

SOPHOS

simple + secure

Sophos Enterprise Manager

Guía de configuración de políticas

Versión: 4.7

Edición: julio de 2011



Contenido

- 1 Acerca de esta guía.....3
- 2 Recomendaciones generales para las políticas.....4
- 3 Configuración de políticas de actualización.....5
- 4 Configuración de políticas antivirus y HIPS.....6
- 5 Configuración de políticas del cortafuegos.....9
- 6 Configuración de políticas de control de dispositivos.....14
- 7 Configuración de políticas de protección contra manipulaciones.....16
- 8 Recomendaciones de escaneado.....18
- 9 Uso del escaneado en acceso.....19
- 10 Uso del escaneado programado.....20
- 11 Uso del escaneado en demanda21
- 12 Excluir elementos del escaneado.....22
- 13 Soporte técnico.....23
- 14 Aviso legal.....24

1 Acerca de esta guía

En esta guía se describe la configuración de las políticas de Sophos Enterprise Manager.

Aquí encontrará información que le ayudará a:

- Entender las recomendaciones sobre políticas.
- Crear e implementar las diferentes políticas.
- Usar las opciones de escaneado para encontrar elementos.
- Determinar los elementos a excluir del escaneado.

Esta guía le será útil si:

- Utiliza Enterprise Manager.
- Necesita consejos para crear e implementar políticas que se ajusten a sus necesidades.

Antes de leer esta guía debe consultar la *Guía de inicio de Sophos Enterprise Manager* .

Toda la documentación de Enterprise Manager está disponible en http://esp.sophos.com/support/docs/Enterprise_Manager-all.html.

2 Recomendaciones generales para las políticas

Al instalar Enterprise Manager se crean las políticas predeterminadas. Estas políticas se aplican a cada grupo nuevo. Las políticas predeterminadas están diseñadas para proporcionar un nivel de protección efectivo. Para utilizar funciones nuevas como el control de dispositivos o la protección contra manipulaciones, debe crear políticas nuevas o modificar las políticas existentes.

Nota: puede crear hasta cuatro políticas nuevas de cada tipo.

Al crear una política:

- Use los valores predeterminados cuando sea posible.
- Tenga en cuenta la función del ordenador antes de cambiar la política aplicada (ver si se trata de una estación de trabajo o de un servidor, por ejemplo).
- Use Enterprise Manager para centralizar la aplicación y cumplimiento de las políticas en la red.
- Modifique la configuración de forma local sólo cuando necesite cambios temporales en un ordenador o para opciones que no se puedan configurar de forma centralizada, como opciones avanzadas de escaneado.
- Cree un grupo a parte con políticas especiales para ordenadores que requieran un trato diferente.

3 Configuración de políticas de actualización

Las políticas de actualización especifican el modo en que las estaciones reciben los nuevos archivos de detección y las actualizaciones del software de Sophos. Mediante las suscripciones de software se especifica la versión del producto de Sophos que se utilizará en las estaciones de trabajo. La política de actualización predeterminada utiliza la suscripción "Recomendada" del software. Al crear una política de actualización:

- Por defecto, las estaciones se actualizan desde la ubicación primaria. Sin embargo, se recomienda también configurar una ubicación secundaria alternativa. Cuando una estación no puede conectar con la ubicación primaria, intentará la actualización desde la ubicación secundaria. Para más información, consulte Sophos Enterprise Manager Ayuda.
- En políticas para portátiles, debería activar la itinerancia. Esta opción permite a los portátiles detectar el servidor de actualización más cercano para optimizar la actualización de la protección. De las direcciones obtenidas, se utilizará la más cercana. Si no es posible realizar la actualización desde estas direcciones, se utilizará la ubicación primaria o secundaria especificadas en la política de actualización. Sólo podrá utilizar la itinerancia si el equipo itinerante se encuentra en una ubicación administrada por el mismo Enterprise Manager. Para más información, consulte Sophos Enterprise Manager Ayuda.
- Asegúrese de que el número de estaciones utilizando la misma política de actualización no se incrementa de forma desmesurada. No debería actualizar más de 1.000 estaciones desde la misma fuente de actualización. El número ideal de ordenadores para actualizarse desde la misma ubicación es 600-700.

Nota: el número de ordenadores que pueden actualizarse desde el mismo directorio depende del servidor en el que se encuentran y de la velocidad de la red. Tenga en cuenta que sólo puede crear hasta cuatro políticas de actualización en Enterprise Manager.

- Si le preocupa el rendimiento de ordenadores antiguos, puede realizar actualizaciones con menor frecuencia (dos o tres veces al día) o incluso fuera del horario de oficina (por las tardes o los fines de semana).



Advertencia: tenga en cuenta que una reducción excesiva de la frecuencia de las actualizaciones puede aumentar los riesgos para la seguridad.

4 Configuración de políticas antivirus y HIPS

4.1 Opciones recomendadas

La política antivirus y HIPS especifica las opciones para la detección y limpieza de virus, troyanos, gusanos, programas espía, aplicaciones publicitarias, aplicaciones no deseadas y comportamiento y archivos sospechosos. Al crear una política antivirus y HIPS:

- Utilice la política antivirus y HIPS predeterminada para la protección contra virus y otras aplicaciones maliciosas. Sin embargo, debe crear nuevas políticas, o modificar la predeterminada, para detectar aplicaciones no deseadas o elementos sospechosos.
- Utilice la protección activa de Sophos, que emplea un sistema de escaneado por Internet desde Sophos para verificar archivos sospechosos en tiempo real. La opción **Activar la protección activa** se encuentra activada por defecto. Para sacar el mayor partido de la protección activa, se recomienda activar también la opción **Enviar automáticamente muestras de archivos a Sophos**.
- Utilice inicialmente la opción **Sólo alertar** al activar la detección de comportamiento sospechoso. Con las alertas se podrá hacer una idea del impacto que esta opción puede tener en su red. Desactive esta opción cuando haya completado la implementación de la política.

4.2 Implementación de la política antivirus y HIPS

Se recomienda implementar la política antivirus y HIPS de la siguiente manera:

1. Crear políticas específicas para cada grupo. Tenga en cuenta que sólo puede crear hasta cuatro políticas antivirus y HIPS en Enterprise Manager.
2. Establecer exclusiones del escaneado en acceso para directorios u ordenadores con bases de datos de gran tamaño y utilice escaneados programados en su lugar. Por ejemplo, debería considerar la exclusión de ciertos directorios en servidores Exchange o en servidores cuyo rendimiento se pueda ver afectado. Para más información, consulte el artículo 12421 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/12421.html>).
3. Protección activa de Sophos. Esta función emplea un sistema de escaneado por Internet desde Sophos para verificar archivos sospechosos en tiempo real. Existen las siguientes opciones:
 - **Activar la protección activa:** Si en un escaneado se detecta algún archivo sospechoso pero no se consigue su identificación con los datos de detección en dicho ordenador, se enviará a Sophos los datos del archivo (como la suma de verificación y otros atributos) para su verificación. Para la comprobación se utilizan las bases de datos de SophosLabs. La respuesta se envía al ordenador, donde se actualiza de forma automática el estado del archivo afectado.

Esta opción está activada por defecto.

- **Enviar archivos de muestra de forma automática a Sophos:** Si algún archivo sospechoso no se puede identificar mediante los datos iniciales, será necesario enviar una muestra del mismo a Sophos. Si activa la opción **Enviar automáticamente muestras de archivos a Sophos**, se enviarán a Sophos los archivos sospechosos que no se puedan identificar. De esta forma Sophos podrá mejorar la detección de amenazas.

Importante: debe asegurarse de que el dominio Sophos es un sitio de confianza en su filtrado web para poder enviar los datos necesarios. Para más información, vea el artículo 62637 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/62637.html>). Si utiliza los productos de filtrado web de Sophos, como WS1000 Web Appliance, no necesita realizar ningún cambio. El dominio de Sophos ya se considera de confianza.

4. Detección de virus y programas espía.
 - a) Utilice el escaneado en acceso o escaneados programados para detectar virus y programas espía. El escaneado en acceso está activado por defecto. Para más información, consulte [Uso del escaneado en acceso](#) en la página 19 o [Uso del escaneado programado](#) en la página 20.
 - b) Configure las opciones de limpieza de virus y programas espía.
5. Detección de archivos sospechosos.

Los archivos sospechosos contienen ciertas características habituales en los programas maliciosos, pero no suficientes como para identificarlos como tales.

 - a) Tanto el escaneado en acceso como los escaneados programados permiten detectar archivos sospechosos.
 - b) Active la opción **Archivos sospechosos (HIPS)**.
 - c) Seleccione las opciones de limpieza.
 - d) Cuando sea necesario, autorice los archivos sospechosos cuyo uso desee permitir.
6. Detección de comportamiento sospechoso y desbordamiento del búfer.

Estas opciones de escaneado permiten controlar procesos en ejecución de forma continua para determinar si el comportamiento es sospechoso. De este modo, podrá evitar peligros para la seguridad.

 - a) Utilice inicialmente la opción **Sólo alertar** para determinar el efecto de estas opciones en su red. Esta opción está activada por defecto.
 - b) Cuando sea necesario, autorice los programas cuyo uso desee permitir.
 - c) Finalmente, desactive la opción **Sólo alertar**.

Así evitará bloquear programas que puedan necesitar los usuarios. Para más información, consulte el artículo 50160 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/50160.html>).
7. Detección de programas publicitarios y aplicaciones no deseadas.

Al utilizar esta opción por primera vez, puede que se detecte un gran número de aplicaciones de este tipo en las estaciones de su red. Utilice un escaneo programado para conocer y revisar los programas detectados.

- a) Realice un escaneo programado con la opción Detectar adware/PUA.
- b) Autorice o desinstale las aplicaciones detectadas.
- c) Active la opción **Adware/PUA** para detectar aplicaciones no deseadas.

Para más información, consulte el artículo 13815 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/13815.html>).

8. Detección de amenazas en páginas web.

- a) Compruebe que **Bloquear acceso a sitios web** se encuentra **Activado** para bloquear sitios web maliciosos. Esta opción se encuentra activa por defecto.
- b) En la opción **Escaneo de descargas** seleccione **Activado** o **Como en acceso** para escanear datos de descarga. Si selecciona la opción **Como en acceso**, opción predeterminada, se utilizará la configuración del escaneo en acceso.
- c) Autorice los sitios web a los que necesite permitir el acceso.

Para más información sobre las opciones de la política antivirus y HIPS, vea la Ayuda de Sophos Enterprise Manager Ayuda.

5 Configuración de políticas del cortafuegos

5.1 Acerca de la política cortafuegos

La política del cortafuegos establece la configuración del cortafuegos en las estaciones de la red. Sólo las aplicaciones especificadas, o clases de aplicaciones, pueden acceder a la red empresarial o Internet.

Nota: Sophos Client Firewall no es compatible sistemas operativos de servidor. Consulte la página de requisitos del sistema en la web de Sophos (<http://esp.sophos.com/products/all-sysreqs.html>).



Advertencia: debe configurar la política cortafuegos antes de utilizarla. Si aplica la política cortafuegos sin configurar (política predeterminada en Enterprise Manager) se producirán errores de comunicación en la red.

No debe utilizar la política cortafuegos predeterminada tal cual. Utilice esta política como base para crear la suya propia.

Por defecto, el cortafuegos se encuentra activado y bloquea el tráfico de red no esencial. No podrá realizar otras acciones como acceder a Internet, enviar mensajes de email o utilizar bases de datos en red. Deberá configurar el cortafuegos para permitir el tráfico, aplicaciones y procesos necesarios, y hacer pruebas antes de implementar la política en toda la red.

5.2 Planear la política cortafuegos

Planifique la política cortafuegos y lo que quiere que haga, antes de crear o modificar las reglas del cortafuegos.

Al planificar la implantación de un cortafuegos, tendrá que tener en cuenta:

- Los ordenadores que deben utilizar Sophos Client Firewall.
- Tanto equipos fijos como portátiles. La ubicación dual es aconsejable para los equipos portátiles.
- Método de detección de la ubicación a utilizar (DNS o gateway).
- Sistemas y protocolos de red.
- Conexiones remotas.

El número de políticas cortafuegos necesarias según las aplicaciones y derechos de acceso a la red para los diferentes grupos. Puede crear un máximo de cuatro políticas cortafuegos. Las políticas cubrirán diferentes aplicaciones e incluirán diferentes restricciones. Los grupos de Enterprise Manager para las políticas creadas.

- No se recomienda el uso de una sola política cortafuegos. Solo tendría que añadir reglas para uno o dos ordenadores (por ejemplo, el del administrador), pero dichas reglas estarían presentes en toda la red, lo que supone un riesgo para la seguridad.
- Por el contrario, un número excesivo de políticas requerirá un mayor esfuerzo de mantenimiento.

Sistemas y protocolos de red

Tenga en cuenta los servicios necesarios en su red. Por ejemplo:

- DHCP
- DNS
- RIP
- NTP
- GRE

La configuración predeterminada del cortafuegos cuenta con reglas para la mayoría de estos servicios. Sin embargo, tenga en cuenta cuáles debería permitir y cuáles no necesita.

Acceso remoto a ordenadores

Tendrá que configurar el cortafuegos para permitir el uso de programas de acceso y monitorización remotos.

Compruebe los programas que utiliza. Por ejemplo:

- RDP
- VPN cliente/servidor
- SSH/SCP
- Terminal services
- Citrix

Compruebe qué tipo de acceso necesita y cree las reglas adecuadas.

5.3 Opciones recomendadas

Al crear una política del cortafuegos:

- Al instalar Sophos Client Firewall, se desactiva el cortafuegos de Windows. Si estaba haciendo uso del cortafuegos de Windows, anote la configuración para transferirla a Sophos Client Firewall.
- Utilice inicialmente la opción **Permitir por defecto**. Con las alertas se podrá hacer una idea del impacto que esta política puede tener en su red.
- Utilice el visualizador de eventos del cortafuegos para ver el tráfico, aplicaciones y procesos necesarios en su red. El visualizador de eventos también le permite crear las reglas correspondientes. Para acceder al visualizador de eventos, haga clic en **Ver > Eventos del cortafuegos**.
- Revise las reglas mediante el visualizador de eventos. Una aplicación puede provocar diferentes evento del cortafuegos, aunque una regla de aplicación debe cubrir todas las acciones de dicha aplicación.
- Permita el uso de navegadores web, programas de email y uso compartido de archivos e impresoras.

- Se recomienda no modificar la configuración predeterminada de ICMP, reglas globales o reglas de aplicaciones a menos que tenga un conocimiento avanzado sobre redes.
- Se recomienda crear reglas de aplicaciones en vez de reglas globales cuando sea posible.
- No utilice el **modo interactivo** en políticas con ubicación dual.
- No utilice el **modo interactivo** en grandes redes ni en entornos de dominio. El **modo interactivo** es útil en redes pequeñas (por ejemplo, hasta 10 estaciones) en grupos de trabajo y equipos independientes.

5.4 Configuración del cortafuegos para ubicación dual

La configuración normal del cortafuegos es apropiada para estaciones de trabajo conectadas permanentemente a la red de la empresa. La configuración de ubicación dual está disponible para ordenadores que se conectan a más de una red, por ejemplo dentro y fuera de la oficina. La ubicación dual es aconsejable para los equipos portátiles.

Se recomienda configurar la ubicación primaria y la secundaria de la siguiente manera:

- La ubicación primaria debería ser la red principal de la empresa, mientras que la secundaria se utiliza para las redes externas.
- Configure la ubicación primaria con un acceso más abierto y la secundaria, con un acceso más restringido.
- Al configurar la detección de la ubicación primaria, se recomienda en general la detección DNS para grandes redes y la detección gateway para redes más pequeñas. La detección DNS requiere un servidor DNS, pero es más fácil de mantener que la detección gateway. Si necesita cambiar el hardware utilizado para la detección gateway, deberá reconfigurar la dirección MAC en la política del cortafuegos.
- Si utiliza detección DNS, se recomienda crear una entrada específica en el servidor DNS con dirección de retorno (como 127.x.x.x). De esta forma evitará que se pueda detectar cualquier otra red como la ubicación primaria.
- En la configuración avanzada del cortafuegos, seleccione la configuración que se aplica según la ubicación. Si desea que la configuración se aplique de forma automática, seleccione la opción **Ubicación detectada**. Si desea aplicar la configuración primaria o secundaria de forma manual, seleccione la opción correspondiente.



Advertencia: se recomienda cautela a la hora de utilizar reglas de subred local como parte de la configuración secundaria. Un portátil que se utiliza fuera de la oficina podría conectarse a una subred desconocida. Si esto ocurre, la configuración secundaria del cortafuegos con subred podría permitir tráfico desconocido.

5.5 Implementación de la política del cortafuegos

Utilice una política inicial que le permita monitorizar el tráfico de la red. Analice los resultados desde el visualizador de eventos del cortafuegos. Utilice esta información para establecer una política básica.

Implemente Sophos Client Firewall por fases, es decir, aplique Sophos Client Firewall a los grupos de uno en uno. Así, evitará saturar el tráfico de la red durante los pasos iniciales.



Advertencia: no realice la distribución en toda la red hasta que no haya comprobado el correcto funcionamiento de los ordenadores de prueba.

1. Implemente Sophos Client Firewall a un grupo de prueba representativo.
2. Inicialmente, utilice la opción **Permitir por defecto**.
 - a) Cree una política nueva. En Enterprise Manager, en el panel **Políticas**, haga clic con el botón derecho en **Cortafuegos** y seleccione **Crear política**. Escriba el nombre de la política y haga doble clic sobre la misma.

Si lo desea, puede modificar la política predeterminada. En el panel de **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en **Predeterminada**.

Se iniciará el **Asistente de políticas del cortafuegos**.
 - b) Haga clic en **Siguiente** para utilizar el asistente de configuración o haga clic en **Opciones avanzadas** para establecer las opciones de forma manual.
 - Con el asistente: Haga clic en **Siguiente**. Seleccione **Ubicación única** y haga clic en **Siguiente**. Seleccione **Monitorizar**, haga clic en **Siguiente** dos veces y haga clic en **Finalizar**.
 - Con las **Opciones avanzadas**: En el cuadro de diálogo **Política cortafuegos**, haga clic en **Configurar** junto a la **Ubicación primaria**. En la ficha **General**, active la opción **Permitir por defecto**. Haga clic en **Aceptar** dos veces.
 - c) Asigne la nueva política cortafuegos al grupo de prueba.
3. Utilice el visualizador de eventos del cortafuegos para ver el tráfico, aplicaciones y procesos necesarios en su red. El visualizador de eventos también le permite crear las reglas correspondientes. Para acceder al visualizador de eventos, haga clic en **Ver > Eventos del cortafuegos**.
4. Monitorice los eventos del cortafuegos y ajuste la política según sus necesidades.
 - a) Cree reglas desde el visualizador de eventos. Haga clic con el botón derecho en un evento para crear una regla. Para más información, consulte la Ayuda de Sophos Enterprise Manager.
 - b) Compruebe si existen puntos débiles en la política (por ejemplo, otorgar demasiado acceso a algunos usuarios).
 - c) Si es necesario, subdivida los grupos y cree políticas y reglas adicionales.
5. Revise las reglas mediante el visualizador de eventos. Una aplicación puede provocar diferentes evento del cortafuegos, aunque una regla de aplicación debe cubrir todas las acciones de dicha aplicación.
6. Divida el resto de la red en grupos de equipos equivalentes, por ejemplo, ventas, informáticos, etc. Tenga en cuenta que sólo puede crear hasta cuatro políticas cortafuegos en Enterprise Manager.
7. Cuando esté satisfecho con la monitorización, cree las políticas con las reglas disponibles y asígnelas a los grupos correspondientes. Distribuya Sophos Client Firewall a los grupos de uno en uno.

8. Una vez probadas las reglas, pase al modo **Bloquear por defecto** para comenzar a proteger los ordenadores.

Para más información, consulte la Ayuda de Sophos Enterprise Manager.

Nota: de forma alternativa, en redes más pequeñas, instale Sophos Client Firewall en un equipo de prueba y utilice el modo **Interactivo**. Abra las aplicaciones que necesitan acceso a la red. Utilice las reglas que vaya creando para realizar la configuración. Para más información, consulte la Ayuda de Sophos Endpoint Security and Control.

6 Configuración de políticas de control de dispositivos

6.1 Opciones recomendadas

Las políticas de control de dispositivos permiten bloquear unidades de almacenamiento y dispositivos de red no autorizados. Al crear una política de control de dispositivos:

- Active la opción **Detectar pero no bloquear**. Para ello, configure el estado de cada tipo de dispositivo que desea detectar como **Bloqueado**. El software no buscará dispositivos de tipos no especificados. Con las alertas se podrá hacer una idea del impacto que esta política puede tener en su red.
- Utilice el visualizador de eventos de control de dispositivos para obtener detalles de cada caso que se presente. Para acceder al visualizador de eventos, haga clic en **Ver > Eventos del control de dispositivos**.
- Utilice el gestor de informes para seguir la tendencia de uso de estos dispositivos por ordenador o usuario.
- Considere un mayor control en ordenadores de usuarios que traten con información delicada.
- Prepare la lista de excepciones antes de implantar el control de dispositivos. Por ejemplo, para permitir al equipo de diseño grabar discos ópticos con imágenes.
- La categoría "Almacenamiento extraíble seguro" puede utilizarse para permitir el uso de unidades externas de almacenamiento con encriptación por hardware. En la web de Sophos podrá encontrar la lista de fabricantes con unidades de este tipo. Para ver la lista de los dispositivos de almacenamiento seguro compatibles, consulte el artículo 63102 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/63102.html>).
- Al añadir excepciones de dispositivos, haga uso del campo **Comentario** para describir la razón para dicha excepción.
- Haga uso del mensaje personalizado de escritorio para informar al usuario sobre los detalles necesarios. Por ejemplo, podría incluir un enlace a la política interna de la empresa sobre el uso de dispositivos.
- Si desea permitir el uso de un dispositivo de red (por ejemplo, un adaptador inalámbrico) cuando el ordenador no se encuentre en la red de la empresa, seleccione la opción **Bloquear puente**.

Nota: el modo de bloqueo de puentes reduce considerablemente el riesgo de puentes entre redes corporativas y no corporativas. El modo Bloquear puente está disponible tanto para módems como dispositivos inalámbricos. Este modo funciona desactivando el adaptador de red inalámbrico o módem cuando una estación está conectada a una red física (normalmente, mediante una conexión Ethernet). Cuando el ordenador se desconecta de la red de la empresa, podrá volver a utilizar los dispositivos inalámbricos o módem.

- Tenga en cuenta las posibles consecuencias antes de implementar una política de control de dispositivos. Tenga en cuenta los diferentes escenarios, especialmente en relación con dispositivos de red.



Advertencia: las políticas se gestionan de forma centralizada desde Enterprise Manager y se implementan a través de la red; así, una vez bloqueado el dispositivo de red, no podrá desbloquearlo desde Enterprise Manager porque no existe conexión de red con las estaciones afectadas.

6.2 Implementación de la política de control de dispositivos

Por defecto, el control de dispositivos está desactivado y se permiten todos los dispositivos. Se recomienda introducir el control de dispositivos de la forma siguiente:

1. Considere los dispositivos que desea restringir.
2. Active el control de dispositivos y seleccione inicialmente la opción **Detectar pero no bloquear**. Para ello, configure el estado de cada tipo de dispositivo que desea detectar como **Bloqueado**. El software no buscará dispositivos de tipos no especificados.
En estos momentos, sólo existe una política de control de dispositivos en la red.
3. Utilice el visualizador de eventos del control de dispositivos para ver el efecto que tendría en su red el bloqueo de los dispositivos seleccionados. Para acceder al visualizador de eventos, haga clic en **Ver > Eventos del control de dispositivos**.
4. Para que cada grupo de equipos tenga acceso a diferentes dispositivos, cree políticas diferentes para cada uno. Por ejemplo, puede que desee bloquear el uso de dispositivos de almacenamiento externo en los departamentos de finanzas y recursos humanos, y permitirlo en los departamentos informáticos y de ventas. Tenga en cuenta que sólo puede crear hasta cuatro políticas de control de dispositivos en Enterprise Manager.
5. Cree excepciones para dispositivos o modelos específicos que no desee bloquear. Por ejemplo, puede crear una excepción para cierto dispositivo USB o para el modem Vodafone 3G.
6. Determine los dispositivos que desee bloquear y cambie su estado a **Bloqueado**. También puede establecer acceso de sólo lectura a ciertos dispositivos de almacenamiento.
7. Cuando desee imponer la política, desactive la opción **Detectar pero no bloquear**.

De esta forma, evitará que se produzcan grandes cantidades de alertas y bloqueos de dispositivos que los usuarios puedan necesitar. Para más información sobre la política de control de dispositivos, consulte la Ayuda de Sophos Enterprise Manager.

7 Configuración de políticas de protección contra manipulaciones

7.1 Opciones recomendadas

La protección contra manipulaciones permite evitar que usuarios no autorizados (administradores locales con conocimientos técnicos limitados) puedan modificar, desinstalar o desactivar el software de seguridad de Sophos. Los usuarios que no dispongan de la contraseña necesaria no podrán realizar dichos cambios.

Nota: esta protección puede no ser efectiva ante usuarios con amplios conocimientos técnicos. También podría ser ineficaz ante programas maliciosos diseñados específicamente para realizar ciertos cambios en el funcionamiento del sistema operativo. Este tipo de programas maliciosos se detecta mediante el escaneado de amenazas y comportamientos sospechosos. Para más información, consulte [Configuración de políticas antivirus y HIPS](#) en la página 6.

Tras activar la protección contra manipulaciones, y establecer la contraseña, los usuarios que no conozcan la contraseña no podrán modificar la configuración del escaneado en acceso o la detección de comportamiento sospechoso en Sophos Endpoint Security and Control, desactivar la protección contra manipulaciones ni desinstalar los componentes de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate o Sophos Remote Management System) o Sophos SafeGuard Disk Encryption desde el Panel de control.

Al crear la política de protección contra manipulaciones:

- Utilice el Visualizador de eventos de la protección contra manipulaciones para tener una idea de los intentos de modificaciones en la empresa. Podrá ver tanto los intentos fallidos de cambio como los realizados con éxito (usuarios autorizados con la contraseña correspondiente). Para acceder al visualizador de eventos, haga clic en **Ver > Eventos de la protección contra manipulaciones**.

7.2 Implementación de la política de protección contra manipulaciones

Por defecto, la protección contra manipulaciones está desactivada. Se recomienda introducir la política de protección contra manipulaciones de la forma siguiente:

1. Active la protección contra manipulaciones y asigne una contraseña segura.
Esta contraseña permitirá a los usuarios autorizados configurar, desactivar y desinstalar el software de seguridad de Sophos.
Nota: la protección contra manipulaciones no afecta a los usuarios que pertenecen a los grupos SophosUser y SophosPowerUser. Cuando active la protección contra manipulaciones, los usuarios de estos grupos podrán seguir realizando las tareas habituales sin necesidad de introducir la contraseña de la protección contra manipulaciones.
2. Si necesita esta protección en diferentes grupos o diferentes contraseñas, cree las políticas necesarias para los diferentes grupos. Tenga en cuenta que sólo puede crear hasta cuatro políticas de protección contra manipulaciones en Enterprise Manager.

Para más información sobre la política de protección contra manipulaciones, consulte la Ayuda de Sophos Enterprise Manager.

8 Recomendaciones de escaneado

A continuación se describen las opciones de la política Antivirus y HIPS. Al establecer las opciones de escaneado:

- Use los valores predeterminados cuando sea posible.
- Configure el escaneado de forma centralizada desde Enterprise Manager.
- Tenga en cuenta el uso del ordenador (estación o servidor).

Extensiones

Para configurar las extensiones para el escaneado en acceso, en el cuadro de diálogo **Política antivirus y HIPS**, haga clic en **Configurar** junto a **Activar el escaneado en acceso** y abra la ficha **Extensiones**.

Para escaneados programados, en el cuadro de diálogo **Política antivirus y HIPS**, en la sección **Escaneado programado**, haga clic en **Extensiones y exclusiones**.

- No se recomienda el uso de la opción **Escanear todos los archivos**. Utilice la opción **Escanear sólo los archivos ejecutables o vulnerables** para detectar amenazas encontradas por SophosLabs. Sólo debe utilizar la primera opción cuando así se lo indiquen desde soporte técnico.

Otras opciones de escaneado

Para configurar otras opciones del escaneado en acceso, en el cuadro de diálogo **Política antivirus y HIPS**, haga clic en **Configurar** junto a **Activar el escaneado en acceso** y abra la ficha **Extensiones**.

Para escaneados programados, en el cuadro de diálogo **Política antivirus y HIPS**, en la sección **Escaneado programado**, seleccione el escaneado programado y haga clic en **Editar**. En el cuadro de diálogo **Configuración del escaneado programado**, haga clic en **Configurar**.

- No utilizar la opción **Escanear dentro de archivos comprimidos**. Los archivos se escanearán cuando se descompriman. No se recomienda el uso de esta opción a menos que utilice archivos comprimidos a menudo.
- Se recomienda activar el escaneado de memoria del sistema. La memoria del sistema es la que utiliza el sistema operativo. La memoria del sistema se escanea en segundo plano de forma periódica mientras tenga activado el escaneado en acceso. También puede incluir el escaneado de memoria del sistema en los escaneados programados. La opción **Escanear memoria del sistema** se encuentra activada por defecto.

9 Uso del escaneado en acceso

Siga estas recomendaciones cuando utilice el escaneado en acceso:

- Use los valores predeterminados cuando sea posible.
- Use la opción **Leer**. Normalmente no son necesarias las opciones **Escribir** o **Editar**. Estas opciones se pueden utilizar cuando algún programa malicioso se esté expandiendo.
- El escaneado en acceso no puede escanear elementos cifrados. Modifique el proceso de inicio del sistema para que los archivos se puedan escanear cuando se active el escaneado en acceso. Para más información sobre cómo utilizar la política Antivirus y HIPS en sistemas con encriptación, consulte el artículo 12790 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/12790.html>).
- En los casos en los que no utiliza el escaneado en acceso, proteja los ordenadores con escaneados programados. Para más información, consulte *Uso del escaneado programado* en la página 20.



Advertencia: tenga en cuenta que al desactivar el escaneado en acceso aumentan los riesgos de seguridad.

10 Uso del escaneado programado

Siga estas recomendaciones cuando utilice el escaneado programado:

- Use los valores predeterminados cuando sea posible.
- Use el escaneado programado para comprobar la existencia de amenazas o aplicaciones no deseadas en su red.
- Utilice el escaneado programado en servidores donde el escaneado en acceso puede afectar al rendimiento del sistema. Por ejemplo, puede crear un grupo para los servidores Exchange en los que utiliza el escaneado programado para ciertos directorios. Para más información, consulte el artículo 12421 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/12421.html>).
- En los casos en los que no utiliza el escaneado en acceso, proteja los ordenadores con escaneados programados. Ponga estos ordenadores en un grupo y defina un escaneado programado.
- Tenga en cuenta el impacto en el rendimiento durante el escaneado programado. Debería programar estos escaneados a las horas de menor actividad.
- En los servidores, tenga en cuenta las tareas en ejecución. Por ejemplo, si tiene alguna tarea de copia de seguridad, no programe el escaneado para la misma hora.
- Establezca una hora de escaneado. Por ejemplo, programe un escaneado para ejecutarse todos los días a las 9 de la noche. Como mínimo, el escaneado programado se debe ejecutar una vez a la semana.
- La opción **Ejecutar escaneado con baja prioridad** permite que los escaneados personalizados se ejecuten con baja prioridad para minimizar el uso de recursos del sistema. Se recomienda activar esta opción; sin embargo, el escaneado tardará más tiempo en completarse.

11 Uso del escaneado en demanda

Siga estas recomendaciones cuando utilice el escaneado en demanda:

- Use el escaneado en demanda para comprobar un ordenador en un momento dado o para tareas de limpieza.

12 Excluir elementos del escaneado

Siga estas recomendaciones al excluir elementos del escaneado:

- Utilice la exclusión de extensiones para excluir un tipo determinado de archivos.
- Es posible excluir archivos, carpetas o unidades. Para excluir unidades utilice la forma X:, para excluir carpetas utilice la forma X:\carpeta\subcarpeta\ y para excluir archivos utilice la forma X:\carpeta\subcarpeta\programa.exe.
- Puede excluir del escaneado en acceso las unidades de reproducción multimedia para usuarios que las utilizan con frecuencia. Durante la reproducción multimedia se crean archivos temporales que deben escanearse cada vez que se utilizan, lo que puede afectar al rendimiento del sistema.
- Utilice la opción **Excluir archivos remotos** para no escanear archivos en unidades de red. Se recomienda el escaneado de todos los archivos, incluidos los remotos; sin embargo, puede que desee utilizar esta opción en servidores.



Advertencia: tenga en cuenta que la exclusión de archivos del escaneado puede incrementar el riesgo de seguridad.

13 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar el fórum SophosTalk en <http://community.sophos.com/> para consultar casos similares.
- Visitar la base de conocimiento de Sophos en <http://esp.sophos.com/support/>.
- Descargar la documentación correspondiente desde <http://esp.sophos.com/support/docs/>.
- Enviar un email a support@sophos.com indicando la versión del producto de Sophos, el sistema operativo y parches aplicados, y el texto exacto de cualquier mensaje de error.

14 Aviso legal

Copyright © 2011 Sophos Limited. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos y Sophos Anti-Virus son marcas registradas de Sophos Limited. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn’t inform anyone that you’re using DOC software in your software, though we encourage you to let us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹² around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters

acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>.

Common Public License

El software de Sophos descrito en este documento incluye o puede incluir software con licencia (o sublicencia) de público común (CPL) que, entre otros derechos, permiten al usuario tener acceso al código fuente. Las licencias de dichos programas, que se distribuyen al usuario en formato de código de objeto, exigen que el código fuente esté disponible. Para cualquiera de tales programas que se distribuya junto con el producto de Sophos, el código fuente se ofrece a petición por correo; envíe su solicitud a Sophos por email a support@sophos.com o por Internet desde <http://www.sophos.com/support/queries/enterprise.html>. Para ver los términos de la licencia CPL, visite <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation
<http://www.imatix.com>.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (ey@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]