

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.

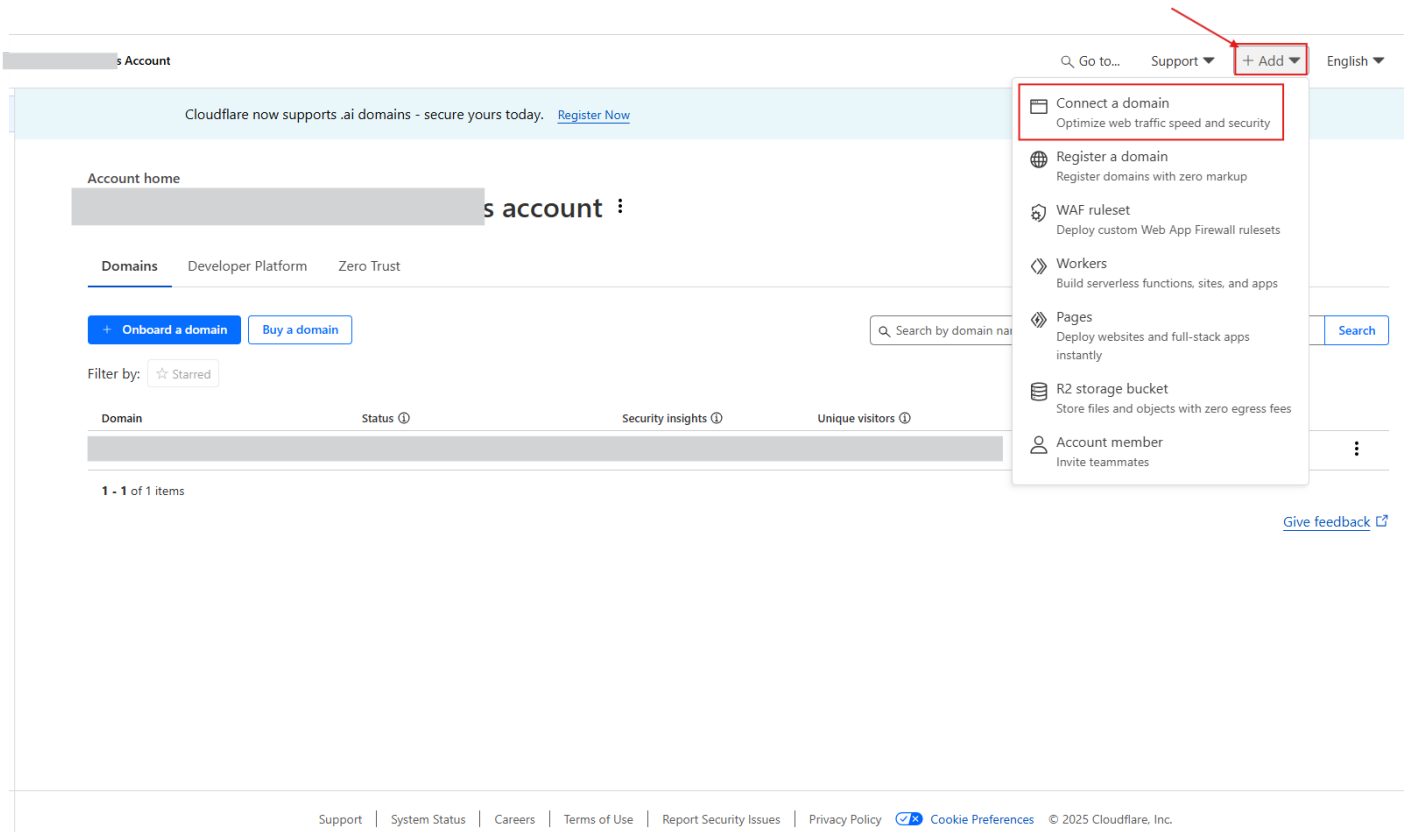
Step 1: Log in to Cloudflare

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

The screenshot shows the Cloudflare dashboard interface. At the top, there's a navigation bar with 'Go to...', 'Support', '+ Add', 'English', and a user profile icon. The left sidebar contains various service categories like 'Account home', 'Discover', 'Domain registration', 'Log Explorer', 'Analytics & logs', 'Security Center', 'Trace', 'WAF', 'Turnstile', 'Load balancing', 'IP addresses', 'Zero Trust', 'Compute (Workers)', 'Secrets Store', 'Workers for Platforms', 'Storage & Databases', and 'R2 object storage'. The main content area is titled 'Account home' and shows 'Account home' and 's account'. Below this, there are tabs for 'Domains', 'Developer Platform', and 'Zero Trust'. The 'Domains' tab is active, showing a search bar and a table of domains. The table has columns: Domain, Status, Security insights, Unique visitors, and Plan. One domain, 'test.com', is listed with a status of 'Invalid nameservers' (indicated by a red circle with an exclamation mark), 'Enable' for security insights, 'No data' for unique visitors, and 'Free' for the plan. There are also buttons for 'Onboard a domain' and 'Buy a domain'.

Step 2: Add Your Website

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



The screenshot shows the Cloudflare dashboard interface. At the top right, there is a navigation bar with 'Go to...', 'Support', '+ Add', and 'English'. A red box highlights the '+ Add' button, and a red arrow points to it from the right. A dropdown menu is open, listing several options: 'Connect a domain' (highlighted with a red box), 'Register a domain', 'WAF ruleset', 'Workers', 'Pages', 'R2 storage bucket', and 'Account member'. The main content area shows the 'Account home' section with a 'Domains' tab selected. Below the tab, there are buttons for '+ Onboard a domain' and 'Buy a domain'. A table below shows a list of domains with columns for 'Domain', 'Status', 'Security insights', and 'Unique visitors'. The footer contains links for 'Support', 'System Status', 'Careers', 'Terms of Use', 'Report Security Issues', 'Privacy Policy', 'Cookie Preferences', and '© 2025 Cloudflare, Inc.'

Step 3: Enter Your Domain

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

Boost your site's speed and security

Connect your domain to start sending web traffic through Cloudflare.

Follow learning path

Enter an existing domain or register a new domain

- Quick scan for DNS records **Recommended**
Cloudflare will scan for common DNS records and import them for you.
- Manually enter DNS records **Advanced**
- Upload a DNS zone file **Advanced**

Control how AI crawlers access your site

Prevent AI crawlers from scraping content for training without your permission.

Block AI training bots

Block on all pages AI training bots will not be able to scrape any content on your site.	Block only on hostnames with ads AI training bots will be blocked on subdomains that show ads, but allowed otherwise.	Do not block (off) AI training bots will be allowed to scrape content.
--	---	--

Instruct AI bot traffic with robots.txt



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**

test.com is currently on a **Free** plan.

Monthly Annual (Save up to 20%)

Pro	Business	Enterprise
<p>Most popular</p> <p>\$20 PER MONTH</p> <p>\$240 Billed Annually</p> <ul style="list-style-type: none">Defend against common attacks including OWASP vulnerabilities with WAFProtect against zero-day threats with WAFDetect and challenge easy-to-detect botsPrioritized loading of key site assetsIntelligent caching for WordPressOne-click image optimizationsCache analytics for CDN optimization <p>And, everything in Free</p> <p>225 Cloudflare Rules</p> <p>20 WAF Rules</p> <p>Support Ticket + community + developer docs</p>	<p>\$200 PER MONTH</p> <p>\$2,400 Billed Annually</p> <ul style="list-style-type: none">Protect against unknown application vulnerabilities with WAFPCI and SOC 2 Type II complianceDetect malicious 3rd-party scripts on web apps and receive alertsCustom SSL certificatesDetect and challenge sophisticated botsCustom nameservers100% uptime guarantee (SLA) <p>And, everything in Pro</p> <p>450 Cloudflare Rules</p> <p>100 WAF Rules</p> <p>Support Chat + ticket + community + developer docs</p>	<p>Custom</p> <ul style="list-style-type: none">Advanced WAF and rate limitingAdvanced DDoS protectionAPI GatewayEnterprise bot managementLogsSingle-Sign-On (SSO) supportCustomer Success support <p>And, everything in Business</p> <p>2,700 Cloudflare Rules</p> <p>1,000 WAF Rules</p> <p>Support Phone + chat + ticket + community + developer docs</p>
<p>Free</p> <p>\$0</p> <p>Support Community + developer docs</p>	<p>Current</p> <ul style="list-style-type: none">Unmetered application layer DDoS protectionIP-based rate limitingProtect against high severity and widespread vulnerabilities with WAFDetect and challenge common bots only	<ul style="list-style-type: none">Universal SSL certificateFast, easy-to-use DNSGlobal CDN70 Cloudflare Rules5 WAF Rules

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).

Search DNS Records



<input type="checkbox"/>	Type ⓘ ▲	Name ⓘ	Content ⓘ	Proxy status ⓘ	TTL ⓘ	Actions
<input type="checkbox"/>	△ A	*		<input checked="" type="checkbox"/> Proxied	Auto	Delete
<input type="checkbox"/>	△ A			<input checked="" type="checkbox"/> Proxied	Auto	Delete
<input type="checkbox"/>	△ A			<input checked="" type="checkbox"/> Proxied	Auto	Delete
<input type="checkbox"/>	△ CNAME	web	9204e20154.nxc...	<input checked="" type="checkbox"/> Proxied	Auto	Delete
<input type="checkbox"/>	△ CNAME	www	h186602-geo.tx...	<input checked="" type="checkbox"/> Proxied	Auto	Delete
<input type="checkbox"/>	NS		ns2.safesecure...	DNS only	Auto ▼	Delete
<input type="checkbox"/>	NS		ns1.safesecure...	DNS only	Auto ▼	Delete
<input type="checkbox"/>	NS		ns3.safesecure...	DNS only	Auto ▼	Delete
<input type="checkbox"/>	TXT	*	"v=spf1 ~all"	DNS only	Auto ▼	Edit ▶
<input type="checkbox"/>	TXT	*	"55d34914-636b-...	DNS only	Auto ▼	Edit ▶
<input type="checkbox"/>	TXT		"google-site-verif...	DNS only	Auto ▼	Edit ▶
<input type="checkbox"/>	TXT		"55d34914-636b-...	DNS only	Auto ▼	Edit ▶

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.

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](#)


3. Replace your current nameservers with Cloudflare nameservers

This is unlikely to cause downtime, but you may skip this and check your [DNS records](#) first.

A. Find the nameservers section

B. Add both of your assigned Cloudflare nameservers:

 [Click to copy](#)

 [Click to copy](#)

C. Delete your other nameservers:

✗ ns1.safesecureweb.com

✗ ns2.safesecureweb.com

✗ ns3.safesecureweb.com

D. Save your changes

[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.

Security

Security rules

Secure your domain with security actions that run on incoming requests. Configure both Cloudflare's managed rules and your own custom security rules. You can build custom security rules from scratch or use templates to help you get started.

[Security rules documentation](#) [Traffic sequence](#)

Security rules DDoS protection

Show all rule types Status [+ Create rule](#) [Templates](#)

Custom rules 0 active [Create rule](#) [Go to detection settings](#)

No Custom rules created

Rate limiting rules 0 active [Create rule](#) [Go to web application exploits settings](#)

No Rate limiting rules created

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