



Administrador y Monitoreo
de acceso a Internet.



Como controlar el acceso y
aplicaciones que los usuarios
utilizan en una organización

¿Existe un excesivo consumo de Internet?

- ⦿ 1 de cada 3 empleados admite utilizar Internet para jugar durante el horario de trabajo.
- ⦿ Un 50% de las estaciones de trabajo tienen programas instalados no relacionados con las Tareas encomendadas.
- ⦿ El 70% del tráfico de Internet es debido a páginas pornográficas durante horario de trabajo.
- ⦿ El 45% de los empleados admite utilizar Internet más de una hora diaria por diversión.



El 60% de la empresas no cuentan con un sistema de monitoreo, administración de acceso a Internet, y en el 30% de los que si cuentan con algún sistema como estos, solo son para navegación, pero aun no conocen como deben controlar los diferentes aplicaciones, servicios y protocolos que se utilizan en las organizaciones, por lo que navegar a paginas inseguras, sexo, drogas, alcohol, tabaco, cines, web mail, paginas de hackeo, etc, cada día se vuelve mas difícil controlarlo, y si a esto le agregamos que en muchas ocasiones no se puede determinar quien esta corriendo aplicaciones como KAZAA, MSN, real tunnel que es utilizado para poder acceder a aplicaciones P2P vía http-, Edonkey, o cualquier otra aplicación que no este permitida por la organización.

El control del acceso a Internet hecho fácil

Las empresas deben ejercitar algún control sobre los hábitos de navegación Web de los usuarios de la red, ya que los productos tradicionales de control de acceso a Internet son caros y complicados.

Existen tres aspectos que toda empresa debe considerar respecto al uso que sus empleados hacen de Internet:

Productividad: Estudios indican que más del 40% de la navegación en horas laborales se emplea para uso personal (visitas a páginas Web deportivas, música, cine, etc.). Este comportamiento resulta en la pérdida de productividad laboral.

Costos de comunicación: Esto resulta obvio en todo tipo de conexiones, pero un uso excesivo de la Web también puede provocar la necesidad de contratar más ancho de banda en líneas dedicadas. Minimizar el uso personal de Internet evitará estos costos.

Responsabilidad de la empresa: En muchos casos la empresa ha sido responsable del mal uso que algunos de sus empleados han hecho de la conexión a Internet mediante la descarga de contenido pornográfico, violento o de otro carácter igualmente ofensivo.

¿Qué es un filtrado de contenido?

Filtrado de contenido es un software que su función es evitar que el usuario vea material encontrado en Internet. Este proceso tiene dos componentes.

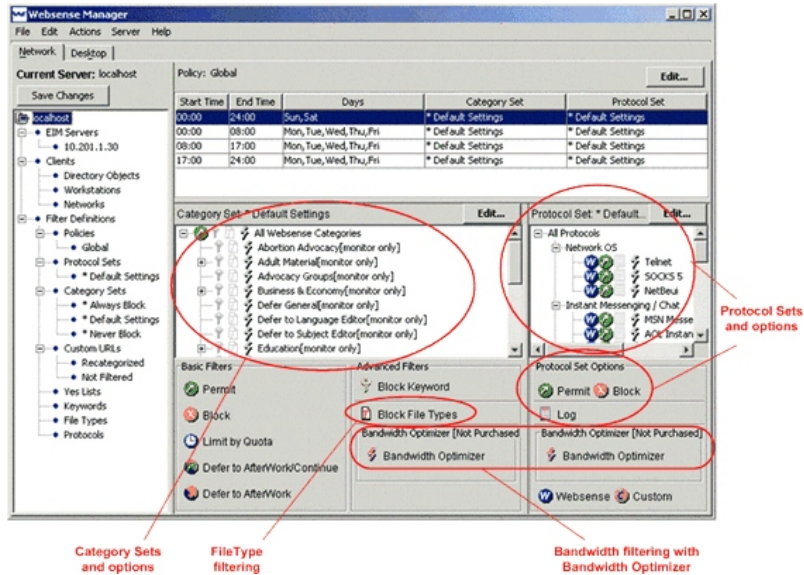
Clasificación: Se utilizan juicios de valor para categorizar sitios Web en base a su contenido. Estas clasificaciones pueden utilizar simples distinciones "permitido o no permitido".

Filtrado: Con cada solicitud de información, el software de filtrado examina el recurso que el usuario ha solicitado. Si el recurso está en la lista de los "no permitidos" o no tiene la clasificación adecuada, el software de filtrado dice al usuario que el acceso le ha sido denegado y el navegador no muestra el contenido de la página solicitada.

Solución para filtrado de contenido

Una solución ideal para ejecutar transparentemente un grado de control sobre los hábitos de navegación de los usuarios y asegurar el cumplimiento legal de forma que no alienará a los usuarios de la red es WebSense.

WebSense Enterprise es una solución amplia para el uso que los empleados hacen de los recursos informáticos, que combate la amenaza que surge del uso de Internet y de las aplicaciones de escritorio y de la red.

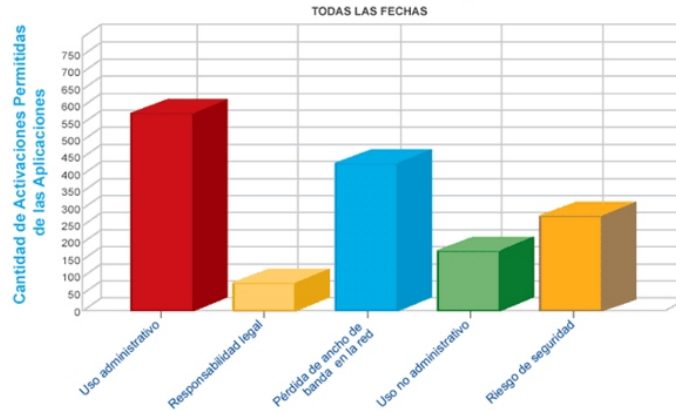


Websense Enterprise le permite:

- ⦿ Administrar el acceso a Internet de los empleados
- ⦿ Bloquear la capacidad para compartir archivos entre pares (P2P)
- ⦿ Administrar la mensajería instantánea (IM) y los archivos anexos de IM
- ⦿ Detener la piratería por parte de los empleados
- ⦿ Administrar el uso de las capacidades de descarga de medios y otras aplicaciones de uso intensivo del ancho de banda
- ⦿ Evitar spyware y códigos móviles maliciosos
- ⦿ Reducir la exposición a las amenazas del día cero



Resumen de Actividades de Riesgo Permitidas



Para más información acerca de este y más productos contáctenos o visite nuestra página de Internet.

RealNet, S.A. de C.V.
 "Administración y Seguridad de Redes"
 Guaymas 11bis Col. Roma C.P. 06700
 México, D.F.
 info@realnet.com.mx
 Tel: (01 55) 5219 8656
 Fax: (01 55) 5208 8201

www.realnet.com.mx