

SAP-ERP Portal — Internet Access Setup Guide

Exposing the portal to remote users outside the office network — domain registration, Cloudflare, and two connection methods (Tunnel vs. classic port forwarding), plus the security hardening that goes with either.

This portal handles SAP logins, GST/financial reports and salary data. Putting it on the public internet is meaningfully higher risk than the internal-only LAN setup (see the companion *ERP-DNS-HTTPS-Setup-Guide*). Read the Security Hardening section (Part D) as seriously as the setup steps themselves — it is not optional once this is live.

What this adds

Component	Value / Notes
Public domain	A newly registered domain (e.g. mitraindustries-erp.com) — separate from the internal-only mipl.com AD zone
DNS + edge proxy	Cloudflare (free plan) — DNS hosting, automatic edge HTTPS, hides origin IP, basic DDoS/bot protection
Application server	10.9.11.210 — same server as the internal setup (Apache/XAMPP reverse proxy in front of the Node app on port 5000)
Connection method	Either a Cloudflare Tunnel (recommended, no exposed ports) or classic router port forwarding

Part A — Domain + Cloudflare

A1. Register a domain

Buy a domain from any registrar (GoDaddy, BigRock, Namecheap, etc.) — e.g. `mitraindustries-erp.com`. This is separate from the internal-only `mip1.com` zone on your AD DNS server; that one stays exactly as it is for LAN use.

A2. Put the domain on Cloudflare (free plan)

- 1 Sign up at cloudflare.com, click **Add a site**, enter the new domain.
- 2 Cloudflare shows two nameservers — go to the registrar's control panel and change the domain's nameservers to those.
- 3 Propagation typically takes minutes to a few hours. Cloudflare's dashboard shows "Active" once it's done.

This gets you free DNS management, automatic HTTPS at Cloudflare's edge, and baseline DDoS/bot filtering — all before the request ever reaches your server.

Part B — Recommended: Cloudflare Tunnel (no open ports)

A Cloudflare Tunnel makes an **outbound-only** connection from 10.9.11.210 to Cloudflare. Nothing listens on your public IP at all — no port forwarding, no firewall exposure, and your router configuration doesn't change. This is the safer way to achieve the same goal as port forwarding.

B1. Install cloudflared

On 10.9.11.210, download `cloudflared` for Windows from Cloudflare's site and install it.

B2. Authenticate and create the tunnel

```
cloudflared tunnel login
cloudflared tunnel create erp-tunnel
```

The login command opens a browser to authorize the tunnel against your Cloudflare account and domain.

B3. Point the tunnel at the app

Create `C:\Users\<you>\.cloudflared\config.yml`:

```
tunnel: erp-tunnel
credentials-file: C:\Users\<you>\.cloudflared\<tunnel-id>.json

ingress:
  - hostname: erp.mitraindustries-erp.com
    service: http://localhost:5000
  - service: http_status:404
```

This points straight at the Node app on port 5000, bypassing Apache entirely for this route (fine, since Cloudflare itself now handles the public HTTPS). Point it at `http://localhost:80` instead if you'd rather route it through the existing Apache reverse proxy alongside your internal vhosts.

B4. Route DNS to the tunnel and run it as a service

```
cloudflared tunnel route dns erp-tunnel erp.mitraindustries-erp.com
cloudflared service install
```

The service ensures the tunnel reconnects automatically on reboot. Test `https://erp.mitraindustries-erp.com` from any internet connection — Cloudflare issues and renews the public certificate automatically; nothing to manage on your end.

Part C — Alternative: Classic Port Forwarding

If a tunnel isn't an option, this achieves the same public access by opening ports on the router. It carries more exposure than Part B (your public IP becomes directly reachable), so the Cloudflare proxy step below is not optional here.

C1. Forward ports on the router

Forward external TCP **80** and **443** to 10.9.11.210:80 and :443. Menu location varies by router/firewall model (usually under "Port Forwarding", "NAT", or "Virtual Server").

Never forward anything beyond 80/443 for this purpose — in particular, RDP (3389) and SQL Server (1433) must never be exposed to the internet.

C2. Add the public DNS record on Cloudflare, proxied

- 1 Cloudflare dashboard → DNS → Add record: Type A, Name erp, Content = your office's static public IP.
- 2 Make sure the proxy status is the orange cloud (**Proxied**), not grey (DNS only) — this is what hides your real IP and adds Cloudflare's protection even with plain port forwarding.

C3. Get a certificate for the Apache origin

Set Cloudflare's SSL/TLS mode to **Full (strict)** — this requires Apache itself to also present a valid certificate (not the internal-only CA cert from the LAN setup, which the public internet won't trust). Cloudflare issues a free long-lived Origin Certificate for exactly this purpose, trusted by Cloudflare's edge only:

- 1 Cloudflare dashboard → SSL/TLS → Origin Server → **Create Certificate** (defaults are fine; 15-year validity is typical).
- 2 Save the two outputs as cf-origin.crt and cf-origin.key into D:\apps\xampp74\apache\conf\ssl\ on 10.9.11.210.

C4. Add a dedicated vhost for the public hostname

This is a **separate** vhost block from the internal wildcard.mipl.com one — different hostname, different certificate, same port 443 (Apache distinguishes them by ServerName via SNI). Leave the internal blocks untouched.

```
<VirtualHost *:443>
    ServerName erp.mitraindustries-erp.com
    SSLEngine on
    SSLCertificateFile "D:/apps/xampp74/apache/conf/ssl/cf-origin.crt"
    SSLCertificateKeyFile "D:/apps/xampp74/apache/conf/ssl/cf-origin.key"

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:5000/
    ProxyPassReverse / http://127.0.0.1:5000/
</VirtualHost>
```

Restart Apache (check httpd.exe -t first) and test https://erp.mitraindustries-erp.com.

Part D — Security Hardening (do this regardless of method)

Once this hostname resolves, it is reachable by anyone on the internet, not just office/VPN users. Treat these as required, not optional:

- **Never** forward or tunnel anything beyond 80/443 to this server — RDP, SQL Server, file shares, etc. must stay LAN-only, always.
- Keep Cloudflare's proxy (orange cloud) switched on for the public record — it absorbs scanning/DDoS traffic before it reaches your server.
- Add a **Rate Limiting** rule (Cloudflare free tier) on the login endpoint to blunt password brute-forcing.
- Consider **Cloudflare Access** (free tier) in front of the whole app — an email one-time-PIN gate before anyone even reaches the login page, if only a known set of remote staff need access.
- Enforce strong, unique passwords for every portal account, especially ones with SAP posting rights or Finance/Salary module access.
- Review Apache access/error logs periodically once this is live — unexpected request patterns are the first sign of scanning or attempted abuse.
- Keep the internal-only LAN setup (companion guide) as the default for on-site staff — only route remote users through this public path.

Companion document: ERP-DNS-HTTPS-Setup-Guide.pdf (internal LAN-only DNS, reverse proxy and internal-CA HTTPS setup). Prepared as an internal setup reference for the SAP-ERP portal.