Prevent Wordpress brute force attacks

What is a brute force attack?

A brute force attack is also sometimes called a dictionary attack. The hacker is trying to guess the password using the automated software, which floods your website with requests every couple of seconds. This is a waste of your resources and if password is not strong enough eventually the hacker will compromise the website.

How to verify that you are being brute forced?

The easiest way is to check the web server access logs for all the IP addresses, which successfully connected to the wp-login.php with HTTP response of 200 OK. Apache web server reports the successful logins like this:
`POST /wp-login.php HTTP/1.1“ 200`

If you are running Apache web server:

1. Login to the server via SSH.
2. Go to the /var/log/httpd
3. Run this command: `cat access_log | egrep -v 'HTTP[^”]*“ (200|204)' | grep wp-login.php`

Example results, with the IP address of the attacker, who attempted to get to the wp-login.php page:
`115.159.126.184` `- - [12/Apr/2020:04:30:49 +0000] “POST /wp-includes/modules/wp-login.php HTTP/1.1” 404 230 ”-“ “Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36”`

Implement a Content Delivery Network (CDN):

A CDN would be able to filter the brute force attacks to at least slow down the attacker on the DNS level. This would put less strain on the server resources. If you dont want to use their Name Servers for your domain, you can use their Wordpress plugin.

- Sucuri CloudProxy
- CloudFlare

Change administrator account username:

Name your admin user daisy or something non generic to limit dictionary/guess attacks. Use a strong non-dictionary password.

Restricting access to the Wordpress admin area:

Create .htaccess file, which will prevent access to the admin area only to the whitelisted IP addresses. This approach will cause some strain on the server resources as the web server have to process every request against the IP address(es) added to the whitelist.

Use a Wordpress plugin:

There is a reason why this is the last resort on our list. Plugins can malfunction during upgrades, they also put some additional stress on your server resources.