Cloudflare “I’m Under Attack” Mode: When to Turn It On, Where to Find It, What Visitors See, and When to Turn It Off

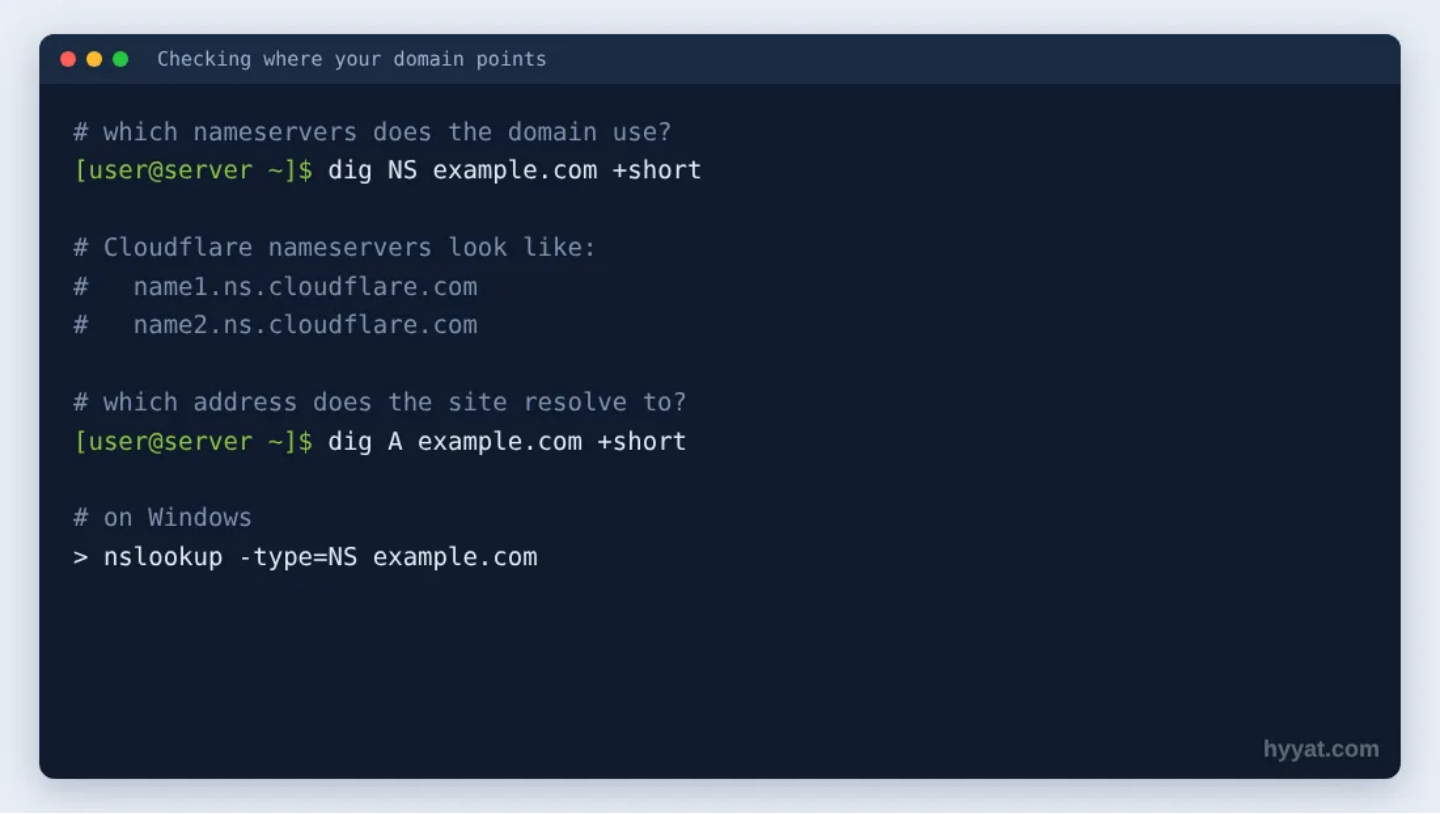
Cloudflare · https://www.hyyat.com/en/knowledgebase/cloudflare-under-attack-mode/

In shortI’m Under Attack mode makes Cloudflare show every visitor a short check page before entering, which stops most automated traffic. Find it in your domain’s Cloudflare dashboard: under **Overview** (quick actions) or **Security › Settings**, depending on the dashboard layout. Use it only during an attack, then turn it off.

Embedded media: https://www.hyyat.com/wp-content/uploads/2026/11/hyyat-w2-cfattack-en.mp4?_=1

When your site is flooded with automated requests, the server slows or stops and visitors see errors such as 508 or 522. This mode puts a barrier in front of the site: every visitor passes a browser check first, and simple bots cannot get through.

When to turn it on



Situation	Turn on Under Attack?
A sudden, huge traffic spike with slowness or downtime, and the visits are not real	Yes
An ad campaign brought real visitors	No, that is normal load
Repeated login attempts on wp-login only	Usually not: a rule for the login page alone fits better
The site is always slow	No, the cause is on the site: why is my site slow?

Turning it on

1. **Log in to Cloudflare** at `dash.cloudflare.com` and pick your domain.
2. **Find Under Attack Mode** in **Overview** under quick actions, or in **Security › Settings**.
3. **Turn it on** it takes effect within seconds.
4. **Watch** the security log in **Security › Events** and whether the site recovers.

This mode only works if the domain really goes through Cloudflare: Cloudflare nameservers and the orange cloud on the site's record. If your site is not on Cloudflare yet: signing up for Cloudflare.

What visitors see

A short page saying the browser is being checked, then an automatic redirect to the site within seconds. Real visitors usually pass without clicking anything, though some may get an extra check.

Side effects

- Monitoring tools and services that call your site automatically, such as payment gateways sending notifications, may be blocked.
- Mobile apps that talk to your site through an API may break.
- The first visit feels slightly slower.

So do not leave it on permanently. Once the attack ends, turn it off and rely on targeted security rules instead of a blanket barrier.

From our support desk: If only the login page is under attack, a challenge rule for `/wp-login.php` alone is better than putting the whole site behind a check. Add a security plugin too, as in security plugins.
Running WordPress? See Hyyat Host WordPress hosting.

Questions we get

Is Under Attack mode free?
Yes, it is available on the free plan.

I turned it on and nothing changed
Make sure the cloud next to the site's record is orange and the nameservers are Cloudflare's.

Does it affect Google?
Cloudflare normally lets known search engine crawlers through. Still, do not leave it on longer than needed.

The attack continues despite the mode
If the attack hits the server address directly, bypassing Cloudflare, send us a support ticket.

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.

Web HostingSaudi Hosting