interweb

Gerado a 15/11/2026 02:05

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Limitar pedidos no nginx: abrandar robôs e tentativas de adivinhar senhas

Segurança e acesso

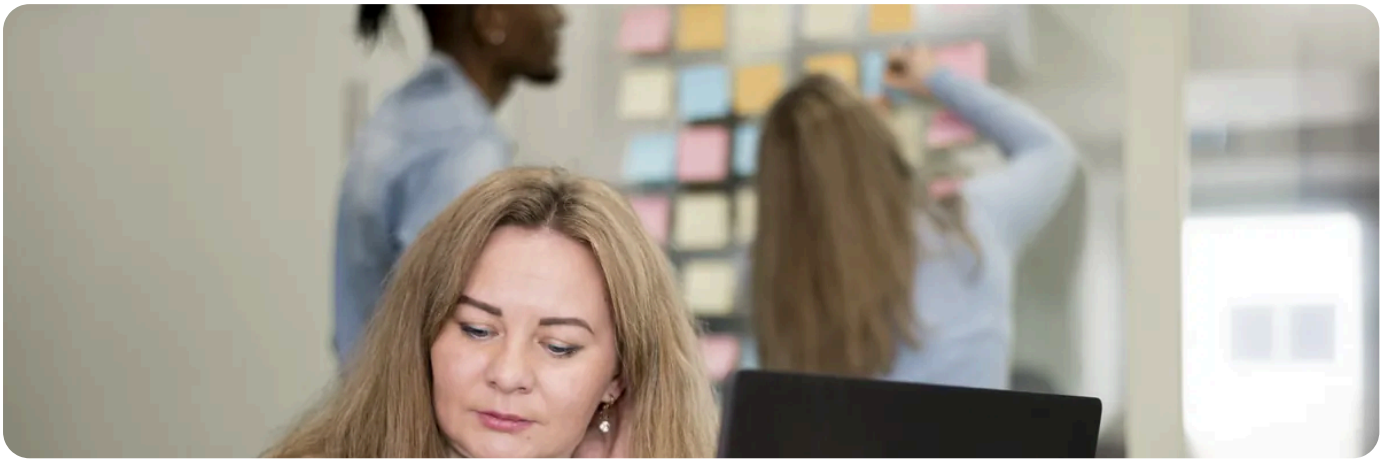
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-MZ-KB-1680	v2026.10.15	Moçambique · Português

Interweb Moçambique
RLX Holdings, S.A. · Grupo RLX Holdings
NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

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

Limitar pedidos no nginx: abrandar robôs e tentativas de adivinhar senhas

Segurança e acesso Criado em **15 de outubro de 2026** 2 min de leitura



A resposta curta: o nginx tem um limitador de pedidos incorporado. Define-se uma «zona» que conta pedidos por endereço e uma regra numa localização, e quem passa do ritmo recebe um erro em vez de uma resposta. É a defesa mais barata contra robôs que martelam o `wp-login.php` ou uma API. Precisa de um VPS com **acesso root** e o nginx a servir o seu site.

O nginx e a configuração são seus: o nosso suporte não os escreve nem repara (veja **Até onde vai o nosso suporte**). Se ainda não tem o nginx montado, comece por **Instalar o nginx no Ubuntu**.

As duas peças

1. **A zona,** num ficheiro dentro de `/etc/nginx/conf.d/` (fica no contexto «http», fora de qualquer site):
   `limit_req_zone $binary_remote_addr zone=login:10m rate=5r/m;`

2. **A regra,** dentro do bloco do seu site, na localização que quer proteger:

```
location = /wp-login.php {
limit_req zone=login burst=5 nodelay;
limit_req_status 429;
# o resto da configuração que já tem aqui
}
```

3. **Teste e aplique:** `sudo nginx -t` confirma que a sintaxe está certa, e `sudo systemctl reload nginx` aplica sem cortar ligações.

Parte	Quer dizer
`zone=login:10m`	O nome da zona e a memória para a sua contabilidade: dez megabytes dão para muitos endereços.
`rate=5r/m`	Cinco pedidos por minuto, por endereço. Pode ser `r/s` para segundos.
`burst=5`	Deixa passar até cinco pedidos a mais de uma vez, antes de começar a recusar. Evita castigar uma pessoa que carrega a página e volta atrás.
`nodelay`	Os pedidos dentro do burst passam já, em vez de serem atrasados.
`limit_req_status 429`	O erro devolvido: 429, «demasiados pedidos». Sem isto é 503, que parece uma avaria.

Atrás do Cloudflare, o endereço que o nginx vê é o do Cloudflare, não o do visitante: o limite passava a valer para toda a gente ao mesmo tempo. Diga ao nginx qual é o endereço verdadeiro com o módulo `realip` (as linhas `set_real_ip_from` e `real_ip_header CF-Connecting-IP`). Veja **O Cloudflare: o que é e o que muda**.

Vários utilizadores podem partilhar o mesmo endereço (uma rede móvel, um escritório). Um limite apertado demais bloqueia pessoas a sério. Comece largo, veja o registo e aperte aos poucos.

O limitador abranda, não impede: um robô paciente continua a tentar. Para banir quem insiste, junte-lhe o **fail2ban**. E para proteger o login do WordPress em si, veja **Proteger o login do WordPress**.

PRECISA DE AJUDA?

Montou o limite e o seu site responde 429 a toda a gente? Abra um pedido com o bloco do nginx e uma linha do registo de acessos.

Abrir pedido de suporte →

VEJA TAMBÉM

- Instalar o nginx no Ubuntu e servir o seu site →
- Instalar o fail2ban num VPS contra tentativas de senha no SSH →

Proteger o login do WordPress: três passos por ordem de efeito

Bloquear um endereço IP de visitar o seu site

interweb

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT	401 191 607
NUEL	105 045 974
CAE	62022
SEDE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Moçambique
CONTACTOS	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-MZ-KB-1680 · v2026.10.15 · Gerado a 15/11/2026 02:05

Versão online deste documento