Custom rules

- Custom rules use cases
  - Path-specific protection
    - Example
  - Custom score thresholds
  - Conditional logic
    - Example
  - Custom actions
  - Detection ID targeting
  - Forwarding bot data to origin
- Execution order

import { GlossaryTooltip, Render } from "~/components";

Bot protection on Cloudflare works through two complementary mechanisms: built-in settings configured through toggles in **Security Settings**, and WAF custom rules that you write using bot management fields. Understanding when to use each approach helps you avoid creating duplicate rules and simplifies your security configuration.

The following features are configured through toggles and dropdowns in Security Settings. They do not require you to write any rule expressions.

Feature	What it does	Availability
Block AI bots	Blocks AI crawlers (GPTBot, ClaudeBot, Bytespider, and others) using an auto-updating managed rule	All plans
AI Labyrinth	Feeds non-compliant AI crawlers into a maze of generated content	All plans
Managed robots.txt	Prepends AI crawler disallow directives to your `robots.txt`	All plans
Super Bot Fight Mode > **Definitely automated**	Blocks or challenges traffic with a bot score of 1	Pro, Business, Enterprise

Feature	What it does	Availability
Super Bot Fight Mode > **Likely automated**	Blocks or challenges traffic with a bot score of 2-29	Business, Enterprise
Verified bots	Managed category of high-trust bots (Googlebot, Bingbot, and others)	Pro, Business, Enterprise
Static resource protection	Extends bot actions to cover static file types	Pro, Business, Enterprise
Optimize for WordPress	Allows WordPress loopback requests through bot protection	Pro, Business, Enterprise
JavaScript detections	Injects a lightweight script to identify clients that cannot execute JavaScript	All plans (automatic on Free)

Bot settings update automatically as Cloudflare identifies new bot signatures and AI crawlers, while custom rules require manual updates. They do not count toward your custom rule limits, and apply uniformly across your domain without the risk of expression errors.

Custom rules use cases

Custom rules are valuable when you need capabilities that built-in settings do not offer. The following scenarios require WAF custom rules with bot management fields. Bot management fields are available to customers with a Bot Management subscription.

Path-specific protection

Since Bot settings apply to all traffic across your domain, you may need an alternative approach to bot handling for different paths using custom rules — for example, stricter protection on `/login/` than on `/public/`.

Example

Block likely automated traffic only on your login endpoint:

```
(cf.bot_management.score lt 30 and not cf.bot_management.verified_bot and
http.request.uri.path eq "/login")
```

Custom score thresholds

The **Definitely automated** and **Likely automated** settings in Super Bot Fight Mode use fixed bot score groupings (1 and 2-29). If you need a different threshold, for example, challenging all traffic with a score below 20, you need a custom rule.

Conditional logic

If you need to combine bot score with other request fields, such as country, ASN, URI path, JA3/JA4 fingerprint, or user agent, you need custom rules. Bot settings do not support compound conditions.

Example

Challenge likely automated traffic only from specific ASNs:

```
(cf.bot_management.score lt 30 and not cf.bot_management.verified_bot and ip.src.asnum in {64496 65536})
```

Custom actions

Bot settings offer **Block**, **Managed Challenge**, and **Allow** as actions.

If you need other actions, such as **Log** (for testing rules before enforcement), **Interactive Challenge**, or **Skip** (to bypass other rules), you need custom rules.

Detection ID targeting

To act on specific bot heuristic detections, such as account takeover or scraping patterns, you need custom rules using the `cf.bot_management.detection_ids` field. Bot settings do not expose individual detection IDs.

Forwarding bot data to origin

To send bot scores, verified bot status, or JA3/JA4 fingerprints to your origin server, use Transform Rules (including Managed Transforms) or Snippets. These are not part of the built-in bot settings.

Execution order

Custom rules execute before Super Bot Fight Mode managed rules. If a custom rule takes a terminating action (such as *Block* or *Managed Challenge*), the request does not reach bot settings.

Refer to Security features interoperability for more information.

□□□ #2
□ □□□ □□□ 2026-11-01 00:04:31 UTC
□ □□□ □□□ 2026-11-01 00:04:32 UTC