Point a domain at your VPS and enable HTTPS

You need a domain you control, DNS access and a website already configured on your VPS. A DNS record directs visitors to an address; it does not install a web server or create the website. This guide covers a normal public website, with SSH kept separate from web traffic.

Check the VPS and website first

1. Open the VPS panel and confirm the assigned public IP under **Overview → Network**.
2. Confirm that your intended web server runs and listens on the required ports. Configure its site or virtual host for your domain before issuing a certificate.
3. Permit the website's HTTP/HTTPS traffic through both the guest firewall and any applicable panel rules. Keep SSH access working while you change rules.
4. If your web server selects sites by hostname, test the configured hostname against the server before changing public DNS. A default page at the raw IP does not prove the intended site works.

Create the DNS records

At your DNS provider, create an **A** record for the name you want to use. For example, `www.example.com` can point to `192.0.2.10`. Replace that documentation address with your assigned VPS IP. Enter no port, path or `https://` in the address field.

Configure the root domain as well if you want visitors to use it. DNS providers may call that name `@` or leave it blank. A `www` CNAME can point to the root hostname when appropriate. Preserve existing mail and verification records.

Add an **AAAA** record only when your VPS has a working assigned IPv6 address and your website and firewall support it. An old AAAA record can send some visitors and certificate checks to the wrong machine even when the A record is correct.

Keep web and SSH hostnames separate

If you use Cloudflare, a website hostname can use its HTTP proxy once the origin configuration works. A hostname used for ordinary SSH should use **DNS only**; the standard website proxy does not carry SSH connections. Consider a separate DNS-only name such as `ssh.example.com`, understanding that its DNS record exposes the origin IP.

Verify your address record with `nslookup www.example.com`. When a website hostname uses Cloudflare's proxy, results show Cloudflare addresses rather than your VPS. For diagnosis, check the record value in your DNS dashboard. Respect the old record's TTL when assessing a recent change.

Issue and verify HTTPS

Use a maintained certificate client or your web server's supported automatic HTTPS feature. Follow the instructions for your actual server software. Include each hostname you intend to serve, such as both `example.com` and `www.example.com`.

Let's Encrypt HTTP-01 validation uses port **80**. Its DNS-01 method uses a DNS TXT record and supports wildcard names. Keep any DNS API credentials restricted and private. Do not keep retrying a failed request without checking the validation error.

Visit the hostname over HTTPS and check the certificate name, browser warnings and redirects. Test renewal using your certificate client's supported method and confirm that its renewal service or timer runs. If you proxy the website through Cloudflare, use an appropriate validated origin certificate and Full (strict) mode. Do not bypass certificate warnings as a fix.

For help, send the hostname, intended IP, web-server software and certificate error. Keep private keys and DNS tokens out of the ticket.

References: Let's Encrypt validation methods and Cloudflare DNS proxy status, plus Full (strict) certificate requirements.

Revision #2
Created 2026-11-08 20:06:28 UTC by CloudExa Hosting Admin
Updated 2026-11-08 20:06:28 UTC by CloudExa Hosting Admin