SonicWall Protection Service Suites

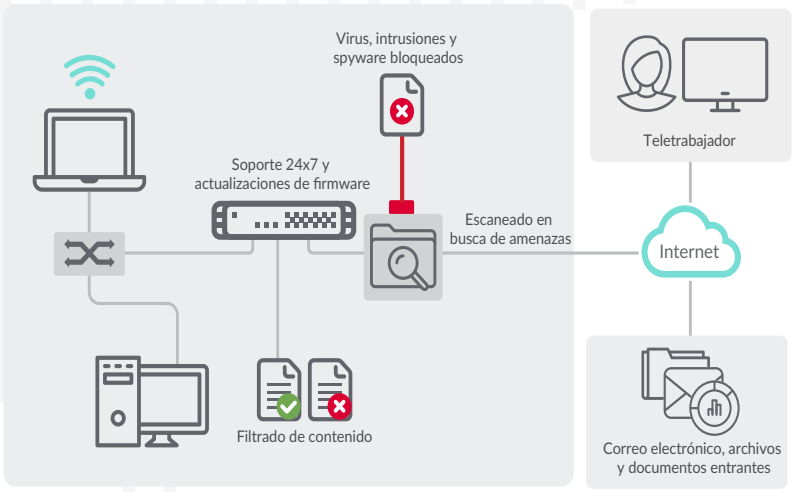
Seguridad de red y gestión de firewall completas en un paquete integrado

Comprender y gestionar una seguridad de red efectiva es un desafío complejo. Afortunadamente, existe una solución sencilla para bloquear los ataques avanzados, evaluar y mitigar el riesgo y facilitar la gestión del firewall.

SonicWall ofrece una amplia gama de servicios de seguridad de red en paquetes cómodos y asequibles: Threat Protection Service Suite, Essential Protection Service Suite y Advanced Protection Service Suite.

VENTAJAS

- Solución completa de seguridad de red.
- Protección antivirus y antispyware en pasarela con certificación ICSA.
- Network Security Manager basado en la nube.
- Comprehensive Anti-Spam Service.
- Tecnología IPS innovadora.
- Inteligencia y control de aplicaciones.
- Seguridad DNS.
- Filtrado de contenido.
- Soporte 24x7 con actualizaciones de firmware y sustitución de hardware.
- Servicio de sandbox multimotor que incluye la tecnología patentada de inspección de memoria profunda en tiempo real de SonicWall (RTDMI™).



FICHA TÉCNICA

Prestaciones y ventajas

Los servicios de protección contra amenazas mantienen su red a salvo de virus, intrusiones, botnets, spyware, troyanos, gusanos y otros ataques maliciosos. En cuanto se identifican las nuevas amenazas (a menudo, antes de que los fabricantes de software pongan a disposición los parches correspondientes), los firewalls de SonicWall y la base de datos de Capture Cloud se actualizan automáticamente con las definiciones que protegen contra estas amenazas. Todos los firewalls de SonicWall incluyen un motor RTDMI™ patentado que escanea el tráfico en busca de múltiples tipos de aplicaciones y protocolos. Gracias a ello, su red estará protegida contra ataques tanto internos como externos y contra vulnerabilidades de aplicaciones las 24 horas del día.

La herramienta de gestión multi-tenant centralizada SonicWall **Network Security Manager (NSM)**, basada en la nube, le permite gestionar de forma centralizada todas las operaciones de firewall sin cometer errores, al adherirse a flujos de trabajo auditables. Los **informes y análisis** ofrecen visibilidad en una sola consola y le permiten monitorizar y descubrir amenazas mediante la unificación y correlación de registros en todos los firewalls.

Capture ATP Service revoluciona la detección de amenazas avanzadas y el sandboxing con una solución multimotor basada en la nube para detener en la pasarela los ataques desconocidos y de día cero. Capture ATP bloquea los ataques de día cero antes de que accedan a su red. Le permite establecer una protección avanzada contra el cambiante panorama de las amenazas, así como analizar una amplia variedad de tipos de archivos.

La protección antivirus en pasarela con certificación ICSA combina tecnología antimalware basada en la red con una base de datos en la nube que contiene decenas de millones de definiciones de malware. La protección dinámica contra spyware bloquea la instalación de spyware malicioso e interrumpe las comunicaciones de este.

La innovadora tecnología IPS ofrece protección contra gusanos, troyanos, vulnerabilidades de software y otras intrusiones. Para ello, escanea todo el tráfico en busca de patrones maliciosos o anómalos, aumentando así la fiabilidad y el rendimiento de la red.

Las **funciones de inteligencia y control de aplicaciones** son un conjunto de políticas granulares para aplicaciones específicas que incorporan tecnología de clasificación de aplicaciones y refuerzo de políticas para ayudar a los administradores a controlar y gestionar tanto las aplicaciones corporativas como las aplicaciones ajenas al negocio.

SonicWall **Comprehensive Anti-Spam Service** ofrece a pequeñas y medias empresas más de un 99 % de efectividad frente al spam y deja más del 80 % del spam en la pasarela, al tiempo que utiliza técnicas antispam avanzadas como Adversarial Bayesian™ y filtrado mediante aprendizaje automático.

Content Filtering Services (CFS) le permite reforzar las políticas sobre el uso de Internet y controlar el acceso interno a contenido Web inapropiado, improductivo y potencialmente ilegal, gracias al filtrado completo del contenido. El Servicio de filtrado de contenido basado en la reputación **CFS 5.0** proporciona una puntuación de la reputación que predice el riesgo de seguridad de una URL a través de 93 categorías web.

El **filtrado DNS** bloquea las páginas web o aplicaciones maliciosas en la capa de DNS para filtrar y expulsar el contenido dañino o inapropiado sin activar el descifrado TLS ni comprometer el rendimiento.

Los **puntos de acceso** altamente seguros de SonicWall pueden gestionarse a través de la nube con SonicWall Wireless Network Manager (WNM) o mediante los firewalls de SonicWall, ofreciendo facilidad de gestión e integración fluida con los productos inalámbricos de SonicWall.

La integración del **control de acceso a la red** con Aruba ClearPass proporciona control de acceso a la red para los clientes de SonicWall y ofrece funciones completas y precisas de elaboración de perfiles, autenticación y autorización para los sistemas y dispositivos que intenten acceder a sus recursos de TI. SonicOS proporciona una API RESTful que soporta Aruba ClearPass como sistema de Control del acceso a la red para integrarse con el NGFW de SonicWall. Esta arquitectura convertirá la seguridad estática en seguridad contextual para ofrecer una protección más flexible y avanzada.

El **soporte 24x7** con actualizaciones de firmware y sustitución de hardware protege su negocio y su inversión en tecnología SonicWall. Incluye el acceso a soporte telefónico y a través de la Web las 24 horas para asistencia básica sobre configuración y resolución de problemas, así como la sustitución del hardware, en caso de que se produzca un fallo.

PRESTACIÓN	THREAT PROTECTION SECURITY SUITE*	ESSENTIAL PROTECTION SECURITY SUITE	ADVANCED PROTECTION SECURITY SUITE
Soporte 24x7	S	S	S
IPS	S	S	S
Control de aplicaciones	S	S	S
Content Filtering Service	S	S	S
Antivirus en pasarela	S	S	S
Seguridad DNS (básica)	S	S	S
Filtrado DNS	N	N	S
Integración del Control de acceso a la red (NAC) con Aruba ClearPass	S	S	S
Integración de Wi-Fi 6	S	S	S
Inspección profunda de paquetes para SSL	S	S	S
Actualizaciones GeoIP	S	S	S
Botnet Service	S	S	S
Comprehensive Anti-Spam Service	N	S	S
Capture ATP - Sandboxing (estática, RTDMI, memoria, hipervisor, emulación)	N	S	S
Gestión NSM (nube)	N	N	S
Informes NSM (nube, retención de 7 días)	N	N	S

* Disponible solo en TZ 270, 370 y 470

Acerca de SonicWall

SonicWall proporciona una ciberseguridad estable, escalable y fluida para la era hiperdistribuida, así como una realidad laboral caracterizada por la movilidad, el teletrabajo y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la ciberseguridad para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com