



# SonicWALL Content Filtering Service

CORTAFUEGOS

**Solución dinámica y escalable para bloquear el contenido Web no productivo**

- **Filtrado granular de contenido**
- **Arquitectura de clasificación actualizada dinámicamente**
- **Cumplimiento de normas y elaboración de informes**
- **Gestión sencilla basada en Web**
- **Arquitectura de clasificación y caché de sitios Web de alto rendimiento**
- **Filtrado de contenido HTTPS basado en IP**
- **Solución rentable y escalable**

Hoy en día, cualquier usuario con un navegador puede acceder sin problemas a páginas Web ilegales o inapropiadas. Estas páginas, aparte de frenar la productividad de los empleados, a menudo contienen malware que no sólo puede utilizarse para robar información confidencial, sino que además puede exponer a la organización a riesgos como el incumplimiento de normas, la denegación de fondos de fomento e incluso la responsabilidad penal. Un ejemplo de estos requerimientos legales en EE.UU. es que las escuelas y bibliotecas inscritas en el programa E-Rate están obligadas por ley a instalar una solución de filtrado de contenido de acuerdo con la ley CIPA (del inglés Children's Internet Protection Act, Ley de Protección de Niños en Internet).

SonicWALL® Content Filtering Service (CFS) ofrece una solución de filtrado de contenido sin igual para empresas, instituciones educativas, bibliotecas, agencias gubernamentales y terminales de Internet públicos. CFS está disponible como servicio de suscripción para todos los cortafuegos SonicWALL TZ, Network Security Appliance (NSA) o E-Class NSA, como parte de la suite Comprehensive Gateway Security o como suscripción TotalSecure. Pensada para organizaciones de todos los tamaños, la solución de SonicWALL bloquea el contenido inapropiado, reduce el riesgo de responsabilidad legal e incrementa la productividad.

SonicWALL CFS utiliza una amplia base de datos con millones de URLs, direcciones IP y sitios Web. Con su arquitectura de clasificación y caché de alto rendimiento, CFS actualiza las clasificaciones de forma dinámica y local en un cortafuegos de seguridad de red SonicWALL para poder realizar una comparación instantánea. Con CFS, los administradores pueden aplicar políticas de acceso o bloqueo basándose en más de 59 categorías de URL, la identidad del individuo o grupo, o la hora del día.

## Prestaciones y ventajas

**Filtrado granular de contenido.** Permite al administrador bloquear y gestionar el ancho de banda para todas las categorías predefinidas, o cualquier combinación de categorías. Los administradores pueden aplicar la autenticación a nivel de usuario (ULA) y el inicio de sesión único (SSO) para imponer el inicio de sesión mediante nombre de usuario y contraseña. CFS puede bloquear el contenido potencialmente peligroso, como Java™, ActiveX®, y Cookies y programar el filtrado según la hora del día, (p.ej., durante el horario escolar o comercial). Además, CFS mejora el rendimiento, ya que elimina las aplicaciones de mensajería instantánea y MP3, los flujos de datos multimedia, el freeware y otros archivos con un consumo elevado de ancho de banda.

**Arquitectura de clasificación actualizada dinámicamente.** Compara las páginas Web solicitadas con una base de datos de alta precisión que incluye millones de URLs, direcciones IP y dominios. El cortafuegos SonicWALL recibe clasificaciones en tiempo real, y las compara con las políticas de seguridad locales. A continuación, el dispositivo acepta o bloquea la solicitud, basándose en las políticas configuradas a nivel local por el administrador.

**Cumplimiento de normas e informes.** Gracias a la integración directa con el galardonado Sistema de gestión global de SonicWALL (GMS®) y el paquete de informes SonicWALL ViewPoint™, la solución permite elaborar informes gráficos detallados o "de un vistazo" a partir de los datos propios de CFS en tiempo real o históricos.

**Gestión sencilla basada en Web.** Permite configurar políticas de forma flexible y tener un control

completo sobre el uso de Internet. Los administradores pueden reforzar múltiples políticas personalizadas para usuarios individuales, grupos o determinados tipos de categorías. Gracias a los filtros de URL locales, es posible aceptar o rechazar determinados dominios o hosts. Para bloquear con mayor eficacia el contenido dudoso, los administradores también pueden crear o personalizar bases de datos de filtrado.

**Arquitectura de clasificación y caché de sitios Web de alto rendimiento.** Permite a los administradores bloquear sitios Web de forma sencilla y automática según categorías. Las clasificaciones de URL se guardan en caché de forma local en el cortafuegos SonicWALL. De esta manera se consigue reducir el tiempo de acceso a las páginas que se visitan con frecuencia a tan solo una fracción de segundo.

**Filtrado de contenido HTTPS basado en IP.** Permite a los administradores controlar el acceso de los usuarios a las páginas Web mediante HTTPS cifrado. El filtrado HTTPS está basado en la clasificación por categorías de los tipos de páginas Web con contenido inapropiado, como p.ej., juegos, banca online, compraventa de acciones online, compras, así como páginas de hackers o de puenteo de proxys.

**Solución rentable y escalable.** Controla el filtrado de contenido desde el cortafuegos SonicWALL, eliminando la necesidad de disponer de hardware adicional y evitando los gastos derivados de implementar un servidor de filtrado separado.

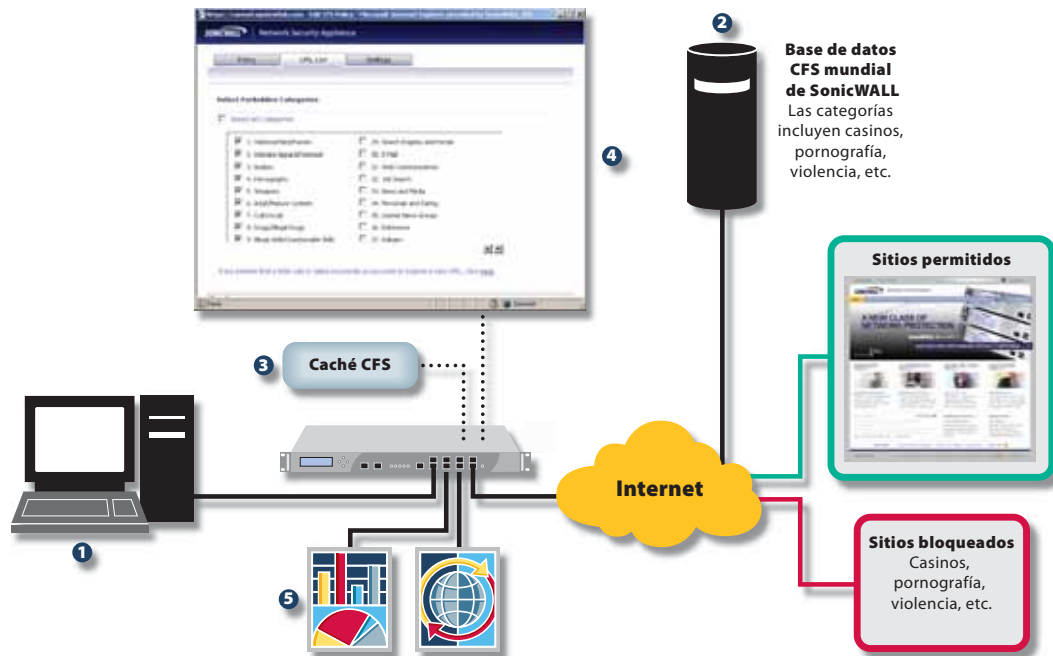
**SONICWALL**®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

# Especificaciones técnicas

## Arquitectura de SonicWALL Content Filtering Service

Administrado mediante una interfaz intuitiva, SonicWALL Content Filtering Service (CFS) permite que tanto el filtrado como el control tengan lugar directamente en la LAN, WLAN o VPN. Al combinarse con los dispositivos de seguridad de red SonicWALL escalables y de alto rendimiento y con las eficaces prestaciones de informes y gestión del Sistema de gestión global de SonicWALL, CFS ofrece una solución de filtrado integrada, sencilla y altamente gestionable para organizaciones de todos los tamaños.



- 1 Usuario SonicWALL CFS
- 2 Base de datos distribuida de clasificaciones de SonicWALL CFS
- 3 Caché de clasificaciones locales de sitios aceptables
- 4 Políticas URL establecidas para bloquear los sitios Web cuestionables o contraproductivos
- 5 Informes mediante SonicWALL ViewPoint o GMS

Prestaciones	CFS Premium
Categorías	59
Políticas usuario/grupo	Sí
Clasificación dinámica	Sí
Informes	ViewPoint*
Caché de páginas Web	Sí
Refuerzo de búsqueda segura	Sí
Refuerzo de políticas CFS por rango IP	Sí

\* ViewPoint se vende por separado.

Disponible en	CFS Premium
TZ 180/180W	Sí
TZ 190/190W	Sí
TZ 100/100W	Sí
TZ 200/200W	Sí
TZ 210/210W	Sí
Serie NSA	Sí
Serie E-Class NSA	Sí

Si desea obtener más información sobre SonicWALL Content Filtering Service y nuestra completa línea de soluciones de seguridad, visite nuestra página Web en <http://www.sonicwall.com>.

### Gama 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 Content Filtering Service

NSA E8500 (1 año)  
01-SSC-8943

NSA E7500 (1 año)  
01-SSC-7329

NSA E6500 (1 año)  
01-SSC-7330

NSA E5500 (1 año)  
01-SSC-7331

NSA 4500 (1 año)  
01-SSC-7346

NSA 3500 (1 año)  
01-SSC-7333

NSA 2400 (1 año)  
01-SSC-7334

Serie NSA 240 (1 año)  
01-SSC-7335

Serie TZ 210 (1 año)  
01-SSC-7371

Serie TZ 200 (1 año)  
01-SSC-8634

Serie TZ 100 (1 año)  
01-SSC-8637

Series TZ 180 y TZ 190 (1 año)  
01-SSC-5650

También hay disponibles números de producto para Content Filtering Service de varios años.

### SonicWALL Iberia

T + 34 653 948 287  
Spain@sonicwall.com

### Contactos de soporte SonicWALL

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

**SONICWALL**

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™