

Sprawozdanie L3: Projekt architektury infrastruktury aplikacji - środowisko cloud

1. Informacje ogólne

Projekt: Forum Dyskusyjne

Zespół: Tomek Trefler, Wojciech Borodziuk, Kogut, Wiktor Barabach

Data: 20.11.2025

Etap: L3 - Projekt architektury infrastruktury w środowisku Cloud Publicznego

2. Cel projektu architektury

Zaprojektowanie skalowalnej, bezpiecznej i wysoko dostępnej infrastruktury cloudowej dla aplikacji forum dyskusyjnego, spełniającej wymagania:

- Load balancing z możliwością skalowania
- Skalowalna baza danych
- Własna domena publiczna z certyfikatem SSL/TLS
- Certyfikat SSL/TLS (nie na serwerze aplikacyjnym)

3. Wybór dostawcy Cloud

AWS + Cloudflare

- **AWS** - hosting aplikacji (EC2, RDS) w Free Tier (12 miesięcy)
- **Cloudflare** - WAF, CDN, SSL, DDoS protection (darmowe permanentnie)

Podział odpowiedzialności:

None

Cloudflare (warstwa zewnętrzna):

- DNS Management
- SSL/TLS Certificate (Let's Encrypt)
- WAF (Web Application Firewall)
- DDoS Protection
- CDN (Content Delivery Network)
- Rate Limiting

AWS (warstwa aplikacji):

- └─ Application Load Balancer
- └─ Auto Scaling Group (EC2)
- └─ RDS PostgreSQL
- └─ CloudWatch (monitoring)
- └─ S3 (storage)

4. Architektura sieciowa (VPC)

4.1 Podział na subnety

Typ	Przeznaczenie	Zawartość
Public Subnets	Dostęp do internetu	ALB
Private Subnets	Backend, aplikacja	EC2 Instances
	Izolowana baza danych	RDS PostgreSQL

4.2 Routing

- Public subnets → Internet Gateway
- Private subnets → NAT Gateway (dla aktualizacji EC2)
- Baza danych → brak routingu do Internetu (tylko lokalny VPC traffic)

5. Architektura aplikacyjna

5.1 Cloudflare → AWS

1. Użytkownik → Cloudflare (HTTPS terminowany na Cloudflare)
2. Cloudflare (proxy) → ALB (HTTPS lub HTTP)
3. ALB przekazuje ruch do target group (EC2 private)

5.2 EC2 Instances

2 × t2.micro w Auto Scaling Group

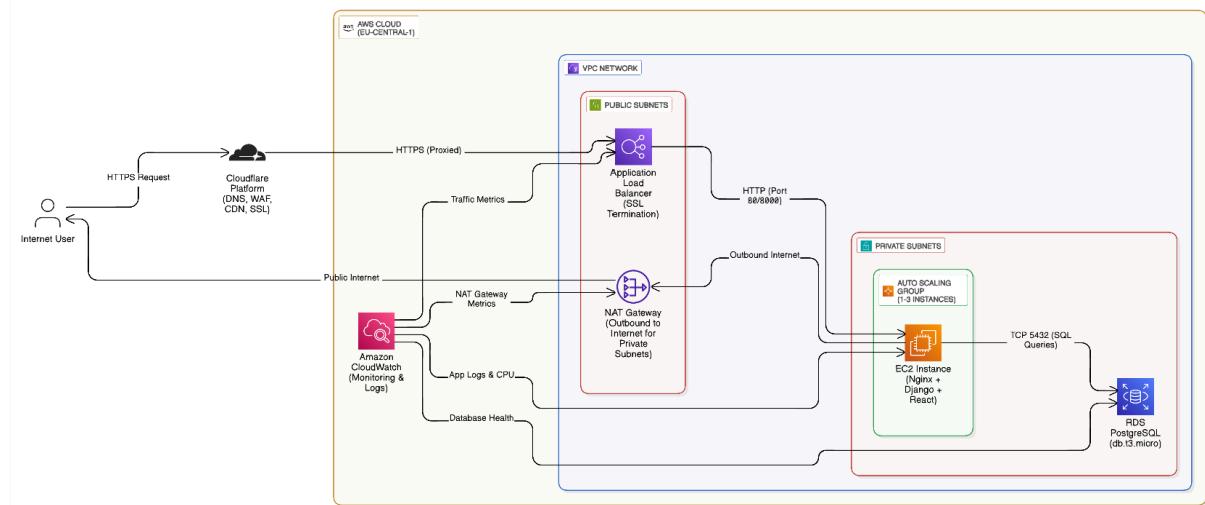
Na każdej instancji:

- **Nginx** (reverse proxy) → port 80
- **Django backend** → port 8000
- **React build** → statyczne pliki serwowane z Nginx
- Security Groups:
 - pozwalają tylko na połączenia z ALB

5.3 RDS PostgreSQL

- 1 instancja
- Private subnet
- SG pozwala tylko na ruch z EC2 (port 5432)
- Brak publicznego adresu IP

6. Diagram architektury



7. Bezpieczeństwo

- WAF + DDoS na poziomie Cloudflare
- Brak publicznych adresów IP dla EC2 i RDS
- SG blokują całkowicie ruch z internetu
- SSL/TLS terminowany:
 - Cloudflare → ALB (Full)
 - Możliwe HTTPS end-to-end (certyfikat ACM na ALB)

8. Monitoring & Logging

- CloudWatch Logs: Django, Nginx, ASG
- CloudWatch Alarms: CPU, status checks, RDS storage

9. Skalowalność

- Auto Scaling Group (min 2, max 4)
- Horizontal scaling backendu
- RDS umożliwia read replicas (opcjonalnie)

