Cloudflare WAF Protection Checklist

☐ Block SQL injection and XSS patterns using Cloudflare managed rules.

☐ Restrict access to /wp-login.php and /wp-admin/ to specific IPs or countries

.

☐ Rate limit login attempts to no more than 5 per 10 minutes per IP.

☐ Block bad bots such as those using 'python-requests/2.25' or with empty user agents.

☐ Block repeated form submissions exceeding 10 per 30 seconds.

☐ Geo-block countries that do not represent your customer base.

☐ Challenge users with threat scores higher than 40.

☐ Use expressions to block traffic combining bad IP reputation. high threat score, and suspicious referrer.

☐ Block or rate limit access to xmlrpc.php unless explicitly needed (e.g., Jetpack).

☐ Block URL parameters matching SQLi patterns like '?id=1+UNION+SELECT'.

☐ Block directory traversal attempts using patterns like ../ or %2e%2e%2f.

☐ Block HTTP methods PUT, DELETE, and OPTIONS unless your application requires them.

☐ Challenge requests with blank or suspicious user agents.