

# Advanced Gateway Security Suite

Seguridad de red completa en un paquete integrado

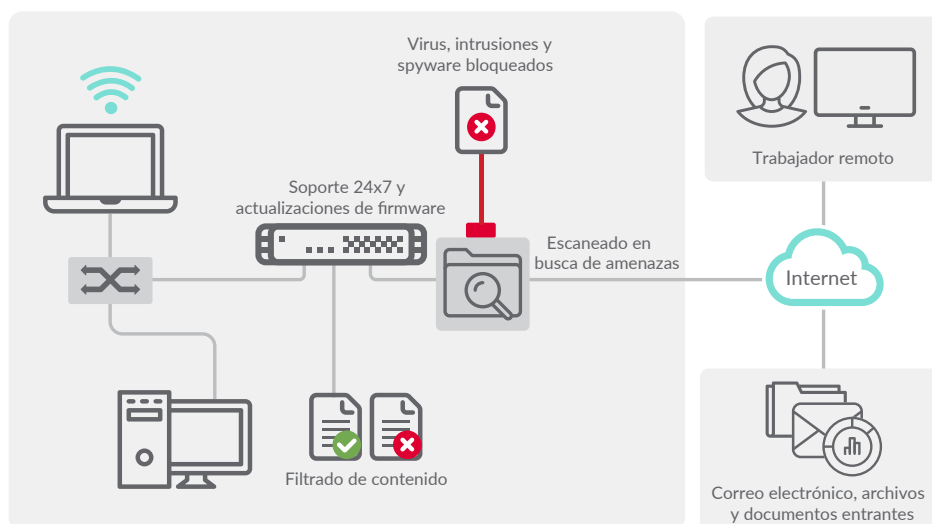
Entender la seguridad de red puede ser una tarea muy difícil. Sin embargo, proteger su red contra amenazas maliciosas, tanto conocidas como desconocidas, no debería serlo. SonicWall Advanced Gateway Security Suite (AGSS) le ahorra la difícil tarea de elegir numerosos servicios de seguridad adicionales, ya que integra todos los servicios necesarios para garantizar la protección total de su red en un paquete cómodo y asequible.

Disponible en todos los dispositivos físicos y virtuales, incluidos los de las series NSsp, NSa, TZ y NSv, SonicWall AGSS protege su red contra los ataques de día cero, virus, intrusiones, botnets, spyware, troyanos, gusanos y otros ataques maliciosos. Inspeccione los archivos sospechosos en la pasarela en un sandbox multicapa basado en la nube para proteger su red contra las amenazas desconocidas. Nada más se identifican las nuevas amenazas (y a menudo antes de que los fabricantes

de software pongan a disposición los correspondientes parches), 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 RFDPI (Reassembly-Free Deep Packet Inspection®) patentado que escanea el tráfico para 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. Además, gracias al filtrado completo del contenido, su solución SonicWall ofrece las herramientas necesarias para reforzar las políticas sobre el uso de Internet y controlar el acceso interno a contenido Web inapropiado, improductivo y potencialmente ilegal. Por último, este paquete de servicios incluye también soporte técnico las 24 horas del día, actualizaciones vitales de firmware y sustitución de hardware.

## Ventajas:

- Solución completa de seguridad de red
- Protección antivirus y anti-spyware en pasarela con certificación ICASA
- Tecnología IPS innovadora
- Inteligencia y control de aplicaciones
- Filtrado de contenido
- Soporte 24x7 con actualizaciones de firmware y sustitución de hardware
- Sandbox de red multimotor con SonicWall RTDMI
- Gestión basada en la nube desde una única consola



## Advanced Gateway Security Suite

NSsp 12800 (1 año)  
01-SSC-6591

NSsp 12400 (1 año)  
01-SSC-6588

NSa 9650 (1 año)  
01-SSC-2036

NSa 9450 (1 año)  
01-SSC-0414

NSa 9250 (1 año)  
01-SSC-0038

NSa 6650 (1 año)  
01-SSC-8761

NSa 5650 (1 año)  
01-SSC-3674

NSa 4650 (1 año)  
01-SSC-3493

NSa 3650 (1 año)  
01-SSC-3451

NSa 2650 (1 año)  
01-SSC-1783

Serie TZ600 (1 año)  
01-SSC-1460

Serie TZ500 (1 año)  
01-SSC-1450

Serie TZ400 (1 año)  
01-SSC-1440

Serie TZ300 (1 año)  
01-SSC-1430

NSv 1600 (1 año) 01-SSC-5787

NSv 800 (1 año) 01-SSC-5737

NSv 400(1 año) 01-SSC-5681

NSv 300 (1 año) 01-SSC-5584

NSv 200 (1 año) 01-SSC-5306

NSv 100 (1 año) 01-SSC-5219

NSv 50 (1 año) 01-SSC-5194

NSv 25 (1 año) 01-SSC-5165

NSv 10 (1 año) 01-SSC-5008

Hay disponibles números SKU de varios años.

Si desea consultar los números de producto de la línea completa de firewalls de SonicWall, visite [www.sonicwall.com](http://www.sonicwall.com).

SonicWall Advanced Gateway Security Suite incluye:

- Suscripción a Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service
- Suscripción a Content Filtering Service
- Suscripción al servicio de soporte 24x7
- Suscripción a Capture Advanced Threat Protection (ATP) Service
- Suscripción a Capture Security Center Lite

### Prestaciones y ventajas

Solución completa de seguridad de red. Integra todo lo necesario para que su red esté completamente protegida contra amenazas como ransomware, virus, spyware, gusanos, troyanos, adware, keyloggers, código móvil malicioso (MMC) y otras aplicaciones y contenidos Web peligrosos.

Capture Advanced Threat Protection (ATP) Service revoluciona la detección de amenazas avanzadas y el sandboxing con una solución multimotor basada en la nube para detener los ataques de día cero desconocidos en la pasarela, y con la implementación automática de definiciones.

Capture ATP incluye la tecnología de Inspección profunda de memoria en tiempo real (RTDMI) de SonicWall, que detecta y bloquea el malware que no muestra ningún comportamiento malicioso u oculta su mecanismo mediante el cifrado. Al obligar al malware a revelar su mecanismo en la memoria, el motor RTDMI detecta y bloquea de forma proactiva las amenazas de día cero y el malware desconocido del mercado de masas utilizando técnicas precisas de Inspección de memoria profunda en tiempo real.

La protección antivirus y anti-spyware 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 para ofrecer una protección profunda contra las avanzadas amenazas de hoy en día.

La tecnología IPS innovadora 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.

Funciones de inteligencia y control de aplicaciones. Proporcionan 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.

Filtrado de contenido. Evita problemas de seguridad y productividad proporcionando los controles necesarios para reforzar las políticas sobre el uso de Internet y bloquear el acceso al contenido Web dañino e improductivo.

Soporte 24x7 con actualizaciones de firmware y sustitución de hardware. Protege su negocio y su inversión en tecnología SonicWall ofreciendo actualizaciones y ampliaciones de firmware, el más sofisticado soporte técnico, la sustitución rápida de hardware y acceso a herramientas electrónicas de autoayuda.

Capture Security Center Lite le permite gestionar su implementación SonicWall y realizar backups/restauraciones de sus preferencias de firewall, todo ello desde una única consola y en la nube.

### Los servicios AGSS

Sandbox multimotor, Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention, Application Intelligence and Control Service

- Motor antivirus en pasarela en tiempo real. Rastrea la red en tiempo real en busca de virus, gusanos, troyanos y demás amenazas de Internet.
- Protección dinámica contra spyware. Bloquea la instalación de spyware malicioso e interrumpe las comunicaciones del spyware.
- Potente prevención de intrusiones. Protege contra una gran variedad de amenazas basadas en la red, como gusanos, troyanos y otros tipos de código malicioso.
- Inteligencia y control de aplicaciones. Proporciona funciones de clasificación de aplicaciones y refuerzo de políticas.

- Base de datos de definiciones actualizada automáticamente. Proporciona protección continua contra las amenazas.
- Sandbox multimotor con RTDMI para prevenir amenazas desconocidas, como los ataques de día cero o el ransomware.

#### **Capture Advanced Threat Protection (Capture ATP)**

- Bloquee los ataques de día cero antes de que accedan a su red.
- Implemente definiciones de las amenazas rápidamente en otros dispositivos de seguridad de red.
- Proporcione protección avanzada contra el cambiante panorama de las amenazas.
- Analice una amplia variedad de tipos de archivos.

#### **Content Filtering Service (CFS)**

- Filtrado completo del contenido. Permite controlar de forma personalizada el acceso interno a contenido Web inapropiado, improductivo y potencialmente ilegal.
- Clasificaciones de sitios Web guardadas en el caché local. Se guardan en los firewalls SonicWall, de modo que el tiempo de respuesta para sitios muy visitados es prácticamente instantáneo.

- Arquitectura de clasificación actualizada dinámicamente. Coteja las páginas Web solicitadas con una base de datos en la nube que contiene millones de URLs, direcciones IP y dominios y a continuación compara cada clasificación con las políticas de seguridad locales.

#### **Content Filtering Client**

- Detenga el malware de forma rápida y precisa con la Inspección profunda de memoria en tiempo real (RTDMI).
- Con SonicWall Content Filtering Client, puede ampliar la seguridad y la productividad aplicando las políticas sobre el uso de Internet en los dispositivos terminales situados fuera del perímetro del firewall. Disponible como servicio de suscripción separado para puntos terminales Windows, Mac OS y Chrome.

#### **Soporte 24x7**

- Actualizaciones y ampliaciones de software y firmware para mantener su red siempre protegida y su solución tan efectiva como si fuera nueva.
- Acceso a soporte telefónico y a través de la Web las 24 horas del día para tareas básicas de configuración y para la resolución de problemas.

- Sustitución de hardware en caso de que se produzca un fallo.
- Suscripción anual a los boletines de servicios de SonicWall y acceso a las herramientas electrónicas de soporte y a grupos de discusión moderados.

#### **Capture Security Center Lite\***

- Portal basado en la nube
- Gestión desde una única consola
- Backup y restauración de sus preferencias de firewall

Si desea obtener más información sobre SonicWall Advanced Gateway Security Suite, visite [www.sonicwall.com](http://www.sonicwall.com).

#### **Acerca de nosotros**

SonicWall lleva más de 27 años combatiendo la industria del crimen cibernético y defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución automatizada de detección y prevención de brechas en tiempo real adaptada a las necesidades específicas de más de 500.000 organizaciones en más de 215 países y territorios, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

\*Para las series SuperMassive 9000, NSa 9250/9450/9650 y NSp 12000, la Gestión CSC está disponible automáticamente al activar la correspondiente suscripción a AGSS