How to Protect a Website with Cloudflare WAF

Introduction

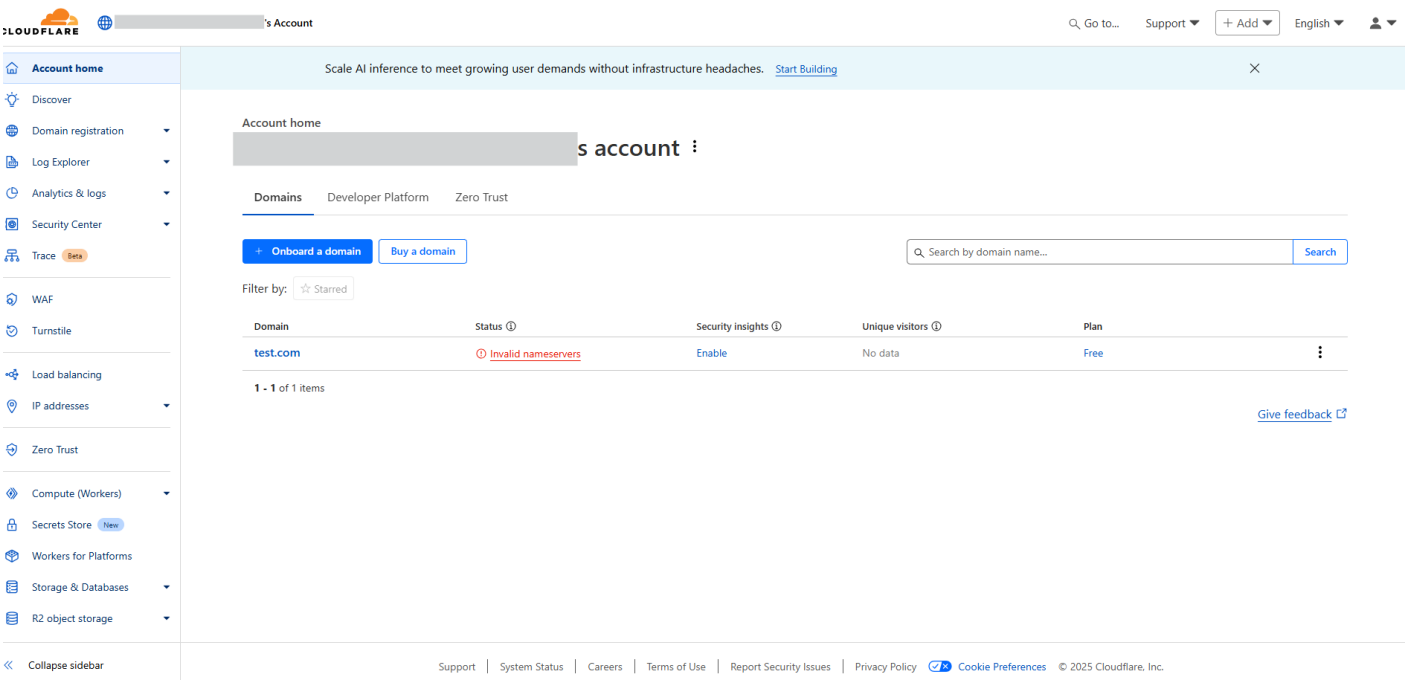
This guide explains how to protect your website using **Cloudflare Web Application Firewall (WAF)**.
Cloudflare sits in front of your website and filters all incoming traffic. By changing your DNS to go through Cloudflare, you get:

- Protection against common web attacks (SQL injection, XSS, etc.)
- Built-in DDoS protection
- Free SSL certificates
- Performance benefits from Cloudflare's global CDN

The process takes a few steps, but once set up, all visitors to your website are automatically filtered through Cloudflare before reaching your server.

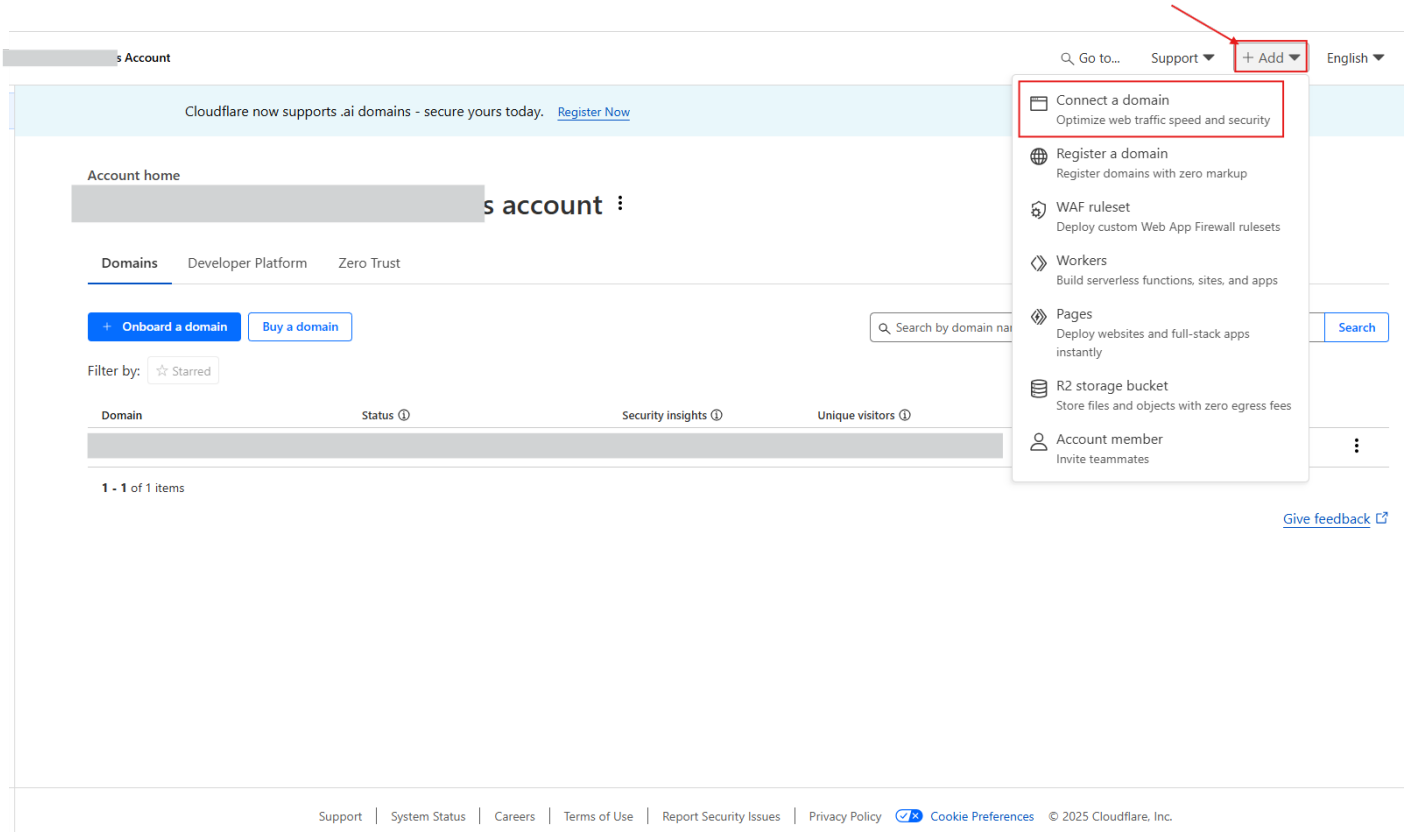
Step 1: Log in to Cloudflare

Go to https://dash.cloudflare.com and log in with your account.



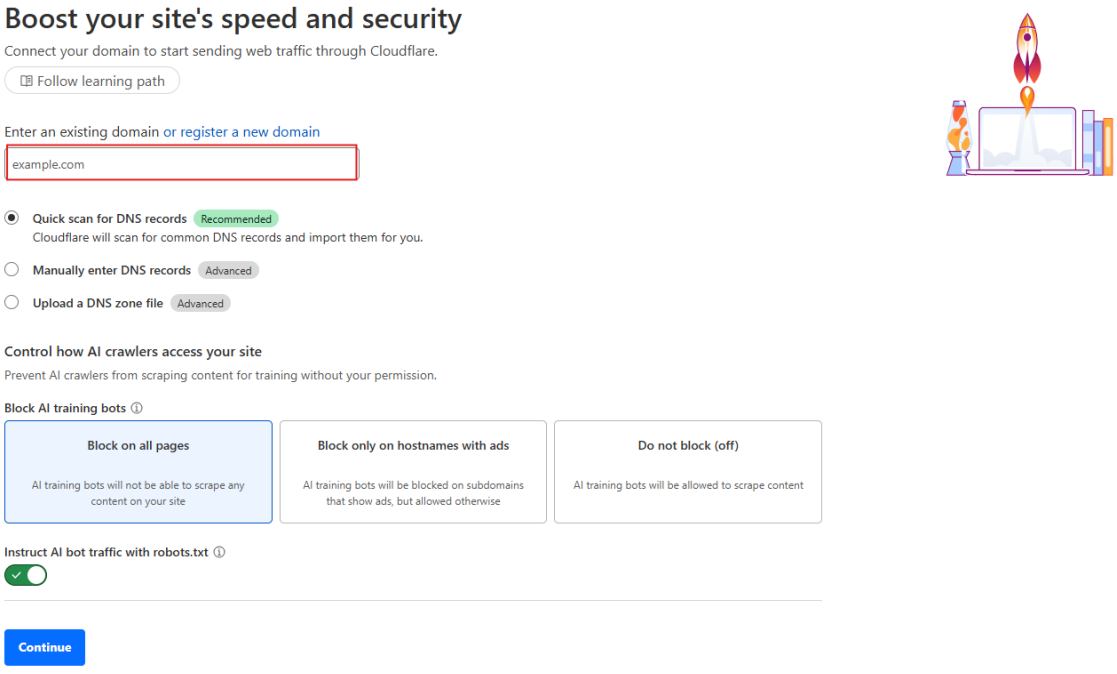
Step 2: Add Your Website

1. In the dashboard, click **+ Add** at the top.
2. Select **Connect a domain**.



Step 3: Enter Your Domain

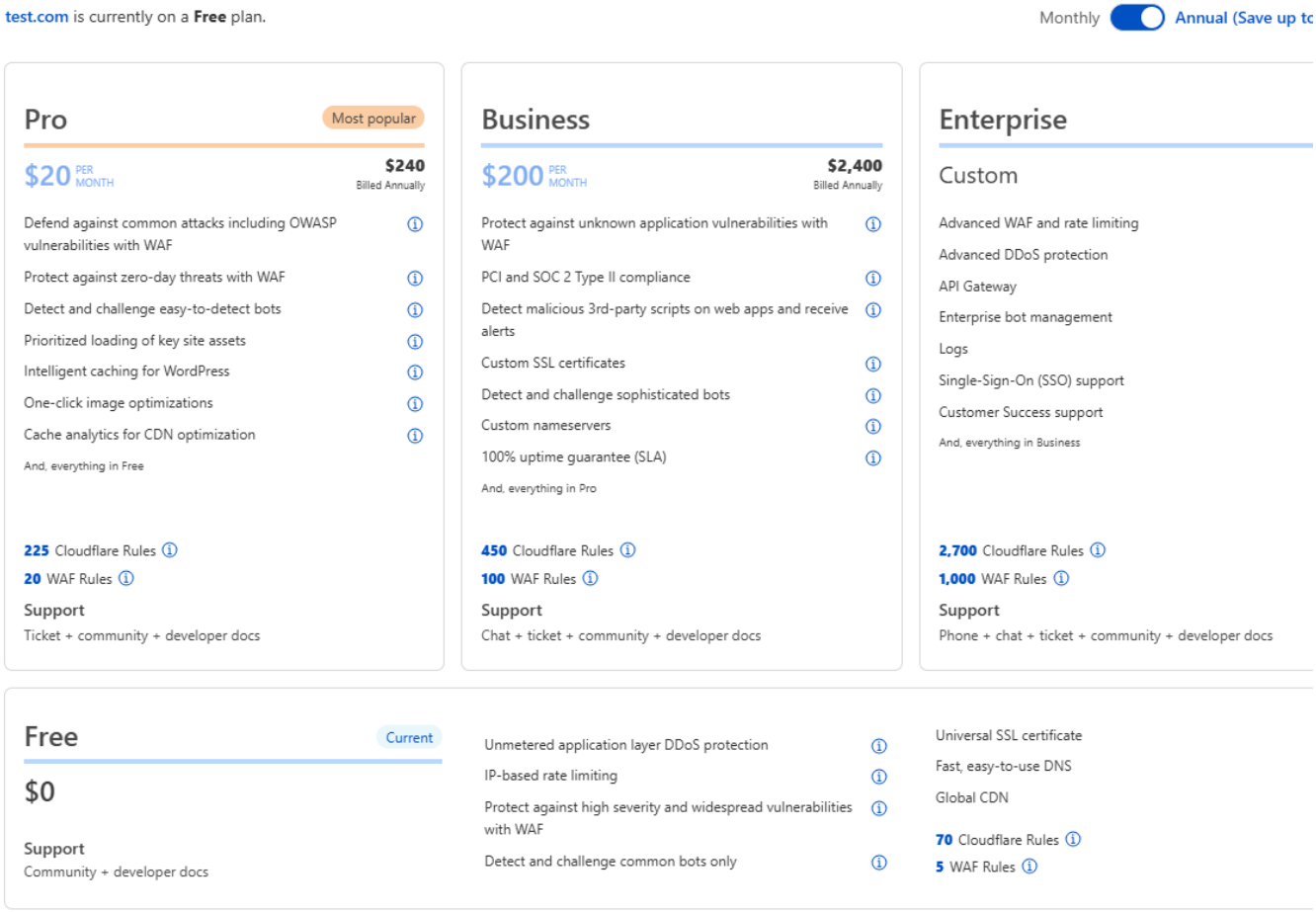
Type your domain name (example: `yourdomain.com`) and click **Continue**.



Step 4: Choose a Plan

Cloudflare will ask you to choose a plan.

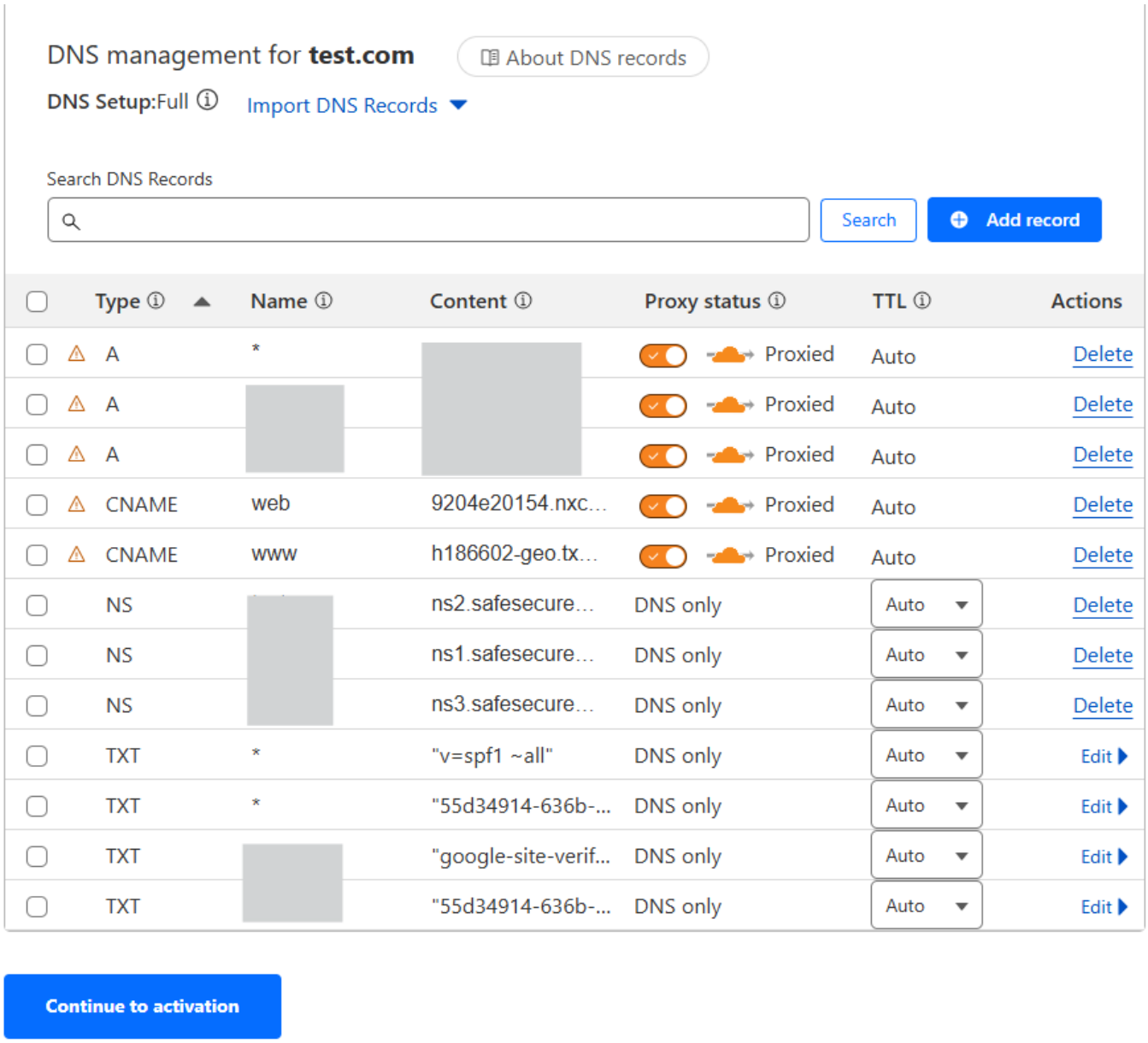
- If you just want the WAF and basic protection, select **Free** (Plan $0).
- Then click **Continue**



Step 5: Review Your DNS Records

Cloudflare scans your existing DNS records.

- Make sure your main records (A and CNAME for your domain and www) are there.
- The **orange cloud (Proxied)** should be ON for the records you want protected by Cloudflare WAF.
- NS (Nameserver) records should remain as **DNS only** (gray cloud).



Once ready, click **Continue** (you don't need to tick the checkboxes).

Step 6: Change Your Nameservers

Cloudflare will give you **two new nameservers**.

> Go to your **Cloudflare dashboard** → **Websites** → select your domain → **DNS** → scroll to **Cloudflare Nameservers** section.

Overview

Last step: Update your nameservers to activate Cloudflare

This is the last step to allow Cloudflare to speed up and protect your web traffic.

Review Cloudflare fundamentals

1. Log into your DNS provider (most likely your registrar)

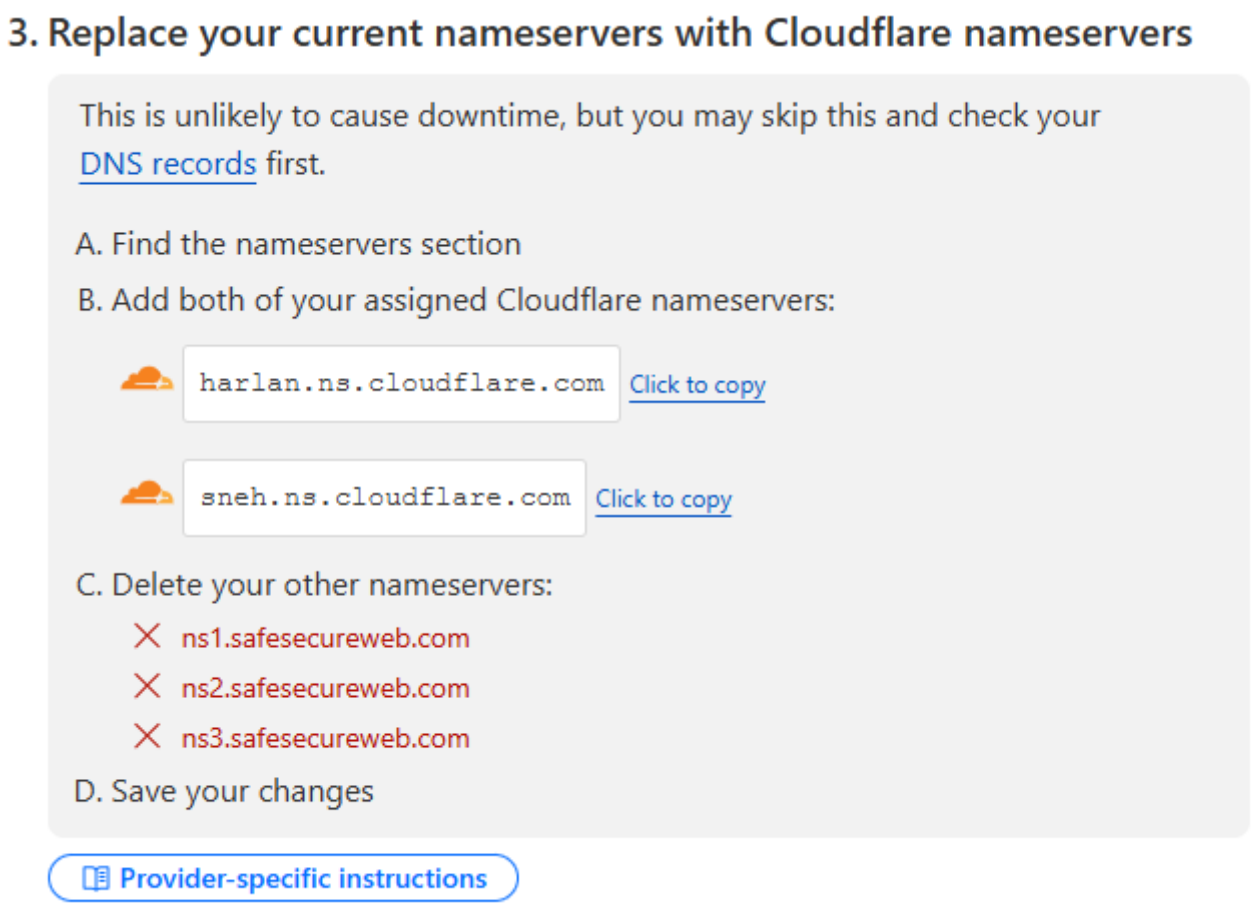
Your registrar is Network Solutions

If you purchased your domain through a reseller (e.g., Squarespace) or use a separate DNS provider, log into that account instead.

2. Make sure DNSSEC is off

Find and turn off the DNS security (DNSSEC) setting if it is on. You can re-enable it later through Cloudflare.

Provider-specific instructions



- Go to your domain registrar (the company where you bought your domain, like GoDaddy or Namecheap).
- Replace the old nameservers with the Cloudflare ones.
- Save changes.

```
Your registrar → Replace:
   ns1.oldprovider.com
   ns2.oldprovider.com

With Cloudflare:
   ada.ns.cloudflare.com
   josh.ns.cloudflare.com
```

Step 7: Wait for Propagation

DNS changes take time. Usually, 15 minutes up to 24 hours.
When Cloudflare detects the change, your site will show as **Active** in the dashboard.

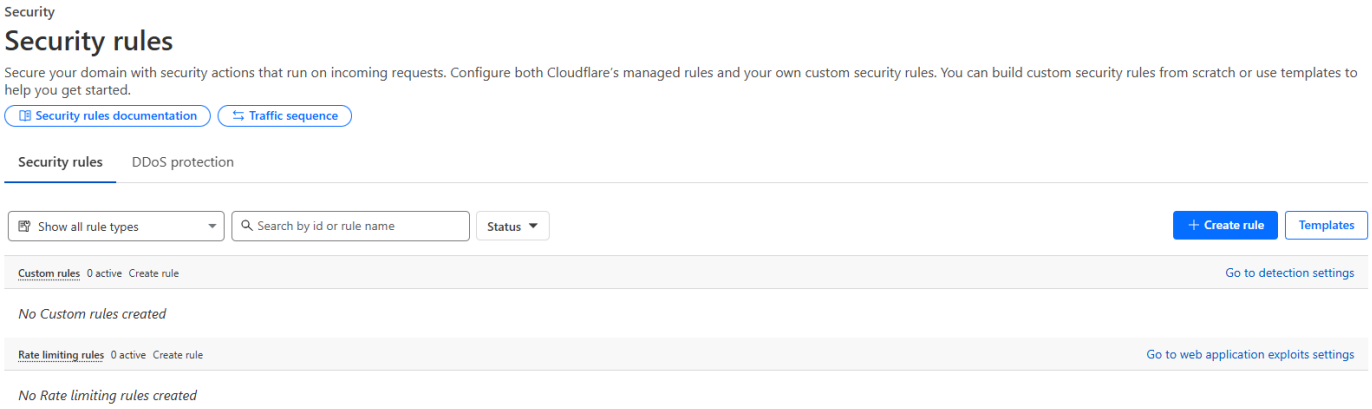
Registrars take up to 24 hours to process nameserver changes (quicker in most cases). We will email you when test.com is active on Cloudflare.

While in this pending state, Cloudflare will respond to DNS queries on your assigned nameservers.

Once activated, SSL/TLS, DDoS protection, caching, and other automatic optimizations will go live for proxied DNS records, along with any custom settings you pre-configure.

Step 8: Enable WAF Protection

- In the dashboard, go to **Security > Security Rules > WAF**.
- Enable **Managed Rulesets** (Cloudflare OWASP Core Ruleset, Cloudflare Managed Ruleset).
- Cloudflare will now filter malicious traffic before it reaches your site.
- Optionally create **Custom Rules** (e.g., block countries, rate limit requests, block SQL injection patterns).
- Test in “Simulate” mode before switching to “Block” to avoid false positives.



Step 9: Verify

- Use a tool like **dig** or **nslookup** to confirm the domain resolves to Cloudflare IPs (not your origin server).
- Try visiting the site; Cloudflare headers like **cf-cache-status** should appear.
- You can also test WAF by visiting **http://yoursite.com/?<script>alert(1)</script>** (Cloudflare should block it if rules are active).

*If you need further assistance, kindly contact our technical support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #3
Created 7 September 2025 07:38:13
Updated 9 September 2025 03:27:48 by Richmond Abella