

SOPHOS

Sophos Endpoint Security and Control Guía de configuración de políticas

Edición: septiembre de 2009



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 de restricción de aplicaciones.....8
- 6 Configuración de políticas de control de dispositivos.....9
- 7 Configuración de políticas de control de datos.....11
- 8 Configuración de políticas del cortafuegos.....16
- 9 Configuración de políticas NAC.....19
- 10 Recomendaciones de escaneado.....21
- 11 Uso del escaneado en acceso.....22
- 12 Uso del escaneado programado.....23
- 13 Uso del escaneado en demanda24
- 14 Exclusión de elementos del escaneado.....25
- 15 Soporte técnico.....26
- 16 Copyright.....27

1 Acerca de esta guía

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

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 Endpoint Security and Control*.

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

2 Recomendaciones generales para las políticas

Al instalar Enterprise Console se crean las políticas predeterminadas. Estas políticas se aplican por defecto 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, 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, debería:

- Usar los valores predeterminados cuando sea posible.
- Tener 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).
- Usar Enterprise Console para centralizar la aplicación y cumplimiento de las políticas en la red.
- Modificar 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.
- Crear 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, debería:

- Utilizar 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.
- Asegurarse 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.

- Especificar una fuente alternativa de actualización si dispone de ordenadores que no están conectados a la red de la empresa de forma constante (como ordenadores portátiles). Si las estaciones no pueden contactar con el servidor primario, lo intentarán con el secundario. Para más información, consulte la Ayuda de Sophos Enterprise Console.
- 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 incrementar 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, debería:

- Utilizar 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 inicialmente la opción **Sólo alertar** al activar el análisis de comportamiento (HIPS). 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

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

1. Cree políticas específicas para cada grupo.
2. Establezca 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 (<http://esp.sophos.com/support/knowledgebase/article/12421.html>).
3. Detecte 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.
 - b) Configure las opciones de limpieza de virus y programas espía.
4. Detecte 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 **Detectar archivos sospechosos (HIPS)**.
 - c) Seleccione las opciones de limpieza.
 - d) Cuando sea necesario, autorice los archivos sospechosos cuyo uso desee permitir.
5. Detecte comportamientos sospechosos y desbordamientos del búfer (HIPS).

Estas opciones de escaneado permiten controlar procesos en ejecución de forma continua para determinar si el comportamiento es sospechoso. De este modo, podrá evitar problemas de 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 (<http://esp.sophos.com/support/knowledgebase/article/50160.html>).

6. Detecte 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.

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

7. Active el escaneado en acceso para proteger los equipos en lo sucesivo. Para más información, consulte *Uso del escaneado en acceso* en la página 22.

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

5 Configuración de políticas de restricción de aplicaciones

5.1 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, debería:

- Usar 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 visor de eventos, haga clic en **Ver < 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.

5.2 Implementación de la política de restricción de aplicaciones

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

1. Considere las aplicaciones que desea restringir.
2. Active el escaneo 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 visor de eventos, haga clic en **Ver < 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 las opciones de la política de restricción de aplicaciones, vea la Ayuda de Sophos Enterprise Console.

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, debería:

- Activar 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.
- Utilizar el visualizador de eventos de control de dispositivos para obtener detalles de cada caso que se presente. Para acceder al visor de eventos, haga clic en **Ver < Eventos del control de dispositivos**.
- Utilizar el gestor de informes para seguir la tendencia de uso de estos dispositivos por ordenador o usuario.
- Considerar un mayor control en ordenadores de usuarios que traten con información delicada.
- Preparar 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.
- Al añadir excepciones de dispositivos, hacer uso del campo **Comentario** para describir la razón para dicha excepción.
- Hacer uso del mensaje personalizado de escritorio para informar al usuario con 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.

6.2 Implementación de la política de control de dispositivos

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

Nota: Si disponía de Enterprise Console 3.1, las funciones de control de dispositivos se encuentran en la política de restricción de aplicaciones. Para transferir la configuración a la política de control de dispositivos, utilice la herramienta de migración. Para más información, consulte la Guía avanzada de actualización de Sophos Endpoint Security and Control.

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 visor 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.
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 las opciones de la política de control de dispositivos, vea la Ayuda de Sophos Enterprise Console.

7 Configuración de políticas de control de datos

7.1 Definición del 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 complicada. 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 de 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, debería:

- Utilizar 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.
- Utilizar 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.

- Utilizar 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.

- Utilizar 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 visor de eventos, haga clic en **Ver < Eventos del control de datos**.
- Utilizar el gestor de informes para seguir la tendencia de los eventos de control de datos por regla, ordenador o usuario.
- Hacer uso del mensaje personalizado de escritorio para informar al usuario con los detalles necesarios. Por ejemplo, podría incluir un enlace a la política interna de la empresa sobre la seguridad de datos.
- Utilizar 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. Sophos aconseja introducir el control de datos de la forma siguiente:

1. Comprenda al funcionamiento del sistema de control de datos:

- **Dispositivos 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 14.

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, Sophos recomienda centrarse en la detección de listas de datos personales. Sophos proporciona reglas de ejemplo que cumplen este requisito.

3. Active el escaneo de control de datos pero seleccione inicialmente la opción **Permitir transferencia y registrar evento** en las reglas seleccionadas.
Importante: Sophos 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 visor de eventos, haga clic en **Ver < 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 las opciones de la política de control de datos, vea la Ayuda de Sophos Enterprise Console.

7.4 Escaneo 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 (<http://esp.sophos.com/support/knowledgebase/article/63016.html>).

Aplicaciones	Acciones escaneadas
Navegadores de Internet	<p>Escaneados</p> <ul style="list-style-type: none"> ■ Cargas de archivos ■ Adjuntos de correo web ■ Cargas de Microsoft SharePoint <p>No escaneados</p> <ul style="list-style-type: none"> ■ Contenido de mensajes de correo web ■ Entradas de blogs ■ Descargas de archivos <p>Nota: En limitadas ocasiones, algunos archivos se escanean al descargarse.</p>

Aplicaciones	Acciones escaneadas
Programas de correo electrónico	<p>Escaneados</p> <ul style="list-style-type: none"> ■ Adjuntos de correo electrónico <p>No escaneados</p> <ul style="list-style-type: none"> ■ 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
Programas de mensajería instantánea	<p>Escaneados</p> <ul style="list-style-type: none"> ■ Transferencias de archivos <p>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.</p> <p>No escaneados</p> <ul style="list-style-type: none"> ■ Contenido de mensajes de aplicaciones de mensajería instantánea ■ Archivos enviados

8 Configuración de políticas del cortafuegos

8.1 Opciones recomendadas

La política del cortafuegos establece la configuración del cortafuegos en las estaciones de la red. Al crear una política del cortafuegos, debería:

- Copiar la configuración existente del cortafuegos de Windows antes de implantar Sophos Client Firewall ya que no se puede tener ambos activos al mismo tiempo.
- Utilizar inicialmente la opción **Permitir por defecto**. Con las alertas se podrá hacer una idea del impacto que esta política puede tener en su red.
- Utilizar 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 visor de eventos, haga clic en **Ver < Eventos del cortafuegos**.
- Utilizar el modo **Interactivo** en los ordenadores de prueba para añadir las aplicaciones necesarias mediante los cuadros de diálogo de aprendizaje.
- En el modo **Interactivo**, se recomienda que desactive la opción **Enviar alerta a la consola de administración si se modifica alguna regla global, aplicación, proceso o suma de verificación** para evitar alertas innecesarias en la consola de administración.
- Permitir el uso de navegadores web, programas de email y uso compartido de archivos e impresoras.
- Sophos recomienda no modificar la configuración predeterminada de ICMP, reglas globales o reglas de aplicaciones a menos que tenga un conocimiento avanzado sobre redes.
- Sophos recomienda crear reglas de aplicaciones en vez de reglas globales cuando sea posible.

8.2 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.

Sophos 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 segunda, con un acceso más restringido.
- Al configurar la detección de la ubicación primaria, Sophos 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, Sophos recomienda crear una entrada específica en el servidor DNS con dirección de retorno (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.

8.3 Cuándo bloquear o permitir tráfico, aplicaciones y procesos

Se pueden presentar diferentes situaciones según su configuración:

- Si el cortafuegos se encuentra en modo **Interactivo**, debe educar al usuario para que pueda decidir cuándo bloquear o permitir tráfico, aplicaciones y procesos.
- Si el cortafuegos se encuentra en modo **Bloquear por defecto**, el administrador es responsable de ajustar la configuración desde Enterprise Console.
- La opción **Bloquear sólo esta vez** sólo se debe utilizar cuando el usuario no está seguro. Esta opción sólo está disponible en el modo **Interactivo**.
- Existen ciertos casos en los que **no** debe bloquear el tráfico. Por ejemplo, en el caso de navegadores web, programas de email, el uso compartido de archivos e impresoras y otros programas que requieren acceso a Internet.
- Una vez establecidas las reglas de acceso para las aplicaciones existentes, sólo se preguntará al instalar nuevas aplicaciones o al actualizarse (sólo en modo **Interactivo**).

8.4 Implementación de la política del cortafuegos

Por defecto, el cortafuegos se encuentra activado y bloquea el tráfico de red no esencial. Deberá configurar el cortafuegos para permitir el tráfico, aplicaciones y procesos necesarios, y hacer pruebas antes de implementar la política en toda la red. Sophos aconseja introducir la política del cortafuegos de la forma siguiente:

1. Planifique la política y lo que quiere que haga, antes de crear o modificar las reglas del cortafuegos.
2. Utilice inicialmente la opción **Permitir por defecto**.
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 visor de eventos, haga clic en **Ver < Eventos del cortafuegos**.
4. Cree las reglas globales y de aplicaciones necesarias.

Nota: Como alternativa a los pasos 1 a 4, puede utilizar el modo **Interactivo** para después importar y editar las reglas creadas. Para más información, consulte la Ayuda de Sophos Endpoint Security and Control.

5. Se aconseja realizar una distribución por fases de Sophos Client Firewall en la red. Así, evitará saturar el tráfico de la red durante los pasos iniciales. Distribuya Sophos Client

Firewall primero en un grupo pequeño de ordenadores que pueda controlar fácilmente. Dicho grupo debería ser representativo de los diferentes roles de la red.



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

- a) Instale y configure Sophos Client Firewall en los ordenadores de prueba.
 - b) Ejecute los programas y procedimientos habituales en dichos ordenadores.
 - c) Compruebe si existen puntos débiles en la configuración de prueba (por ejemplo, otorgar demasiado acceso a algunos usuarios).
 - d) Cree reglas adicionales en los ordenadores necesarios.
 - e) Una vez probadas las reglas, pase al modo **Bloquear por defecto** para comenzar a proteger los ordenadores.
6. Una vez completada la fase de prueba, podrá instalar Sophos Client Firewall en toda su red.
- Es importante que no sature la red. No implemente la política en toda la red al mismo tiempo.
- Seleccione hasta 100 ordenadores cada vez.
 - Realice la distribución a los grupos por partes.

Para más información sobre las opciones de la política del cortafuegos, vea la Ayuda de Sophos Enterprise Console. Para más información sobre la configuración predeterminada del cortafuegos, consulte el artículo 14464 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/14464.html>).

Para más información sobre las nuevas funciones del cortafuegos en Enterprise Console 4.0, consulte el artículo 54750 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/54750.html>).

9 Configuración de políticas NAC

9.1 Políticas NAC predefinidas

Las políticas NAC especifican las condiciones que cada ordenador debe cumplir para obtener acceso a la red de la empresa. Por defecto, Sophos NAC permite el acceso a todos los ordenadores. Debe implementar una política NAC para controlar el acceso a la red.

Utilice las políticas predefinidas para imponer el cumplimiento de la seguridad en estaciones tanto administradas como no. Puede modificar las políticas predeterminadas desde NAC Manager para cambiar el modo de funcionamiento, los perfiles o las plantillas de acceso utilizados.

Se ofrecen las siguientes políticas:

- **Predeterminada:** Esta política se usa cuando una estación tiene el agente instalado pero no se ha asignado ninguna otra política. El modo de funcionamiento está configurado por defecto para sólo enviar informes. Esta política realiza acciones de remediación en la estación si el modo de funcionamiento se configura para remediar o imponer.
- **Managed:** Esta política se usa en ordenadores administrados desde Enterprise Console y que disponen del agente. El modo de funcionamiento está configurado por defecto para sólo enviar informes. Esta política realiza acciones de remediación en la estación si el modo de funcionamiento se configura para remediar o imponer.
- **Unmanaged:** Esta política puede utilizarse para equipos que no pertenecen a la empresa. Esta política no realiza acciones de remediación en las estaciones. El agente soluble utiliza la política no administrada.

Para más información sobre la actualización de las políticas predefinidas, consulte la ayuda de Sophos NAC Manager.

9.2 Implementación de la política NAC

Al instalar NAC por primera vez, se aplica la política NAC predeterminada a los equipos. Si desea hacer cambios en la política o utilizar una distinta, utilice Sophos NAC Manager para hacer los cambios y Enterprise Console para aplicarla a los equipos. Sophos aconseja introducir la política NAC de la forma siguiente:

1. En Enterprise Console, utilice el asistente para proteger ordenadores para instalar el agente en las estaciones de la red.
2. En NAC Manager, compruebe que las políticas NAC contienen los perfiles y plantillas de acceso necesarias.
3. Utilice Enterprise Console para aplicar la política Managed a los diferentes grupos.
El agente comprobará el cumplimiento de la política inicialmente en modo de sólo informes.
4. Utilice los informes de NAC Manager para determinar el estado de cumplimiento actual en la red.

Los informes ofrecen una visión general del grado de cumplimiento de acuerdo con la política NAC.

5. Utilice NAC Manager para actualizar la política Managed. Cambie el modo de funcionamiento de sólo informes al de remediación.
6. Utilice los informes de NAC Manager para determinar el estado de cumplimiento actual en la red.

Con el tiempo, las estaciones que no cumplen las políticas o que sólo las cumplen parcialmente, se adecuarán de forma automática a las condiciones de la política.

7. Utilice NAC Manager para actualizar la política Managed. Cambie el modo de funcionamiento al de imposición.
8. Utilice los informes de NAC Manager para determinar el estado de cumplimiento actual en la red.

Las estaciones que no cumplan las políticas deberán remediarse o se les denegará el acceso a la red.

Para más información sobre la configuración de NAC, vea la ayuda de Sophos NAC Manager.

10 Recomendaciones de escaneado

Las opciones de escaneado que se describen en las siguientes secciones se configuran desde la política antivirus y HIPS; aunque ciertas opciones, como extensiones y exclusiones, también se aplican a la política de restricción de aplicaciones. Al establecer las opciones de escaneado, debería:

- Usar los valores predeterminados cuando sea posible.
- Configurar el escaneado de forma centralizada desde Enterprise Console.
- Tener en cuenta el uso del ordenador (estación o servidor).
- Utilizar el escaneado **Normal** y no el **Exhaustivo**. En el escaneado normal se comprueban las partes de los archivos que pueden contener virus, mientras que en el escaneado exhaustivo se comprueba el contenido completo. Sólo debe utilizar el escaneado exhaustivo cuando así se lo indiquen desde soporte técnico.
- No utilizar 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.
- No utilizar la opción **Escanear dentro de archivos comprimidos**. Los archivos se escanearán cuando se descompriman. Sophos no recomienda el uso de esta opción a menos que utilice archivos comprimidos a menudo.

11 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 encriptados. 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 (<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 23.



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

12 Uso del escaneo programado

Siga estas recomendaciones cuando utilice el escaneo programado:

- Use los valores predeterminados cuando sea posible.
- Use el escaneo programado para comprobar la existencia de amenazas o aplicaciones no deseadas en su red.
- Utilice el escaneo programado en servidores donde el escaneo en acceso puede afectar al rendimiento del sistema. Por ejemplo, puede crear un grupo para los servidores Exchange en los que utiliza el escaneo programado para ciertos directorios. Para más información, consulte el artículo 12421 de la base de conocimiento (<http://esp.sophos.com/support/knowledgebase/article/12421.html>).
- En los casos en los que no utiliza el escaneo en acceso, proteja los ordenadores con escaneados programados. Ponga estos ordenadores en un grupo y defina un escaneo programado.
- Tenga en cuenta el impacto en el rendimiento durante el escaneo 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 escaneo para la misma hora.
- Establezca una hora de escaneo. Por ejemplo, programe un escaneo para ejecutarse todos los días a las 9 de la noche. Como mínimo, el escaneo programado se debe ejecutar una vez a la semana.

13 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.

14 Exclusión de elementos del escaneo

Siga estas recomendaciones al excluir elementos del escaneo:

- 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 escaneo 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. Sophos recomienda el escaneo 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 escaneo puede incrementar el riesgo de seguridad.

15 Soporte técnico

Para recibir soporte técnico, vaya a <http://esp.sophos.com/support>.

Cuando se ponga en contacto con el servicio de soporte técnico, ofrezca toda la información posible, incluyendo:

- La versión del software de Sophos
- Los sistemas operativos y parches
- El texto exacto de cualquier mensaje de error

16 Copyright

Copyright © 2009 Sophos Group. 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 Plc y Sophos Group. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

El software de Sophos descrito en este documento incluye o puede incluir software bajo licencia (o sublicencia) Common Public License (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 el usuario. Para cualquiera de tales programas, el código fuente está disponible mediante solicitudes por correo ordinario; por email a support@sophos.com o desde la página web <http://www.sophos.com/support/queries/enterprise.html>. Puede encontrar una copia de los términos de licencia en <http://opensource.org/licenses/cpl1.0.php>