

Security features interoperability



- [Execution order](#)
 - [Features outside the Ruleset Engine](#)
 - [Security features overview](#)
 - [DDoS protection](#)
 - [Custom rules](#)
 - [Rate limiting rules](#)
 - [Managed Rules](#)
 - [Bot Fight Mode](#)
 - [Super Bot Fight Mode](#)
 - [Bot Management](#)
 - [Key interaction rules](#)
 - [Common scenarios](#)
 - [Small business website \(Free plan\)](#)
 - [E-commerce site \(Pro or Business plan\)](#)
 - [Enterprise API and website \(Enterprise plan\)](#)
 - [Troubleshoot conflicts](#)
 - [Identify which feature blocked a request](#)
 - [Resolve Bot Fight Mode false positives](#)
 - [Resolve Super Bot Fight Mode false positives](#)
 - [Resolve Managed Rules false positives](#)
-

```
import { Details, Steps, DashButton, GlossaryTooltip } from "~/components";
```

Cloudflare applies multiple security features to every incoming request. Each feature runs at a specific stage, and the order determines which feature acts first. Understanding this order helps you avoid conflicts and reduce false positives.

Execution order

Cloudflare security features powered by the [Ruleset Engine](#) run in a fixed sequence of phases. When a request arrives, it passes through each phase in order. If a rule takes a terminating action (for example, *Block* or *Managed Challenge*), the request stops and does not reach later phases.

The security-related request phases, in execution order, are:

Phase name	Product
<code>ddos_l7</code>	HTTP DDoS Attack Protection
<code>http_request_firewall_custom</code>	Custom rules
<code>http_ratelimit</code>	Rate limiting rules
<code>http_request_firewall_managed</code>	Managed Rules
<code>http_request_sbfm</code>	Super Bot Fight Mode

Within each phase, account-level rulesets run before zone-level rulesets.

:::note [Bot Fight Mode](#) does not use the Ruleset Engine. It operates outside this phase system and cannot be skipped with custom rules. :::

The Ruleset Engine powers many Cloudflare products beyond security. Refer to [Phases list](#) for the complete list of request and response phases.

Features outside the Ruleset Engine

The following security features are not powered by the Ruleset Engine and are evaluated independently:

- [IP Access Rules](#)
- [Zone Lockdown](#)
- [User Agent Blocking](#)
- [Browser Integrity Check](#)
- [Hotlink Protection](#)
- [Security Level](#)

Because these features run independently, they do not follow the phase order described above.

Security features overview

DDoS protection

[DDoS protection](#) is always on for all Cloudflare plans. L7 HTTP DDoS Attack Protection detects and mitigates application-layer DDoS attacks. L3/4 Network-layer DDoS Attack Protection handles network-layer attacks. You do not need to turn on or configure anything for DDoS protection to work.

Custom rules

[Custom rules](#) are rules you define. They run in the `http_request_firewall_custom` phase and support actions like *Block*, *Managed Challenge*, *Skip*, and *Log*. You can reference [bot score](#) fields, [WAF attack score](#) fields, and all standard request fields in your expressions.

Rate limiting rules

[Rate limiting rules](#) throttle or block traffic that exceeds a defined request rate. They run in the `http_ratelimit` phase, after custom rules.

Managed Rules

[Managed Rules](#) are pre-configured rulesets maintained by Cloudflare. These include the [Cloudflare Managed Ruleset](#) and the [OWASP Core Ruleset](#). They run in the `http_request_firewall_managed` phase.

Bot Fight Mode

[Bot Fight Mode](#) is available on Free plans. It is a simple on/off toggle that challenges traffic matching patterns of known bots. You cannot customize its behavior or skip it with custom rules.

Super Bot Fight Mode

[Super Bot Fight Mode](#) (SBFM) is available on Pro, Business, and Enterprise plans (without the Bot Management add-on). It runs in the `http_request_sbfm` phase and offers more control than Bot Fight Mode. You can configure separate actions for **Definitely automated**, **Likely automated**, and **Verified bots** traffic. You can skip SBFM for specific requests using the [Skip action](#) in custom rules.

Bot Management

[Bot Management](#) is an Enterprise add-on. It generates a bot score from `1` to `99` for every request. Lower scores indicate more automated traffic. You write custom rules using the

`cf.bot_management.score` field to take action based on this score. For more information, refer to [Bot Management variables](#).

Key interaction rules

These rules govern how security features interact:

- **Terminating actions stop the request evaluation workflow.** If a rule blocks or challenges a request, Cloudflare does not evaluate later phases for that request.
- **Custom rules run before SBFM.** A terminating action in custom rules prevents Super Bot Fight Mode from evaluating the request.
- **Skip actions bypass later phases.** You can use the [Skip action](#) in custom rules to bypass rate limiting rules (`http_ratelimit`), Super Bot Fight Mode (`http_request_sbfm`), and Managed Rules (`http_request_firewall_managed`).
- **Bot Fight Mode cannot be skipped.** Because Bot Fight Mode is not part of the Ruleset Engine, custom rules cannot skip it. If you need to exempt traffic from bot protection, upgrade to Super Bot Fight Mode or Bot Management.
- **Bot Management scores are available in custom rules.** Enterprise customers with Bot Management can use `cf.bot_management.score` in custom rule expressions to define custom thresholds per path, user agent, or any other request property.
- **Same-zone snippet subrequests are not evaluated by custom rules or managed rules.** When a snippet uses `fetch()` to call a proxied hostname in the same zone, WAF custom rules and WAF managed rules on the target hostname do not apply to that subrequest. Refer to [Subrequests made by a snippet](#).

Common scenarios

Small business website (Free plan)

A Free plan includes DDoS protection and Bot Fight Mode.

- DDoS protection runs automatically on every request.
- Turn on **Bot Fight Mode** under **Security > Settings** to challenge known bot patterns.
- Turn on **Block AI Bots** to prevent AI crawlers from scraping your content.

Because Bot Fight Mode cannot be skipped or customized, you cannot create exceptions for specific bots. If Bot Fight Mode causes false positives for legitimate automated traffic (for example, monitoring services or payment processors), consider upgrading to a Pro or Business plan that includes Super Bot Fight Mode.

E-commerce site (Pro or Business plan)

A Pro or Business plan adds Super Bot Fight Mode, custom rules, and Managed Rules.

- DDoS protection runs automatically.
- Turn on **Super Bot Fight Mode** to block automated and likely automated traffic.
- Deploy **Managed Rules** for protection against known vulnerabilities like SQL injection and cross-site scripting.
- Create custom rules with the *Skip* action to allow legitimate automated traffic while SBFM blocks bad bots everywhere else. Use the following rule configuration:
 - Set the rule expression to match the IP addresses or user agents of your payment processor.
 - Set the action to *Skip*, and select **Super Bot Fight Mode**.

Enterprise API and website (Enterprise plan)

An Enterprise plan with the Bot Management add-on provides the most flexibility.

- DDoS protection runs automatically.
- Bot Management generates a bot score on every request.
- Create custom rules that reference `cf.bot_management.score` to define your own thresholds. For example, block requests with a bot score below 30 for website paths, while allowing all scores on API paths that authenticated partners use.
- Use rate limiting rules to throttle abusive traffic patterns.
- Deploy Managed Rules to protect against known vulnerabilities.

Troubleshoot conflicts

When security features interfere with legitimate traffic, use the following steps to identify and resolve the issue.

Identify which feature blocked a request

Use [Security Events](#) to identify the feature that blocked a request:

1. In the Cloudflare dashboard, go to the **Analytics** page.
2. Select the **Events** tab.
3. Find the blocked request in the log.
4. Check the **Service** field to determine which product took the action. This field tells you which feature to adjust.

Resolve Bot Fight Mode false positives

Bot Fight Mode does not support exceptions. You have two options:

- Turn off Bot Fight Mode entirely under **Security > Settings**.
- Upgrade to a plan with Super Bot Fight Mode, which supports skip rules.

For more information, refer to [Handle false positives from Bot Fight Mode or Super Bot Fight Mode](#).

Resolve Super Bot Fight Mode false positives

Create a custom rule with the *Skip* action to bypass SBFM for the affected traffic:

1. In the Cloudflare dashboard, go to the **Security rules** page.
2. Select **Create rule > Custom rules**.
3. Define an expression that matches the legitimate traffic (for example, a specific IP range or user agent).
4. Set the action to *Skip* and select **Super Bot Fight Mode**.

For more information, refer to [Handle false positives from Bot Fight Mode or Super Bot Fight Mode](#).

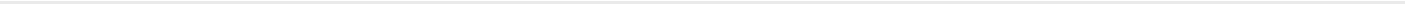
:::caution If you use [Cloudflare Tunnel](#), keep **Definitely Automated** set to **Allow** in your Super Bot Fight Mode configuration. Otherwise, tunnels might fail with a `websocket: bad handshake` error. :::

Resolve Managed Rules false positives

If a managed rule blocks legitimate traffic:

- Create a [WAF exception](#) to skip specific rules or rulesets for matching requests.
- Disable individual rules within a managed ruleset if they do not apply to your application.

For detailed guidance, refer to [Troubleshoot managed rules](#).



🔍 #2	
📅 🕒	📅 2026-11-01 05:14:08 UTC
📅 🕒	📅 2026-11-01 05:14:10 UTC