



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.

Total Security: Firewall, Captcha, 2FA & Malware Scanner

Your security score, the web application firewall, captcha, two-factor authentication and the local malware scanner are all managed on the configuration page.

 [Go to configuration](#)

El panel Configurar abre la página de configuración completa

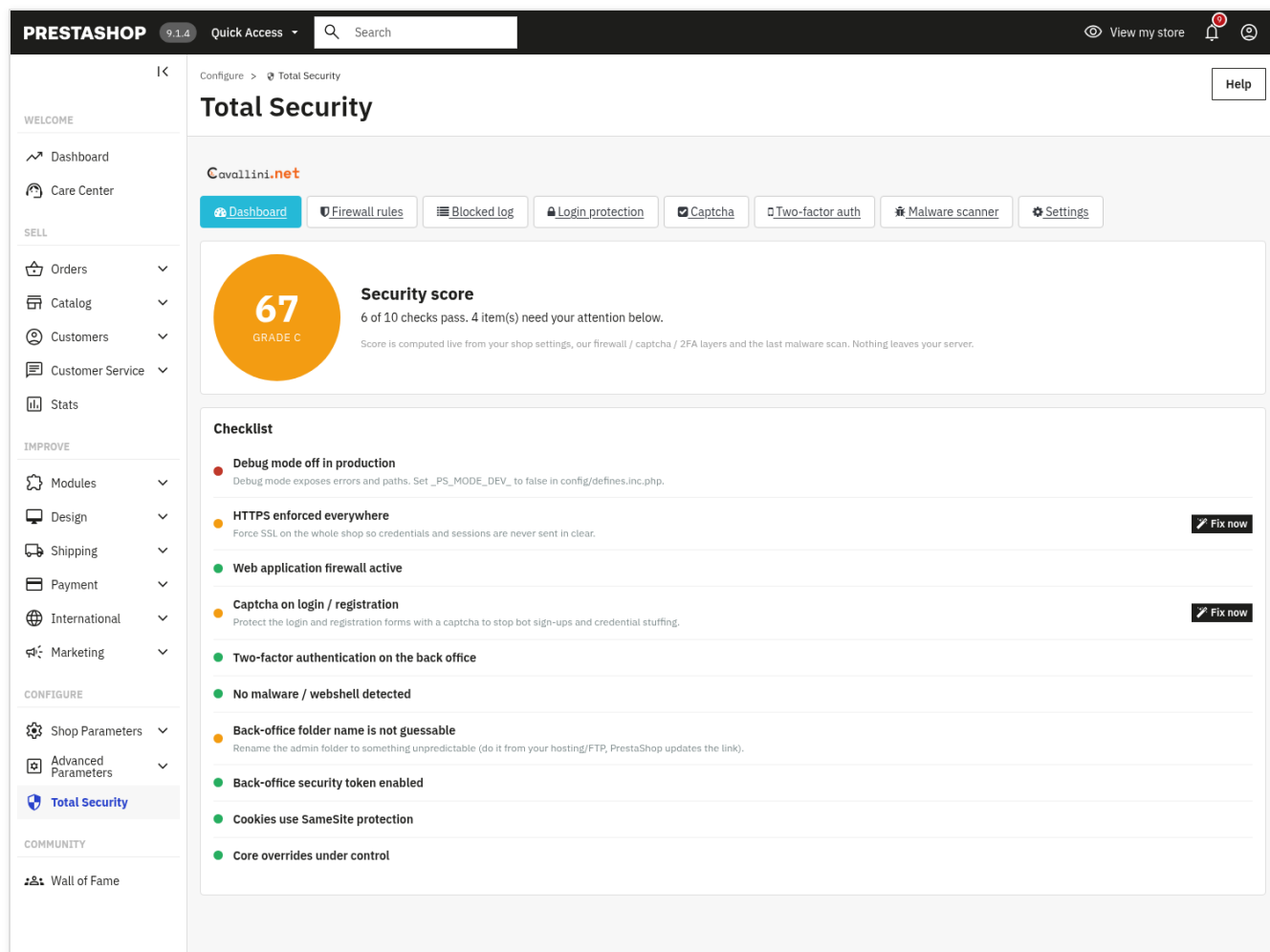
Las actualizaciones son automáticas. Las actualizaciones están incluidas. Los dominios de desarrollo (`.local` , `.test` , `localhost`) siempre están permitidos. Cuando hay una nueva versión disponible, se muestra directamente dentro del módulo.

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.



The screenshot displays the PrestaShop 9.1.4 interface, specifically the 'Total Security' section. The top navigation bar includes the PrestaShop logo, version 9.1.4, a 'Quick Access' dropdown, a search bar, and links for 'View my store', notifications, and user profile. The left sidebar contains a 'WELCOME' section and a 'Total Security' menu item. The main content area is titled 'Total Security' and features a 'Cavallini.net' logo. Below the logo is a row of tabs: 'Dashboard' (active), 'Firewall rules', 'Blocked log', 'Login protection', 'Captcha', 'Two-factor auth', 'Malware scanner', and 'Settings'. The 'Dashboard' tab shows a 'Security score' of 67 (Grade C) with a note that 6 of 10 checks pass and 4 items need attention. A 'Checklist' section follows, listing 10 items with status indicators (red for failed, green for passed) and 'Fix now' buttons for failed items. The checklist items are: 'Debug mode off in production' (failed), 'HTTPS enforced everywhere' (failed), 'Web application firewall active' (passed), 'Captcha on login / registration' (failed), 'Two-factor authentication on the back office' (passed), 'No malware / webshell detected' (passed), 'Back-office folder name is not guessable' (failed), 'Back-office security token enabled' (passed), 'Cookies use SameSite protection' (passed), and 'Core overrides under control' (passed).

Item	Status	Action
Debug mode off in production	Failed	Fix now
HTTPS enforced everywhere	Failed	Fix now
Web application firewall active	Passed	
Captcha on login / registration	Failed	Fix now
Two-factor authentication on the back office	Passed	
No malware / webshell detected	Passed	
Back-office folder name is not guessable	Failed	Fix now
Back-office security token enabled	Passed	
Cookies use SameSite protection	Passed	
Core overrides under control	Passed	

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.

PRESTASHOP

9.1.4

Quick Access

Search

View my store

Configure > Total Security

Help

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

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

Your current IP is 172.18.0.1. It is NOT whitelisted. Add it to the whitelist before enabling lockdown / BO-whitelist-only.

Add a rule

Whitelist IP / CIDR

e.g. 203.0.113.10 or 203.0.113.0/24 or RU or badbot

note (optional)

+ Add

Whitelist (trusted IP / CIDR, bypass everything) 2

Value	Note	Added
::1	Auto-added at install (anti-lockout)	2026-07-08 19:20:48
127.0.0.1	Auto-added at install (anti-lockout)	2026-07-08 19:20:48

Blacklist (blocked IP / CIDR) 0

Value	Note	Added
No rules.		

Country rules (ISO-2) 0

Value	Note	Added
No rules.		

Bad user-agents (substring match) 0

Value	Note	Added
No rules.		

Custom attack patterns (substring match) 0

Value	Note	Added
No rules.		

Pattern whitelist (URI substrings exempt from pattern blocking) 0

Value	Note	Added
No rules.		

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.

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

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

All reasons

IP contains...

Filter

Export CSV

Clear log

27

Date	IP	Country	Reason	Detail	URI	User-Agent	
2026-07-21 21:44:19	172.18.0.1		user_agent	sqlmap	/favicon.ico	sqlmap/1.5.2#stable (http://sqlmap.org)	
2026-07-21 21:44:19	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.5.2#stable (http://sqlmap.org)	
2026-07-21 21:41:08	172.18.0.1		attack_pattern	lf_passwd	/?x=/etc/passwd	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	
2026-07-21 21:41:07	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.5.2	
2026-07-21 21:22:29	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.0	
2026-07-18 23:42:15	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=7257d964683_NHtiQxo543LAipa3jNk2QdZUnudD4D7j4k05yCCpvo	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:41:15	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=ccf7.gzXn9F..lrgtWuq9vAdAKzJ2je_y9ktTS4Q	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:40:34	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=7ba68255093..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:38:09	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=500b134a561..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:36:28	172.18.0.1		attack_pattern	xss_script	/address?id_address=0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:26:39	172.18.0.1		attack_pattern	xss_handler	/admin-dev/?controller=AdminController&token=b1260b7..7.dvpMRQfjNh_HiDu4FF4..Z7LVHwo2EtMUp	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:26:37	172.18.0.1		attack_pattern	xss_handler	/admin-dev/?controller=AdminController&token=b1260b7..7.dvpMRQfjNh_HiDu4FF4..Z7LVHwo2EtMUp	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:25:47	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=724e95e..Zr5o..wVZ7Q16fGh	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:25:46	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=724e95e..Zr5o..wVZ7Q16fGh	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:24:21	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=5822b68..x0L7QvvpdM..3aLDLv	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:24:21	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=5822b68..x0L7QvvpdM..3aLDLv	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:23:29	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=566e2be783b..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:22:28	172.18.0.1		attack_pattern	xss_script	/?x=%3Cscript%3Ealert(1)%3C/script%3E	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:21:12	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=15a5721..Y4owHw7gMJN9G8qihFQhzyOR95yfmk..cklOUF435..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 19:16:02	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:59	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:45	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:45	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:36	172.18.0.1		user_agent	curl/	/index.php?fc=module&module=cli_withdrawal&controlle..	curl/8.14.1	
2026-07-18 19:15:36	172.18.0.1		user_agent	curl/	/	curl/8.14.1	
2026-07-18 19:15:30	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:30	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	

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).

PRESTASHOP 9.1.4Quick AccessSearch

View my store

WELCOME

DashboardCare Center

SELL

OrdersCatalogCustomersCustomer ServiceStats

IMPROVE

ModulesDesignShippingPaymentInternationalMarketing

CONFIGURE

Shop ParametersAdvanced ParametersTotal Security

COMMUNITY

Wall of Fame

Configure > Total Security

Help

Total Security

Cavallini.net

DashboardFirewall rulesBlocked logLogin protectionCaptchaTwo-factor authMalware scannerSettings

Back-office login attempts

Failed back-office logins are tracked per IP and username. After the configured threshold the source is locked out temporarily.

IP	Username	Attempts	Locked until	State
No failed back-office login attempts recorded.				

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.

PRESTASHOP 9.1.4

Quick Access

Search

View my store

Configure > Total Security

Help

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

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

Captcha provider

Enable captcha protection

Provider

Choose your anti-spam provider. Create the keys in the provider dashboard. The Lightweight provider needs no keys and keeps everything on your server.

Site key (public)

Secret key (server-side only)

reCAPTCHA v3 score threshold (0.0 bot, 1.0 human)

Widget theme

Badge position (v3 / invisible / Turnstile)

Lightweight token lifetime (seconds)

Protected forms

Login

Registration

Forgot password

Contact form

Newsletter

Product review

Guest checkout

Advanced

Fail closed (block when the provider is unreachable)

Skip captcha for logged-in customers

Verification timeout (seconds, 1 to 30)

Trusted IP whitelist (one per line, skip captcha)

Verify hostname (reject tokens solved on another domain)

Expected hostname (optional, empty = auto)

Verify action (reCAPTCHA v3 and Turnstile)

Rate limiting

Rate-limit failed captcha attempts

Max failed attempts (1 to 1000)

Window in minutes (1 to 1440)

Save captcha settings

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.

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

Cavallini.net

Dashboard Firewall rules Blocked log Login protection Captcha Two-factor auth Malware scanner Settings

Your account

Two-factor authentication for the account you are signed in with. Not set up

Set up 2FA on my account

You will scan a QR code with an authenticator app (Google Authenticator, Authy, 1Password) and enter a 6-digit code to confirm.

Two-factor authentication

Time-based one-time codes (Google Authenticator, Authy, 1Password and any compatible app). Nothing leaves your server: secrets are encrypted at rest and verified locally.

Enable 2FA for the back office (staff) Yes No

This makes 2FA available: an employee can turn it on for their own account, and is then asked for a code at every login. To make it mandatory instead, list the profiles below.

Enable 2FA for customers (front office) Yes No

Force 2FA for these employee profiles (comma-separated IDs) 1, 2

Employees in these profiles cannot use the back office until they enrol. Leave empty to keep 2FA optional. Profiles: 1 = SuperAdmin 2 = Logistician 3 = Translator 4 = Salesman

Tolerance window (steps of 30s, 0 to 5) 1

Number of backup codes (4 to 20) 8

Issuer name shown in the app (empty = shop name) PrestaShop

Save 2FA settings

Enrolled employees 0

ID	Name	Email	Status	Updated
No one has enrolled yet.				

Enrolled customers 0

ID	Name	Email	Status	Updated
No one has enrolled yet.				

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**.

PRESTASHOP 9.1.4Quick AccessSearch

View my store

Configure > Total Security

Help

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

Total Security

Cavallini.net

DashboardFirewall rulesBlocked logLogin protectionCaptchaTwo-factor authMalware scannerSettings

0

SUSPICIOUS FILES

18105

FILES IN BASELINE

2026-07-18 23:19:01

LAST SCAN

Local malware / webshell scan

Scans your shop for known webshell and obfuscation signatures, executable code hidden in media folders, and files added or changed since your trusted baseline. Everything runs on this server: no file, hash or path ever leaves your shop.

Run scan nowSet current files as trusted baseline

Findings

Severity	What	File	Seen
Clean: no suspicious or changed files found.			

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.

Max failed attempts	5
Attempt window (seconds)	900
Lockout duration (seconds)	900
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
Log blocked requests	☒ Yes ☐ No
Log retention (days)	30
Drop all data on uninstall	☐ Yes ☒ No

Weekly security report

Once a week we run a scan, compute your security score and email you a short report. It runs in the background in small steps, so it never slows the shop down.

Send the weekly security report	☒ Yes ☐ No
Send to (leave empty for the shop email)	admin@dev.local

Save settings	Send a test report now	<i>The test report uses your most recent scan.</i>
--	---	--

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.

403 Forbidden

Your request has been blocked by the site firewall.

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.