



SonicWALL Web Application Firewall Service

ACCESO REMOTO SEGURO

Gestión de amenazas de aplicaciones Web

- **Protección contra las vulnerabilidades Top 10 de la OWASP**
- **Protección contra ataques de falsificación de petición en sitios cruzados**
- **Actualizaciones automáticas de definiciones**
- **Autenticación y autorización sólidas**
- **Protección contra fugas de información**
- **Interfaz de usuario robusta**
- **Configuración flexible de políticas**
- **Amplia protocolización para auditorías**
- **Protección contra la modificación de cookies**
- **Gestión segura de sesiones**
- **Medidas anti-evasión**
- **Inspección HTTPS**
- **Funciones de aceleración**
- **Encubrimiento de sitios Web**
- **Cadenas de reglas personalizadas**

Cada vez son más los negocios y usuarios que utilizan aplicaciones Web 2.0 en sus plataformas informáticas. Al mismo tiempo aumentan los ataques maliciosos contra estas aplicaciones, como inyección SQL, manipulación de parámetros, cross-site scripting y denegación de servicio (DOS). Mientras las pymes amplían cada vez más su presencia en Internet, a menudo no disponen del personal adecuado para hacer frente a los desafíos de la seguridad Web, en constante desarrollo. Dadas las directrices de cumplimiento normativo, los ataques a las aplicaciones Web son un problema especialmente importante para los proveedores de servicios financieros, de salud y de aplicaciones así como para las empresas de comercio electrónico.

SonicWALL® Web Application Firewall (WAF) Service ofrece a las empresas una solución de cumplimiento para aplicaciones Web asequible, bien integrada y fácil de gestionar e implementar. Ofrece soporte para las amenazas top 10 de la OWASP y para el cumplimiento del estándar PCI DSS. Proporciona protección contra el robo de números de tarjetas de crédito o de la Seguridad Social, ataques de inyección y cross-site scripting (XSS), así como ataques de modificación de cookies y de falsificación de petición en sitios cruzados. Las reglas personalizadas y las actualizaciones dinámicas de las definiciones ofrecen un alto nivel de seguridad frente a las vulnerabilidades conocidas y desconocidas. Web Application Firewall Service es capaz de detectar ataques sofisticados basados en Web, proteger las aplicaciones Web (incluyendo los portales SSL VPN), denegar el acceso en caso de encontrar malware de aplicaciones Web y redireccionar a los usuarios a una página de error explicativa. De esta forma ofrece al usuario una solución fácil de implementar, dotada de funciones avanzadas de estadística e informes para el cumplimiento de normas. Asimismo, el análisis de las aplicaciones proporciona a los administradores datos detallados sobre el tráfico Web que llega a sus servidores y les permite crear reglas de forma automática.

Prestaciones y ventajas

Protección contra las vulnerabilidades Top 10 de la fundación OWASP (Proyecto de seguridad de aplicaciones Web abiertas). Incluye los riesgos de seguridad más importantes según gravedad y propagación de los ataques, de acuerdo con PCI DSS 6.6 y otros estándares de la industria.

Protección contra ataques de falsificación de petición en sitios cruzados. SonicWALL WAF ofrece asimismo protección contra ataques de inyección y cross-site scripting (XSS).

Actualizaciones automáticas de definiciones. Esta prestación y la función de análisis adaptativo de aplicaciones ofrecen protección contra las amenazas conocidas y desconocidas.

Autenticación y autorización sólidas para cualquier sitio Web interno o externo (p.ej., sitios Web de comercio electrónico). Soporta iniciativas de cumplimiento de normas al prevenir el acceso no autorizado a sus páginas Web internas y externas. El soporte de autenticación incluye autenticación de doble factor con token, autenticación de certificado cliente y contraseñas de un solo uso sin token. Mediante las políticas de acceso granular puede autorizarse el acceso a diferentes servidores Web según nombre de host, subred, dirección IP, puerto y ruta URL.

Protección contra fugas de información. Permite bloquear el acceso a sitios Web con expresiones o palabras clave definidas por el administrador para evitar la fuga de información sensible. Asimismo ofrece protección contra la filtración (DLP) de números de tarjetas de crédito o de la Seguridad Social.

Interfaz de usuario robusta. Proporciona una interfaz de gestión basada en Web y fácil de usar con estadísticas avanzadas. Puede utilizarse para supervisar el estado del servidor Web. Mediante la página de estado también puede obtenerse una visión detallada de todas las actividades de supervisión y bloqueo de amenazas (p.ej.,

estado de la base de datos de definiciones, amenazas detectadas y bloqueadas, así como amenazas top 10 de la OWASP).

Configuración flexible de políticas. Permite a los administradores configurar las definiciones según la gravedad de la amenaza y definir una lista de exclusiones por definición.

Amplia protocolización para auditorías. Ofrece funciones de protocolización e informes para fines de auditoría, cumplimiento y elaboración de informes.

Protección contra la modificación de cookies. Reduce la probabilidad de que se produzcan brechas debido a la modificación de cookies.

Gestión de sesiones. Permite configurar tiempos límite globales para la inactividad de usuarios.

Medidas anti-evasión. Normalización de peticiones (p.ej., estandarizando nombres de rutas o conjuntos de caracteres cifrados o sospechosos) antes del análisis.

Inspección HTTP. Permite bloquear ataques ocultos en paquetes cifrados por SSL.

Funciones de aceleración. Incluye caché de contenidos, compresión y multiplexación de conexiones. Mejora el rendimiento de las páginas Web protegidas, reduciendo considerablemente los costes de transacción.

Encubrimiento de sitios Web. Impide a los hackers conocer la implementación del servidor Web y explotar sus vulnerabilidades.

Cadena de reglas personalizadas. Permite al administrador crear sus propias reglas y definiciones personalizadas, adicionalmente a las reglas desarrolladas por SonicWALL. Asimismo permite aplicar modelos de seguridad positivos o negativos.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Especificaciones técnicas

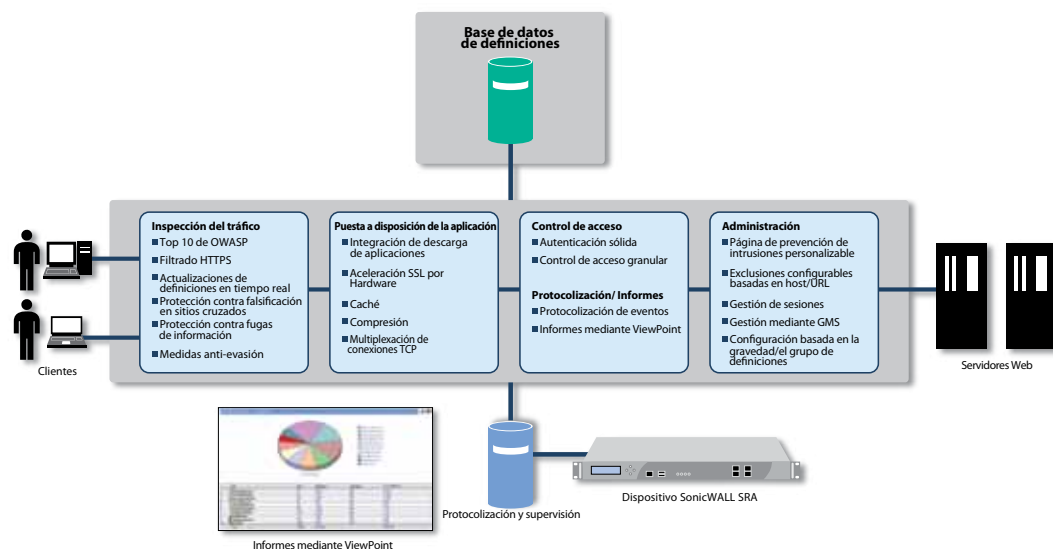


Servicios de suscripción

- SonicWALL Web Application Firewall Service para SRA 1200 (1 año)
01-SSC-8877
- SonicWALL Web Application Firewall Service para SRA 1200 (2 años)
01-SSC-8878
- SonicWALL Web Application Firewall Service para SRA 1200 (3 años)
01-SSC-8879
- SonicWALL Web Application Firewall Service para SRA 4200 (1 año)
01-SSC-6055
- SonicWALL Web Application Firewall Service para SRA 4200 (2 años)
01-SSC-6056
- SonicWALL Web Application Firewall Service para SRA 4200 (3 años)
01-SSC-6057

Si desea consultar los números de producto de la línea completa de dispositivos Secure Remote Access de SonicWALL, visite www.sonicwall.com.

Arquitectura SonicWALL Web Application Firewall



Dispositivos

- Secure Remote Access 1200
 - Secure Remote Access 4200
 - Secure Remote Access Virtual Appliance
- Se requiere suscripción a Web Application Firewall Service*

Capacidad

- Rendimiento SRA 1200: 25 Mbps
- SRA 1200
Servidores back-end soportados: sin restricciones, se recomiendan entre 1 y 5 servidores*
- Rendimiento SRA 4200: 50 Mbps
- SRA 4200
Servidores back-end soportados: sin restricciones, se recomiendan entre 5 y 10 servidores*
- Rendimiento de SRA Virtual Appliance: 250 Mbps*
Servidores back-end soportados por SRA Virtual Appliance: 5-20

**El número real de servidores Web dependerá de su entorno de red, de la configuración de sus políticas y de sus servidores Web y del hardware físico utilizado para los dispositivos virtuales*

Seguridad de las aplicaciones Web

- Validación de protocolo HTTP
- Protección contra ataques comunes
 - Inyección SQL
 - Inyección de comandos de sistema operativo
 - Cross-site scripting
 - Ataques de falsificación de petición en sitios cruzados
- Seguridad adaptable con cadenas de reglas personalizadas
 - Soporte de limitación de velocidad
- Protección contra la modificación de cookies
- Análisis de aplicaciones para la generación automática de reglas (solo SRA 4200)
- Encubrimiento de sitios Web
- Control de respuesta
 - Bloqueo de cliente
 - Redireccionamiento
 - Respuesta personalizada
- Protección contra el robo de datos salientes
 - Protección contra la filtración (DPL) de números de tarjetas de crédito o de la Seguridad Social.
- Actualizaciones automáticas de las definiciones
- Verificación de límite de protocolo
- Control de carga de archivos

Puesta a disposición y aceleración de aplicaciones

- Alta disponibilidad (SRA 4200)
- Descarga SSL
- Equilibrio de carga con reconexión
- Aceleración SSL de hardware (SRA 4200)
- Caché
- Compresión
- Multiplexación de conexiones TCP

Protocolización, supervisión y elaboración de informes

- Protocolización del sistema
- Protocolización de Web Application Firewall
- Protocolización del acceso
- Protocolización de auditoría
- Soporte Syslog
- Informe de cumplimiento PCI
- Panel de estadísticas globales
 - Amenazas detectadas y bloqueadas en todo el mundo
- Estadísticas e informes WAF avanzados
- Integración Viewpoint

Autenticación y autorización

- BANCO DE DATOS LDAP/RADIUS/DE USUARIOS LOCAL
- Certificados de cliente
- Inicio de sesión única
- Autenticación de doble factor
 - RSA Securid
 - VASCO
 - Contraseña de un solo uso

Línea de soluciones de seguridad dinámica de SonicWALL



SEGURIDAD DE RED



ACCESO REMOTO SEGURO



SEGURIDAD DE WEB Y EMAIL



BACKUP Y RECUPERACIÓN



POLÍTICAS Y GESTIÓN

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL Iberia
T + 34 935 041 694
Spain@sonicwall.com

Contactos de soporte SonicWALL
www.sonicwall.com/emea/4724.html