Homelab Certificate Management

HLB - August 2025

21 August 2025

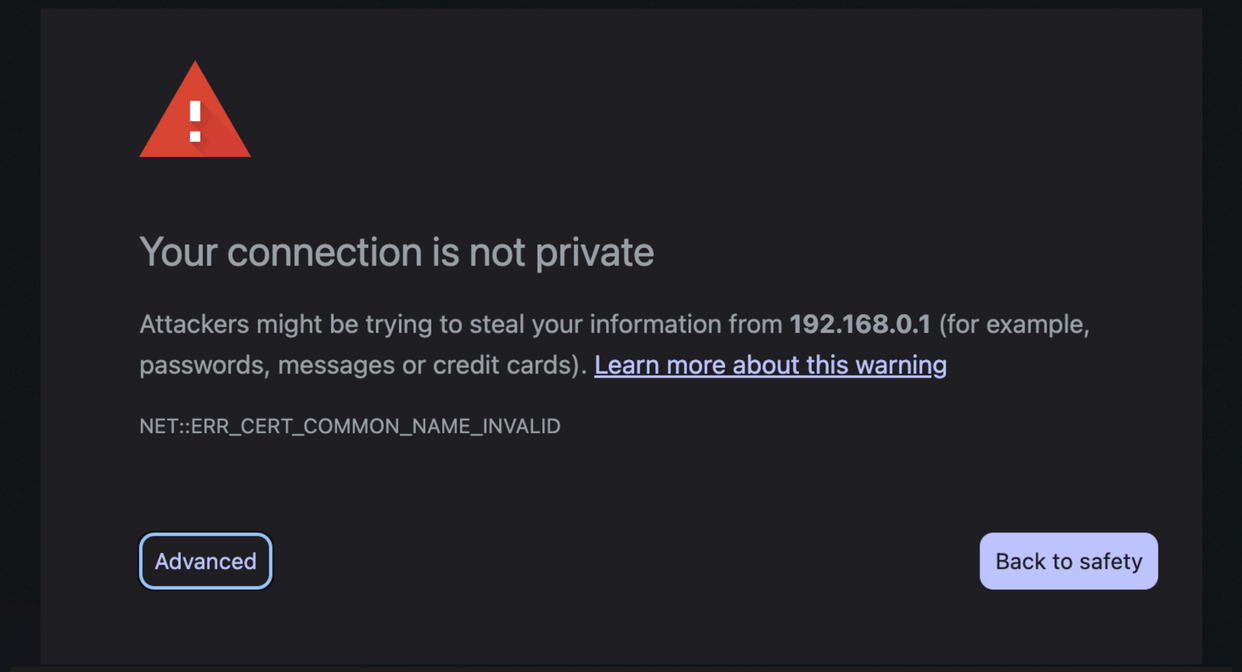
Overview

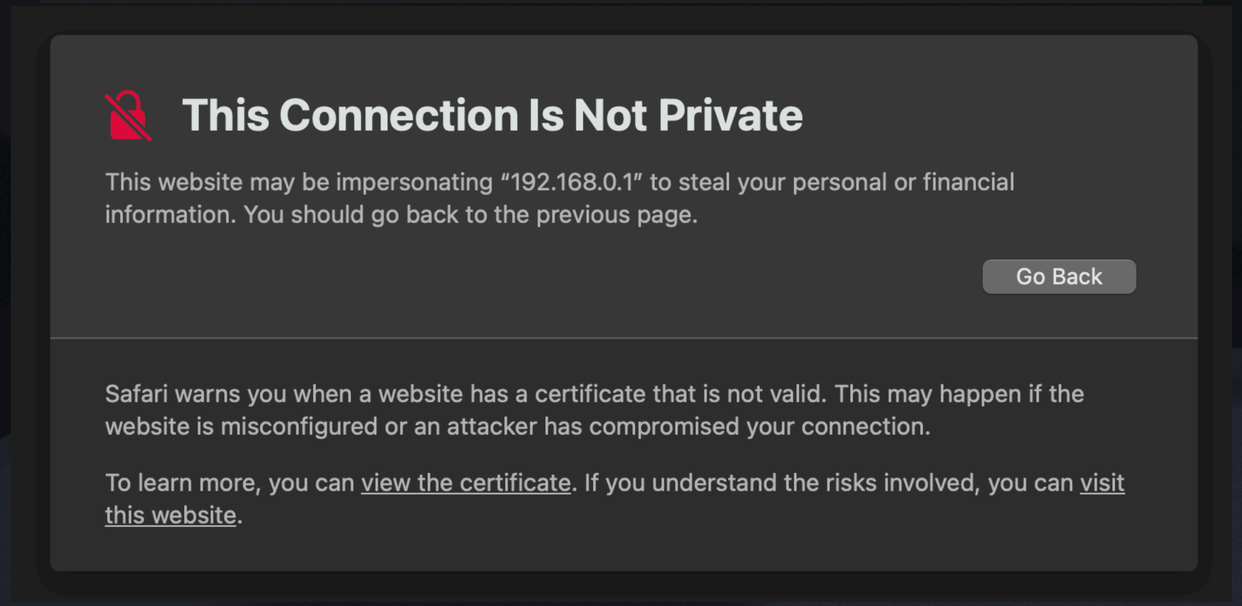
- Specifically discussing SSL/TLS certificates (e.g., code signing, S/MIME out of scope)
- Why issue certificates?
- Options for obtaining SSL/TLS certificates
- Certificate Transparency

Why?

Solely to eliminate Self-Signed certificate warnings

Self-signed certificates are still encrypted, just not validated by a third-party

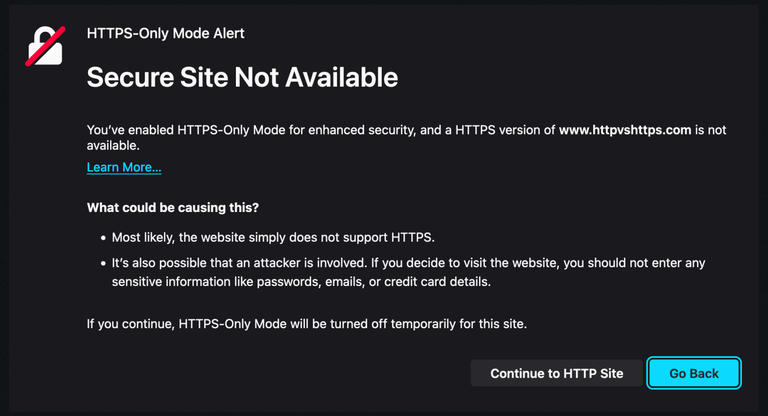


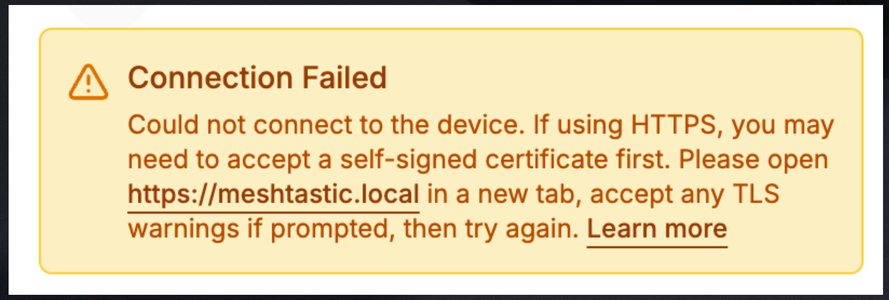


Certificates in the Homelab

Why?

- Anything public facing *needs* HTTPS now
- Life is becoming harder without HTTPS
  Homelab topics from the Discourse (e.g., n8n, Meshtastic, all beginning to mandate HTTPS or head in that direction)
- Human Factors implication of conditioning local users to “just click past that security warning”





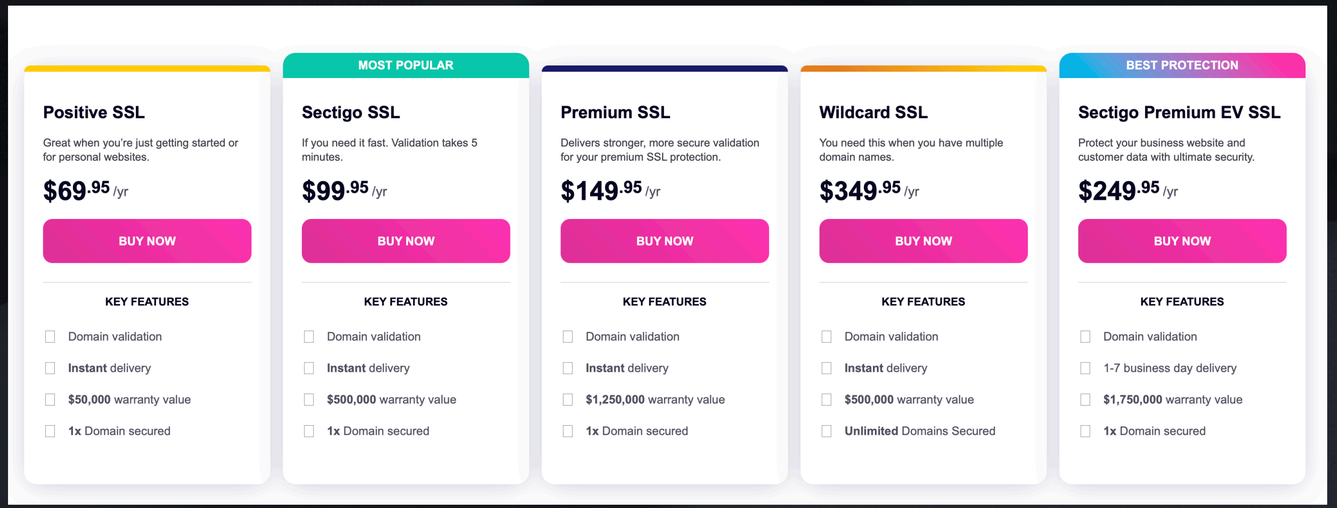
Homelab Certificates

Options

- Self-signed (including operating your own Certificate Authority; CA)
- Buy a cert
- Cloudflare
- Automatic Certificate Management Environment (ACME) based options (e.g., Caddy, acme.sh, Traefik, Nginx Proxy Manager)
- Wildcards versus individual subdomain certs

Spend Some $$$?

- The “established” way - Generate a Certificate Signing Request (CSR) and send it to a Certificate Authority
- Gets expensive quickly if multiple domains are involved (or using wildcard certificates)
- Domain Validation is sufficient for Homelab use - why pay for what you can get for free?



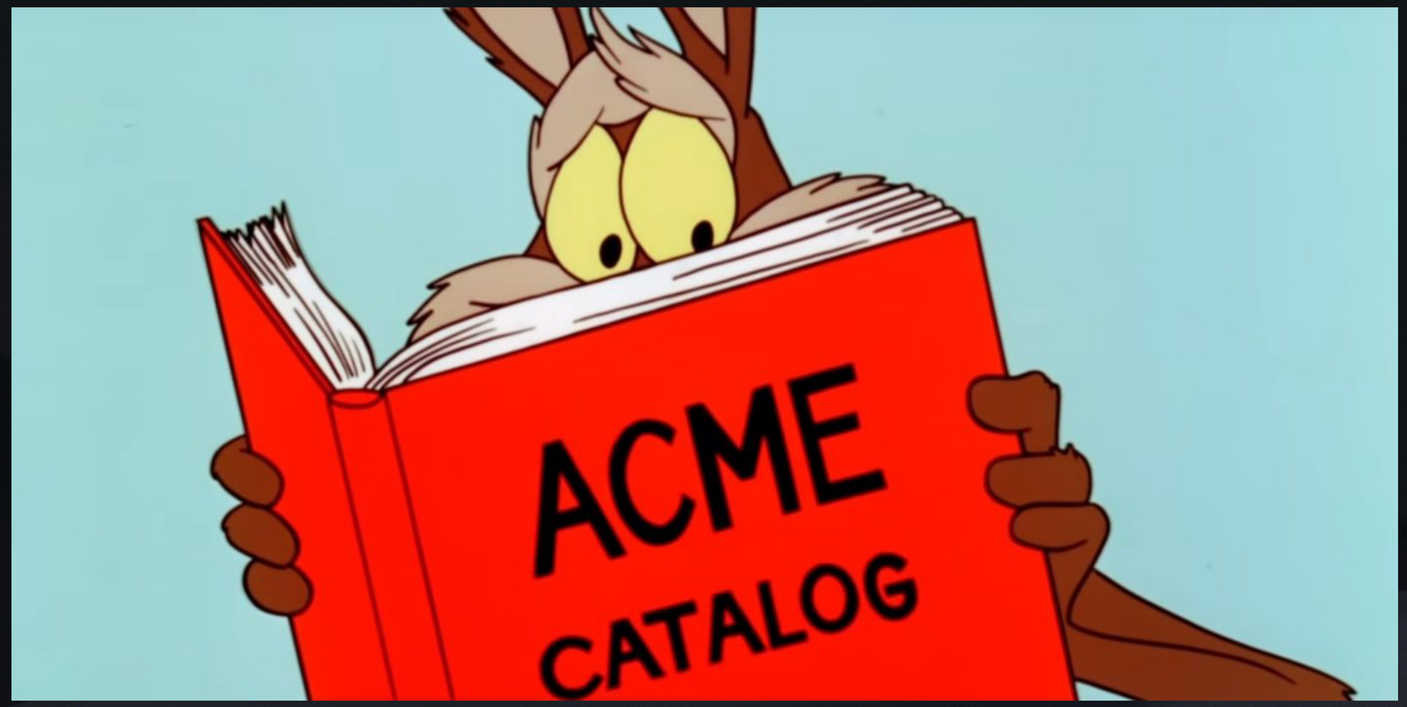
	MOST POPULAR			BEST PROTECTION
Positive SSL	**Sectigo SSL**	**Premium SSL**	**Wildcard SSL**	**Sectigo Premium EV SSL**
Great when you're just getting started or for personal websites.	If you need it fast. Validation takes 5 minutes.	Delivers stronger, more secure validation for your premium SSL protection.	You need this when you have multiple domain names.	Protect your business website and customer data with ultimate security.
$69.95 /yr	**$99.95** /yr	**$149.95** /yr	**$349.95** /yr	**$249.95** /yr
BUY NOW	BUY NOW	BUY NOW	BUY NOW	BUY NOW
KEY FEATURES	KEY FEATURES	KEY FEATURES	KEY FEATURES	KEY FEATURES
Domain validation	Domain validation	Domain validation	Domain validation	Domain validation
Instant delivery	**Instant** delivery	**Instant** delivery	**Instant** delivery	1-7 business day delivery
$50,000 warranty value	**$500,000** warranty value	**$1,250,000** warranty value	**$500,000** warranty value	**$1,750,000** warranty value
1x Domain secured	**1x** Domain secured	**1x** Domain secured	**Unlimited** Domains Secured	**1x** Domain secured

Cloudflare

- Free Universal SSL (shared) Certificate
- Domain must be hosted at Cloudflare
- Cloudflare handle the renewals
- Cloudflare choose the CA(s)
- Wildcard and single level subdomain only
  (e.g., *.domain.tld, aaa.domain.tld, bbb.domain.tld, but not ccc.ddd.domain.tld)
- Service must be proxied by Cloudflare (e.g., HTTP/HTTPS, public facing services only)
  Your service may still be accessible directly - configure your firewall

ACME Based Options

- Clients include
  - Caddy
  - acme.sh
  - Traefik
  - Nginx Proxy Manager
  - cert-manager (Kubernetes)
  - Most web hosting providers “Free SSL” will use some variation of ACME under the hood
- Free providers include
  - Let’s Encrypt
  - ZeroSSL
  - BuyPass



ACME

- Options will vary per client
- Can issue certs on domains and wildcards
- DNS and HTTP/HTTPS challenges (to prove domain ownership)
- Some clients allow you to pick your desired CA
- Some clients allow you to pick validity period
  Be aware: all certificates will have max 47-day validity by 2028

Caddy

- Self-hosted, cross platform, several plugins available
- ACME and self-signed certificate support (e.g., can run your own CA)
- Choose your CA (Let’s Encrypt, ZeroSSL, BuyPass, etc.)
- Automatic renewal and flexible renewal times
- HTTP/HTTPS challenge easy, custom builds needed for DNS challenges and wildcards
- Configurable via API, command line, and “Caddyfile”
- Can serve websites itself, or act as a reverse proxy for other services
  Reverse proxy: your service may still be accessible directly/via HTTP only

acme.sh

- Shell script implementation of ACME
- Used in other software (e.g., Proxmox)
- Most flexible ACME client (in my opinion!)
- Easy to issue wildcard certificates or certificates with multiple common names
  Example: **acme.sh --issue --dns -d example.com -d www.example.com -d *.**example.com
- Outputs .cer files to use however you please, or integrates with other software (e.g., Nginx Apache)
- Can automatically renew certificates, etc. using cron

Certificate Transparency

- Certificates issued by CAs are entered into public CT logs
- Certificate Transparency logs are immutable records of a certificate being issued
- Most browsers now require certificates to be in CT logs for the cert to be considered valid (e.g., Chromium/Firefox/Safari) - checked by embedded Signed Certificate Timestamp (SCT)

Certificate Transparency - So what?

- Can be used to assess which certificates are valid, expired, revoked
- Can be used to monitor rogue certificate issuance by otherwise “trusted” CAs due to technical issues, compromise, or poor governance (e.g., formerly trusted CAs Thawte, StartCom, Symantec)
- Can inadvertently and permanently release information into the public domain

Certificate Transparency Monitoring

- Individual subdomain certificates
  - May be easier to work with
  - May limit impact if a certificate is compromised
  - Hostnames permanently recorded in CT logs (via Common Name)

VS

- Wildcard domain certificates
  - One certificate to cover everything
  - No hostnames embedded in CT logs
  - If that certificate gets compromised *everything* using that certificate will need a new one

CT Homelab Considerations

- Certificate Common Name (i.e., DNS name) may or may not reveal more about your network than you’re willing to share
- Wildcard certificates used on everything may have a large “blast radius” if the certificate is compromised
- Automate, automate, automate. Max certificate validity is currently 398 days, gradually reducing to 47 days over the coming years. Typical validity is currently 90 days - that WILL reduce.

Conclusion

- ACME Clients make issuing certificates in the homelab easy and free
- Consider your needs, e.g.
  - DNS vs. HTTP/HTTPS validation
  - Wildcards vs. individual subdomains
  - Ease of use required flexibility