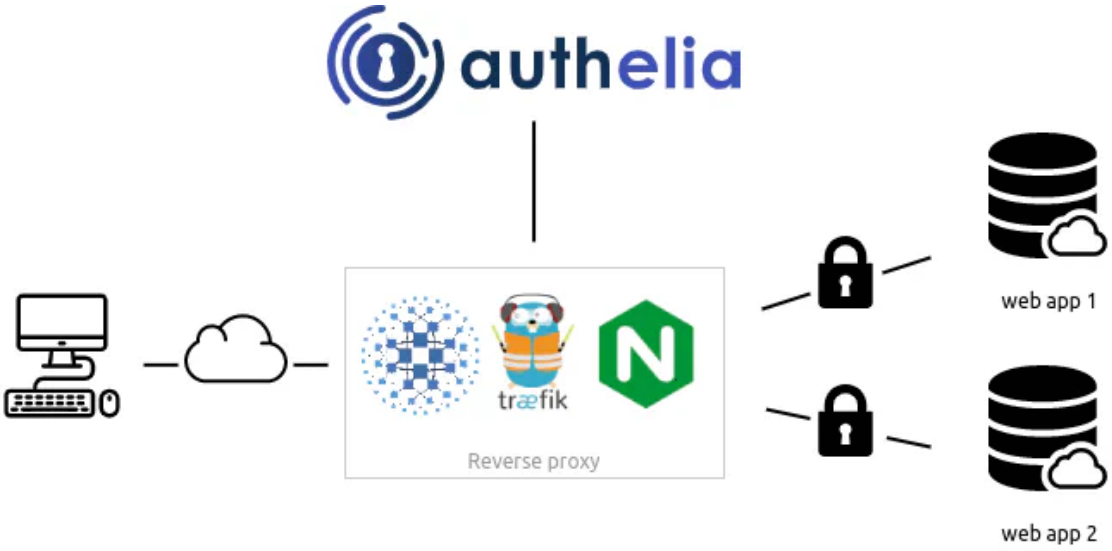
This is a list of the key features of Authelia:

- □□ Several second factor methods:
  - □□ Security Keys that support FIDO2 WebAuthn with devices like a YubiKey.
  - □ Time-based One-Time password with compatible authenticator applications.
  - □□ Mobile Push Notifications with Duo.
- ✉ Password reset with identity verification using email confirmation.
- □□ Access restriction after too many invalid authentication attempts.
- □□ Fine-grained access control using rules which match criteria like subdomain, user, user group membership, request URI, request method, and network.
- ⚙ Choice between one-factor and two-factor policies per-rule.
- □□ Support of basic authentication for endpoints protected by the one-factor policy.
- □□ Highly available using a remote database and Redis as a highly available KV store.
- □□ Compatible with Traefik out of the box using the ForwardAuth middleware.

Architecture

Authelia integrates seamlessly with reverse proxies like Traefik (see the full list of supported proxies). It enhances these proxies by adding authentication and authorization features alongside a login portal.

Authelia is connected to the reverse proxy but does not directly interact with the backend applications. Payloads sent by clients to the protected applications never reach Authelia; only authentication-related information, such as the `Authorization` header, is processed. This allows Authelia to protect any HTTP-based APIs, including REST and GraphQL APIs, without interfering with application data.



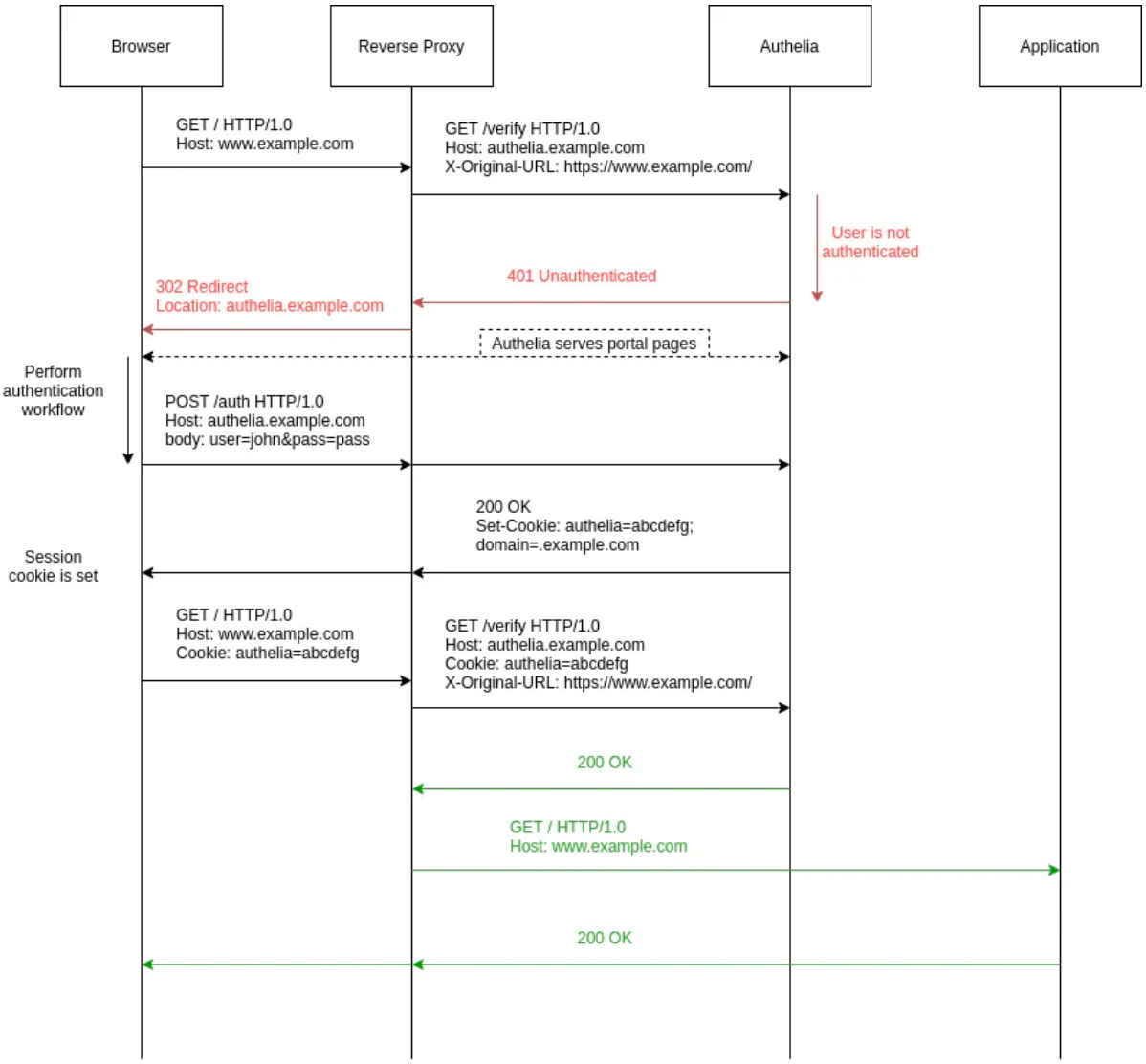
Workflow

Reverse proxies configured with Authelia send all incoming requests to Authelia for authentication verification. Authelia instructs the reverse proxy to either:

- ✔ Allow the request to pass through if the user is authenticated, or
- □ Block the request if the user is unauthenticated or unauthorized.

Step-by-Step Workflow

1. □ **Unauthenticated User Request:**
   When an unauthenticated user sends their first request to the reverse proxy, Authelia determines the user is not authenticated (no session cookie provided). The user is redirected to the Authelia login portal.
2. □□ **Authentication Portal:**
   The user completes the authentication workflow via Authelia's portal. Upon successful authentication, a session cookie is issued, valid for all subdomains of the protected domain.
3. ✔ **Authenticated User Request:**
   The user revisits the initial website, now including the session cookie in their requests. Authelia verifies the session and instructs the reverse proxy to allow the request to pass through.



Revision #16
Created 8 January 2025 20:35:13 by aeoneros
Updated 8 January 2025 20:51:45 by aeoneros