SOPHOS
Security made simple.

Sophos Enterprise Console
Guía de configuración de políticas

Versión: 5.4
Edición: abril de 2016

Contenido

1 Acerca de esta guía

En esta guía se describe la configuración de las políticas de Sophos Enterprise Console y Sophos Endpoint Security and Control.

Nota: las funciones que no se incluyan en su licencia no estarán disponibles.

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 Console.
- Necesita consejos para crear e implementar políticas que se ajusten a sus necesidades.

Antes de leer esta guía, consulte la *Guía rápida de inicio de Sophos Enterprise Console*.

Toda la documentación de Enterprise Console está disponible en http://www.sophos.com/es-es/support/documentation/enterprise-console.aspx.

2 Recomendaciones generales para las políticas

Cuando instale Enterprise Console, se crearán políticas predeterminadas. Estas políticas se aplican a cada grupo nuevo. Las políticas predeterminadas están diseñadas para proporcionar un nivel de protección efectivo. Si desea utilizar funciones como la restricción de aplicaciones, gestión de parches, control de dispositivos, control de datos o control de acceso a la red, deberá crear nuevas políticas o modificar las predeterminadas. 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 Console 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:

- Utilice inicialmente la suscripción "Recomendada" del software para las estaciones de trabajo. Si desea evaluar versiones nuevas del software antes de implementarlas en la red, puede utilizar las versiones fijas del software mientras evalúa las nuevas. Las versiones fijas reciben actualizaciones de los datos de detección, pero no del software.
- 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.

- 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 la Ayuda de Sophos Enterprise Console, sección Actualizar ordenadores > *Configurar la política de actualización.*

- 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 Console y utiliza la misma suscripción de software. El cortafuegos debe estar configurado para permitir la comunicación con otras estaciones. Por defecto, se utiliza el puerto 51235, aunque se puede cambiar.

  Para más información, consulte la Ayuda de Sophos Enterprise Console, sección *Actualizar ordenadores > Configurar la política de actualización > Configurar la ubicación del servidor de actualización.* Para consultar dudas frecuentes sobre la itinerancia, vea el artículo 112830 en la base de conocimiento de Sophos (http://www.sophos.com/es-es/support/knowledgebase/112830.aspx).

- Si le preocupa el rendimiento de ordenadores antiguos, puede suscribirse a una versión fija del software y cambiarla de forma manual cuando decida utilizar una versión más reciente. De esta forma, los ordenadores recibirán sólo actualizaciones de los datos de detección. También 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.
- Para sacar el máximo provecho a la protección activa de Sophos, que viene activada de forma predeterminada, se recomienda activar también la opción **Enviar automáticamente muestras de archivos a Sophos**.
- Active la detección de tráfico malicioso, que detecta las comunicaciones entre equipos y servidores de comando y control utilizados en un ataque de bots u otros ataques maliciosos. La opción **Detección de tráfico malicioso** viene activada de forma predeterminada para nuevas instalaciones de Enterprise Console 5.3 o posterior. Si ha actualizado desde una versión anterior de Enterprise Console, es necesario activar esta opción para poder utilizar la función.

  Nota: la detección del tráfico malicioso actualmente solo se puede llevar a cabo actualmente con Windows 7 y versiones de sistemas operativo que no sean para servidor de versiones posteriores. Requiere Sophos Live Protection.

- 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.

Para más información, consulte el artículo 114345 de la base de conocimiento de Sophos (http://www.sophos.com/es-es/support/knowledgebase/114345.aspx).

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.

2. Protección activa de Sophos. Esta función emplea un sistema de escaneado por Internet desde Sophos para verificar archivos sospechosos en tiempo real. Las funciones de detección de tráfico malicioso y reputación de descargas requieren Sophos Live Protection.

   - Asegúrese de que las opciones **Activar protección activa para el escaneado en acceso** y **Activar protección activa para el escaneado en demanda** estén seleccionadas. 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.
   - Seleccione la opción **Enviar automáticamente muestras de archivos a Sophos**. Si algún archivo sospechoso no se puede identificar mediante los datos iniciales, será necesario enviar una muestra del mismo a Sophos. Con la protección activa activada, si se activa la opción **Enviar automáticamente muestras de archivos a Sophos** y Sophos no tiene ya una muestra del archivo, el archivo se enviará automáticamente. 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, consulte el artículo 62637 de la base de conocimiento (http://www.sophos.com/es-es/support/knowledgebase/62637.aspx). 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.

3. 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 30 o Uso del escaneado programado en la página 31.

   b) Configure las opciones de limpieza de virus y programas espía.

4. 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) Seleccione la opción **Archivos sospechosos**.

   c) Seleccione las opciones de limpieza.

   d) Cuando sea necesario, autorice los archivos sospechosos cuyo uso desee permitir.

5. Detectar comportamiento malicioso y sospechoso, desbordamiento del búfer y tráfico malicioso (control de comportamiento).

Estas opciones permiten monitorizar procesos para detectar cualquier comportamiento malicioso o sospechoso. Esto le ayudará a evitar peligros para la seguridad.

a) Active el control de comportamiento para el escaneado en acceso. Esta opción está activada por defecto.

b) Asegúrese de haber seleccionado la opción **Detectar tráfico malicioso**.

c) Utilice inicialmente la opción **Sólo alertar** para determinar el efecto de estas opciones en su red. Esta opción está activada por defecto.

d) Cuando sea necesario, autorice los programas cuyo uso desee permitir.

e) 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://www.sophos.com/es-es/support/knowledgebase/50160.aspx).

6. 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 escaneado programado para conocer y revisar los programas detectados.

   a) Realice un escaneado 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://www.sophos.com/es-es/support/knowledgebase/13815.aspx).

7. Detección de amenazas en páginas web.

   Esta opción permite bloquear sitios web con contenido malicioso y escanear descargas.

   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 **Escaneado de contenido**, seleccione **Activado** o **Como en acceso** para escanear y bloquear datos descargados maliciosos. Si selecciona la opción **Como en acceso**, opción predeterminada, se utilizará la configuración del escaneado en acceso.

   c) Autorice los sitios web a los que necesite permitir el acceso.

   d) Asegúrese de que la comprobación de la reputación de archivos esté activada.

   Nota: además, puede emplear la política de control web para bloquear el acceso a sitios web no deseados en 14 categorías. Para más información sobre cómo configurar la política de control web, consulte Configuración de políticas de control web en la página 26.

Para más información sobre la política antivirus y HIPS, consulte la Ayuda de Sophos Enterprise Console.

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 con sistemas operativos de servidor. Consulte la página de requisitos del sistema en la web de Sophos (http://www.sophos.com/es-es/products/all-system-requirements).

Advertencia: debe configurar la política cortafuegos antes de utilizarla. Si distribuye la política del cortafuegos sin configurar desde Enterprise Console se producirán errores en el funcionamiento de 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:

- En qué ordenadores instalará 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. Las políticas cubrirán diferentes aplicaciones e incluirán diferentes restricciones. Los grupos de Enterprise Console para las políticas creadas.

- No es recomendable usar tan solo una política de firewall en el cliente de Sophos. 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 **Eventos** > **Eventos del cortafuegos**.
- Revise las reglas mediante el visualizador de eventos. Una aplicación puede provocar diferentes eventos del cortafuegos (según la acción), aunque una regla de aplicación debe cubrir todas las acciones de dicha aplicación. Por ejemplo, un programa de correo electrónico puede provocar eventos diferentes al enviar y recibir correo, sin embargo, la regla de aplicación para este programa debe cubrir ambas acciones.
- 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, en la ficha **General**, en la sección **Ubicación actual**, 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 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 Console, 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.

   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 **Eventos** > **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 sobre cómo crear reglas del cortafuegos, consulte la Ayuda de Sophos Enterprise Console, sección*Configurar políticas > Política del cortafuegos*.

   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 eventos del cortafuegos (según la acción), aunque una regla de aplicación debe cubrir todas las acciones de dicha aplicación. Por ejemplo, un programa de correo electrónico puede provocar eventos diferentes al enviar y recibir correo, sin embargo, la regla de aplicación para este programa debe cubrir ambas acciones.
6. Divida el resto de la red en grupos de equipos equivalentes, por ejemplo, ventas, informáticos, etc.
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 sobre cómo configurar la política del cortafuegos, consulte la Ayuda de Sophos Enterprise Console, sección *Configurar políticas > Política del cortafuegos*.

Nota: de forma alternativa, en redes más pequeñas o en ordenadores independientes con Windows 7 o anterior, 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 restricción de aplicaciones

6.1 Opciones recomendadas

La política de restricción de aplicaciones permite especificar los tipos de aplicaciones que desea bloquear en su red. Al crear una política de restricción de aplicaciones:

- Use inicialmente la opción **Detectar pero permitir ejecución** para ver las aplicaciones que se verían afectadas. Con las alertas se podrá hacer una idea del impacto que esta política puede tener en su red.
- Utilice el visualizador de eventos de la restricción de aplicaciones para ver el uso de aplicaciones a restringir. Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos de la restricción de aplicaciones**.
- Utilice el gestor de informes para seguir la tendencia de uso de estas aplicaciones por ordenador o usuario.
- Considere el uso de la opción "Todas las añadidas por Sophos en el futuro" para bloquear las nuevas aplicaciones del tipo seleccionado que Sophos añada a la lista en sucesivas actualizaciones. Por ejemplo, si está bloqueando en su red las aplicaciones de mensajería instantánea, puede que desee bloquear las nuevas aplicaciones de este tipo que vayan apareciendo.

6.2 Implementación de la política de restricción de aplicaciones

Por defecto no se bloquea ninguna aplicación. Se recomienda introducir la restricción de aplicaciones de la forma siguiente:

1. Considere las aplicaciones que desea restringir.
2. Active el escaneado en acceso, pero seleccione la opción **Detectar pero permitir ejecución** para aplicaciones restringidas.

   En estos momentos, sólo existe una política de control de aplicaciones en la red.
3. Utilice el visualizador de eventos de la restricción de aplicaciones para ver el efecto que tendría en su red la restricción de las aplicaciones o tipos de aplicaciones que desea bloquear. Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos de la restricción de aplicaciones**.
4. Para que cada grupo de equipos tenga acceso a diferentes aplicaciones, cree políticas diferentes para cada uno. Por ejemplo, puede prohibir el uso de aplicaciones de VoIP a los equipos internos, pero permitirlo en los equipos remotos.
5. Determine las aplicaciones o tipos de aplicaciones que desea bloquear.
6. Cuando desee imponer la política, desactive la opción **Detectar pero permitir ejecución**.

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

Nota: la restricción de aplicaciones puede bloquear el programa CScript.exe utilizado por el control de parches. Si utiliza la restricción de aplicaciones y el control de parches, no debe bloquear **Microsoft WSH CScript** en la categoría **Herramienta de programación/scripting**. Por defecto, esta categoría está autorizada.

7 Configuración de políticas de control de datos

7.1 Definir políticas de control de datos

Las políticas de control de datos permiten minimizar el riesgo asociado a la copia accidental de datos importantes.

Cada empresa debe definir cuáles son esos datos importantes. Por ejemplo:

- Datos de clientes con información personal.
- Datos de cuentas bancarias y números de tarjetas de crédito.
- Documentos confidenciales.

El sistema de control de datos de Sophos permite monitorizar posibles puntos de salida de estos datos:

- Transferencia de archivos a dispositivos de almacenamiento (externo, óptico o disquetes).
- Envío de archivos (por email, navegador web o programas de mensajería instantánea).

Una regla de control de datos consta de tres elementos:

- Condición: contenido, tipo de archivo, nombre de archivo, etc.
- Destino: unidades de almacenamiento, aplicaciones, etc.
- Acciones: las acciones disponibles son "Permitir transferencia y registrar evento" (modo de control), "Pedir confirmación al usuario y registrar evento" (modo de aprendizaje) y "Bloquear transferencia y registrar evento" (modo restringido).

Por ejemplo, puede utilizar reglas de control de datos para registrar la subida de hojas de cálculo mediante Internet Explorer o permitir la copia de direcciones de clientes a un DVD tras la confirmación del usuario.

La definición de información importante según el contenido puede resultar compleja. Para simplificar la tarea, Sophos incluye una biblioteca con definiciones de información importante, denominadas listas de control de contenido. Sophos mantiene actualizada esta biblioteca que cubre datos personales y financieros de diferentes países. También es posible definir listas personalizadas para el control del contenido.

Al igual que el resto de las políticas de Sophos, la imposición se realiza incluso en ordenadores fuera de la red empresarial.

7.2 Opciones recomendadas

Al crear una política de control de datos:

- Utilice inicialmente la opción **Permitir transferencia y registrar evento** para detectar transferencias, pero sin interferir. Con las alertas se podrá hacer una idea del impacto que esta política puede tener en su red.
- Utilice la opción **Pedir confirmación al usuario y registrar evento** para informar al usuario del posible riesgo que conlleva copiar ciertos archivos. De esta forma podrá reducir

la salida accidental de datos en su empresa sin una carga excesiva en el departamento informático.

- Utilice la función de cantidad en las reglas de contenido para establecer el umbral permitido. Por ejemplo, una regla que detecte direcciones en documentos será más permisiva si establece un mínimo de 50.

  Nota: Sophos establece una cantidad estándar en cada lista de control de contenido.

- Utilice el visualizador de eventos de control de datos para obtener detalles de cada caso que se presente. Los eventos y acciones de control de datos se registran en Enterprise Console. Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos del control de datos**.
- Utilice el gestor de informes para seguir la tendencia de los eventos de control de datos por regla, ordenador o usuario.
- 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 la seguridad de datos.
- Utilice el registro detallado para obtener más información sobre la precisión de las reglas de control de datos. Desactive el registro detallado tras la evaluación de las reglas.

  Nota: el registro detallado debe activarse en cada ordenador. La información se almacena de forma local. El registro detallado almacena cada cadena que contenga el valor de las reglas especificadas. La información adicional le permitirá identificar las frases o cadenas en los documentos detectados.

7.3 Implementación de la política de control de datos

Por defecto, el control de datos está desactivado y no existen reglas para el control o para la restricción de transferencias de archivos a través de aplicaciones o a dispositivos de almacenamiento. Se recomienda introducir el control de datos de la forma siguiente:

1. Comprenda al funcionamiento del sistema de control de datos:
   - **Dispositivo de almacenamiento:** El control de datos intercepta todos los archivos que se copian en dispositivos de almacenamiento controlados mediante el Explorador de Windows (incluido el Escritorio). Sin embargo, no se interceptan los archivos que se guardan desde aplicaciones, como Microsoft Word, o mediante transferencias desde la línea de comandos.

     Las acciones "Pedir confirmación al usuario y registrar evento" y "Bloquear transferencia y registrar evento" permiten hacer que el uso del Explorador de Windows sea obligatorio para todas las transferencias a dispositivos de almacenamiento controlados. En ambos casos, el control de datos impide la transferencia de archivos desde la línea de comandos o que se guarden directamente desde una aplicación, y aparece una alerta para que el usuario utilice el Explorador de Windows.

     Cuando las políticas de control de datos sólo contienen reglas para la acción "Permitir transferencia y registrar evento", es posible guardar archivos directamente desde aplicaciones y realizar transferencias desde la línea de comandos. Esta configuración permite que los usuarios utilicen dispositivos de almacenamiento libremente. Sin embargo, se siguen registrando eventos de control de datos de las transferencias realizadas mediante el Explorador de Windows.

     Nota: esta restricción no afecta al control de aplicaciones.

- **Aplicaciones:** El control de datos intercepta archivos y documentos cargados en aplicaciones controladas. Para garantizar que sólo se controlan los archivos cargados por los usuarios, ciertas carpetas del sistema están excluidas del control de datos. Para más información sobre el contenido o acciones de aplicaciones que se escanean o no, consulte Escaneado del control de datos de aplicaciones en la página 18.

  Nota: el escaneado del control de datos escanea todos los adjuntos, sin escanear el contenido de los mensajes de correo electrónico. La solución Sophos Email Security and Data Protection puede utilizarse si es necesario escanear el contenido del correo electrónico.

2. Considere el tipo de información que desea identificar y cree las reglas apropiadas. Sophos proporciona reglas de ejemplo que pueden utilizarse para establecer su política de control de datos.

   Importante: a la hora de crear reglas de contenido, es aconsejable tener en cuenta que el escaneado de contenido puede ser un proceso intenso. Realice pruebas de cada regla para establecer el posible impacto antes de implantarlas en toda la red.

   Nota: al crear la política inicial, se recomienda centrarse en la detección de listas de datos personales. Sophos proporciona reglas de ejemplo que cumplen este requisito.

3. Active el escaneado de control de datos pero seleccione inicialmente la opción **Permitir transferencia y registrar evento** en las reglas seleccionadas.

   Importante: se recomienda utilizar esta opción en las reglas nuevas antes de implantarlas. De esta forma podrá verificar la efectividad de cada regla sin afectar a la productividad.

4. Realice la implantación de la política de control de datos de forma escalonada.
5. Utilice el visualizador de eventos de control de datos para corregir posibles problemas (por ejemplo, si una regla es demasiado sensible). Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos del control de datos**.
6. Una vez terminado el proceso de prueba, realice los ajustes necesarios y distribuya la política al resto de la red. Ahora es el momento de:
   - Cambiar acciones por las reglas necesarias para **Pedir confirmación al usuario y registrar evento** o **Bloquear transferencia y registrar evento**.
   - Crear políticas específicas para cada grupo. Por ejemplo, puede permitir que los equipos del departamento de recursos humanos sean los únicos que puedan realizar transferencias de datos personales.

Para más información sobre la política de control de datos, consulte la Ayuda de Sophos Enterprise Console.

7.4 Escaneado del control de datos de aplicaciones

Esta lista enumera los elementos o acciones de las aplicaciones compatibles que se escanean o no.

Para ver una lista completa de las limitaciones conocidas del control de datos, consulte el artículo 63016 de la base de conocimiento de Sophos (http://www.sophos.com/es-es/support/knowledgebase/63016.aspx).

Applications	Acciones escaneadas
Navegadores de Internet	**Escaneados:** ▪ Cargas de archivos ▪ Adjuntos de correo web ▪ Cargas de Microsoft SharePoint **No escaneados** ▪ Contenido de mensajes de correo web ▪ Entradas de blogs ▪ Descargas de archivos **Nota:** en limitadas ocasiones, algunos archivos se escanean al descargarse.
Programas de correo electrónico	**Escaneados** ▪ Adjuntos de correo electrónico **No escaneados** ▪ Contenido de mensajes de correo electrónico ▪ Adjuntos reenviados ▪ Adjuntos enviados mediante la opción "Enviar por correo electrónico" de aplicaciones como el Explorador de Windows o Microsoft Office ▪ Adjuntos enviados mediante la opción "Enviar este archivo por correo electrónico" del Explorador de Windows ▪ Adjuntos copiados de un correo electrónico a otro ▪ Adjuntos guardados **Nota:** en limitadas ocasiones, algunos archivos se escanean al guardarse.
Programas de mensajería instantánea	**Escaneados** ▪ Transferencias de archivos **Nota:** ciertos archivos se escanean dos veces: al cargarlos en programas de mensajería instantánea y cuando el destinatario los acepta. Ambos escaneados tienen lugar en el equipo del remitente. **No escaneados** ▪ Contenido de mensajes de aplicaciones de mensajería instantánea ▪ Archivos enviados

8 Configuración de políticas de control de dispositivos

8.1 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 **Eventos** > **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://www.sophos.com/es-es/support/knowledgebase/63102.aspx).
- 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 Console y se implementan a través de la red; así, una vez bloqueado el dispositivo de red, no podrá desbloquearlo desde Enterprise Console porque no existe conexión de red con las estaciones afectadas.

8.2 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 **Eventos** > **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.
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 Console.

9 Configuración de políticas de protección contra manipulaciones

9.1 Acerca de la política de protección contra manipulaciones

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 7.

Después de que active la protección contra manipulaciones y cree una contraseña de protección contra manipulaciones, los usuarios que no conozcan la contraseña no podrán reconfigurar el escaneado en acceso ni la detección de comportamientos sospechosos en Sophos Endpoint Security and Control, desactivar la protección contra manipulaciones ni desinstalar componentes de Sophos Endpoint Security and Control (como Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate o Sophos Remote Management System) 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 **Eventos** > **Eventos de la protección contra manipulaciones**.

9.2 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.

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

10 Configuración de políticas de parches

Nota: esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte http://www.sophos.com/es-es/products/endpoint/endpoint-protection/pricing.aspx.

10.1 Acerca de la política de parches

Las políticas de parches permiten comprobar que los equipos tienen instalados los parches más recientes.

El nivel de gravedad permite identificar los problemas de seguridad más críticos relacionados con los parches para resolverlos con prontitud. Para establecer el nivel de gravedad, SophosLabs tiene en cuenta las amenazas más recientes que se aprovechan de agujeros de seguridad.

Al configurar su política de parches, considere utilizar el visualizador de eventos del control de parches para comprobar la falta de parches en los equipos de su empresa. Se mostrará información sobre los parches de seguridad. Puede ver el estado del control de parches por equipo, grupo o peligrosidad. Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos del control de parches**.

Nota: el control de parches utiliza CScript.exe, que puede bloquearse mediante la restricción de aplicaciones. Si utiliza la restricción de aplicaciones y el control de parches, no debe bloquear **Microsoft WSH CScript** en la categoría **Herramienta de programación/scripting** en la política de **Restricción de aplicaciones**. Por defecto, esta categoría está autorizada.

10.2 Implementación de la política de parches

Inicialmente, la política de parches predeterminada se aplica a todas las estaciones. El control de parches no se encuentra activado en la política predeterminada.

Al activar el control de parches en las estaciones, se realiza la comprobación inicial. Puede tardar unos minutos. Las comprobaciones posteriores se realizan con la frecuencia establecida (por defecto, a diario).

Nota: si las estaciones realizan la comprobación antes de que Enterprise Console haya descargado los datos de parches desde Sophos, el visualizador de eventos de parches no mostrará nada. La descarga inicial puede tardar varias horas. Para comprobar si se ha completado la descarga, vea el campo **Actualización de parches** en el **Visualizador de eventos del control de parches**.

Se recomienda introducir la política de parches de la forma siguiente:

1. Distribuya el agente de parches a las estaciones mediante el Asistente para proteger ordenadores. (En la página **Seleccionar funciones** del asistente, seleccione **Parches**.)

   Nota: debe volver a proteger mediante el Asistente para proteger ordenadores las estaciones con Endpoint Security and Control que no dispongan del control de parches.

2. Active el control de parches en la política predeterminada.

   De momento, sólo dispone de una política de control de parches.

3. Utilice el visualizador de eventos del control de parches para revisar el estado de actualización de la red. Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos del control de parches**.

   Nota: instale los parches necesarios en los equipos de la red.

4. Si desea disponer de diferentes opciones en diferentes grupos, cree las políticas necesarias para los diferentes grupos.

Para más información sobre la política de parches, consulte la Ayuda de Sophos Enterprise Console.

11 Configuración de políticas de control web

Nota: esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte http://www.sophos.com/es-es/products/endpoint/endpoint-protection/pricing.aspx.

La política de control web permite restringir los sitios web a los que se permite el acceso.

Por defecto, el control web se encuentra desactivado, por lo que se permite el acceso a todos los sitios web que no estén restringidos en Enterprise Console. Se ofrece control de sitios web inapropiados y control web completo. A continuación se describen ambos.

11.1 Opciones recomendadas

Se ofrecen dos tipos de control web: Control de sitios web inapropiados y Control web completo. Las opciones recomendadas son diferentes en cada caso. Al crear una política de control web:

Control de sitios web inapropiados

- Revise la acción para cada tipo de categoría web. Para que cada grupo de equipos tenga acceso web diferenciado, cree políticas diferentes para cada uno. Por ejemplo, puede que desee bloquear el acceso a ciertos sitios web en ciertos departamentos y no en otros.
- Prepare la lista de excepciones antes de implantar el control web. Puede introducir sitios web de forma manual en la ficha **Excepciones de sitios web** para excluirlos de la política. Por ejemplo, puede crear excepciones para direcciones web locales o bloquear ciertos sitios web en alguna categoría permitida.
- Utilice el visualizador de eventos del control web para obtener detalles de cada caso que se presente. Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos web**. Ajuste la acción para las diferentes categorías según sus necesidades.

Control web completo

Importante: debe disponer de Sophos Web Appliance o Security Management Appliance para utilizar el control web completo.

- Para la configuración de estos dispositivos consulte la Guía de configuración de Sophos Web Appliance y la Guía de configuración de Security Management Appliance. Los dispositivos disponen de un asistente para realizar la configuración según sus necesidades.
- Puede configurar diferentes políticas para los diferentes tipos de usuario. Consulte la documentación de Web Appliance para más información.

  La documentación de Sophos Web Appliance está disponible en http://wsa.sophos.com/docs/wsa/.

- Prepare la lista de excepciones antes de implantar el control web. Por ejemplo, puede que desee utilizar la opción de horario especial para permitir un acceso menos restrictivo

fuera de las horas de trabajo. También puede crear políticas adicionales para ciertos usuarios, como excepción a la política predeterminada y horario especial.

- Establezca la acción a realizar cuando no se pueda determinar la categoría de un sitio web. Por defecto, la opción **Bloquear si no se puede determinar la categoría del sitio web *no*** se encuentra activada. Esto significa que se permite el acceso a todos los sitios web si falla el servicio de categorización. Si activa esta opción, se bloquearán los sitios web mientras no se conozca la categoría.

Para más información, consulte la documentación de Sophos Enterprise Console y Sophos Web Appliance.

11.2 Implementación de la política de control web

Decida el tipo de filtrado a emplear: Control de sitios web inapropiados o Control web completo. Debe disponer de Sophos Web Appliance o Security Management Appliance para utilizar el control web completo.

Para más información sobre la política de control web, consulte la Help de Sophos Enterprise Console.

11.2.1 Implementación de la política de control de sitios web inapropiados

Este control web básico incluye 14 categorías. Está diseñado para evitar el acceso a sitios web inapropiados. Al implementar una política de control web, tenga en cuenta los siguientes aspectos. Consulte la documentación de Enterprise Console.

1. Compruebe que el tiene activado el control web.
2. Ajuste la configuración a las necesidades de su empresa para bloquear sitios web que considere inapropiados.
3. Para permitir el acceso a diferentes sitios web en los diferentes grupos, cree una política para cada grupo.
4. Tenga en cuenta los grupos a los que debe aplicar el control web y el tipo de control que desea emplear.
5. Revise la acción para cada tipo de categoría web. Puede cambiar la acción desde el cuadro desplegable correspondiente. Las acciones disponibles son: bloquear, permitir y avisar.
6. Para añadir excepciones, utilice las listas **Sitios web autorizados** y **Sitios web bloqueados**.

   Nota: si existe algún conflicto entre las listas 'Bloquear' y 'Permitir', la de bloquear siempre tiene preferencia. Por ejemplo, si añade la misma dirección IP en las listas Bloquear y Permitir, dicha dirección será bloqueada. Además, si un dominio se encuentra en la lista Bloquear, también se bloquearán los subdominios aunque se encuentren en la lista Permitir.

7. Utilice el visualizador de eventos del control web para comprobar la efectividad de la política. Para acceder al visualizador de eventos, haga clic en **Eventos** > **Eventos web**. Compruebe los eventos del control web. Realice los ajustes necesarios.

Para más información, consulte la documentación de Enterprise Console.

11.2.2 Implementación de la política de control web completo

Este es el modo de control web más completo. De esta forma podrá realizar un control completo y detallado del acceso a Internet y dispondrá de informes de tráfico web. Debe disponer de Sophos Web Appliance o Security Management Appliance.

1. Configure Sophos Web Appliance o Security Management Appliance como se describe en la documentación del dispositivo, y asegúrese de que se encuentra activada la opción **Endpoint Web Control**.
2. Compruebe que tiene activado el control web en Enterprise Console.
3. Ajuste la configuración a las necesidades de su empresa para bloquear sitios web que considere inapropiados.
4. Para permitir el acceso a diferentes sitios web en los diferentes grupos, cree una política para cada grupo.
5. Considere los sitios web que desea controlar Qué categorías desea bloquear. Qué categorías desea permitir. Qué categorías desea avisar.
6. Determine las excepciones web e introdúzcalas en el dispositivo web (Local Site List).
7. Con el control web completo, puede utilizar Sophos LiveConnect. Puede utilizar LiveConnect para distribuir las políticas y realizar el registro incluso cuando los usuarios no se conectan desde la red de la empresa.

Para más información, consulte la documentación de Sophos Enterprise Console y Sophos Web Appliance.

12 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.
- Configurar el escaneado de forma centralizada desde Enterprise Console.
- 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.

13 Uso del escaneado en acceso

Siga estas recomendaciones cuando utilice el escaneado en acceso:

- Use los valores predeterminados cuando sea posible.
- Las opciones del escaneado en acceso **Leer**, **Escribir** y **Cambiar nombre** se activan por defecto en instalaciones nuevas. Para las actualizaciones desde versiones anteriores, deberá activarlas de forma manual.
- 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://www.sophos.com/es-es/support/knowledgebase/12790.aspx).
- 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 31.

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

14 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.
- 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.

15 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.

16 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.

17 Soporte técnico

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

- Visitar la comunidad de Sophos en community.sophos.com/ para consultar casos similares.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx.
- Descargar la documentación correspondiente desde www.sophos.com/es-es/support/documentation.aspx.
- Abrir un ticket de incidencia con nuestro equipo de soporte en https://secure2.sophos.com/support/contact-support/support-query.aspx.

18 Aviso legal

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, 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. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

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

Douglas C. 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

Boost C++ Libraries

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the “Software”) to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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, el código fuente está disponible mediante solicitudes por correo ordinario a Sophos, por correo electrónico a soporte@sophos.com o desde la página

web https://www.sophos.com/es-es/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at 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.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL Cryptography and SSL/TLS 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 © 1998–2011 The OpenSSL Project. Todos los derechos reservados.

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

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (eay@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 (eay@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 license 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 license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT HOLDER 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.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: https://sourceforge.net/projects/wtl/files/

zlib data compression library

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu