Total Security Guide d'utilisation

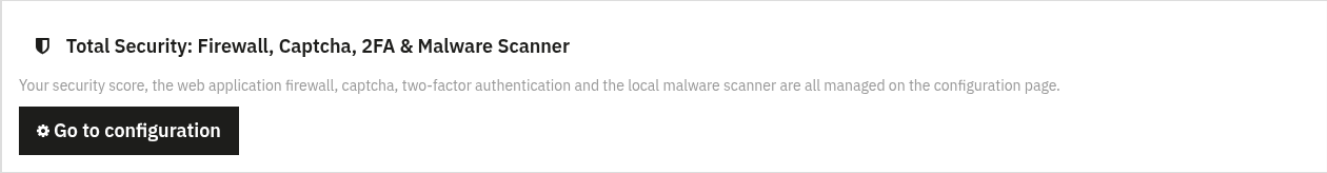
Module PrestaShop · Compatible avec PrestaShop 1.7 → 9

Pare-feu, captcha, 2FA et scanner de malwares, en un seul module

Total Security réunit dans un seul module un pare-feu applicatif, un captcha pour les formulaires de la boutique, l'authentification à deux facteurs (2FA) pour le back-office et les clients, un scanner local de malwares/webshells et un score de sécurité en temps réel qui vous indique quoi améliorer. Tout s'exécute sur votre propre serveur : rien ne quitte votre boutique. Aucun code, aucune modification de thème.

1. Installation

1. Dans le back-office, allez dans **Modules → Gestionnaire de modules → Ajouter un module** et sélectionnez le fichier ZIP du module.
2. Une fois le module installé, cliquez sur **Configurer**. Un court panneau s'ouvre avec un bouton **Aller à la configuration** qui mène à la page complète.



Le panneau Configurer ouvre la page de configuration complète

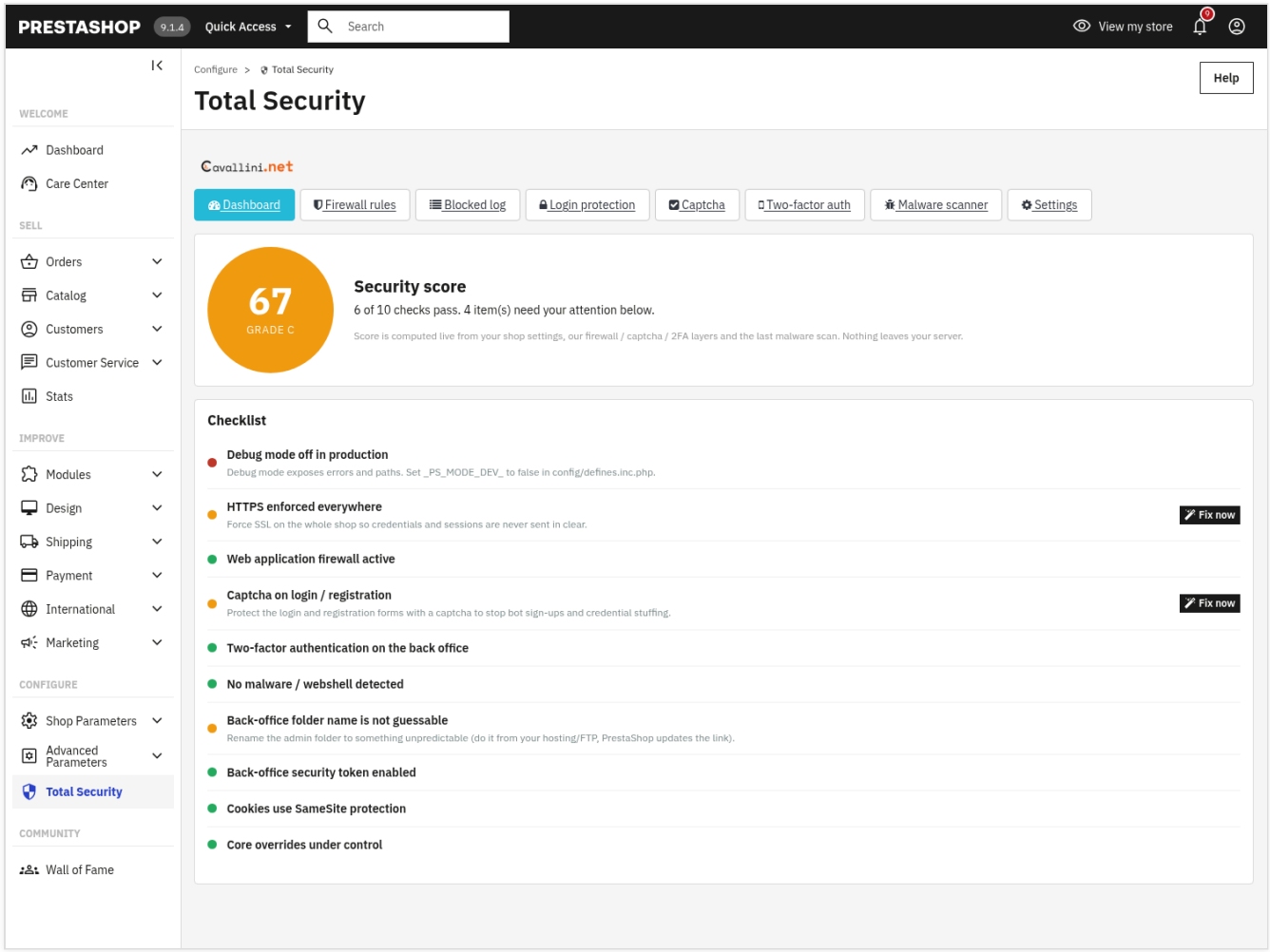
> **Les mises à jour sont automatiques.** Les mises à jour sont incluses. Les domaines de développement (`.local` , `.test` , `localhost`) sont toujours autorisés. Quand une nouvelle version est disponible, elle s'affiche directement dans le module.

2. Configuration — les onglets

La page du module est organisée en onglets en haut de l'écran : **Dashboard**, **Règles du pare-feu**, **Journal des blocages**, **Protection des connexions**, **Captcha**, **Authentification à deux facteurs**, **Scanner de malwares** et **Paramètres**.

Dashboard score de sécurité

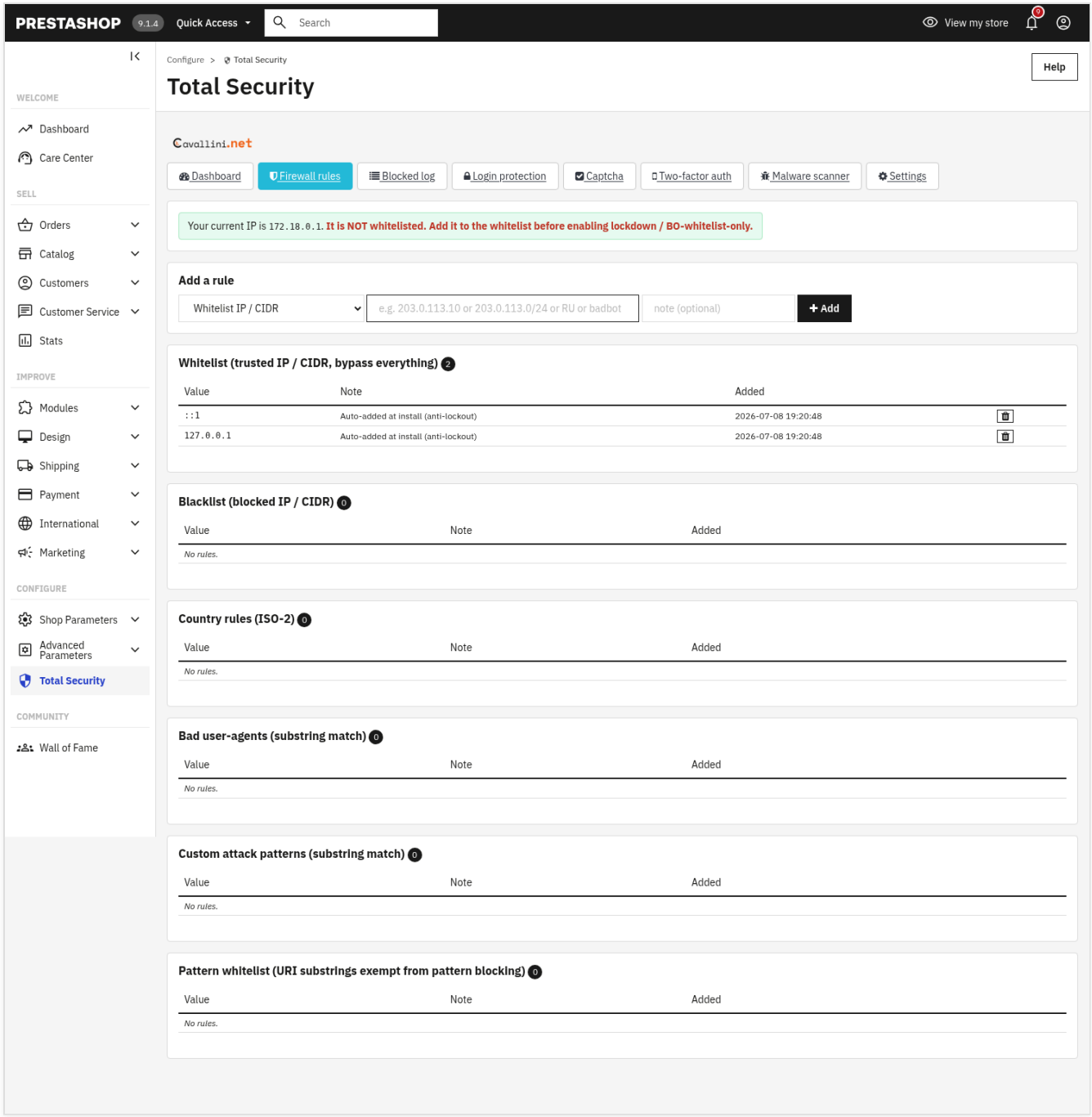
Un **score de sécurité** en temps réel avec une note en lettre (A/B/C/D), calculé à partir des réglages de votre boutique, des couches pare-feu/captcha/2FA et du dernier scan de malwares (rien ne quitte votre serveur). En dessous, une **Checklist** des contrôles de sécurité (exemples visibles : mode debug désactivé en production, HTTPS forcé partout, pare-feu applicatif actif, captcha sur la connexion/l'inscription, authentification à deux facteurs sur le back-office, aucun malware/webshell détecté, nom du dossier back-office non devinable, jeton de sécurité du back-office activé). Les éléments à corriger affichent un raccourci **Corriger maintenant** qui mène directement au réglage concerné.



Dashboard — score de sécurité et checklist

Règles du pare-feu

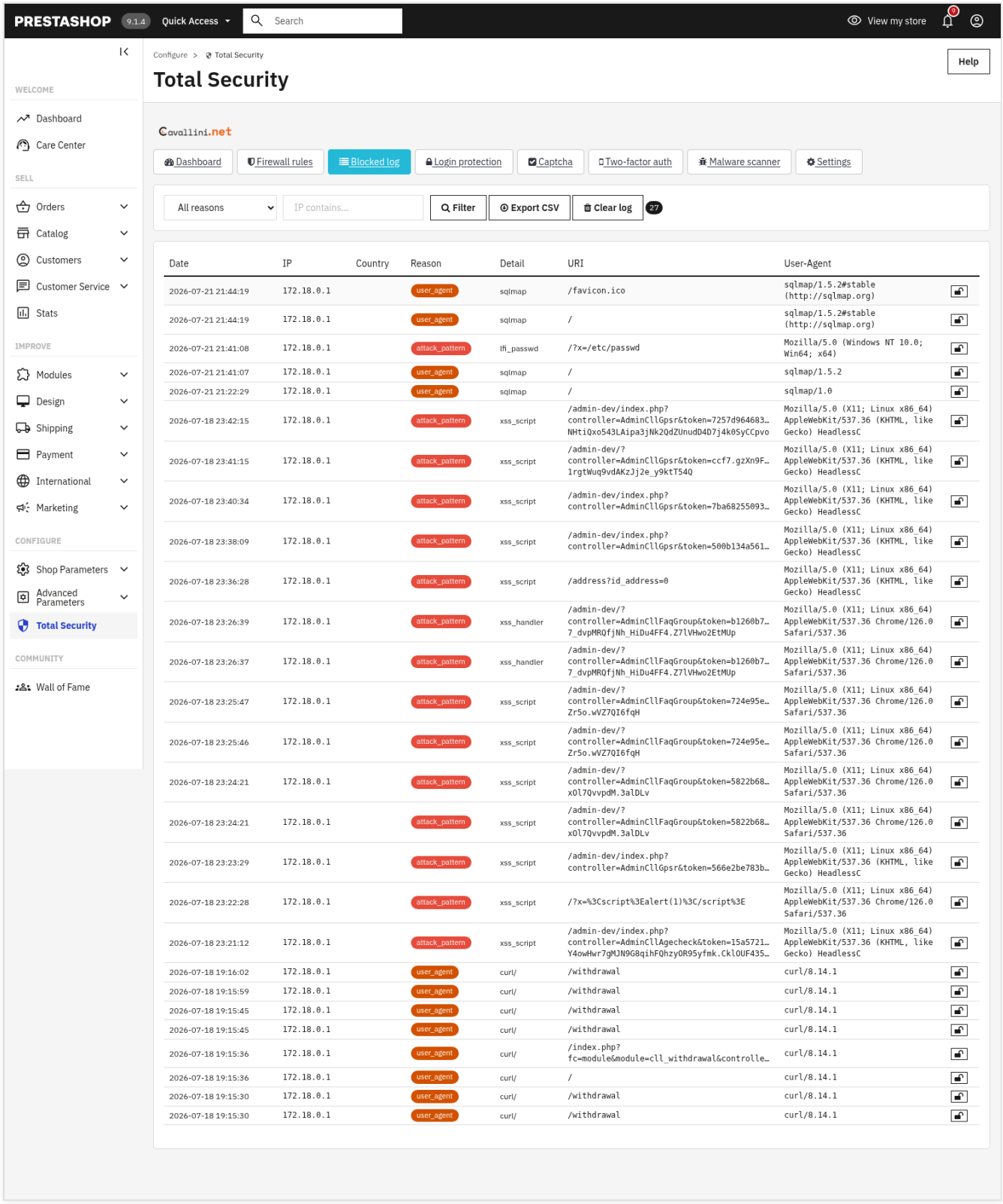
Ajoutez et gérez les listes de règles avec un seul formulaire **Ajouter une règle** : **Liste blanche IP/CIDR** (adresses de confiance, qui contournent tous les contrôles), **Liste noire IP/CIDR** (adresses bloquées), **Règles par pays** (codes ISO-2), **User-agents indésirables** (correspondance par sous-chaîne), **Motifs d'attaque personnalisés** (correspondance par sous-chaîne), et une **Liste blanche de motifs** (sous-chaînes d'URI exemptées du blocage par motif). Une bannière affiche votre IP actuelle et vous avertit de la mettre en liste blanche avant d'activer le mode verrouillage ou le back-office réservé aux IP en liste blanche, afin de ne jamais vous retrouver bloqué à l'extérieur.



Règles du pare-feu — liste blanche, liste noire, pays, user-agents et motifs

Journal des blocages

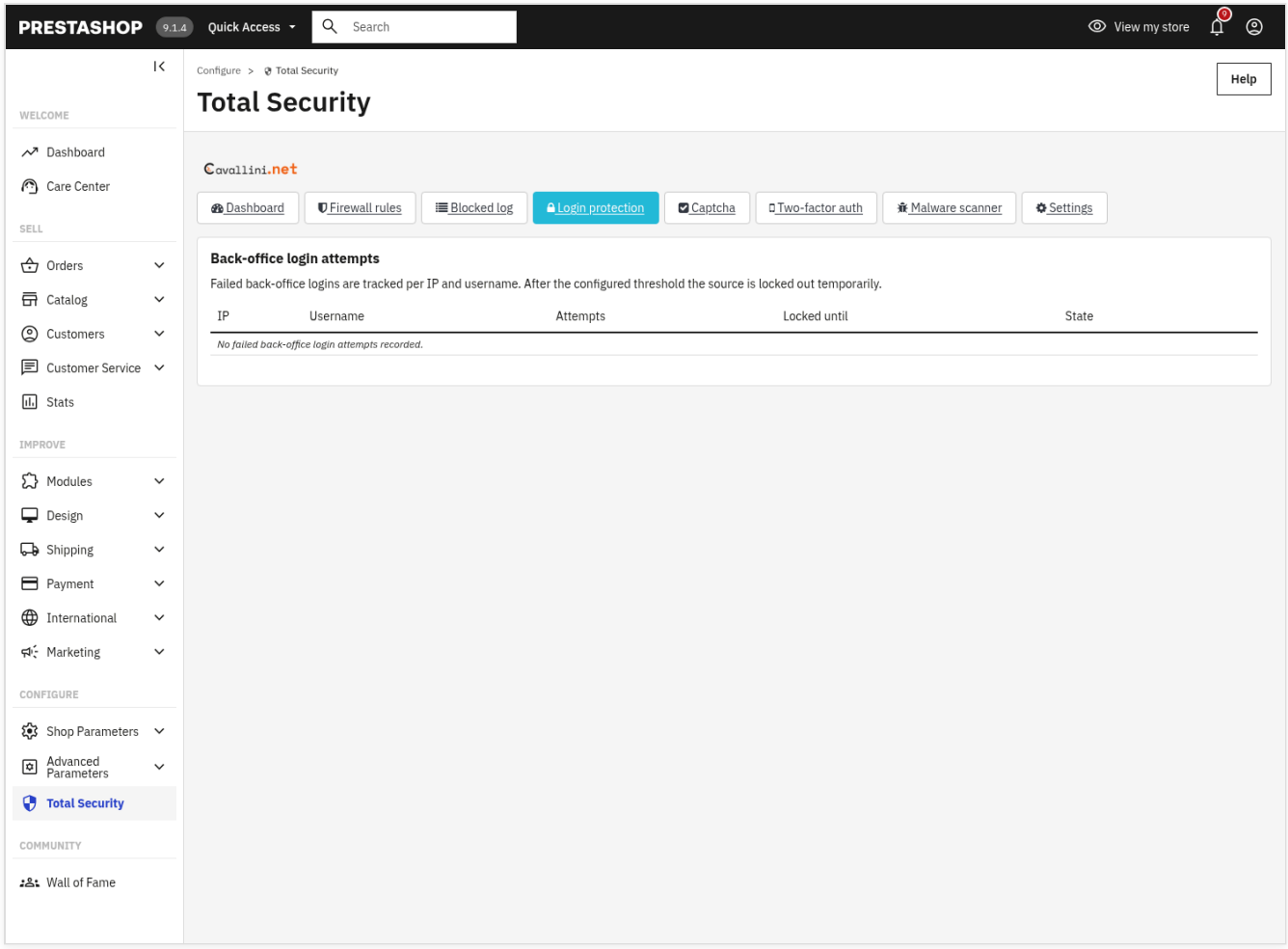
Chaque requête bloquée est enregistrée avec la date, l'IP, le pays, le motif (par ex. `user_agent`, `attack_pattern`, `ip`, `rate`, `login`), le détail, l'URI demandée et le user-agent. Filtrez par motif ou par IP, **Exporter en CSV**, **Vider le journal**, ou débloquez une IP directement depuis cette page.



Journal des blocages — filtrer, exporter ou débloquer une IP

Protection des connexions

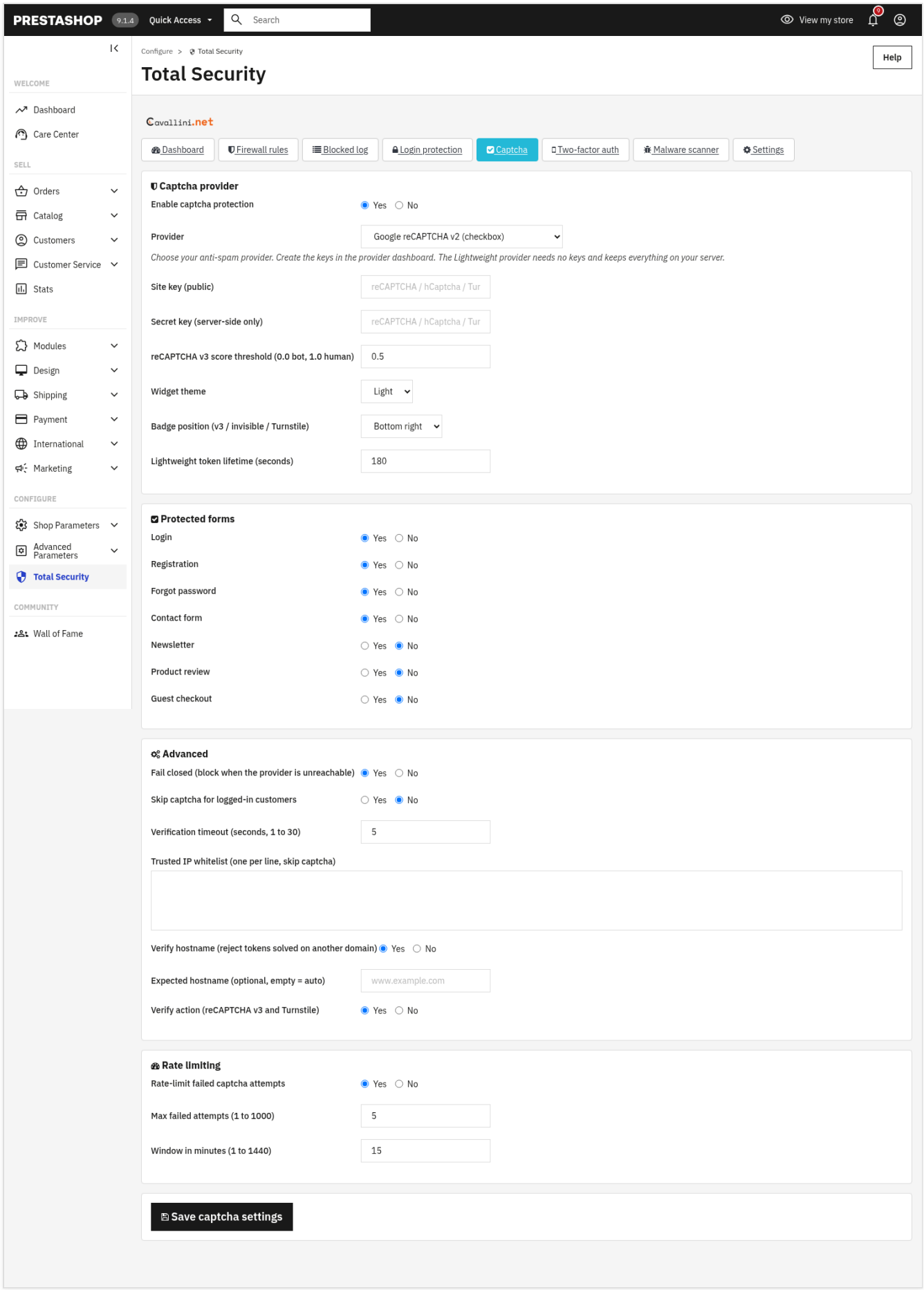
Surveille les tentatives de connexion au back-office et bloque un compte/une IP après trop de tentatives échouées dans une fenêtre de temps donnée ; vous pouvez débloquer une entrée manuellement. Configurez les seuils dans Paramètres (Protection des connexions au back-office).



Protection des connexions — tentatives échouées et blocages actifs

Captcha

- **Fournisseur de captcha** — choisissez Google reCAPTCHA v2 (case à cocher), reCAPTCHA v3, hCaptcha, Cloudflare Turnstile, ou le fournisseur **Lightweight** qui ne nécessite aucune clé et reste entièrement sur votre serveur.
- **Clé de site / Clé secrète** — depuis le tableau de bord du fournisseur choisi, **seuil de score reCAPTCHA v3**, **thème du widget**, **position du badge**, **durée de vie du jeton** pour le fournisseur Lightweight.
- **Formulaires protégés** — Connexion, Inscription, Mot de passe oublié, Formulaire de contact, Newsletter, Avis produit, Commande invité (chacun activable/désactivable).
- **Avancé** — **Fail closed** (bloquer quand le fournisseur est injoignable), **Ignorer le captcha pour les clients connectés**, **Délai de vérification**, **Liste blanche d'IP de confiance**, **vérification du hostname**, **vérification de l'action**.
- **Rate limiting** — limite les tentatives de captcha échouées avec un maximum et une fenêtre de temps.

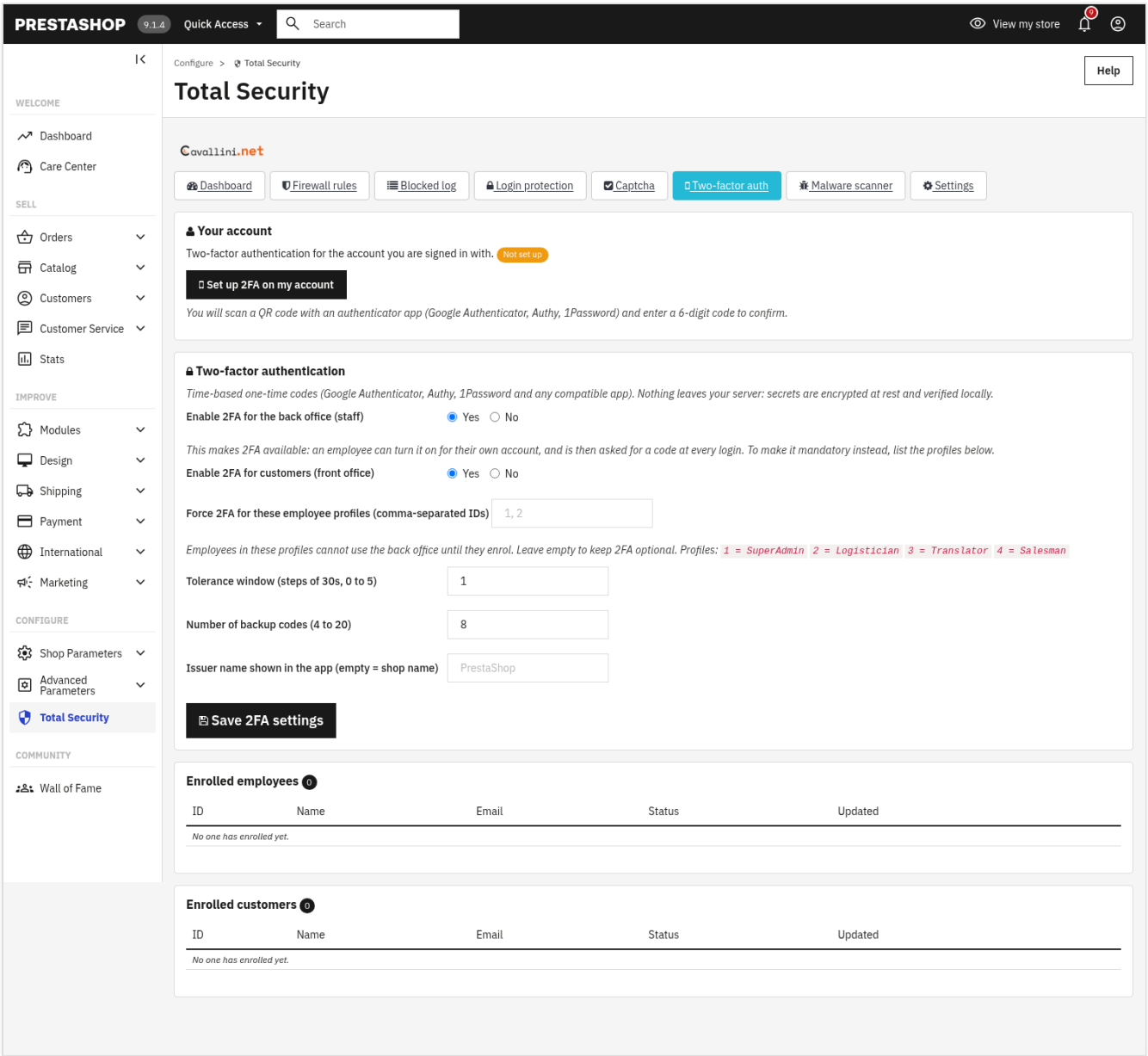


Captcha — fournisseur, formulaires protégés et rate limiting

Authentification à deux facteurs (2FA)

Codes à usage unique basés sur le temps (Google Authenticator, Authy, 1Password et toute application compatible). Rien ne quitte votre serveur : les secrets sont chiffrés au repos et vérifiés localement.

- **Votre compte** — activez la 2FA pour le compte avec lequel vous êtes connecté (scannez un QR code, saisissez un code à 6 chiffres).
- **Activer la 2FA pour le back-office** (personnel) et/ou **pour les clients** (front-office).
- **Forcer la 2FA pour des profils employé spécifiques**, par ID (1 = SuperAdmin, 2 = Logisticien, 3 = Traducteur, 4 = Vendeur) ; les profils listés ne peuvent pas utiliser le back-office tant qu'ils ne se sont pas inscrits.
- **Fenêtre de tolérance**, **nombre de codes de secours**, **nom de l'émetteur** affiché dans l'application.
- **Employés inscrits** et **clients inscrits** sont listés et peuvent être réinitialisés.

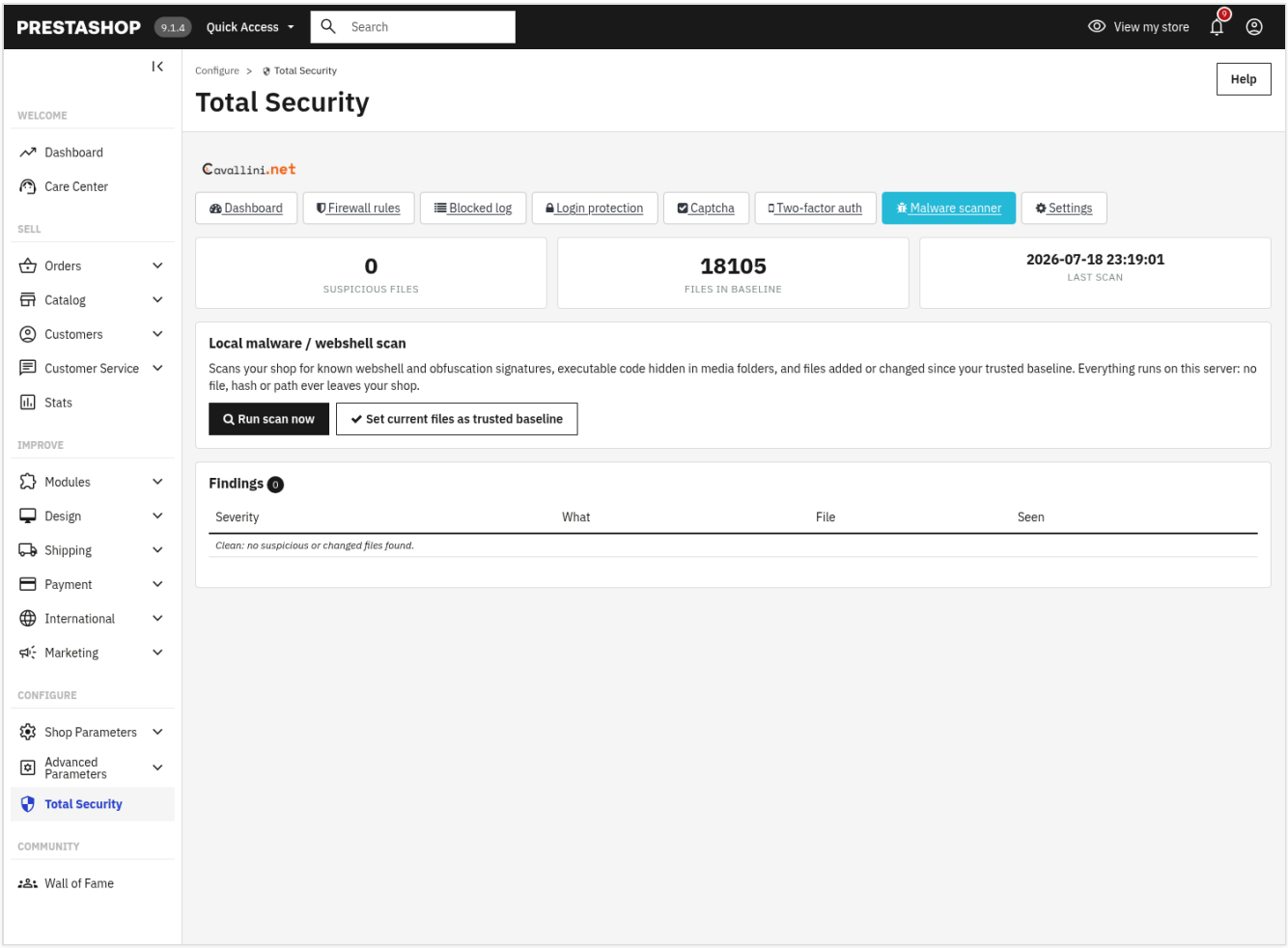


2FA — inscription, profils forcés et utilisateurs inscrits

Scanner de malwares

Analyse locale de malwares/webshells : recherche les signatures connues de webshells et de code obfusqué, le code exécutable caché dans les dossiers médias, et les fichiers ajoutés ou modifiés depuis votre base de référence de confiance. Tout s'exécute sur le serveur : aucun fichier, hash ou chemin ne quitte jamais la boutique.

- **Métriques** — fichiers suspects, fichiers en référence, dernière analyse.
- **Lancer l'analyse maintenant** et **Définir les fichiers actuels comme base de référence de confiance**.
- Les résultats sont listés avec la **gravité**, le **quoi**, le **fichier** et le **quand**.

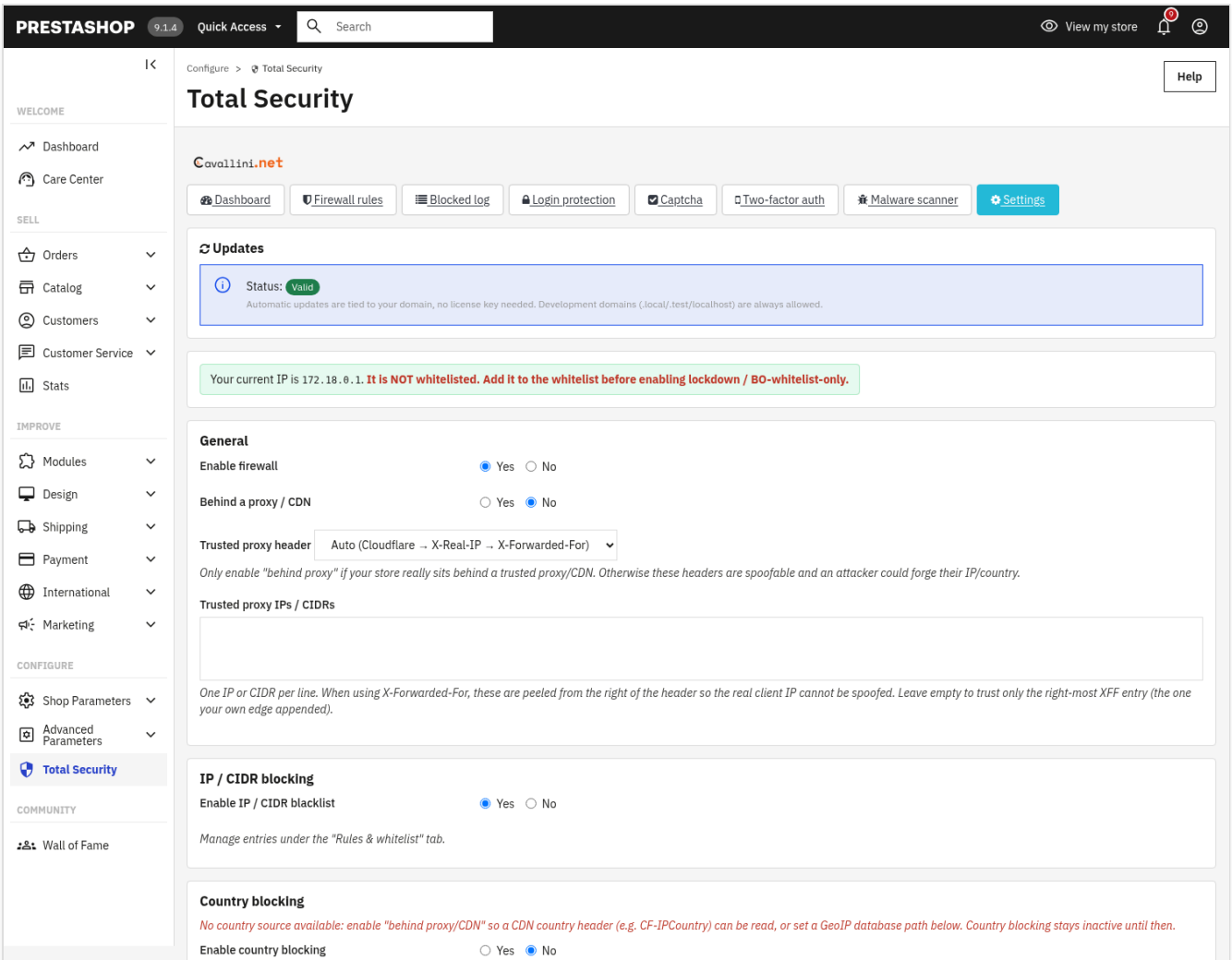


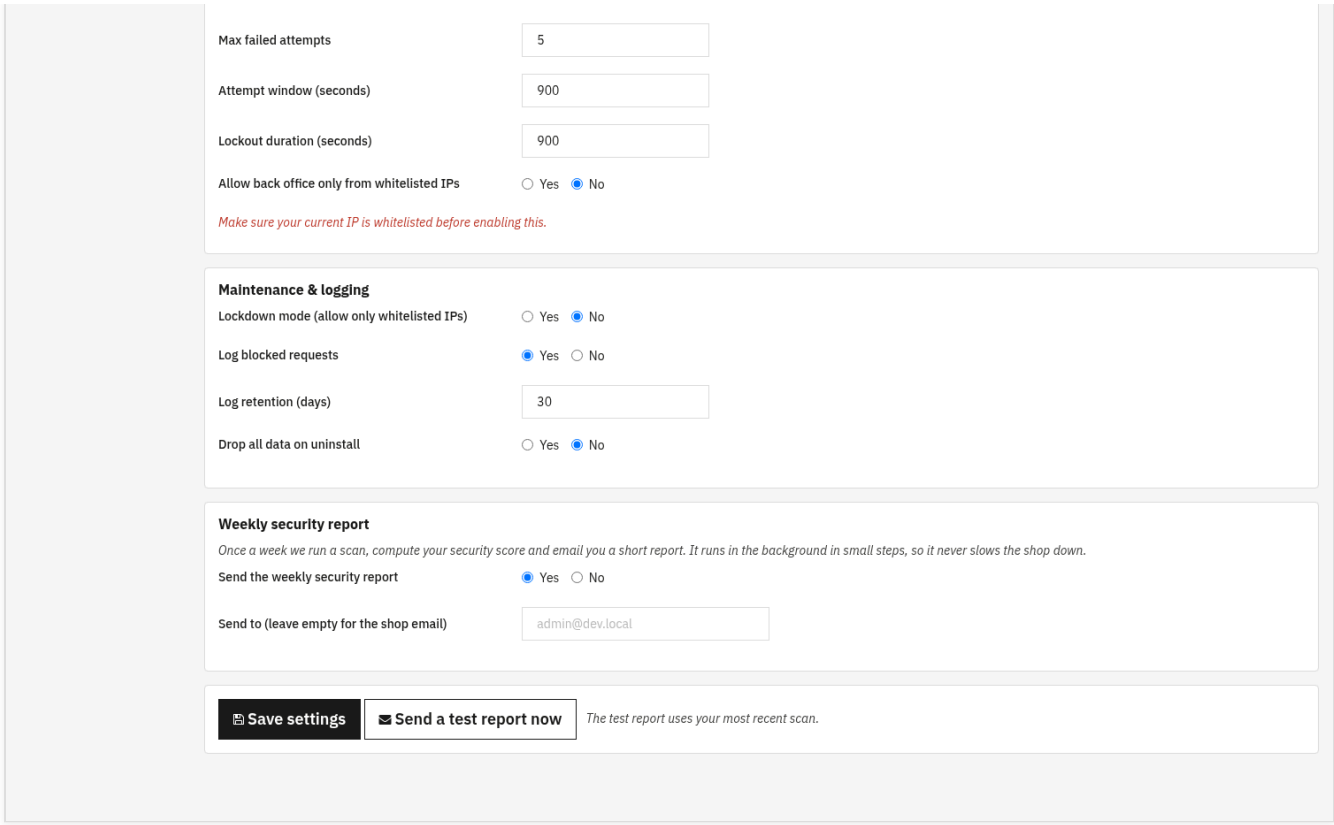
Scanner de malwares — métriques, analyse et résultats

Paramètres configuration du pare-feu

La configuration propre du pare-feu, regroupée par section.

- **Général** — Activer le pare-feu ; **Derrière un proxy/CDN** avec un en-tête de proxy de confiance et des IP/CIDR de proxy de confiance — n'activez cette option que derrière un proxy réellement fiable, sinon les en-têtes IP/pays peuvent être falsifiés.
- **Blocage IP/CIDR**.
- **Blocage par pays** — mode liste noire ou liste blanche, codes ISO-2, chemin optionnel vers une base MaxMind GeoLite2 ou un en-tête CDN indiquant le pays — la base n'est jamais fournie avec le module, pour des raisons de licence.
- **Bots / user-agents indésirables** — activer le blocage par user-agent, bloquer les user-agents vides, sous-chaînes supplémentaires à bloquer fusionnées avec une liste intégrée.
- **Rate limiting** — nombre maximum de requêtes par fenêtre, durée de la fenêtre en secondes, durée du blocage temporaire.
- **Blocage par motifs d'attaque** — SQLi/XSS/LFI/probing.
- **Protection des connexions au back-office** — nombre maximum de tentatives échouées, fenêtre de tentative, durée du blocage, autoriser le back-office uniquement depuis les IP en liste blanche.
- **Maintenance et journalisation** — **Mode verrouillage** (autoriser uniquement les IP en liste blanche), journaliser les requêtes bloquées, durée de conservation du journal en jours, supprimer toutes les données à la désinstallation.
- **Rapport de sécurité hebdomadaire** — envoie un court rapport par e-mail ; s'exécute en arrière-plan par petites étapes pour ne jamais ralentir la boutique.

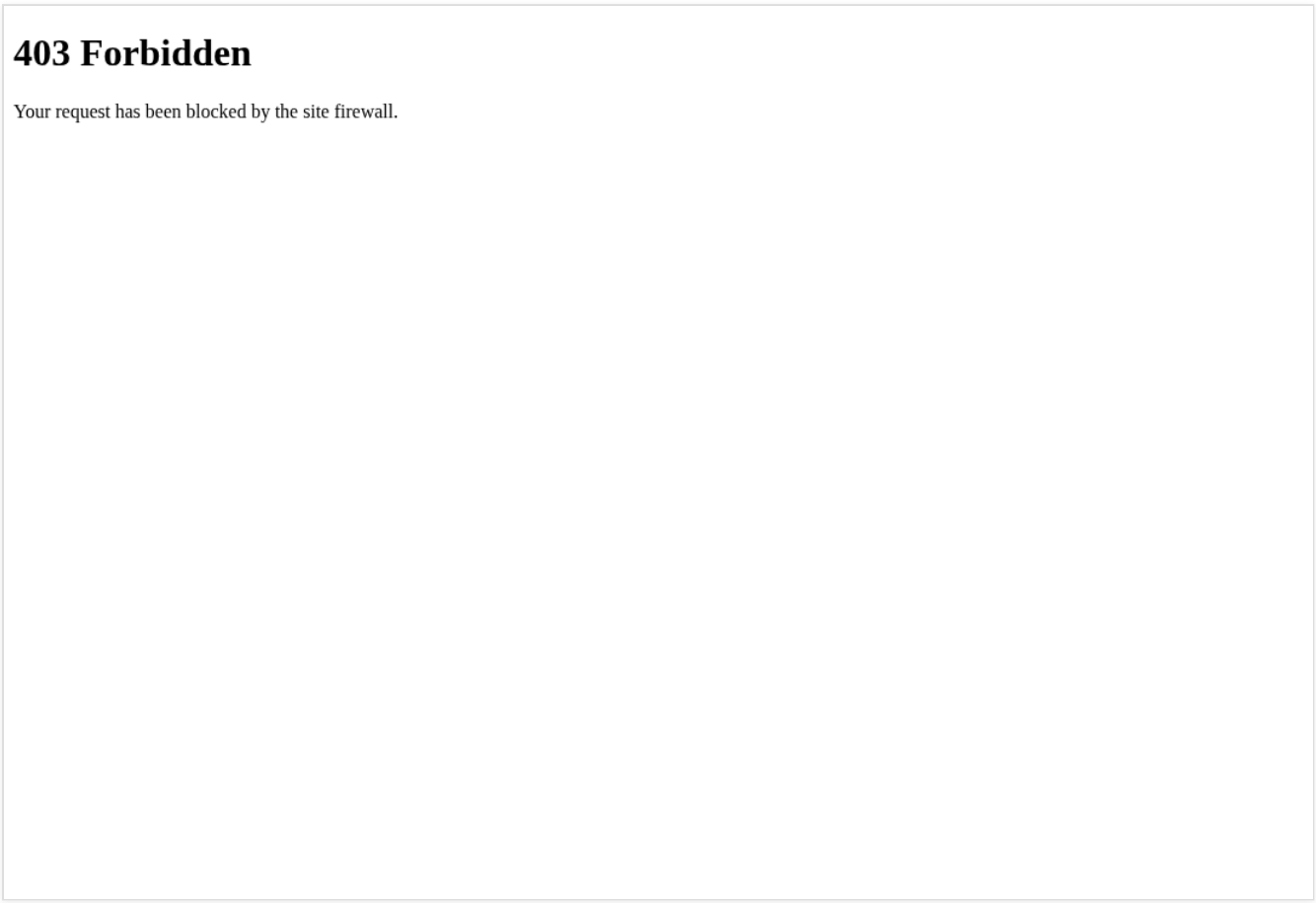

PRESTASHOP
9.1.4
Quick Access
Search
View my store
WELCOME
Dashboard
Care Center
SELL
Orders
Catalog
Customers
Customer Service
Stats
IMPROVE
Modules
Design
Shipping
Payment
International
Marketing
CONFIGURE
Shop Parameters
Advanced Parameters
Total Security
COMMUNITY
Wall of Fame
Configure > Total Security
Total Security
Help
Cavallini.net
Dashboard
Firewall rules
Blocked log
Login protection
Captcha
Two-factor auth
Malware scanner
Settings
Updates
Status: Valid
Automatic updates are tied to your domain, no license key needed. Development domains (.local/.test/localhost) are always allowed.
Your current IP is 172.18.0.1. It is NOT whitelisted. Add it to the whitelist before enabling lockdown / BO-whitelist-only.
General
Enable firewall
Yes
No
Behind a proxy / CDN
Yes
No
Trusted proxy header
Auto (Cloudflare → X-Real-IP → X-Forwarded-For)
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.
Trusted proxy IPs / CIDRs
One IP or CIDR per line. When using X-Forwarded-For, these are peeled from the right of the header so the real client IP cannot be spoofed. Leave empty to trust only the right-most XFF entry (the one your own edge appended).
IP / CIDR blocking
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.
Enable country blocking
Yes
No
Mode
Block-list (block listed countries)
Country codes (ISO-2, comma separated)
RU, CN, KP
GeoIP database path (optional MaxMind GeoLite2 .mmdb)
/path/to/GeoLite2-Country.m
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
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
Max requests per window
120
Window (seconds)
60
Temporary block duration (seconds)
300
Attack-pattern blocking
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



Paramètres — configuration du pare-feu par section

Dans le front-office

Quand le pare-feu bloque une requête, le visiteur voit une simple page 403 « Forbidden — votre requête a été bloquée par le pare-feu du site » : les bots et les scanners n'atteignent jamais votre boutique.



Dans le front-office — la page 403 affichée quand le pare-feu bloque une requête

3. Vérifier que tout fonctionne

- Ouvrez le *Dashboard* et consultez votre score de sécurité et la checklist.
- Envoyez une requête avec un user-agent semblable à celui d'un scanner (ou une URL de probing) et vérifiez que vous obtenez la page de blocage 403 et une nouvelle ligne dans le *Journal des blocages*.
- Après plusieurs échecs de connexion au back-office, le compte/l'IP est bloqué dans *Protection des connexions*.
- Activez le captcha et vérifiez qu'il apparaît sur le formulaire de connexion/d'inscription.
- Configurez la 2FA sur votre compte et reconnectez-vous avec un code à 6 chiffres.
- Lancez le *Scanner de malwares* et consultez les résultats.

4. FAQ

Est-ce que cela ralentit la boutique ?

Non : le pare-feu s'exécute en premier avec des vérifications légères et indexées ; le scanner et le rapport hebdomadaire s'exécutent en arrière-plan.

Est-ce que je risque de me retrouver bloqué à l'extérieur ?

Mettez d'abord votre IP actuelle en liste blanche (la page vous avertit, et `127.0.0.1` / `::1` sont en liste blanche dès l'installation) ; n'activez le mode verrouillage ou le back-office réservé aux IP en liste blanche qu'après.

Des données quittent-elles mon serveur ?

Non : le pare-feu, l'option de captcha Lightweight, les secrets 2FA et le scanner de malwares s'exécutent tous localement sur votre serveur.

Remplace-t-il des modules séparés de pare-feu / captcha / 2FA ?

Oui : c'est la suite de sécurité unique et unifiée.

Dois-je modifier mon thème ?

Non : il fonctionne via les hooks standards et est compatible avec tous les thèmes.
