Server Hardening & Cloudflare Documentation

Security Notice

This document describes architecture and defensive principles only. Secrets, credentials, internal IP addresses, and sensitive operational procedures are intentionally omitted.

Detta dokument beskriver steg-för-steg hur servern har hårdnats (hardening) och skyddats bakom Cloudflare med flera säkerhetslager. Dokumentet är avsett som teknisk referens och emergency-dokumentation.

1. Grundläggande mål

1. All publik HTTP/HTTPS-trafik ska endast nå servern via Cloudflare.
2. Origin-servern ska inte vara direkt nåbar från internet.
3. Admin-ytor ska vara strikt begränsade och isolerade.

2. Cloudflare & DNS

Domäner och subdomäner hanteras via Cloudflare med proxy aktiverad. DNS används både för trafikstyrning och som första säkerhetslager.

3. Firewall & Network Layer

Origin-servern skyddas med UFW och ipset. Endast Cloudflare IP-intervall tillåts nå port 80/443. All övrig trafik blockeras.

4. Application & Access Control

1. Admin-tjänster körs på separata subdomäner.
2. HTTPS-only med säkerhetsheaders.
3. Cloudflare Access och ytterligare autentisering används.

5. Slutlig säkerhetsmodell

Internet → Cloudflare → Firewall/ipset → Webserver → Access Control → Applikation.