T.I RESCUE
SEGURIDAD INFORMÁTICA

RESCUE WAF

Solución avanzada de firewall de aplicaciones web diseñada para proteger tus aplicaciones y datos de accesos no autorizados y ciberataques.

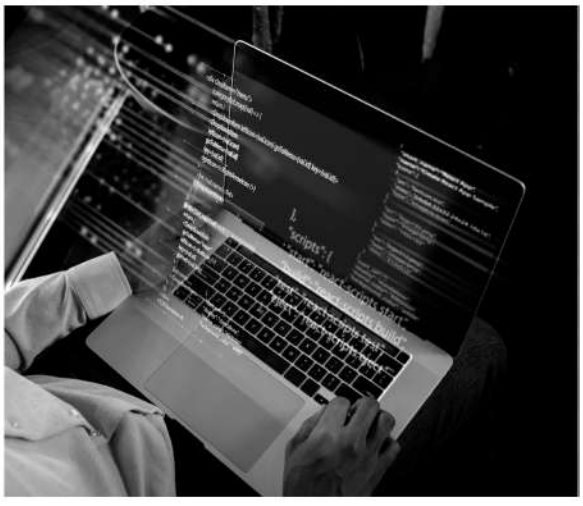
+57 300 913 7356
www.tirescue.com
Cra. 65 #8B - 91 Ofic. 485, Medellín

SOBRE
TI RESCUE

NOSOTROS

Con un equipo altamente calificado, garantizamos soluciones de TI que superan las expectativas.

CONECTA,
COMUNICA
CONVIERTE



OBJETIVOS

Impulsar la transformación digital con estrategias de seguridad personalizadas y soporte tecnológico continuo.

SOMOS UN OUTSOURCING TÉCNOLÓGICO EN COLOMBIA

Soluciones integrales de TI, adaptadas a la innovación y crecimiento de tu empresa

CALIDAD Y SEGURIDAD CERTIFICADAS

Nuestros procesos y servicios están respaldados por normas internacionales de calidad y ciberseguridad.

icontec ISO 9001	icontec ISO / IEC 27001	icontec ISO / IEC 20000-1	icontec ISO 22301	IQNET CERTIFIED MANAGEMENT SYSTEM
SC-CER900888	SI-CER900889	TI-CER988544	CO-CNCER988779	

Rescue **WAF**

Las aplicaciones web son objetivos frecuentes de ataques cibernéticos, y la cantidad y sofisticación de estas amenazas solo sigue en aumento. Entre las amenazas más comunes se encuentran la **inyección SQL, los ataques de fuerza bruta, el cross-site scripting (XSS) y ataques DDoS.** En este contexto, se hace indispensable contar con una protección robusta y en tiempo real para asegurar tus aplicaciones y datos.

Análisis de **tráfico web**

Seguridad Basada en **Reglas Avanzadas**

Implementar Rescue WAF reduce la exposición a amenazas cibernéticas, protege la reputación de tu empresa y salvaguarda los datos de tus clientes. Esto se traduce en un **ahorro significativo** de recursos y en una **mayor tranquilidad para tu equipo de IT y tus usuarios.**

Filtros personalizables: Permite ajustes precisos para diferentes tipos de tráfico y configuraciones de aplicaciones.

Monitorización en tiempo real: Proporciona visibilidad en tiempo real de eventos y datos de seguridad.

Inteligencia y **Monitoreo Continuo**

Rescue WAF se mantiene actualizado con la información más reciente sobre amenazas globales, lo que le permite anticiparse y bloquear ataques nuevos y sofisticados. A través de su sistema de inteligencia avanzada, **detecta patrones emergentes de amenazas y ajusta automáticamente sus defensas**. Además, Rescue WAF genera informes detallados y envía **alertas en tiempo real,** brindándote una visión completa y actualizada del estado de seguridad de tu aplicación. Esto te permite estar al tanto de cualquier actividad sospechosa y tomar decisiones informadas para fortalecer tu entorno de seguridad.

Integración con Threat Intelligence:

Actualización continua de bases de datos de amenazas para bloquear patrones y direcciones IP nuevas.

Generación de Reportes de Seguridad Detallados:

Informes automatizados sobre eventos y actividad sospechosa, para revisión y cumplimiento.

Alertas y Notificaciones en Tiempo Real

Notificaciones automáticas para eventos críticos, permitiendo una respuesta rápida.

Análisis de Tráfico en Tiempo Real:

Monitoreo constante para bloquear comportamientos sospechosos y asegurar acceso legítimo.

01. **Monitoreo de Actividad Anómala:** Rescue WAF detecta patrones inusuales en el tráfico y alerta sobre comportamientos sospechosos de inmediato, permitiendo identificar amenazas potenciales antes de que puedan convertirse en ataques reales. Esta vigilancia constante asegura que cualquier actividad irregular sea interceptada de manera proactiva.

02. **Prevención de Escalación de Ataques:**Nuestro sistema identifica intentos de ataque que aumentan en intensidad, bloqueándolos antes de que afecten la aplicación o los datos de los usuarios.

03. **Análisis Predictivo de Amenazas** A través de inteligencia avanzada, Rescue WAF anticipa posibles vectores de ataque basados en actividad global, reforzando la seguridad proactivamente.

04. **Optimización de Políticas de Seguridad:** Actualización automática de reglas de seguridad, ajustándose a nuevas amenazas sin intervención manual, para una defensa continua y eficaz.

Control de accesos
Por Geolocalización

Rescue WAF permite restringir o permitir el acceso a la aplicación en función de la ubicación geográfica del usuario. Esto es útil para bloquear tráfico proveniente de regiones conocidas por ser fuentes de actividad maliciosa, minimizando el riesgo de ataques desde ubicaciones no deseadas. **Al definir reglas basadas en geolocalización, se añade una capa adicional de seguridad que protege la aplicación sin afectar el acceso de los usuarios legítimos.**

Distribución Geográfica
del **Tráfico Malicioso**

China (21%), Estados Unidos (19%), Rusia (14%), Brasil (8%), India (6%).

Protección Contra Amenazas Globales

Rescue WAF ofrece una defensa robusta contra ataques originados en las principales zonas de riesgo cibernético a nivel mundial. **Con inteligencia avanzada y monitoreo continuo, identifica y bloquea tráfico malicioso en tiempo real,** asegurando que solo el acceso legítimo llegue a tus aplicaciones.

Gestión de listas
Blancas y Negras

Rescue WAF facilita la creación de listas blancas y negras de geolocalización para controlar el tráfico de manera más precisa. Con las listas blancas, se permite el acceso solo desde ubicaciones confiables, mientras que con **las listas negras se bloquea el tráfico de zonas específicas con antecedentes de amenazas**. Esta gestión flexible asegura que solo el tráfico relevante y seguro llegue a la aplicación, mejorando la protección y reduciendo la exposición a ataques.

Control y gestión de tráfico

Incluye funciones que detectan y bloquean ataques automáticamente, brindando una defensa proactiva. **Rescue WAF** identifica patrones de amenazas y detiene intrusiones antes de comprometer tus aplicaciones, protegiendo la integridad y confidencialidad de tus datos. Con herramientas avanzadas, reconoce y neutraliza tráfico malicioso, como hackers y bots. **Rescue WAF** se adapta a nuevas amenazas y vulnerabilidades, ofreciendo protección en tiempo real sin afectar el rendimiento ni requerir intervención de tu equipo.

Capacidades clave:

Supervisión y optimización del tráfico web

- **Limitación de Solicitudes (Rate Limiting):** Evita ataques DDoS y sobrecargas de tráfico.
- **Control de Sesiones:** Monitorea y administra el uso de sesiones activas en tiempo real.
- **Filtrado de Cargas y Archivos:** Inspección de archivos para bloquear malware y scripts maliciosos.

Rate Limiting y Control de Sesiones:

Limitación de solicitudes para evitar DDoS y control exhaustivo de sesiones.

Análisis de Cabeceras HTTP:

Revisión y sanitización de cabeceras para prevenir ataques de falsificación y manipulación.

Desinfección de Cargas y Archivos:

Filtrado de archivos cargados para bloquear malware y scripts maliciosos en adjuntos.

Gracias a las funciones avanzadas de Control y Gestión de Tráfico de Rescue WAF, **mantenemos tu aplicación protegida frente a intentos de sobrecarga, acceso no autorizado y archivos maliciosos**. Estas capacidades no solo aseguran que solo el tráfico legítimo llegue a tu sistema, sino que también optimizan el rendimiento y la disponibilidad de tu aplicación, brindando una experiencia segura y fluida para tus usuarios.

Protección Específica en la **capa de Aplicación (Layer 7)**

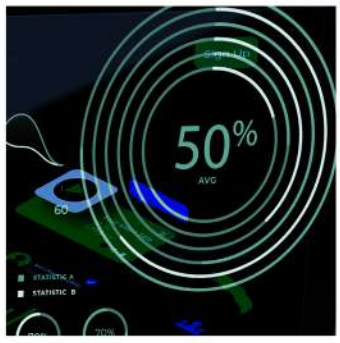
Esta capa se enfoca en brindar seguridad directamente en la aplicación web, **protegiendo áreas sensibles como formularios, sistemas de autenticación y procesos que manejan datos confidenciales**. Al asegurar estos puntos críticos, **Rescue WAF** previene que los atacantes aprovechen vulnerabilidades en el código o en las interacciones de los usuarios para acceder a información sensible.

Seguridad en Tráfico cifrado

Rescue WAF inspecciona el tráfico cifrado, **analizando conexiones HTTPS para detectar amenazas ocultas, como ataques que intentan disfrazarse en conexiones seguras**. Todo esto se realiza sin comprometer la privacidad de los datos ni el rendimiento de la aplicación, garantizando una comunicación segura y libre de riesgos para tus usuarios y clientes.

- **Defensa Ante Ataques de Layer 7:** Protección avanzada para formularios, autenticación y lógica empresarial.
- **Soporte para TLS/SSL y Decrypting:** Inspección de tráfico cifrado sin comprometer la seguridad de la comunicación..

Prevención y detección de amenazas



Rescue WAF incluye funciones que detectan y bloquean ataques automáticamente. Rescue WAF **identifica patrones de amenazas y bloquea intrusiones antes de que puedan afectar tus aplicaciones**, garantizando así la integridad y confidencialidad de tus datos. Con herramientas avanzadas que reconocen y frenan el tráfico de hackers, bots y otras fuentes maliciosas, Rescue WAF se adapta constantemente a nuevas amenazas y vulnerabilidades, manteniendo segura tu aplicación de forma continua y sin interrupciones en el servicio.

Protecccción Automática

> Rescue WAF detecta y bloquea amenazas de manera continua. Con inteligencia para **reconocer patrones de ataque y frenar el tráfico sospechoso,** mantiene tus aplicaciones seguras sin intervención adicional.

- **Prevención de** intrusiones (IPS):

  Inspección profunda de paquetes para detectar y bloquear patrones de ataque conocidos en tiempo real.

- **Bloqueo automático de** IPs maliciosas:

  Detección y bloqueo de direcciones IP sospechosas y de ataques de fuerza bruta.

- **Protección contra** inyecciones de código:

  Filtrado específico para evitar inyecciones SQL, XSS y otros vectores de ataque.

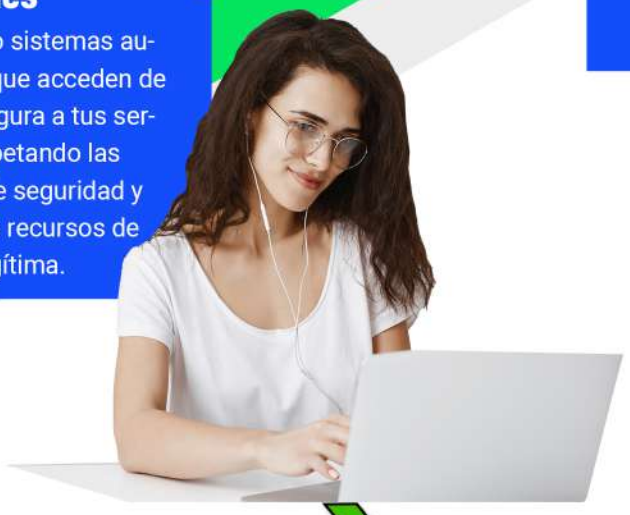
- **Protección contra Bots y** automatización maliciosa:

  Identificación y bloqueo de bots maliciosos que intentan scraping o ataques automatizados.

Web application **Firewall**

Usuarios confiables

Personas o sistemas autorizados que acceden de manera segura a tus servicios, respetando las políticas de seguridad y usando los recursos de manera legítima.



Bots útiles

Robots automatizados diseñados para realizar tareas beneficiosas, como indexación de contenido por buscadores o monitoreo legítimo de sistemas.

Amenazas **maliciosas**

Individuos o grupos con intenciones de explotar vulnerabilidades, robar datos, o interrumpir los servicios mediante accesos no autorizados.

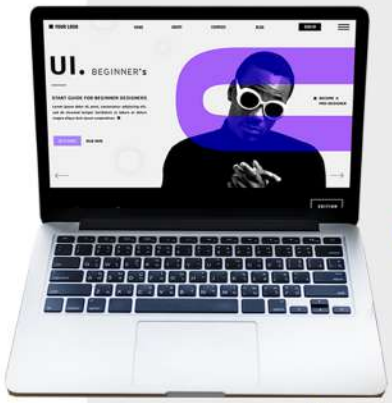
Bots **maliciosos**

Programas automatizados creados para ejecutar ataques, como scraping de datos, sobrecarga de servidores o intentos de fraude.

Envío de tráfico
limpio al servidor

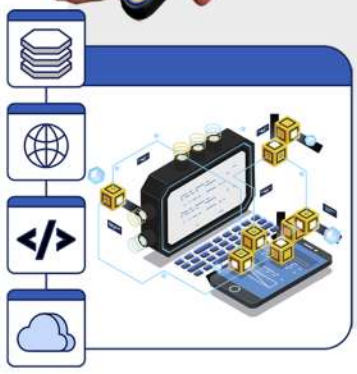
Después del análisis, únicamente las solicitudes autorizadas llegan al backend del cliente, donde se encuentran los servidores y las aplicaciones web. Este proceso asegura:

- **Protección de datos sensibles.**
- **Continuidad operativa sin interrupciones por ataques.**
- **Integridad de las aplicaciones web frente a vulnerabilidades.**

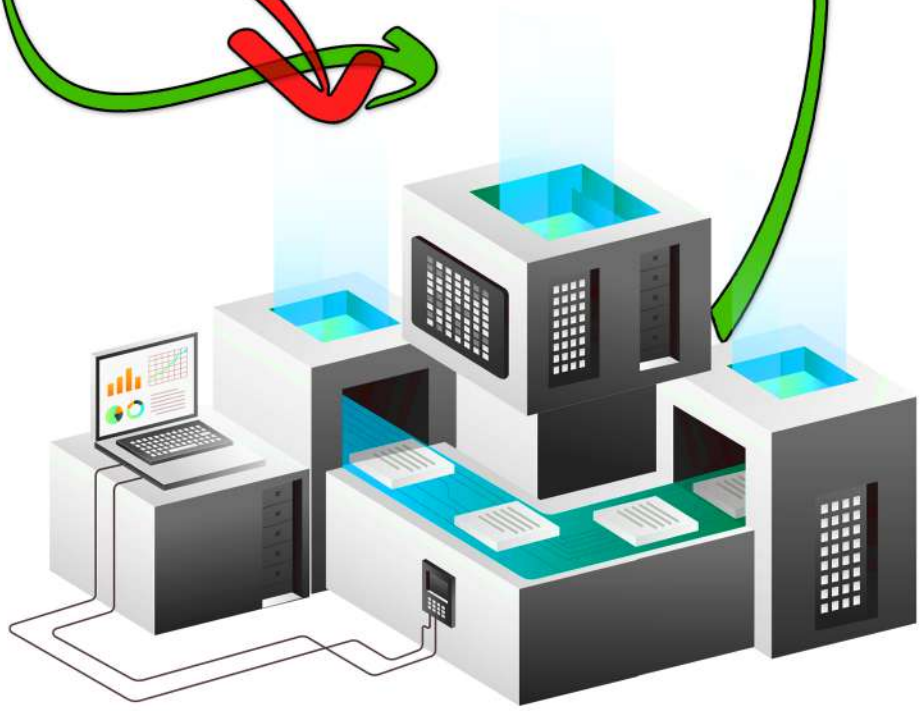


WEB SITES

WEB APPS



APIS



Rescue **WAF**

Rescue WAF es una barrera avanzada que protege aplicaciones web con precisión. **Analiza cada solicitud** en la capa de aplicación para detectar y bloquear amenazas, garantizando una experiencia fluida para usuarios legítimos. Su supervisión en tiempo real asegura que cada encabezado, cookie y parámetro cumpla con los **estándares de seguridad**, manteniendo las aplicaciones seguras y operativas.

T.I RESCUE

SEGURIDAD INFORMATICA

WWW.TIRESCUE.COM

Expertos en Ciberseguridad