

Firewall de aplicaciones web

Proteja su sitio web frente a ataques de inyección de código SQL o ejecución de comandos en sitios cruzados, entre otros

El firewall de aplicaciones web (WAF) de Cloudflare protege su sitio web frente a ataques de inyección de código SQL, de ejecución de comandos en sitios cruzados (XSS) y de día cero, que incluyen vulnerabilidades y amenazas dirigidas a la capa de aplicación y están reconocidas por el OWASP. Entre nuestros clientes se incluyen los 50 primeros puestos del ranking Alexa, instituciones financieras, empresas de comercio electrónico y grandes compañías. Totalmente integrado con nuestra protección frente a DDoS, nuestro WAF bloquea millones de ataques diariamente, al tiempo que aprende de forma automática de cada nueva amenaza.

Un robusto motor de reglas para adaptarse a sus necesidades

Nuestro WAF ejecuta los conjuntos de reglas ModSecurity listos para usar, que le protegen frente a los fallos de seguridad de aplicación web más críticos reconocidos por el OWASP. También puede gestionar sus conjuntos de reglas y reglas personalizadas existentes. Las reglas se hacen efectivas en menos de 30 segundos.

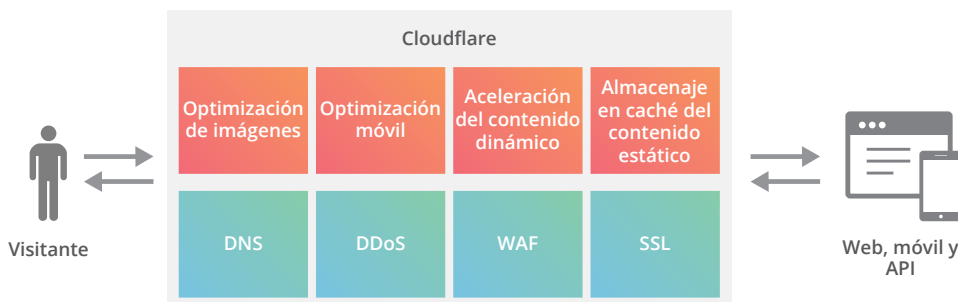
Implementación de nube más mitigación de DDoS y CDN

Como servicio basado en la nube, el WAF de Cloudflare no requiere instalación ni mantenimiento de hardware o software. Implemente el WAF con un solo clic y personalícelo para adaptarse a sus necesidades.

Su integración en el servicio general de Cloudflare implica que obtenga funcionalidades adicionales de forma gratuita. Puede asegurar su sitio web frente a ataques DDoS y usar nuestra red de entrega de contenido global para una ejecución más rápida.

Aspectos destacados:

- **Protección automática** frente a diversas amenazas, con potentes conjuntos de reglas predeterminados y amplias posibilidades de personalización, que proporciona protección de capa 7 y está completamente integrada con la mitigación de DDoS.
- **Tiempos de procesamiento extremadamente rápidos de 0,3 ms**, con actualizaciones globales instantáneas.
- **Cumplimiento con los requisitos del PCI DSS 6.6:** el WAF de Cloudflare le permite satisfacer el cumplimiento del PCI de forma eficaz y rentable.
- **Informes en tiempo real:** el potente registro le permite ver qué sucede de forma instantánea.
- **Implementación de nube** sin necesidad de hardware, software ni configuración.



Características principales	Beneficios
Seguridad	
Inspección profunda de paquetes, aplicaciones de cobertura/capa 7	Asegura la protección de sus aplicaciones web personalizadas y estándar frente a ataques de inyección de código SQL y ejecución de comandos en sitios cruzados, entre muchos otros.
SSL	Finalice las conexiones SSL sin sobrecarga ni latencia adicional. Aplique su política de WAF para tráfico SSL cifrado sin tener que cargar certificados o invertir en soluciones de hardware costosas.
Para solicitudes HTTP/S GET y POST	Cubre la gama de tráfico HTTP/S
Conjuntos de reglas personalizadas específicas de URL	Le permite incluir/excluir URAL o subdominios específicos para el análisis de la protección de WAF de dominios o incluir/excluir subdominios específicos.
Integración de mitigación de DDoS	Permite la protección completa frente a DDoS. No requiere implementación adicional.
Integración de base de datos de reputación de IP	Inteligencia en tiempo real sobre más de mil millones de IP únicas utilizadas para bloquear tráfico malicioso. No requiere implementación adicional.
Parcheo virtual	Fija una vulnerabilidad antes de que parchee su servidor o actualice su código, lo que permite más tiempo para parchear y probar actualizaciones.
Restricción por IP o geolocalización	Puede clasificar en listas negra y blanca tráfico de direcciones IP específicas o países para protegerlas frente a hackers de IP o países específicos.
Falso positivo bajo	Un índice general de 1/50 M de falsos positivos garantiza que le alcance tráfico legítimo.
Integración completa con el servicio de CDN, que ofrece la transformación de contenido saliente	Reduce la latencia de la web para los visitantes de su sitio. No requiere implementación adicional.
Conjuntos de reglas	
Aprendizaje automático emparejado con investigación orientada a la seguridad	Protege contra vulnerabilidades de día cero o nuevas amenazas con parches automáticamente implementados por nuestro equipo de seguridad.
Compatibilidad con lógica y formato de ModSecurity	Permite importar conjuntos de reglas de forma sencilla para mantener la protección existente.
Conjunto de reglas Core OWASP ModSecurity	Protege frente a las vulnerabilidades de OWASP, los fallos más críticos reconocidos por el proyecto abierto de seguridad en aplicaciones web (OWASP). Se incluye de forma predeterminada sin coste adicional.
Conjuntos de reglas de día cero de Cloudflare	Confíe en el equipo de seguridad de Cloudflare para protegerle frente a amenazas identificadas a través de nuestra base de clientes. Se incluye de forma predeterminada sin coste adicional.
Conjuntos de reglas específicos de plataforma para plataformas grandes de comercio electrónico y sistemas de gestión de contenidos	Reciba protección lista para usar sin coste adicional para plataformas como WordPress, Joomla, Plone, Drupal, Magento e IIS, entre otras.
Reglas personalizadas	Cubra situaciones únicas para su aplicación web, que se incluyen de forma predeterminada y sin coste adicional para los clientes Business e Enterprise.
Configuraciones de WAF	
Bloqueo	El bloqueo de un ataque detendrá cualquier acción antes de que se publique en su sitio web.
Simulación	Para hacer la prueba de falsos positivos, establezca el WAF en modo Simulate (Simulación), que registrará la respuesta a posibles ataques sin desafiar o bloquear.
Desafío	Una página del desafío pide a los visitantes que envíen un CAPTCHA para entrar en su sitio web.
Ajuste de la sensibilidad/umbral	Establezca reglas para accionar más o menos en función de la sensibilidad.
Páginas de bloqueo personalizables	Personalice la página que un visitante visualiza cuando resulta bloqueado, por ejemplo, "Llame a este número de teléfono para pedir asistencia". Disponible para clientes Enterprise.
Elaboración de informes	
Registro en tiempo real	Adquiera visibilidad para configurar el WAF de forma precisa.
Acceso a archivos de registro sin procesar	Los clientes Enterprise pueden llevar a cabo análisis en profundidad que cubren todas las solicitudes de WAF.
Administración	
Alta disponibilidad; servicio integrado que ofrece acuerdos de nivel de servicio (ANS)	Los clientes Business y Enterprise disfrutan de una garantía de tiempo de actividad del 100 % y sanciones financieras en caso de incumplimiento.
No requiere hardware, software ni configuración	Regístrese con un simple cambio en el DNS.
Certificación PCI	El servicio de Cloudflare ha obtenido la certificación de proveedor de servicio de nivel 1.