interweb

Generated on 15/11/2026 01:49

KNOWLEDGE BASE · PUBLIC DOCUMENT

Rate limiting in nginx: slowing down bots and password guessing

Security & Access

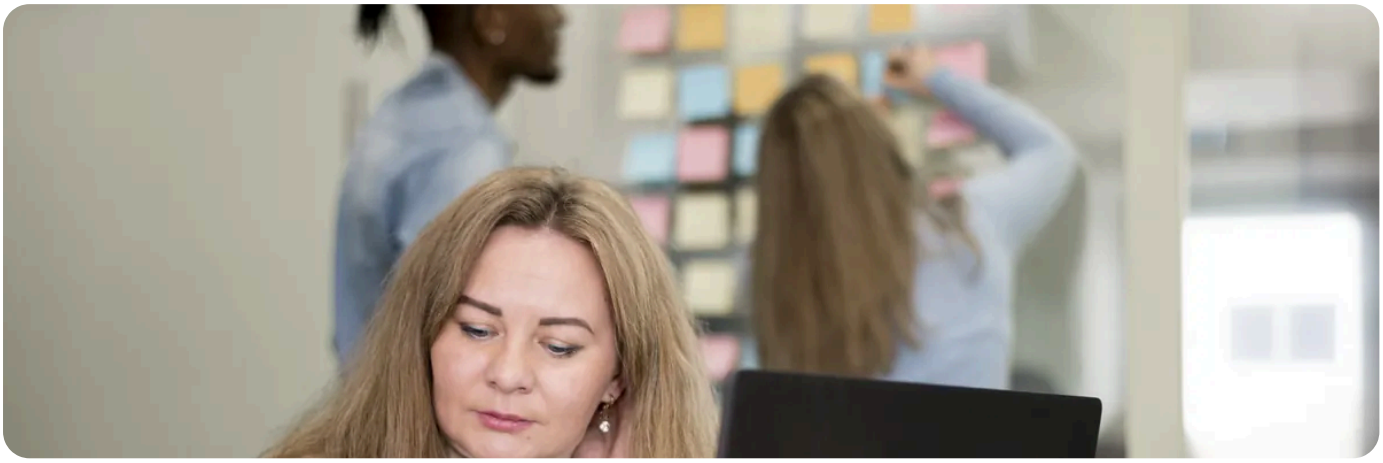
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1680	v2026.10.15	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/1680

Rate limiting in nginx: slowing down bots and password guessing

Security & Access Created on **October 15, 2026** 2 min read



The short answer: nginx has a built-in request limiter. You define a "zone" that counts requests per address and a rule on a location, and anyone above the pace gets an error instead of an answer. It is the cheapest defence against bots hammering `wp-login.php` or an API. You need a VPS with **root access** and nginx serving your site.

nginx and its configuration are yours: our support does not write them or repair them (see **How far our support goes**). If you do not have nginx set up yet, start with **Installing nginx on Ubuntu**.

The two pieces

1. **The zone,** in a file inside `/etc/nginx/conf.d/` (it lives in the "http" context, outside any site):
   `limit_req_zone $binary_remote_addr zone=login:10m rate=5r/m;`

2. **The rule,** inside your site's block, on the location you want to protect:

```
location = /wp-login.php {
limit_req zone=login burst=5 nodelay;
limit_req_status 429;
# the rest of the configuration you already have here
}
```

3. **Test and apply:** `sudo nginx -t` confirms the syntax is right, and `sudo systemctl reload nginx` applies it without cutting connections.

Part	What it means
`zone=login:10m`	The zone name and the memory for its bookkeeping: ten megabytes is enough for many addresses.

Part	What it means
`rate=5r/m`	Five requests a minute, per address. It can be `r/s` for seconds.
`burst=5`	Lets up to five extra requests through at once before it starts refusing. It avoids punishing a person who loads the page and goes back.
`nodelay`	Requests inside the burst go through now, instead of being delayed.
`limit_req_status 429`	The error returned: 429, “too many requests”. Without it, it is 503, which looks like a fault.

Behind Cloudflare, the address nginx sees is Cloudflare’s,
not the visitor’s: the limit would apply to everybody at once. Tell nginx the real address with the `realip` module (the `set_real_ip_from` and `real_ip_header CF-Connecting-IP` lines). See **Cloudflare: what it is and what changes**.

Several users can share one address
(a mobile network, an office). A limit that is too tight blocks real people. Start wide, watch the log and tighten gradually.

The limiter slows, it does not stop: a patient bot keeps trying. To ban those who insist, add **fail2ban**. And to protect the WordPress login itself, see **Protecting the WordPress login**.

NEED A HAND?

Set the limit and your site now answers 429 to everyone? Open a ticket with the nginx block and one line of the access log.

Open a support ticket →

SEE ALSO

- How to install nginx on Ubuntu and serve your website from a folder →
- Installing fail2ban on a VPS to stop SSH password guessing →
- Protecting the WordPress login: three steps in order of effect →

Blocking an IP address from visiting your site

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-1680 · v2026.10.15 · Generated on 15/11/2026 01:49