Content Filtering Service y Content Filtering Client

Potente solución de protección y productividad para bloquear el acceso a contenido Web dañino e improductivo

Las instituciones educativas, empresas y agencias gubernamentales asumen riesgos considerables al proporcionar a sus alumnos y empleados ordenadores gestionados por el departamento de TI con acceso a Internet, incluso si el equipo se halla dentro del perímetro del firewall, donde se refuerzan las políticas internas sobre el uso de la Web. El problema es especialmente grave cuando los usuarios acceden a sitios que contienen información o imágenes inapropiadas, peligrosas o incluso ilegales. Además, estos sitios pueden estar infectados con malware que puede descargarse involuntariamente y que los ciberdelincuentes pueden utilizar para robar información confidencial.

Las escuelas, en particular, son responsables de proteger a los alumnos contra el contenido Web inapropiado y dañino. Además, para recibir financiamiento del programa E-Rate, tanto las escuelas como las bibliotecas 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). Para las empresas y agencias gubernamentales, proporcionar a los empleados acceso a la Web no controlado puede llevar a un uso improductivo, dando lugar a enormes pérdidas de productividad, por no hablar del riesgo de responsabilidad legal.

En combinación con una solución de Gestión unificada de amenazas o un firewall de próxima generación de SonicWall, SonicWall Content Filtering Service (CFS) proporciona una eficaz solución de protección y productividad que incluye funciones incomparables de filtrado de contenido para instituciones educativas, empresas, bibliotecas y agencias gubernamentales. Con SonicWall CFS, las organizaciones pueden controlar las páginas Web a las que tienen acceso los alumnos y empleados desde sus ordenadores gestionados por el departamento de TI y situados detrás del firewall.

SonicWall CFS compara las páginas Web solicitadas con una enorme base de datos en la nube que contiene millones de URLs, direcciones de IP y páginas Web clasificadas. CFS proporciona a los administradores las herramientas necesarias para crear y aplicar políticas que permitan o denieguen el acceso a los sitios Web en función de la identidad del individuo o grupo, o de la hora del día, para más de 56 categorías predefinidas. Además, CFS guarda en caché las clasificaciones de los sitios Web de forma dinámica en el firewall de SonicWall para ofrecer tiempos de respuesta casi instantáneos.

Con el fin de evitar problemas de seguridad y productividad en los ordenadores portátiles que se utilizan fuera del perímetro del firewall, el cliente de filtrado de contenido SonicWall Content Filtering Client aplica los controles también en estos equipos para bloquear el contenido Web dañino e improductivo. El cliente se implementa automáticamente y se pone a disposición a través de un firewall de SonicWall. Además de proporcionar a los administradores de TI las herramientas necesarias para controlar el acceso basado en Web desde dispositivos itinerantes, Content Filtering Client puede configurarse para cambiar automáticamente a las políticas internas una vez que el dispositivo se reconecta al firewall de la red. El cliente es gestionado y monitorizado utilizando un potente motor de políticas e informes en la nube al que puede accederse fácilmente desde la interfaz del firewall. Si un cliente anticuado intenta conectarse a la red interna para acceder a Internet, se rechaza la conexión y el usuario recibe un mensaje con los pasos que debe seguir para actualizar el cliente.

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

Ventajas:

- La mejor protección de su categoría
- Controles de filtrado granular de contenido
- Arquitectura de clasificación actualizada dinámicamente
- Análisis del tráfico de aplicaciones
- 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
- Content Filtering Client para dispositivos itinerantes

SonicWall Content Filtering Service	
NSsp 12800 (1 año)	01-SSC-7850
NSsp 12400 (1 año)	01-SSC-7698
NSa 9650 (1 año)	01-SSC-2136
NSa 9450 (1 año)	01-SSC-1158
NSa 9250 (1 año)	01-SSC-0331
NSa 6650 (1 año)	01-SSC-8972
NSa 5650 (1 año)	01-SSC-3692
NSa 4650 (1 año)	01-SSC-3583
NSa 3650 (1 año)	01-SSC-3469
NSa 2650 (1 año)	01-SSC-1970
Serie TZ600 (1 año)	01-SSC-0234
Serie TZ500 (1 año)	01-SSC-0464
Serie TZ400 (1 año)	01-SSC-0540
Serie TZ300 (1 año)	01-SSC-0608
Serie SOHO (1 año)	01-SSC-0676
NSv 1600 (1 año)	01-SSC-5801
NSv 800 (1 año)	01-SSC-5774
NSv 400 (1 año)	01-SSC-5690
NSv 300 (1 año)	01-SSC-5649
NSv 200 (1 año)	01-SSC-5335
NSv 100 (1 año)	01-SSC-5238
NSv 50 (1 año)	01-SSC-5203
NSv 25 (1 año)	01-SSC-5177
NSv 10 (1 año)	01-SSC-5129

SonicWall Content Filtering Client	
5 usuarios (1 año)	01-SSC-1222
10 usuarios (1 año)	01-SSC-1252
25 usuarios (1 año)	01-SSC-1225
50 usuarios (1 año)	01-SSC-1228
100 usuarios (1 año)	01-SSC-1231
250 usuarios (1 año)	01-SSC-1255
500 usuarios (1 año)	01-SSC-1237
750 usuarios (1 año)	01-SSC-1240
1.000 usuarios (1 año)	01-SSC-1243
2.000 usuarios (1 año)	01-SSC-1246
5.000 usuarios (1 año)	01-SSC-1249

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 laboral). 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 elevado consumo de ancho de banda.

Hay disponibles números de producto para Content Filtering Service y Content Filtering Client de varios años.

Si desea obtener más información sobre las soluciones SonicWall Content Filtering y sobre nuestra línea completa de productos de seguridad, visite nuestra página Web en www.sonicwall.com.

La 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 firewall de 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.

La **suite de Análisis del tráfico de aplicaciones** incluye las herramientas SonicWall Capture Security Center, SonicWall Global Management System (GMS®) y SonicWall Analyzer. Todas ellas proporcionan análisis históricos y en tiempo real de los datos transmitidos a través del firewall, incluidas las páginas Web bloqueadas y las visitadas por el usuario.

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 cuestionable e improductivo, los administradores también pueden crear o personalizar listas de filtrado.

La **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 firewall 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 las páginas Web que contienen información o imágenes cuestionables o improductivas, como violencia, odio, banca online, compras, etc.

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

Content Filtering Client para dispositivos itinerantes. Amplía el refuerzo de las políticas internas sobre el uso de la Web para bloquear el contenido de Internet cuestionable e improductivo desde dispositivos situados fuera del perímetro del firewall. El cliente refuerza las políticas de seguridad y productividad siempre que el dispositivo se conecta a Internet, independientemente del lugar donde se establezca la conexión.

Arquitectura de las soluciones de filtrado de contenido de SonicWall

Implementado y gestionado a través de un firewall de SonicWall, SonicWall Content Filtering Service permite a los administradores de TI crear y reforzar políticas sobre el uso de Internet que bloquean el acceso de los dispositivos terminales gestionados por el departamento de TI y situados detrás del firewall a sitios Web inapropiados o

improductivos a través de una LAN, una LAN inalámbrica o una VPN.

Para los dispositivos itinerantes situados fuera del perímetro del firewall, SonicWall Content Filtering Client amplía las políticas de seguridad y productividad siempre que el dispositivo se conecta a Internet, independientemente de dónde se establezca la conexión. La implementación se simplifica utilizando las funciones de refuerzo de un firewall de SonicWall y el cliente se gestiona y monitoriza con un potente motor de políticas e informes.

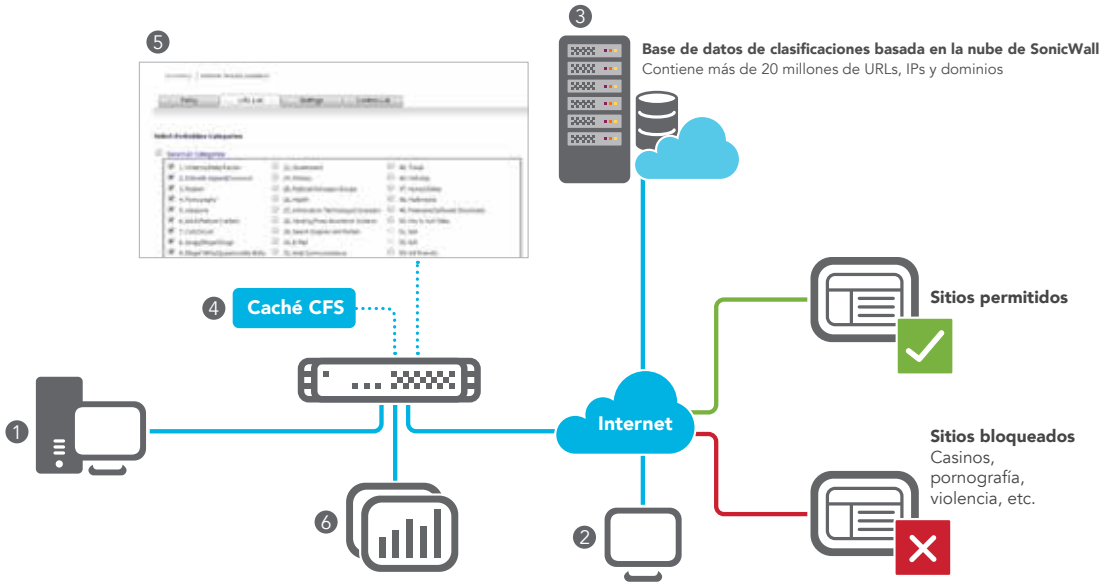
Con SonicWall Analyzer, SonicWall Capture Security Center o GMS, los administradores de TI pueden crear informes históricos y en tiempo real sobre el uso de la Web.

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

	Content Filtering Service (CFS) Premium	Content Filtering Client
Categorías	56+	56+
Políticas usuario / grupo	✓	✓
Clasificación dinámica	✓	✓
Informes	Analyzer*, Capture Security Center* y GMS*	✓
Caché de páginas Web	✓	✓
Refuerzo de búsqueda segura	✓	✓
Refuerzo de políticas CFS por rango IP	✓	✓
Disponible en: • Serie TZ • Serie NS*a* • Serie NS*sp*	 ✓ ✓ ✓	Dispositivos terminales con Windows, Chrome OS o Mac OS implementados a través de un firewall de SonicWall
YouTube para centros educativos	✓	✓
Filtrado de contenido HTTPS	✓	✓
Filtrado según horario	✓	✓
Base de datos de filtrado de contenido	Base actualizada dinámicamente con más de 20 millones de URLs, IPs y dominios	
Versiones de firmware / sistemas operativos soportados	SonicOS 5.x y posterior	Firewall – 5ª gen.: SonicOS 5.9.0.4 y posterior, 6ª gen.: SonicOS 6.1.1.6 y posterior; Portátil – Microsoft Windows 7/8/10/Windows Server 3/ Server 8/Server 12, Chrome OS, Mac OS 10.8 y posterior

**Analyzer, Capture Security Center y GMS son opcionales y se venden por separado.*



1. Usuario de SonicWall CFS detrás del firewall
2. Usuario de CF Client itinerante fuera del perímetro del firewall
3. Base de datos distribuida de clasificaciones de SonicWall CFS
4. Caché de clasificaciones locales de sitios aceptables
5. Políticas URL establecidas para bloquear los sitios Web cuestionables o contraproductivos
6. Informes en tiempo real e históricos mediante SonicWall Analyzer, Capture Security Center o GMS

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

Datasheet-ContentFilteringService-US-VG-MKTG2926

SONICWALL®