



# SonicWALL Application Intelligence, Control and Visualization

CORTAFUEGOS

Inteligencia, control granular y visualización de aplicaciones

Los administradores de TI se enfrentan hoy a un reto importante: tienen que garantizar la disponibilidad y eficacia de las aplicaciones críticas de negocio, y al mismo tiempo, controlar el uso que los empleados hacen de aplicaciones, a menudo peligrosas, que requieren un elevado ancho de banda. Priorizar el ancho de banda para las aplicaciones críticas es imprescindible, al igual que lo es frenar o incluso bloquear por completo el consumo de ancho de banda de las aplicaciones de medios sociales o juegos. Los cortafuegos de inspección dinámica de paquetes que todavía utilizan muchas organizaciones simplemente no son capaces de solucionar este problema, ya que su tecnología basada en puertos y protocolos no es apta para identificar las aplicaciones. Dicho de otra manera: los cortafuegos de inspección dinámica de paquetes no tienen "inteligencia" suficiente para distinguir entre los "buenos" y los "malos".

Al escanear cada byte y cada paquete del tráfico de red, SonicWALL® determina exactamente qué aplicaciones están activas y quién las está utilizando, proporcionando así inteligencia y control de aplicaciones, independientemente del puerto o protocolo. Los cortafuegos de próxima generación de SonicWALL ofrecen una base de datos de definiciones de amenazas en continua expansión que reconoce miles de aplicaciones y millones de amenazas de malware para proteger la red completa de forma automática. La solución de SonicWALL detecta malware, intrusiones, fugas de datos y violaciones de políticas antes de que causen daños a la red corporativa o a sus usuarios.

Con su nueva facilidad de uso y gestión, SonicWALL Application Intelligence and Control devuelve el control a los administradores de TI, poniendo en sus manos una herramienta eficaz para la supervisión de las aplicaciones y los usuarios. Los administradores pueden crear fácilmente políticas de gestión del ancho de banda basadas en categorías predefinidas (como p.ej., medios sociales o juegos), aplicaciones individuales e incluso usuarios y grupos. Nada más surgen nuevas aplicaciones, los cortafuegos reciben automáticamente las definiciones apropiadas. Las políticas correspondientes se actualizan automáticamente sin que los administradores tengan que gastar tiempo en ese tipo de tareas. Gracias al análisis del tráfico de aplicaciones, los administradores pueden reaccionar con mayor rapidez y eficacia a las interrupciones de la red y a las amenazas de seguridad, garantizando así el rendimiento inmediato de la inversión. Asimismo, los análisis del tráfico de aplicaciones proporcionan una visión completa de los eventos y las actividades que contribuye a fomentar la concienciación sobre la seguridad y permite gestionar el uso de la red por parte de los empleados.

Application Intelligence and Control está disponible o bien en combinación con SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention (suscripción de 1, 2 ó 3 años) o bien integrada en las suscripciones SonicWALL Comprehensive Gateway Security Suite para los cortafuegos de las series TZ 210, Network Security Appliance (NSA) y E-Class NSA.

## Prestaciones y ventajas

**Inteligencia de aplicaciones.** Escanea cada paquete mediante la tecnología Reassembly-Free Deep Packet Inspection™ de SonicWALL para determinar qué aplicaciones están activas y quién las está utilizando. SonicWALL utiliza una base de datos continuamente actualizada para proteger las redes de forma automática.

**Control de aplicaciones.** Permite definir políticas de aplicaciones flexibles y configurables para frenar o bloquear aplicaciones, archivos, URLs, y archivos adjuntos al correo electrónico según tipo de aplicación, usuario de red, horarios, definiciones personalizadas, etc.

**Visualización de aplicaciones.** Proporciona gráficos en tiempo real de las aplicaciones, del ancho de banda entrante y saliente consumido, de los sitios Web que están siendo visitados, de los usuarios, etc. Asimismo, permite exportar la misma información a cualquier herramienta de análisis NetFlow/IPFIX para procesar fuera de línea los datos históricos de la actividad de red (monitoreo, diagnóstico, resolución de errores).

El **análisis del tráfico de aplicaciones** proporciona análisis históricos y en tiempo real de los datos transmitidos a través del cortafuegos, incluidas las actividades que realizan los usuarios con las aplicaciones.

**Prevención de fuga de datos.** Bloquea y controla la salida no autorizada de datos sensibles o bien a través de descargas FTP, o bien como archivos adjuntos de servicios de e-mail personales como Hotmail® o Gmail® o como correos electrónicos corporativos SMTP y POP3.

**Gestión del ancho de banda a nivel de aplicaciones.** Garantiza la calidad de servicio (QoS) asignando niveles de rendimiento para aplicaciones o grupos de misión crítica según diferentes horas del día.

**Notificaciones y actualizaciones automatizadas.** Facilita la gestión garantizando una protección fiable contra las más recientes amenazas.

**Inspección profunda de paquetes para tráfico SSL.** Extiende la protección al tráfico cifrado por SSL, garantizando el cumplimiento óptimo de las normas, el filtrado de contenidos y la prevención de fuga de datos y eliminando un posible canal para el malware. El tráfico cifrado se descifra, se inspecciona y se vuelve a cifrar de forma transparente para el usuario, pudiéndose configurar tanto para conexiones entrantes como salientes.\*

\*01-SSC-8680 Licencia de ampliación DPI SSL para NSA 220 y superior.

**SONICWALL**®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

- **Inteligencia de aplicaciones**
- **Control de aplicaciones**
- **Visualización de aplicaciones**
- **Suite de análisis del tráfico de aplicaciones**
- **Prevención de fugas de datos**
- **Gestión del ancho de banda a nivel de aplicaciones**
- **Actualizaciones y notificaciones automatizadas**
- **Inspección profunda de paquetes para tráfico SSL**

## Cortafuegos de próxima generación con inteligencia, control y visualización de aplicaciones

### Identificar

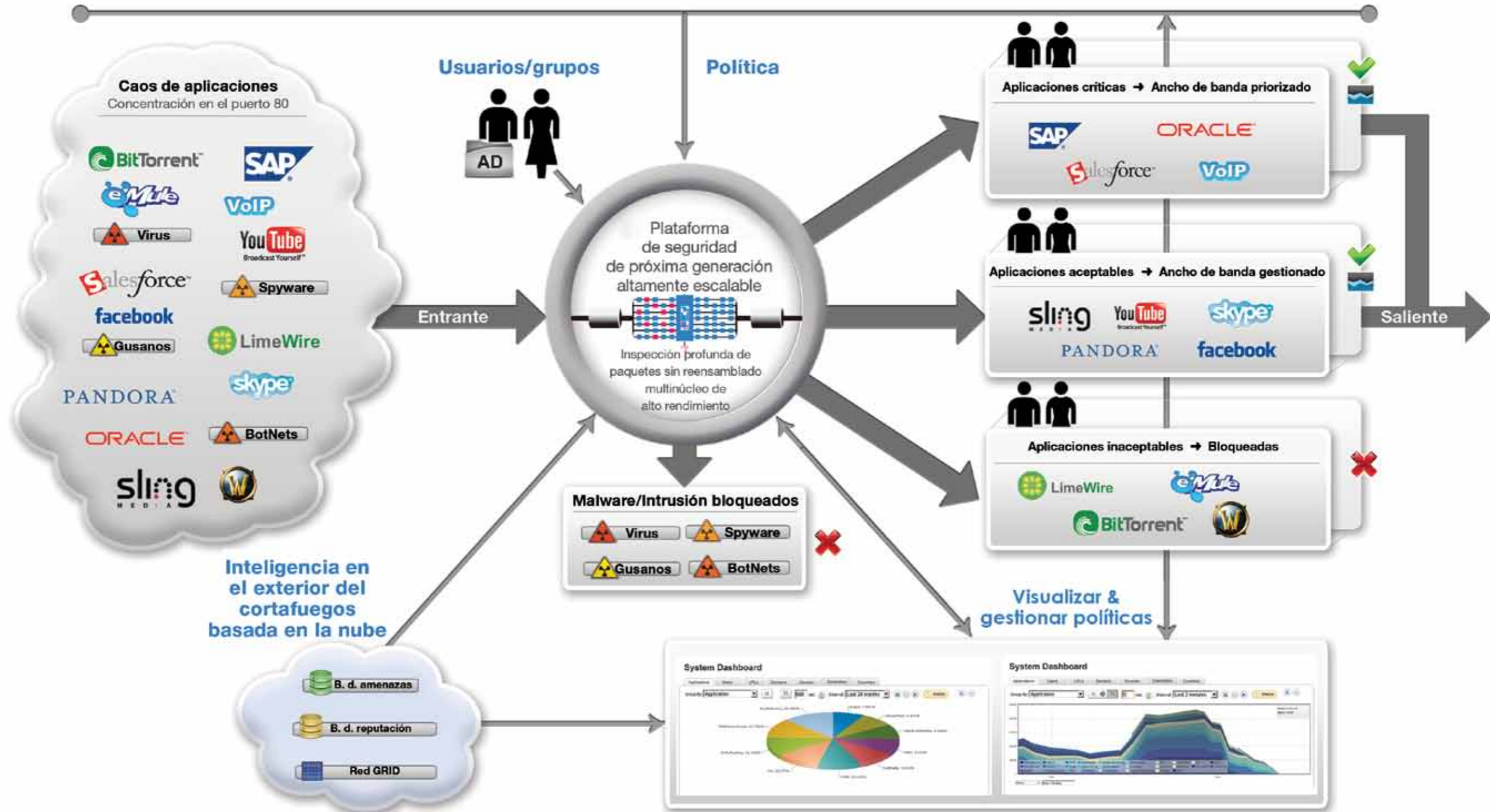
- Según aplicación
  - No según puerto y protocolo
- Según usuario/grupo
  - No según IP
- Según inspección de contenido
  - No según nombre de archivo

### Clasificar

- Según aplicación
- Según categoría de aplicación
- Según destino
- Según contenido
- Según usuario/grupo

### Controlar

- Priorizar aplicaciones según políticas
- Gestionar aplicaciones según políticas
- Bloquear aplicaciones según políticas
- Detectar y bloquear malware
- Detectar y bloquear tentativas de intrusión



# Especificaciones técnicas



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

NSA E7500 (1 año)  
01-SSC-6130

NSA E6500 (1 año)  
01-SSC-6131

NSA E5500 (1 año)  
01-SSC-6132

NSA 5000 (1 año)  
01-SSC-6159

NSA 4500 (1 año)  
01-SSC-6133

NSA 3500 (1 año)  
01-SSC-6134

NSA 2400 (1 año)  
01-SSC-6135

Serie NSA 250M (1 año)  
01-SSC-4570

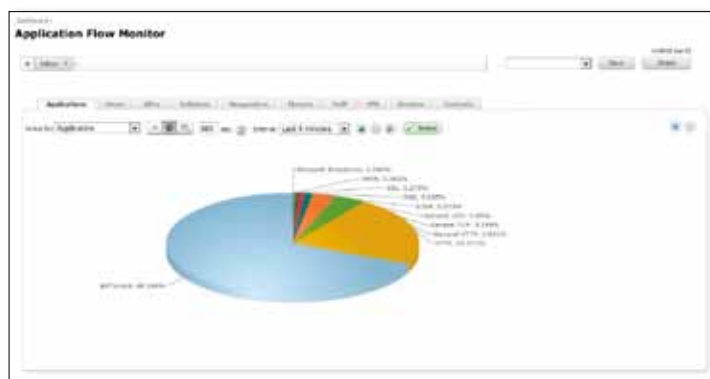
Serie NSA 220 (1 año)  
01-SSC-4612

TZ 210 Series (1 año)  
01-SSC-6165

También hay disponibles servicios de suscripción de varios años. Si desea consultar los números de producto de la línea completa de dispositivos de seguridad de red de SonicWALL, visite [www.sonicwall.com](http://www.sonicwall.com).

## Visualización de aplicaciones

Los gráficos en tiempo real de las aplicaciones, del ancho de banda entrante y saliente, de los sitios Web visitados y de todas las actividades de los usuarios permiten a los administradores modificar las reglas de las aplicaciones para adaptarlas a las políticas de red.



## Lista de prestaciones

### Funciones de inteligencia de aplicaciones

- Escanea e identifica todo el tráfico independientemente de puertos o protocolos para garantizar un control completo
- Función de prevención de fugas de datos con contenidos a supervisar definidos por el usuario
- Gestión del ancho de banda a nivel de aplicaciones basado en una extensa base de datos de definiciones de aplicaciones en constante crecimiento y en potentes funciones de creación de reglas
- Acciones predefinidas y personalizadas: protocolizar, protocolizar y bloquear, mensajes de usuario personalizados, eludir DPI y gestión del ancho de banda
- Inspección profunda del tráfico que utiliza protocolos con cifrado SSL

### Base de datos de definiciones

- Base de datos actualizada dinámicamente con miles de definiciones de aplicaciones y de contenidos

### Protocolización y análisis del tráfico de aplicaciones

- Informes syslog avanzados de próxima generación
- Análisis del tráfico de aplicaciones mediante SonicWALL Analyzer, Scrutinizer o Global Management System
- Netflow/IPFIX con protocolización de extensiones para el análisis y la visualización "off-the-box" adicionales del tráfico

### Escalabilidad

- Capacidad para escanear un número elevado de descargas simultáneas con cualquier tamaño de archivo

Si desea más información sobre los servicios de seguridad de SonicWALL de valor añadido, como Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Application Intelligence and Control, Comprehensive Anti-Spam Service, Enforced Client Anti-Virus and Anti-Spyware and Content Filtering Service, visite nuestra página Web en <http://www.sonicwall.com>.



### SonicWALL Iberia

T + 34 935 041 694  
Spain@sonicwall.com

### Contactos de soporte SonicWALL

[www.sonicwall.com/emea/4724.html](http://www.sonicwall.com/emea/4724.html)

### 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™