Stop malicious bots while allowing legitimate traffic (Free, Pro, and Business)

The right defense against malicious bot traffic depends on the traffic patterns on your site and your plan. This guide covers a layered approach using Cloudflare Bots, Cloudflare Application Security (also known as Web Application Firewall or WAF), and Turnstile, from baseline protection to targeted custom rules. The core workflow uses features on Free, Pro, and Business plans, with callouts for Enterprise options.

> **Note**
> Most procedures in this guide are configured per domain or zone. Select your domain in the Cloudflare dashboard before starting. Turnstile is the exception: widgets are configured at the account level.

Review your bot traffic

Before you change any bot settings, review your traffic data to understand what bots are doing on your site.

Find your bot analytics

Bot analytics show you how much of your traffic is automated, which pages bots target, and how Cloudflare scores each request.

Bot Analytics requires a Business plan or above

Bot score distribution data and detailed bot analytics are available on Business and Enterprise plans. Free and Pro plan users can review basic security metrics through Security Events. For full bot analytics capabilities, refer to Bot Analytics.

New dashboard | Old dashboard

1. In the Cloudflare dashboard, go to the **Analytics** page.

   Go to **Analytics**

2. Select the **Bot analysis** tab.

Review the following:

- **Bot score distribution chart**: Scores closer to 1 indicate automated traffic. Scores closer to 99 indicate human traffic.
- **Top requested paths**: Which endpoints receive the most bot traffic. Login pages, API endpoints, and checkout flows are common targets.
- **Traffic patterns**: Sudden spikes in low-score traffic, specific user agents appearing at high volume, or geographic concentration of requests can indicate bot activity worth investigating.

Understand bot categories

Cloudflare classifies bot traffic into categories based on bot scores and verification status:

- **Verified bots**: Crawlers and services that Cloudflare has confirmed as legitimate, such as Googlebot, Bingbot, and uptime monitors. Cloudflare maintains a verified bot list with strict requirements.
- **Automated** (score 1): Cloudflare is quite certain the request is automated.
- **Likely automated** (scores 2-29): Probably a bot. This category and Automated are the primary targets for security rules, including scrapers, credential stuffing tools, and spam submitters.
- **Likely human** (scores 30-99): These requests appear to come from real users. Do not challenge or block this traffic.

Block automated traffic with Bot Fight Mode

Bot Fight Mode identifies requests that match known bot patterns and issues a computational challenge. It reduces automated traffic across your entire site without requiring you to write any rules.

What Bot Fight Mode does

Bot Fight Mode is included with Free plans. When enabled, it:

- Identifies traffic matching patterns of known bots
- Issues computationally expensive challenges in response to these bots
- Protects entire domains without endpoint restrictions
- Cannot be customized, adjusted, or reconfigured via custom rules
- Cannot be bypassed with custom rule Skip actions. If Bot Fight Mode challenges a request you want to allow, you can turn off Bot Fight Mode or upgrade to Super Bot Fight Mode for more granular control.

For more details, refer to Bot Fight Mode considerations.

Turn on Bot Fight Mode (Free plan)

New dashboard | Old dashboard

1. In the Cloudflare dashboard, go to the **Security Settings** page.

   Go to **Settings**

2. Filter by **Bot traffic**.
3. Go to **Bot fight mode**.
4. Turn **Bot fight mode** on.

Enable Super Bot Fight Mode (Pro, Business, and Enterprise)

Super Bot Fight Mode adds verified bot allowlisting, per-category actions, static resource protection, and JavaScript detections.

Note

If you are upgrading from Bot Fight Mode to Super Bot Fight Mode, you must disable Bot Fight Mode in your Bot settings.

- Old dashboard: **Security** > **Bots**, and select **Configure Bot Fight Mode**.
- New dashboard: **Security** > **Settings**. Filter by **Bot traffic** and turn **Bot fight mode** off.

New dashboard | Old dashboard

1. In the Cloudflare dashboard, go to the **Security Settings** page.

   Go to **Settings**

2. Filter by **Bot traffic**.
3. Go to **Super Bot fight mode**.
4. Turn **Super Bot fight mode** on.
5. Choose how your domain should respond to various types of traffic by selecting the associated edit icon:

   - For more details on verified bots, refer to Verified Bots.
   - For more details on supported file types, refer to Static resource protection.
   - For more details on invisible code injection, refer to JavaScript detections.
   - For more details on WordPress optimization, refer to Super Bot Fight Mode for WordPress.

Plan availability

Super Bot Fight Mode is available on Pro, Business, and Enterprise plans. Free plan users can use Bot Fight Mode for baseline protection. Enterprise customers who need machine learning-based bot scoring and custom allow/block rules can add Bot Management.

Warning

If your organization uses Cloudflare Tunnel, keep **Definitely Automated** set to **Allow** in Super Bot Fight Mode. Otherwise, tunnels might fail with a `websocket: bad handshake` error.

Protect forms from automated abuse

Turnstile and Application Security rate limiting rules protect form endpoints in different ways and work best together.

Turnstile versus rate limiting

Turnstile challenges suspected bots before they can submit a form (login, signup, contact, or checkout), without showing visitors a CAPTCHA. It can be embedded into any website without sending traffic through Cloudflare. Use Turnstile when you need to challenge automated form submissions.

Rate limiting allows you to define rate limits for requests matching an expression and the action to perform when those limits are reached. Use rate limiting to protect endpoints from abuse, such as brute-force attacks on a login page or excessive API calls from a single client.

Both together provide the strongest coverage. Turnstile challenges automated submissions at the form level. Rate limiting catches high-volume attacks that bypass or do not encounter the form, such as direct `POST` requests to the endpoint that skip the client-side widget.