Automação de Autenticação e Teste de Segurança em Aplicações Web Baseada no ZAP

Lucas Sacramento, Italo Cunha, Gabriel Cardoso,
Artur Souza, Antônio Franco, Leonardo Oliveira

UFMG

RNP

HACKERS DO BEM

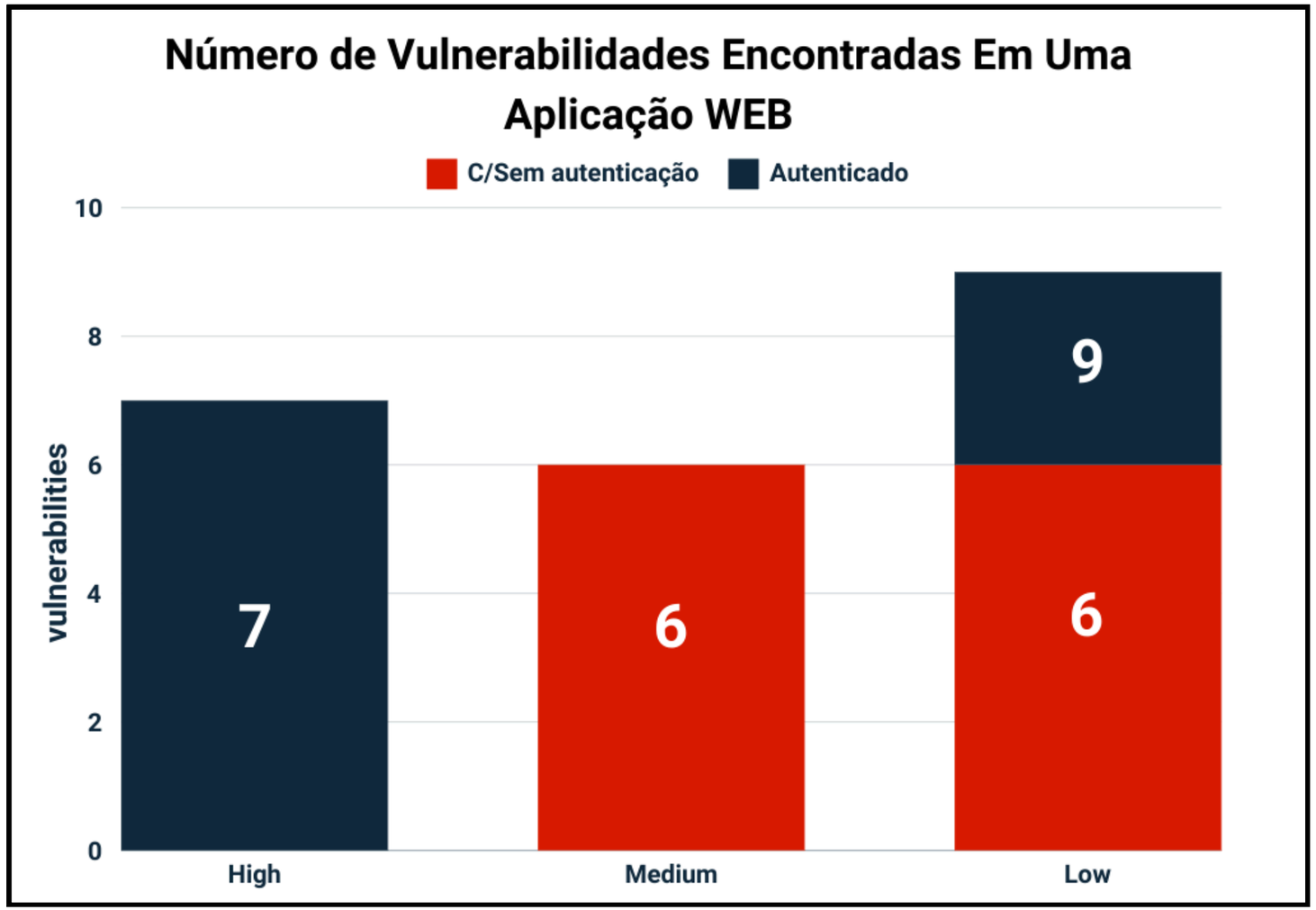
KIDER
cybersecurity for all

Motivação

- **A ausência de autenticação durante os testes reduz a visibilidade das vulnerabilidades nas aplicações.**

Motivação

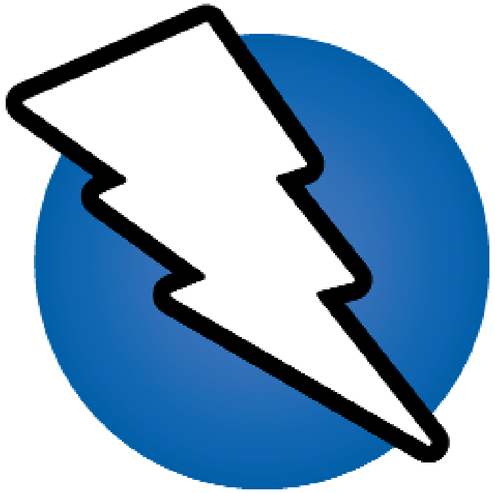
- A ausência de autenticação durante os testes reduz a visibilidade das vulnerabilidades nas aplicações.



Solução Proposta - Ferramenta utilizada

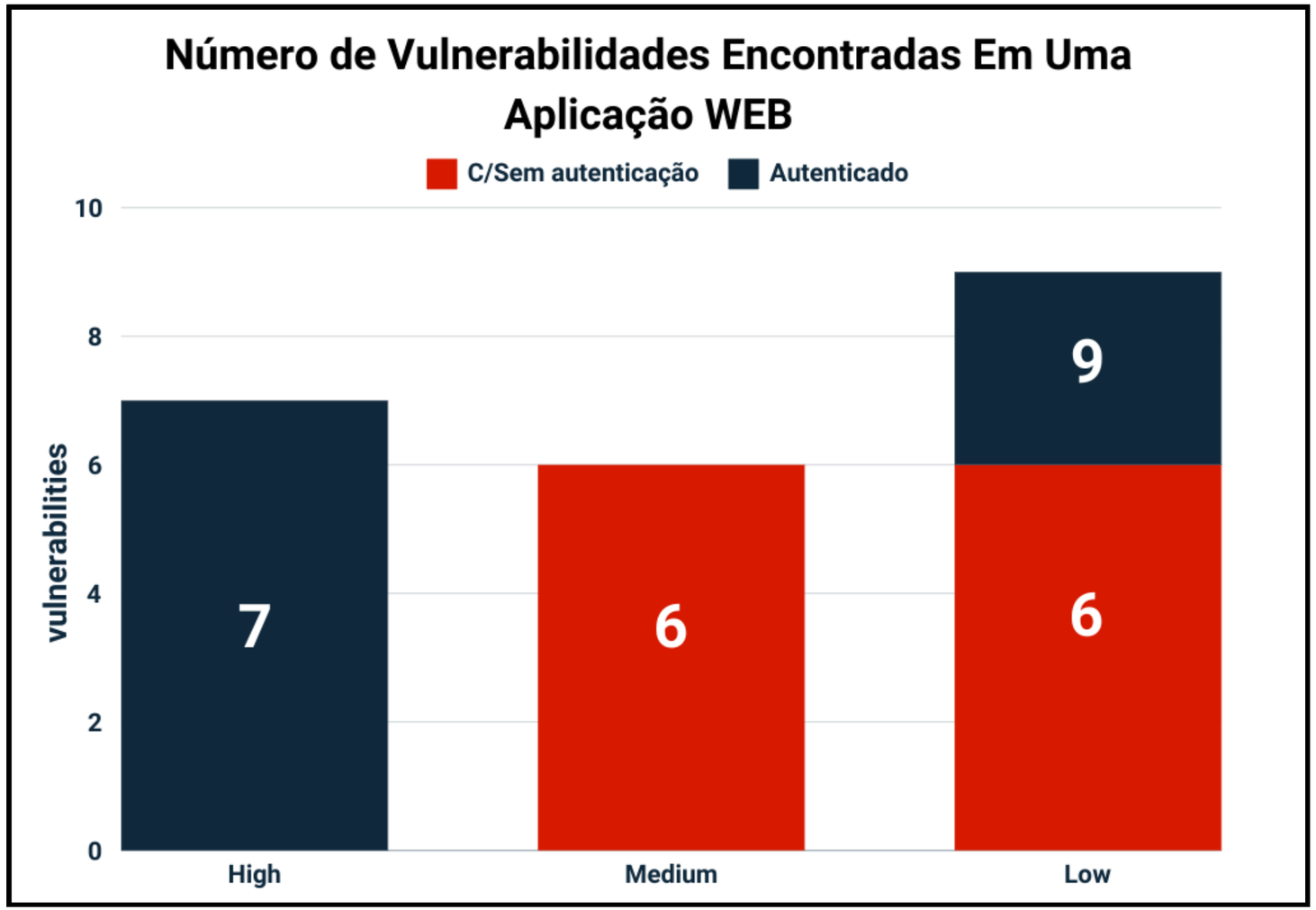
- ZAP (Zed Attack Proxy)
- Lançado em 2010 com nome OWASP ZAP
- Software gratuito e código aberto

- Proxy que inspeciona o tráfego, permitindo analisar e modificar solicitações e respostas para testes de vulnerabilidades.



Motivação

- A ausência de autenticação durante os testes reduz a visibilidade das vulnerabilidades nas aplicações.
- A execução do scan requer uma curva de aprendizado da ferramenta por parte do usuário.



Desafio(s)

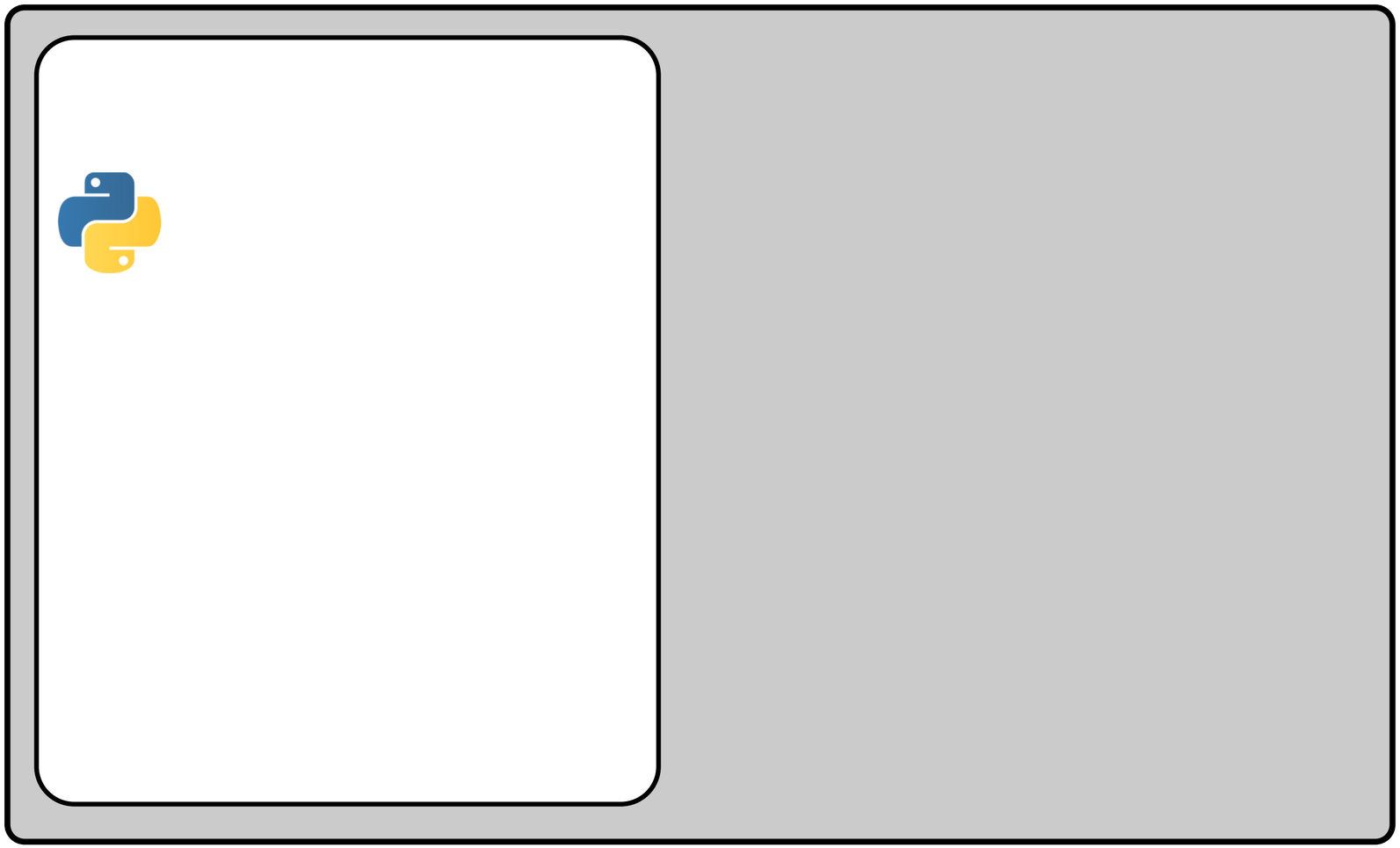
Desenvolver um arcabouço capaz de identificar diferentes mecanismos de autenticação

Desafio(s)

Desenvolver um arcabouço capaz de identificar diferentes mecanismos de autenticação

Capturar os diferentes tipos de elementos presentes em formulários necessários para a autenticação

Solução Proposta - Arquitetura do Arcabouço

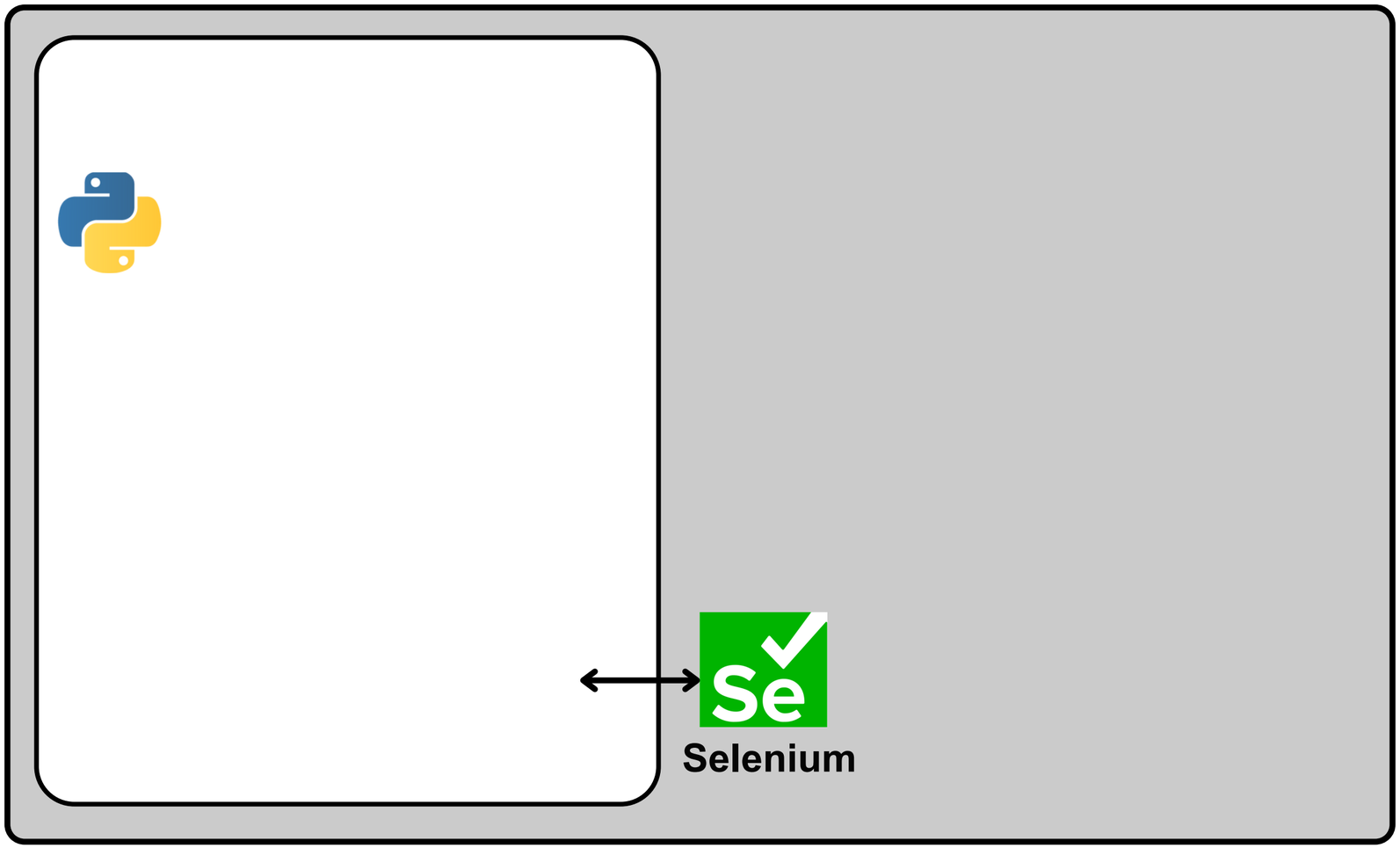


Local

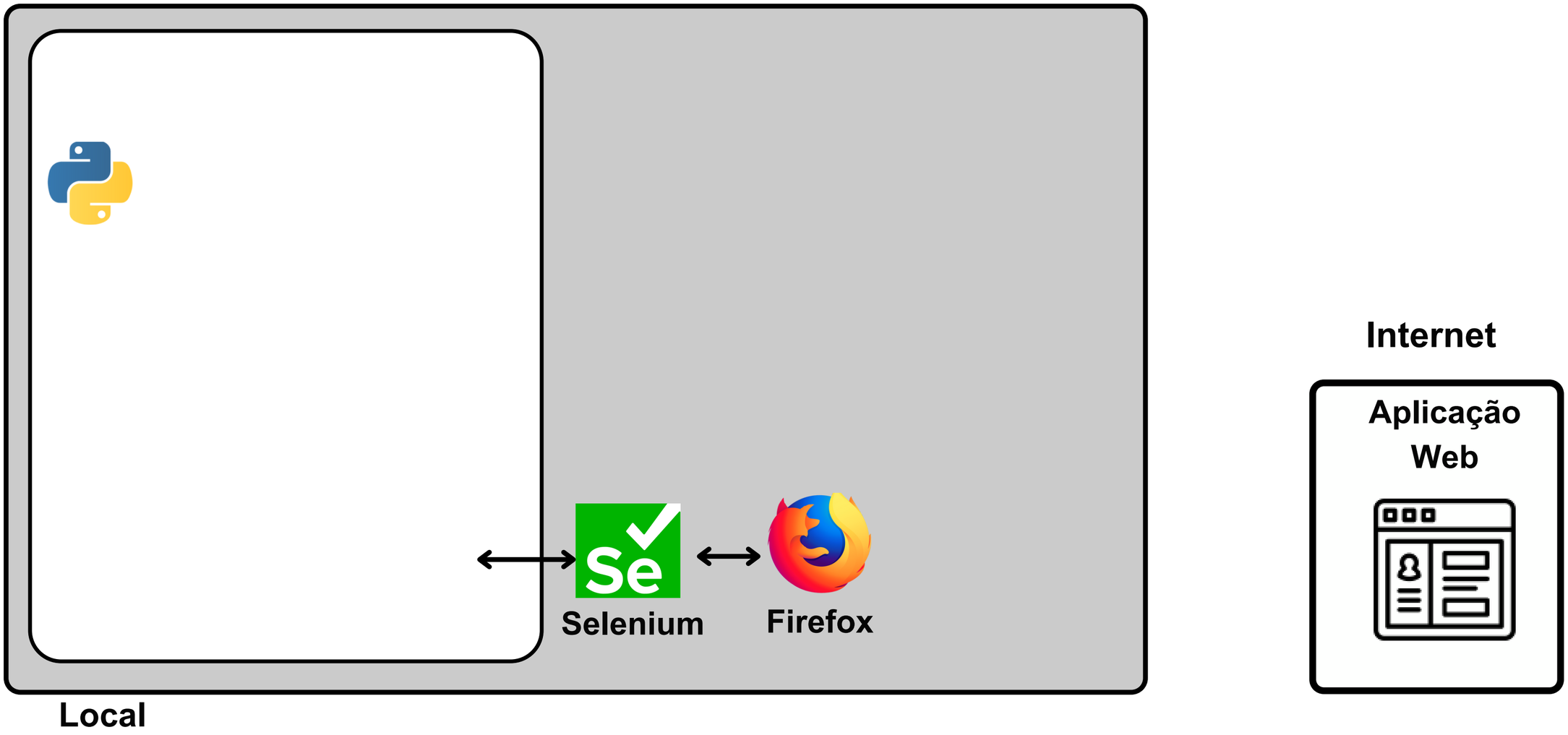
Internet

Aplicação Web

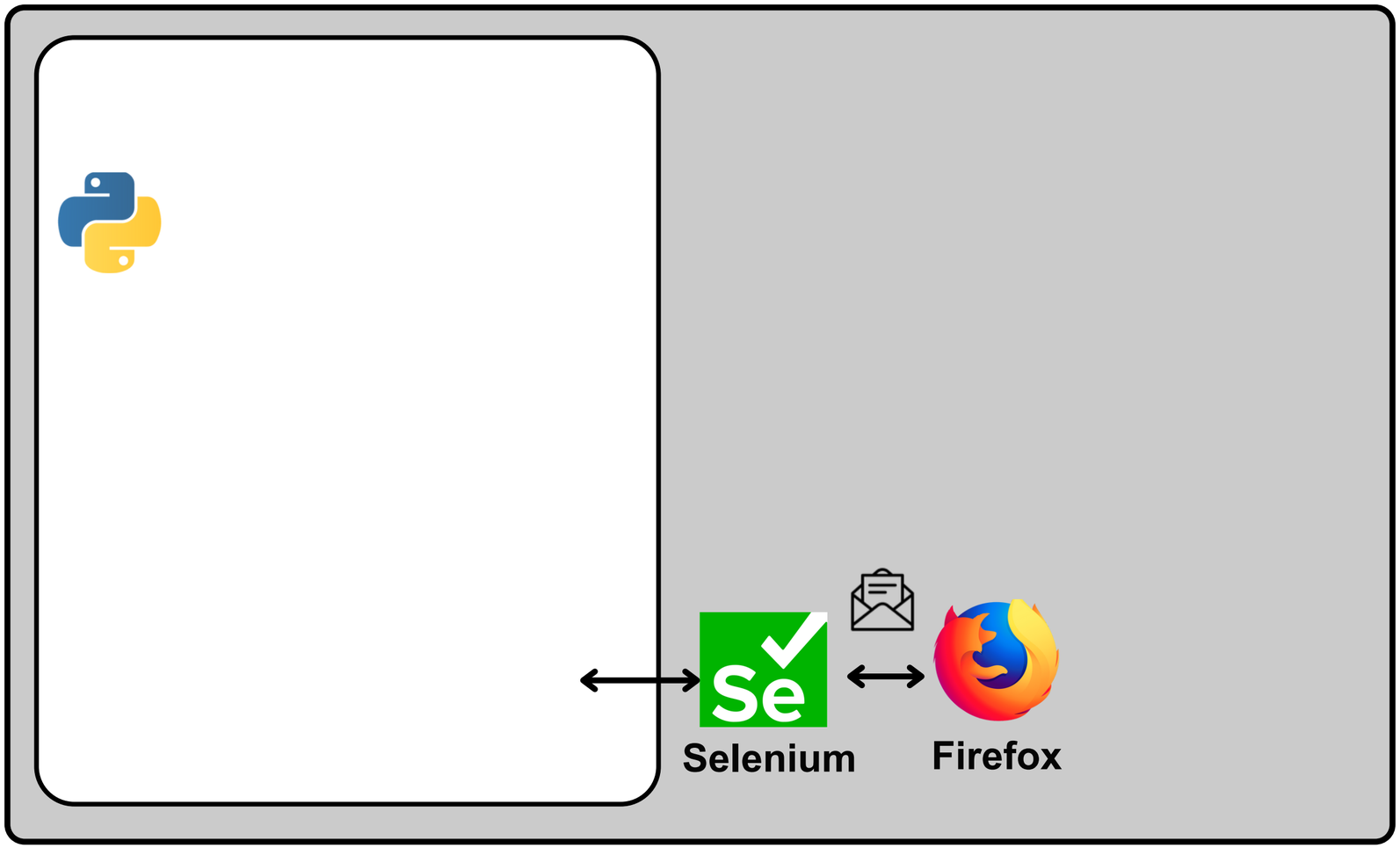
Solução Proposta - Arquitetura do Arcabouço



Solução Proposta - Arquitetura do Arcabouço



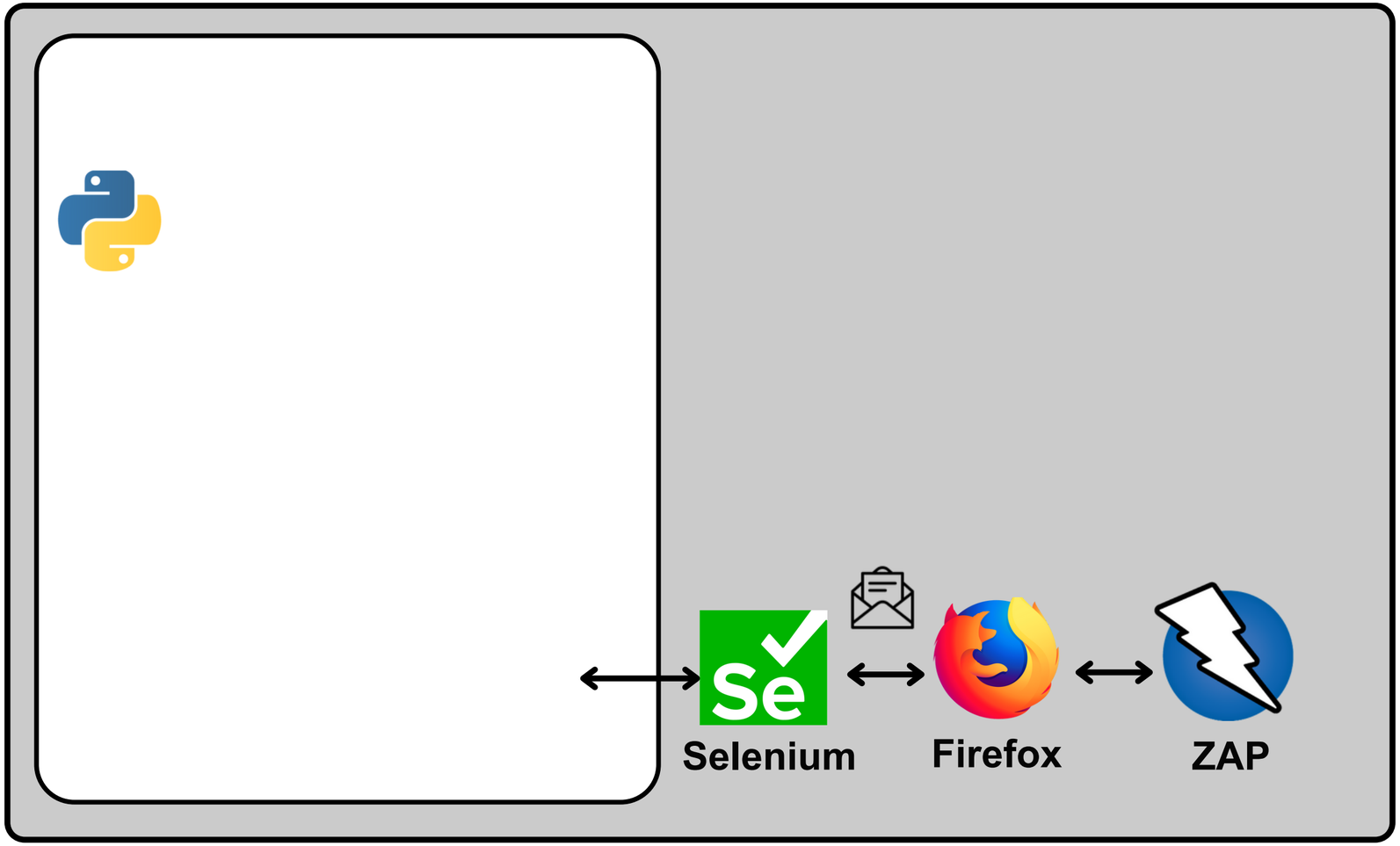
Solução Proposta - Arquitetura do Arcabouço



Internet

Aplicação Web

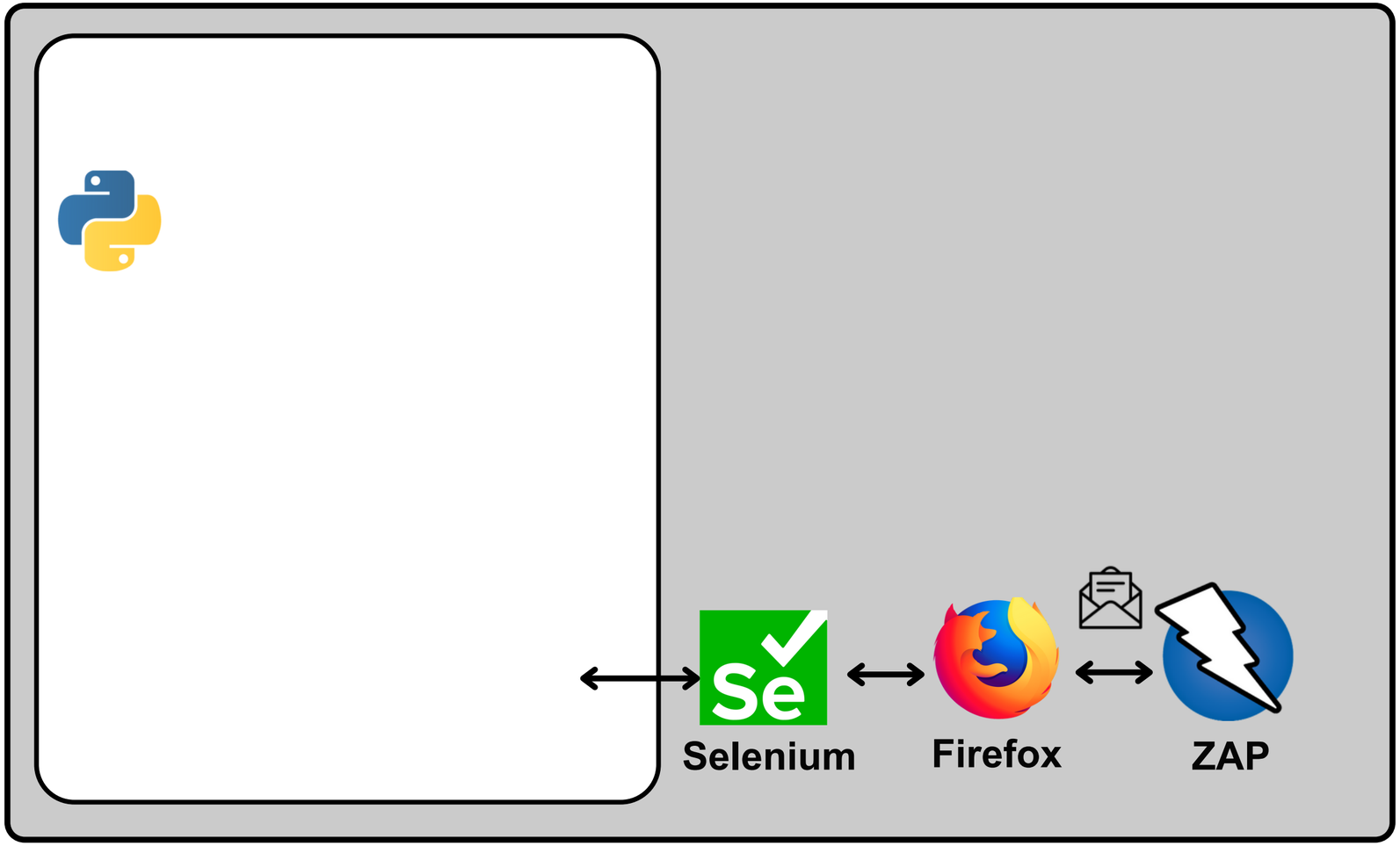
Solução Proposta - Arquitetura do Arcabouço



Internet

Aplicação Web

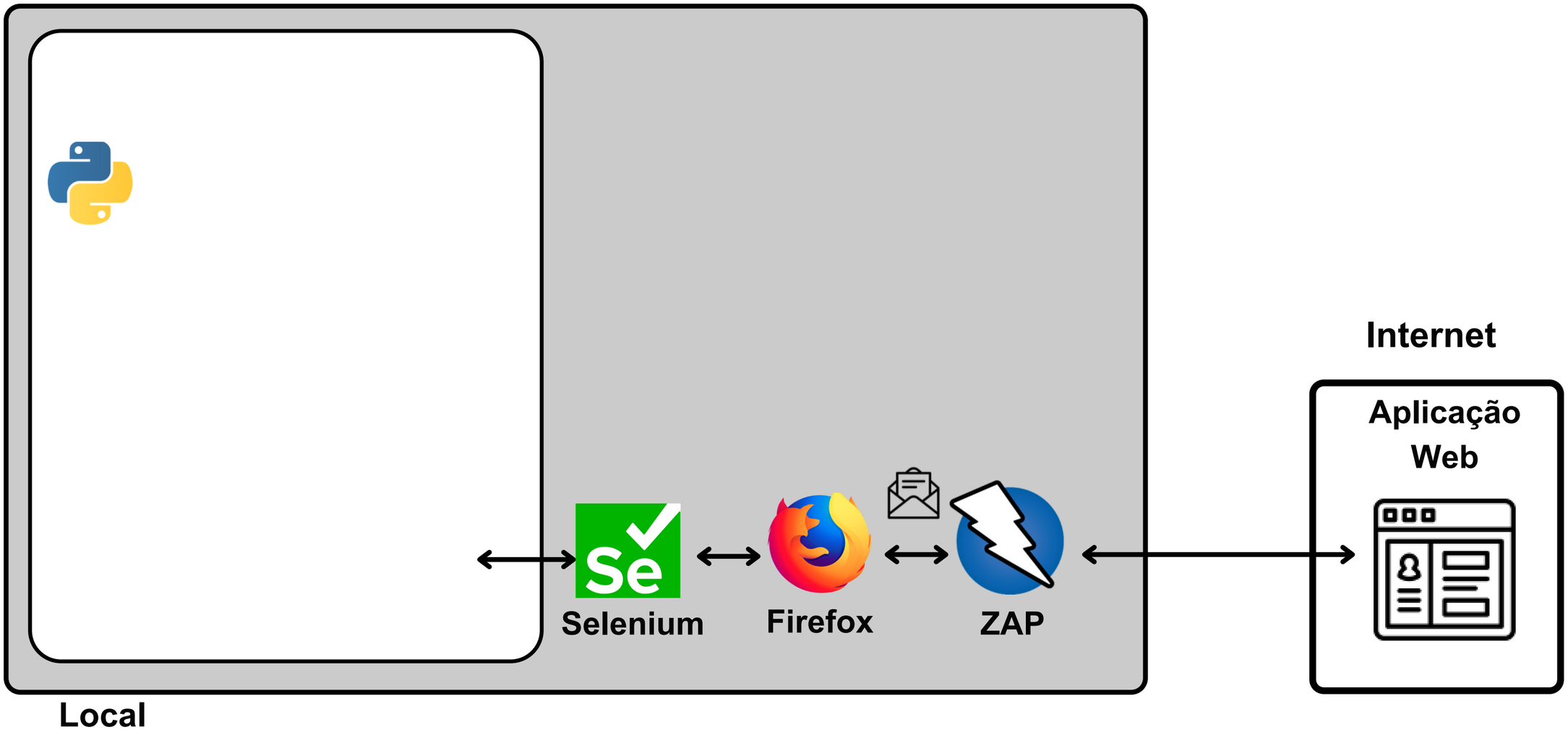
Solução Proposta - Arquitetura do Arcabouço



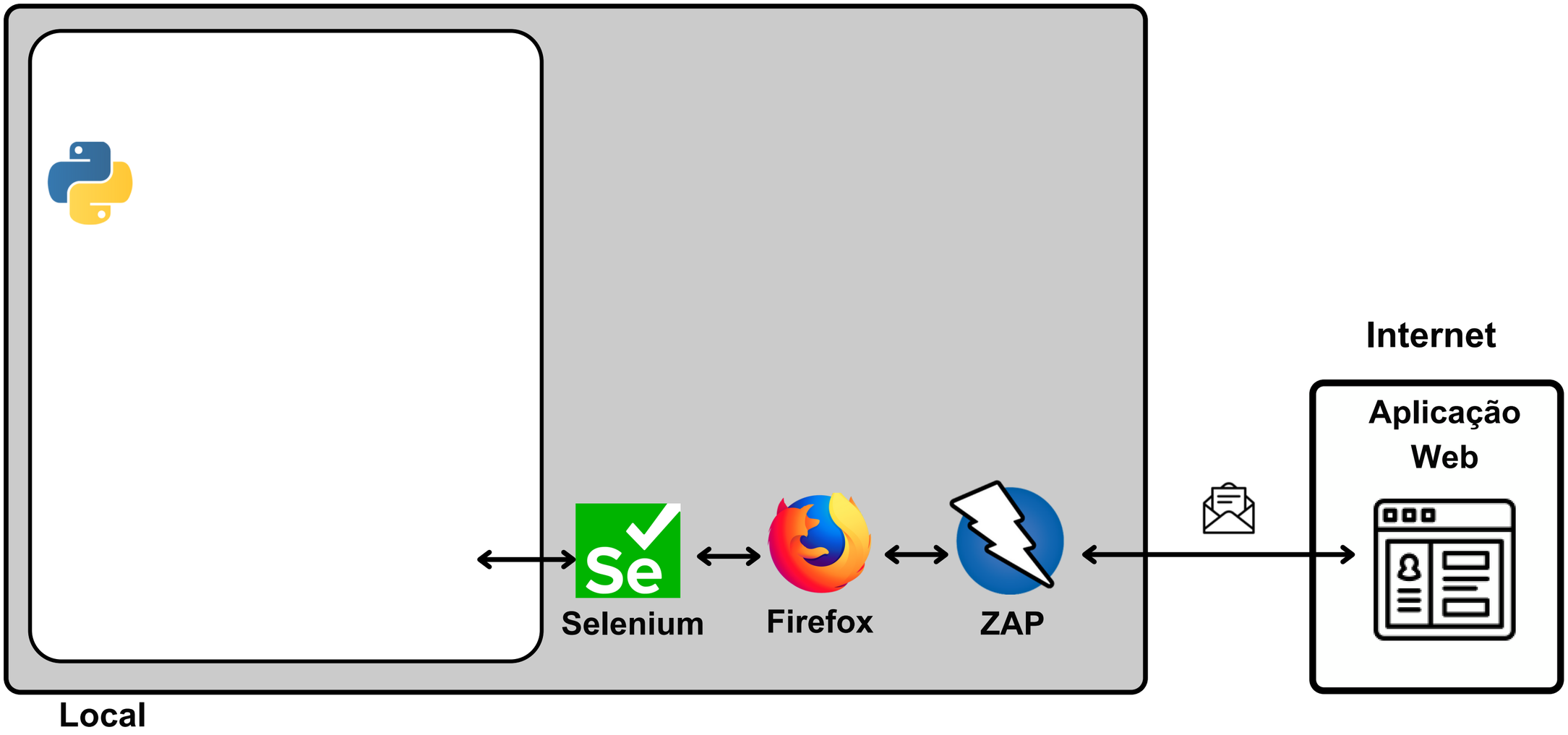
Internet

Aplicação Web

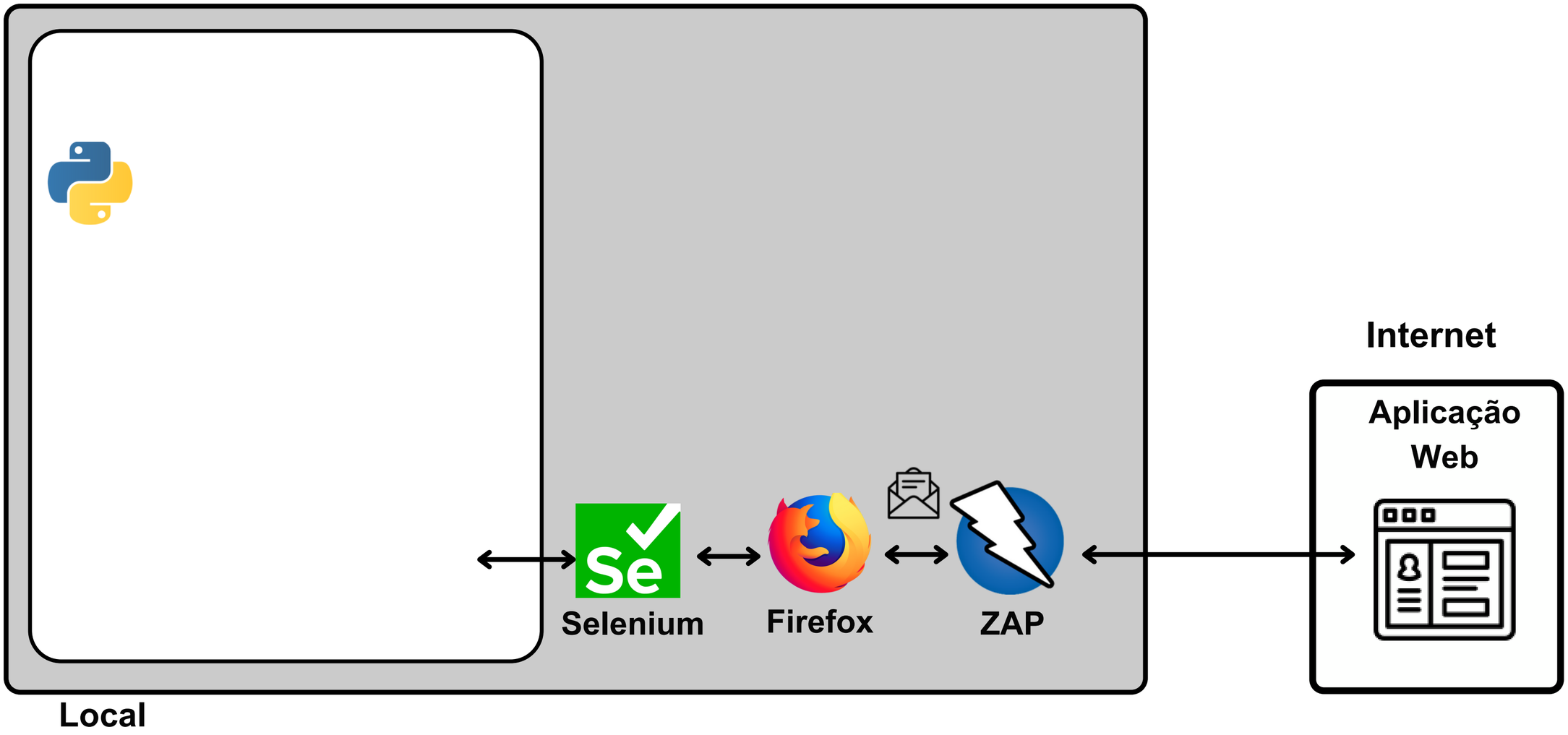
Solução Proposta - Arquitetura do Arcabouço



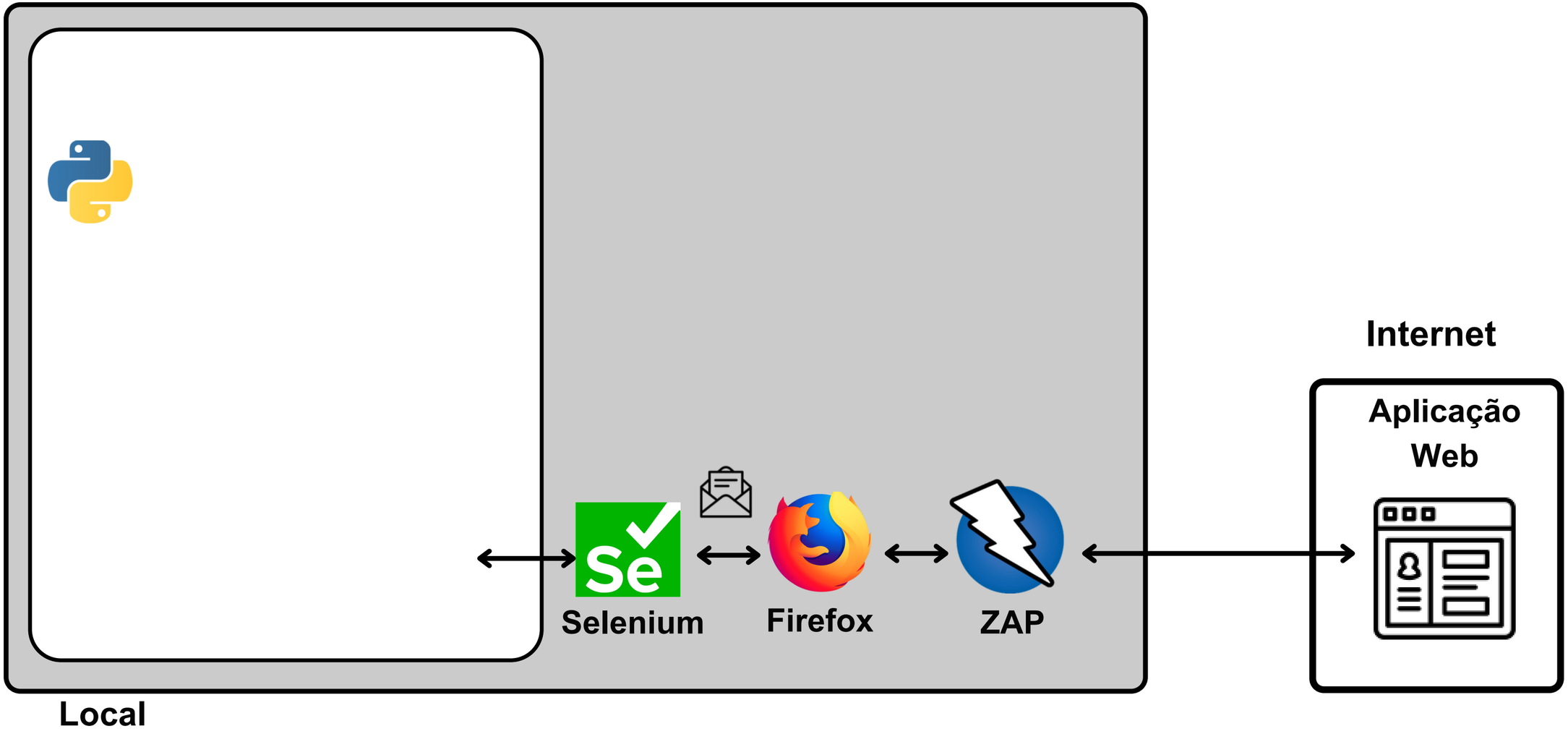
Solução Proposta - Arquitetura do Arcabouço



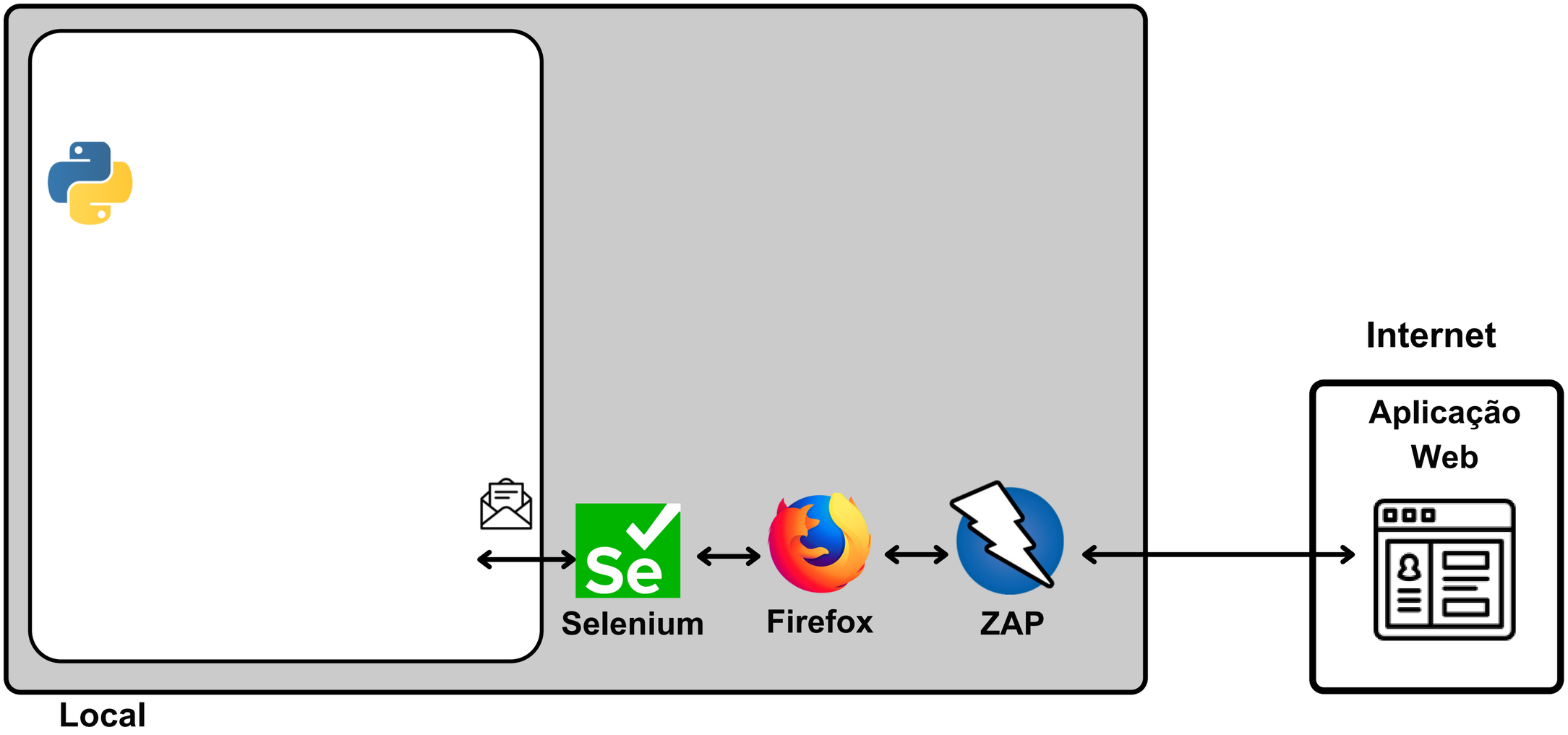
Solução Proposta - Arquitetura do Arcabouço



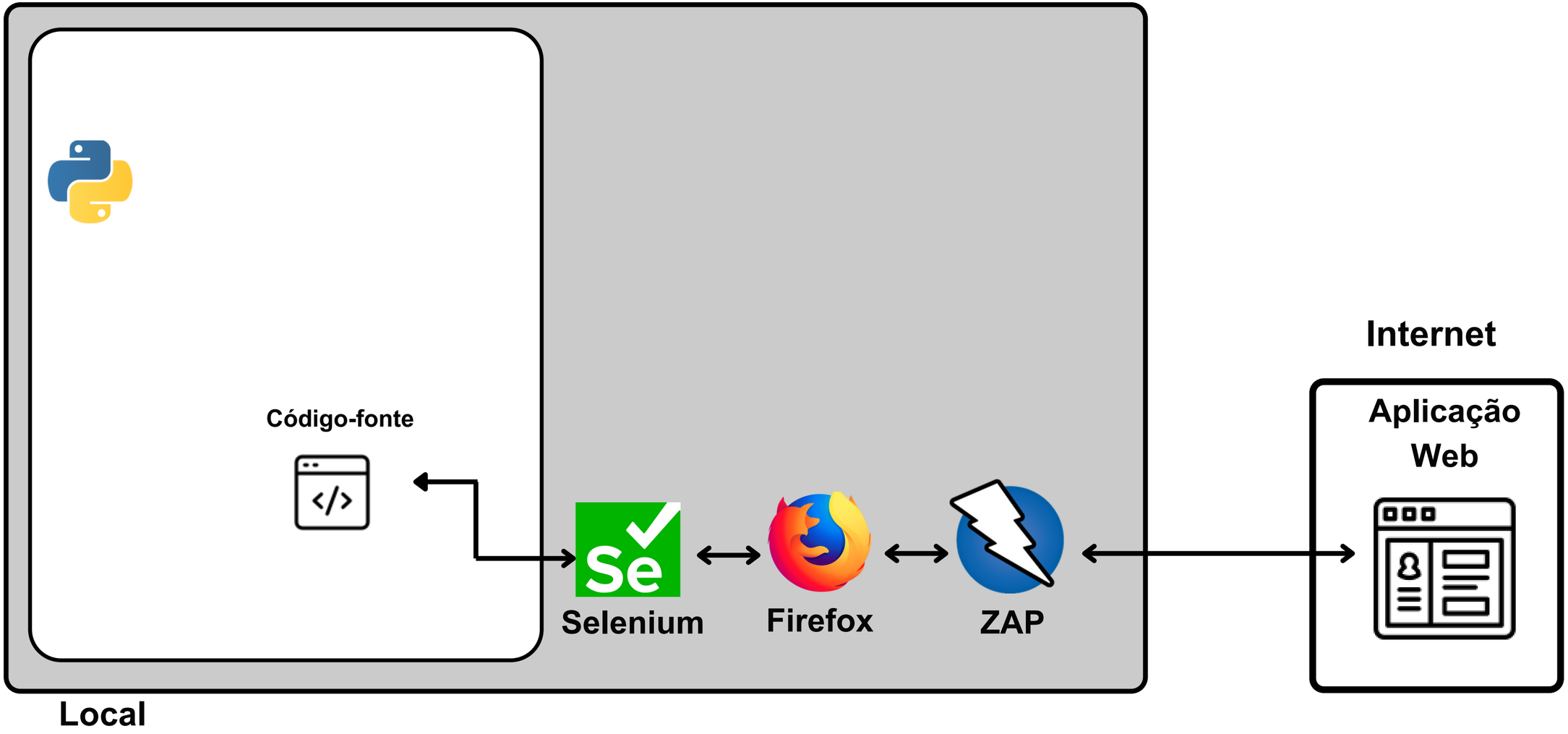
Solução Proposta - Arquitetura do Arcabouço



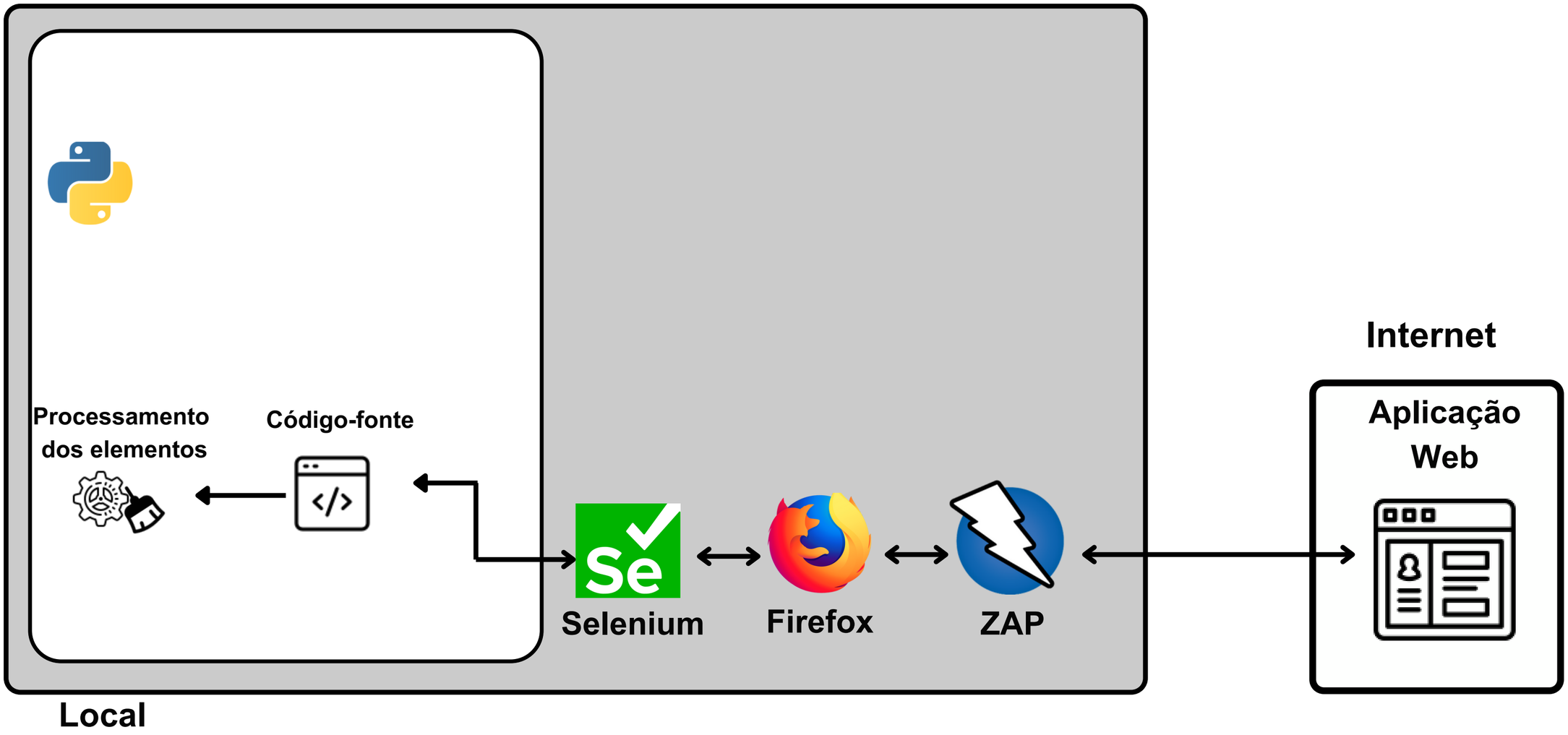
Solução Proposta - Arquitetura do Arcabouço



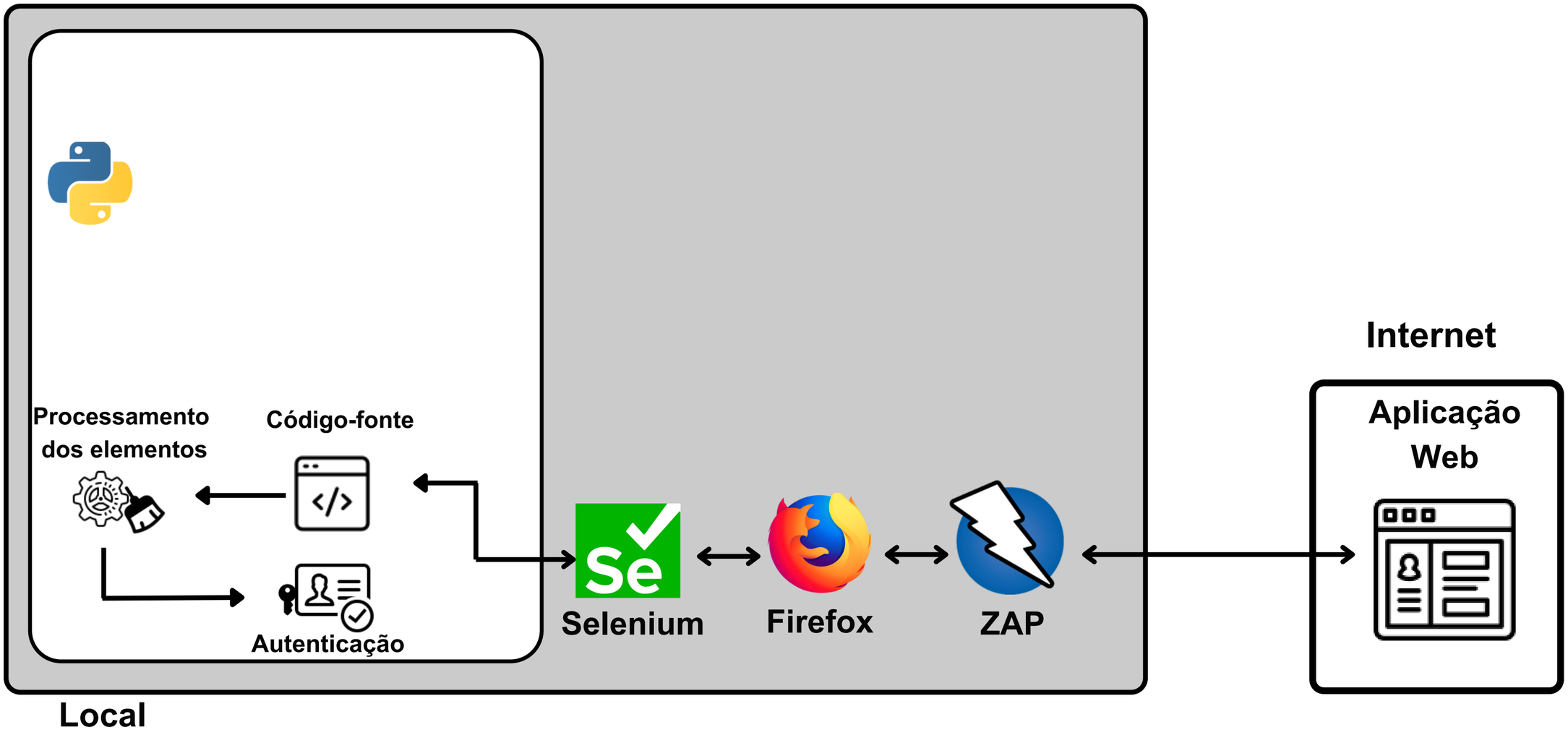
Solução Proposta - Arquitetura do Arcabouço



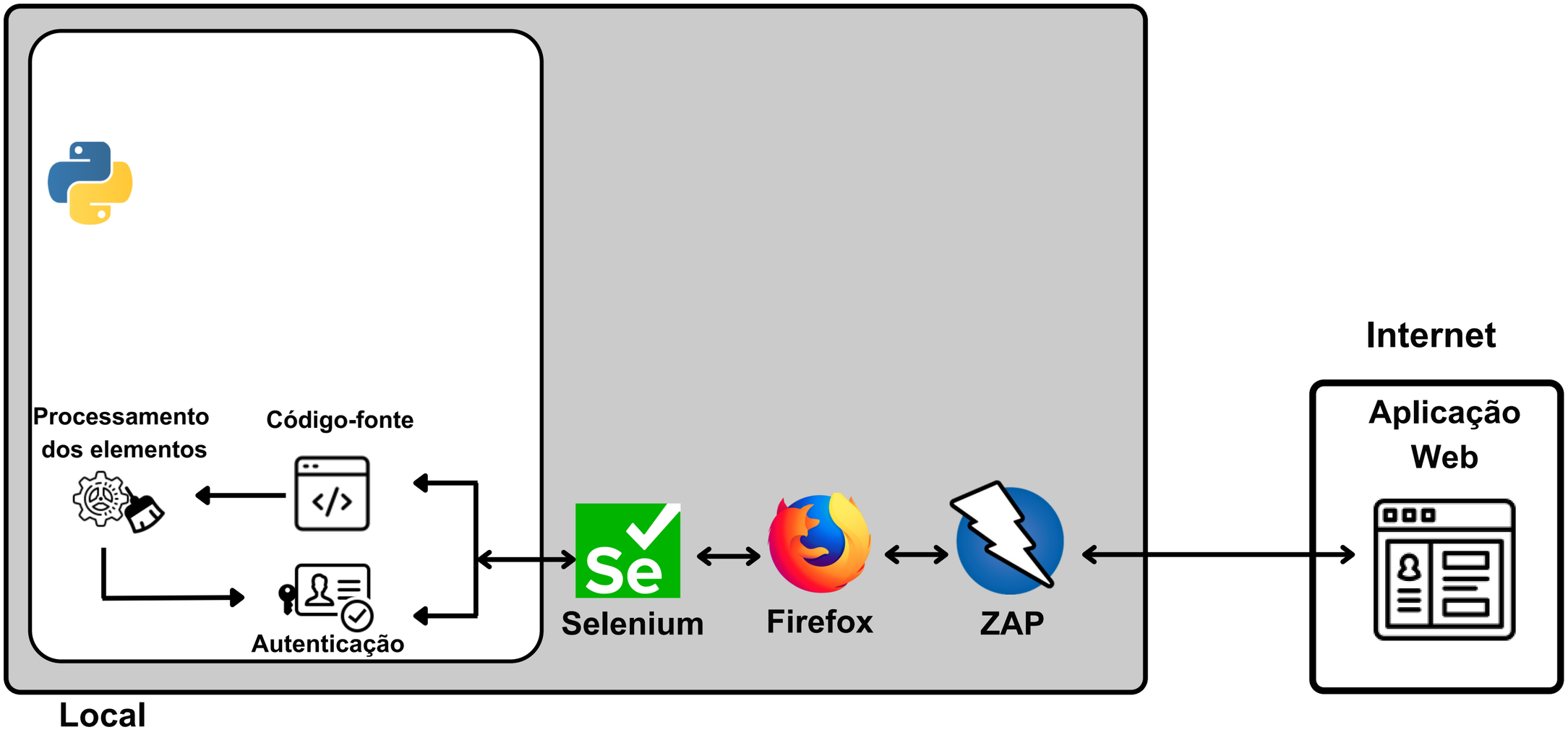
Solução Proposta - Arquitetura do Arcabouço



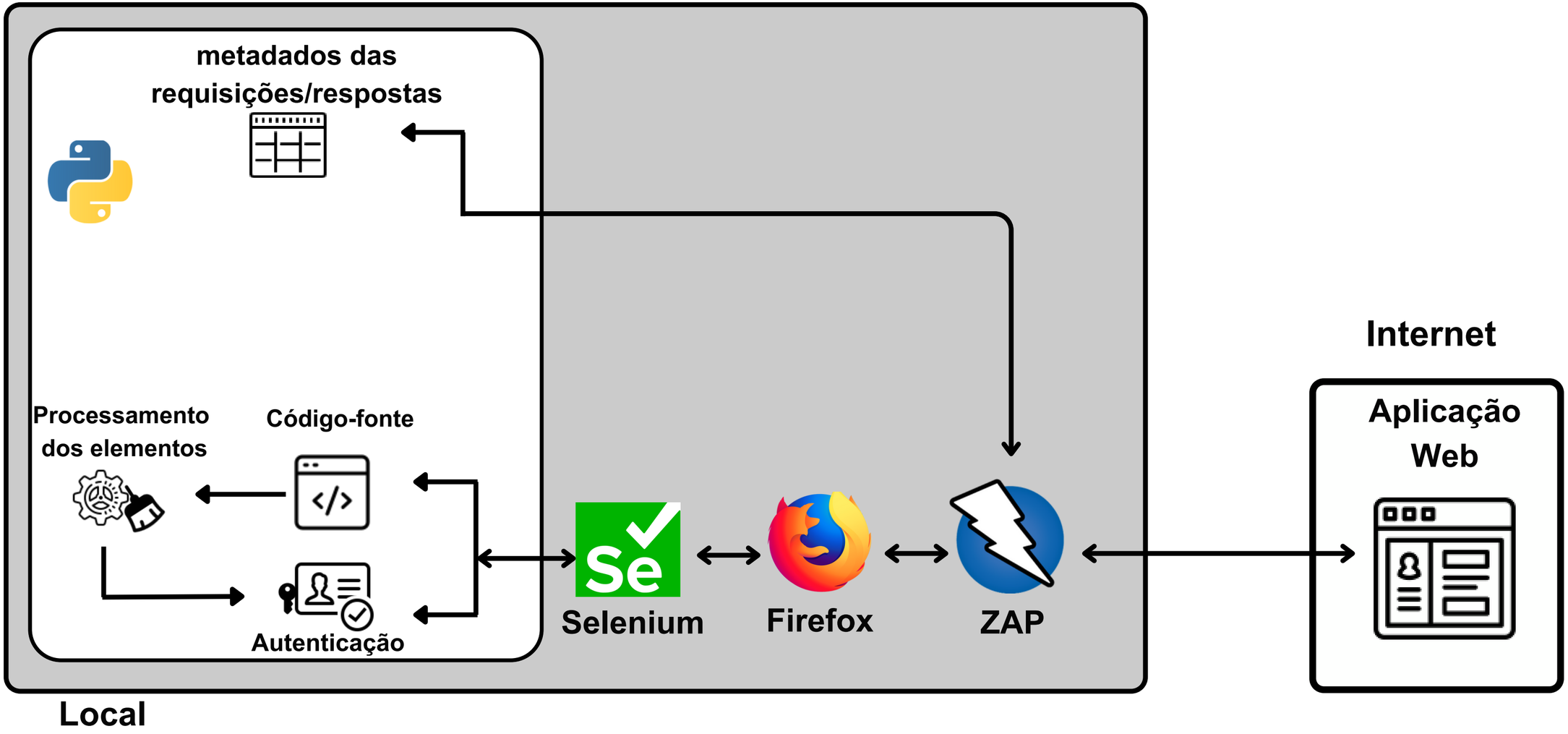
Solução Proposta - Arquitetura do Arcabouço



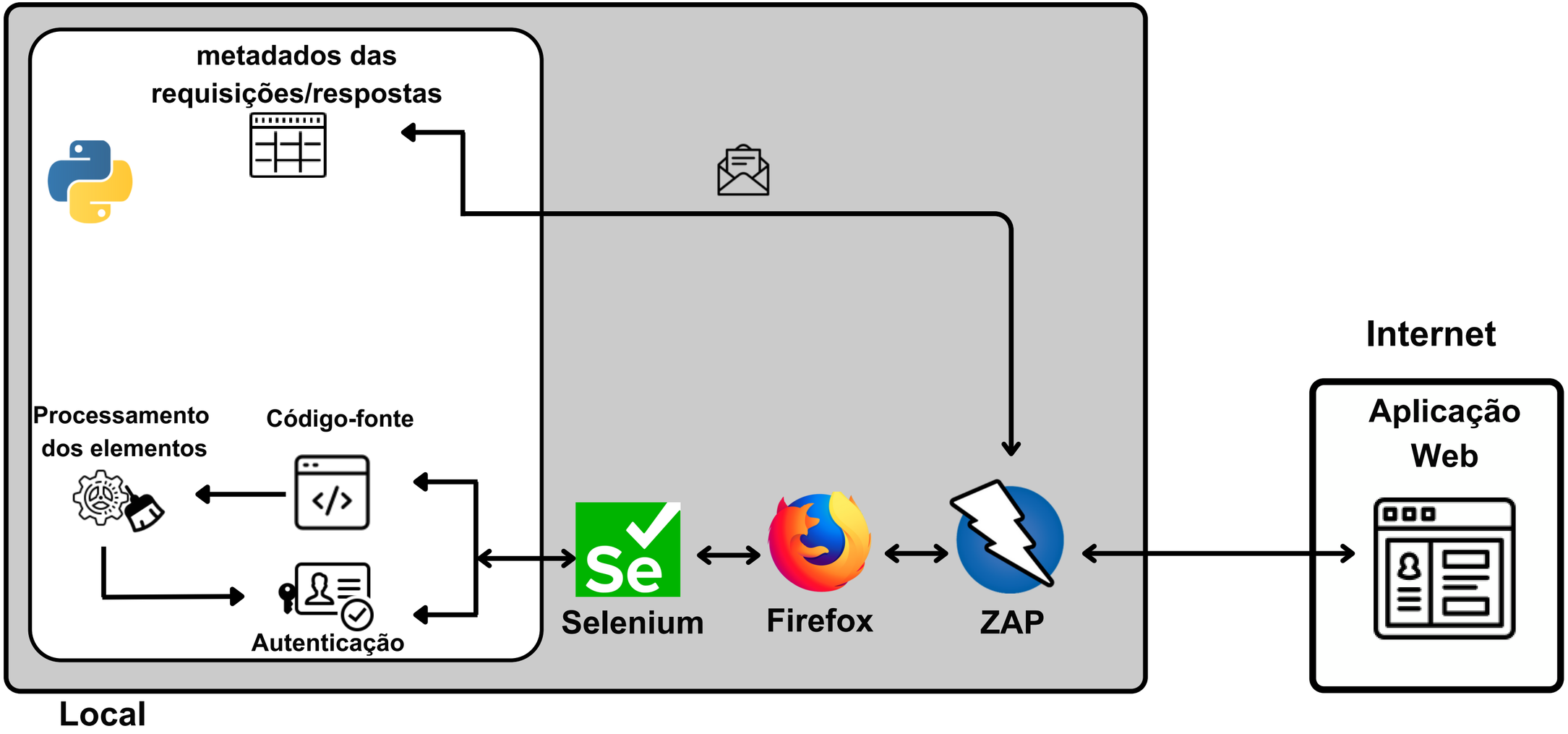
Solução Proposta - Arquitetura do Arcabouço



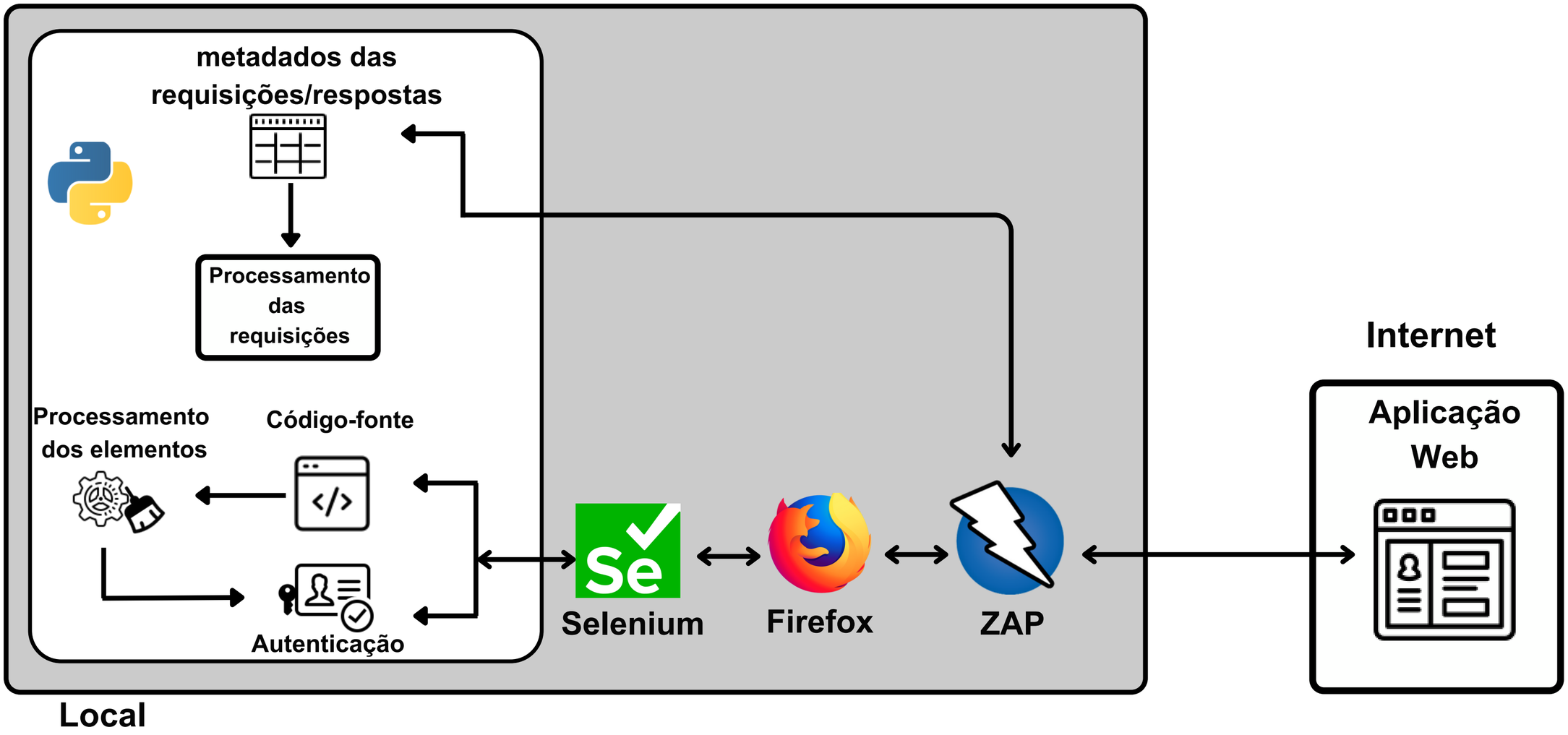
Solução Proposta - Arquitetura do Arcabouço



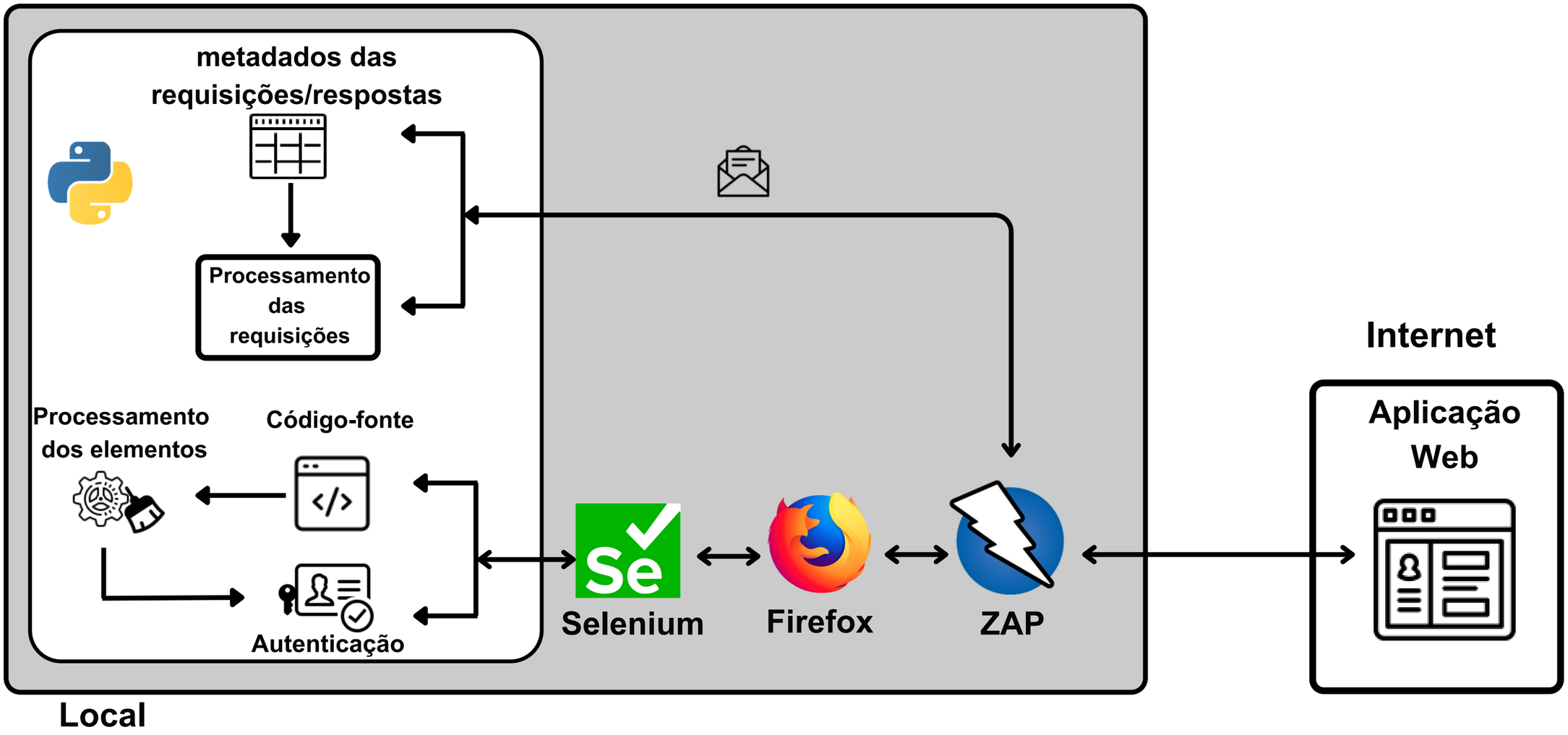
Solução Proposta - Arquitetura do Arcabouço



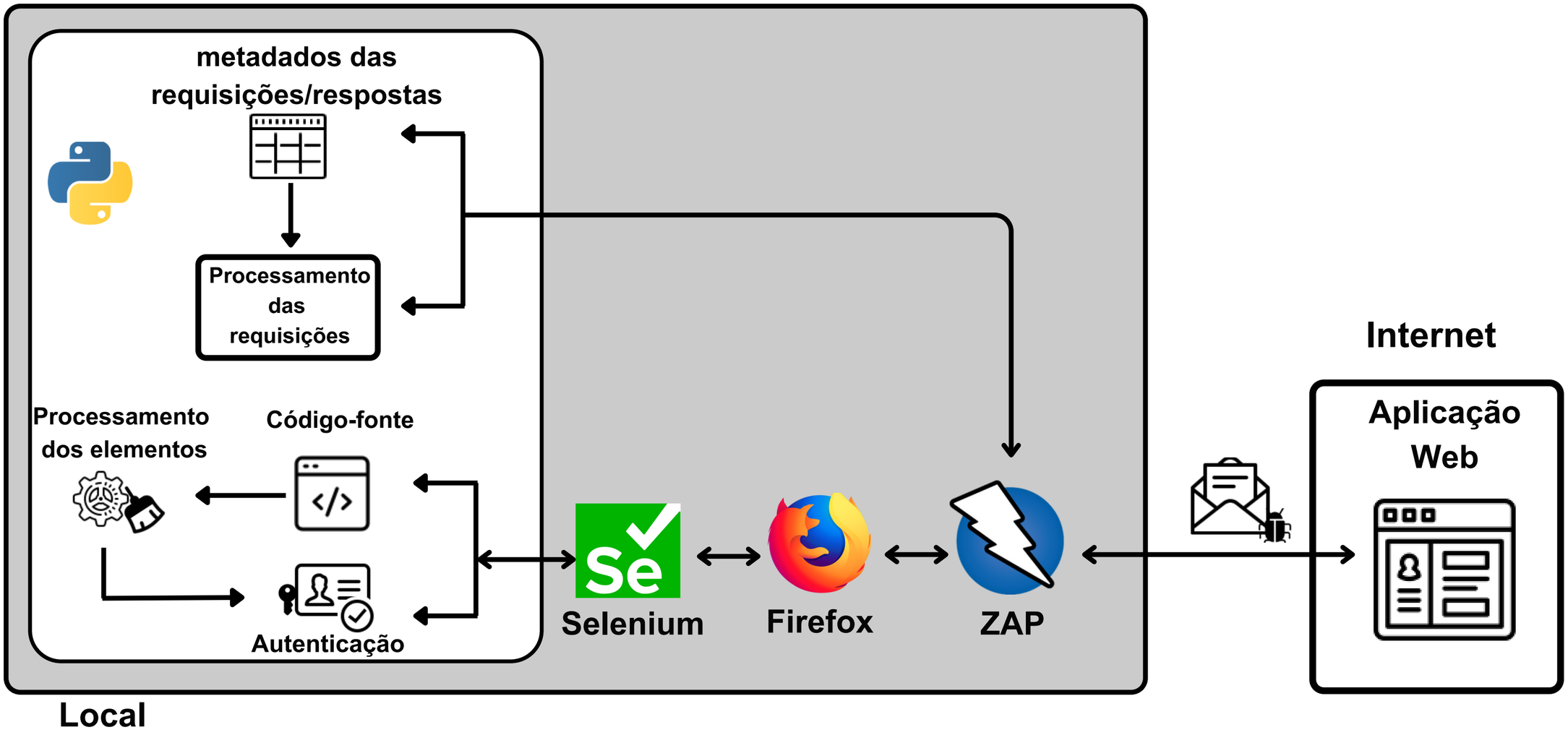
Solução Proposta - Arquitetura do Arcabouço



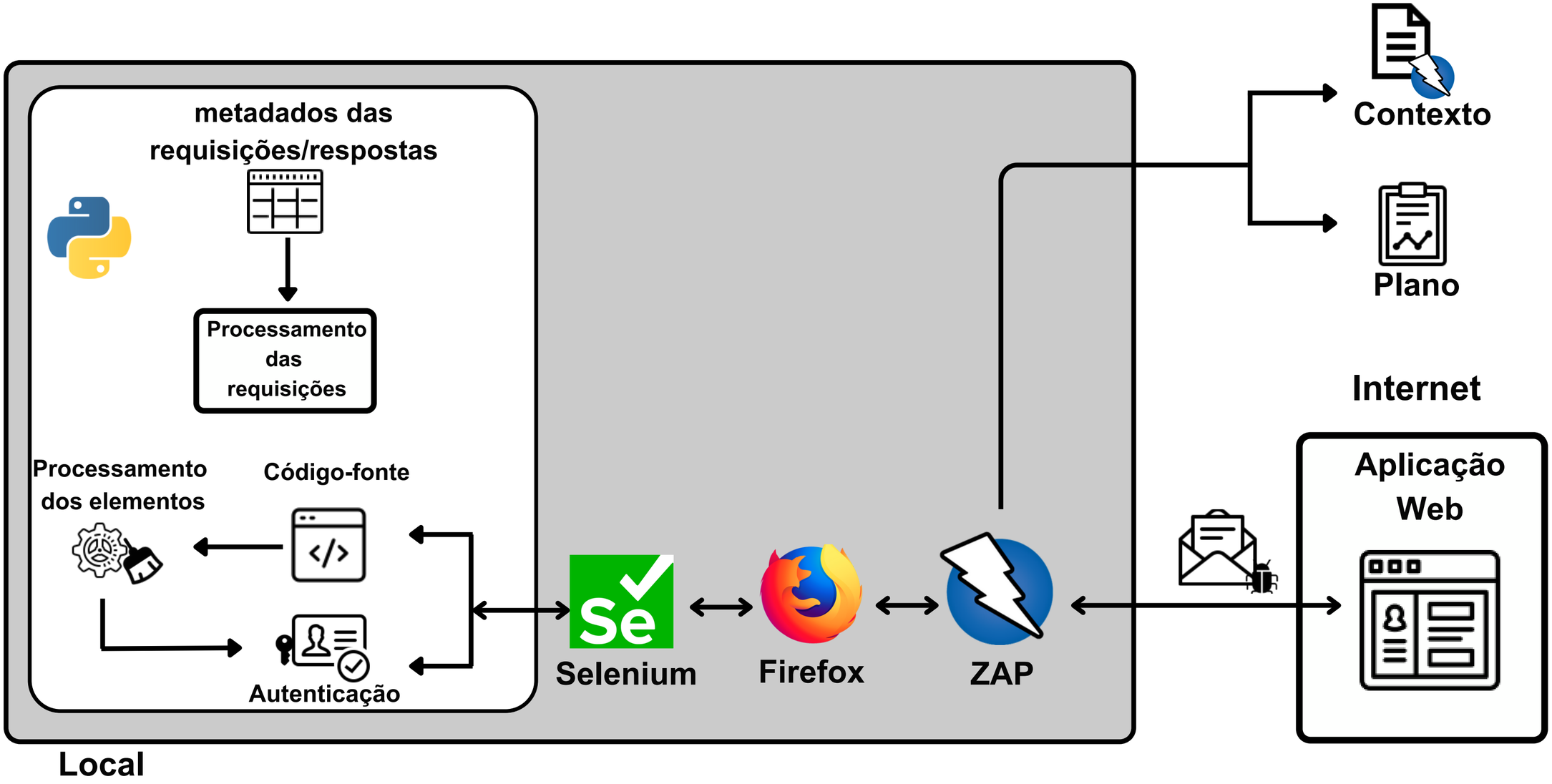
Solução Proposta - Arquitetura do Arcabouço



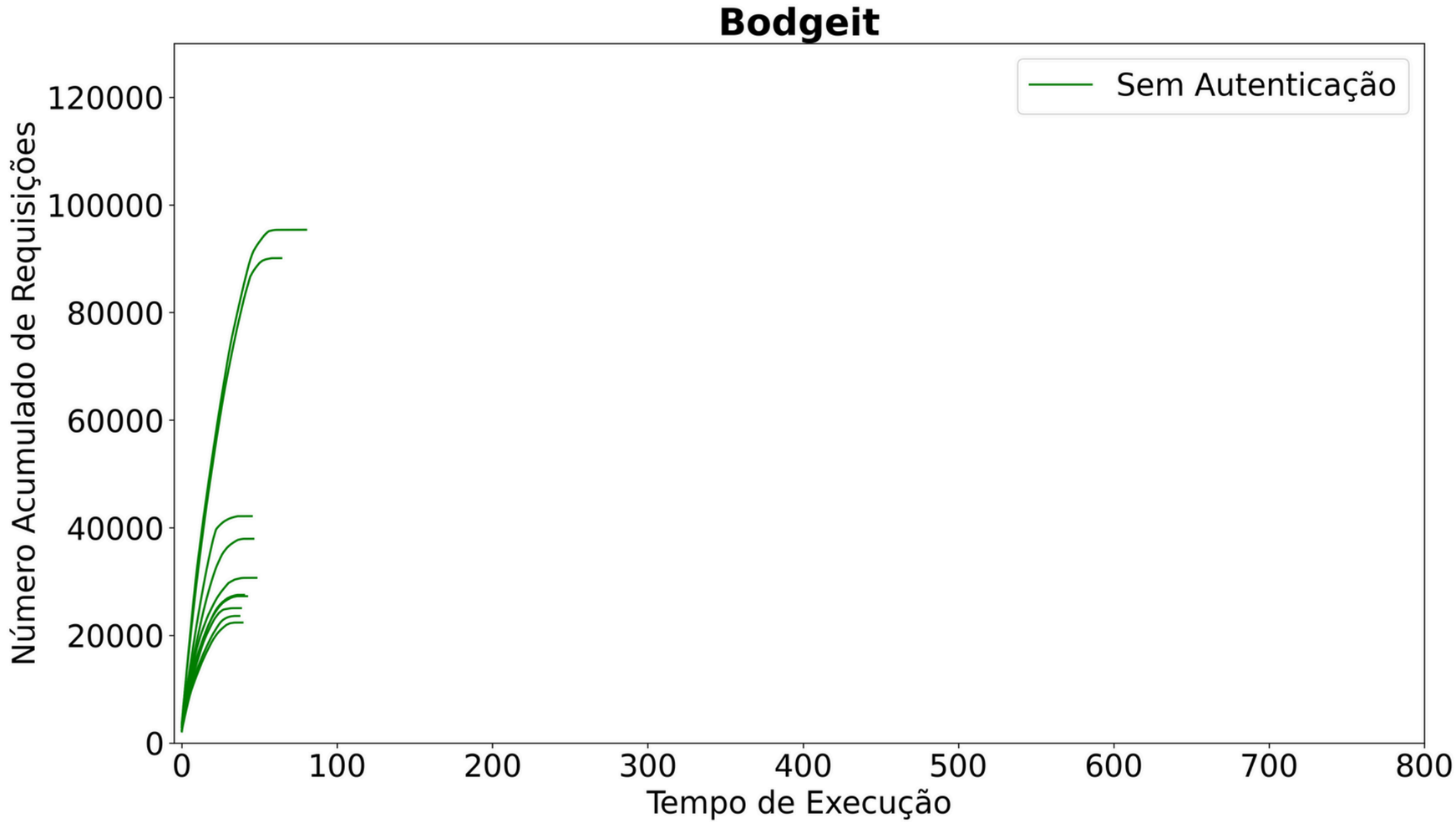
Solução Proposta - Arquitetura do Arcabouço



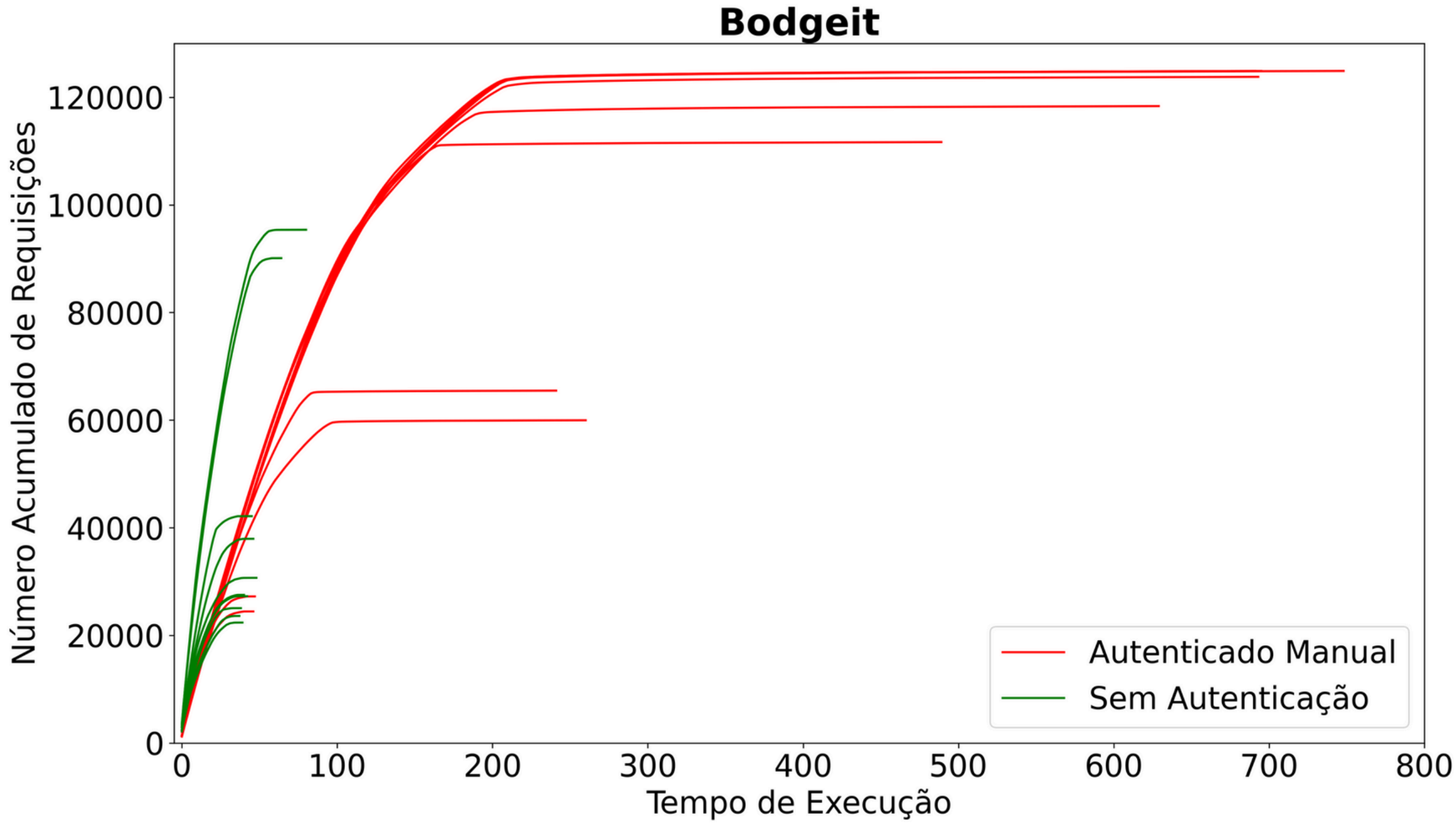
Solução Proposta - Arquitetura do Arcabouço



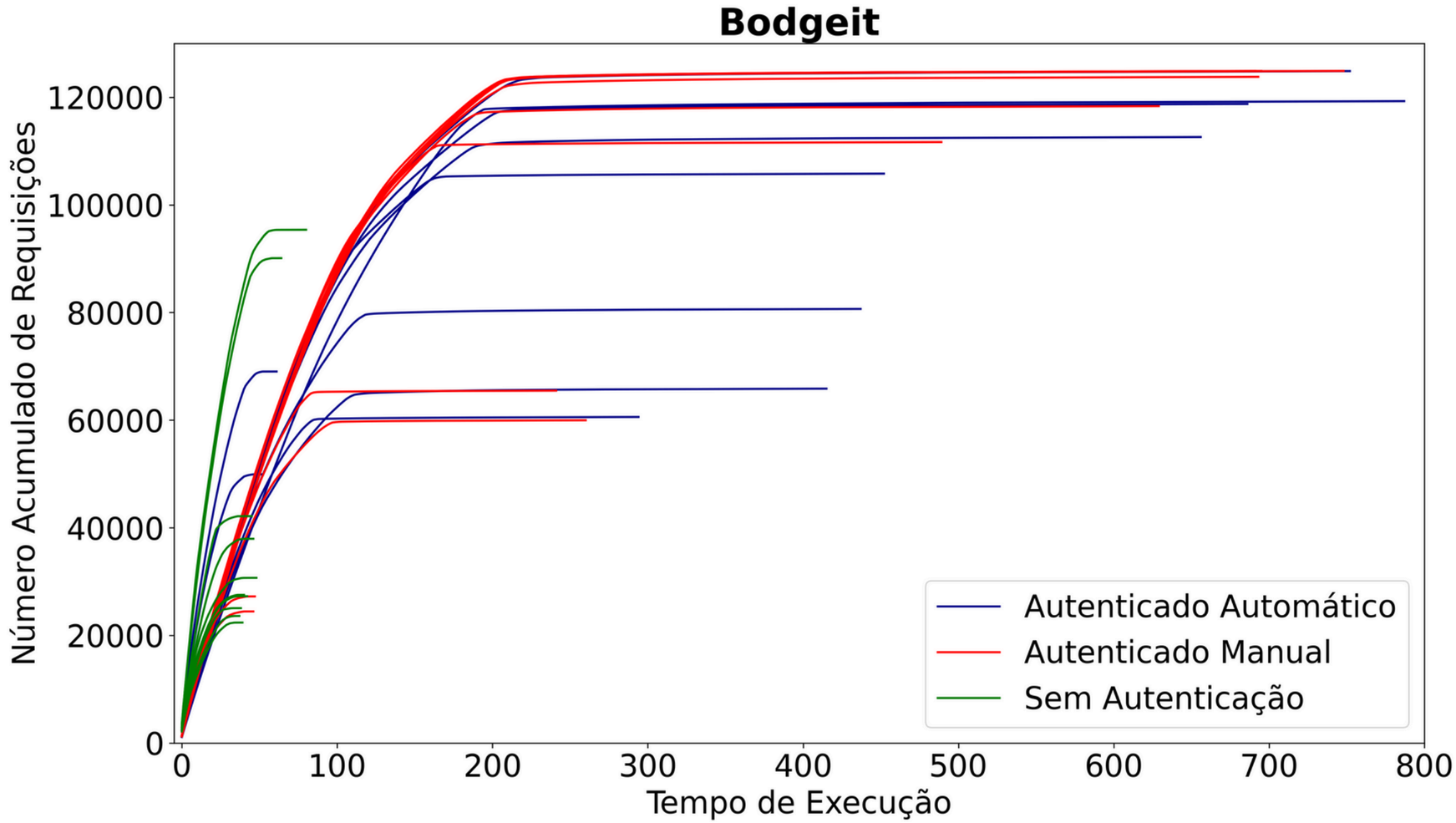
Avaliação - Testes Realizados



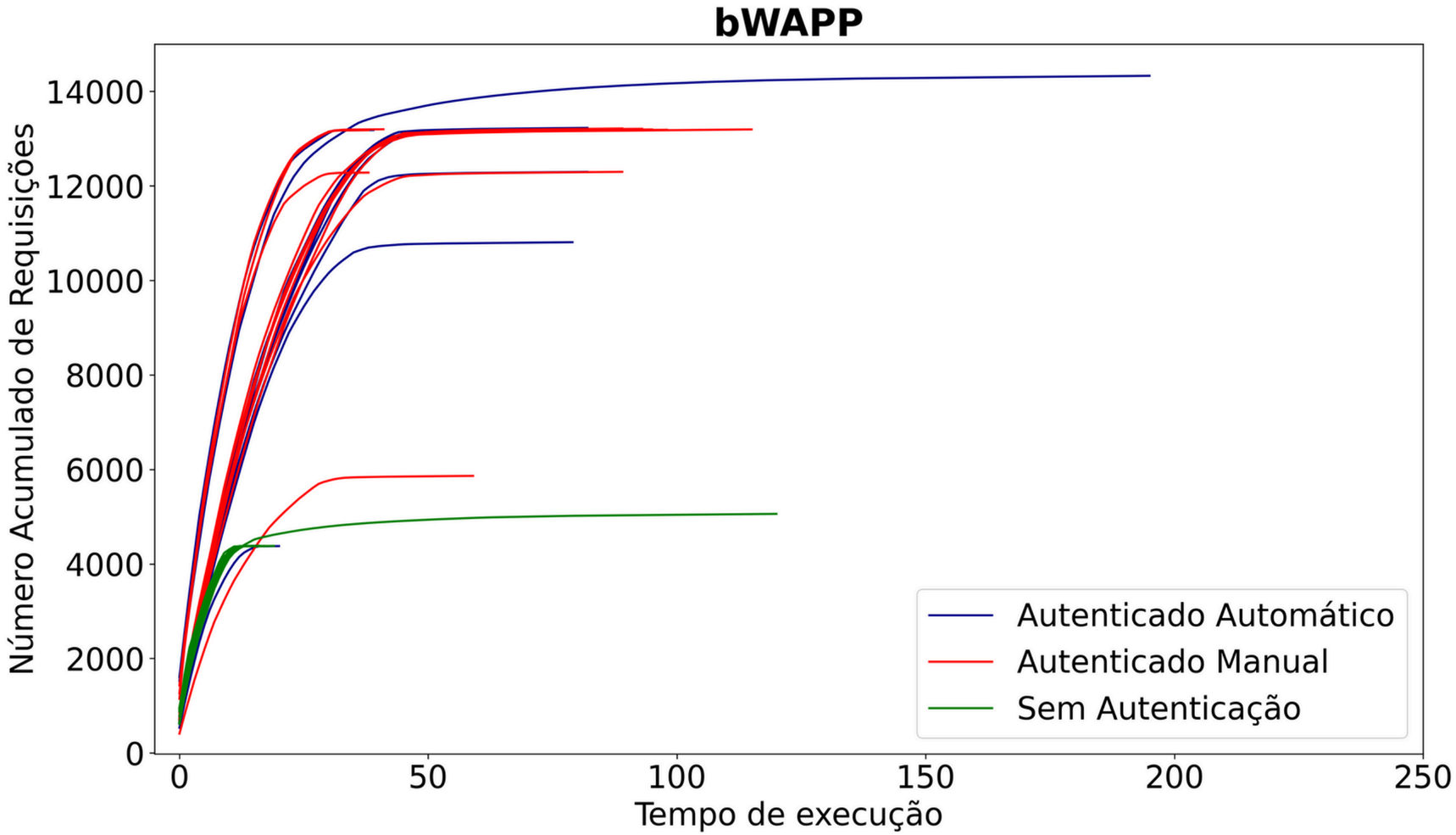
Avaliação - Testes Realizados



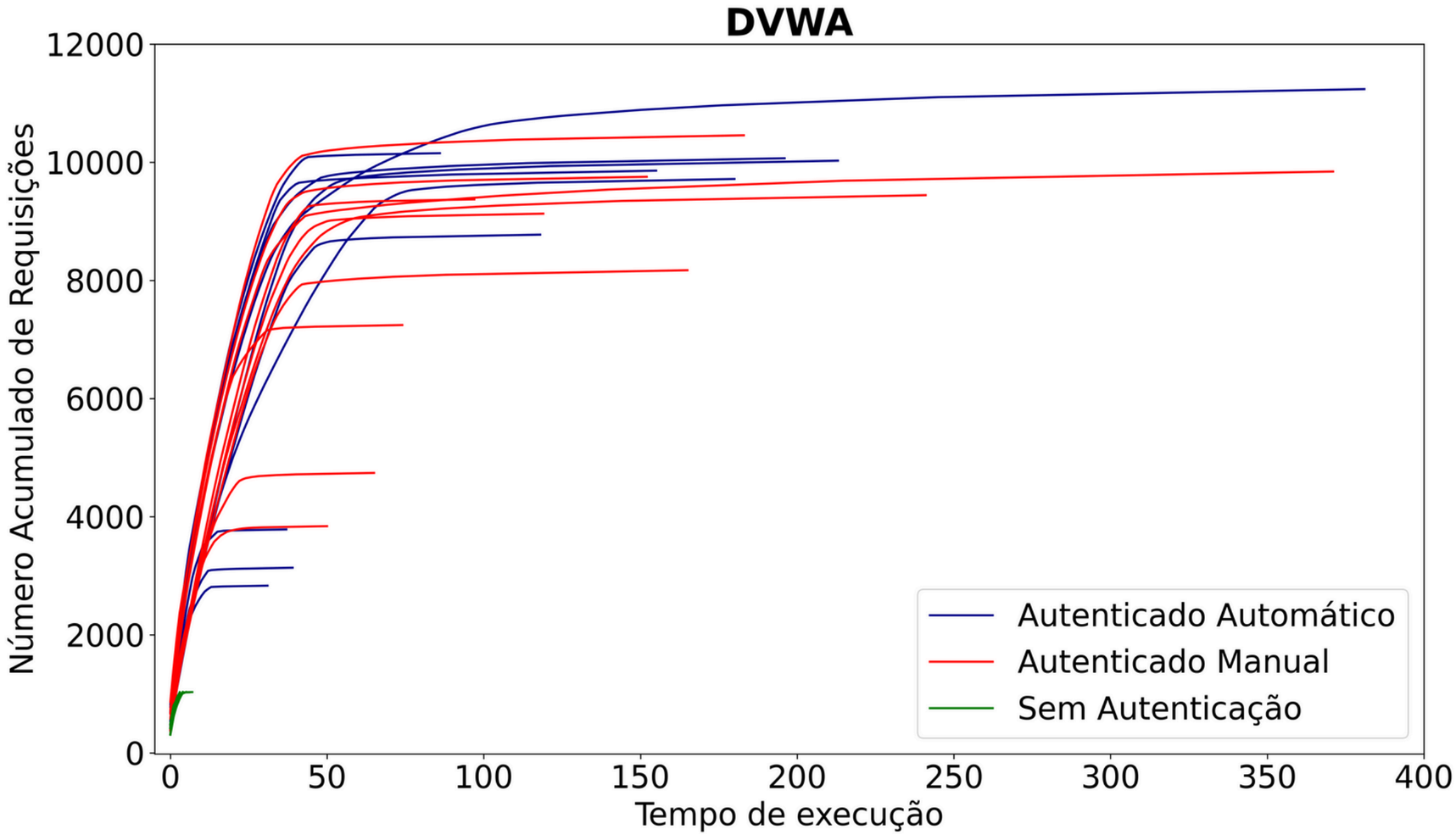
Avaliação - Testes Realizados



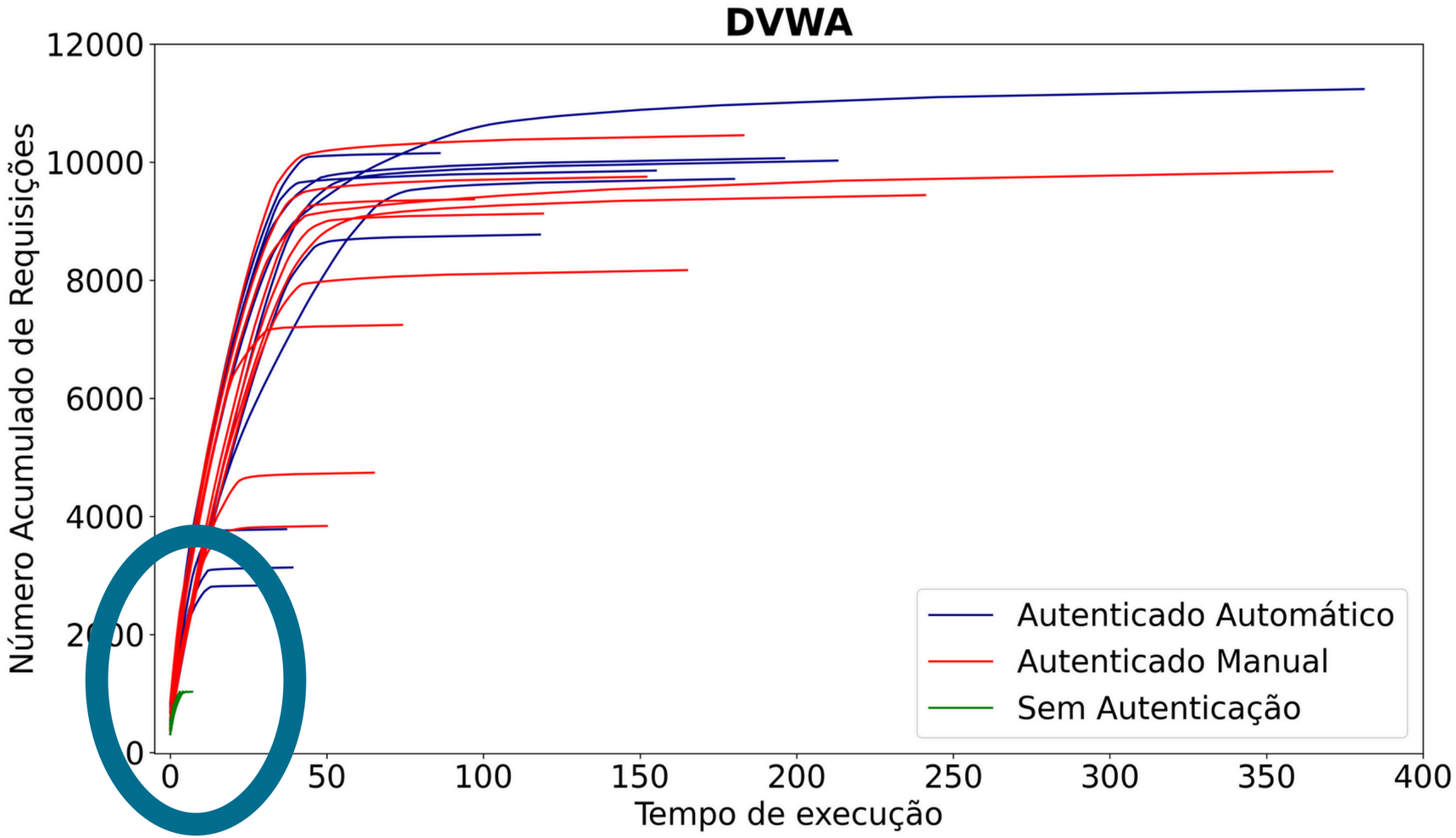
Avaliação - Testes Realizados



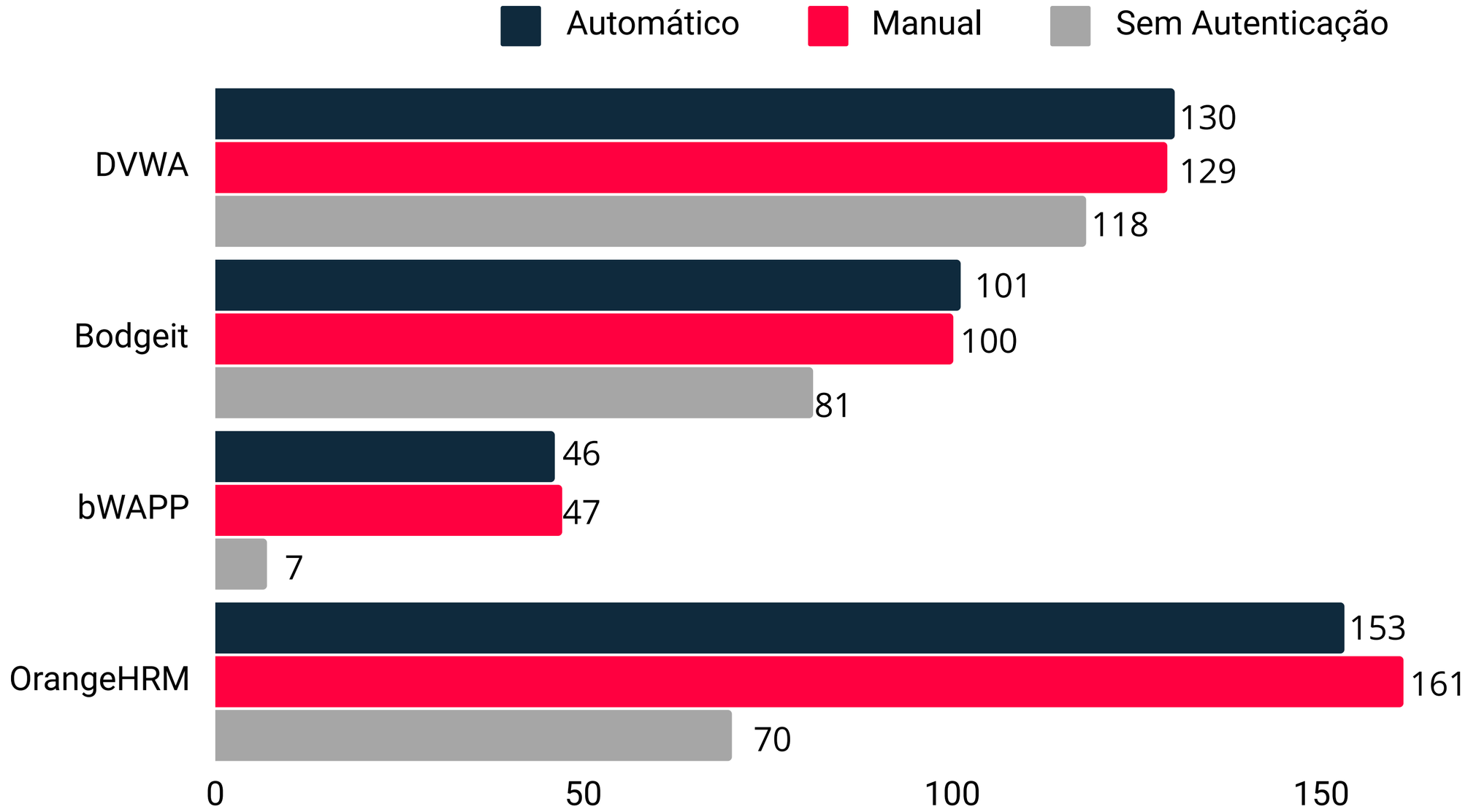
Avaliação - Testes Realizados



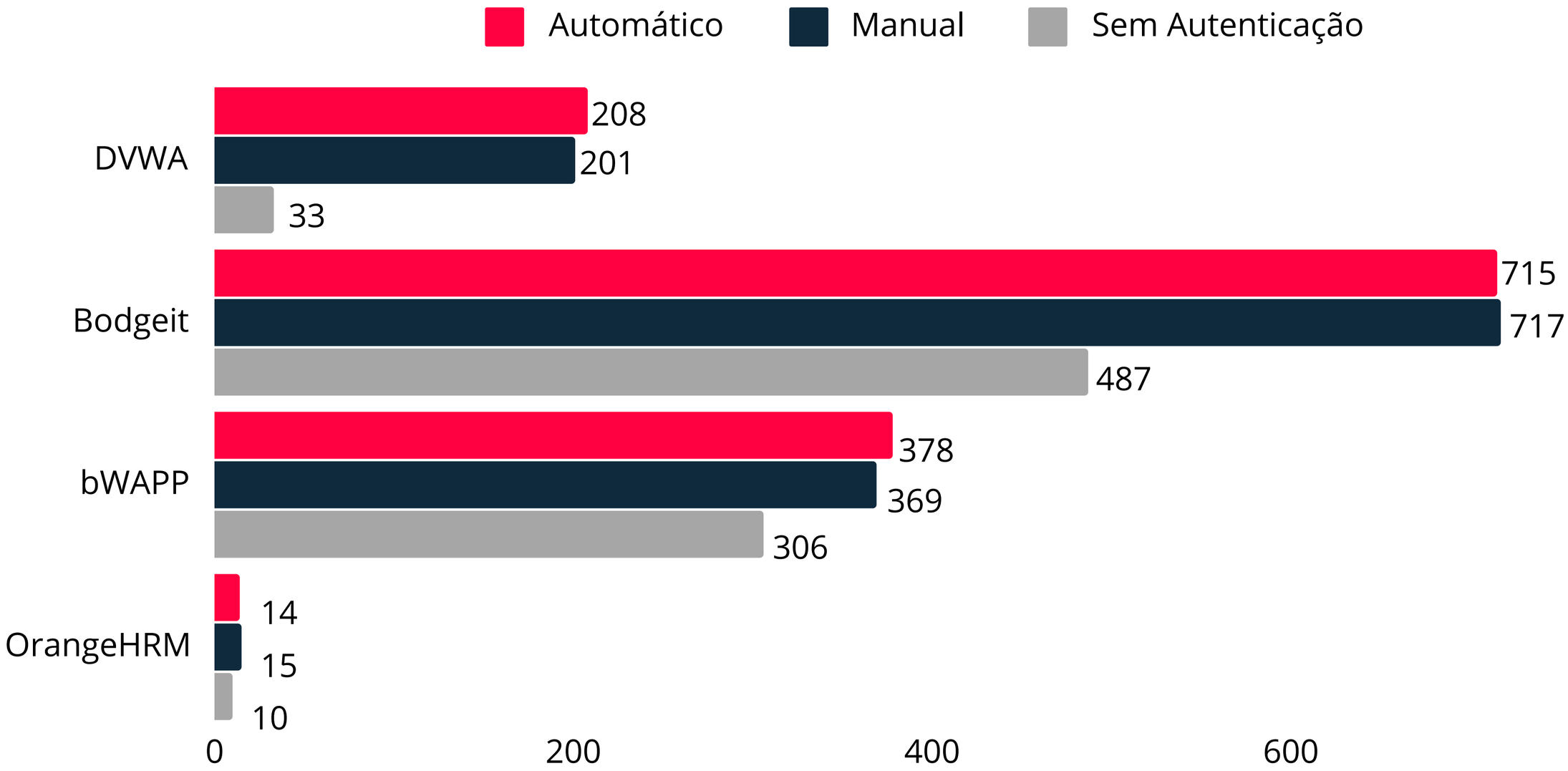
Avaliação - Testes Realizados



Avaliação - Cobertura das urls



Avaliação - Instancias de vulnerabilidades



Trabalhos futuros

- Estender o suporte aos demais tipos de autenticação.
- Estender o suporte para paginas geradas dinamicamente com JavaScript

Considerações finais

- Simplificamos o método de criação do contexto
- Geração do contexto preliminar para as aplicações
- Possibilidade de cobertura de uma grande quantidade de aplicações

Obrigado!

Lucas Sacramento
lucas.sacramento@dcc.ufmg.br