

Application Services Assignment

Purpose: This assignment is intended to evaluate your hands-on capabilities, give you a taste for the work we do, and show us how you communicate complex subjects in writing. You can refer to: Application Services, Cloudflare Docs and the Cloudflare Dashboard.

1. Project Overview

Project Name: Application Services Assignment

Created By: Micael Santos

Date: 18/02/2026

Cloud Provider: CloudFlare/AWS

2. Introduction

This document describes the implementation of a secure web application architecture using Cloudflare Application Services, as requested in the assignment.

The solution integrates multiple Cloudflare products including DNS, SSL/TLS, Cloudflare Tunnel, Zero Trust Access, Workers and R2 Storage, together with an AWS EC2 origin environment running a Flask application behind an NGINX reverse proxy.

The goal was to demonstrate the ability to design, deploy and secure an application using Cloudflare services while following best practices and documenting the process clearly.

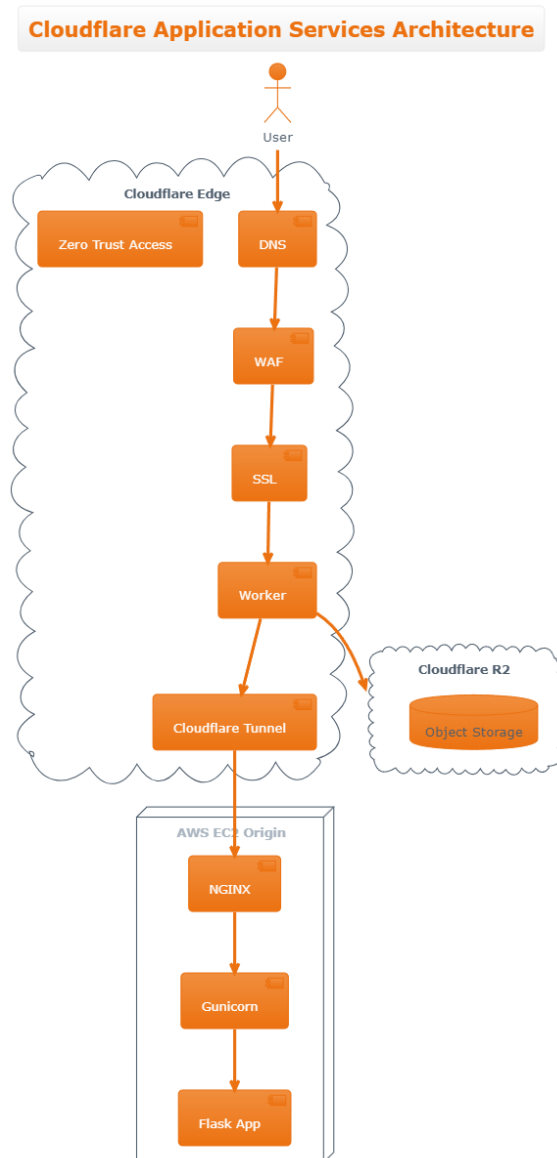


Fig. 1 Architecture diagram

3. Architecture Overview

The implemented architecture consists of two main traffic flows:

1. Public Application Flow:

User → Cloudflare Edge → Cloudflare Tunnel → AWS EC2 → NGINX → Gunicorn → Flask Application

Public Flow - Headers Application (Cloudflare -> Tunnel -> EC2)

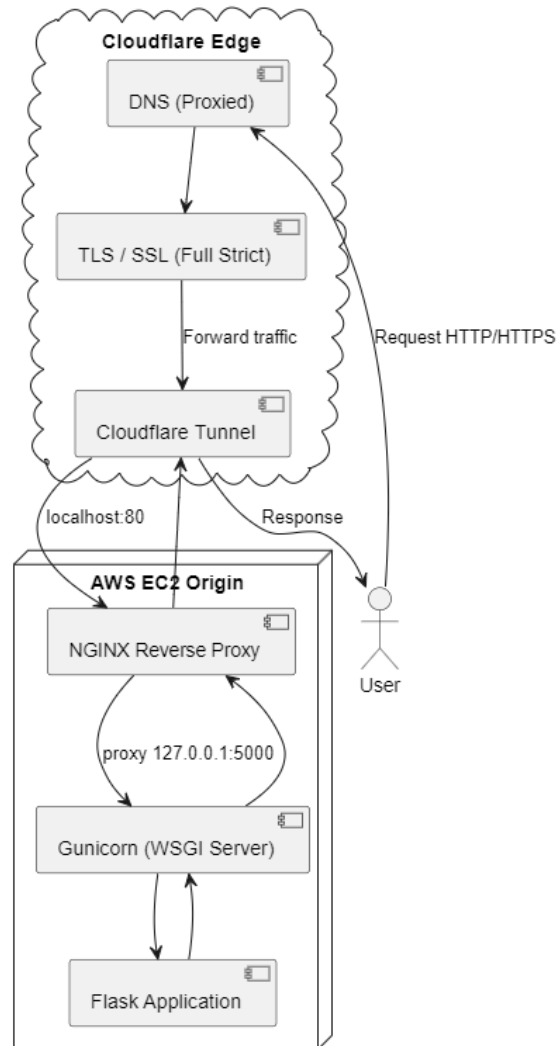


Fig. 2Public diagram

2. Secure Application Flow:

User → Cloudflare Edge → Zero Trust Access → Cloudflare Worker → Private R2 Bucket

The origin server is not directly exposed to the Internet, as all traffic is routed through Cloudflare Tunnel.

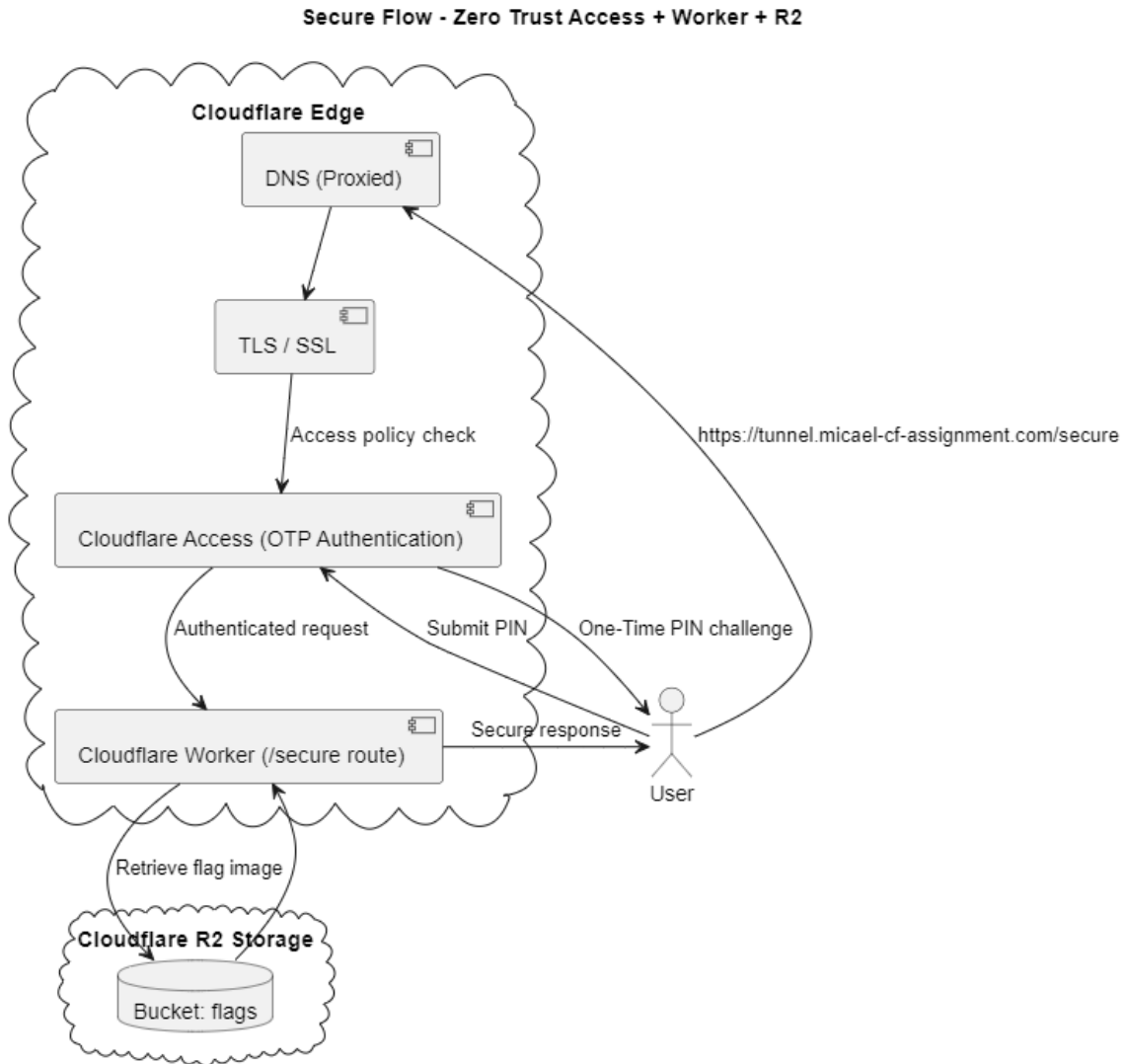


Fig. 3Secure diagram

4. Implementation Steps

Origin Web Server

An origin server was deployed on AWS EC2 using Ubuntu Linux.

A Flask application was created to return all HTTP request headers in the response body. The application was served using Gunicorn as a WSGI server and placed behind an NGINX reverse proxy.

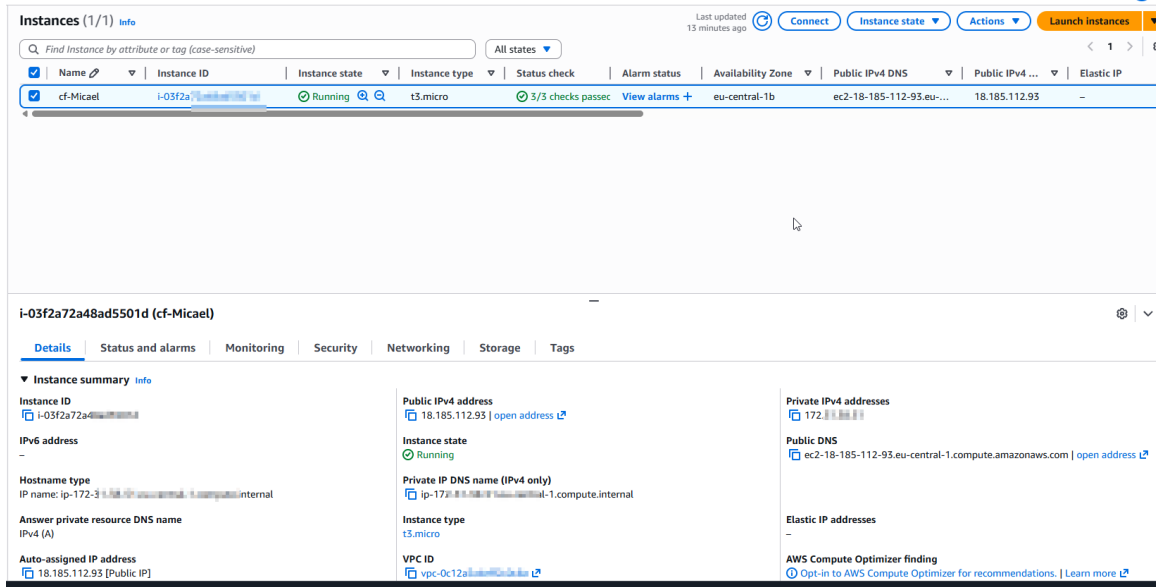


Fig. 4 EC2 instance running



Fig. 5 NGINX config file


```

Account registered.
Requesting a certificate for micalael-cf-assignment.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/micalael-cf-assignment.com/fullchain.pem
Key is saved at: /etc/letsencrypt/live/micalael-cf-assignment.com/privkey.pem
This certificate expires on 2026-05-18.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for micalael-cf-assignment.com to /etc/nginx/sites-enabled/default
Congratulations! You have successfully enabled HTTPS on https://micalael-cf-assignment.com

-----
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
 * Donating to EFF: https://eff.org/donate-le
-----
ubuntu@ip-172-31-38-51:/$

```

Fig. 10App certificate Let's Encrypt

Host: micalael-cf-assignment.com X-Real-IP: 104.23.241.25 Connection: close Priority: u=0, i Sec-Ch-Ua: (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, br Accept-Language: pt-BR CF-Visitor: {"scheme":"https"} X-Forwarded-Proto: https X-Forwarded-For: 2a02:a020:555:70e0:2518:41:3:1

Visualizador de certificados: micalael-cf-assignment.com

Geral Detalhes

Emitido para

Nome comum (CN)	micalael-cf-assignment.com
Organização (OI)	<Não faz parte do certificado>
Unidade organizacional (OU)	<Não faz parte do certificado>

Emitido por

Nome comum (CN)	WE1
Organização (OI)	Google Trust Services
Unidade organizacional (OU)	<Não faz parte do certificado>

Período de validade

Emitido em	terça-feira, 17 de fevereiro de 2026 às 14:18:52
Expira em	segunda-feira, 18 de maio de 2026 às 16:16:44

Impressões digitais SHA-256

Certificado	c735e70795f1185d3bb35afbe2cc6766d3444e7a80de22af42839f35516d597a
Chave pública	a8d72bf8d286292f04501bb6344e36b476adecf0a28cb81be9834916e720a

Fig. 11Certificate details browser (Cloudflare)

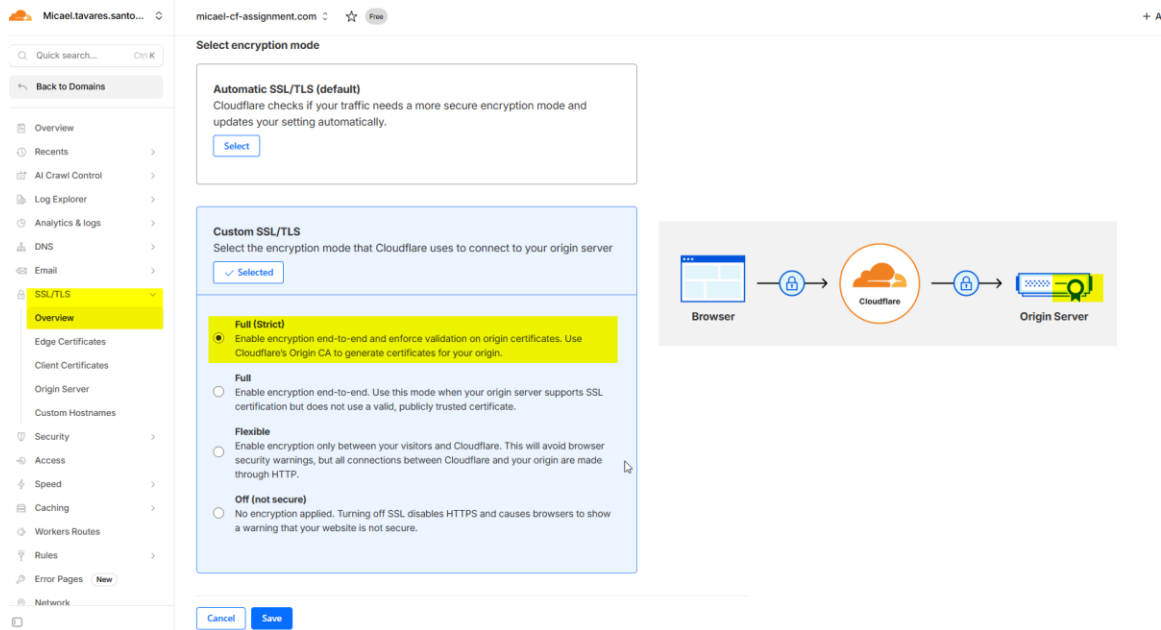


Fig. 12 Cloudflare SSL settings page

Cloudflare Tunnel

Cloudflare Tunnel was installed and configured on the origin server to securely expose the application without opening inbound firewall ports.

A subdomain tunnel.mydomain.com was configured to route traffic to the local NGINX service.

```
ubuntu@ip-172-31-38-51:/$ cloudflared tunnel login
Please open the following URL and log in with your Cloudflare account:
https://dash.cloudflare.com/tunnel?aud=c&callback=https%3A%2F%2Flogin.cloudflareaccess.org%2FyeivVR702CDgGiekI5zIDx1zrOu08QxASruiF_E42hs%3D

Leave cloudflared running to download the cert automatically.
2026-02-17T20:24:27Z INF Waiting for login...
2026-02-17T20:25:20Z INF Waiting for login...
2026-02-17T20:25:21Z INF You have successfully logged in.
If you wish to copy your credentials to a server, they have been saved to:
/home/ubuntu/.cloudflared/cert.pem
```

Fig. 13 cloudflared running

```
ubuntu@ip-172-31-38-51:/$ sudo cloudflared tunnel --config /etc/cloudflared/config.yml run cf-tunnel
2026-02-17T20:40:43Z INF Starting tunnel tunnelID=c69ccf08-c8fb-4de6-a100-a1c59e4f60b
2026-02-17T20:40:43Z INF Version 2026.2.0 (Checksum 176746db3e7dc7bd48f3dd287c8930e4545bb6e6700f883fddda54c307c16)
2026-02-17T20:40:43Z INF GOOS: linux, GOVERSION: go1.24.13, GOARCH: amd64
2026-02-17T20:40:43Z INF Settings: map[config:/etc/cloudflared/config.yml cred-file:/home/ubuntu/.cloudflared/c69ccf08-c8fb-4de6-a100-a1c59e4f60b.json credentials-file:/home/ubuntu/.cloudflared/c69ccf08-c8fb-4de6-a100-a1c59e4f60b.json]
2026-02-17T20:40:43Z INF cloudflared will not automatically update when run from the shell. To enable auto-updates, run cloudflared as a service: https://developers.cloudflare.com/cloudflare-one/connections/connect-apps/configure-tunnels/local-management/as-a-service/
2026-02-17T20:40:43Z INF Generated Connector ID: 0b86de5-fa18-402f-a0cb-2f9d57c4aa2
2026-02-17T20:40:43Z INF Initial protocol quit
2026-02-17T20:40:43Z INF ICMP proxy will use 172.31.38.51 as source for IPv4
2026-02-17T20:40:43Z INF ICMP proxy will use fe80::42e:6dff:fe41:8d89 in zone ena5 as source for IPv6
2026-02-17T20:40:43Z INF The user running cloudflared process has a GID (group ID) that is not within ping_group_range. You might need to add that user to a group within that range, or instead update the range to encompass a group the user is already in by modifying /proc/sys/net/ipv4/ping_group_range. Otherwise cloudflared will not be able to ping this network error="group 12 is not between ping group 1 to 0"
2026-02-17T20:40:43Z INF ICMP proxy feature is disabled
2026-02-17T20:40:43Z INF ICMP proxy will use 172.31.38.51 as source for IPv4
2026-02-17T20:40:43Z INF ICMP proxy will use fe80::42e:6dff:fe41:8d89 in zone ena5 as source for IPv6
2026-02-17T20:40:43Z INF Starting metrics server on 127.0.0.1:20241/metrics
2026-02-17T20:40:43Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveP256] connIndex=0 event=0 ip=198.41.192.167
2026-02-17T20:40:43Z INF Registered tunnel connection connIndex=0 connection=84dfa72-4b1a-41e9-ac9b-4f979bfb44 event=0 ip=198.41.192.167 location=fra10 protocol=quic
2026-02-17T20:40:43Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveP256] connIndex=1 event=0 ip=198.41.200.113
2026-02-17T20:40:43Z INF Registered tunnel connection connIndex=1 connection=54765e55-68a9-44ed-baba-54879079ef4b event=0 ip=198.41.192.7 location=fra08 protocol=quic
2026-02-17T20:40:43Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveP256] connIndex=2 event=0 ip=198.41.200.113 location=fra20 protocol=quic
2026-02-17T20:40:43Z INF Registered tunnel connection connIndex=2 connection=cad60b45-4f4f-4af1-a80e-0df013f90874 event=0 ip=198.41.200.53
2026-02-17T20:40:43Z INF Registered tunnel connection connIndex=3 connection=cad60b45-4f4f-4af1-a80e-0df013f90874 event=0 ip=198.41.200.53
```

Fig. 14 Tunnel running

Host: tunnel.micael-cf-assignment.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Accept-Encoding: gzip, br Accept-Language: pt-PT;q=0.9,en-US;q=0.8,en;q=0.7 Cache-Control: max-age=0 Cdn-Loop: cloudflare; loop=1 Cf-Connecting-Ip: 2a02:a020:555:7060:2518:4473:2583:8e18 Cf-IpCountry: BE Cf-Ray: 9c823f5c9dcb726-BRU CF-Visitor: {"scheme":"https"} CF-Warp-Tag-Id: a2806e2-a0f0-4f5e-bf2a-588e43a6b72f Connection: keep-alive Priority: u=0, i Sec-Ch-Ua: "Not(A)Brand",v="8", "Chromium",v="144", "Google Chrome",v="144" Sec-Ch-Ua-Mobile: ?0 Sec-Ch-Ua-Platform: "Windows" Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: none Sec-Fetch-User: ?1 Upgrade-Insecure-Requests: 1 X-Forwarded-For: 2a02:a020:555:7060:2518:4473:2583:8e18 X-Forwarded-Proto: https

Fig. 15 Browser accessing tunnel URL

Zero Trust IdP

Cloudflare Zero Trust Access was configured using One-Time PIN (OTP) authentication as the Identity Provider.

This allowed secure user authentication without integrating an external identity platform.

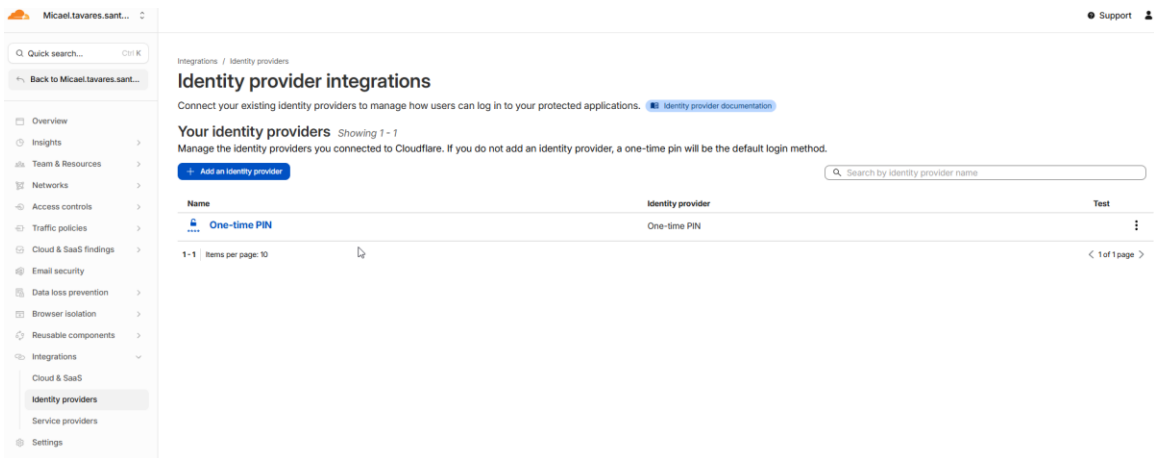


Fig. 16 IdP OTP

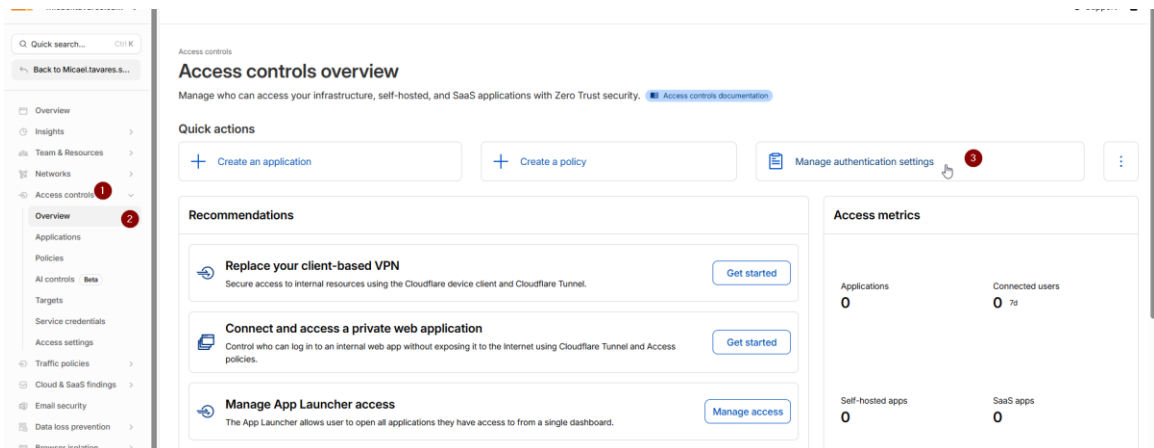


Fig. 17 App config for OTP

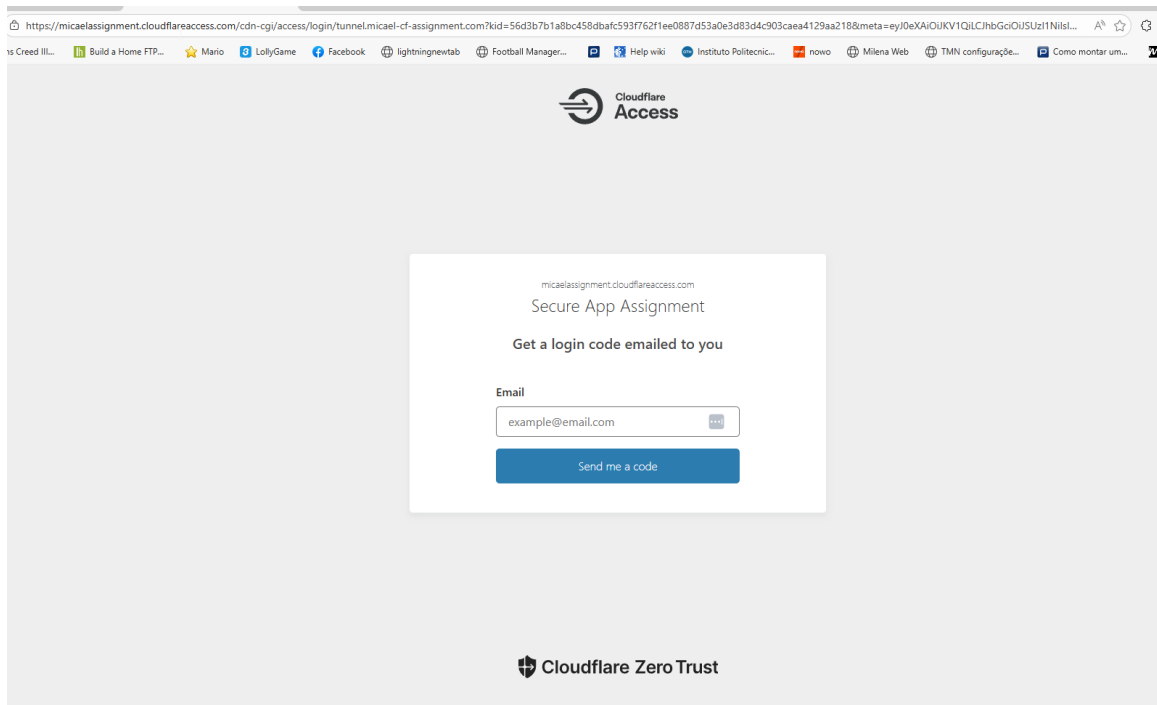


Fig. 18 Login screen

Secure Path Protection

Access policies were configured to protect the /secure path of the tunnel subdomain.

Access was restricted to:

- The project owner email
- Users with @cloudflare.com domain

Direct access to the origin IP was prevented by security group configuration and by routing traffic exclusively through Cloudflare Tunnel.

[← Back to Applications](#)

Add an application

Configure the policies, authentication, and settings of your application.

Select type > **Configure application** > Experience settings (optional) > Advanced settings (optional)

Basic information

Configure your application's basic details and paths. Enter hostnames or IPs to protect an entire website or specific subdomains and paths.

Application name (Required)

Assignment Secure App

21 / 350

Session Duration (Required)

1 month ▼

Public hostname

Input method

D... ▼

Subdomain

tunnel

Domain (Required)

micael-cf-assignment.com ▼

×

Path

/ secure*

+ Add public hostname + Add private hostname + Add private IP

Fig. 19 Access Policy rule

Include OR

If more than one Include rule is configured, users only need to meet one of the criteria.

Selector (Required)

Emails

Value

micael.tavares.santos@gmail.com + email@example.com

Selector (Required)

Emails ending in

Value

@cloudflare +

x

+ Add include + Add require + Add exclude

Policy tester

The policy tester evaluates the last seen identity of active users. Login decisions may differ if there are changes to user attributes evaluated by this policy.

Test policy

✓ 1 user (100%) is blocked

Username	Email	Status
micaelsantos_69	micaelsantos_69@hotmail.com	BLOCKED

1 - 1

Items per page: 5

<

1 of 1 page

>

Fig. 20Block test

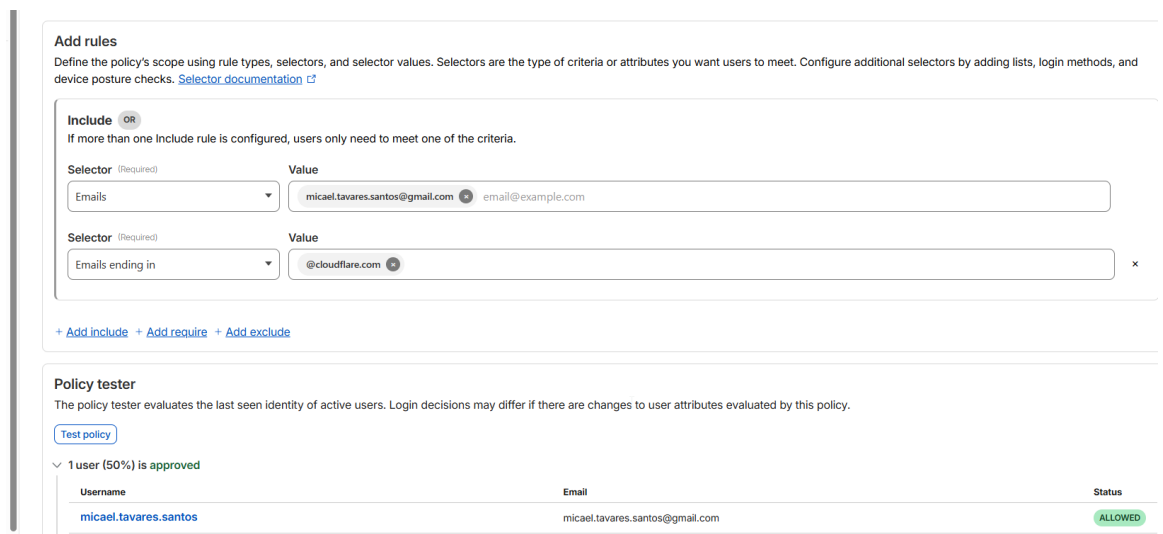
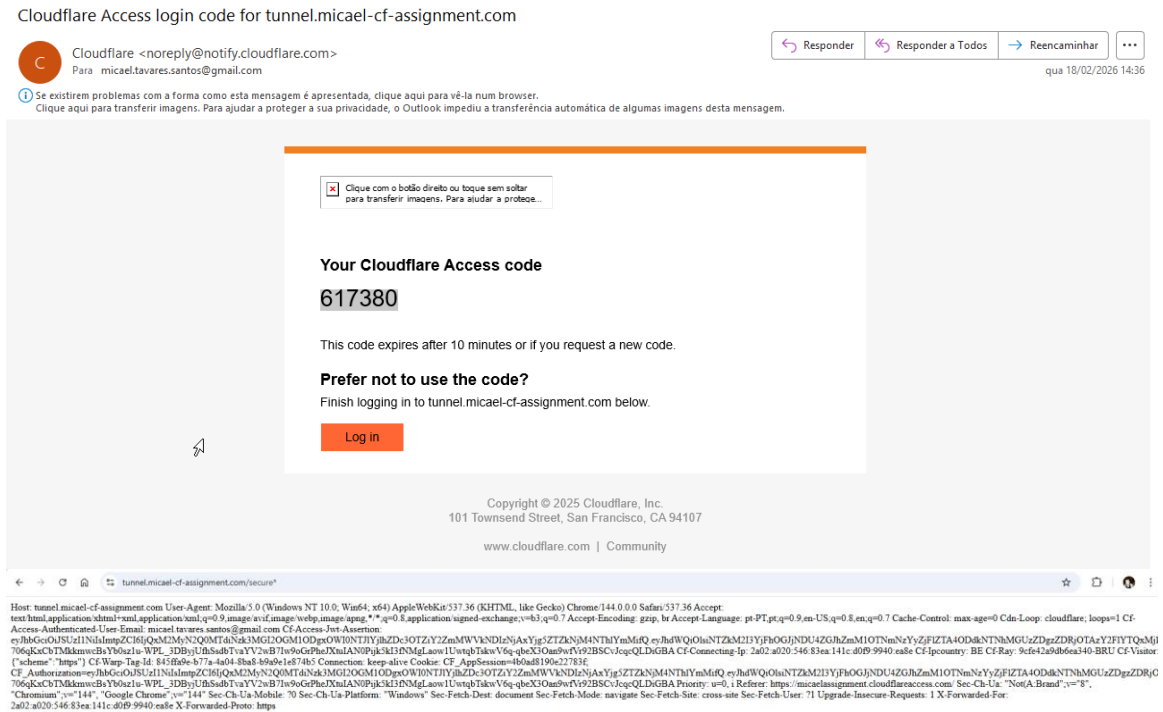


Fig. 21 Working Test

Worker + R2

A Cloudflare Worker was created to run on the /secure path.

The Worker:

- Extracts user identity information from Cloudflare Access headers
- Displays authentication metadata

- Retrieves country flag images from a private R2 bucket

The Worker was deployed using the Wrangler CLI and code was uploaded to a public Git repository.

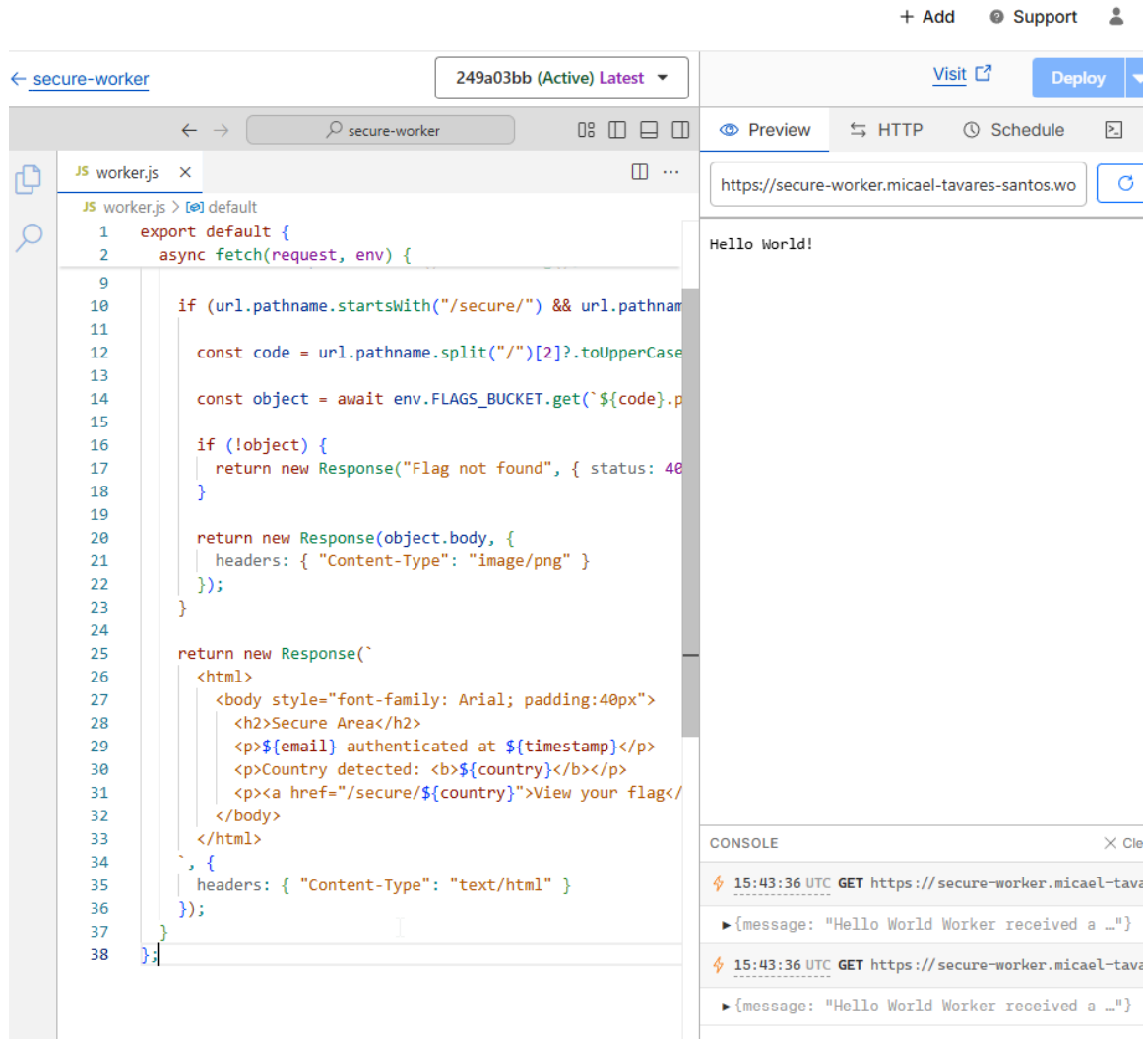


Fig. 22 Worker code

R2 Object Storage > flags

+ Add

Support

Default Storage Class ⓘPublic Access ⓘBucket SizeClass A Operations ⓘClass B Operations ⓘ

Standard

Disabled

0 B

10

30

Objects

Metrics

Settings

Search objects by prefix

Search

☒ View prefixes as directories ⓘ

flags /

Upload

+ Add directory

<input type="checkbox"/>	Objects	Type	Storage Class	Size	Modified
<input type="checkbox"/>	BE.png	image/png	Standard	292 B	18 Feb 2... WE↑••
<input type="checkbox"/>	DE.png	image/png	Standard	151 B	18 Feb 2... WE↑••
<input type="checkbox"/>	ES.png	image/png	Standard	3.28 ...	18 Feb 2... WE↑••
<input type="checkbox"/>	FR.png	image/png	Standard	254 B	18 Feb 2... WE↑••
<input type="checkbox"/>	IT.png	image/png	Standard	253 B	18 Feb 2... WE↑••
<input type="checkbox"/>	LU.png	image/png	Standard	151 B	18 Feb 2... WE↑••

Drag and drop to start uploading

Fig. 23R2 bucket



Metrics

Deployments

Bindings

Observability

Settings

</> Edit code

Visit ↗

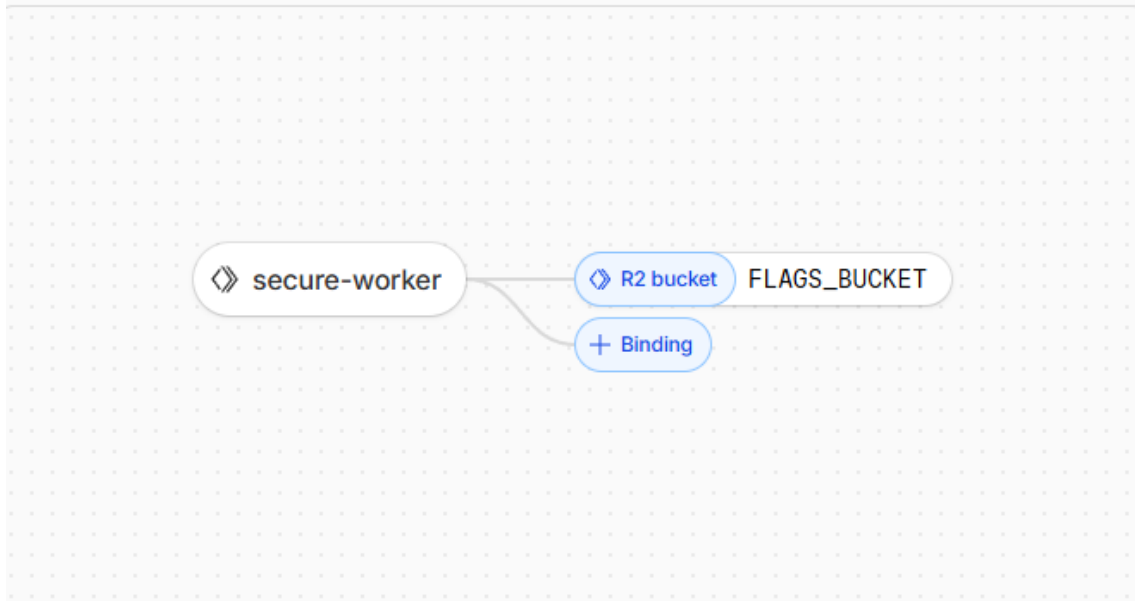
Bindings

Add and connect external resources to your Worker without needing to manage permissions or API keys.

View docs ↗

Add binding +

Connected Bindings





Type	Name	Value	
R2 bucket	FLAGS_BUCKET	flags	 

Fig. 24Worker binding

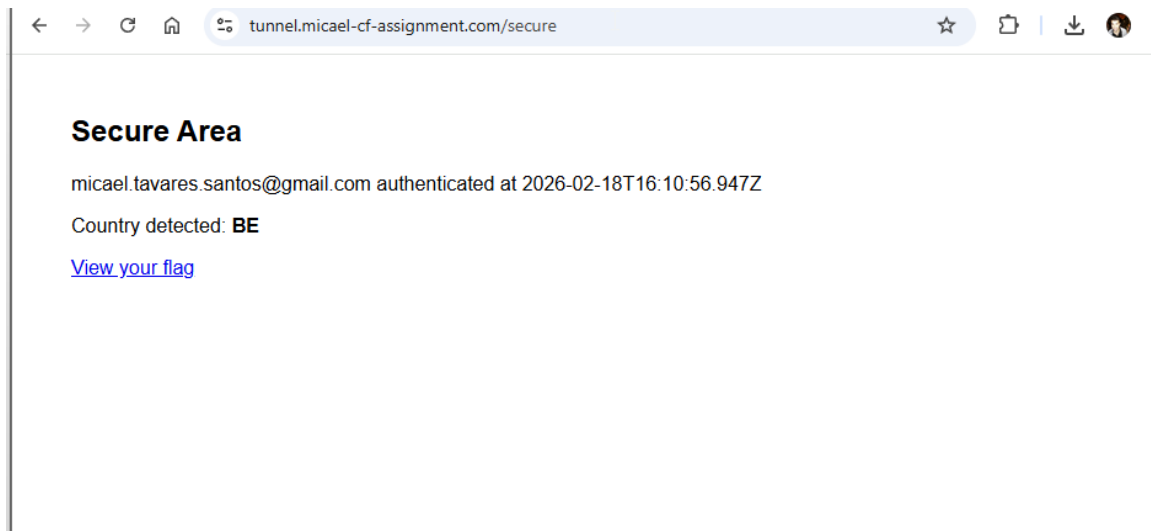


Fig. 25 Secure page working

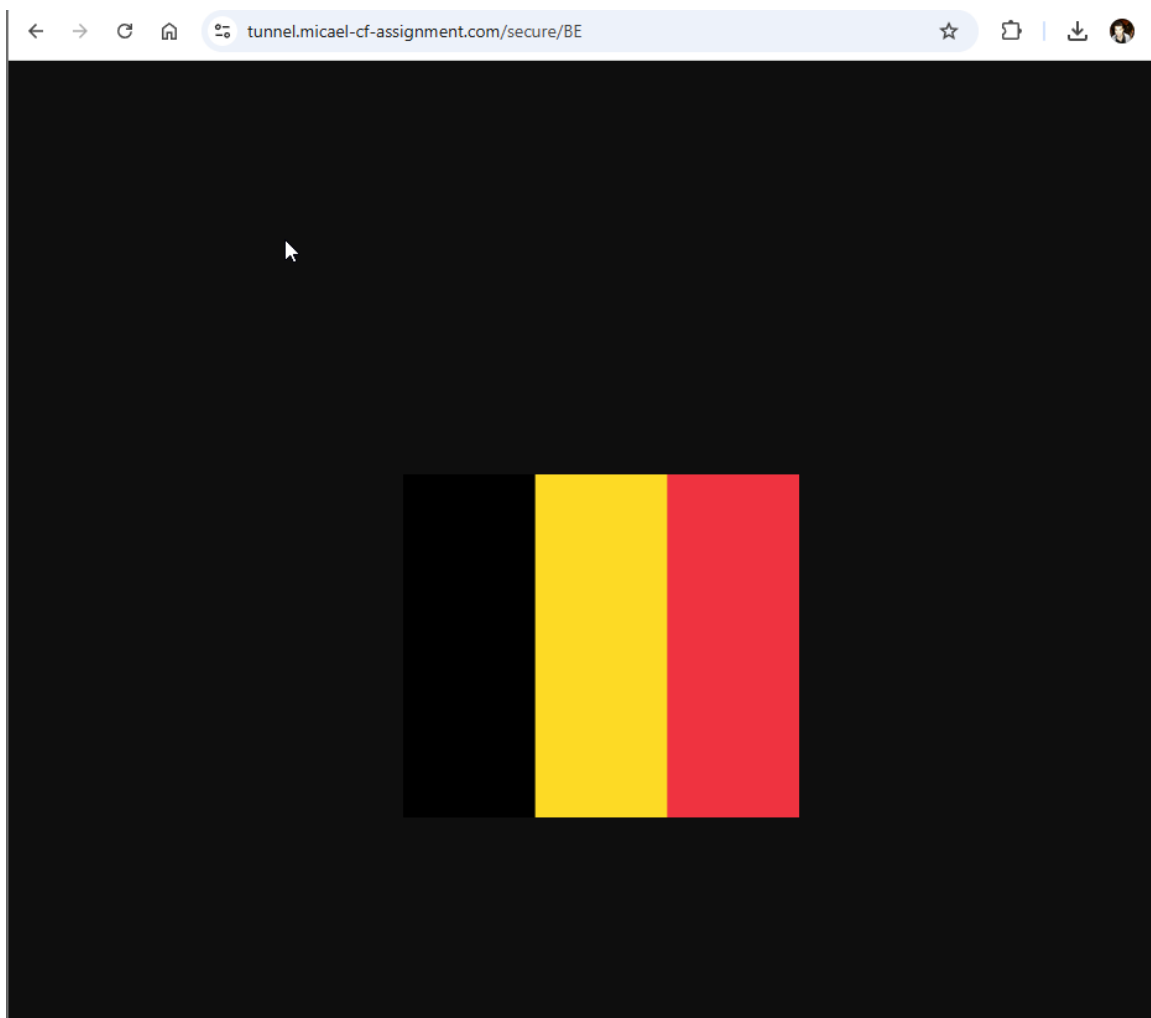


Fig. 26 Flag displayed

5. Security Controls Implemented

The following security controls were implemented:

- TLS encryption end-to-end
- Full Strict certificate validation
- Cloudflare Tunnel to eliminate exposed ports
- Zero Trust authentication policies
- Identity-based access control
- Private object storage with R2
- Reverse proxy isolation
- Origin firewall restrictions

6. Use Cases

The implemented architecture is relevant for multiple enterprise scenarios:

- Secure remote access to internal applications
- Zero Trust replacement for VPN access
- Protection of legacy applications without modification
- Identity-aware content delivery
- Secure asset delivery using object storage
- Dev/Test environment exposure without public IP risks

7. Knowledge Gaps and Research

During the implementation process, several knowledge gaps were identified and addressed through research and experimentation.

Examples include:

- Cloudflare Tunnel configuration and troubleshooting
- Systemd service configuration for persistent application execution
- Cloudflare Zero Trust Access policy behaviour
- Worker and R2 integration
- SSL Full Strict troubleshooting

Primary research sources included:

- Official Cloudflare documentation
- Community technical resources
- Hands-on testing and validation
- AI-assisted guidance for development efficiency

AI tools were used specifically to accelerate:

- Code generation (Flask and Worker examples)
- Troubleshooting ideas
- Documentation structure guidance

All configurations were validated manually to ensure correctness.

8. Customer Experience Perspective

From a customer perspective, the experience would be highly positive.

Cloudflare provides a unified platform to secure applications without requiring significant infrastructure changes.

The ability to deploy Zero Trust controls, secure tunnels and edge compute capabilities rapidly demonstrates strong value, particularly for organizations seeking to modernize legacy environments or reduce VPN dependency.

The learning curve is moderate, but documentation quality and platform integration significantly reduce operational complexity.

9. Conclusion

This project successfully demonstrates the deployment of a secure application architecture using Cloudflare Application Services.

The implementation shows practical understanding of Cloudflare's core capabilities including secure connectivity, identity-based access control and edge computing.

The architecture is scalable, secure and aligned with modern Zero Trust principles.

10. Appendix (GitHub + URLs)

Public Application:

<https://tunnel.micael-cf-assignment.com>

Secure Application:

<https://tunnel.micael-cf-assignment.com/secure>

GitHub Repository:

<https://github.com/MicaelTavaresSantos/cloudflare-assignment-Micael.git>