EnoLogic NetFilter Home
Manual del usuario

Contenidos

1. Introducción

Internet es un lugar maravilloso para que los niños busquen información y se eduquen. Sin embargo, Internet es el mayor canal mundial de distribución de pornografía, y los niños, al ser expuestos a ella, corren un gran peligro. Muchos chicos son enfrentados a la pornografía más cruda, aunque ellos no la busquen activamente. Una inocente búsqueda por palabra puede conducir a su hijo a sitios de sexo contra su propio deseo, porque las palabras de búsqueda populares, como por ejemplo "Britney Spears", son usadas para atraer a la gente a esos sitios.

EnoLogic NetFilter Home protege a su hijo contra los contenidos inapropiados de Internet dentro de las siguientes categorías:

- pornografía
- odio, racismo y discriminación
- violencia y humor vulgar
- actividades peligrosas o ilegales
- violaciones al derecho de autor (piratería)

El núcleo de NetFilter EnoLogic es un avanzado algoritmo que filtra contenidos, que analiza imágenes y texto en cada página visitada. Si una página es considerada inapropiada, aparecerá en su lugar otra con una advertencia sobre lo inadecuado de los contenidos. Usted tiene la posibilidad de especificar si sus hijos pueden continuar en tales páginas o si a ellos solo se les permite volver a la página anterior. Si se elige continuar no obstante la advertencia, esto será guardado en el Registro de actividades (LOG).

EnoLogic NetFilter también puede bloquear el chat y los programas en los que se comparten archivos con otras personas, prevenir la revelación de información personal, bloquear el streaming de audio y video, bloquear o registrar transferencias de MP3 y archivos grandes, por ejemplo, películas y software. Adicionalmente, es posible bloquear la bajada de archivos basada en su nombre/extensión.

2. Instalación

La instalación de Enologic NetFilter se compone de dos pasos. Primero, hay que instalar EnoLogic NetFilter en la computadora. Luego, los navegadores de la red en la computadora deben ser configurados para usar EnoLogic NetFilter como un servidor proxy.

2.1 Requisitos de Sistema

Requisitos mínimos:

- 200 MHz Pentium-compatible CPU
- 32 MB RAM
- 50 MB de espacio libre en el disco duro
- Microsoft Windows 98, ME, NT 4, 2000, o XP

Todos los navegadores que pueden usar un proxy HTTP son, en principio, compatibles. Los siguientes navegadores son configurados automáticamente:

- Microsoft Internet Explorer 4 y posteriores
- Netscape Navigator y Communicator 4
- Netscape 6 y posteriores y Mozilla
- Opera 5 y posteriores

Otros navegadores pueden ser configurados manualmente para usar EnoLogic NetFilter

2.2 Instalación de EnoLogic NetFilter

Si usted tiene un CD-ROM de instalación de EnoLogic NetFilter, la instalación comenzará automáticamente cuando el CD sea ubicado en la unidad de CD-ROM si Windows está configurado para esto (AUTORUN). Si la instalación no se inicia automáticamente, haga click en *Mi PC* en el escritorio de Windows (o el menú Inicio en Windows XP) y haga un doble click en el ícono de EnoLogic NetFilter. Si ha bajado el archivo de instalación del sitio web de EnoLogic o del sitio web de su proveedor de Internet (ISP), deberá hacer un doble click en el archivo bajado para poder iniciar la instalación.

El programa de instalación lo conducirá a través de los pasos necesarios para la instalación de EnoLogic NetFilter. Luego de que la instalación se haya completado, EnoLogic NetFilter estará instalado como un servicio y comenzará automáticamente la próxima vez que la máquina sea reiniciada. Se le ofrecerá la posibilidad de reiniciar la máquina inmediatamente o esperar y hacerlo manualmente.

2.3 Configuración de navegadores

Los navegadores compatibles, enumerados en la sección 2.1, se configuran automáticamente para el uso del filtro EnoLogic NetFilter. Si usted desea utilizar el filtro en otro navegador, puede hacerlo configurándolo para usar EnoLogic NetFilter como HTTP proxy. El modo de llevarlo a cabo se describe en el manual o función-ayuda para el navegador. La dirección del proxy NetFilter es *localhost*. El puerto es 3128.

3. Configuración y supervisión de EnoLogic NetFilter

Cuando la computadora ha sido reiniciada después de la instalación de EnoLogic NetFilter, un nuevo ícono aparecerá en el área de estado en la barra de tareas (Próximo al reloj). Este ícono muestra el estado del filtro y advierte sobre problemas potenciales.

El filtro está activo.

El filtro no está activo.

El filtro está activo, pero uno o más navegadores pueden no estar configurados para usarlo. Si un navegador no está configurado para usar el filtro, tendrá acceso sin filtro a Internet, aunque el filtro esté activado. En algunos casos, no tendrá acceso a Internet.

El filtro no está activo y los navegadores pueden no estar configurados para usarlo. En algunos casos esto puede significar que los navegadores no tienen acceso a Internet.

El estado es desconocido o el servicio de EnoLogic NetFilter no está funcionando. Esto puede ocurrir a menudo cuando la computadora está siendo iniciada. En circunstancias normales la cruz roja desaparecerá después de pocos segundos.

Al hacer click en el ícono de la barra de tareas con el botón derecho del ratón, aparecerá un menú con las siguientes entradas:

- *Ejecute NetUpdate*, (si el EnoLogic NetUpdate está instalado)
- *Configuraciones para EnoLogic NetFilter*
- *Desactivar filtro* o *Activar filtro*, (dependiendo del estado actual del filtro)
- *Estado*
- *Cambiar perfil,* si los perfiles están habilitados
- *Salir del perfil "xxxx",* si los perfiles están habilitados
- *Ayuda*

Las opciones *Cambiar perfil* y *Salir del perfil...* serán visibles solamente cuando los perfiles estén habilitados. Los perfiles le permiten a usted acceder a diferentes conjuntos de configuraciones para diferentes usuarios, y son descriptos en detalle en la sección 3.7.

Ayuda es un submenú desde donde usted puede acceder a la documentación e información de soporte, por favor seleccione la opción *Soporte Técnico* para saber a quien debe contactar en caso ser necesario.

Si se elige *Estado*, aparecerá una ventana con la información del estado. *Desactivar filtro* o *Activar filtro* pueden ser usados para desactivar y activar velozmente el filtro y requieren contraseña, como se muestra en la Figura 1. Si se selecciona *Configuraciones para EnoLogic NetFilter*, el programa EnoLogic NetFilter Admin se iniciará. Este programa también necesita contraseña. Si el nombre de usuario y la contraseña no han sido modificados con EnoLogic NetFilter Admin, ambos son "admin".

Si se elige *Ejecute NetUpdate*, se pone en funcionamiento el programa EnoLogic NetUpdate que se usa para realizar actualizaciones automáticas de los productos Enologic instalados vía Internet. Este programa está descrito a detalle en la sección 4.

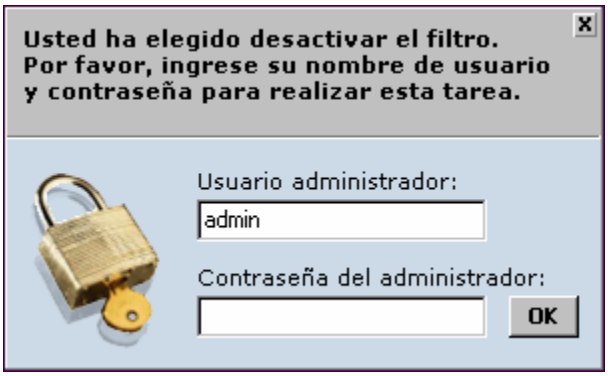

Figura 1: *Desactivando el filtro desde el ícono de la barra.*

La computadora en la que EnoLogic NetFilter está funcionando es denominada "servidor de filtrado". Cuando EnoLogic NetFilter Home es instalado en su computadora, su computadora es el servidor de filtrado. Con EnoLogic NetFilter Admin también es posible realizar administración remota de un servidor de filtrado si el programa ha sido configurado para mostrar las configuraciones avanzadas, como se describe en la sección 3.6.1.

La configuración por default para el programa es no mostrar las configuraciones avanzadas, ya que la mayoría de los usuarios privados no necesitan cambiarlas, pero en la descripción que sigue, la interfaz del usuario se describe tal cual se verían si esas configuraciones fuesen mostradas.

3.1 Ingreso

Cuando se inicie EnoLogic NetFilter Admin, aparecerá una ventana para ingresar, como se muestra en la Figura 2. En esta ventana, la dirección IP del servidor de filtrado debe ser especificada junto con el número de puerto de administración para EnoLogic NetFilter.

Nota: Si EnoLogic NetFilter Admin está configurado para no mostrar las configuraciones avanzadas, la dirección y el puerto del servidor de filtrado no pueden ser especificados. En este caso se supone que EnoLogic NetFilter está funcionando en la misma computadora que el programa de administración.

Si EnoLogic NetFilter Admin ha sido iniciado en el servidor de filtrado, la dirección IP 127.0.01 que se refiere al *localhost*, esto es, la computadora en la que EnoLogic NetFilter Admin ha sido iniciada, no necesita

ser modificada. De lo contrario, se ingresa la dirección IP del servidor de filtrado para administrar. El número de puerto 9600 puede no cambiarse, a menos que EnoLogic NetFilter haya sido manualmente configurado para usar otro puerto. Si ese es el caso, debería ingresarse, en cambio, ese número de puerto. En la sección 3.4.1, se describe cómo modificar el puerto de administración.

Figura 2: *Ingreso al servidor de filtrado.*

Por razones de seguridad es necesario ingresar al servidor de filtrado con un nombre de usuario y una contraseña antes de que sea posible administrarlo. Si es la primera vez que se inicia EnoLogic NetFilter Admin, tanto la contraseña como el nombre de usuario son "admin". Es muy importante que la contraseña sea cambiada inmediatamente después del primer ingreso para evitar accesos no autorizados al servidor de filtrado. Vea sección 3.6.1 para más información.

Cuando el nombre de usuario y la contraseña han sido ingresados, se presiona el botón *Ingresar*. Si el ingreso al servidor de filtrado es exitoso, aparecerá una pantalla como se muestra en la Figura 3. Si el ingreso no es exitoso, se mostrará, en cambio, un mensaje de error.

3.2 Navegación en EnoLogic NetFilter Admin

Después de un ingreso exitoso, aparecerá una página de inicio como muestra la Figura 3. En ella se ofrece una información general acerca de la versión y las estadísticas. Es posible navegar en EnoLogic NetFilter Admin seleccionando entre las secciones ubicadas en la parte superior derecha de la ventana. La sección que se activa después de ingresar es *Filtro*. Algunas de las secciones están divididas en subsecciones. Estas pueden elegirse haciendo click en las lengüetas que se ven en la parte inferior de la ventana. Para la sección *Filtro*, la primera lengüeta es *Estado*.

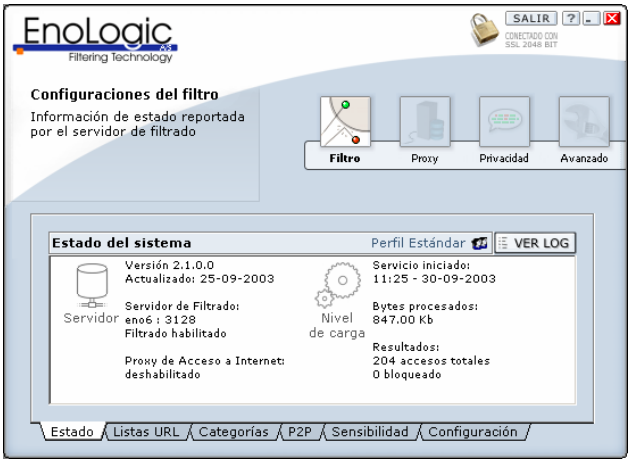

Figura 3: *Página Estado que aparece después de ingresar.*

3.3 Sección Filtro

La sección *Filtro* contiene información y opciones de configuración estándar para EnoLogic NetFilter. Las diferentes lengüetas para *Filtro* se describen en las siguientes secciones.

3.3.1 Estado

La lengüeta Estado permite ver información relacionada con EnoLogic NetFilter. Como puede observarse en la Figura 3, es posible leer el número de versión de EnoLogic NetFilter, en qué máquina y puerto el filtro está funcionando, si el filtro está activado y si el filtro está utilizando un Internet proxy. También pueden verse estadísticas acerca del filtro, tales como cuándo el filtro fue iniciado, cuánta información ha sido enviada a través del filtro medida en bytes, y cuántas páginas han sido visitadas a través del filtro y cuántas han sido bloqueadas.

Además es posible obtener estadísticas más detalladas al presionar el botón VER LOG. De este modo se abrirá un navegador con una página de estadísticas exhaustivas exhibiendo tanto el tráfico

autorizado y bloqueado a través del filtro como los intentos bloqueados para revelar información personal, etc.

3.3.2 Listas URL

3.3.2.1 Lista de permitidos

La lengüeta *Lista de permitidos*, que puede verse en la Figura 4, permite agregar URLs que nunca deberían ser bloqueados por EnoLogic NetFilter, sin importar su contenido. Para agregar un URL se entra en el campo URL y se presiona el botón *"Agegrar URL"*. Para eliminar un URL, se selecciona con el ratón y se presiona el botón *"Borrar URL"*.

Un URL en la lista de permitidos cubre todos los sub-URLs. Por ejemplo, el acceso a http://www.enologic.com/test/ será siempre autorizado con las configuraciones mostradas en la Figura 4. Inversamente, http://www.test.com podría ser bloqueado incluso si http://www.test.com/algo/ hubiese sido agregado a la lista.

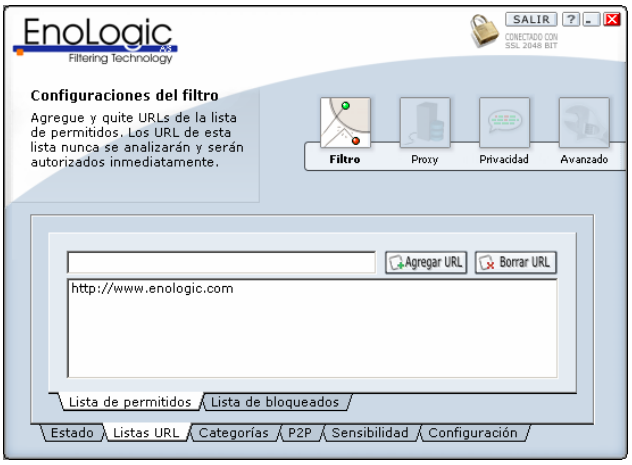

Figura 4: *Lista de permitidos. Las direcciones de esta lista nunca serán bloqueadas.*

3.3.2.2 Lista de bloqueados

La lengüeta *Lista de bloqueados*, que aparece en la Figura 5, permite agregar URLs que, cualquiera sea su contenido, deben ser bloqueados. Esto ofrece la posibilidad de agregar páginas que no están incluidas en las categorías, por ejemplo, apuestas u otro material no deseado. Para agregar un URL, se entra en el campo URL y se presiona el botón "Agregar *URL"*. Para eliminar un URL, selecciónelo con el ratón y presione *"Borrar URL"*.

Un URL que es especificado en la lista de bloqueados cubre todos los sub-URLs.

Por ejemplo, http://www.apuestas.com/test/ siempre será bloqueado con las configuraciones mostradas en la Figura 5. Inversamente, http://www.test.com puede ser autorizado incluso si http://www.test.com/basura/ ha sido agregado a la lista.

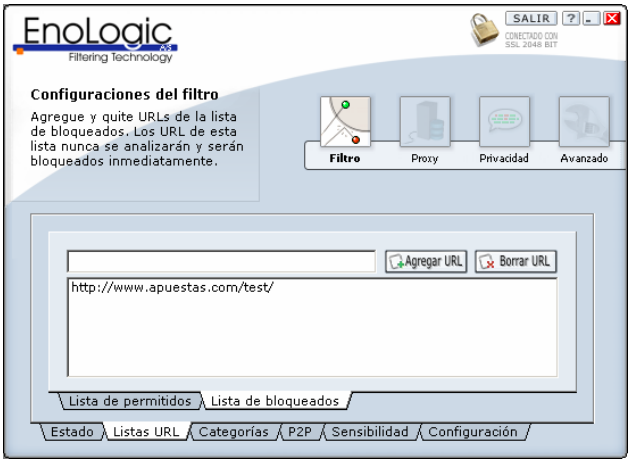

Figura 5: *Lista de bloqueados. Las direcciones en esta lista siempre serán bloqueadas.*

3.3.3 Categorías

En *Categorías* es posible elegir qué categorías debe bloquear el filtro. Esto se realiza seleccionando las categorías deseadas en la lista que muestra la Figura 6. Cuando se señala una categoría, sobre la derecha aparece su descripción.

Las siguientes categorías están configuradas:

- *Pornografía.* Páginas con contenido pornográfico. Las páginas sexualmente educativas solo se bloquean si el contenido es muy explícito o extremo.

- *Odio, racismo y discriminación*. Páginas que basadas en la raza, la religión o la orientación sexual apoyan la discriminación contra un grupo, expresan odio hacia un grupo,

alientan ataques a un grupo o presentan un grupo como superior a otros.

- *Violencia y humor vulgar*. Páginas con contenido violento o relacionadas con violencia, asesinato, suicidio, muerte, accidentes, enfermedades, modificaciones del cuerpo, canibalismo, necrofilia y funciones del cuerpo.

- *Violaciones al derecho de autor*. Páginas que violan el derecho de autor ofreciendo o proveyendo acceso a software, películas, música, etc.

- *Actividades peligrosas o ilegales*. Páginas que proporcionan instrucciones para la construcción/producción de armas, explosivos, fuegos artificiales y sustancias químicas tóxicas, cuyo uso puede ser peligroso o ilegal, y para el fraude con tarjetas de crédito, robo y otras actividades peligrosas y criminales.

Figura 6: *Categorías. El filtro bloquea las categorías que han sido seleccionadas en la lista.*

3.3.4 P2P (Peer-2-Peer)

La lengüeta Peer-2-peer permite bloquear los programas peer-2-peer que se usan para la distribución de software, música, películas, etc. entre computadoras de Internet. Las dos razones más importantes para bloquear esos programas son que los archivos intercambiados a menudo son grandes y, por ende, caros de transferir, y que los programas generalmente se usan para piratería.

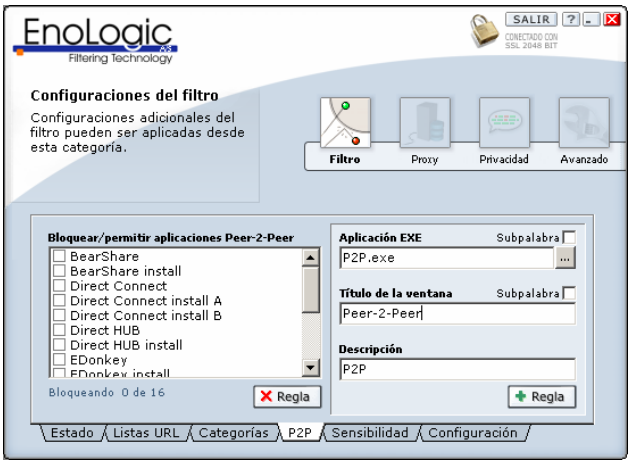

Figura 7: *Bloqueo de programas peer-2-peer.*

En la lista de la izquierda de la Figura 7, se puede escoger qué programas peer-2-peer deben ser bloqueados. La lista predeterminada contiene los programas peer-2-peer más comunes y usted mismo puede agregar otros.

Si usted hace click con el botón derecho del ratón, se despliega un menú con las siguientes funciones:

- *Habilitar todos los valores por default.* Activa el bloqueo de todos los programas de la lista predeterminada.
- *Deshabilitar todos los valores por default.* Desactiva el bloqueo de todos los programas de la lista predeterminada.
- *Bloquear todo.* Activa el bloqueo de todos los programas de la lista, incluyendo aquellos agregados por el usuario.
- *Permitir todo.* Desactiva el bloqueo de todos los programas de la lista, incluyendo aquellos agregados por el usuario.

Para agregar un programa a la lista, hay que ingresar el nombre del archivo ejecutable del programa y/o el título de su ventana. El nombre que usted quiere que aparezca en la lista se ingresa en el campo *Descripción*. El programa es agregado al presionar el botón "*+ Regla*".

Cuando presione el botón con los tres puntos que está a la derecha del campo de texto para el nombre

del archivo, se abrirá una ventana donde el archivo podrá ser seleccionado.

Si se ingresan tanto el nombre del archivo como el título de la ventana, los programas que contengan el nombre del archivo o el título de la ventana especificados serán bloqueados.

Es posible hacer coincidir por subpalabra (subcadena de caracteres) tanto el nombre del archivo como el título de la ventana. En el caso del nombre del archivo, el programa es bloqueado si el nombre de su archivo ejecutable contiene el texto especificado. Por ejemplo, si usted especifica "p2p" como nombre de archivo y señala *Coincidencia por subpalabra*, "p2p.exe", "mip2p.exe" y "p2p programa.exe" serán bloqueados. La coincidencia por subpalabra trabaja de la misma forma para el título de ventana. Hay que utilizar la coincidencia por subpalabra con MUCHO CUIDADO ya que, de otro modo, usted corre el riesgo de bloquear un programa por error.

El bloqueo funciona cerrando los programas. Pasarán algunos segundos antes de que esto suceda. Si el título de la ventana es utilizado para la coincidencia, el programa solo se cerrará si la ventana está activa.

Un programa agregado por el usuario puede ser quitado de la lista seleccionándolo y presionando *"X Regla".* Los programas de la lista predeterminada no pueden ser eliminados.

3.3.4 Sensibilidad

Como se ve en la Figura 8, la lengüeta *Sensibilidad* permite ajustar la sensibilidad de EnoLogic NetFilter en relación con el material inapropiado. Usted puede elegir entre tres configuraciones para la sensibilidad: *Baja*, *Normal* y *Alta*.

Si selecciona *Baja* sensibilidad, el filtro realizará un análisis menos agresivo, lo que implica que mayor cantidad de páginas serán autorizadas al ser consideradas adecuadas por el filtro. Esta configuración puede ser ideal si desea un filtro menos restrictivo. Cuando la sensibilidad es configurada *Baja*, el riesgo de que material inapropiado pase a través del filtro es mayor, pero el riesgo de que material que no es inadecuado sea bloqueado es menor.

Normal es la configuración estándar para el filtro y se recomienda para un uso normal.

Puede elegir Sensibilidad *alta* si desea un análisis más agresivo. Esto significa que el filtro será más sensible al material inapropiado. Esta configuración provocará que más páginas sean consideradas inadecuadas. El riesgo de que el filtro clasifique como inapropiadas páginas apropiadas es mayor, pero el riesgo de que material inadecuado pase a través del filtro es menor.

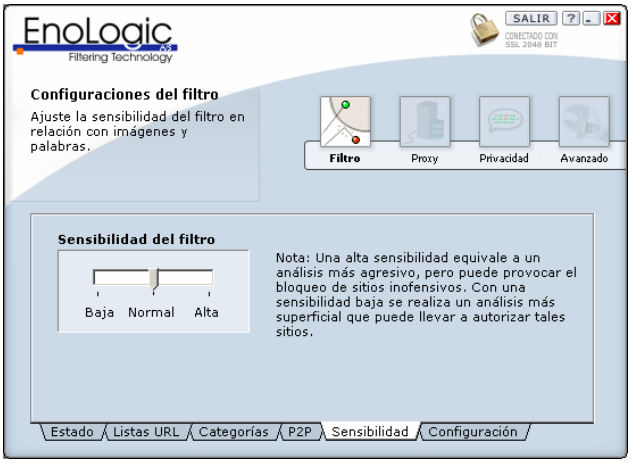

Figura 8: *Ajuste de la sensibilidad del filtro.*

3.3.5 Configuración

La lengüeta *Configuración* permite activar y desactivar varias propiedades del filtro. La página está dividida en una serie de lengüetas para las diferentes propiedades.

Bajo la lengüeta *General*, que aparece en la Figura 9, las siguientes opciones están disponibles:

- *Deshabilitar el filtro completamente.* Permite apagar y encender el filtro. Puede ser útil si usted desea autorizar todo el tráfico en su red por un breve período de tiempo.

- *Modo optimizado para módems.* Cuando se selecciona esta opción, el filtro se optimiza para conexiones lentas de Internet como las del módem de 56 Kbps. Si usted usa módem u otra conexión lenta, se le recomienda activarlo.

Bajo la lengüeta *MP3*, que aparece en la Figura 10, pueden ser configurados la detección y el bloqueo de los archivos de MP3:

- *Habilitar la detección de MP3.* Si se habilita esta propiedad, todo el tráfico de MP3 quedará registrado. La detección de MP3 requiere un poco más de recursos cuando está habilitada. La detección y el bloqueo de MP3 se basan en análisis de contenido. Es decir, el filtro también detecta archivos MP3 aun si están "disfrazados" como otros archivos. Por ejemplo, el archivo MichaelJackson.gif será detectado/bloqueado si es un archivo MP3 con el nombre cambiado.

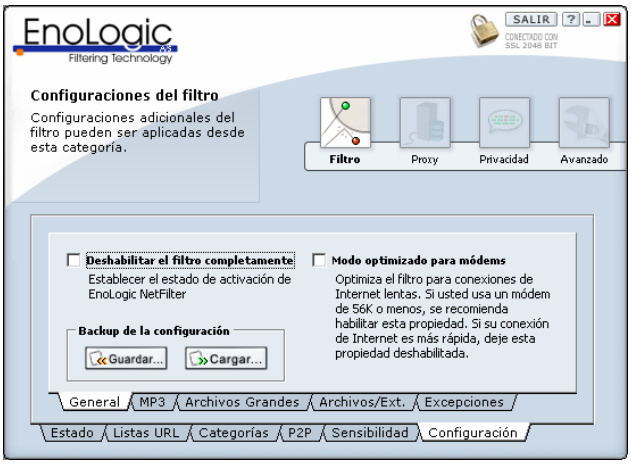

Figura 9: *Configuraciones generales para el filtro.*

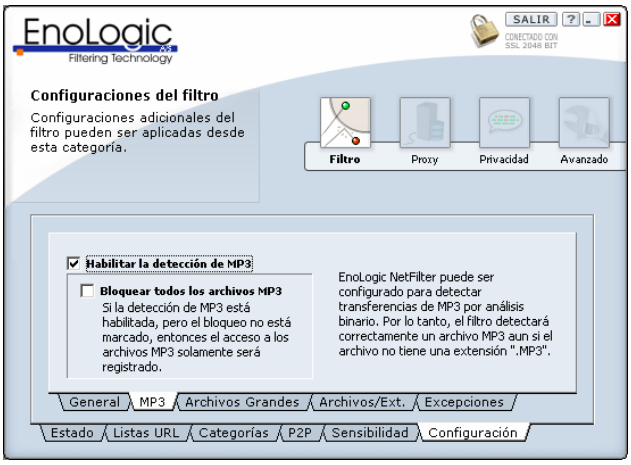

Figura 10: *Detección y bloqueo de MP3.*

- *Bloquear todos los datos de MP3.* Bloquea el tráfico de MP3. Del mismo modo que la detección de MP3, esta propiedad también provocará una demanda de recursos apenas mayor.

Bajo la lengüeta *Archivos Grandes*, que aparece en la Figura 11, puede configurarse la detección y el bloqueo de archivos grandes.

- *Habilitar la detección de archivos grandes.* Es posible detectar la transferencia de archivos grandes a través del filtro, de esta forma, si esto sucede, tal evento quedará registrado. Dependiendo de las circunstancias, puede variar la definición de lo que se considera "grande", por lo tanto es posible especificar qué tamaño debe tener un archivo para ser considerado "grande". De acuerdo con la configuración estándar, un archivo es grande si su tamaño es mayor a 5.242.880 bytes (5 MB).

- *Bloquear archivos más grandes que.* Bloqueo de la transferencia de archivos más grandes que el límite especificado y registro de los intentos de transferencia.

Bajo la lengüeta *Archivos/Ext.,* que aparece en Figura 12, es posible configurar el bloqueo usando reglas basadas en el nombre de archivo.

Si se elige *Bloquear los tipos comunes de streaming media*, son agregadas las reglas para los tipos más comunes de streaming multimedia (audio y video).

Es posible agregar reglas en tres categorías diferentes:

- *Solo extensión*. Ingrese una extensión, por ejemplo "exe" o "zip", en el campo de texto y presione *"+ Regla"* para agregar la extensión a la lista. Ahora los archivos con la extensión especificada serán bloqueados.

- *Nombre de archivo exacto.* Para bloquear archivos con un nombre específico, ingrese un nombre de archivo, por ejemplo "foo.exe", en el campo de texto. Luego presione "*+ Regla* para agregarlo a la lista.

- *Subpalabra: Nombre del archivo.* Use esta categoría para bloquear un archivo cuyo nombre contiene un texto particular. Ingrese el texto que el nombre del archivo debe contener en el campo de texto y presione "*+ Regla"* para agregar la regla.

Una regla puede ser suprimida al seleccionar la regla en la lista y al presionar "*X Regla*".

Bajo *Excepciones*, como muestra la Figura 13, es posible especificar los URLs y los dominios para los cuales el filtro no deberá usarse. El tráfico a las direcciones especificadas evitará el filtro y, por lo tanto, no quedará registrado. Los contenidos de la lista pueden ser modificados editando el texto en el campo contiguo al botón *Aplicar*. Las direcciones se separan usando el signo punto y coma (;). Haga click en *Aplicar* para activar los cambios realizados en la lista.

Para acceder a una cuenta de Hotmail a través del Outlook Express, es necesario agregar los servidores usados para Hotmail a las excepciones. Usted puede hacerlo seleccionando *Servidores de Hotmail (para Outlook Express)*.

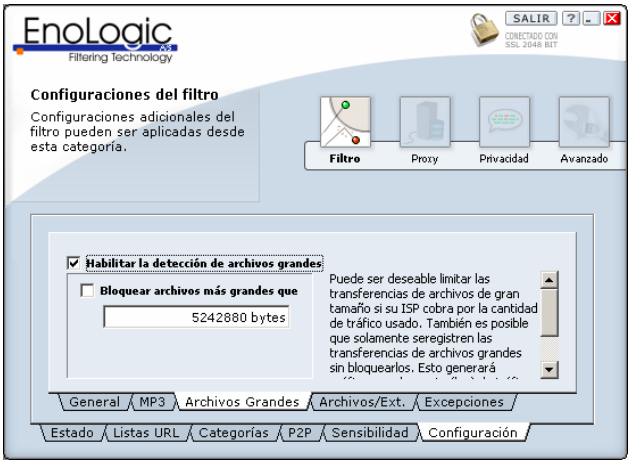

Figura 11: *Detección y bloqueo de archivos grandes.*

3.4 Sección Proxy

Esta sección permite configurar tanto en qué puertos opera EnoLogic NetFilter como si el tráfico de EnoLogic NetFilter debiera ser dirigido a través de un proxy externo. En la Figura 14 aparece la pantalla de la sección Proxy.

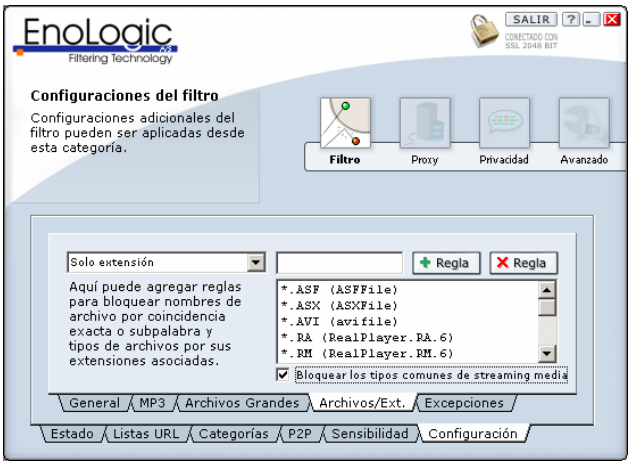

Figura 12: *Bloqueo por nombre.*

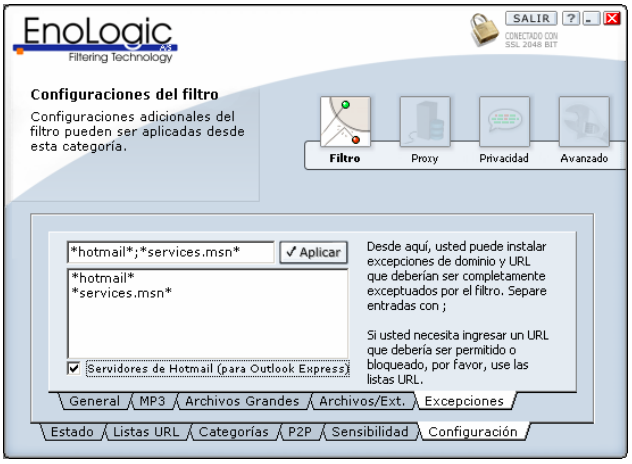

Figura 13: *Configuraciones de excepciones.*

3.4.1 NetFilter Proxy

En ella es posible configurar qué puerto debe ser usado por los navegadores para el acceso a Internet a través de EnoLogic NetFilter. El valor por default para este puerto es 3128, que es el puerto utilizado con frecuencia por los servidores proxy. Si se desea otro puerto, hay que ingresarlo en el campo *Puerto del Filtro*. Si EnoLogic NetFilter es usado sin un servidor proxy externo, generalmente no es necesario cambiar este puerto. Vea debajo para mayor información acerca del uso de un servidor de proxy externo.

Se puede cambiar el puerto de EnoLogic NetFilter que es usado para comunicación con EnoLogic NetFilter

Admin. Originalmente este está configurado en el 9600. Si se desea otro puerto, hay que ingresarlo en el campo de Puerto de Admin. Recuerde que para subsiguientes ingresos a EnoLogic NetFilter Admin debe ingresarse el puerto nuevo, como se describe en la sección 3.1.

Las modificaciones de las configuraciones del puerto no se activarán hasta que el botón *Aplicar* sea presionado. Por favor, note que EnoLogic NetFilter estará inactivo por un corto período de tiempo mientras se adapta a los cambios.

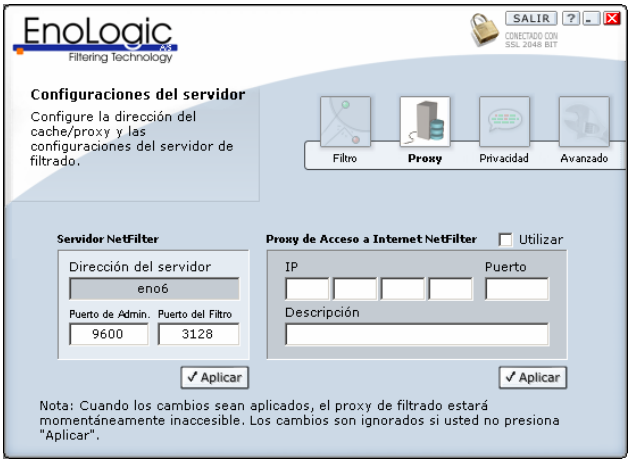

Figura 14: *Configuración de los números de puerto y proxy externo de EnoLogic NetFilter.*

3.4.2 Proxy de Acceso a Internet de NetFilter

Es posible conectar EnoLogic NetFilter con un servidor de proxy externo. Esto puede ser una ventaja si, por ejemplo, un servidor proxy ya está en uso en la red. El acceso a Internet se producirá a través del servidor proxy externo, y EnoLogic NetFilter filtrará el tráfico entre el proxy externo y los clientes.

Para dirigir el tráfico a través de un servidor proxy externo, la dirección IP del servidor proxy externo se ingresa en el campo *IP* bajo el *Proxy de Acceso a Internet del NetFilter*. Del mismo modo, el puerto del servidor proxy externo es especificado en el campo *Puerto*. Además, es posible agregar una descripción del servidor proxy externo. Esta información no es utilizada por EnoLogic NetFilter, sino que es para uso exclusivo del usuario (por ejemplo, el nombre de dominio del proxy).

Cualquier cambio se activa haciendo click en el botón *Aplicar*, siempre que el campo *on/off* esté seleccionado. Note que EnoLogic NetFilter estará inactivo por un corto período de tiempo mientras se adapta a los cambios.

3.5. Sección Privacidad

Bajo *Privacidad* es posible activar el filtrado o el bloqueo del chat.

3.5.1 Bloqueo del chat

La pantalla para el bloqueo del chat puede verse en la Figura 15. En la lista de la izquierda es posible elegir qué tipos de chat deben ser bloqueados. Si se selecciona *Browser/web chat*, los sitios web que ofrecen chat serán bloqueados. Las otras entradas en la lista son algunos de los programas de chat más comunes.

Si usted hace click con el botón derecho del ratón, se despliega un menú con las siguientes funciones:

- *Habilitar todos los valores por default.* Activa el bloqueo de todos los programas de la lista predeterminada.
- *Deshabilitar todos los valores por default.* Desactiva el bloqueo de todos los programas de la lista predeterminada.
- *Bloquear todo.* Activa el bloqueo de todos los programas de la lista, incluyendo aquellos agregados por el usuario.
- *Permitir todo.* Desactiva el bloqueo de todos los programas de la lista, incluyendo aquellos agregados por el usuario.

Para agregar un programa a la lista, hay que ingresar el nombre del archivo ejecutable del programa y/o el título de su ventana. El nombre que usted quiere que aparezca en la lista se ingresa en el campo Descripción. El programa es agregado al presionar el botón *"+ Regla".*

Cuando presione el botón con los tres puntos que está a la derecha del campo de texto para el nombre del archivo, se abrirá una ventana donde el archivo podrá ser seleccionado.

Si se ingresan tanto el nombre del archivo como el título de la ventana, los programas que contengan el

nombre del archivo o el título de la ventana especificados serán bloqueados.

Es posible hacer coincidir por subpalabra (subcadena de caracteres) tanto el nombre del archivo como el título de la ventana. En el caso del nombre del archivo, el programa es bloqueado si el nombre de su archivo ejecutable contiene el texto especificado. Por ejemplo, si usted especifica "p2p" como nombre de archivo y señala *Coincidencia por subpalabra*, "p2p.exe", "mip2p.exe" y "p2p programa.exe" serán bloqueados. La coincidencia por subpalabra trabaja de la misma forma para el título de ventana. Hay que utilizar la coincidencia por subpalabra con cuidado ya que, de otro modo, usted corre el riesgo de bloquear un programa por error.

El bloqueo funciona cerrando los programas. Pasarán algunos segundos antes de que esto suceda. Si el título de la ventana es utilizado para la coincidencia, el programa solo se cerrará si la ventana está activa.

Un programa agregado por el usuario puede ser quitado de la lista seleccionándolo y presionando *"X Regla".* Los programas de la lista predeterminada no pueden ser eliminados.

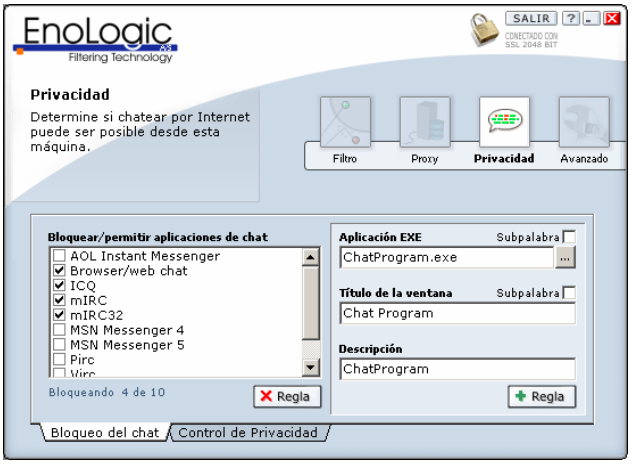

Figura 15: *Bloqueo de chat.*

3.5.2 Control de privacidad

Como muestra la Figura 16, en la página *Control de Privacidad* es posible especificar la información que debería permanecer confidencial. Al ingresar dicha información, usted previene que sea revelada a extraños vía Internet.

La información puede incluir apellido, dirección y número telefónico. Si usted tiene hijos que usan Internet para chatear, se le recomienda esta función para protegerlos de pedófilos y otros que quieran inducirlos a que les provean información con el propósito de contactarlos después.

Para activar esta función, hay que seleccionar el campo *Bloquear transmisión de información confidencial*. Luego la información puede ser agregada eligiendo el tipo de información bajo *Tipo* y entrando un texto en el campo bajo *Información confidencial*. Cuando se presiona *Agregar*, lo ingresado se sumará a la lista. Para eliminar un fragmento de información agregado previamente, se lo elige de la lista, y se presiona *Eliminar*.

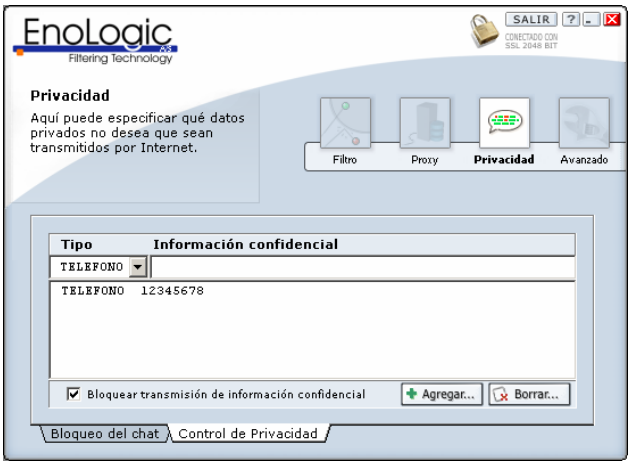

Figura 16: *Bloqueo de transmisión de información confidencial.*

La transmisión de información confidencial es bloqueada, en cada golpe de tecla, al analizar el texto que el usuario está ingresando. Cuando se ingresa la última letra de una de las palabras o números de la lista, se elimina la información ingresada y aparece una advertencia informándole al usuario que revelar información personal es peligroso y, por lo tanto, no está permitido.

Los fragmentos de información que están incluidos en la lista deberían ser elegidos cuidadosamente y tendrían que incluir solo información importante como para ser protegida. Cuando agregue información considere lo siguiente:

1. Deberían evitarse las palabras cortas y los números de cinco dígitos porque pueden

prevenir que otra información no personal pueda ser ingresada. Por ejemplo, si el nombre "Teo" está incluido en la lista, no será posible ingresar la palabra "teoría", ya que la primera parte de esta palabra es idéntica al nombre "Teo".

2. Evitar información que es demasiado específica. Por ejemplo, una dirección podría ser "Calle NetFilter 17", pero especificando esta dirección no podrá prevenir que el nombre de la calle "Calle Netfilter" sea revelado. A menudo será mejor tan solo agregar "Calle Netfilter" como dirección, ya que protege a ambos, tanto al nombre de la calle "Calle Netfilter" como a la dirección "Calle Netfilter 17", de ser revelados.

3. Información tal como dirección y número telefónico pueden abreviarse a los primeros caracteres para prevenir que la primera parte de la información sea revelada. Por ejemplo, "Call Netfilter" puede ser transmitido aunque "Calle Netfilter" haya sido agregado a la lista. Sin embargo, si "Netfilt" está en la lista, no es posible transmitir "Call Netfilter", sino solo "Netfil" que puede no ser suficiente para el receptor para descubrir cuál es el nombre de la calle. Note que este uso de abreviaturas puede causar problemas si la parte de la palabra que es especificada coincide con una parte de otras palabras, como se describe en el punto 1.

4. Es posible ingresar varios fragmentos de información del mismo tipo. Por ejemplo, dos fragmentos de información del tipo *Dirección* pueden ser agregados, donde uno contiene el nombre de la calle y el otro contiene el nombre de la ciudad.

Note que solo tiene la posibilidad de agregar un fragmento nuevo de información por vez. Si, por ejemplo, deben agregarse dos números telefónicos, primero se ingresa uno de ellos, presionando *Agregar*, y luego se le agrega el otro.

El filtro puede bloquear únicamente lo que está incluido en la lista. Siempre será posible camuflar un fragmento de información y, de ese modo, evitar que el filtro bloquee la transmisión. El filtro debería ser considerado fundamentalmente una ayuda para recordar acerca del peligro de revelar información personal. Asegúrese de hablar con sus hijos acerca de los peligros que acarrea revelar información a extraños en Internet, donde es fácil hacerse pasar por otra persona.

3.6. Sección Avanzado

Una pantalla de esta sección aparece en la Figura 17. En ella es posible configurar propiedades más avanzadas relacionadas tanto con EnoLogic NetFilter Admin como con EnoLogic NetFilter. Las cinco lengüetas dentro de la sección *Avanzado* permiten ajustar las propiedades que a menudo no necesitan cambios en circunstancias normales.

3.6.1 Configuración de NetFilter Admin

Esta lengüeta, como muestra la Figura 17, permite configurar las propiedades de EnoLogic NetFilter Admin. Si usted desea que aparezcan las opciones de configuración más avanzada, seleccione *Mostrar configuraciones avanzadas*. La configuración estándar es mostrar las opciones avanzadas. Si no se selecciona el casillero de *Mostrar...,* la interfaz del usuario será más simple pero también más limitada.

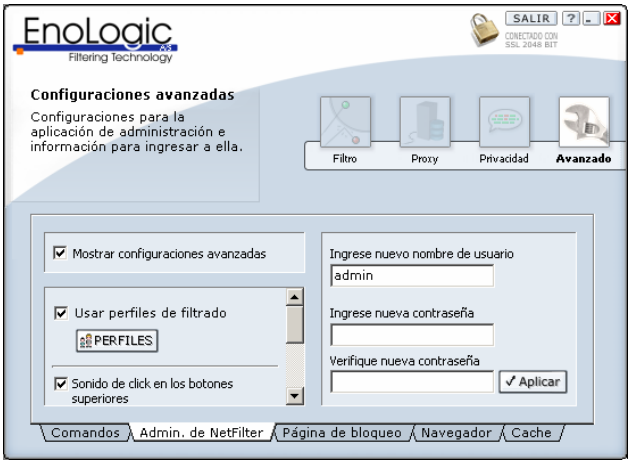

Figura 17: *Configuraciones avanzadas para EnoLogic NetFilter Admin.*

Seleccione *Probar la conexión SSL* en el caso de que EnoLogic NetFilter Admin deba verificar periódicamente si la conexión entre EnoLogic NetFilter Admin y EnoLogic NetFilter está abierta. Del mismo modo, es posible elegir la frecuencia con la que EnoLogic NetFilter Admin tiene que realizar la verificación. Con *Salir automáticamente al minimizar*

la aplicación usted puede elegir si el programa debe salir del servidor de filtrado cuando EnoLogic NetFilter Admin es minimizado. Esto sirve para evitar olvidarse de salir cuando deja de usar la computadora.

Si desea un nuevo nombre de usuario y una nueva contraseña, puede cambiarlos ingresándolos en los campos ubicados a la derecha de la ventana. Note que debe ingresar la nueva contraseña una segunda vez en *Verifique nueva contraseña* para protegerlo de errores en la contraseña ingresada. Cuando presione el botón *OK*, se le pedirá que ingrese su contraseña actual. Ingrésela y presione *OK* para completar el cambio de contraseña.

3.6.2 Comandos del cliente

La lengüeta *Comandos*, que muestra la Figura 18, permite cambiar las propiedades de la "página bloqueada" que aparece cuando se intenta acceder al material clasificado por el filtro como inapropiado. Si usted selecciona el campo Habilitar los comandos interactivos del cliente en la "página bloqueada", todo comando será incluido en la página bloqueada.

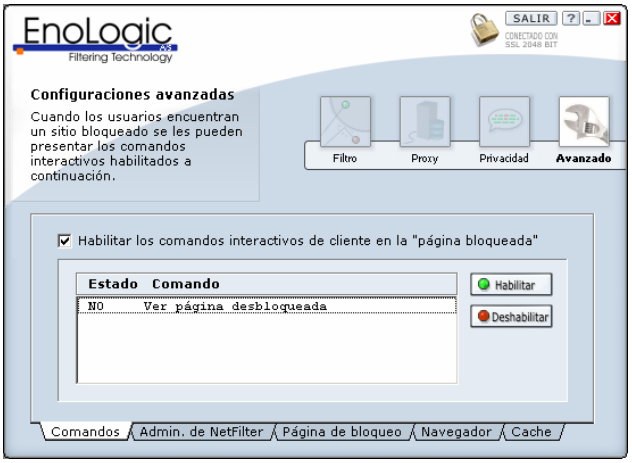

Figura 18: *Configuración de los Comandos del Cliente.*

El comando *Ver página desbloqueada* le agrega un botón extra a la página de bloqueo. Este botón permite continuar de la página de bloqueo al material que ha sido considerado inapropiado. En la página de bloqueo se mostrará que el evento quedará registrado. El comando se activa al señalarlo con el ratón y presionando el botón *Habilitar,* y se desactiva presionando el botón *Deshabilitar*.

Gracias a este comando dependerá del usuario la decisión de continuar o no hacia la página. Esto puede ser apropiado si, por ejemplo, un usuario tiene una necesidad relacionada con lo laboral para acceder al material que el filtro clasificará de inapropiado. El usuario evita tener que contactar al administrador de sistema para ver la página y puede continuar libremente en la página si la cree relevante para su trabajo.

3.6.3 Página de bloqueo

Como muestra la Figura 19, el idioma de la página de bloqueo puede cambiarse. Es posible elegir entre español, inglés y danés. La página de bloqueo es la página que se muestra en lugar de la página solicitada, cuando NetFilter ha encontrado material inapropiado.

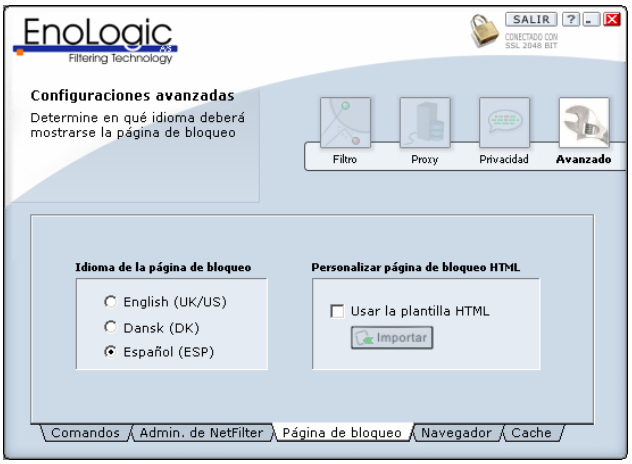

Figura 19: *Configuración de la página de bloqueo.*

Además, es posible reemplazar la página de bloqueo estándar por una página basada en una plantilla HTML. Para hacerlo hay que crear una página HTML que contenga una o más de las siguientes marcas en su código:

`[%enologic-netfilter-report%]` – Esta marca será reemplazada por un mensaje que declare que la página ha sido bloqueada, al igual que los links para los comandos elegidos por el cliente.

[%enologic-netfilter-message%] – Esta marca será reemplazada por un mensaje que diga que la página ha sido bloqueada.

[%enologic-imgbtn-view src="IMAGEURL"%] – Esta marca será reemplazada por un botón Ver. La imagen en la ubicación especificada (IMAGEURL) será usada como botón. El botón solo será mostrado si el comando de cliente *Ver página desbloqueada* está activo.

[%enologic-imgbtn-back src="IMAGEURL"%] – Esta marca será reemplazada por un botón "Atrás". La imagen en la ubicación especificada (IMAGEURL) será usada como botón.

{%enologic-insert-blocked-url%} – Esta marca será reemplazada por el URL que esta siendo bloqueado.

{%enologic-insert-timestamp%} – Esta marca será reemplazada por la hora en que la página fue bloqueada.

Para usar la plantilla, hay que importarla con la función *Importar* y seleccionar *Usar la plantilla HTML*.

NOTA:

`[%%` Estas marcas deben estar en su propia línea.

`{%%}` Estas marcas pueden encontrarse en cualquier lugar del texto.

3.6.4 Configuraciones del Navegador

Durante la instalación, las configuraciones en los navegadores compatibles quedarán trabadas de tal modo que el tráfico HTTP sea enviado a través del servidor de NetFilter. Esto puede apreciarse en la Figura 20. Si existe la necesidad de modificar las configuraciones que no son accesibles cuando los navegadores están asegurados, los navegadores pueden destrabarse desmarcando el campo *Trabar las configuraciones del navegador*. Se recomienda que los navegadores sean trabados tan pronto como las configuraciones hayan sido cambiadas. Note que los cambios en las configuraciones proxy de HTTP serán sobrescritos cuando los navegadores sean trabados de nuevo.

Cuando elija el campo *Optimizar las configuraciones de IE*, Internet Explorer se optimizará para ser usado con el servidor de NetFilter. Es recomendable que este campo se mantenga seleccionado. El cambio de esta configuración tendrá efecto a partir de la próxima vez que ingrese o reinicio.

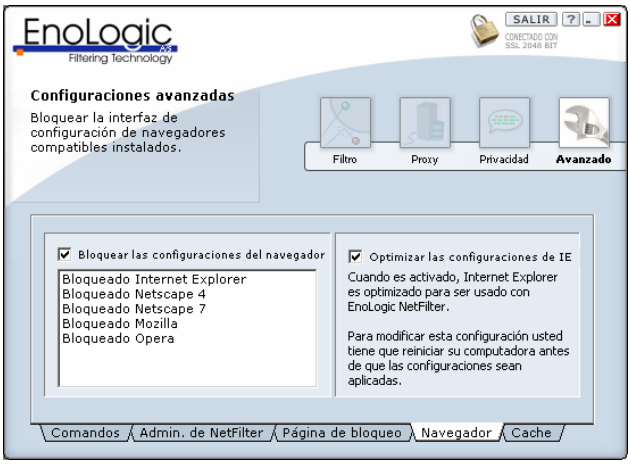

Figura 20: *Configuraciones del navegador.*

3.6.5 Cache

EnoLogic NetFilter archiva los sitios visitados en un cache para mejorar la velocidad cuando las páginas se visitan de nuevo. Usted puede eliminar los contenidos de este cache con el botón *Vaciar*. Los números que están sobre el botón *Vaciar* especifican la memoria y el espacio en el disco usado para el cache.

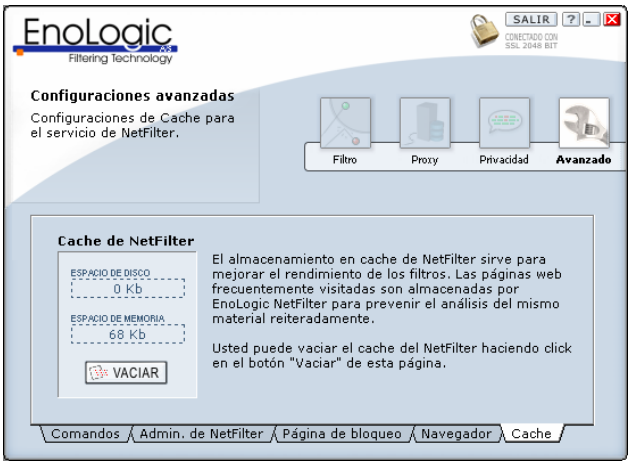

Figura 21: *Cache.*

3.7 Perfiles

3.7.1 Creando perfiles

Con los perfiles, usted puede usar diferentes conjuntos de configuraciones para diferentes usuarios en su computadora. Hasta que usted crea sus propios perfiles personalizados, el único perfil disponible es el perfil estándar, que será utilizado para todos los usuarios.

Los nombres de usuario de Windows son detectados y listados automáticamente dentro del perfil estándar, como puede ver en la Figura 22. Para crear un perfil personalizado para uno de sus usuarios, haga click derecho (de opciones) sobre el nombre de usuario y seleccione *Personalizar este perfil* en el menú. Se le solicitará una contraseña para este perfil. Entonces el usuario/perfil será movido a la sección *Perfiles Personalizados*.

Cuando un perfil personalizado ha sido creado para un usuario de Windows, este perfil será cargado automáticamente cuando el usuario inicie su sesión de Windows. Incluso es posible cambiar de perfil en cualquier momento haciendo uso de su contraseña. Esto se encuentra descrito en la Sección 3.7.2.

Cuando un perfil personalizado acaba de ser creado, será idéntico al perfil estándar. Para modificar sus configuraciones, haga doble click en el perfil o bien selecciónelo y haga click sobre el botón *APLICAR*. Esto lo llevará nuevamente a la página de estado principal que es mostrada luego de ingresar. Al lado del botón *VER LOG*, se mostrará el nombre del perfil siendo modificado. Todos los cambios hechos a las configuraciones serán aplicados solamente al perfil seleccionado.

Algunas configuraciones son compartidas para todos los perfiles y no pueden ser cambiadas para un perfil personalizado en particular, sino solamente para el perfil estándar. Las configuraciones que no puedan ser modificadas figurarán como deshabilitadas ("grisadas"). Para poder modificar estas configuraciones, deberá volver al perfil estándar.

Cualquier usuario puede cambiarse al perfil estándar. Por lo tanto, el perfil estándar debe ser configurado para ser tanto o más restrictivo que el perfil personalizado más restrictivo. Le recomendamos que configure el perfil estándar de la forma más apropiada para el integrante más joven de su familia o quien a quiera restringir más, y que luego agregue los perfiles personalizados que sean necesarios y que sean menos restrictivos en su acceso a Internet.

También es posible agregar nuevos perfiles personalizados que no se correspondan con ningún usuario de Windows. Los usuarios pueden cambiar a estos perfiles utilizando el icono en la barra de tareas de Windows. Esto resulta particularmente útil cuando diferentes personas utilizan de forma compartida una máquina con una sola cuenta de usuario de Windows, lo cual resulta probablemente la forma de uso más común actualmente.

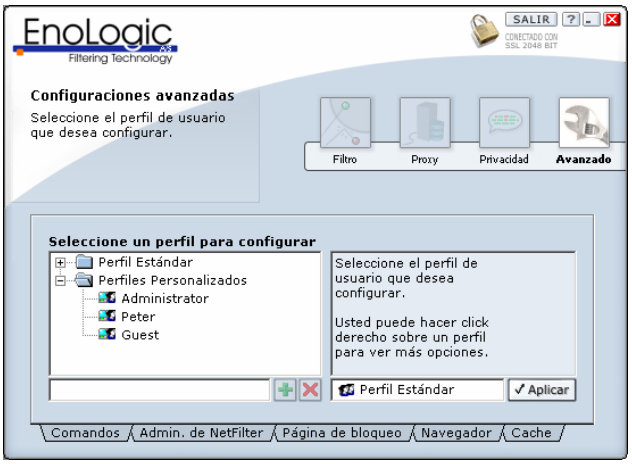

Figura 22: *Perfiles.*

Para agregar un nuevo perfil, ingrese el nombre del perfil en el campo debajo de la lista de perfiles y presione el botón "+". El nombre del perfil aparecerá debajo del *Perfil Estándar*. Para modificar las configuraciones de este nuevo perfil siga los pasos descriptos anteriormente.

Un perfil agregado manualmente anteriormente puede ser eliminado estando seleccionado y apretando el botón "X" o haciéndole click derecho de opciones y seleccionado la opción *Borrar perfil*.

Los perfiles que correspondan a usuarios de Windows NO pueden ser eliminados, pero pueden ser movidos nuevamente al perfil estándar. Esto puede hacerse mediante el click derecho de opciones sobre el perfil y seleccionando *Mover al perfil estándar*.

Para cambiar la contraseña de un perfil personalizado, basta con hacer click derecho sobre el perfil y seleccionar la opción *Configurar contraseña*. La nueva contraseña deberá ser ingresada dos veces en los campos de la derecha. Presione OK para finalizar.

3.7.2 Utilizando los perfiles

Cuando se habilitan los perfiles, dos opciones adicionales estarán disponibles en el menú emergente que aparece al hacer click derecho de opciones sobre el icono de EnoLogic NetFilter en la barra de tareas de Windows:

- *Cambiar perfil*
- *Salido del perfil "xxxx"*

Para utilizar otro perfil sin tener que cambiar su sesión de Windows seleccione *Cambiar perfil*. Esto abrirá la ventana mostrada en la Figura 23. Elija el perfil al que desea cambiar e ingrese su contraseña y luego presione el botón *OK* para realizar el cambio.

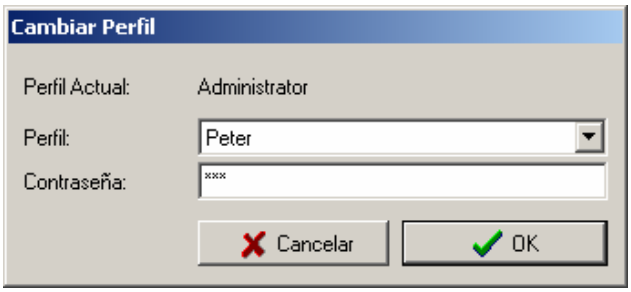

Figura 23: *Cambiar perfil.*

Cambiar al perfil estándar no requiere contraseña. Esto puede realizarse usando la ventana *Cambiar perfil* o bien eligiendo la opción S*alir del perfil "xxxx"* dentro del menú.

Los cambios de perfil solo son mantenidos hasta que el usuario termina su sesión de Windows o reinicia la PC. Cuando el usuario inicia nuevamente su sesión de Windows, se utilizará automáticamente el perfil correspondiente al nombre de usuario de Windows, por ej. el perfil que tiene el mismo nombre que el usuario de Windows, y si este no existe, entonces se utilizará el perfil estándar.

4. Actualizaciones automáticas con EnoLogic NetUpdate

EnoLogic NetUpdate se usa para actualizar vía Internet los productos EnoLogic instalados. El programa se inicia desde el ícono para EnoLogic NetFilter que está en la bandeja o desde el menú de Inicio. En la Figura 24 se muestra una pantalla desde la interfaz del usuario.
Si está usando Windows NT, 2000, o XP, usted debe haber ingresado como administrador cuando ejecute el programa, porque de otro modo no siempre será posible realizar las actualizaciones.

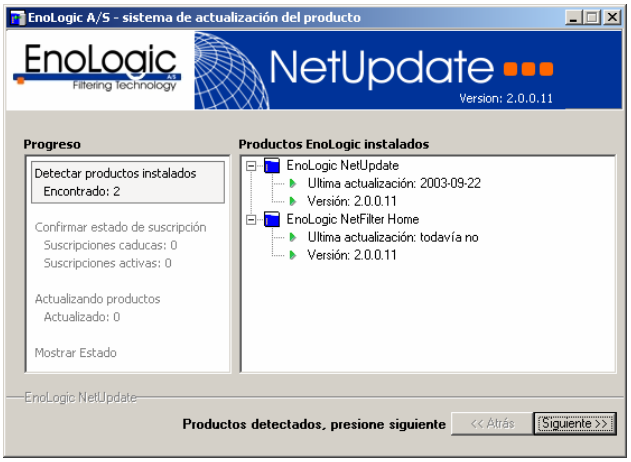

Figura 24: *EnoLogic NetUpdate.*

5. Desinstalación

EnoLogic NetFilter se desinstala usando la función "Agregar/Quitar Programas" del Panel de Control. Haga como sigue:

- Abra el Panel de Control
- Abra "Agregar/Quitar Programas"
- Elija "EnoLogic NetFilter Home"
- Presione "Eliminar" o "Remover"

EnoLogic NetFilter estará ahora desinstalado. Si EnoLogic NetUpdate está instalado, puede ser desinstalado usando un procedimiento similar.

6. Guía de problemas

En esta sección, se describen algunos de los problemas que pueden surgir usando EnoLogic NetFilter.

Sin conexión a Internet a través de EnoLogic NetFilter

Si de lo contrario hay conexión a Internet, la causa del problema puede ser que el puerto del filtro, que es usado para la comunicación entre EnoLogic NetFilter y los navegadores, esté siendo usado por otro programa en la computadora. En este caso, EnoLogic NetFilter informará acerca del problema cuando la computadora sea reiniciada. El problema puede solucionarse de dos formas:

- configurando (o desinstalando) el otro programa para que no use el mismo puerto que EnoLogic NetFilter, o
- configurando EnoLogic NetFilter y los navegadores para usar otro puerto de filtro, como se describe en la sección 3.4.1.

EnoLogic NetFilter Admin no puede establecer conexión con el servidor de EnoLogic NetFilter

Determine si otro servidor está usando el puerto, que se usa para la comunicación entre el servidor de EnoLogic NetFilter y EnoLogic NetFilter Admin. La configuración estándar es el puerto 9600. Si este es el caso, el número de puerto para uno de los servidores debe ser cambiado. Usted puede cambiar el número de puerto para EnoLogic NetFilter creando un archivo de texto con el nombre *ProxyAdminPort.cfg* en la carpeta Información, que se ubica en la carpeta EnoLogic NetFilter, y en este archivo especifique otro número de puerto, luego de lo cual su computadora deberá ser reiniciada. Alternativamente, usted puede detener el otro servidor, ingresar al servidor de EnoLogic NetFilter usando EnoLogic NetFilter Admin, y configurar *Puerto Admin* (en *Proxy*) a otro puerto. (Para hacerlo, debe seleccionar *Mostrar configuraciones avanzadas*, que se halla en la sección *Avanzado.*)

Las páginas inapropiadas no están siendo bloqueadas

Inicie EnoLogic NetFilter Admin y verifique si el filtrado está activado (esto puede ser visto en la lengüeta *Estado* que aparece cuando se inicia el programa). Si no, active el filtrado eligiendo la lengüeta *Configuraciones* en la sección *Filtro* y desmarcando la configuración *Deshabilitar el filtro completamente*.

En la lengüeta *Categorías* en *Filtro*, verifique si la categoría a la cual pertenecen las páginas particulares está activa. Si no lo está, actívela.

Verifique si las páginas particulares inapropiadas están incluidas en la *Lista de permitidos*. Si es necesario, cambie las configuraciones.

Determine si el navegador está configurado para usar EnoLogic NetFilter como un servidor proxy. Si no lo está, configure el navegador con la dirección y el puerto para el servidor de EnoLogic NetFilter.

Si tanto el filtro como el navegador están configurados correctamente, la causa de este problema puede ser que el filtro clasifique mal las páginas particulares. Usted puede agregar las páginas a la *Lista de bloqueados* en EnoLogic NetFilter Admin. Si el problema es sustancial, la sensibilidad del filtro puede ser aumentada.

Las páginas inocentes están siendo bloqueadas

Verifique si las páginas particulares están incluidas en la *Lista de Permitidos*. Si es necesario cambie las configuraciones.

En algunos casos, el algoritmo que filtra contenido puede fallar y clasificar páginas "inocentes" como inapropiadas. Las páginas mal clasificadas pueden agregarse a la *Lista de permitidos* en EnoLogic NetFilter Admin, de este modo los accesos a ellas serán siempre autorizados. Si el problema es sustancial, la sensibilidad del filtro puede ser disminuida.

Imágenes que faltan en la página

Este problema puede surgir por varios motivos. Si usted está usando Norton Internet Security y después de haber instalado Norton Internet Security ha actualizado a Internet Explorer 6, deberá instalar Norton Internet Security de nuevo.

Si está usando Norton Internet Security es importante que *EnoLogic NetFilter.exe* tenga acceso **completo** a Internet. Esta configuración puede cambiarse en el programa de administración del Norton Internet Security, que se muestra en la Figura 25. La configuración para EnoLogic NetFilter debería ser *Permitir Todo*.
Otro motivo puede ser que el navegador no esté usando HTTP 1.1 para la comunicación con el NetFilter. Para Internet Explorer, esta configuración puede ser cambiada en *Opciones de Internet*, bajo la lengüeta *Avanzados*. Debe seleccionar *Use HTTP 1.1 a través de conexiones proxy*.

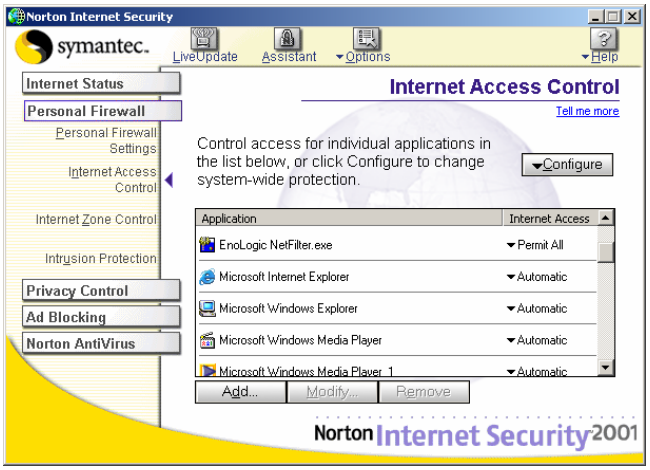

Figura 25: *Configuración del acceso a Internet en Norton Internet Security.*

El problema también puede surgir si partes de la configuración para el Internet Explorer han sido cambiadas, de modo tal que la comunicación entre el navegador y EnoLogic NetFilter no cumple con el estándar. Estas partes de la configuración no pueden ser cambiadas directamente por el usuario, pero tal vez hayan sido cambiadas por otro programa en la computadora. El problema puede ser actualizado con el archivo msie_fix.reg, que está ubicado en la carpeta Scripts en el directorio de instalación de EnoLogic NetFilter. Haga un click en el botón derecho del ratón sobre el archivo y elija Merge. Este script también le asegurará que Internet Explorer use HTTP 1.1 para la comunicación con NetFilter.

Finalmente, las imágenes pueden faltar porque fueron correctamente bloqueadas debido a su contenido por EnoLogic NetFilter, aunque la página no haya sido bloqueada.

Después de solicitar una página no ocurre nada por un largo tiempo, luego la página aparece de golpe

Cuando no se usa EnoLogic NetFilter, las páginas web se muestran progresivamente porque el texto y las imágenes se bajan de Internet. Esto significa que usted verá rápidamente parte de la página después de solicitarla (al presionar un link o ingresando un URL). EnoLogic NetFilter analiza la página entera antes de pasársela al navegador, ya que esto asegura la mayor precisión posible. Debido a eso usted experimentará una demora. Sin embargo, luego la página aparecerá velozmente porque fue incorporada al cache por EnoLogic NetFilter. La cantidad de tiempo desde que se solicita la página hasta que aparece la página entera en el navegador será apenas mayor cuando se usa EnoLogic NetFilter.

La lengüeta "Conexiones" en las configuraciones de Internet está trabada

Durante la instalación, esta lengüeta está trabada para prevenir que el usuario pueda desactivar el filtrado. Si usted necesita cambiar las configuraciones disponibles desde esta lengüeta, puede destrabarla usando el NetFilter Admin como se describe en la sección 3.6.4.

No es posible modificar las configuraciones proxy para el navegador

Los navegadores compatibles están configurados para usar EnoLogic NetFilter como HTTP proxy. Si usted debe usar un proxy para acceder a Internet, puede especificar el proxy en NetFilter Admin, como se describe en la sección 3.4.2. Si en Internet Explorer desea configurar un proxy para otro protocolo además de HTTP, primero deberá destrabar el navegador como se describe en la sección 3.6.4. Luego podrá configurar Internet Explorer.

7. Servicio al Cliente

Las actualizaciones para el producto y las respuestas a preguntas formuladas con frecuencia están disponibles en nuestro sitio web:

http://www.enologic.com/support

En caso que necesite soporte técnico, podrá obtener información sobre a quien contactar mediante la opción:

Ayuda > Soporte Técnico

del menú de la barra de tareas. Este menú puede ser accedido mediante un click derecho de opciones sobre el ícono de EnoLogic NetFilter de la barra de tareas. Ver sección 3.