Total Security Guía de uso

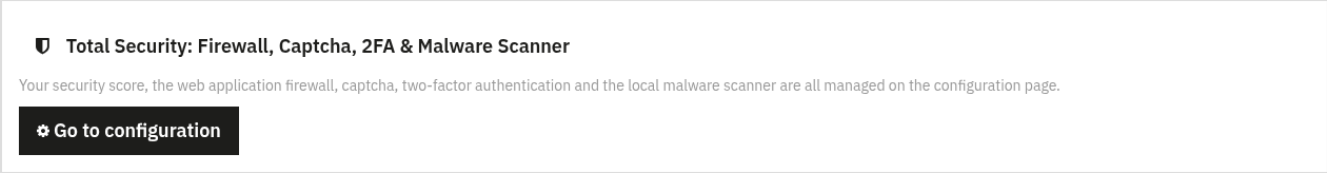
Módulo PrestaShop · Compatible con PrestaShop 1.7 → 9

Cortafuegos, captcha, 2FA y escáner de malware, en un solo módulo

Total Security reúne en un solo módulo un cortafuegos de aplicaciones web, un captcha para los formularios de la tienda, la autenticación de dos factores (2FA) para el back office y los clientes, un escáner local de malware/webshells y una puntuación de seguridad en tiempo real que te indica qué mejorar. Todo se ejecuta en tu propio servidor: nada sale de tu tienda. Sin necesidad de programar, sin modificar el tema.

1. Instalación

1. En el back office ve a **Módulos → Gestor de módulos → Subir un módulo** y selecciona el ZIP del módulo.
2. Una vez instalado, haz clic en **Configurar**. Se abre un breve panel con un botón **Ir a la configuración** que lleva a la página completa.



El panel Configurar abre la página de configuración completa

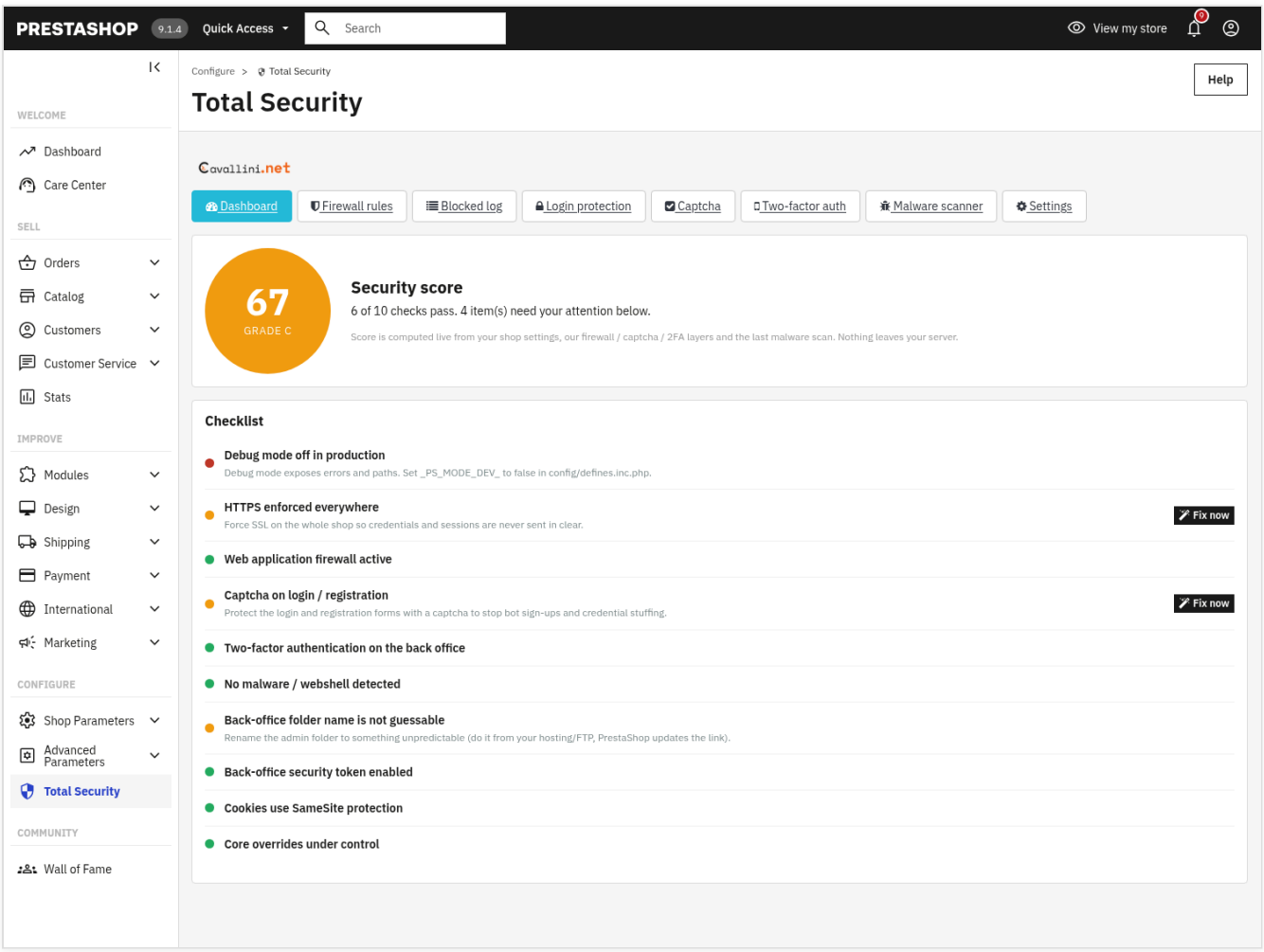
> **Las actualizaciones son automáticas.** Las actualizaciones están incluidas. Los dominios de desarrollo (`.local` , `.test` , `localhost`) siempre están permitidos. Cuando hay una nueva versión disponible, se muestra directamente dentro del módulo.

2. Configuración — las pestañas

La página del módulo está organizada en pestañas en la parte superior: **Dashboard**, **Reglas del cortafuegos**, **Registro de bloqueos**, **Protección de inicio de sesión**, **Captcha**, **Autenticación de dos factores**, **Escáner de malware** y **Configuración**.

Dashboard puntuación de seguridad

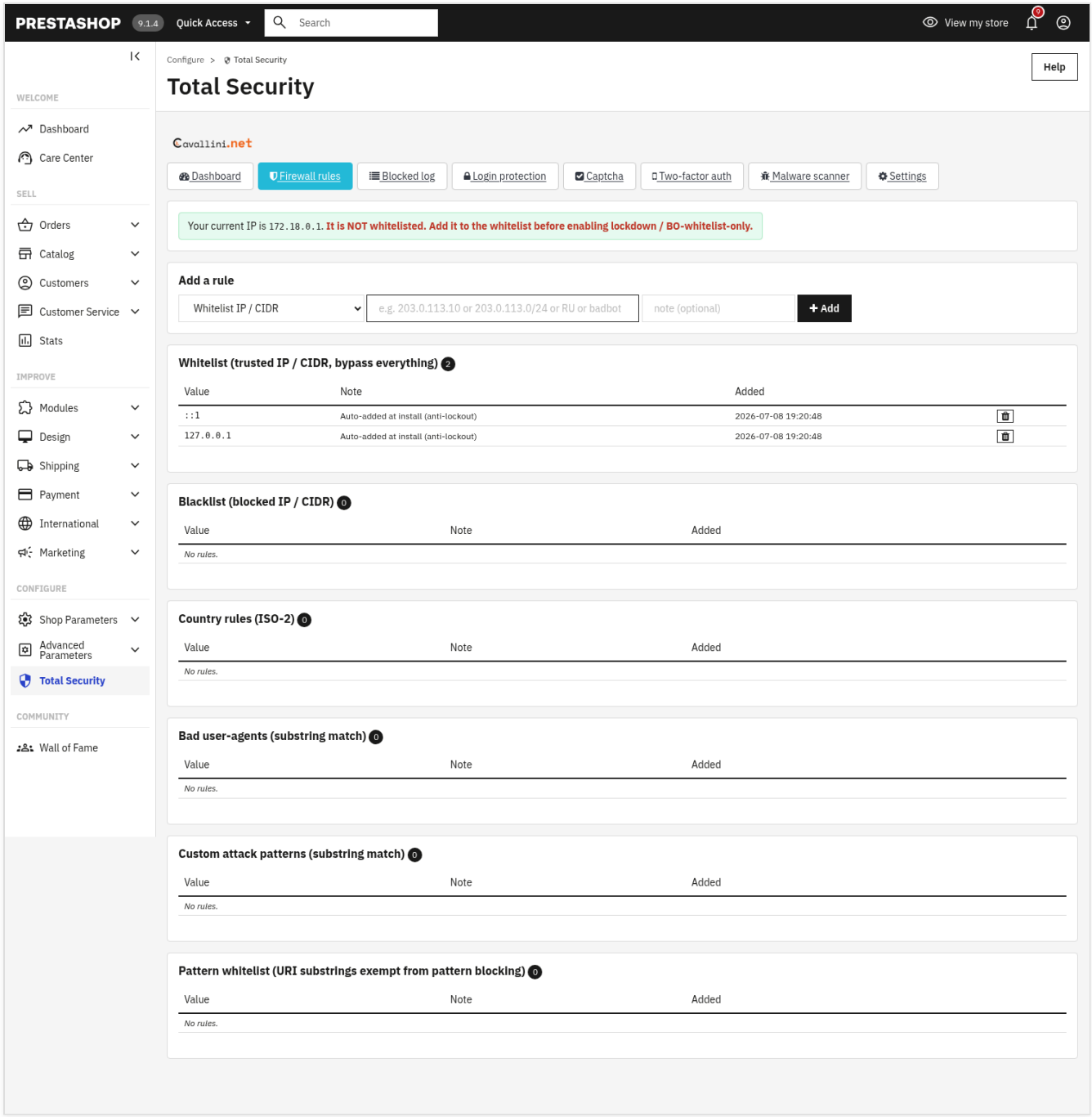
Una **puntuación de seguridad** en tiempo real con una nota en letra (A/B/C/D), calculada a partir de los ajustes de tu tienda, las capas de cortafuegos/captcha/2FA y el último análisis de malware (nada sale de tu servidor). Debajo encontrarás una **Checklist** de comprobaciones de seguridad (ejemplos visibles: modo debug desactivado en producción, HTTPS forzado en todas partes, cortafuegos de aplicaciones activo, captcha en el inicio de sesión/registro, autenticación de dos factores en el back office, ningún malware/webshell detectado, nombre de la carpeta del back office no adivinable, token de seguridad del back office activado). Los elementos que necesitan atención muestran un acceso directo **Corregir ahora** que lleva directamente al ajuste correspondiente.



Dashboard — puntuación de seguridad y checklist

Reglas del cortafuegos

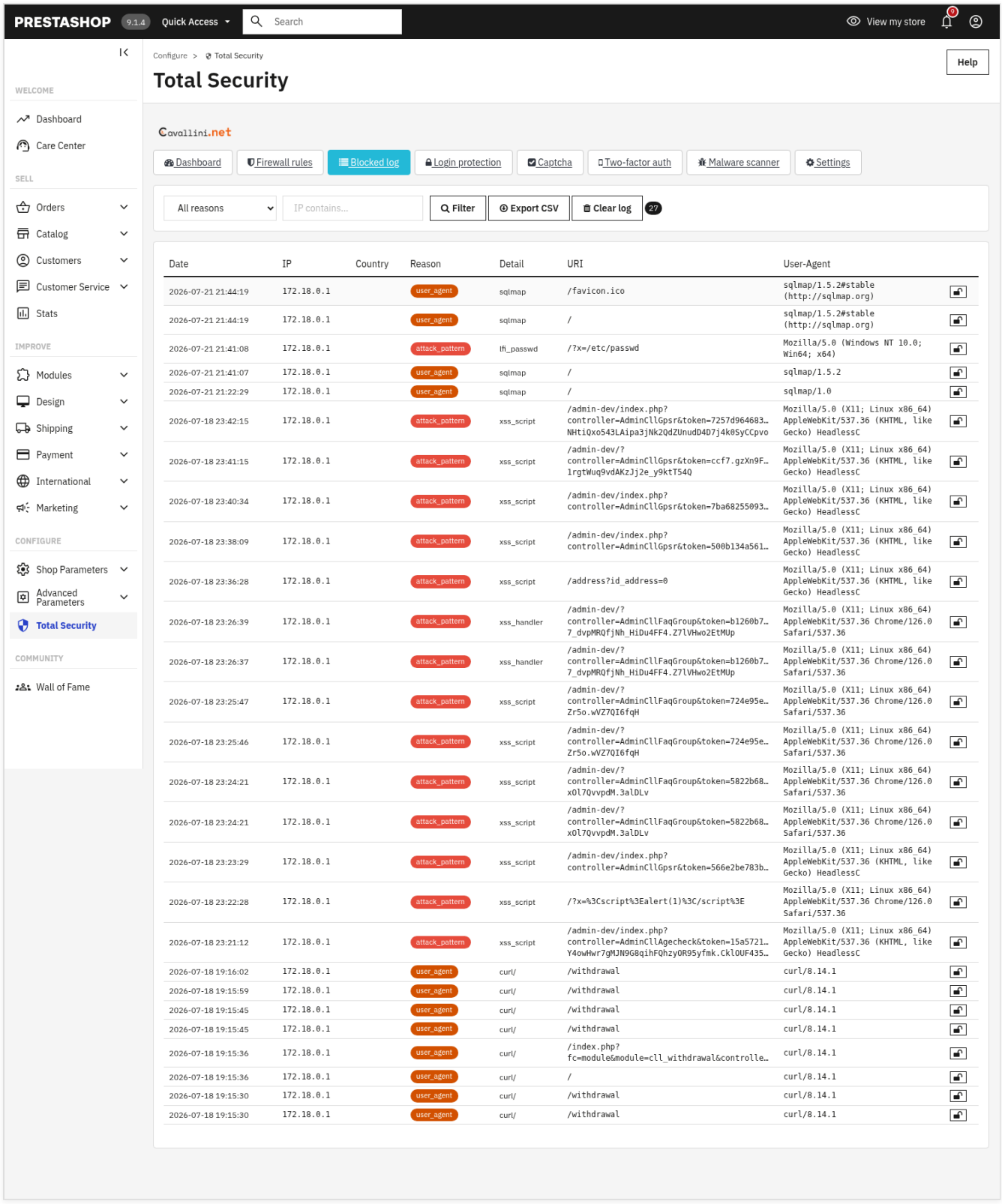
Añade y gestiona las listas de reglas con un único formulario **Añadir una regla**: **Lista blanca IP/CIDR** (direcciones de confianza, que omiten todos los controles), **Lista negra IP/CIDR** (direcciones bloqueadas), **Reglas por país** (códigos ISO-2), **User-agents sospechosos** (coincidencia por subcadena), **Patrones de ataque personalizados** (coincidencia por subcadena) y una **Lista blanca de patrones** (subcadenas de URI exentas del bloqueo por patrón). Un banner muestra tu IP actual y te avisa de añadirla a la lista blanca antes de activar el modo de bloqueo total o el back office restringido a IP en lista blanca, para que nunca te quedes fuera.



Reglas del cortafuegos — lista blanca, lista negra, países, user-agents y patrones

Registro de bloqueos

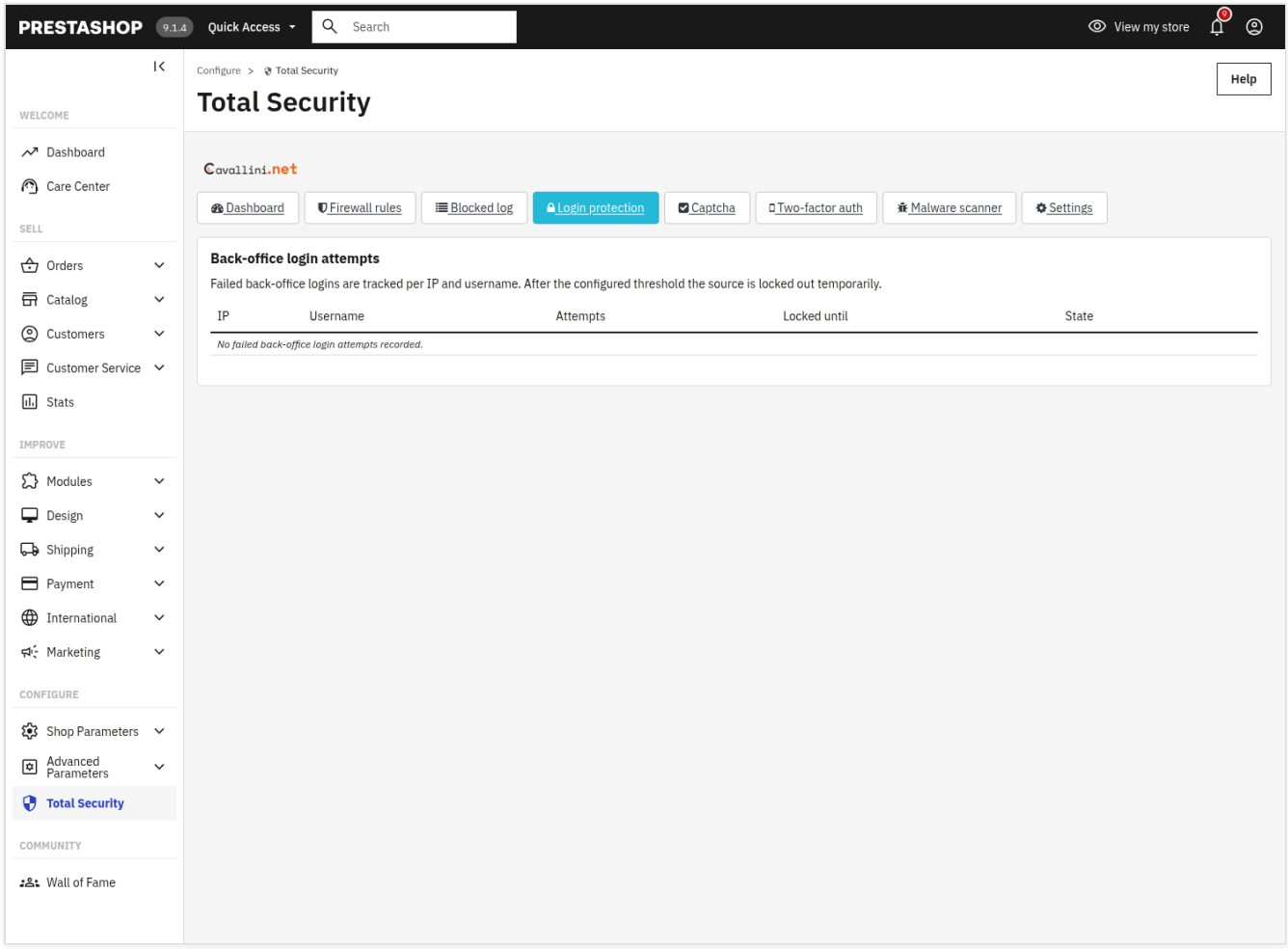
Cada solicitud bloqueada se registra con fecha, IP, país, motivo (por ejemplo `user_agent`, `attack_pattern`, `ip`, `rate`, `login`), detalle, la URI solicitada y el user-agent. Filtra por motivo o IP, **Exportar a CSV**, **Vaciar registro**, o desbloquea una IP directamente desde aquí.



Registro de bloqueos — filtrar, exportar o desbloquear una IP

Protección de inicio de sesión

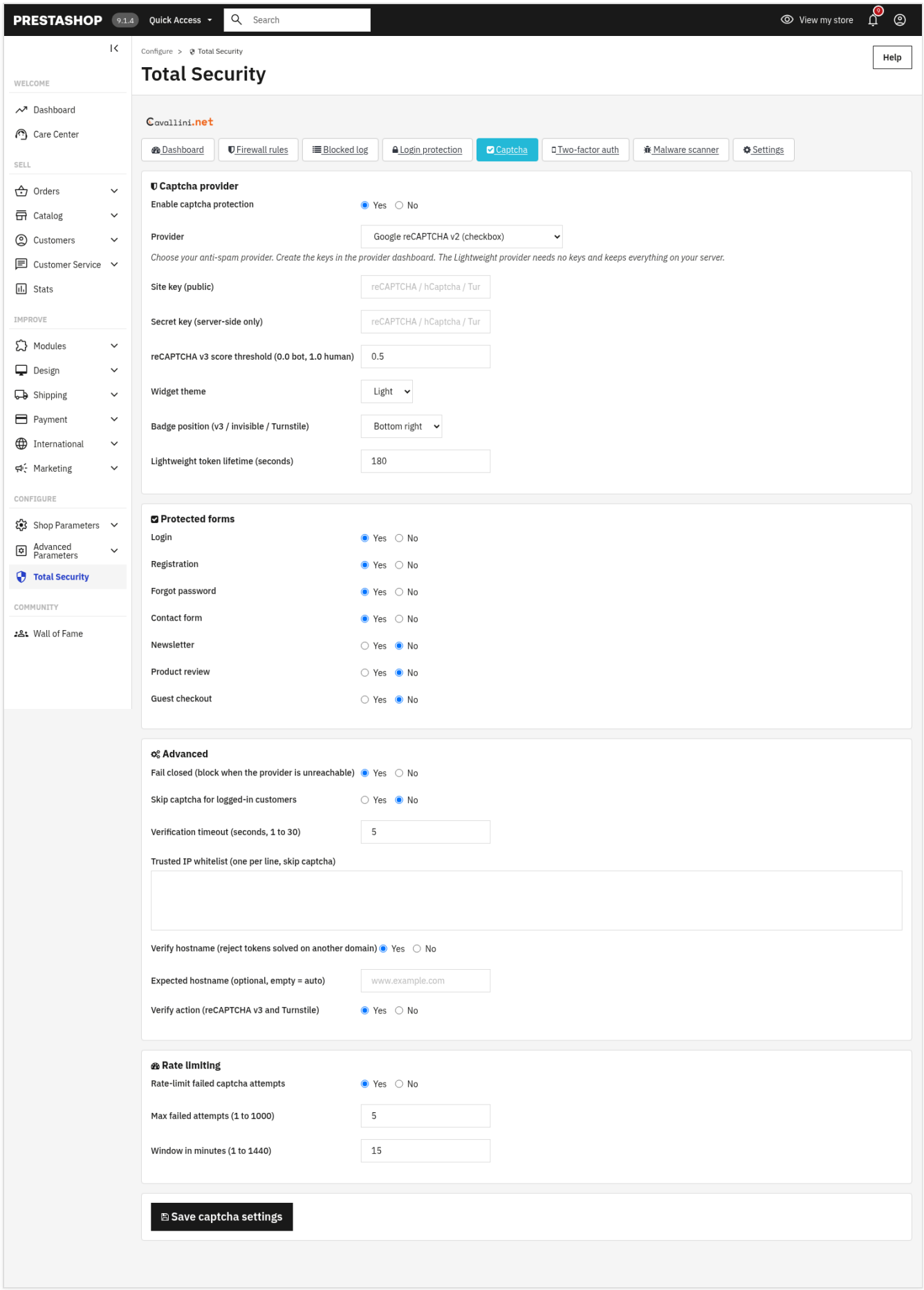
Registra los intentos de inicio de sesión en el back office y bloquea una cuenta/IP tras demasiados intentos fallidos dentro de una ventana de tiempo; puedes desbloquear una entrada manualmente. Configura los umbrales en Configuración (Protección de inicio de sesión del back office).



Protección de inicio de sesión — intentos fallidos y bloqueos activos

Captcha

- **Proveedor de captcha** — elige Google reCAPTCHA v2 (casilla de verificación), reCAPTCHA v3, hCaptcha, Cloudflare Turnstile, o el proveedor **Lightweight**, que no necesita ninguna clave y se mantiene por completo en tu servidor.
- **Clave de sitio / Clave secreta** — desde el panel del proveedor elegido, **umbral de puntuación de reCAPTCHA v3**, **tema del widget**, **posición del badge**, **duración del token** del proveedor Lightweight.
- **Formularios protegidos** — Inicio de sesión, Registro, Contraseña olvidada, Formulario de contacto, Newsletter, Reseña de producto, Compra como invitado (cada uno activable/desactivable).
- **Avanzado** — **Fail closed** (bloquear cuando el proveedor no esté disponible), **Omitir el captcha para clientes con sesión iniciada**, **Tiempo de espera de verificación**, **Lista blanca de IP de confianza**, **verificación de hostname**, **verificación de action**.
- **Rate limiting** — limita los intentos de captcha fallidos con un máximo y una ventana de tiempo.

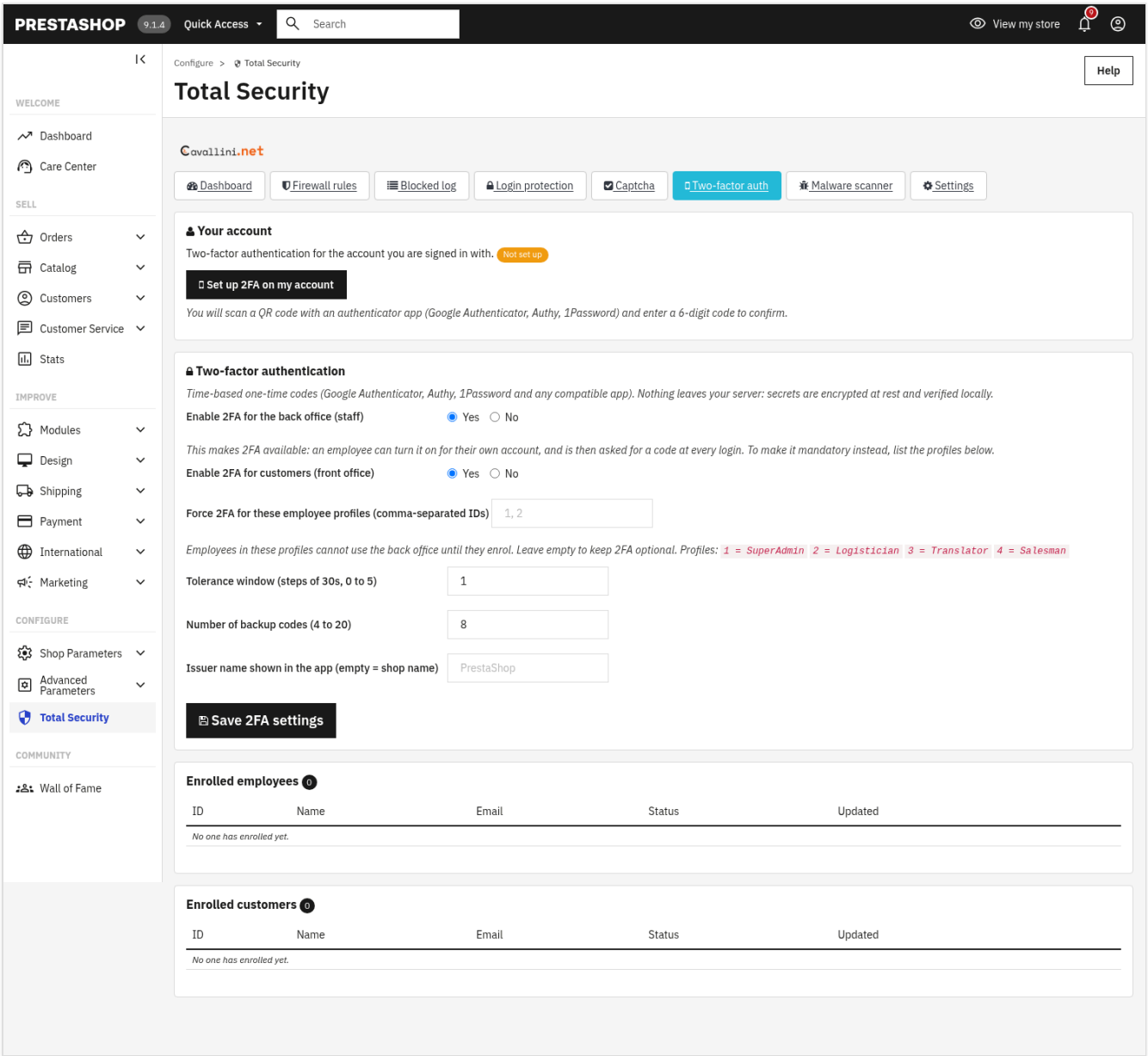


Captcha — proveedor, formularios protegidos y rate limiting

Autenticación de dos factores (2FA)

Códigos de un solo uso basados en el tiempo (Google Authenticator, Authy, 1Password y cualquier aplicación compatible). Nada sale de tu servidor: los secretos se cifran en reposo y se verifican localmente.

- **Tu cuenta** — configura la 2FA para la cuenta con la que has iniciado sesión (escanea un código QR, introduce un código de 6 dígitos).
- **Activar la 2FA para el back office** (personal) y/o **para los clientes** (front office).
- **Forzar la 2FA para perfiles de empleado específicos**, por ID (1 = SuperAdmin, 2 = Logístico, 3 = Traductor, 4 = Vendedor); los perfiles indicados no podrán usar el back office hasta que se registren.
- **Ventana de tolerancia**, **número de códigos de respaldo**, **nombre del emisor** mostrado en la aplicación.
- **Empleados registrados** y **clientes registrados** aparecen listados y se pueden restablecer.

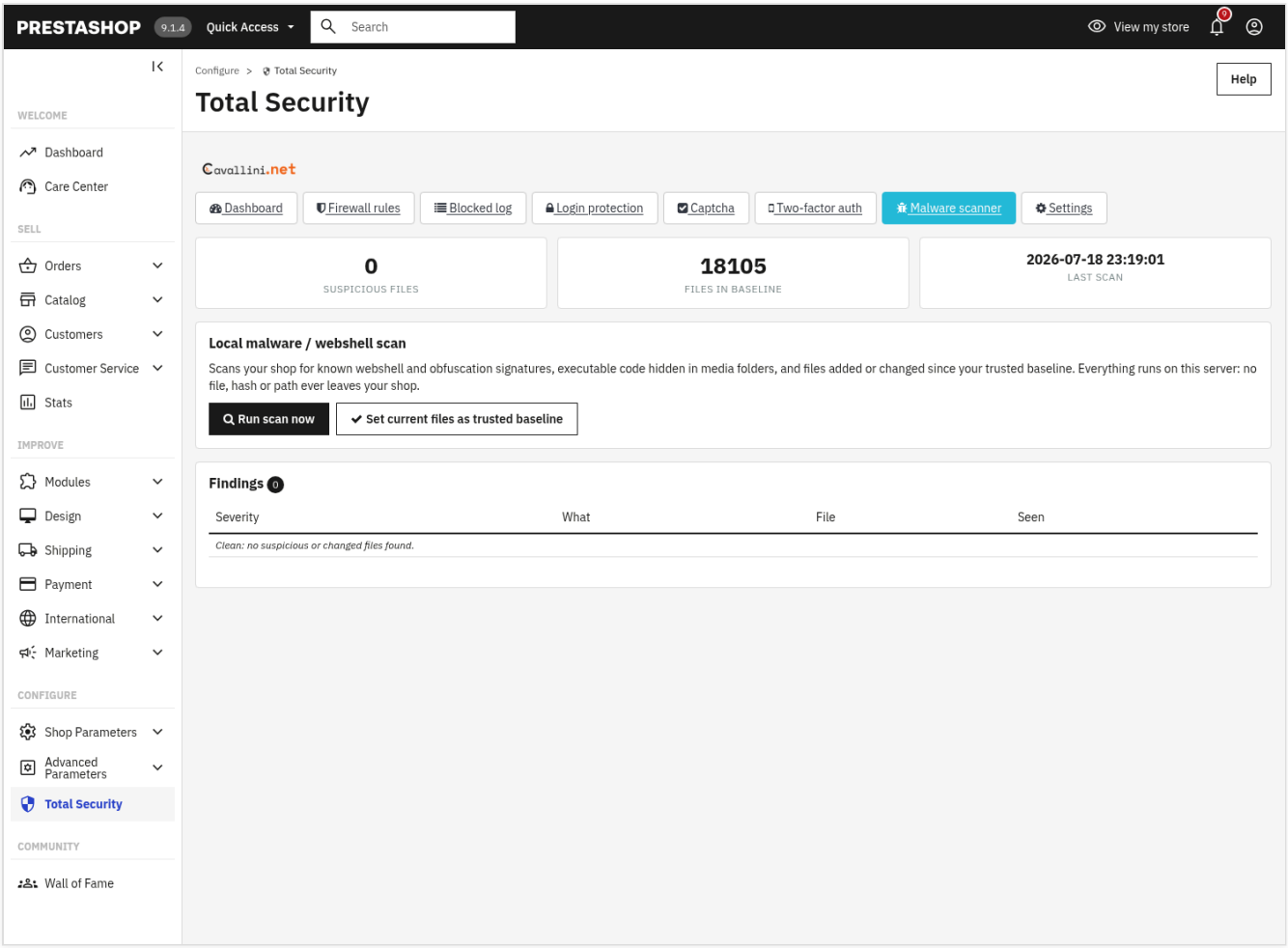


2FA — registro, perfiles forzados y usuarios registrados

Escáner de malware

Análisis local de malware/webshells: busca firmas conocidas de webshells y ofuscación, código ejecutable oculto en carpetas de medios, y archivos añadidos o modificados desde tu línea base de confianza. Todo se ejecuta en el servidor: ningún archivo, hash o ruta sale jamás de la tienda.

- **Métricas** — archivos sospechosos, archivos en la línea base, último análisis.
- **Ejecutar análisis ahora** y **Establecer los archivos actuales como línea base de confianza**.
- Los resultados se listan con **gravedad**, **qué**, **archivo** y **cuándo**.

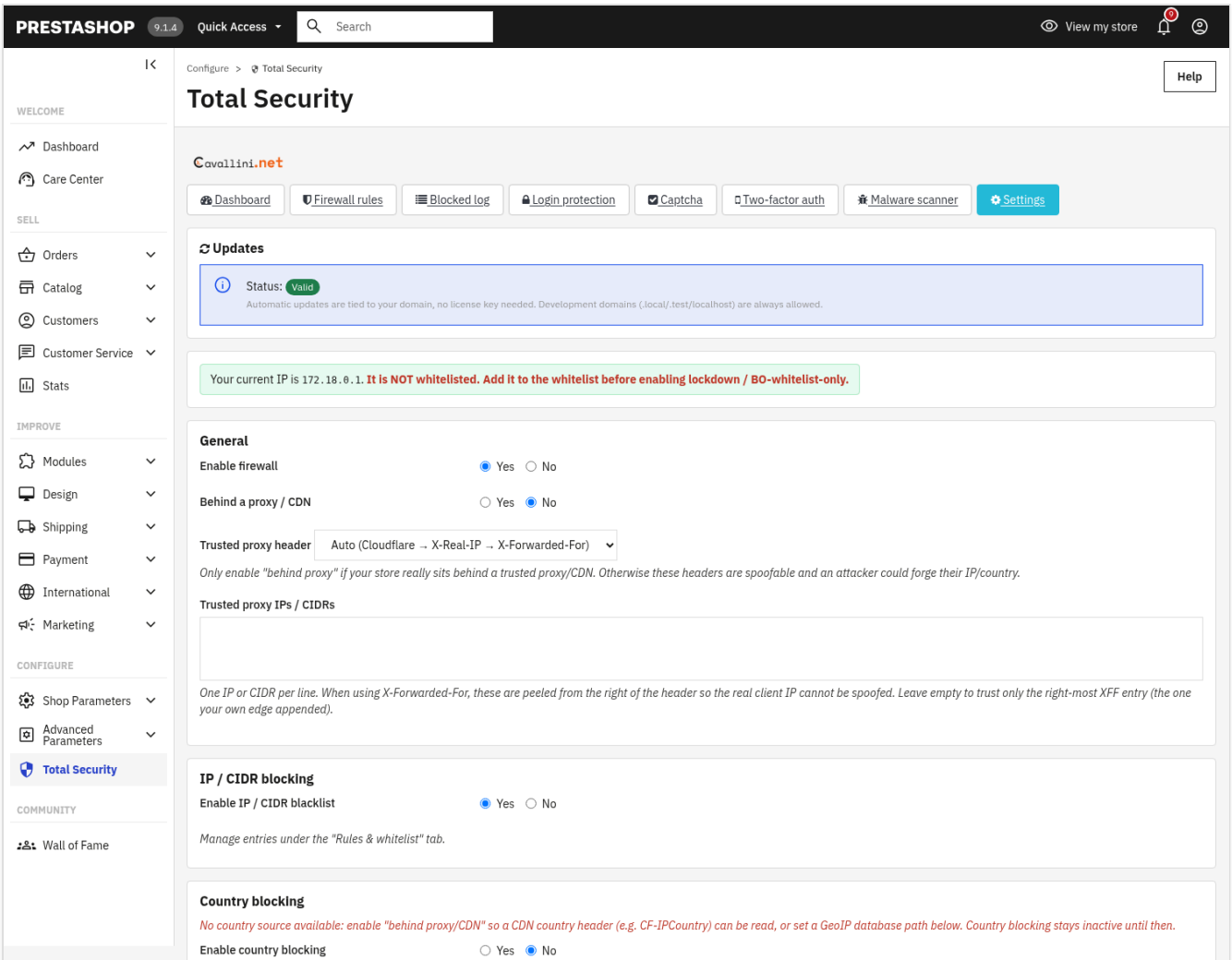


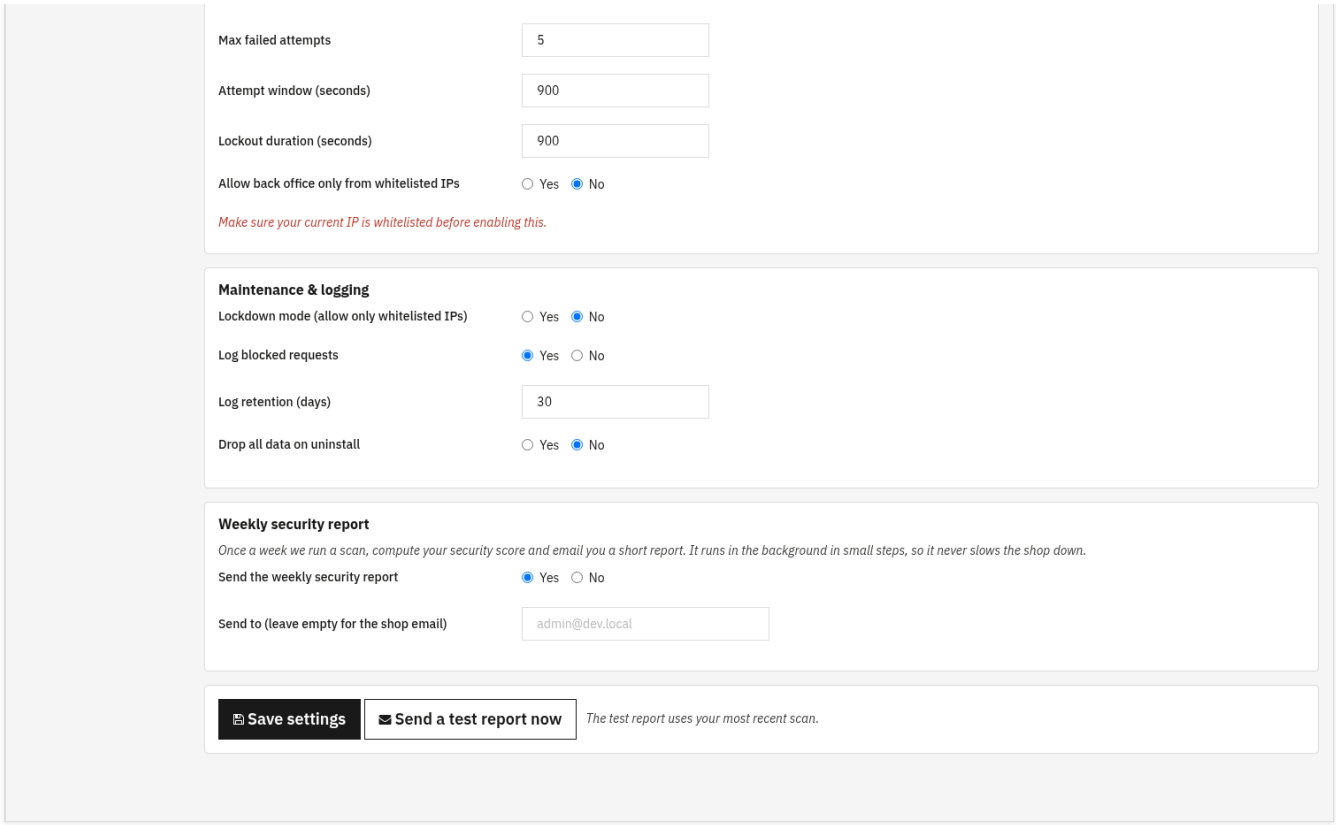
Escáner de malware — métricas, análisis y resultados

Configuración `configuración del cortafuegos`

La configuración propia del cortafuegos, organizada por secciones.

- **General** — Activar cortafuegos; **Detrás de un proxy/CDN** con una cabecera de proxy de confianza e IP/CIDR de proxy de confianza — actívalo solo si hay un proxy realmente de confianza detrás, de lo contrario las cabeceras de IP/país se pueden falsificar.
- **Bloqueo IP/CIDR**.
- **Bloqueo por país** — modo lista negra o lista blanca, códigos ISO-2, una ruta opcional a una base de datos MaxMind GeoLite2 o una cabecera CDN con el país — la base de datos nunca se incluye, por motivos de licencia.
- **Bots / user-agents maliciosos** — activar el bloqueo por user-agent, bloquear user-agent vacío, subcadenas adicionales a bloquear combinadas con una lista integrada.
- **Rate limiting** — máximo de solicitudes por ventana, segundos de la ventana, duración del bloqueo temporal.
- **Bloqueo por patrones de ataque** — SQLi/XSS/LFI/probing.
- **Protección de inicio de sesión del back office** — máximo de intentos fallidos, ventana de intentos, duración del bloqueo, permitir el back office solo desde IP en lista blanca.
- **Mantenimiento y registro** — **Modo de bloqueo total** (permitir solo IP en lista blanca), registrar solicitudes bloqueadas, días de conservación del registro, eliminar todos los datos al desinstalar.
- **Informe semanal de seguridad** — envía un breve informe por correo; se ejecuta en segundo plano en pequeños pasos para no ralentizar nunca la tienda.

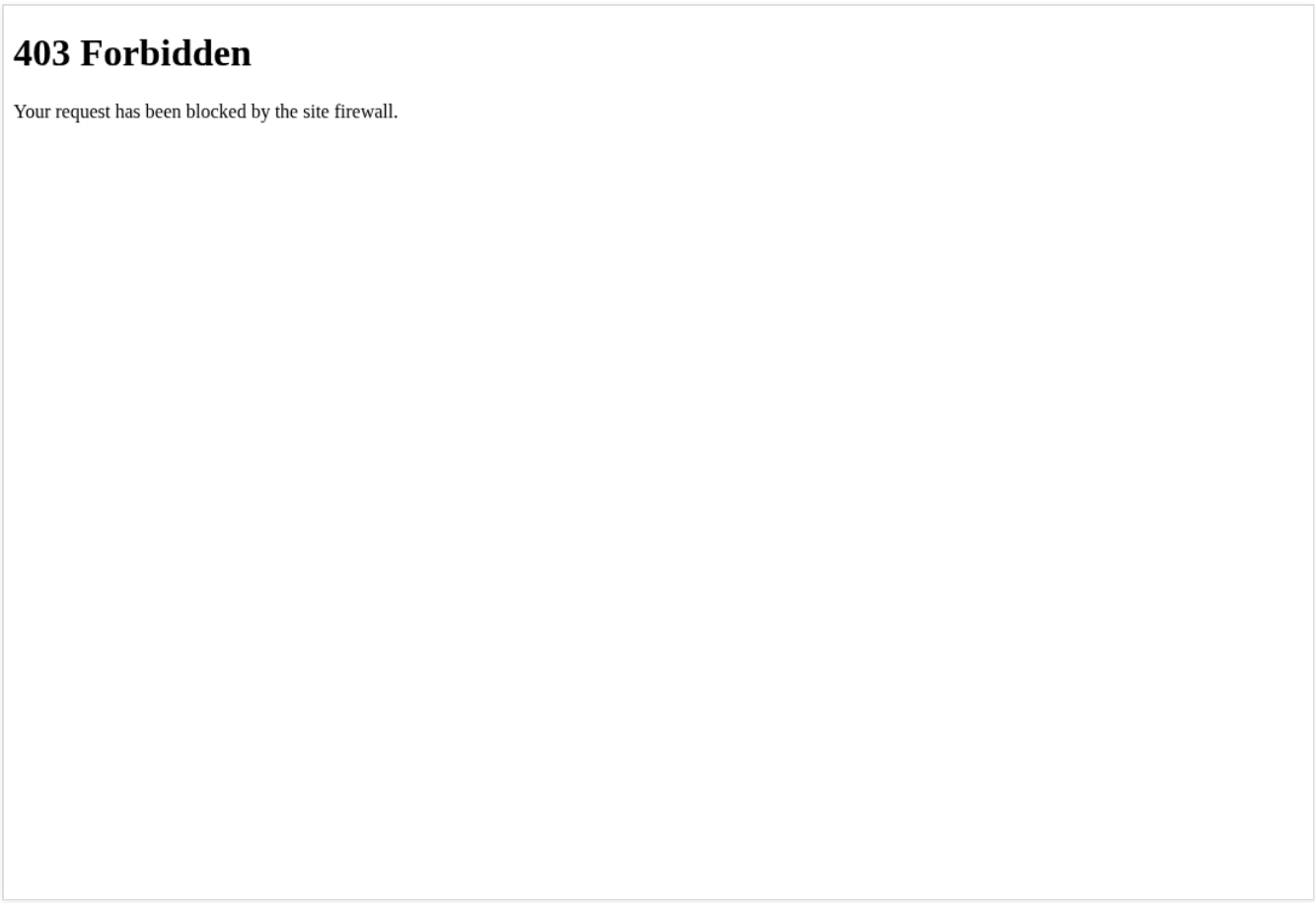

PRESTASHOP
9.1.4
Quick Access
Search
View my store
WELCOME
Dashboard
Care Center
SELL
Orders
Catalog
Customers
Customer Service
Stats
IMPROVE
Modules
Design
Shipping
Payment
International
Marketing
CONFIGURE
Shop Parameters
Advanced Parameters
Total Security
COMMUNITY
Wall of Fame
Configure > Total Security
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



Configuración — configuración del cortafuegos por sección

En el front office

Cuando el cortafuegos bloquea una solicitud, el visitante ve una simple página 403 «Forbidden — tu solicitud ha sido bloqueada por el cortafuegos del sitio»: los bots y escáneres nunca llegan a tu tienda.



En el front office — la página 403 mostrada cuando el cortafuegos bloquea una solicitud

3. Comprueba que funciona

- Abre el *Dashboard* y consulta tu puntuación de seguridad y la checklist.
- Envía una solicitud con un user-agent similar al de un escáner (o una URL de sondeo) y confirma que obtienes la página de bloqueo 403 y una nueva línea en el *Registro de bloqueos*.
- Tras varios inicios de sesión fallidos en el back office, la cuenta/IP queda bloqueada en *Protección de inicio de sesión*.
- Activa el captcha y confirma que aparece en el formulario de inicio de sesión/registro.
- Configura la 2FA en tu cuenta y vuelve a iniciar sesión con un código de 6 dígitos.
- Ejecuta el *Escáner de malware* y consulta los resultados.

4. Preguntas frecuentes

¿Ralentiza la tienda?

No: el cortafuegos se ejecuta primero con comprobaciones ligeras e indexadas; el escáner y el informe semanal se ejecutan en segundo plano.

¿Me puede dejar fuera de mi propio sitio?

Añade primero tu IP actual a la lista blanca (la página te lo advierte, y `127.0.0.1` / `::1` están en la lista blanca desde la instalación); activa el modo de bloqueo total o el back office restringido a lista blanca solo después de eso.

¿Sale algún dato de mi servidor?

No: el cortafuegos, la opción de captcha Lightweight, los secretos de la 2FA y el escáner de malware se ejecutan todos localmente en tu servidor.

¿Sustituye a módulos independientes de cortafuegos / captcha / 2FA?

Sí: es la suite de seguridad única y unificada.

¿Necesito modificar mi tema?

No: funciona mediante hooks estándar y es compatible con cualquier tema.
