Post Install ACME Falining Fix

This guide walks you through the exact steps to diagnose and fix ACME certificate issues during a Pangolin installation. These steps cover the most common real-world causes: DNS mismatches, blocked ports, Traefik misconfiguration, and redirect loops. Follow the checklist in order—each step rules out a specific failure point so you can quickly identify what’s wrong and get ACME issuing certificates again.

Troubleshoot Steps

Verify DNS is pointing to the correct server

ACME will always fail if DNS points to the wrong IP.

- `A yourdomain.com → <your VPS IP>`
- `A *.yourdomain.com → <your VPS IP>`

1. Check your server’s public IP and make sure it matches your DNS records

```
curl ifconfig.me
```

Test port 80 from outside the server

ACME HTTP-01 requires port 80 to be reachable publicly.

1. From your laptop or phone:

```
curl -I http://yourdomain.com
```

Interpret the result:

- **200 / 301 / 404** → Port 80 is open (good)
- **Timeout** → Firewall or provider is blocking port 80
- **Connection refused** → Traefik is not listening on port 80

Check VPS firewall (UFW)

```
sudo ufw status
```

You should see

```
80/tcp   ALLOW
443/tcp  ALLOW
```

If missing:

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

Check hosting provider firewall

For example Hetzner has an external firewall that overrides UFW

1. Go to your VPS dashboard
2. Server → Networking → Firewalls

```
TCP 80
TCP 443
```

If port 80 is missing → ACME will fail every time.

Confirm Traefik is listening on port 80

1. SSH into server and run following command

```
sudo ss -tulpn | grep :80
```

Expected:

```
docker-proxy ... LISTEN ... :80
```

If nothing is listening → Traefik didn’t bind to port 80.

Disable HTTP→HTTPS redirect during ACME

This is the most common Traefik issue.

If Traefik redirects ACME requests to HTTPS before a certificate exists, ACME fails.

1. SSH into the server, and go to dynamic-compose.yaml. Usually in config > traefik folder

```
main-app-router-redirect:
  entryPoints:
    - web
  middlewares:
    - redirect-to-https
```

2. Temporarily comment out the redirect:

```
# - redirect-to-https
```

3. Restart Traefik:

```
sudo docker compose restart traefik
```

Uncomment the redirect after successful redirect

Ensure ACME is using HTTP-01 on the correct entrypoint

In traefik onfig yaml

```
httpChallenge:
  entryPoint: web
```

Entrypoints must be:

```
entryPoints:
  web:
    address: ":80"
  websecure:
    address: ":443"
```

Revision #2
Created 2026-03-04 16:58:48 UTC by lumxux
Updated 2026-03-04 18:22:26 UTC by lumxux