



Web Application Firewall Guida d'uso

Modulo PrestaShop · Compatibile con PrestaShop 1.7, 8 e 9

Blocca il traffico cattivo prima che arrivi al negozio

Web Application Firewall blocca IP abusivi, intervalli CIDR, interi Paesi e bot malevoli, limita i client troppo aggressivi, protegge il login del back office dal brute force e ferma i pattern di attacco più comuni (SQLi / XSS / LFI / probing). Una whitelist affidabile con protezione anti-lockout ti tiene al sicuro e ogni richiesta bloccata viene registrata. Nessun codice, nessuna modifica al tema.

1. Installazione

1. Nel back office vai su **Moduli** → **Gestione moduli** → **Carica un modulo** e seleziona lo ZIP del modulo.
2. A installazione completata, clicca **Configura** per aprire la procedura guidata.

Gli aggiornamenti sono automatici. Sono legati al tuo dominio — nessuna chiave di licenza da inserire. I domini di sviluppo (`.local` , `.test` , `localhost`) sono sempre ammessi. Quando esce una nuova versione viene segnalata dentro al modulo.

2. Configurazione — passo per passo

Il modulo è organizzato in schede: **Regole e whitelist**, **Log bloccati**, **Protezione login** e **Impostazioni**. Le sezioni seguenti seguono la scheda *Impostazioni*, dove ogni protezione ha il suo interruttore.

Generale **interruttore generale**

L'interruttore on/off dell'intero firewall e il modo in cui viene letto l'IP del client.

- **Abilita firewall** — interruttore generale. Off = non viene filtrato nulla sul front office.
- **Dietro un proxy / CDN** — attiva solo se il negozio è davvero dietro un proxy o CDN affidabile. Altrimenti gli header proxy sono falsificabili e un attaccante potrebbe falsare IP/Paese.
- **Header proxy affidabile** — quale header porta il vero IP del client: *Auto* (Cloudflare → X-Real-IP → X-Forwarded-For), *CF-Connecting-IP*, *X-Real-IP* o *X-Forwarded-For*.

Enable firewall	<input checked="" type="radio"/> Yes <input type="radio"/> No
Behind a proxy / CDN	<input type="radio"/> Yes <input checked="" type="radio"/> No
Trusted proxy header	Auto (Cloudflare → X-Real-IP → X-Forwarded-For) ▼
<small>Only enable "behind proxy" if your store really sits behind a trusted proxy/CDN. Otherwise these headers are spoofable and an attacker could forge their IP/country.</small>	
IP / CIDR blocking	
Enable IP / CIDR blocking	<input checked="" type="radio"/> Yes <input type="radio"/> No

Generale — interruttore generale e rilevamento proxy/IP

Blocco IP / CIDR

Blocca singoli indirizzi IP o interi intervalli CIDR.

- **Abilita blacklist IP / CIDR** — attiva il blocco di IP/intervalli.
- Le voci di blacklist e whitelist si gestiscono nella scheda **Regole e whitelist**. Un IP/CIDR in whitelist scavalca ogni altro controllo.

Enable IP / CIDR blacklist Yes No

Manage entries under the "Rules & whitelist" tab.

Country blocking

No country source available: enable "behind proxy/CDN" so a CDN country header (e.g. CF-IPCountry) can be read, or set a GeoIP database path below. Country blocking stays inactive until then.

Blocco IP / CIDR — gestito insieme alla whitelist

Blocco per Paese

Consenti o nega i visitatori per Paese (codici ISO-2).

- **Abilita blocco per Paese** — attiva il filtro geografico.
- **Modalità** — *Block-list* (blocca i Paesi elencati) o *Allow-list* (consenti solo i Paesi elencati).
- **Codici Paese** — codici ISO-2 separati da virgola, es. `RU, CN, KP`.
- **Percorso database GeoIP** — percorso opzionale al tuo file MaxMind GeoLite2 `.mmdb`. Nessun database GeoIP è incluso (vincoli di licenza); forniscine uno tuo, oppure usa l'header Paese del CDN (es. CF-IPCountry) attivando "dietro proxy/CDN".

No country source available: enable "behind proxy/CDN" so a CDN country header (e.g. CF-IPCountry) can be read, or set a GeoIP database path below. Country blocking stays inactive until then.

Enable country blocking Yes No

Mode

Country codes (ISO-2, comma separated)

GeoIP database path (optional MaxMind GeoLite2 .mmdb)

We never bundle a GeoIP database (license restrictions). Provide your own .mmdb and the geoip2 library or PECL geoip extension, or rely on the CDN country header.

Bad bots / user-agents

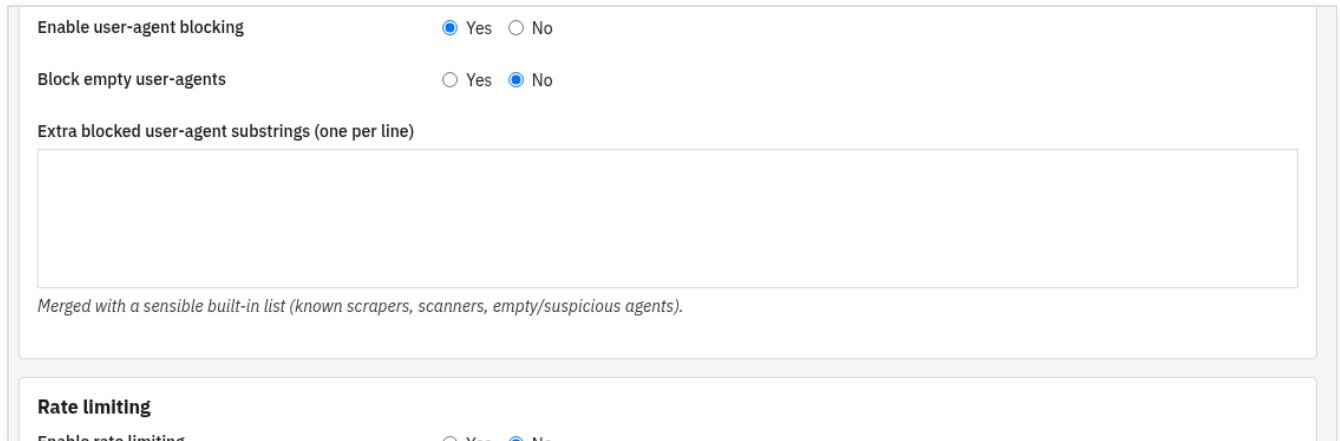
Enable user-agent blocking Yes No

Blocco per Paese — block-list o allow-list per codice ISO-2

Bot malevoli / user-agent

Blocca scraper, scanner e client sospetti noti tramite il loro User-Agent.

- **Abilita blocco user-agent** — attiva il filtro UA.
- **Blocca user-agent vuoti** — rifiuta le richieste che non inviano alcun User-Agent.
- **User-agent extra da bloccare (sottostringhe)** — una sottostringa per riga; unita a una lista interna sensata di scraper e scanner noti.



Enable user-agent blocking Yes No

Block empty user-agents Yes No

Extra blocked user-agent substrings (one per line)

Merged with a sensible built-in list (known scrapers, scanners, empty/suspicious agents).

Rate limiting

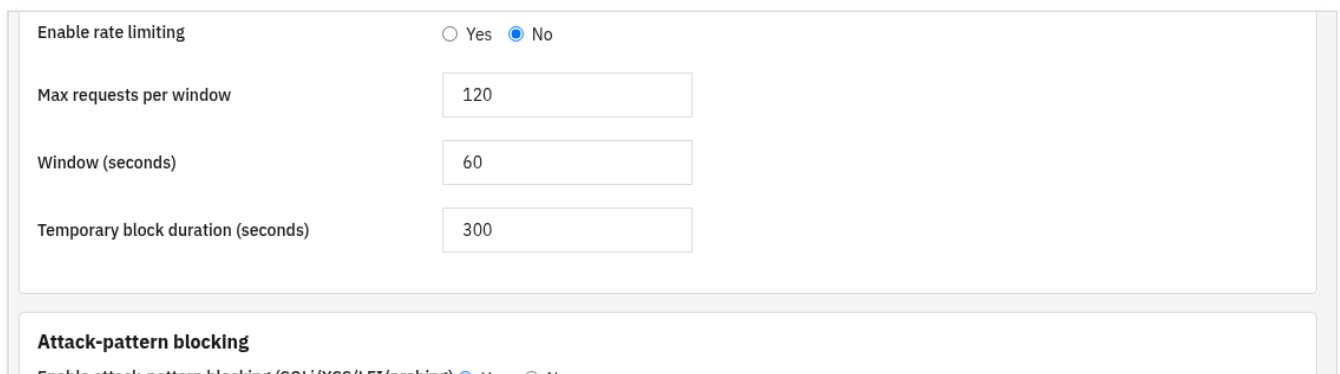
Enable rate limiting Yes No

Bot malevoli / user-agent — lista interna più le tue sottostringhe

Rate limiting

Limita i client che inviano troppe richieste in poco tempo.

- **Abilita rate limiting** — attiva il limitatore.
- **Max richieste per finestra** — quante richieste può inviare un IP prima di essere limitato.
- **Finestra (secondi)** — l'intervallo entro cui vengono contate le richieste.
- **Durata blocco temporaneo (secondi)** — per quanto tempo resta bloccato l'IP.



Enable rate limiting Yes No

Max requests per window

Window (seconds)

Temporary block duration (seconds)

Attack-pattern blocking

Enable attack-pattern blocking (SQLi/XSS/LEET/probing) Yes No

Rate limiting — richieste, finestra e durata del blocco

Blocco pattern di attacco

Rileva e blocca le firme di attacco più comuni nelle richieste.

- **Abilita blocco pattern di attacco** — blocca pattern SQLi, XSS, LFI e probing.
- Aggiungi pattern personalizzati, o metti in whitelist URL legittimi che altrimenti corrisponderebbero, nella scheda **Regole e whitelist**.

Enable attack-pattern blocking (SQLi/XSS/LFI/probing) Yes No

Add custom patterns or whitelist legitimate URLs under the "Rules & whitelist" tab.

Back-office login protection

Enable login protection Yes No

Blocco pattern di attacco — SQLi / XSS / LFI / probing

Protezione login back office

Difende il login admin dai tentativi di brute force.

- **Abilita protezione login** — traccia i login falliti del back office per IP e username.
- **Max tentativi falliti, Finestra tentativi (secondi) e Durata blocco (secondi)** — dopo troppi fallimenti nella finestra, la sorgente viene bloccata temporaneamente.
- **Consenti il back office solo da IP in whitelist** — limita l'accesso admin agli IP in whitelist. Assicurati prima che il tuo IP attuale sia in whitelist (la pagina mostra il tuo IP e ti avvisa se non lo è).

Enable login protection Yes No

Max failed attempts

Attempt window (seconds)

Lockout duration (seconds)

Allow back office only from whitelisted IPs Yes No

Make sure your current IP is whitelisted before enabling this.

Maintenance & logging

Lockdown mode (allow only whitelisted IPs) Yes No

Protezione login back office — anti brute force e restrizione per IP

Manutenzione e logging

Modalità lockdown e log delle richieste bloccate.

- **Modalità lockdown** — consenti l'accesso al negozio solo agli IP in whitelist (blocco d'emergenza). Metti prima in whitelist il tuo IP.
- **Registra richieste bloccate** — registra ogni richiesta bloccata (consultabile ed esportabile nella scheda **Log bloccati**).
- **Conservazione log (giorni)** — per quanto tempo vengono mantenute le righe di log.
- **Elimina tutti i dati alla disinstallazione** — se attivo, rimuovendo il modulo vengono cancellati anche regole e log.

Lockdown mode (allow only whitelisted IPs) Yes No

Log blocked requests Yes No

Log retention (days)

Drop all data on uninstall Yes No

[Save settings](#)

Manutenzione e logging — lockdown, log e conservazione

3. Verifica che funzioni

- Nella scheda *Regole e whitelist*, il banner mostra il tuo IP attuale e se è in whitelist — aggiungilo prima di attivare lockdown o solo-whitelist-BO.
- Aggiungi una sottostringa di test come user-agent cattivo, poi richiedi una pagina con quello User-Agent — dovrebbe essere bloccata e comparire nel *Log bloccati*.
- Apri la scheda *Log bloccati*: le richieste bloccate compaiono con IP, Paese, motivo e URI; puoi filtrare, esportare in CSV o svuotare il log.
- La scheda *Protezione login* elenca i login falliti del back office e permette di sbloccare un lockout con un clic.

4. Domande frequenti

Rischio di bloccare me stesso?

La scheda Regole mostra sempre il tuo IP attuale e ti avvisa se non è in whitelist. Mettilo in whitelist prima di attivare lockdown o solo-whitelist-BO e non potrai bloccarti.

Il blocco per Paese richiede un servizio esterno?

No. Legge un header Paese del CDN quando sei dietro proxy/CDN, oppure il tuo database MaxMind GeoLite2. Nessun dato GeoIP è incluso e nessuna chiamata esce dal tuo server.

Rallenta il negozio?

No. I controlli sono leggeri e vengono eseguiti all'inizio della richiesta; i visitatori legittimi non vengono influenzati.

Devo modificare il tema?

No. Il firewall funziona tramite hook standard ed è compatibile con qualsiasi tema.

