# Dokumentacja Projektowa

## Architektura Bezpieczeństwa Systemu Obsługi Klienta

Zespół Architektury Bezpieczeństwa

31 stycznia 2026

---

# 1 Wstęp

Niniejszy dokument przedstawia szczegółowy opis zaprojektowanej architektury bezpieczeństwa dla nowoczesnego systemu obsługi klientów indywidualnych firmy. Projekt realizuje podejście **Defense in Depth** (obrona w głębokości) oraz zasady **Zero Trust Network Access** (ZTNA), zapewniając ochronę danych wrażliwych oraz wysoką dostępność usług.

# 2 Założenia projektowe

## 2.1 Charakterystyka systemu

System obsługi klientów integruje następujące kluczowe interfejsy i kanały dostępu:

- **Self-care**: Dostęp webowy oraz mobilny dla klientów końcowych.
- **Customer-care**: Portal wewnętrzny dla pracowników biurowych.
- **POS (Point of Sales)**: Fizyczne punkty sprzedaży połączone przez Internet publiczny.

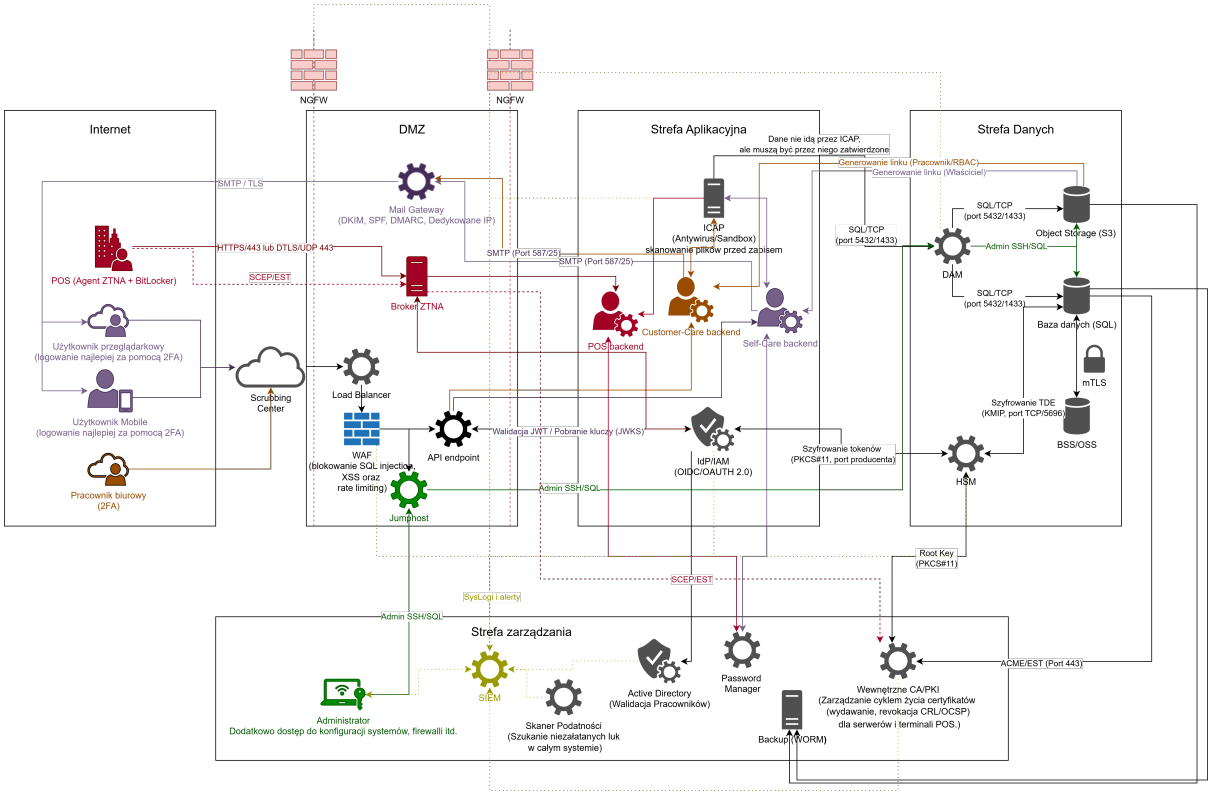
## 2.2 Opis zaprojektowanej architektury

Poniżej przedstawiono strukturę logiczną systemu z podziałem na strefy izolacji.

### 2.2.1 Główne komponenty i strefy sieciowe

Zaprojektowana architektura opiera się na ścisłej segmentacji sieciowej w celu minimalizacji powierzchni ataku. Wyróżniono następujące strefy:

- **Strefa Internet (Untrusted)**: Zawiera użytkowników końcowych oraz punkty POS. Ruch wchodzący jest filtrowany przez **Scrubbing Center** (np. CloudFlare) w celu mitygacji ataków wolumetrycznych (DDoS) jeszcze przed dotarciem do infrastruktury firmy.
- **DMZ (Demilitarized Zone)**: Strefa buforowa dostępu z Internetu.
  - **NGFW**: Zapewniają aktywne wykrywanie ataków.
  - **WAF**: Chroni przed atakami warstwy 7 (SQL Injection, XSS) oraz realizuje Rate Limiting.




Rysunek 1: Referencyjny schemat segmentacji sieciowej i mechanizmów kontrolnych.

- **Broker ZTNA**: Służy do bezpiecznego zestawiania tuneli z punktami POS. Komunikuje się z IdP/IAM w celu uwierzytelniania użytkownika kluczami trzymanymi w HSM.
- **Mail Gateway**: Obsługuje ruch pocztowy z zabezpieczeniami DKIM, SPF i DMARC; służy do wysyłania faktur.
- **Jumphost**: Służy do bezpiecznego dostępu administracyjnego (SSH/SQL).
- **API Gateway/Endpoint**: Centralny punkt wejścia dla zapytań API, realizujący wstępne uwierzytelnienie systemem IdP/IAM oraz walidację schematu.

- **Strefa Aplikacyjna**: Tutaj przetwarzana jest logika biznesowa. Ruch trafia tu wyłącznie po wcześniejszej weryfikacji w DMZ.
  - **Backend**: Obsługuje usługi POS, Self-Care oraz Customer-Care.
  - **Serwer ICAP**: Realizuje skanowanie antywirusowe i sandboxing plików przesyłanych przez użytkowników przed ich zapisaniem do bazy danych.
  - **IdP/IAM**: Centralny system tożsamości obsługujący protokoły OIDC/OAuth 2.0.
- **Strefa Danych**: Najbardziej strzeżony segment sieci.
  - **Bazy SQL i Object Storage (S3)**: Przechowywanie danych z szyfrowaniem TDE.
  - **Systemy BSS/OSS**: Komunikują się przez mTLS.
  - **HSM (Hardware Security Module)**: Bezpieczne przechowywanie kluczy kryptograficznych (POS, Root Key CA, TDE).
  - **DAM (Database Access Monitoring)**: Kontrola i audyt dostępu do baz danych w czasie rzeczywistym.
- **Strefa Zarządzania**: Odseparowana sieć dla administratorów i narzędzi bezpieczeństwa.
  - **Password Manager**: Centralny sejf haseł i zarządzania sesjami uprzywilejowanymi.

- **Backup WORM**: System Write Once, Read Many, chroniący kopie przed ransomware.
- **SIEM**: Zbieranie logów i alertów ze wszystkich systemów.
- **Skanery podatności**: Automatyczne wykrywanie luk i najnowszych CVE.
- **Active Directory**: Uwierzytelnianie pracowników biurowych.
- **Wewnętrzne CA/PKI**: Zarządzanie cyklem życia certyfikatów z możliwością rewokacji (CRL/OCSP).

## 3 Zastosowane mechanizmy bezpieczeństwa

W projekcie wykorzystano podejście **Defense in Depth** (obrona w głębokości):

- **Ochrona Brzegowa**: Scrubbing Center przeciwko DDoS oraz klastry firewalli NGFW do filtracji ruchu L3/L4.
- **Bezpieczeństwo Aplikacji Web (WAF)**: Blokowanie ataków z listy OWASP Top 10 oraz walidacja tokenów JWT na poziomie API Endpoint.
- **Zero Trust Network Access (ZTNA)**: Agent ZTNA na stacji POS (zabezpieczonej BitLockerem) zapewnia dostęp tylko do konkretnych aplikacji.
- **Inspekcja Treści (ICAP)**: Przesyłanie plików do skanera AV/Sandbox przed ich utrwaleniem.
- **Ochrona Danych (Data Protection)**: Szyfrowanie baz danych (TDE) kluczami KMIP w zewnętrznym HSM oraz wymuszone TLS/mTLS.

## 4 Bezpieczeństwo procesu wytwórczego (DevSecOps)

Integralną częścią systemu jest bezpieczny potok dostarczania oprogramowania (CI/CD Pipeline) realizujący podejście **Shift-Left Security**:

- **SAST**: Statyczna analiza kodu źródłowego na etapie commitowania do repozytorium.
- **DAST**: Automatyczne testy penetracyjne uruchamiane na środowiskach testowych.
- **Skanowanie Obrazów (Container Security)**: Kontrola obrazów pod kątem znanych podatności (CVE) przed trafieniem do rejestru.
- **Podpisywanie Artefaktów**: Weryfikacja cyfrowego podpisu kontenerów przed uruchomieniem w Strefie Aplikacyjnej.