McAfee Host Intrusion Prevention 8.0

Guía de instalación

Contenido

Instalación de McAfee Host Intrusion Prevention **5**

Componentes 6

Introducción a la instalación 7

Novedades de esta versión 8

Recomendaciones para un éxito rápido **11**

1. Creación de estrategias 13

2. Preparar un entorno de seguimiento 16

3. Instalación y configuración 19

4. Realizar el ajuste inicial 20

5. Activar modo Adaptación (opcional) 23

6. Ajustes 25

7. Realizar tareas de mantenimiento y expansión 26

Instalación en ePolicy Orchestrator **28**

Instalación de la extensión 29

Eliminación de la extensión 30

Migración de directivas **31**

Migración de directivas de versiones anteriores 32

Migración de directivas a través de un archivo .xml 33

Instalación del cliente Windows **34**

Detalles del cliente Windows 34

Instalación remota del cliente Windows 36

Instalación local del cliente Windows 36

Aplicación de directivas y actualizaciones de contenido IPS 37

Eliminación del cliente Windows 37

Cómo solucionar problemas de instalación de Windows 38

Detención del cliente Windows 39

Reinicio del cliente Windows 40

Instalación del cliente Solaris **41**

Detalles del cliente Solaris 41

Instalación remota del cliente Solaris 43

Instalación local del cliente Solaris. 43
Aplicación de directivas y actualizaciones de contenido IPS. 44
Eliminación del cliente Solaris. 44
Cómo solucionar problemas de instalación de Solaris. 44
Detención del cliente Solaris. 45
Reinicio del cliente Solaris. 45
Instalación del cliente Linux. **46**
Detalles del cliente Linux. 46
Instalación remota del cliente Linux. 48
Instalación local del cliente Linux. 49
Aplicación de directivas y actualizaciones de contenido IPS. 50
Eliminación del cliente Linux. 50
Cómo solucionar problemas de instalación de Linux. 50
Detención del cliente Linux. 51
Reinicio del cliente Linux. 51

Instalación de McAfee Host Intrusion Prevention

Esta guía ofrece toda la información necesaria para instalar y empezar a usar el software Host Intrusion Prevention 8.0 en un entorno gestionado. La extensión del producto se instala en las versiones 4.0, 4.5 y 4.6 del servidor de ePolicy Orchestrator. El cliente se instala en las estaciones de trabajo Windows y en servidores Windows, Solaris y Linux.

Características del producto

Host Intrusion Prevention proporciona un efectivo firewall final para sistemas Windows y una solución de prevención de intrusiones gestionable y escalable para estaciones de trabajo, portátiles y servidores, incluidos servidores web y de bases de datos, tanto de Windows como de otros sistemas. Bloquea proactivamente el tráfico de red malicioso o no deseado y los ataques tanto conocidos como nuevos mediante una tecnología patentada y galardonada. Hay dos versiones de Host Intrusion Prevention 8.0 disponibles: una versión solo con firewall y una versión completa que incluye firewall y protección IPS.

Capacidad de gestión y de escalado

Host Intrusion Prevention se gestiona por medio de ePolicy Orchestrator, que proporciona y aplica sus directivas junto con otras soluciones fundamentales de seguridad, como la protección antivirus. Este enfoque reduce la cantidad de comunicación entre aplicaciones y proporciona una solución centralizada con una implementación masiva (hasta 100.000 sistemas cliente), en varios idiomas y en la totalidad de una empresa para una cobertura global completa.

Seguridad

Host Intrusion Prevention combina reglas comportamentales, firmas y un sistema de firewall de estado que bloquea ataques y reduce la urgencia de los parches para las nuevas amenazas. El usuario obtiene una protección con la configuración predeterminada, que permite una implementación rápida y a gran escala. Para obtener más protección, puede aplicar directivas predeterminadas o personalizadas más estrictas.

La base de datos de ePO contiene datos de contenido de seguridad, firmas incluidas, que se muestran en las directivas de Host Intrusion Prevention. Las actualizaciones se llevan a cabo mediante un paquete de actualización de contenido que contiene información de la versión y secuencias de comandos de actualización. Al incorporarlo, la versión del paquete se compara con el contenido más reciente de la base de datos. Si el paquete es más nuevo, los datos del contenido se extraen y se almacenan. A continuación, este nuevo contenido se pasa a los clientes en la siguiente comunicación entre el servidor y el agente.

NOTA: Las actualizaciones de contenido de Host Intrusion Prevention se comprueban de forma manual o automática con una tarea de extracción en el repositorio de ePO y, a continuación, se distribuyen entre los clientes con una tarea de actualización. Los clientes de Host Intrusion Prevention únicamente obtienen actualizaciones estableciendo comunicación con el servidor ePO.

Cómo funciona la protección

ePolicy Orchestrator comunica información de directivas a los clientes de Host Intrusion Prevention a intervalos regulares a través del agente de ePO. Los clientes de Host Intrusion Prevention aplican las directivas, recopilan información de eventos y retransmiten la información a ePolicy Orchestrator a través de McAfee Agent.

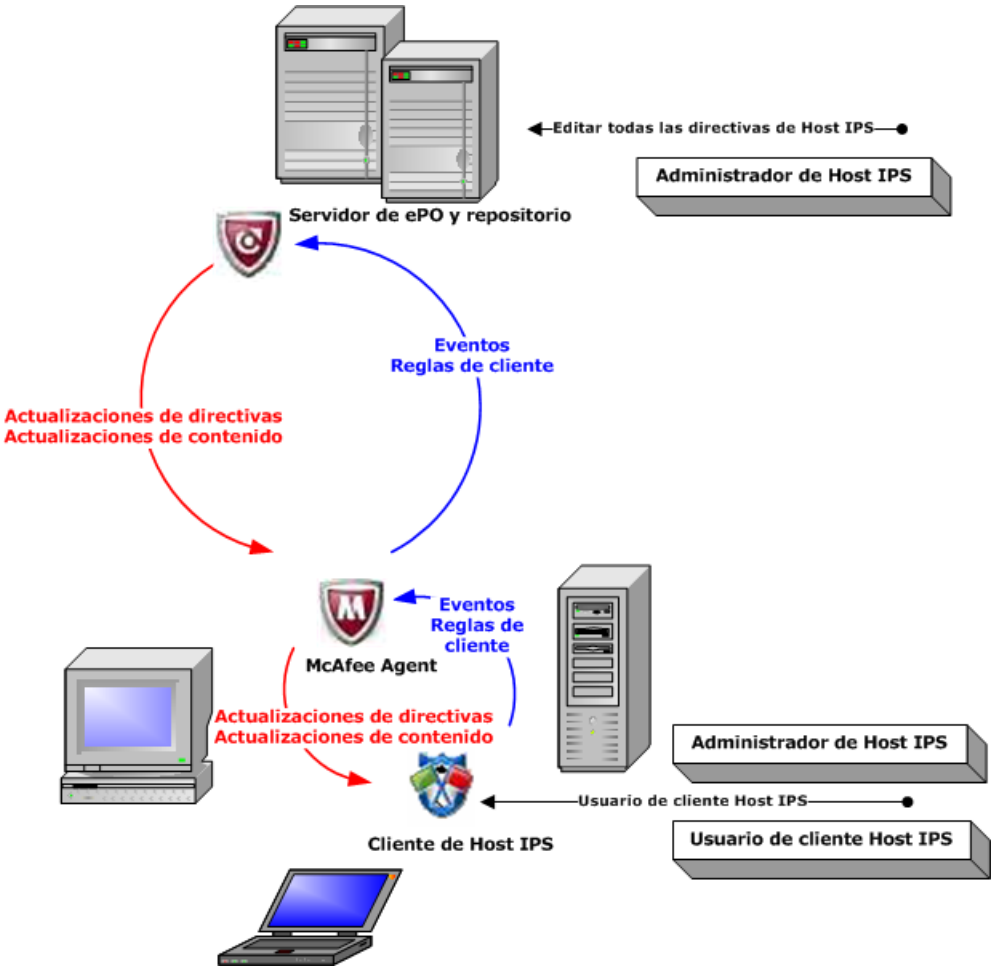

Figura 1: Protección de Host Intrusion Prevention

Contenido

- Componentes
- Introducción a la instalación
- Novedades de esta versión

Componentes

El software de Host Intrusion Prevention requiere instalar y ejecutar varios componentes para que la protección sea efectiva.

Componentes de Host Intrusion Prevention:

- Servidor y repositorio de ePolicy Orchestrator: herramienta de gestión que instala software, implementa directivas, supervisa la actividad, crea informes y almacena y distribuye actualizaciones de contenido y software.
- McAfee Agent: agente instalado en un equipo gestionado que actúa como intermediario entre el cliente de Host Intrusion Prevention y la consola y la base de datos de ePolicy Orchestrator. Envía datos al cliente desde el servidor de ePO y viceversa.
- Extensiones de Host Intrusion Prevention: constituyen la interfaz de gestión de directiva en la consola de ePolicy Orchestrator.
- Cliente de Host Intrusion Prevention: proporciona protección en la estación de trabajo o servidor donde esté instalado.
- Actualizaciones de contenido de Host Intrusion Prevention (solo para protección de IPS): contenido de seguridad actualizado, firmas y aplicaciones de confianza incluidas, entregado en intervalos regulares para mantener actualizada la protección de IPS.

Introducción a la instalación

Host Intrusion Prevention solo se instala en un entorno de ePolicy Orchestrator. Un servidor y una base de datos de ePO deben estar activos y McAfee Agent, instalado en cada sistema cliente en el que quiera instalar Host Intrusion Prevention. Para obtener más detalles acerca de los requisitos y las instrucciones para configurar este entorno de ePO, consulte la *Guía de instalación de ePolicy Orchestrator*.

Con el servidor y los agentes de ePO dispuestos, instale la extensión correcta de Host Intrusion Prevention en ePO. La versión del producto que haya comprado (solo protección de firewall o protección de firewall e IPS) y la versión de ePO que esté usando determinan qué extensiones deben instalarse. Para más información, consulte Instalación en ePolicy Orchestrator.

El último paso es instalar Host Intrusion Prevention en los equipos cliente que ejecuten Windows, Linux o Solaris donde ya se haya instalado una versión de McAfee Agent. Para más información, consulte Instalación del cliente Windows, Instalación del cliente Solaris, o Instalación del cliente Linux.

NOTA: La función Firewall de Host Intrusion Prevention solo es válida en los equipos con Windows.

Debido a los cambios de arquitectura de esta versión, los clientes de Host Intrusion Prevention 8.0 solo se gestionan por medio de la extensión de Host Intrusion Prevention 8.0. Sin embargo, junto con la versión 8.0 de la extensión puede mantenerse también la versión 7.0 y gestionar así las versiones anteriores de cliente hasta que se esté preparado para migrar a la versión 8.0. Para más información, consulte Migración de directivas.

Tabla 1: Versiones de componentes

En el servidor de ePolicy Orchestrator		**En los equipos cliente**		
Versión	**Extensiones de Host IPS 8.0**	**Windows**	**Solaris**	**Linux**
4.0 parche 6 y posteriores	Firewall solo en ePO 4.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Windows	–	–

En el servidor de ePolicy Orchestrator		En los equipos cliente		
Versión	**Extensiones de Host IPS 8.0**	**Windows**	**Solaris**	**Linux**
		• Cliente de Host IPS 8.0		
	Firewall e IPS para ePO 4.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Windows • Cliente de Host IPS 8.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Solaris • Cliente de Host IPS 8.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Linux • Cliente de Host IPS 8.0
4.5	Firewall solo en ePO 4,5	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Windows • Cliente de Host IPS 8.0	–	–
	Firewall e IPS para ePO 4,5	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Windows • Cliente de Host IPS 8.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Solaris • Cliente de Host IPS 8.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Linux • Cliente de Host IPS 8.0
4.6	Firewall solo en ePO 4,6	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Windows • Cliente de Host IPS 8.0	–	–
	Firewall e IPS para ePO 4,6	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Windows • Cliente de Host IPS 8.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Solaris • Cliente de Host IPS 8.0	• McAfee Agent 4.0 (parche 3 y posterior) o McAfee Agent 4.5 (parche 1 y posterior) para Linux • Cliente de Host IPS 8.0

Novedades de esta versión

Esta versión del producto incluye varias características nuevas, mejoras y cambios.

IPS

- Nuevas funciones para la directiva Opciones de IPS:
  - Protección de inicio: Protección de inicio, antes del comienzo de los servicios de IPS
- Nuevas funciones para la directiva Reglas de IPS:
  - Excepciones basadas en la dirección IP o en las firmas de red de IPS
  - Redes de confianza tanto para las firmas de IPS como para las reglas de firewall
  - El emparejamiento de ejecutables para aplicaciones se realiza ahora por ruta, hash, firma digital y descripción del archivo, para firmas y excepciones, en lugar de solo por ruta.

Firewall

- Nuevas funciones para la directiva Opciones de firewall:
  - Clasificación y bloqueo TrustedSource: Las reglas del firewall bloquean o permiten el tráfico de entrada y de salida de acuerdo con las clasificaciones McAfee TrustedSource
  - Protección contra falsificación de IP: Las reglas del firewall bloquean el tráfico de salida cuando la dirección IP local no se corresponde con una de las direcciones IP de los sistemas locales y cuando una dirección MAC local no es una dirección MAC invitada de VM
  - Soporte de puente de VM: Las reglas del firewall permiten el tráfico con una dirección MAC que no sea la dirección MAC del sistema, pero que sea una de las direcciones MAC en el campo del software compatible VM
  - Protección de inicio: Las reglas del firewall bloquean todo el tráfico de entrada antes de que hayan comenzado los servicios del firewall
- Directiva de firewall adicional: Bloqueo DNS del firewall que consta de un conjunto de patrones de nombres de dominio que han de bloquearse. Esta directiva sustituye la regla de dominio que bloqueaba la resolución DNS para ciertos nombres de dominio especificados por el usuario.
- Nuevas funciones para la directiva Reglas de firewall:
  - Las reglas del firewall son mucho más flexibles: ahora, una sola regla puede incluir múltiples acciones (antes solo podía incluir una), múltiples redes (antes solo podía incluir una), una red local y una red remota (antes solo podía incluir una red remota) y un tipo de medios VPN además de los cableados e inalámbricos.
  - Los grupos para conexión ahora son simplemente grupos de firewall que tienen información de ubicaciones y programas, con accesos temporizados para las conexiones asociadas a ellos.
  - El emparejamiento de ejecutables para aplicaciones se realiza ahora por ruta, hash, firma digital y descripción del archivo para reglas y firewall, y no solo por ruta y hash.

General

- Se han eliminado las directivas Opciones de bloqueo de aplicaciones y Reglas de bloqueo de aplicaciones y sus funciones han sido sustituidas por dos firmas de contenido (6010 y 6011) en la directiva Reglas de Host IPS
- Las directivas Opciones de cuarentena del firewall y Reglas de cuarentena se han eliminado, y la opción de cuarentena inicial se ha movido a la opción de protección inicial Opciones del firewall

- Nuevo catálogo de Host IPS Catalog para organizar y activar la reutilización de los componentes de directivas comunes entre directivas, en especial en grupos, ubicaciones, reglas, ejecutables y redes de firewall
- Conjunto de comodines simples estándar que se usan en el producto
- Los registros se ubican en una carpera común, con algunos registros simplificados para facilitar su lectura

Plataformas admitidas

- Igualdad total de funciones en las plataformas Windows de 32 y 64 bits.
- Agregado: compatibilidad con Windows 7; Linux SUSe10 SP3, SUSe 11 y Solaris Zone
- Eliminado: Windows 2000, Solaris 8 y SUSe Linux 9

Compatibilidad SQL

- Agregado: SQL 2005, SQL 2008
- Eliminado: SQL 2000

Funcionalidad de extensión/cliente

- Dos versiones de Host Intrusion Prevention 8.0: una versión solo con firewall y una versión completa que incluye firewall y protección IPS
- Compatibilidad de extensiones de Host IPS con las versiones 4.0, 4.5 y 4.6 de ePolicy Orchestrator
- Capacidad para instalar la extensión de Host IPS 8.0 en ePolicy Orchestrator incluso con versiones previas de Host IPS instaladas
- La extensión de Host IPS 8.0 solo gestiona los clientes de Host IPS 8.0, no es compatible con versiones anteriores de los clientes
- Tanto la protección de IPS como de firewall se desactiva en el cliente después de la instalación inicial y necesita de la aplicación de una directiva para activarla
- En todas las plataformas, la actualización de la versión de evaluación a una versión con licencia de ePolicy Orchestrator puede realizarse sin reiniciar el cliente

Recomendaciones para un éxito rápido

McAfee Host Intrusion Prevention ofrece un gran valor a su empresa mediante la reducción de la frecuencia y la urgencia de la aplicación de parches, la conservación de la continuidad de los negocios y la productividad de los empleados, la protección de la confidencialidad de los datos y el cumplimiento de las normas regulatorias. Ofrece protección mediante un sistema de prevención de intrusiones de firma y comportamentales (IPS) y un firewall de control con estados para proteger todos los puntos finales (equipos de sobremesa, portátiles y servidores) de amenazas conocidas y desconocidas.

Introducción

Cualquier elemento que influya en los usuarios finales y las aplicaciones fundamentales para el negocio debe implementarse con cuidado a fin de evitar alteraciones en la actividad comercial. Aquí presentamos un resumen del desarrollo del producto reducido en etapas pequeñas y manejables, que aumentan con cuidado los niveles de protección, permiten el ajuste de directivas para que sean compatibles con los matices del negocio y minimicen los cambios de los usuarios. Este procedimiento, lento pero seguro, proporciona el máximo de protección con el mínimo de esfuerzo administrativo, con un tiempo estimado de entre uno y tres meses.

Si ha adquirido tanto protección de IPS como mediante firewall, recomendamos que empiece con la función IPS, a no ser que ciertas razones regulatorias o de riesgo conviertan al firewall en su primera opción. La función IPS ofrece protección fundamental y universal contra amenazas conocidas y nuevas. Con la configuración de directivas predefinida de McAfee y una pequeña inversión de su tiempo, conseguirá que McAfee Host Intrusion Prevention comience a proteger sus sistemas contra ataques y vulnerabilidades.

Si ha activado con éxito la protección de IPS, podrá comenzar a centrarse en la activación del firewall con confianza. La estrategia de seguimiento que se describe aquí puede aplicarse al desarrollo del firewall, aunque las directivas específicas, las respuestas de reacción y las reglas pueden variar.

NOTA: Si solo ha adquirido la protección con firewall, o si prefiere comenzar con la implementación de un firewall, use la estrategia que se describe aquí, pero consulte la guía del producto o la ayuda para obtener detalles acerca de la definición y la activación de directivas de firewall. La clave es desarrollar el sistema en etapas, así que recomendamos este orden:

- IPS en portátiles y equipos de sobremesa normales
- IPS en servidores fundamentales
- IPS en equipos de sobremesa de usuarios con permisos
- Firewall en portátiles
- Firewall en servidores
- Firewall en equipos de sobremesa de usuarios con permisos

La mayoría de los administradores puede realizar los pasos enumerados aquí. En caso necesario, los socios y los profesionales de asistencia de McAfee pueden ayudarle.

La secuencia recomendada consta de siete pasos:

1 Estrategia y planificación
2 Preparación del entorno
3 Instalación y configuración
4 Ajustes iniciales
5 Modo Adaptación opcional
6 Mejora de la protección y ajustes avanzados
7 Mantenimiento y expansión más allá de IPS

Tanto los equipos de sobremesa como los servidores siguen un proceso de implementación similar. Sin embargo, recomendamos temporizaciones de fase y protección de puntos de inicio, más conservadores, para sus servidores y equipos de sobremesa más importantes de usuarios con permisos.

Tiempos y expectativas

Para una implementación con éxito (frustración mínima, mitigación máxima del riesgo), el proceso de adopción puede llevar de uno a tres meses. El trabajo directo solo lleva un par de días durante este periodo, pero debe pasar tiempo entre las etapas, para que el producto pueda recopilar datos de uso que ayuden al ajuste.

La variable más grande de la implementación es la gama de sistemas y de perfiles de usuario en su lugar de trabajo. Cuanto más variada sea la población de usuarios, más tiempo se tardará en implementar McAfee Host Intrusion Prevention en todos los sistemas seleccionados. Debe activar las protecciones sin mermar la productividad de los usuarios y las funciones de las aplicaciones. Cada sistema significativo y perfil de usuario merecen un ajuste y una prueba.

Muchos entornos necesitan de la aprobación de la gestión de IT para la implementación, la migración al modo bloqueo y el uso del firewall. Considere algo de tiempo adicional para estas aprobaciones.

NOTA: Para obtener más detalles sobre cualquier aspecto de este proceso, consulte la Ayuda o la *Guía del producto de McAfee Host Intrusion Prevention 8.0*.

Tabla 2: Posibles fallos y soluciones

Cosas que no hay que hacer	Recomendaciones
Bloquee las firmas de gravedad media y alta sin obtener primero información del inicio de sesión.	Bloquee primero las firmas de gravedad alta. Este nivel solo protege contra las vulnerabilidades más importantes, pero genera pocos eventos falsos. Las firmas de nivel medio se basan en comportamientos y, por lo tanto, a menudo necesitan algunos ajustes para limitar las llamadas a la asistencia técnica.
Asuma que todos los sistemas usarán las mismas directivas.	Separe los equipos de sobremesa para que reflejen las aplicaciones y los privilegios. Comience con los sistemas más simples y cree perfiles de uso estándar para los grupos principales. A medida que conozca los equipos, agregue más usuarios y más perfiles de uso.
Realice pocas pruebas en la experiencia de usuario.	Tome algunos grupos de usuarios importantes, realice el seguimiento con los usuarios importantes que se comprometan a proporcionar opiniones, compruebe que las aplicaciones aún funcionan correctamente y, después, implemente las directivas cuando se demuestre que funcionan sin interferir en la productividad. Es necesario que la primera impresión de los usuarios sea positiva.
Trate el IPS del host como "configurar y olvidar".	A diferencia de lo que sucede con los antivirus, el seguimiento y mantenimiento regular son necesarios para mantener la precisión y la efectividad de la protección.

Cosas que no hay que hacer	Recomendaciones
	Disponga de tiempo para revisar los registros y actualizar las reglas una vez al mes, una vez que complete la implementación.
Encienda IPS y el firewall simultáneamente.	Comience con IPS y después agregue el firewall si es necesario. Sabrá cómo crear directivas y familiarizarse con los tipos de protección que sean apropiados, y podrá relacionar los cambios con los resultados con más facilidad.
Deje las funciones IPS del host o firewall en modo Adaptación de manera indefinida.	Use el modo Adaptación durante periodos breves de tiempo, cuando tenga tiempo de realizar el seguimiento de las reglas que haya creado.
Bloquee inmediatamente cualquier cosa que el sistema detecte como una intrusión.	Tómese algo de tiempo para comprobar que el tráfico que ve es, sin duda, malicioso. Use capturas de paquetes, IPS de red o cualquier medio del que disponga.

- 1. Creación de estrategias
- 2. Preparar un entorno de seguimiento
- 3. Instalación y configuración
- 4. Realizar el ajuste inicial
- 5. Activar modo Adaptación (opcional)
- 6. Ajustes
- 7. Realizar tareas de mantenimiento y expansión

1. Creación de estrategias

El primer paso del proceso de ajuste es meditar su estrategia de protección de sistemas. Propóngase objetivos realistas y cree un plan de implementación y seguimiento al que ajustarse.

Defina las prioridades del seguimiento

Asegúrese de que entiende sus objetivos de seguridad y cree un proceso de seguimiento acorde. Podrá identificar algunos problemas específicos que podrá bloquear inmediatamente, o permitir un periodo de seguimiento general para obtener más información sobre lo que ocurre en la comunidad del cliente. Cada organización elige un equilibrio distinto entre protección y productividad. Tener las prioridades claras al principio simplifica el proceso.

Hágase las siguientes preguntas:

- ¿Cuáles son las áreas de exposición de seguridad específicas o cuáles son los últimos incidentes acaecidos en las auditorías?
- ¿Qué sistemas son más vulnerables?
- ¿Los equipos portátiles son una prioridad?
- ¿Las regulaciones implican que debo reducir las vulnerabilidades en una comunidad de usuarios clave o grupo de sistemas?

Para muchos clientes, las vulnerabilidades más importantes se dan en los portátiles que salen del entorno controlado de la empresa. Estos sistemas son un primer objetivo excelente para IPS. Algunos clientes prefieren aumentar las protecciones de los servidores clave. Sugerimos que estos sistemas, fundamentales para las empresas, se sigan con un ritmo más conservador. Escriba sus objetivos clave y emplee los siguientes pasos para establecer prioridades.

Defina el entorno de seguimiento

Elija un conjunto pequeño de sistemas de seguimiento en los que ejecutar las pruebas de implementación. Si selecciona menos de 100 nodos en tres subredes, podrá incrementar la implementación gradualmente, partiendo de niveles de protección muy conservadores. Una expansión paso a paso le permitirá gestionar con facilidad todos los problemas que surjan.

Diferencie entre las clases principales de sistemas e inclúyalos de manera selectiva en su seguimiento. Host IPS es compatible, empezando desde la menor complejidad de implementación, con:

- Equipos de sobremesa o portátiles estándar en los que los usuarios generales no tienen permisos administrativos para instalar o eliminar aplicaciones. Puede crear múltiples perfiles de usuario, cada uno con un entorno de aplicación estándar definido.
- Equipos de sobremesa o portátiles personalizados de usuarios con permisos, en los que los usuarios especializados tienen privilegios administrativos para instalar sus propias aplicaciones. Los usuarios con permisos suelen ser administradores y desarrolladores de software. A veces, los privilegios administrativos aparecen como un artefacto de la empresa. Idealmente, sería necesario eliminar estos privilegios de cualquier sistema que no requiera control administrativo para reducir el grupo de tipos de sistemas que deben perfilarse y ajustarse.
- Servidores que ejecutan bases de datos específicas, aplicaciones de correo electrónico, de Internet u otras aplicaciones, así como servidores de archivos y de impresión.

¿Laboratorio o mundo real?

Muchas empresas exigen pruebas de laboratorio como paso estándar en la instalación de nuevos productos. Hacen copias de los sistemas de producción y prueban estas copias en un entorno controlado antes de la implementación.

Con McAfee Host Intrusion Prevention, este acercamiento proporciona las primeras líneas de base de reglas, pero es menos efectivo en general, porque ignora la variable del usuario. Los analizadores intentan imitar la conducta del usuario de manera artificial, así que resulta difícil capturar detalles auténticos en actividades legítimas. Los usuarios y el software malintencionado a menudo generan eventos con los que hay que enfrentarse inmediatamente o escapan a la detección, si se permiten como una excepción de un comportamiento normal. Estos resultados consumen tiempo y pueden crear problemas posteriormente.

La mayoría del aprendizaje tiene lugar con sistemas activos en un entorno de producción. Las mejores pruebas de producción emplean sistemas elegidos a dedo y a usuarios objetivo que realizan tareas habituales. Este acercamiento proporciona la línea de base más fiable, porque son los usuarios reales los que manejan sus sistemas y aplicaciones. Pueden proporcionar opiniones inmediatas sobre el impacto de los cambios.

Una buena opción es combinar los dos modelos. Un periodo de pruebas de laboratorio puede aumentar la confianza y ayuda a que se familiarice con los procesos y las directivas de McAfee Host Intrusion Prevention. Después de haber probado algunos perfiles de uso, éstos pueden trasladarse a un equipo de seguimiento de los sistemas de producción. Cualquier actividad o aplicación que se haya obviado en la prueba de laboratorio puede detectarse en el seguimiento de producción. Este proceso de dos pasos es el adecuado para las organizaciones muy conservadoras.

SUGERENCIA: Los administradores deben poder acceder físicamente con facilidad a los sistemas de seguimiento lo que, por lo general, elimina las oficinas sin personal y los teletrabajadores.

Asegure que los usuarios estén adecuadamente representados.

Una vez entienda los tipos de sistema, lo siguiente que debe hacer es identificar los perfiles de uso y los sistemas de seguimiento. Incluya distintos tipos de usuario de varias secciones de su comunidad de usuarios objetivo. Esta amplitud le ayudará a crear reglas y directivas que reflejen las necesidades empresariales normales y sus usos. Por ejemplo, en un centro de atención o de asistencia estándar, tendrá gestores y encargados de asistencia de primera y de segunda línea. Asegúrese de incluir, al menos, un elemento de cada uno de los perfiles de uso para que McAfee Host Intrusion Prevention pruebe y establezca directivas para todo el espectro de uso.

Estrategia de implementación, opción 1: Empiece por lo fácil

Para implementar rápidamente las protecciones iniciales y permitir una curva de aprendizaje adecuada para las protecciones más avanzadas, sugerimos activar las protecciones básicas en los equipos de sobremesa y portátiles estándar, junto con la activación de registros en los servidores y equipos de sobremesa de los usuarios con permisos.

En primer lugar, active la protección mediante la aplicación de la directiva **Opciones de IPS** con la protección de IPS seleccionada y, a continuación, aplique la directiva básica **Reglas de IPS predeterminadas de McAfee**. Esta directiva bloquea las actividades que inician firmas de gravedad altas, no necesita de ajustes y genera pocos eventos. Su configuración incluye:

- Se bloquean las actividades que inician firmas de gravedad alta y se ignoran las demás firmas.
- Las aplicaciones de McAfee se enumeran como aplicaciones de confianza para todas las reglas, excepto para las reglas de protección automática de IPS. Como aplicaciones de confianza, funcionan sin generar eventos de excepciones.
- Se protegen las aplicaciones y los procesos predefinidos.

Aunque las marcas y los modelos de los equipos difieren, pueden encuadrarse en un conjunto de variaciones relativamente reducido. Una amplia experiencia permite que la función IPS cubra los problemas de gravedad alta con gran precisión. Por ejemplo, McAfee ha demostrado que más del 90 por ciento de los problemas de Microsoft con los "Martes de parches" se evitaron usando el nivel de protección básico que viene con el programa. Incluso mediante la activación de la protección predeterminada se consiguen importantes valores.

Recomendamos encarecidamente que se siga esta estrategia de comenzar por lo más fácil. Puede que los servidores sean los sistemas más importantes que proteger, pero también son los más difíciles. Necesitan más atención durante la implementación, ya que las reglas de IPS deben ajustarse inevitablemente para legitimar las operaciones de aplicaciones legítimas y reflejar el rendimiento cuidadoso y la optimización del sistema de la mayoría de los servidores. El ajuste de reglas mediante ensayo y error puede ser peligroso en sistemas activos que sean básicos para el funcionamiento.

De la misma manera, los sistemas de los usuarios con permisos tienden a tener un conjunto de aplicaciones distintos y privilegios especiales, como el derecho de ejecutar líneas de comandos. La activación de IPS puede generar un gran número de eventos que se deben revisar con cuidado para asegurar permisos o bloqueos adecuados. Los usuarios con permisos y los servidores necesitan de más tiempo para conocer los usos legítimos.

Supervisión y creación de informes

A medida que crece la confianza durante las pruebas, puede trasladar las firmas del simple registro a la aplicación por clases de sistema, ajustando las reglas y refinando las directivas a medida que aprenda cuáles son las actividades legítimas. Describiremos este proceso más adelante en esta guía.

Al activar la protección básica en sus sistemas de sobremesa estándar, también puede iniciar la creación de informes sobre problemas de gravedad media en dichos sistemas. Esta supervisión le ayudará a descubrir otros eventos que IPS indica cuando comience a cerrar más los controles. En el modo de creación de informes, puede ver el volumen de uso así como los tipos de uso, así que puede aprender mucho sobre el comportamiento del sistema. Recomendamos la creación de informes en esta primera fase para evitar sorpresas o interrupciones del trabajo. Es una buena idea crear registros de los eventos durante todo un periodo empresarial (al menos un mes y, a ser posible, un trimeste) para ver toda la variedad de aplicaciones y actividades. Use la directiva **Preparación para protección mejorada** para hacerlo automáticamente. Esta configuración evita las firmas de gravedad alta y de gravedad media de registro, pero ignora el resto.

Para los demás sistemas, servidores y equipos de usuarios con permisos, establezca la supervisión y la creación de registros para niveles de gravedad media y alta. No hay ninguna configuración predeterminada que registre tanto los niveles medios como los altos, así que habrá que duplicar la directiva existente y personalizarla. Observar solo los eventos de gravedad media y alta proporciona un buen nivel de información relevante sin agobiarle con los detalles. Descubrirá variaciones de sistema en las que los servidores están ajustados según ejemplos específicos de aplicaciones o en los que los desarrolladores tengan sus herramientas preferidas o sus compiladores arcanos.

SUGERENCIA: La activación de la supervisión y de la creación de registros no afectará a las operaciones del sistema o de las aplicaciones, pero siempre está bien supervisar los sistemas de cerca cuando se instala McAfee Host Intrusion Prevention, incluso si es solo para crear registros. Como el producto funciona por interacciones de nivel bajo con aplicaciones y sistemas operativos, siempre es posible que afecte al rendimiento de algunas aplicaciones.

Planear la expansión

A medida que crece la confianza durante las pruebas, puede trasladar las firmas del simple registro a la aplicación por clases de sistema, ajustando las reglas y refinando las directivas a medida que aprenda cuáles son las actividades legítimas. Describiremos este proceso más adelante en esta guía.

Estrategia de implementación, opción 2: Uso de directivas predeterminadas

Para algunos entornos, un acercamiento legítimo puede ser aprovechar la experiencia de McAfee que se proporciona en la configuración predeterminada e implementar el perfil de protección básica en todos los sistemas. Este acercamiento funciona bien para los usuarios que buscan la protección clave de IPS sin demasiados ajustes ni esfuerzos. Si la razón principal de la compra del producto no es IPS, esta estrategia proporciona una implementación con un mínimo esfuerzo que activa una protección inmediata contra los ataques grandes.

Seleccione su opción

La opción 1 le ayuda a obtener más ventajas de la protección que ofrece su inversión en IPS. La opción 2 presenta una estrategia sencilla y de confianza. Elija la estrategia que mejor se adapte a los riesgos que espera.

2. Preparar un entorno de seguimiento

Después de haber definido las prioridades, los objetivos y la estrategia de protección, debe asegurarse de que el entorno cumpla con los requisitos técnicos previos y eliminar cualquier

problema de sistema antes de la instalación. Esta preparación le permitirá centrarse en la implementación de IPS y evitar problemas potenciales no relacionados con esta función.

Instalar o actualizar McAfee ePolicy Orchestrator y McAfee Agent

Antes de instalar McAfee Host Intrusion Prevention, debe haber instalado el servidor de ePolicy Orchestrator y debe instalar McAfee Agent en los hosts objetivo.

Necesitará entender la implementación de directivas con ePolicy Orchestrator para adoptar McAfee Host Intrusion Prevention de forma correcta. Si no está familiarizado con la creación de directivas con ePolicy Orchestrator, consulte la documentación de ePolicy Orchestrator.

¿Por qué ePolicy Orchestrator?

McAfee Host Intrusion Prevention necesita ePolicy Orchestrator porque su implementación se basa en directivas específicas de la empresa y en reglas que se ajustan de forma rutinaria a medida que cambian las comunidades de usuarios y los negocios. McAfee Host Intrusion Prevention aprovecha la infraestructura demostrada de ePolicy Orchestrator, que aumenta la consistencia de la aplicación de directivas, disminuye los errores y mejora la visibilidad y el control de los administradores.

Descripción del proceso:

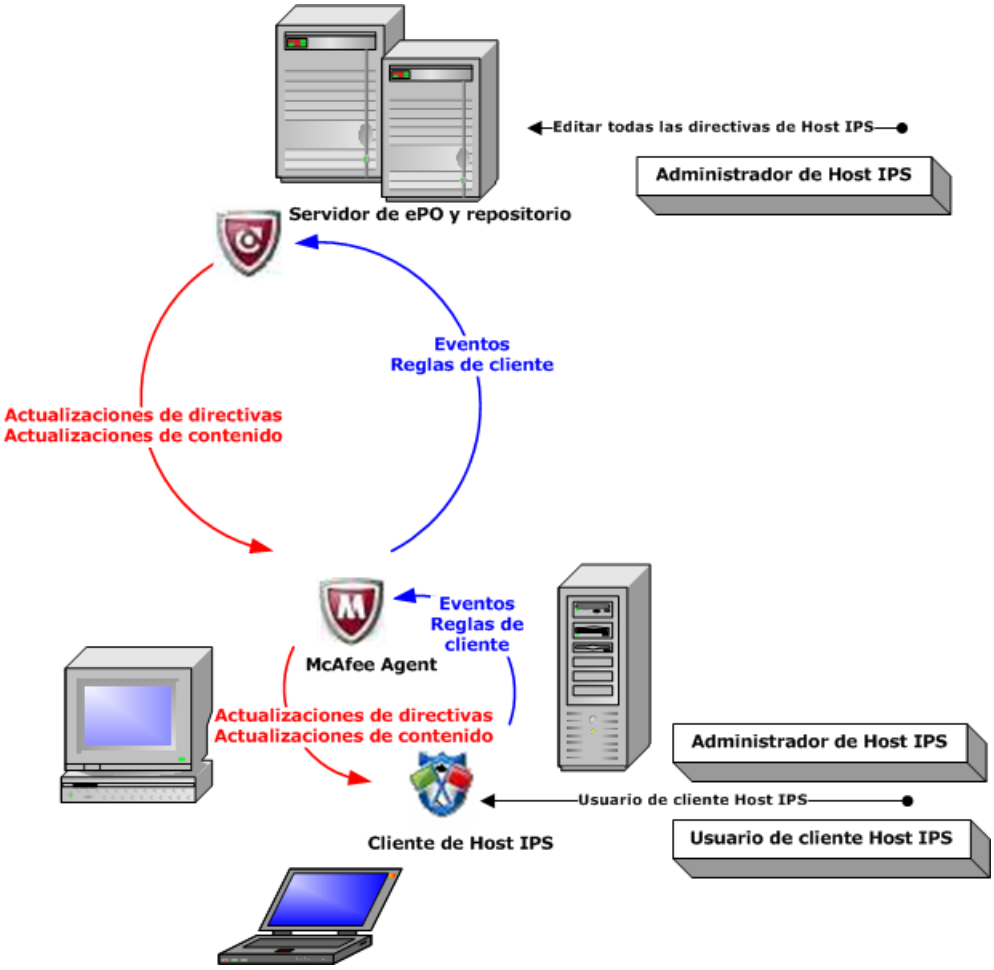

Figura 2: Instalación y mantenimiento de Host Intrusion Prevention con ePolicy Orchestrator

- El servidor de ePO funciona con McAfee Agent en cada host para instalar el cliente de IPS en cada sistema objetivo.

- Las directivas de IPS se crean y mantienen en la consola ePO.
- El servidor de ePO comunica las directivas al agente del sistema host.
- El agente comunica las directivas al cliente de IPS.
- El cliente de IPS aplica las directivas y genera información de eventos, que manda al agente.
- El agente transmite la información del evento a ePolicy Orchestrator.
- Según intervalos programados, o cuando se requiera, el servidor de ePO toma actualizaciones de contenido y de funcionamiento del repositorio de McAfee y el agente los toma del servidor para actualizar el cliente de IPS.
- A medida que cambian las directivas, el agente las toma para actualizar el cliente de IPS.

Use el servidor de ePO para establecer clientes y perfiles de uso.

Para cada tipo distinto de uso (servidores web, portátiles, quioscos), cree un perfil de uso de ePO distinto. Después podrá asociar estos perfiles con las directivas específicas de IPS, y será útil tener los perfiles ya establecidos a la hora de gestionar excepciones.

Agrupe los clientes de forma lógica. Los clientes se pueden agrupar según cualquier criterio que se ajuste a la jerarquía del árbol del sistema de ePO. Por ejemplo, puede agrupar el primer nivel por ubicación geográfica y el segundo nivel por sistema operativo o dirección IP. Se recomienda agrupar los clientes en función de criterios de configuración de Host Intrusion Prevention, incluidos el tipo de sistema (servidor o equipo de escritorio), el uso de aplicaciones principales (web, base de datos o servidor de correo) y ubicaciones estratégicas (DMZ o Intranet).

SUGERENCIA: El servidor de ePO permite el etiquetado lógico de los sistemas. Las etiquetas son indicadores que se pueden asignar a sistemas de forma automática o manual. Agrupe los sistemas en grupos de seguimiento según sus etiquetas y use las etiquetas para criterios de informes.

Las convenciones a la hora de poner nombres son importantes. Lo ideal es establecer una convención para poner nombres que resulte fácil de interpretar para todo el mundo. Los clientes se identifican por su nombre en el árbol del sistema, en ciertos informes y en datos de eventos generados por las actividades del cliente.

Compruebe la salud de los sistemas de seguimiento.

Ahora que ha identificado los clientes, asegúrese de que no hay problemas ya existentes en los sistemas que podrían alterar la implementación. Examine los archivos de registro relevantes del servidor de ePO, así como los registros de eventos del sistema. Busque errores o fallos que indiquen una configuración no adecuada y anomalías del sistema que deberían solucionarse antes de la instalación de McAfee Host Intrusion Prevention. Los siguientes son algunos elementos clave que buscar:

- **Niveles de parche**: ¿están actualizados todos los controladores y las aplicaciones? Reproductores multimedia o de audio antiguos, Internet Explorer y los controladores de tarjetas de red suelen crear inconsistencias que causan errores en la implementación. Aplique los últimos parches y soluciones de emergencia.
- **Software incompatible**: ¿se ejecutan otras aplicaciones de detección de intrusiones o de firewall en el host? Debería desactivarlas o eliminarlas.
- **Acceso administrativo**: debe tener acceso administrativo al sistema. Compruebe también si el usuario tiene acceso administrativo. ¿Por qué? Los usuarios pueden interrumpir el proceso de prueba si instalan una aplicación nueva durante las pruebas. Considere poner este sistema en un perfil de uso distinto, como usuario con permisos, si no puede eliminar el acceso administrativo de los usuarios.

- **Consideraciones organizativas**: algunos sistemas necesitan atención especial porque usan un idioma distinto, son aplicaciones específicas de ciertas ubicaciones o son aplicaciones internas. Considere reservar estos sistemas hasta la segunda fase de la implementación, o excluir las aplicaciones especializadas de la protección de IPS hasta que tenga tiempo de registrar y analizar sus comportamientos.

3. Instalación y configuración

En el servidor de ePO, instale la extensión Host IPS que le permite comunicarse con la gestión de directivas de Host IPS. Importe el cliente de Host IPS en el repositorio de ePO.

Busque parches o artículos de Knowledge Base en McAfee Service Portal (https://mysupport.mcafee.com/Eservice/Default.aspx). Descargue el contenido actualizado de http://www.mcafee.com/us/downloads/.

Establecer los niveles de protección iniciales y las respuestas

Defina o asocie los niveles de protección con cada perfil de uso. Si va a seguir una estrategia de "primero lo más simple", active la protección básica para los perfiles de uso estándar de equipos de sobremesa. Consulte *Configurar directivas de IPS* o *Configurar directivas de firewall* en la guía del producto para obtener más detalles.

Refinar las directivas de líneas de base (opcional)

Algunos administradores cambian los valores predeterminados de las directivas inmediatamente, antes de iniciar la implementación. Puede proteger automáticamente las aplicaciones de alto riesgo (las que se inician como servicios en puertos abiertos a la red) y las aplicaciones internas. Las aplicaciones desarrolladas internamente, a menudo, se excluyen de IPS al inicio de una implementación, especialmente si se comunican por medio de conexiones de red. Los desarrolladores de software internos puede que no sean tan rigurosos como los desarrolladores comerciales al programar comportamientos esperados y seguros. Por ejemplo, un programa que enlace con Internet Explorer puede iniciar, de forma inadvertida, una firma de protección de Internet Explorer, si el programa se comporta de manera no adecuada. Dado que las aplicaciones desarrolladas internamente no son objetivos normales de ataques, presentan menos riesgos de aprovechamiento.

Considere agregar las direcciones de IP de sus análisis de vulnerabilidad a su lista de redes de confianza. Las directivas de ePolicy Orchestrator y de seguridad pueden proporcionar indicios adicionales acerca de actividades que bloquear o que permitir para perfiles de uso concretos. Finalmente, puede usar el modo Adaptación para definir reglas de manera selectiva para aplicaciones excluidas, y para implementar la protección. Este paso puede realizarse cuando haya establecido protecciones de línea de base y esté cómodo con las firmas y directivas de IPS.

Notificar a los usuarios y planear anulaciones

Antes de la activación de la protección IPS, notifique a los usuarios que van a recibir una protección nueva y que pueden anular el sistema en ciertos casos. Esta comunicación reducirá el riesgo percibido para la productividad de usuario, lo que es especialmente importante para los usuarios con portátiles que se desplacen mucho. Para que el usuario anule los bloqueos de IPS, el administrador debe proporcionar a los usuarios lo siguiente:

- Una contraseña de tiempo limitado.
- Instrucciones acerca de cómo desactivar las características.

- Capacidad para eliminar Host IPS si es necesario.

No ofrezca estos atajos de forma demasiado liberal: no conviene que los usuarios acaben evitando la implementación. Dos de ellos se eliminarán más adelante en el seguimiento. Consulte *Definir funciones del cliente* en la guía del producto para obtener más detalles.

Implique al equipo del departamento de asistencia

Comunique a su departamento de asistencia que va a activar Host IPS. Aunque debería haber pocos problemas, el departamento de asistencia deberá estar preparado para reconocer los síntomas que puedan presentarse al activar la protección IPS.

Instalar Host IPS en hosts de seguimiento

Empiece con poco, instalando solo algunos clientes, y después amplíe a más sistemas en incrementos más amplios, a medida que crezca la confianza. Comience con uno y después pase a 10, 20, 50 y hasta 100 sistemas. Ésta es la secuencia de implemenación:

1. Asegúrese de que los hosts seleccionados reciben alimentación, están conectados a la red y se comunican con ePolicy Orchestrator.
2. Use una tarea de implementación de ePO para que los agentes de Host IPS entren en una serie de hosts dentro del grupo de seguimiento.
3. Compruebe que la instalación haya tenido éxito. Solucione los problemas y haga los ajustes que sean necesarios.
4. Expanda la instalación a más sistemas.

A medida que la instalación progresa, compruebe los sistemas de seguimiento y su funcionamiento adecuado y supervise los registros de ePO para eventos de servidor y para cualquier efecto importante que tengan en el rendimiento de red. Pueden surgir algunos problemas. Por eso es tan importante el seguimiento y la lentitud en la implementación. Haga lo siguiente:

1. Compruebe que los servicios de Host IPS (FireSvc.exe, mfefire.exe, mfevtp.exe) y los servicios de marco (McAfeeFramework.exe) se hayan iniciado.
2. Muy importante: ejecute aplicaciones simples, como la contabilidad, edición de documentos, correo electrónico, acceso a Internet, aplicaciones multimedia o herramientas de desarrollo para comprobar que funcionan correctamente. ¿Podrán los usuarios realizar sus trabajos normalmente? Lo que intenta es demostrar y comprobar la detección operacional adecuada.
3. Si ve problemas en el cliente, puede examinar los registros del cliente de IPS y los registros de sistemas operativos del cliente para buscar errores. Consulte *Trabajo con clientes de Host Intrusion Prevention* en la guía del producto.
4. Repita estos pasos para expandir la instalación a más sistemas, hasta que haya poblado el grupo de seguimiento.

SUGERENCIA: Recuerde hacer pruebas tras cada instalación o cambio de directiva para asegurar que los usuarios finales puedan hacer con éxito sus trabajos. Estas pruebas pueden ser las actividades más importantes a la hora de asegurar una implementación con éxito.

4. Realizar el ajuste inicial

Cuando su grupo de seguimiento esté preparado y en funcionamiento, es el momento de esperar y observar. Deje de dos a siete días para que se acumulen los eventos y esté preparado para responder a cualquier llamada de asistencia.

Supervisión diaria

Deje un par de minutos cada día para revisar los registros de eventos de IPS y realizar el seguimiento de los volúmenes y tipos de actividad. Este hábito le ayudará a conseguir una línea de base de los niveles normales de funcionamiento y de los patrones de actividades. Por ejemplo, durante la supervisión diaria, debería observar los procesos normales y los niveles de actividad de mantenimiento de servidores y actualizaciones de aplicaciones. Con el conocimiento de estas actividades, reconocerá inmediatamente cualquier actividad inusual que se dé.

Sus revisiones diarias deben ayudar a refinar reglas, directivas y excepciones a medida que ocurran nuevos eventos. Host IPS proporciona un control muy minucioso, ya que puede supervisar todas las llamadas de sistemas y de API y bloquear aquellas que puedan ser maliciosas. Igual que en un sistema de red de IPS, de vez en cuando se hace necesario ajustar las reglas adicionales a medida que cambian las aplicaciones, las necesidades empresariales y los requisitos de directivas.

El mantenimiento continuo de la implementación de IPS incluye la supervisión, el análisis y la reacción a actividades; cambiar y actualizar directivas, y realizar tareas de sistema, como la definición de permisos de usuario, de tareas de servidor, de notificaciones y de actualizaciones de contenido. Es necesario presupuestar estas actividades en un nivel operacional para mantener la salud y la efectividad de las funciones de IPS.

Revisar los registros

Los registros de eventos pueden ayudarle a refinar directivas para equilibrar la protección y la libertad de acceso a informaciones y aplicaciones. A menudo, este equilibrio es distinto para cada tipo de usuario. Llegados a esta etapa, debería ajustar las directivas a mano por medio del servidor de ePO. Para más información sobre ajuste automático de directivas, consulte 5. Activar modo Adaptación (opcional).

Es posible acceder a la información del evento desde la ficha **Host IPS 8.0 | Eventos**, dentro de **Informes**, en el servidor de ePO. Puede analizar los detalles de un evento, incluso es posible saber qué procesos iniciaron el evento, cuándo se generó el evento y qué cliente lo ha generado. Deberá buscar banderas rojas, como falsos positivos o firmas de gravedad alta.

Compruebe que los procesos y servicios sean correctos. Las aplicaciones que espere que se ejecuten se deberían estar ejecutando, mientras que las que no espera no deberían aparecer. Si ve eventos registrados basados en actividades legítimas (se suelen dar con aplicaciones internas), puede resolver estos falsos positivos en el siguiente paso.

SUGERENCIA: A menudo, al analizar datos de registro repetitivos, pueden pasarse por alto especificaciones que iniciarían una decisión de regla diferente. Si va a hacer una revisión exhaustiva, descanse cada cierto tiempo para evitar estas situaciones.

Comenzar el ajuste de la protección

Desde los datos de registro de evento, puede trabajar para lo siguiente:

- Elevar la protección para los eventos registrados que deban bloquearse.
- Eliminar los falsos positivos basados en actividades empresariales legítimas.

Comience haciendo lo siguiente:

1 **Editar reacciones para firmas**. No olvide que un cliente puede reaccionar de tres maneras distintas:
   - **Ignorar**: no hay reacción. El evento no se registra y el proceso no se previene.
   - **Registrar**: el evento se registra y el proceso no se previene.
   - **Prevenir**: el evento se registra y el proceso se previene.

Aplique la reacción Prevención a cualquier firma de gravedad alta.

2 **Crear excepciones**. Identifique los eventos que indiquen comportamientos legítimos que deberían permitirse o, tal vez, que deberían permitirse y registrarse.

   Las reglas de excepción anulan una directiva de seguridad en circunstancias específicas. Puede establecer una respuesta de reacción para ignorar, y los eventos dejarán de registrarse. Por ejemplo, aunque una directiva estime que cierta secuencia de comandos sea ilegal, algunos sistemas de sus grupos pueden necesitar ejecutarla. Cree excepciones para que estos sistemas puedan funcionar con normalidad, mientras la directiva sigue evitando secuencias de comandos en otros sistemas. Haga que estas excepciones formen parte de una directiva de servidor que cubra solo los sistemas donde se permite.

   Las excepciones le permiten reducir las alertas de falsos positivos y minimizan el flujo de datos innecesarios e irrelevantes a su consola. Al reducir el ruido, identificará con más facilidad los eventos importantes en su supervisión diaria.

   SUGERENCIA: Haga que la excepción sea lo suficientemente genérica para que funcione en todos los sistemas similares con las mismas circunstancias, o similares.

3 **Crear aplicaciones de confianza**.

   Las aplicaciones de confianza son procesos de aplicaciones que están exentos de las reglas de IPS y de firewall. Limite las aplicaciones de confianza para procesos que causen tantos falsos positivos que sea imposible crear excepciones bien ajustadas. Las aplicaciones de confianza pueden variar según el perfil de uso. Por ejemplo, puede permitir ciertas aplicaciones de software en su organización de asistencia técnica, pero evitar que se usen en su departamento de finanzas; por lo tanto, puede configurar estas aplicaciones como de confianza en los sistemas de la asistencia técnica para permitir este uso. Consulte *Configurar una directiva de aplicaciones de confianza* en la guía del producto para obtener más detalles.

4 **Realizar consultas**

   Use las consultas para obtener datos acerca de un elemento particular y filtre los datos para subconjuntos específicos de dichos datos. Por ejemplo, eventos de alto nivel informados desde clientes particulares durante un periodo de tiempo específico. Busque las firmas que se inicien con más frecuencia. ¿Se trata de funciones empresariales legítimas que deberían permitirse en el día a día? Ajuste el nivel de gravedad a un nivel más bajo para estas firmas. Algunas excepciones de equipos de sobremesa se demuestran como comportamientos erróneos de aplicaciones legítimas, y no necesita permitir dichos comportamientos. Compruebe que la aplicación de usuario funcione correctamente y continúe bloqueando.

SUGERENCIA: Es común que los eventos se generen y se bloqueen sin efectos visibles para el usuario en el funcionamiento de la aplicación. Por ejemplo, los sobres de VMware y las aplicaciones de Adobe, a menudo, muestran este comportamiento. Es seguro ignorar estos eventos si puede confirmar que la experiencia de usuario no se ve modificada. Así podría cerrar un círculo, como una vulnerabilidad de comandos entre dos sitios, que podría aprovecharse de forma maliciosa.

Ajustar el proceso

¿Ha recibido quejas de los usuarios? Comúniquese con ellos directamente para comprobar que sus aplicaciones estén funcionando de manera adecuada. A medida que tome decisiones de ajuste durante el seguimiento, siga este proceso:

1 **Editar directivas**: use ePolicy Orchestrator para editar y crear directivas y reacciones.

2 **Aplicar las directivas de manera selectiva**: use ePolicy Orchestrator para aplicar las directivas a los sistemas seleccionados (no es automático).

3 **Activar los cambios**: cuando cambia las directivas de Host IPS en la consola de ePO, los cambios entran en funcionamiento en los sistemas gestionados en la siguiente comunicación entre agente y servidor. De manera predeterminada, este intervalo se da una vez cada 60 minutos. Para aplicar las directivas inmediatamente, envíe una llamada de activación del agente a la consola de ePO.

4 **Probar los cambios**: confirme el éxito de funcionamiento de estos cambios y la compatibilidad con los sistemas empresariales (permitiendo las actividades legítimas). Compruebe que se minimiza el tráfico de IPS y que se reducen los falsos positivos que estaba buscando.

5 **Aplicar las directivas con más amplitud**: si las nuevas directivas funcionan, aplíquelas a los sistemas relevantes.

6 **Continuar con la supervisión diaria**.

Consulte *Configurar directivas de IPS* en la guía del producto para obtener detalles acerca del trabajo con directivas de IPS, incluidas la configuración de reacciones de firmas y la creación de excepciones y de aplicaciones de confianza a partir de eventos. Consulte *Configurar directivas de firewall* en la guía de producto para obtener detalles acerca de trabajar con directivas de firewall.

Configurar paneles e informes

Ahora que ha impuesto más orden y precisión en los eventos, puede usar el servidor de ePO para mejorar la organización y la comunicación de la información de IPS y del firewall.

- Configure los paneles de ePO para obtener una vista general rápida del cumplimiento de las directivas, de las tendencias de los eventos, de los resultados de las consultas y de los problemas. Guarde los paneles únicos que reflejen la supervisión diaria, las revisiones semanales y los informes de gestión.
- Configure notificaciones para alertar a usuarios específicos cuando se produzcan eventos concretos. Por ejemplo, una notificación puede enviarse cuando se inicia un evento de gravedad alta en un servidor concreto.
- Programe los informes para que se ejecuten automáticamente y se envíen a grupos concretos como correo electrónico.

Consulte *Gestionar la protección* en la guía del producto para obtener detalles acerca del trabajo con paneles e informes.

Espere y observe

Supervise los eventos a diario al menos durante otras dos semanas y compruebe las llamadas de ayuda, las anomalías y los falsos positivos. Con esta estrategia de implementación, relativamente conservadora, no debería haber demasiados problemas ni llamadas de asistencia, así que los ajustes deberían ser mínimos.

Asegúrese de desactivar los atajos para evitar que los usuarios y el software malintencionado puedan esquivar las protecciones de IPS. No permita la desactivación de módulos ni la eliminación del cliente de Host IPS.

5. Activar modo Adaptación (opcional)

Después de completar un ciclo empresarial con el software instalado, empiece a implementar reglas bien definidas para crear conjuntos de directivas personalizadas. Estas directivas pueden definirse manualmente, pero el modo Adaptación proporciona una potente herramienta para

crear reglas de IPS basadas en la actividad del host, sin interacción por parte del administrador. A medida que se usa una aplicación, se crea una excepción para permitir cada acción. El modo Adaptación no inicia eventos de IPS ni bloquea actividades, excepto vulnerabilidades de seguridad maliciosas (firmas de gravedad alta). Las excepciones se registran en el servidor ePO como Reglas de cliente de IPS, así puede supervisar el progreso.

Al configurar hosts representativos en el modo Adaptación durante el seguimiento, puede crear una configuración de ajuste para cada perfil de uso o aplicación. La función IPS permite tomar cualquiera, todas o ninguna de las reglas de cliente y convertirlas en directivas impuestas por el servidor. Cuando acabe de ajustar, apague el modo Adaptación para fortalecer la prevención de intrusiones del sistema.

El modo Registro le ayudó a entender la frecuencia de las actividades. De manera correspondiente, el modo Adaptación le informa de la gama completa y del tipo de actividades. Al usar estas dos herramientas de manera conjunta, obtiene una buena línea de base funcional para las actividades empresariales legítimas de su negocio. Debe esperar que haya actividades irregulares que no se capturen durante el ciclo de seguimiento, así que esté preparado para revisar las excepciones y crear reglas manuales si son necesarias. El usuario puede ejecutar una aplicación interna una vez cada cuatro meses, por ejemplo, para obviar los modos Registro y Adaptación.

El modo Adaptación bloquea todas las firmas de gravedad alta de manera predeterminada, así que use el modo Adaptación para gestionar las firmas de gravedad media y alta. Esta combinación le da una buena vista general de la actividad sin demasiadas complicaciones.

El modo Adaptación crea reglas de excepción de manera muy eficiente. Sin embargo, no es probable que se permitan todas las actividades en un sistema determinado, o podría dejar de considerar protecciones nuevas. Por esta razón, debería usar el modo Adaptación durante un tiempo limitado. Revise cada excepción creada (solo hay un ejemplo de cada excepción) y desactive las reglas inaceptables que cree el modo Adaptación.

Si aplica el modo Adaptación, elija la opción de directiva **Conservar reglas de clientes**. De lo contrario, tras cada intervalo de aplicación de directivas se eliminarán las nuevas reglas y será necesario volverlas a aprender. Finalmente, cuando apague el modo Adaptación y pase a la aplicación, apague la opción **Conservar reglas de clientes** y elimine cualquier regla que no sea aplicada por una directiva proporcionada por ePO.

Aplicar el modo Adaptación

1. Aplique el modo Adaptación durante un periodo específico (de una a cuatro semanas).
2. Evalúe las reglas de clientes.
3. Desactive las reglas no adecuadas.
4. En la ficha **Reglas de clientes de IPS**, mueva las reglas de clientes legítimas directamente a una directiva para su aplicación a otros clientes.
5. Apague el modo Adaptación.
6. Apague la función **Conservar reglas de clientes** si está encendida.

SUGERENCIA: Recuerde apagar el modo Adaptación para que no se creen más reglas sin su consentimiento.

Recomendaciones

- Ejecute los clientes en el modo Adaptación durante, al menos, una semana, para hallar todas las actividades normales. Elija momentos de actividad programada, como realización de copias de seguridad o procesamiento de secuencias de comandos.

- Realice el seguimiento de las reglas de cliente en la consola ePO, para verlas en las vistas normal, filtrada y agregada.
- Use reglas de cliente creadas automáticamente para definir directivas nuevas y más detalladas, o añada las reglas a las directivas existentes y aplique las directivas actualizadas a otros clientes.
- Seleccione la opción de directiva **Conservar reglas de clientes**. Si no lo hace, las reglas se eliminarán después de cada intervalo de aplicación de directivas.
- Revise las excepciones que se creen. Apague el modo Adaptación si no puede revisar así, para evitar actividades de riesgo.
- Encienda brevemente el modo Adaptación para crear excepciones para una nueva aplicación y después promuévalas a directiva.

Consulte *Configurar directivas de IPS* en la guía de producto para obtener detalles acerca de trabajar con directivas IPS con el modo Adaptación. Consulte *Configurar directivas de firewall* en la guía de producto para obtener detalles sobre cómo trabajar con directivas de firewall con el modo Adaptación.

NOTA: El modo Adaptación permite tanto actividades legítimas como no legítimas. Las reglas que acepten estas actividades se crearán sin aprobación del administrador. Solo se registra un evento de excepción por regla creada, así que las mismas actividades quedan sin documentar después de la creación de la regla. Solo recibirá un aviso, así que debe revisar y responder con diligencia para prevenir las reglas inaceptables.

6. Ajustes

Ahora que ha establecido y ajustado las respuestas de línea de base a las actividades, puede comenzar a aumentar los niveles de protección y aplicación. Para ello, se debe seleccionar la categoría apropiada de la directiva de **Protección IPS**. Estos ajustes pueden realizarse en el contexto de una supervisión diaria, o puede elegir repetir los pasos formales del seguimiento. Después de cada paso, espere al menos dos semanas antes de considerar la introducción de más cambios. Este tiempo le asegura que los sistemas funcionan correctamente en sus niveles de protección actuales.

De protección básica a protección mejorada y máxima

La categoría de **Protección mejorada** de la directiva de Protección IPS evita las firmas de gravedad alta y media e ignora el resto, mientras que la categoría **Preparación para la protección mejorada** da el paso intermedio de registrar primero los riesgos de gravedad media. Recuerde que el registro proporciona detalles acerca de las actividades que pueden verse afectadas cuando aumenta el nivel de protección. Puede servir como guía para gestionar directivas de forma precisa y limitar las sorpresas.

Cuando esté seguro de que el negocio continuará sin interrupciones, cambie los ajustes a protección mejorada. Repita este proceso para los demás sistemas de su red. La categoría de **Protección máxima** es adecuada para los entornos operativos que más trabajan. La protección máxima debería aplicarse con mucho cuidado únicamente después de exhaustivas pruebas, ya que bloquea incluso las firmas de gravedad baja. Utilice la categoría **Preparación para la protección máxima** como prueba para descubrir el impacto de los cambios antes de activar la protección máxima.

Las organizaciones más conservadoras pueden implementar cada cambio de nivel de protección en su propio equipo de seguimiento, siguiendo los pasos dados. Recuerde activar y desactivar

los mecanismos de escape y el modo Adaptación antes y después de los ciclos de prueba que validan los cambios.

Continúe el ajuste

Revise las excepciones y todos los problemas que surjan. Gestione éstas como se indica en los pasos de ajuste iniciales.

- Supervise las llamadas del departamento de asistencia y los comentarios de los usuarios acerca de quejas o problemas empresariales derivados de accesos bloqueados, falsos positivos o nuevos comportamientos de aplicaciones. Estos problemas deberían ser mínimos, pero siempre se dan nuevos requisitos.
- Revise con regularidad las excepciones generadas.
- Ajuste las directivas de manera acorde. Recuerde usar el servidor de ePO para enviar actualizaciones de directivas a los sistemas del host. Necesitará aplicarlas conscientemente a los sistemas que quiera que afecten.

7. Realizar tareas de mantenimiento y expansión

Los pasos anteriores definen el proceso básico de implementación. Una vez que sus sistemas dispongan de niveles medios de protección, podrá pasar a la protección más avanzada. Necesitará continuar con el seguimiento habitual, actualizar las directivas y mantener los sistemas. Ahora también deberá considerar la expansión de los sistemas protegidos y mejorar la protección para incluir directivas más rigurosas y otras funciones de Host IPS.

Mantenimiento

McAfee a menudo publica actualizaciones de contenido para nuevas firmas, así como actualizaciones ocasionales de funciones y parches. Entre las recomendaciones se incluye:

- Establezca un programa de actualizaciones para que el servidor de ePO busque en el repositorio de McAfee actualizaciones y para que sus clientes las reciban.
- Lleve los contenidos de Host IPS a la rama Evaluación de su repositorio para probarlos en un grupo de sistemas de seguimiento si tiene un alto número de aplicaciones personalizadas que necesiten ajustarse durante las implementaciones iniciales. Una vez que su grupo de seguimiento haya certificado el nuevo contenido, puede moverlo a la rama Actual para implementarlo en los demás sistemas.
- Programe las descargas de contenido para que coincidan con las ediciones de los "Martes de parches" si usa productos de Microsoft.
- Use el modo Adaptación para sistemas con perfiles específicos y envíe las reglas de cliente resultantes al servidor cuando se instalen aplicaciones nuevas, porque es posible que no tenga tiempo o recursos para ajustarlas inmediatamente. Puede promover estas reglas de cliente a directivas nuevas o existentes y después aplicar la directiva a otros equipos para manejar el software nuevo.
- Introduzca las pruebas de IPS en sus procesos de cambio de gestión y de edición de software. Cuando se prepare para implementar un parche de Microsoft, un Service Pack o un producto, pruébelo y hágale el seguimiento en los sistemas de IPS, para poder hacer los ajustes adecuados antes de la implementación general.

Expansión

Según sea su organización, considere cualquiera de las siguientes opciones para expandir la implementación. Recuerde continuar con la implementación de cambios de manera lenta y decidida, para minimizar las molestias a los usuarios y diagnosticar las anomalías con rapidez. Es mejor trabajar despacio que equivocarse o pasar por alto opciones útiles de protección.

Para expandir:

- Implemente las mismas protecciones en sistemas adicionales con los perfiles de uso comprobados. Puede gestionar con facilidad la implementación de Host IPS en miles de equipos, ya que la mayoría se ajusta en pocos perfiles de uso. La gestión de un gran despliegue se reduce a mantener unas cuantas reglas de directivas.
- Repita el proceso para los usuarios con permisos y los servidores, si solo ha estado realizando el seguimiento de los equipos de sobremesa estándar, comenzando con la creación de registros y el uso del modo Adaptación.
- Agregue nuevos perfiles de uso y comunidades de usuarios.
- Implemente las reglas del firewall. Siga el proceso de seguimiento, pero consulte la guía del producto para obtener detalles específicos acerca de las reglas y del modo Aprendizaje.

Instalación en ePolicy Orchestrator

Esta versión de Host Intrusion Prevention necesita que instale una o varias extensiones en ePolicy Orchestrator, según la cobertura de protección que haya adquirido y la versión de ePolicy Orchestrator que esté ejecutando.

A continuación se da una lista de las extensiones necesarias:

Tabla 3: Solo función de firewall

Versión de McAfee ePO	Nombre del archivo	Extensiones necesarias	Funcionalidad
4.0	**HOSTIPS_8000.zip**	Host Intrusion Prevention 8.0.0	Función Firewall
	help_epo_103x.zip	Ayuda de ePO	Ayuda de ePO con la información de Host Intrusion Prevention 8.0
4.5	**HOSTFW_8000_45.zip**	Host Intrusion Prevention 8.0.0	Función Firewall
		Extensión de Host IPS Advanced	Función Respuestas automáticas*
		Contenido de la ayuda: hip_800_help	Ayuda de ePO con la información de Host Intrusion Prevention 8.0
4.6	**HOSTFW_8000_46.zip**	Host Intrusion Prevention 8.0.0	Función Firewall
		Extensión de Host IPS Advanced	Función Respuestas automáticas*
		Contenido de la ayuda: hip_800_help	Ayuda de ePO con la información de Host Intrusion Prevention 8.0

* Válido solo si está instalada la extensión Host Intrusion Prevention 8.0.0.

Tabla 4: Funciones IPS y Firewall

Versión de McAfee ePO	Nombre del archivo	Extensiones necesarias	Funcionalidad
4.0	**HOSTIPS_8000.zip**	Host Intrusion Prevention 8.0.0	Función Firewall
	HostIPSLicense.zip	Extensión de licencia de Host IPS	Función IPS*
	help_epo_103x.zip	Ayuda de ePO	Ayuda de ePO con la información de Host Intrusion Prevention 8.0
4.5	**HOSTIPS_8000_45.zip**	Host Intrusion Prevention 8.0.0	Función Firewall
		Extensión de Host IPS Advanced	Función Respuestas automáticas*
		Extensión de licencia de Host IPS	Función IPS*
		Contenido de la ayuda: hip_800_help	Ayuda de ePO con la información de Host Intrusion Prevention 8.0
4.6	**HOSTIPS_8000_46.zip**	Host Intrusion Prevention 8.0.0	Función Firewall
		Extensión de Host IPS Advanced	Función Respuestas automáticas*
		Extensión de licencia de Host IPS	Función IPS*

Versión de McAfee ePO	Nombre del archivo	Extensiones necesarias	Funcionalidad
		Contenido de la ayuda: hip_800_help	Ayuda de ePO con la información de Host Intrusion Prevention 8.0

* Válido solo si está instalada la extensión Host Intrusion Prevention 8.0.0.

Cada una de las extensiones que se usan con ePolicy Orchestrator 4.5 y 4.6 contienen múltiples archivos .zip que se instalan como extensiones independientes, una para cada tipo de función enumerada más arriba. Si ha instalado Host Intrusion Prevention 8.0 en ePolicy Orchestrator 4.0 y actualiza a la versión 4.5 o 4.6, necesitará instalar dos extensiones más, la extensión de Host IPS Advanced (HostIpsAdv.zip) y la extensión de contenido de la ayuda (help_hip_800.zip). Puede hacerlo mediante la instalación de la extensión Host Intrusion Prevention para la versión de ePolicy Orchestrator o mediante la apertura de la extensión o la instalación de las extensiones que falten. A continuación se da el contenido de cada uno de los .zip de extensión:

Tabla 5: Contenido de las extensiones de múltiples .zip

HOSTFW_8000_45.zip	HOSTFW_8000_46.zip	HOSTIPS_8000_45.zip	HOSTIPS_8000_46.zip
• HOSTIPS_8000.zip • HostIpsAdv.zip • help_hip_800.zip	• HOSTIPS_8000_Lite.zip • HostIpsAdv.zip • help_hip_800.zip	• HOSTIPS_8000.zip • HostIPSLicense.zip • HostIpsAdv.zip.zip • help_hip_800.zip	• HOSTIPS_8000_Lite.zip • HostIPSLicense.zip • HostIpsAdv.zip • help_hip_800.zip

Contenido

▸ Instalación de la extensión
▸ Eliminación de la extensión

Instalación de la extensión

Para instalar Host Intrusion Prevention, debe agregar el archivo de extensión de producto en ePolicy Orchestrator. Utilice este proceso para actualizar o sustituir una extensión IPS de host.

Antes de empezar

Si tiene instaladas las extensiones de Host Intrusion Prevention 6.1/7.0, primero actualice a la extensión Host Intrusion Prevention 7.0.5 antes de instalar la extensión Host Intrusion Prevention 8.0. Así se asegura una instalación y migración segura a las directivas de la versión 8.0.

Tarea

1 Vaya a **Configuración | Extensiones** (ePolicy Orchestrator 4.0) o seleccione **Software | Extensiones** (ePolicy Orchestrator 4.5 y posteriores).

2 Haga clic en **Instalar extensión**.

3 En el cuadro de diálogo **Instalar extensión**, indique la ruta del archivo .zip de extensión del IPS de host y haga clic en **Aceptar**.

NOTA: Esta operación puede tardar varios minutos en completarse.

4 Una vez instalada la extensión, aparecerá la pantalla de resumen; haga clic en **Aceptar**.

5 Repita los pasos del 2 al 4 para instalar las extensiones adicionales que sean necesarias.

- En ePolicy Orchestrator 4.0, Host Intrusion Prevention 8.0.0 y Host IPS License Extension, si está instalado, aparecen en la lista **Productos gestionados**, bajo Extensiones.
- En ePolicy Orchestrator 4.5 y 4.6, Host Intrusion Prevention aparece en la lista **Productos gestionados**, bajo Extensiones, y todas las extensiones instaladas del producto aparecen en el panel derecho.

Eliminación de la extensión

Para eliminar Host Intrusion Prevention 8.0 del servidor de ePolicy Orchestrator, elimine sus extensiones.

NOTA: Si elimina las extensiones, eliminará todas las directivas y las asignaciones de directiva. No recomendamos hacer esto como parte de un procedimiento de solución de problemas, a menos que se haga durante una consulta con la asistencia de McAfee.

- En ePolicy Orchestrator 4.0: Vaya a **Configuración | Extensiones**, seleccione **Host Intrusion Prevention 8.0.0** (o **Host IPS License Extension**, si está instalado) en la lista **Productos gestionados** y, después, haga clic en **Eliminar**.
- En ePolicy Orchestrator 4.5 y superiores: Seleccione **Software | Extensiones**, seleccione **Host Intrusion Prevention** en la lista **Productos gestionados** y, después, en la página izquierda, haga clic en el vínculo **Eliminar** de la extensión instalada.

NOTA: Si hay más de una extensión de Host Intrusion Prevention 8.0 instalada, debe eliminarlas en este orden:

1. Extensión de licencia de Host IPS
2. Extensión de Host IPS Advanced
3. Host Intrusion Prevention 8.0.0

Si quita la extensión de licencia de Host IPS y, a continuación, la reinstala, se desactivarán tanto Host como Network IPS y deberá reactivarlos manualmente en la directiva Opciones de IPS.

Migración de directivas

No es posible usar directivas de McAfee Host Intrusion Prevention 6.1 o 7.0 con los clientes de la versión 8.0 sin migrar antes las directivas de la versión 6.1 o 7.0 al formato de la versión 8.0. Host Intrusion Prevention 8.0 proporciona medios sencillos para migrar directivas con la función **Migración de directivas de Host IPS** de ePolicy Orchestrator, que encontrará en **Automatización**. Esta migración implica la traducción y el traslado de las directivas. Después de que se haya migrado la directiva, aparecerá en el Catálogo de directivas que se corresponda a la función y categoría de Host IPS 8.0, con **[6.1]** o **[7.0]** detrás del nombre de la directiva.

Todas las directivas se traducen y se migran a directivas de la versión 8.0, a excepción de las siguientes:

- Las directivas de Opciones de bloqueo de aplicaciones no se migran, ya que se eliminaron en la versión 8.0.
- Las directivas de Reglas de bloqueo de aplicaciones se migran como directivas de Reglas de IPS llamadas Interceptación de aplicaciones y Protección de invocaciones <nombre> [6.1 o 7.0] (dichas directivas se eliminaron en la versión 8.0). Una vez migradas estas directivas a directivas de Reglas de IPS, la lista Reglas de protección de aplicación correspondiente estará en blanco y la lista Excepciones contendrá excepciones para todas las aplicaciones de confianza predeterminadas configuradas como "De confianza para la interceptación de aplicaciones". Si desea utilizar esta directiva migrada, también deberá asignar la directiva Mis reglas IPS predeterminadas en una configuración de varias directivas, ya que contiene la última lista de protección de aplicaciones por medio de actualizaciones de contenido.

  NOTA: Las aplicaciones para las que se bloquea el enlace en Reglas de bloqueo de aplicación no se migran y necesitan agregarse manualmente a las Reglas de protección de aplicaciones en la directiva Reglas de IPS después de la migración.

- Las directivas de Opciones de cuarentena del firewall no se migran, ya que se eliminaron en la versión 8.0.
- Las directivas de Reglas de cuarentena del firewall no se migran, ya que se eliminaron en la versión 8.0.
- Las Reglas de cliente de IPS y las Reglas de cliente de firewall no se migran.

NOTA: Las asignaciones de directivas se transportan automáticamente durante la migración, a no ser que se haya roto la herencia. Revise siempre la asignación de directivas después de migrar directivas.

Situaciones de migración

La migración de directivas a la versión 8.0 es similar a la de las directivas de las versiones 6.1 y 7.0. Esto se verifica en todas las plataformas.

Para migrar esta versión de Host Intrusion Prevention...	A la versión 8.0, haga esto...
6.1	• Instale las extensiones de Host IPS 8.0 en ePolicy Orchestrator.

Para migrar esta versión de Host Intrusion Prevention...	A la versión 8.0, haga esto...
	• Migre las directivas de 6.1 a directivas de 8.0 mediante la ejecución de la función de migración de Host IPS 8.0. Revise las directivas migradas y las asignaciones de directivas. • Implemente los clientes de Host IPS 8.0 para que sustituyan a los clientes de Host IPS 6.1. • Implemente la última actualización de contenido para los clientes de Host IPS 8.0.
7.0.x	• Instale las extensiones de Host IPS 8.0 en ePolicy Orchestrator. • Migre las directivas de 7.0 a directivas de 8.0 mediante la ejecución de la función de migración de Host IPS 8.0. Revise las directivas migradas y las asignaciones de directivas. • Implemente los clientes de Host IPS 8.0 para que sustituyan a los clientes de Host IPS 7.0. • Implemente la última actualización de contenido para los clientes de Host IPS 8.0.

SUGERENCIA: Si tiene instaladas las extensiones de Host Intrusion Prevention 6.1/7.0, primero actualice a la extensión Host Intrusion Prevention 7.0.5 antes de instalar la extensión Host Intrusion Prevention 8.0. Así se asegura una instalación y migración segura a las directivas de la versión 8.0.

Contenido

▸ Migración de directivas de versiones anteriores
▸ Migración de directivas a través de un archivo .xml

Migración de directivas de versiones anteriores

Si la extensión Host Intrusion Prevention 6.1 o 7.0 sigue presente en ePolicy Orchestrator después de instalar Host Intrusion Prevention 8.0, la manera más sencilla de migrar *todas* las directivas existentes es migrar las directivas directamente.

Tarea

1 Haga clic en **Automatización | Migración de directivas de Host IPS**.

2 En Acción, en **Directivas de Host IPS 6.1 en el catálogo de directivas de ePO** o **Directivas de Host IPS 7.0 en el catálogo de directivas de ePO**, haga clic en **Migrar**.

3 Cuando se haya completado la migración de directivas, haga clic en **Cerrar**.
Todas las directivas de las versiones 6.1 o 7.0 de IPS, de firewall y de funcionamiento general se convierten en directivas de la versión 8.0 y aparecen con [6.1] o [7.0] después de su nombre. Las directivas de Reglas de bloqueo de aplicaciones se convierten en directivas de Protección de interceptación de aplicaciones [6.1] o [7.0] directivas de Reglas de IPS.

NOTA: Si se ejecuta la migración de directivas por segunda vez, se sobrescriben todas las directivas con el mismo nombre que ya se hubieran migrado. Este proceso no es selectivo,

se migran todas las directivas existentes de 6.1 o 7.0. Si desea migrar las directivas de manera selectiva, debe emplear el proceso de migración a través de un archivo .xml.

Migración de directivas a través de un archivo .xml

Si la extensión 6.1 o 7.0 de McAfee Host Intrusion Prevention no está instalada y ya ha exportado las directivas individuales seleccionadas a un archivo .xml, o si desea migrar directivas de manera selectiva, deberá hacerlo empleando un archivo .xml. El proceso requiere que primero se exporten las directivas 6.1 o 7.0 a formato .xml mediante la conversión de los contenidos del archivo .xml a versiones de directiva de McAfee Host Intrusion Prevention 8.0 y que, a continuación, se importe el archivo .xml migrado al catálogo de directivas de Host IPS 8.0.

Antes de empezar

Para seguir este proceso, deberá existir previamente un archivo .xml con directivas exportadas. Para exportar directivas a un archivo .xml, haga clic en **Exportar** en la página del Catálogo de directivas o en la página de Host IPS correspondiente a la directiva.

Tarea

1. Haga clic en **Automatización | Migración de directivas de Host IPS**.
2. En Acción, en directivas de Host IPS 7.0 en archivo .xml, haga clic en **Migrar**.
3. En el cuadro de diálogo Archivo XML de directivas, localice el archivo .xml de la versión Host IPS 6.1 o Host IPS 7.0 que desee migrar y haga clic en **Aceptar**. El archivo .xml se convierte al formato de directiva de la versión 8.0.
4. Haga clic con el botón derecho del ratón en el enlace del archivo .xml convertido y guárdelo para importarlo.
5. Importe el archivo .xml al catálogo de directivas de ePO. Para obtener información más detallada sobre cómo exportar e importar directivas, consulte la documentación de ePolicy Orchestrator.

Instalación del cliente Windows

En esta sección se describen los requisitos, las propiedades y la instalación del cliente de McAfee Host Intrusion Prevention 8.0 para estaciones de trabajo y servidores Windows.

Contenido

- Detalles del cliente Windows
- Instalación remota del cliente Windows
- Instalación local del cliente Windows
- Aplicación de directivas y actualizaciones de contenido IPS
- Eliminación del cliente Windows

Detalles del cliente Windows

Esta versión del cliente de McAfee Host Intrusion Prevention 8.0 para Windows funciona con ePolicy Orchestrator 4.0 y posteriores, McAfee Agent 4.0 y posteriores y la extensión de McAfee Host Intrusion Prevention 8.0. Para obtener información más detallada sobre la instalación y el uso de ePolicy Orchestrator, así como los requisitos de sistema, base de datos y software, consulte la *Guía de instalación de ePolicy Orchestrator*.

Requisitos mínimos de hardware

Requisitos de hardware y red para el cliente de Windows para estaciones de trabajo y servidores:

- Procesador: Intel o AMD x86 y x64
- Espacio libre en el disco duro (cliente): 15 MB (100 MB durante la instalación)
- Memoria: 256 MB RAM.
- Entorno de red: redes Microsoft o Novell NetWare. Las redes NetWare requieren TCP/IP
- NIC: tarjeta de interfaz de red; 10Mbps o superior.

Sistemas operativos compatibles

Windows XP SP2, SP3 (solo 32 bits)

- Professional Edition

Windows Vista, Vista SP1 (32 o 64 bits)

- Business Edition
- Enterprise Edition
- Ultimate Edition

Windows 7 (32 o 64 bits)

- Professional Edition

- Enterprise Edition
- Ultimate Edition

Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (32 o 64 bits)

- Todas las ediciones

Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (32 o 64 bits)

- Todas las ediciones

Clientes de red privada virtual (VPN) compatibles

- AT&T Global Network Services Client 7.6, 8.1
- CheckPoint VPN Client R60, R71
- Cisco IPSec VPN Client version 5.0
- Cisco SSL VPN Client 2.4
- Citrix SSL 4.5.6
- F5 Firepass 1200 6.1 (6031.2009.1010.312)
- iPass 3.5
- Juniper Netscreen VPN Client 10.7
- Juniper Network Connect SSL VPN v6.4
- Microsoft Forefront UAG 2010
- Microsoft VPN
- NCP Secure Entry Client para Win32/64
- NetMotion Mobility XE 7.2
- Nortel Contivity VPN Client 10.x
- SafeNet HARemote v2.0 VPN Clients
- SonicWALL Global VPN Client 4.0
- WatchGuard VPN

Plataforma de virtualización compatible

- VMware ESX 3.5, 4.0
- VMware Vsphere 4.0
- VMware View 4 3.1, 4.0
- VMware Thin App 4.0, 4.5
- VMware ACE 2.5 2.6
- VMware Workstation 6.5, 7.0
- VMware Player 2.5, 3.0
- VMware Server 1.0, 2.0
- Citrix Xen Server 5.0, 5.5
- Citrix Xen Desktop 3.0, 4.0
- Citrix Xen App 5.0, 6.0
- Microsoft Hyper-V Server 2008, 2008 R2
- Microsoft Windows Server 2008 Hyper-V 2008, 2008 R2
- Microsoft VDI (Bundle)

  - MED-V 1.0, 1.0 SP1
  - App-V 4.5, 4.6
  - SCVMM 2008, 2008 R2
  - SCCM 2007SP2, 2007 R2
  - SCOM 2007, 2007 R2
- Microsoft App-V 4.5, 4.6
- XP Mode Windows 7 32- and 64-bit

Bases de datos compatibles

- MS SQL 2000
- MS SQL 2005
- MS SQL 2008, 2008 R2

Instalación remota del cliente Windows

Para desplegar el cliente desde el servidor de ePO, agregue su paquete de despliegue al repositorio principal de ePolicy Orchestrator y, a continuación, despliéguelo en los equipos cliente. Para obtener más información, consulte la *Guía del producto de ePolicy Orchestrator*.

Tarea

1. Vaya a **Software | Repositorio principal** y haga clic en **Incorporar paquete** (ePolicy Orchestrator 4.0), o bien seleccione **Acciones | Incorporar paquete** (ePolicy Orchestrator 4.5 y posteriores).
2. Seleccione **Producto o actualización (.ZIP)** y haga clic en **Examinar**.
3. Localice el archivo .zip del paquete del cliente Host IPS y haga clic en **Abrir**.
4. Haga clic en **Siguiente** y, a continuación, haga clic en **Guardar**.
5. Vaya a **Sistemas | Árbol de sistemas** y seleccione el grupo de sistemas en los que desea instalar el componente cliente.
6. Vaya a **Tareas cliente** y haga clic en **Nueva tarea** (ePolicy Orchestrator 4.0), o seleccione **Acciones | Nueva tarea** (ePolicy Orchestrator 4.5 y posteriores).
7. En el Asistente para crear tareas, asigne un nombre a la tarea, seleccione **Despliegue del producto** en la lista de tareas y haga clic en **Siguiente**.
8. Seleccione la plataforma de cliente, seleccione **Host Intrusion Prevention 8.0** como producto que se instalará y haga clic en **Siguiente**.
9. Programe la tarea para que se ejecute, haga clic en **Siguiente** y luego en **Guardar**. Si planificó la tarea para que se ejecute inmediatamente, realice una llamada de reactivación del agente.

Instalación local del cliente Windows

Puede instalar el software cliente localmente en una estación de trabajo, un equipo portátil o un servidor Windows sin utilizar ePolicy Orchestrator. Puede hacerlo manualmente o bien utilizar software de terceros para distribuirlos a un conjunto de sistemas.

Antes de empezar

Si existe una versión anterior del cliente, asegúrese de desactivar la protección de IPS antes de empezar la instalación.

Tarea

1. Copie el archivo del paquete de instalación del cliente en el equipo cliente.
2. Ejecute el programa de instalación (McAfeeHip_ClientSetup.exe) en el paquete.
3. Siga las instrucciones en pantalla para completar la instalación.

Aplicación de directivas y actualizaciones de contenido IPS

Una vez instalado el cliente, compruebe que se informa a la consola de ePO de las propiedades del Sistema de información y de Host Intrusion Prevention 8,0. Para obtener más detalles, consulte la *Guía del producto de ePolicy Orchestrator*.

Ya está en disposición de supervisar y desplegar directivas IPS para el cliente Windows. Para obtener más detalles, consulte la *Guía del producto de Host Intrusion Prevention 8.0*.

Para asegurarse de que el cliente tiene el contenido más actualizado, descargue el último paquete de contenido actualizado de Host Intrusion Prevention e introdúzcalo en el repositorio de ePO para su implementación. El cliente solo puede obtener las actualizaciones de contenido mediante el comando Actualizar ahora de McAfee Agent, siempre que el administrador de Host Intrusion Prevention haya configurado el proceso de actualización. Para obtener más detalles sobre estas operaciones, consulte las *Actualizaciones de protección de Host IPS* en la *Guía del producto de McAfee Host Intrusion Prevention*.

Para desplegar parches y actualizaciones de producto desde la consola de ePO, siga los procedimientos definidos en la *Guía del producto de ePolicy Orchestrator*.

Para instalar parches y actualizaciones de producto localmente, asegúrese siempre de que la protección de IPS no está activada y, a continuación, siga los procedimientos para la instalación local del producto que se exponen en este capítulo.

McAfee ofrece una utilidad (client_control.exe) para ayudar a automatizar las actualizaciones y otras tareas de mantenimiento cuando se utiliza software de terceros para desplegar Host Intrusion Prevention en equipos cliente. Esta utilidad de línea de comandos, que se puede incluir en las secuencias de comandos de instalación y mantenimiento para desactivar temporalmente la protección IPS y activar funciones de registro, se incluye en el paquete del cliente. Consulte el *Apéndice B, utilidad Clientcontrol.exe* de la *Guía del producto de McAfee Host Intrusion Prevention* para obtener indicaciones de uso, incluyendo información detallada sobre parámetros y seguridad.

Eliminación del cliente Windows

Puede quitar el cliente de Host Intrusion Prevention desde remoto al ejecutar una tarea de despliegue desde el servidor de ePolicy Orchestrator o directamente en el equipo cliente.

Desde el servidor de ePO

- Ejecute una tarea de despliegue para el cliente y seleccione **Eliminar** como Acción para Host Intrusion Prevention.

Directamente en el equipo cliente

Si la consola del cliente no está disponible desde el icono de la bandeja de sistema, dispóngalo para permitir la eliminación del cliente.

Tarea

1. Desde el servidor de ePO, seleccione el sistema del que desea quitar el software.
2. Aplique la opción de directiva **Mostrar producto en la lista de agregar o quitar** de IU de cliente de Host Intrusion Prevention.
3. Configure la tarea de implementación de Host Intrusion Prevention como **Ignorar**.
4. En el equipo cliente, desbloquee la interfaz de cliente con una contraseña.
5. Quite la selección de **Activar Host IPS**.
6. Utilice el panel de control **Agregar o quitar programas** para quitar Host Intrusion Prevention.
7. Reinicie el equipo.

Cómo solucionar problemas de instalación de Windows

Si ha surgido algún problema al instalar o desinstalar el cliente, hay varias cosas que investigar. Entre ellas, asegúrese de que todos los archivos se han instalado en el directorio correcto, compruebe que el cliente se esté ejecutando y verifique los registros del proceso.

Compruebe los archivos de instalación de Windows

Después de la instalación, compruebe que las carpetas y los archivos se instalaron en el cliente. La carpeta C:\Progarm Files\McAfee\Host Intrusion Prevention debe estar instalada y debe contener los siguientes archivos y carpetas esenciales:

Nombre del archivo	Descripción
FireSvc.exe, VSCore/Release/mfefire.exe, VSCore/Release/mfrvtp.exe	Servicios de Host Intrusion Prevention
McAfeeFire.exe	Consola del cliente

El historial de instalación se escribe en C:\Windows\Temp\McAfeeLogs\McAfeeHip8_Install_<version>.log. Para comprobar que el cliente se ha instalado correctamente, busque en este archivo la siguiente entrada: *Producto: McAfee Host Intrusion Prevention -- Operación de instalación completada con éxito*.

Los archivos de registro se encuentran en C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\ o C:\ProgramData\McAfee\Host Intrusion Prevention en Vista y Windows 7.

Compruebe que el cliente Windows se ejecuta

Puede que el cliente se haya instalado correctamente, pero pueden darse problemas de funcionamiento. Si, por ejemplo, el cliente no aparece en la consola de ePO, compruebe que se está ejecutando mediante este comando: Abra una línea de comandos, escriba tasklist \svc y compruebe que se ejecutan los siguientes servicios:

- FireSvc.exe
- mfefire.exe
- mfevtp.exe

Si no es el caso, haga lo siguiente:

1. Ejecute **C:\Program Files\McAfee\Host Intrusion Prevention\McAfeeFire.exe** para abrir la consola del cliente.
2. Desbloquee la consola: Seleccione **Tarea | Desbloquear interfaz de usuario** y escriba abcde12345 como contraseña predeterminada.
3. Establezca la depuración: Seleccione **Ayuda | Solución de problemas** y active la creación de registros para la depuración completa para firewall e IPS.
4. Asegúrese de que tanto Host IPS como Network IPS están desactivados.
5. Abra una línea de comandos y ejecute net start enterceptagent para iniciar el servicio del cliente.

Si el servicio sigue sin iniciarse, compruebe el archivo FireSvc.log para buscar mensajes de error o advertencia que puedan dar pistas acerca de por qué no se inicia el servicio.

Compruebe que los eventos de Host IPS se inician correctamente

Tras comprobar que el cliente se ha instalado correctamente y está ejecutándose, puede comprobar si la protección de IPS está funcionando. Primero asegúrese de que Host IPS está activado en la consola del cliente. A continuación, cree un nuevo documento de texto en el directorio de instalación del cliente: C:\Progarm Files\McAfee\Host Intrusion Prevention. Esta acción debería bloquearse y se debería dar un mensaje de error para indicar que no tiene permisos para guardar en esta ubicación. Compruebe el archivo HipShield.log y busque alguna infracción, desde abajo y hacia arriba. Compruebe que se ha iniciado la siguiente firma: 1001 Blindaje del agente Windows -- Modificación de archivos.

Detención del cliente Windows

Puede que sea necesario detener un cliente en ejecución y reiniciarlo como parte de la solución de un problema.

Tarea

1. Desactive la protección de IPS si está activada. Utilice uno de estos procedimientos:
   - Configure **Opciones de IPS** como **Desactivada** en la consola de ePO y aplique la directiva al cliente.
   - Abra la consola del cliente y, en la ficha Directiva IPS, elimine la selección de **Activar Host IPS**.

   NOTA: No es necesario desactivar la protección del firewall para detener el cliente.
2. Abra una línea de comandos e introduzca: net stop enterceptagent

Reinicio del cliente Windows

Puede que sea necesario reiniciar un cliente como parte de la solución de un problema.

Tarea

1. Abra una línea de comandos e introduzca: net start enterceptagent
2. Si ha desactivado la protección de IPS, emplee uno de los siguientes procedimientos para reactivarla:
   - Configure **Opciones de IPS** como **Activada** en la consola de ePO y aplique la directiva al cliente.
   - Abra la consola del cliente y, en la ficha Directiva IPS, seleccione **Activar Host IPS**.

Instalación del cliente Solaris

En esta sección se describen los requisitos, las propiedades y la instalación del cliente de McAfee Host Intrusion Prevention 8.0 para Solaris, que ayuda a identificar y evitar acciones que podrían resultar perjudiciales y poner en peligro los archivos y aplicaciones de un servidor Solaris. Protege el sistema operativo del servidor y los servidores Web Apache y Sun, y previene especialmente ataques de desbordamiento del búfer.

Contenido

- Detalles del cliente Solaris
- Aplicación de directivas y actualizaciones de contenido IPS
- Eliminación del cliente Solaris
- Cómo solucionar problemas de instalación de Solaris
- Detención del cliente Solaris
- Reinicio del cliente Solaris

Detalles del cliente Solaris

El cliente de Host Intrusion Prevention 8.0 para Solaris funciona con ePolicy Orchestrator 4.0 y posteriores, McAfee Agent 4.0 y el componente de gestión de Host Intrusion Prevention 8.0. Para obtener información más detallada sobre la instalación y el uso de ePolicy Orchestrator, consulte la *Guía de instalación de ePolicy Orchestrator*.

Requisitos mínimos de hardware

- Plataforma SPARC sun4u/sun4v (32 y 64 bits)
- 256 MB RAM
- 10 MB de espacio libre en el disco duro

Sistemas operativos compatibles

- SPARC Solaris 9, sun4u (kernel de 32 ó 64 bits)
- SPARC Solaris 10, sun4u, sun4v (64-bit kernel)

Servidores web compatibles

- Servidor web Apache 1.3.6 y posteriores
- Servidor web Apache 2.0.42 y posteriores
- Servidor web Apache 2.2.3 y posteriores
- Servidor Sun Java Web 6.1
- Servidor Sun Java Web 7.0

Implementación de directivas

No todas las directivas del Host Intrusion Prevention 8.0 están disponibles para el cliente Solaris. Resumiendo, Host Intrusion Prevention protege el servidor host de ataques perjudiciales, pero no ofrece protección del firewall. A continuación se enumeran las directivas válidas.

Directiva	Opciones disponibles
HIP 8.0 GENERAL:	
IU de cliente	Ninguna excepto **administrador** o una **contraseña basada en tiempos** para permitir el uso de la herramienta de solución de problemas**.**
Redes de confianza	Ninguna
Aplicaciones de confianza	Todas excepto **Marcar como confianza para el firewall**.
HIP 8.0 IPS:	
Opciones de IPS	• **Activar IPS de host** • **Activar el modo Adaptación** • **Conservar reglas de cliente existentes**
Protección de IPS	Todas
Reglas de IPS	• **Reglas de excepción** • **Firmas** (solo reglas de HIPS predeterminadas y personalizadas) NOTA: Las firmas NIPS y las **Reglas de protección de aplicación** no están disponibles.
Eventos de IPS	Todas
Reglas IPS de cliente	Todas
HIP 8.0 FIREWALL:	
Opciones del firewall	Ninguna
Reglas del firewall	Ninguna
Bloqueo DNS del firewall	Ninguno

NOTA: El cliente es compatible tanto con la zona global como con las zonas locales. La instalación se realiza solo en la zona global.

Compatibilidad de zona de Solaris

El cliente es compatible tanto con la protección de zona local como con la zona global, pero siempre se instala en zona global. La restricción de la protección a zonas particulares se realiza mediante la edición de las firmas de la directiva Reglas de IPS, en la que se agrega una sección de zona y se incluye el nombre de la zona como valor.

Por ejemplo, si tiene una zona llamada "app_zone" cuyo directorio raíz es /zones/app, la regla de firma se aplicaría solo al archivo de la zona "app_zone" y no a la zona global. Tenga en cuenta que en esta versión la protección del servidor web no puede restringirse a una zona concreta. El código de esta regla contendría:

Rule {

...

file { Include "/tmp/test.log" }

zone { Include "app_zone" }

... }

Para obtener más información acerca de la edición de firmas, consulte *Apéndice A: Escribir firmas personalizadas* en la guía del producto o en la ayuda.

Instalación remota del cliente Solaris

Para desplegar el cliente desde el servidor de ePO, agregue su paquete de despliegue al repositorio principal de ePolicy Orchestrator y, a continuación, despliéguelos en los equipos cliente. Para obtener más información, consulte la *Guía del producto de ePolicy Orchestrator*.

Tarea

1. Vaya a **Software | Repositorio principal** y haga clic en **Incorporar paquete** (ePolicy Orchestrator 4.0), o bien seleccione **Acciones | Incorporar paquete** (ePolicy Orchestrator 4.5 y posteriores).
2. Seleccione **Producto o actualización (.ZIP)** y haga clic en **Examinar**.
3. Localice el archivo .zip del paquete del cliente Host IPS y haga clic en **Abrir**.
4. Haga clic en **Siguiente** y, a continuación, haga clic en **Guardar**.
5. Vaya a **Sistemas | Árbol de sistemas** y seleccione el grupo de sistemas en los que desea instalar el componente cliente.
6. Vaya a **Tareas cliente** y haga clic en **Nueva tarea** (ePolicy Orchestrator 4.0), o bien seleccione **Acciones | Nueva tarea** (ePolicy Orchestrator 4.5 y posteriores).
7. En el Asistente para crear tareas, asigne un nombre a la tarea, seleccione **Despliegue del producto** en la lista de tareas y haga clic en **Siguiente**.
8. Seleccione la plataforma de cliente, seleccione **Host Intrusion Prevention 8.0** como producto que se instalará y haga clic en **Siguiente**.
9. Programe la tarea para que se ejecute, haga clic en **Siguiente** y luego en **Guardar**. Si planificó la tarea para que se ejecute inmediatamente, realice una llamada de reactivación del agente.

Instalación local del cliente Solaris

Puede instalar el software cliente localmente en un servidor Solaris sin utilizar ePolicy Orchestrator. Copie el archivo de instalación del cliente en el equipo del cliente y ejecute el comando adecuado. Si existe una versión anterior del cliente, asegúrese de desactivar la protección de IPS antes de empezar la instalación.

NOTA: El cliente solo puede instalarse en la zona global, pero es compatible con las zonas locales.

Tarea

1. Descargue los archivos **MFEhip.pkg** y **install_hip_solaris** desde el paquete de instalación del cliente.
2. Inicie sesión como administrador y ejecute el siguiente comando: ./install_hip_solaris MFEhip.pkg

Aplicación de directivas y actualizaciones de contenido IPS

Una vez instalado el cliente, compruebe que se informa al servidor de ePO de las propiedades del Sistema de información y de Host Intrusion Prevention 8.0. Para obtener más detalles, consulte la *Guía del producto de ePolicy Orchestrator*.

Ya está en disposición de supervisar y desplegar directivas IPS para el cliente Windows. Para obtener más detalles, consulte la *Guía del producto de McAfee Host Intrusion Prevention 8.0*.

Para asegurarse de que el cliente tiene el contenido más actualizado, descargue el último paquete de contenido actualizado de Host Intrusion Prevention e introdúzcalo en el repositorio de ePO para su implementación. Para obtener más detalles sobre esta operación, consulte las *Actualizaciones de protección de Host IPS* en la *Guía del producto de McAfee Host Intrusion Prevention*.

Eliminación del cliente Solaris

Puede quitar el cliente de Host Intrusion Prevention desde remoto al ejecutar una tarea de despliegue desde el servidor de ePolicy Orchestrator o directamente en el equipo cliente.

Desde el servidor de ePO

- Ejecute una tarea de despliegue para el cliente y seleccione **Eliminar** como Acción para Host Intrusion Prevention.

Directamente en el equipo cliente

En primer lugar, debe desactivar las directivas IPS del cliente en el servidor de ePO antes de eliminarlas manualmente del equipo cliente.

- Inicie sesión en el equipo cliente como administrador y ejecute el siguiente comando:
  /opt/McAfee/hip/install_hip_solaris -uninstall

Cómo solucionar problemas de instalación de Solaris

Si ha surgido algún problema al instalar o desinstalar el cliente, hay varias cosas que investigar. Entre ellas, asegúrese de que todos los archivos se han instalado en el directorio correcto, compruebe que el cliente se esté ejecutando y verifique los registros del proceso.

Compruebe los archivos de instalación de Solaris

Después de una instalación, compruebe que los archivos se instalaron en el directorio del cliente adecuado. El directorio /opt/McAfee/hip deberá incluir estos archivos y directorios esenciales:

Archivo/Nombre de directorio	Descripción
HipClient; HipClient-bin	Cliente Solaris
HipClientPolicy.xml	Reglas de directiva
hipts; hipts-bin	Herramienta de diagnóstico

Archivo/Nombre de directorio	Descripción
*.so	Módulo de objetos compartidos de Host Intrusion Prevention y agente de ePO
directorio del registro	Contiene los archivos de registro: HIPShield.log y HIPClient.log

El historial de instalación se escribe en /opt/McAfee/etc/hip-install.log. Consulte este archivo para cualquier duda acerca del proceso de instalación o eliminación del cliente de Host Intrusion Prevention.

Compruebe que el cliente Solaris se ejecuta

Puede que el cliente se haya instalado correctamente, pero pueden darse problemas de funcionamiento. Si el cliente no aparece en la consola de ePO, por ejemplo, compruebe que se está ejecutando mediante alguno de estos comandos:

- /etc/rc2.d/S99hip status
- ps –ef | grep Hip

Detención del cliente Solaris

Puede que sea necesario detener un cliente en ejecución y reiniciarlo como parte de la solución de un problema.

Tarea

1. Desactivar la protección de IPS. Utilice uno de estos procedimientos:
   - Configure **Opciones de IPS** como **Desactivada** en la consola de ePO y aplique la directiva al cliente.
   - Inicie sesión como administrador y ejecute el siguiente comando: hipts engines MISC:off
2. Ejecute el comando: /etc/rc2.d/S99hip stop

Reinicio del cliente Solaris

Puede que sea necesario detener un cliente en ejecución y reiniciarlo como parte de la solución de un problema.

Tarea

1. Ejecute el comando: /etc/rc2.d/S99hip restart
2. Activación de la protección de IPS. Siga uno de estos procedimientos, según cuál haya utilizado para detener el cliente:
   - Configure **Opciones de IPS** como **Activada** en la consola de ePO y aplique la directiva al cliente.
   - Inicie sesión como administrador y ejecute el siguiente comando: hipts engines MISC:on

Instalación del cliente Linux

En esta sección se describen los requisitos, las propiedades y la instalación del cliente de McAfee Host Intrusion Prevention 8.0 para Linux, que ayuda a identificar y a evitar acciones que podrían resultar perjudiciales y poner en peligro los archivos y las aplicaciones de un servidor Linux.

Contenido

- Detalles del cliente Linux
- Aplicación de directivas y actualizaciones de contenido IPS
- Eliminación del cliente Linux
- Cómo solucionar problemas de instalación de Linux
- Detención del cliente Linux
- Reinicio del cliente Linux

Detalles del cliente Linux

El cliente de Host Intrusion Prevention 8.0 para Linux funciona con ePolicy Orchestrator 4.0 y posteriores, McAfee Agent 4.0 y posteriores y el componente de gestión de Host Intrusion Prevention 8.0. Para obtener información más detallada sobre la instalación y el uso de ePolicy Orchestrator, consulte la *Guía de instalación de ePolicy Orchestrator*.

Requisitos mínimos de hardware

- Intel o AMD x86 y x64
- 512 MB RAM
- 20 MB de espacio libre en el disco duro

Sistemas operativos compatibles

- Red Hat Linux Enterprise 4, 32-bit
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64-bit
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32-bit
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE

- Red Hat Linux Enterprise 5, 64-bit
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10, 32-bit
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 10, 64-bit
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, 32-bit
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, 64-bit
  - 2.6.27.19-5-default

Servidores web compatibles

- Servidor web Apache 1.3.6 y posteriores
- Servidor web Apache 2.0.42 y posteriores
- Servidor web Apache 2.2.3 y posteriores

Sistema de archivos y protección HTTP

El cliente Linux protege los archivos y procesos del sistema operativo. No ofrece protección de red, prevención de desbordamientos de búfer ni supervisión del tráfico HTTP.

Aplicación de directivas con el cliente Linux

No todas las directivas del Host Intrusion Prevention 8.0 están disponibles para el cliente Linux. Resumiendo, Host Intrusion Prevention protege el servidor host de ataques perjudiciales, pero no ofrece protección del firewall. A continuación se enumeran las directivas válidas.

Directiva	**Opciones disponibles**
HIP 8.0 GENERAL:	
IU de cliente	Ninguna excepto **administrador** o una **contraseña basada en tiempos** para permitir el uso de la herramienta de solución de problemas**.**
Redes de confianza	Ninguna
Aplicaciones de confianza	Todas excepto **Marcar como confianza para el firewall**.
HIP 8.0 IPS:	
Opciones de IPS	• **Activar HIPS** • **Activar el modo Adaptación** • **Conservar reglas de cliente existentes**
Protección de IPS	Todos
Reglas de IPS	• **Reglas de excepción**

Directiva	Opciones disponibles
	• **Firmas** (solo reglas de HIPS predeterminadas y personalizadas) NOTA: Las firmas NIPS y las **Reglas de protección de aplicación** no están disponibles.
Eventos de IPS	Todos
Reglas IPS de cliente	Todas
HIP 8.0 FIREWALL:	
Opciones del firewall	Ninguna
Reglas del firewall	Ninguna
Bloqueo DNS del firewall	Ninguno

Instalación remota del cliente Linux

Para desplegar el cliente desde el servidor de ePO, agregue su paquete de despliegue al repositorio principal de ePolicy Orchestrator y, a continuación, despliéguelos en los equipos cliente. Para obtener más información, consulte la *Guía del producto de ePolicy Orchestrator*.

Tarea

1. Vaya a **Software | Repositorio principal** y haga clic en **Incorporar paquete** (ePolicy Orchestrator 4.0), o bien seleccione **Acciones | Incorporar paquete** (ePolicy Orchestrator 4.5 y posteriores).
2. Seleccione **Producto o actualización (.ZIP)** y haga clic en **Examinar**.
3. Localice el archivo .zip del paquete del cliente Host IPS y haga clic en **Abrir**.
4. Haga clic en **Siguiente** y, a continuación, haga clic en **Guardar**.
5. Vaya a **Sistemas | Árbol de sistemas** y seleccione el grupo de sistemas en los que desea instalar el componente cliente.
6. Vaya a **Tareas cliente** y haga clic en **Nueva tarea** (ePolicy Orchestrator 4.0), o bien seleccione **Acciones | Nueva tarea** (ePolicy Orchestrator 4.5 y posteriores).
7. En el Asistente para crear tareas, asigne un nombre a la tarea, seleccione **Despliegue del producto** en la lista de tareas y haga clic en **Siguiente**.
8. Seleccione la plataforma de cliente, seleccione **Host Intrusion Prevention 8.0.0** como producto que se instalará y haga clic en **Siguiente**.
9. Programe la tarea para que se ejecute, haga clic en **Siguiente** y luego en **Guardar**. Si planificó la tarea para que se ejecute inmediatamente, realice una llamada de reactivación del agente.

   NOTA: Si está actualizando el cliente a partir de la versión 7.1.0, deberá reiniciar el sistema Linux.

Instalación local del cliente Linux

Puede instalar el software cliente directamente en un servidor Solaris sin utilizar ePolicy Orchestrator. Copie el archivo de instalación del cliente en el equipo del cliente y ejecute el comando adecuado. Si existe una versión anterior del cliente, asegúrese de desactivar la protección de IPS antes de empezar la instalación.

Tarea

1 Copie el archivo .rpm adecuado del paquete de instalación del cliente en el sistema Linux:

- Red Hat Linux Enterprise 4, 32-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.RH4.i386.rpm
  2. MFEhiplsm-8.0.0.-<número de versión>.RH4.i386.rpm
- Red Hat Linux Enterprise 4, 64-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.RH4.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<número de versión>.RH4.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<número de versión>.RH4.i386.rpm
- Red Hat Linux Enterprise 5, 32-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.RH5.i386.rpm
  2. MFEhiplsm-8.0.0.-<número de versión>.RH5.i386.rpm
- Red Hat Linux Enterprise 5, 64-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.RH5.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<número de versión>.RH5.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<número de versión>.RH5.i386.rpm
- SUSE Linux Enterprise 10, 32-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.SUSE10.i386.rpm
  2. MFEhiplsm-8.0.0.-<número de versión>.SUSE10.i386.rpm
- SUSE Linux Enterprise 10, 64-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.SUSE10.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<número de versión>.SUSE10.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<número de versión>.SUSE10.i386.rpm
- SUSE Linux Enterprise 11, 32-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.SUSE11.i386.rpm
  2. MFEhiplsm-8.0.0.-<número de versión>.SUSE11.i386.rpm
- SUSE Linux Enterprise 11, 64-bit
  1. MFEhiplsm-kernel-8.0.0.-<número de versión>.SUSE11.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<número de versión>.SUSE11.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<número de versión>.SUSE11.i386.rpm

2 Ejecute el comando: rpm -i <nombre del archivo .rpm> para cada archivo .rpm, en el orden en el que se enumeran.

NOTA: Si está actualizando el cliente a partir de la versión 7.1.0, deberá reiniciar el sistema Linux.

Aplicación de directivas y actualizaciones de contenido IPS

Una vez instalado el cliente, compruebe que se informa al servidor de ePO de las propiedades del Sistema de información y de Host Intrusion Prevention 8.0. Para obtener más detalles, consulte la *Guía del producto de ePolicy Orchestrator*.

Ya está en disposición de supervisar y desplegar las directivas IPS para el cliente Linux. Para obtener más detalles, consulte la *Guía del producto de Host Intrusion Prevention 8.0*.

Para asegurarse de que el cliente tiene el contenido más actualizado, descargue el último paquete de contenido actualizado de Host Intrusion Prevention e introdúzcalo en el repositorio de ePO para su implementación. Para obtener más detalles sobre esta operación, consulte la *Guía del producto de ePolicy Orchestrator*.

Para asegurarse de que el cliente tiene el contenido más actualizado, descargue el último paquete de contenido actualizado de Host Intrusion Prevention e introdúzcalo en el repositorio de ePO para su implementación. Para obtener más detalles sobre estas operaciones, consulte las *Actualizaciones de protección de Host IPS* en la *Guía del producto de McAfee Host Intrusion Prevention*.

Eliminación del cliente Linux

Puede quitar el cliente de Host Intrusion Prevention desde remoto al ejecutar una tarea de despliegue desde el servidor de ePolicy Orchestrator o directamente en el equipo cliente.

Desde el servidor de ePO

- Ejecute una tarea de despliegue para el cliente y seleccione **Eliminar** como Acción para Host Intrusion Prevention.

Directamente en el equipo cliente

En primer lugar, debe desactivar las directivas IPS del cliente en el servidor de ePO antes de eliminarlas manualmente del equipo cliente.

- Inicie sesión en el equipo cliente como administrador y ejecute el siguiente comando: rpm -e MFEhiplsm; MFEhiplsm-kernel; MFEhiplsm-apache

Cómo solucionar problemas de instalación de Linux

Si ha surgido algún problema al instalar o desinstalar el cliente, hay varias cosas que investigar. Entre ellas, asegúrese de que todos los archivos se han instalado en el directorio correcto, compruebe que el cliente se esté ejecutando y verifique los registros del proceso.

Compruebe los archivos de instalación de Linux

Después de una instalación, compruebe que los archivos se instalaron en el directorio del cliente adecuado. El directorio /opt/McAfee/hip deberá incluir estos archivos y directorios esenciales:

Archivo/Nombre de directorio	Descripción
HipClient; HipClient-bin	Cliente Linux

Archivo/Nombre de directorio	Descripción
HipClientPolicy.xml	Reglas de directiva
hipts; hipts-bin	Herramienta de diagnóstico
*.so	Módulo de objetos compartidos de Host Intrusion Prevention y agente de ePO
directorio del registro	Contiene los archivos de registro: HIPShield.log y HIPClient.log

El historial de instalación se escribe en /opt/McAfee/etc/hip-install.log. Consulte este archivo para cualquier duda acerca del proceso de instalación o eliminación del cliente de Host Intrusion Prevention.

Compruebe que el cliente Linux se ejecuta

Puede que el cliente se haya instalado correctamente, pero pueden darse problemas de funcionamiento. Si el cliente no aparece en la consola de ePO, por ejemplo, compruebe que se está ejecutando mediante este comando: ps –ef | grep Hip

Detención del cliente Linux

Puede que sea necesario detener un cliente en ejecución y reiniciarlo como parte de la solución de un problema.

Tarea

1. Para detener un cliente en ejecución, desactive primero la protección IPS. Utilice uno de estos procedimientos:
   - Configure **Opciones de IPS** como **Desactivada** en la consola de ePO y aplique la directiva al cliente.
   - Inicie sesión como administrador y ejecute el siguiente comando: hipts engines MISC:off
2. Ejecute el comando: hipts agent off

Reinicio del cliente Linux

Puede que sea necesario detener un cliente en ejecución y reiniciarlo como parte de la solución de un problema.

Tarea

1. Para reiniciar un cliente, ejecute el comando: hipts agent on
2. Activación de la protección de IPS. Siga uno de estos procedimientos, según cuál haya utilizado para detener el cliente:
   - Configure **Opciones de IPS** como **Activada** en la consola de ePO y aplique la directiva al cliente.
   - Inicie sesión como administrador y ejecute el siguiente comando: hipts engines MISC:on