

Configuración del router y SDM y de la CLI de Cisco IOS en Cisco IOS IPS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Habilitar Cisco IOS IPS con un SDF predeterminado de fábrica](#)

[Agregar firmas adicionales después de habilitar el SDF predeterminado](#)

[Seleccionar firmas y trabajar con categorías de firmas](#)

[Actualizar firmas para archivos SDF predeterminados](#)

[Información Relacionada](#)

[Introducción](#)

En Cisco Router and Security Device Manager (SDM) 2.2, la configuración de Cisco IOS[®] IPS se integra en la aplicación SDM. Ya no es necesario que inicie una ventana independiente para configurar Cisco IOS IPS.

En Cisco SDM 2.2, un nuevo asistente de configuración IPS le guiará a través de los pasos necesarios para habilitar Cisco IOS IPS en el router. Además, todavía puede utilizar las opciones de configuración avanzadas para habilitar, inhabilitar y ajustar Cisco IOS IPS con Cisco SDM 2.2.

Cisco recomienda ejecutar Cisco IOS IPS con los archivos de definición de firma (SDF) preconfigurados: attack-drop.sdf, 128MB.sdf y 256MB.sdf. Estos archivos se crean para routers con diferentes cantidades de memoria. Los archivos se agrupan con Cisco SDM, que recomienda SDF cuando active por primera vez Cisco IOS IPS en un router. Estos archivos también se pueden descargar desde <http://www.cisco.com/pcqi-bin/tablebuild.pl/ios-sigup> (sólo clientes registrados).

El proceso para habilitar los SDF predeterminados se detalla en [Habilitar Cisco IOS IPS con un SDF Predeterminado de Fábrica](#). Cuando los SDF predeterminados no son suficientes o desea agregar nuevas firmas, puede utilizar el procedimiento descrito en [Agregar firmas adicionales después de Habilitar el SDF predeterminado](#).

[Prerequisites](#)

[Requirements](#)

Se necesita Java Runtime Environment (JRE) versión 1.4.2 o posterior para utilizar Cisco SDM 2.2. Un archivo de firma recomendado y optimizado por Cisco (basado en DRAM) se incluye con Cisco SDM (cargado en la memoria flash del router con Cisco SDM).

Componentes Utilizados

La información de este documento se basa en el router y el administrador de dispositivos de seguridad (SDM) de Cisco 2.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Habilitar Cisco IOS IPS con un SDF predeterminado de fábrica

Procedimiento CLI

Complete este procedimiento para utilizar la CLI para configurar un Cisco 1800 Series Router con Cisco IOS IPS para cargar 128MB.sdf en la memoria flash del router.

1. Configure el router para habilitar la notificación de eventos de intercambio de dispositivos de seguridad (SDEE).

```
yourname#conf t
```

2. Ingrese los comandos de configuración (uno por línea) y luego presione Cntl+Z para finalizar.

```
yourname(config)#ip ips notify sdee
```

3. Cree un nombre de regla IPS que se utilice para asociar a interfaces.

```
yourname(config)#ip ips name myips
```

4. Configure un comando de ubicación IPS para especificar de qué archivo leerá las firmas el sistema IPS de Cisco IOS. Este ejemplo utiliza el archivo en flash: 128 MB.sdf. La parte de la URL de ubicación de este comando puede ser cualquier URL válida que utilice flash, disco o protocolos a través de FTP, HTTP, HTTPS, RTP, SCP y TFTP para señalar los archivos.

```
yourname(config)#ip ips sdf location flash:128MB.sdf
```

Nota: Debe habilitar el comando **terminal monitor** si configura el router a través de una sesión Telnet o no verá los mensajes SDEE cuando se construya el motor de firma.

5. Active IPS en la interfaz donde desea habilitar Cisco IOS IPS para analizar el tráfico. En este caso, habilitamos en ambas direcciones en la interfaz fastEthernet 0.

```
yourname(config)#interface fastEthernet 0
```

```
yourname(config-if)#ip ips myips in
```

*Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS:
SDF loaded successfully from opacl

*Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS:
SDF loaded successfully from flash:128MB.sdf

*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
OTHER - 4 signatures - 1 of 15 engines

*Oct 26 00:32:30.921: %IPS-6-ENGINE_READY:
OTHER - 0 ms - packets for this engines will be scanned

*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
MULTI-STRING - 0 signatures - 2 of 15 engines

*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED:
MULTI-STRING - there are no new signature definitions for this engine

*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
STRING.ICMP - 1 signatures - 3 of 15 engines

*Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
STRING.ICMP - 20 ms - packets for this engine will be scanned

*Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING:
STRING.UDP - 17 signatures - 4 of 15 engines

*Oct 26 00:32:31.393: %IPS-6-ENGINE_READY:
STRING.UDP - 448 ms - packets for this engine will be scanned

*Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING:
STRING.TCP - 58 signatures - 5 of 15 engines

*Oct 26 00:32:33.641: %IPS-6-ENGINE_READY:
STRING.TCP - 2248 ms - packets for this engine will be scanned

*Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING:
SERVICE.FTP - 3 signatures - 6 of 15 engines

*Oct 26 00:32:33.657: %IPS-6-ENGINE_READY:
SERVICE.FTP - 16 ms - packets for this engine will be scanned

*Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING:
SERVICE.SMTP - 2 signatures - 7 of 15 engines

*Oct 26 00:32:33.685: %IPS-6-ENGINE_READY:
SERVICE.SMTP - 28 ms - packets for this engine will be scanned

*Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
SERVICE.RPC - 29 signatures - 8 of 15 engines

*Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
SERVICE.RPC - 92 ms - packets for this engine will be scanned

*Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING:
SERVICE.DNS - 31 signatures - 9 of 15 engines

*Oct 26 00:32:33.801: %IPS-6-ENGINE_READY:
SERVICE.DNS - 20 ms - packets for this engine will be scanned

*Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING:
SERVICE.HTTP - 132 signatures - 10 of 15 engines

*Oct 26 00:32:44.505: %IPS-6-ENGINE_READY:
SERVICE.HTTP - 10704 ms - packets for this engine will be scanned

*Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING:
ATOMIC.TCP - 11 signatures - 11 of 15 engines

*Oct 26 00:32:44.513: %IPS-6-ENGINE_READY:
ATOMIC.TCP - 4 ms - packets for this engine will be scanned

*Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING:
ATOMIC.UDP - 9 signatures - 12 of 15 engines

*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
ATOMIC.UDP - 4 ms - packets for this engine will be scanned

*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
ATOMIC.ICMP - 0 signatures - 13 of 15 engines

*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED:
ATOMIC.ICMP - there are no new signature definitions for this engine

*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines

*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
ATOMIC.IPOPTIONS - 0 ms - packets for this engine will be scanned

*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
ATOMIC.L3.IP - 5 signatures - 15 of 15 engines

*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
ATOMIC.L3.IP - 0 ms - packets for this engine will be scanned

```
yourname(config-if)#ip ips myips out
yourname(config-if)#ip virtual-reassembly
```

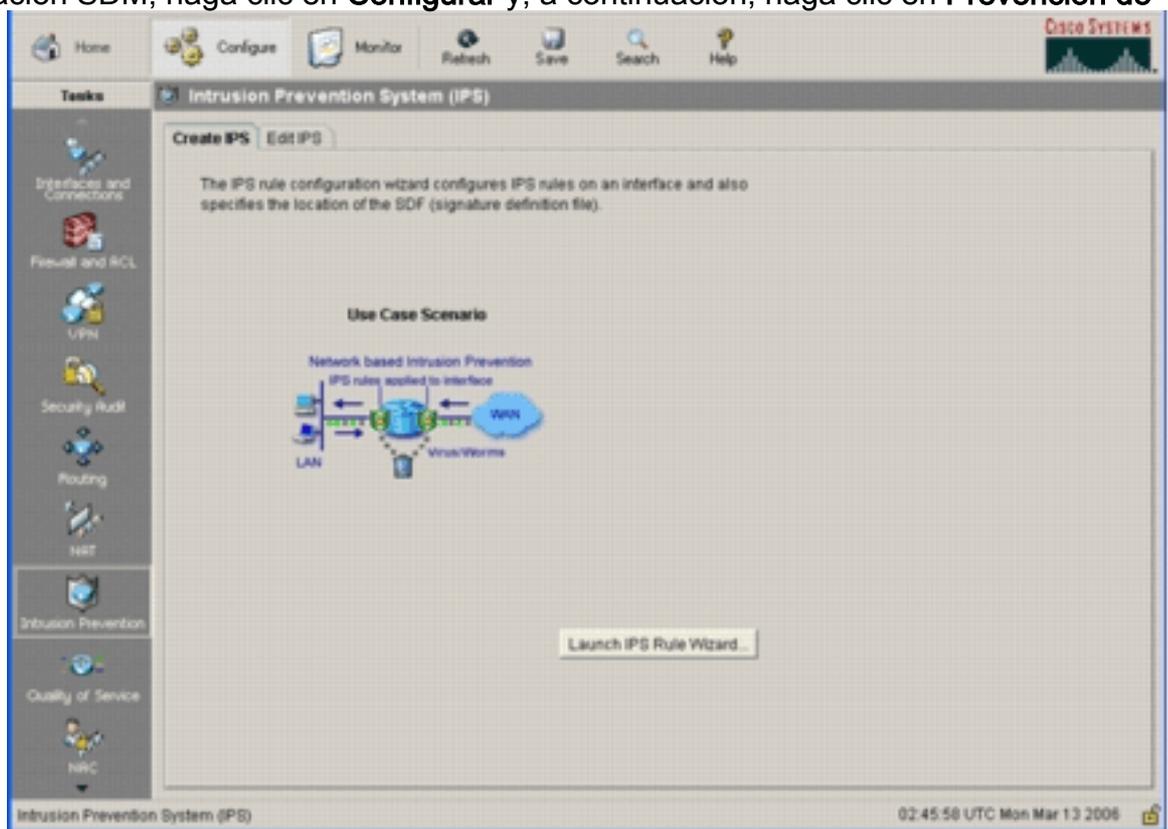
La primera vez que se aplica una regla IPS a una interfaz, Cisco IOS IPS inicia las firmas generadas desde el archivo especificado por el comando de ubicaciones SDF. Los mensajes SDEE se registran en la consola y se envían al servidor syslog si están configurados. Los mensajes SDEE con *<number>* de *<number>* motores indican el proceso de construcción del motor de firma. Por último, cuando los dos números son iguales, todos los motores están contruidos.**Nota:** El reensamblado virtual IP es una función de interfaz que (cuando está activada) reensambla automáticamente los paquetes fragmentados que entran en el router a través de esa interfaz. Cisco recomienda que habilite ip virtual-assembly en todas las interfaces donde el tráfico entra en el router. En el ejemplo anterior, además de activar "ip virtual-assembly" en la interfaz fastEthernet 0, lo configuramos también en la interfaz interna VLAN 1.

```
yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly
```

Procedimiento SDM 2.2

Complete este procedimiento para utilizar Cisco SDM 2.2 para configurar un Cisco 1800 Series Router con Cisco IOS IPS.

1. En la aplicación SDM, haga clic en **Configurar** y, a continuación, haga clic en **Prevención de**



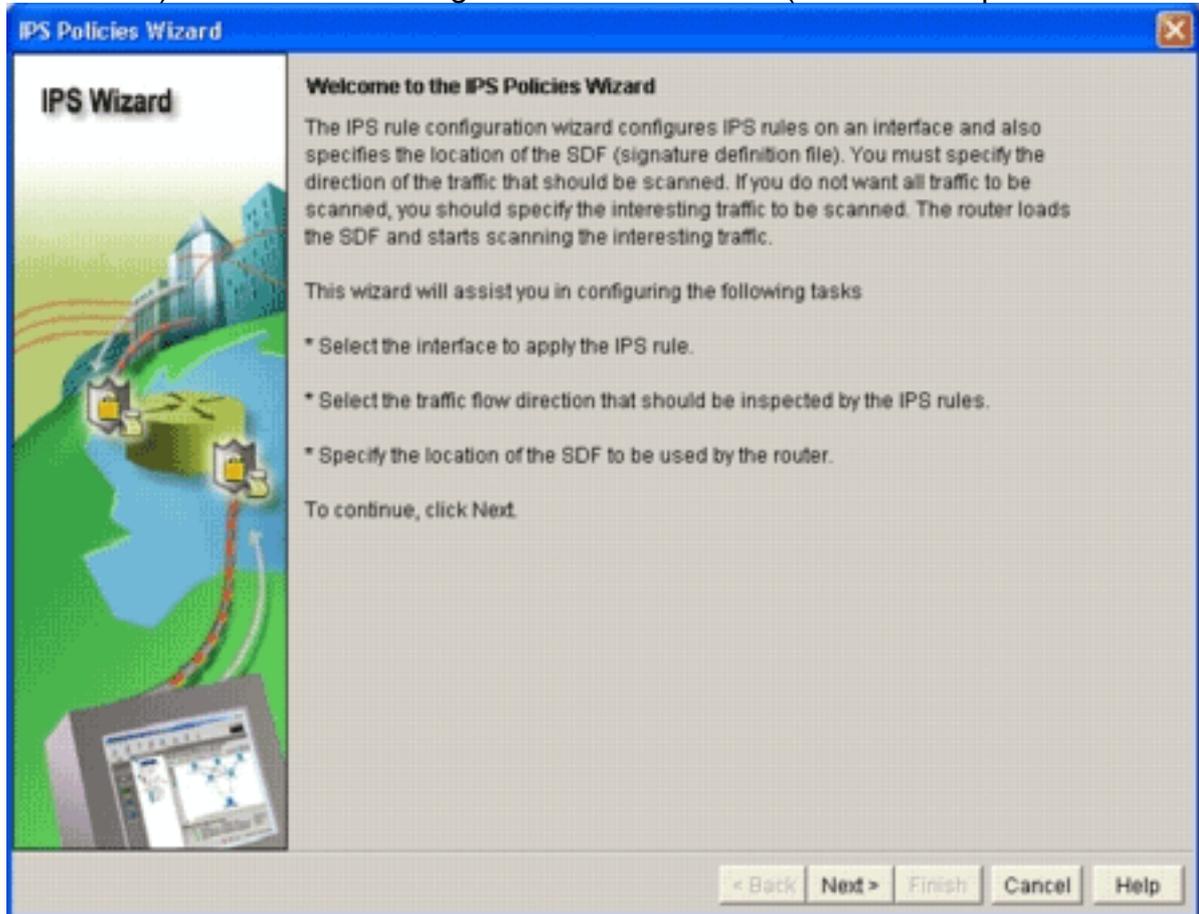
intrusiones.

2. Haga clic en la ficha **Create IPS** y, a continuación, haga clic en **Launch IPS Rule Wizard**. Cisco SDM requiere la notificación de eventos IPS a través de SDEE para configurar la función Cisco IOS IPS. De forma predeterminada, la notificación SDEE no está habilitada. Cisco SDM le solicita que active la notificación de eventos IPS a través de SDEE, como se



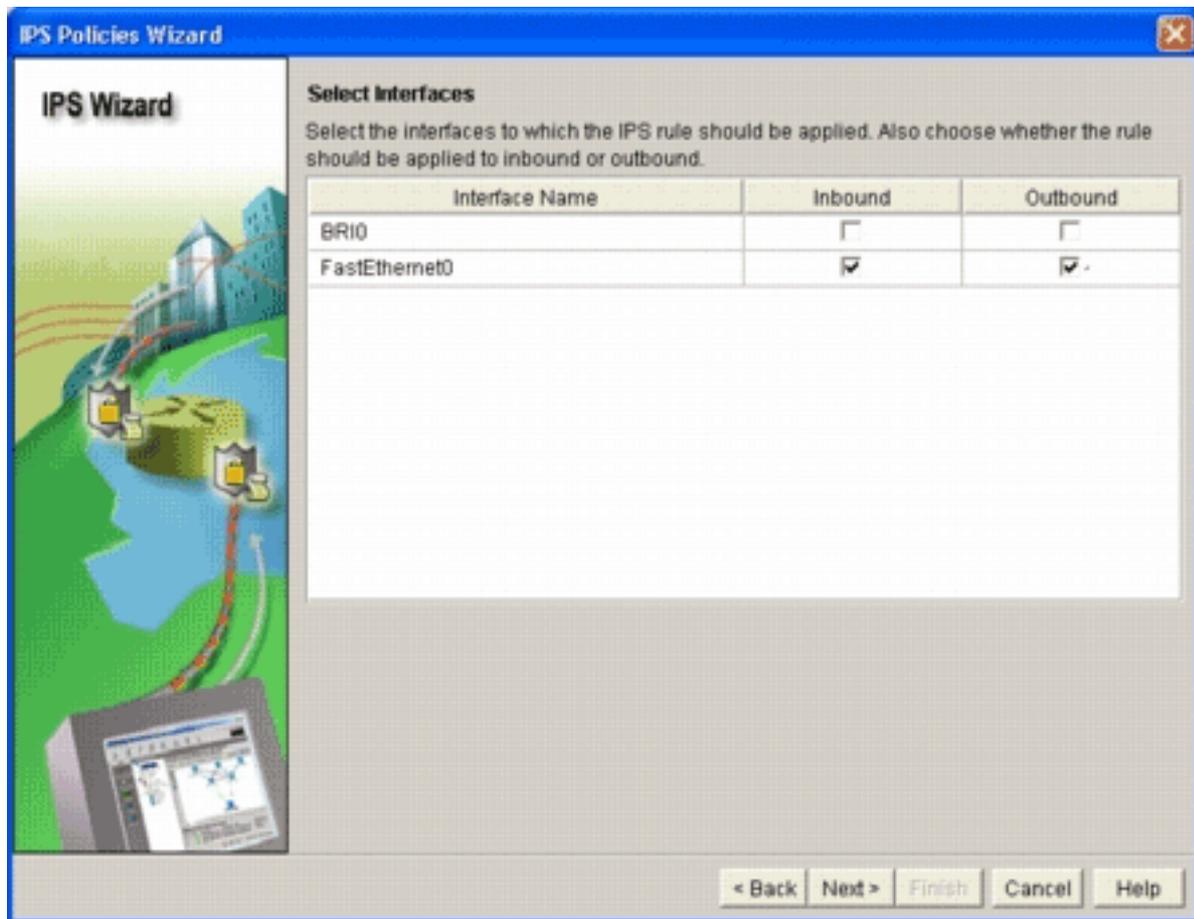
muestra en esta imagen:

3. Click OK. Aparecerá la ventana Welcome to the IPS Policies Wizard (Bienvenido al Asistente de políticas IPS) del cuadro de diálogo IPS Policies Wizard (Asistente de políticas

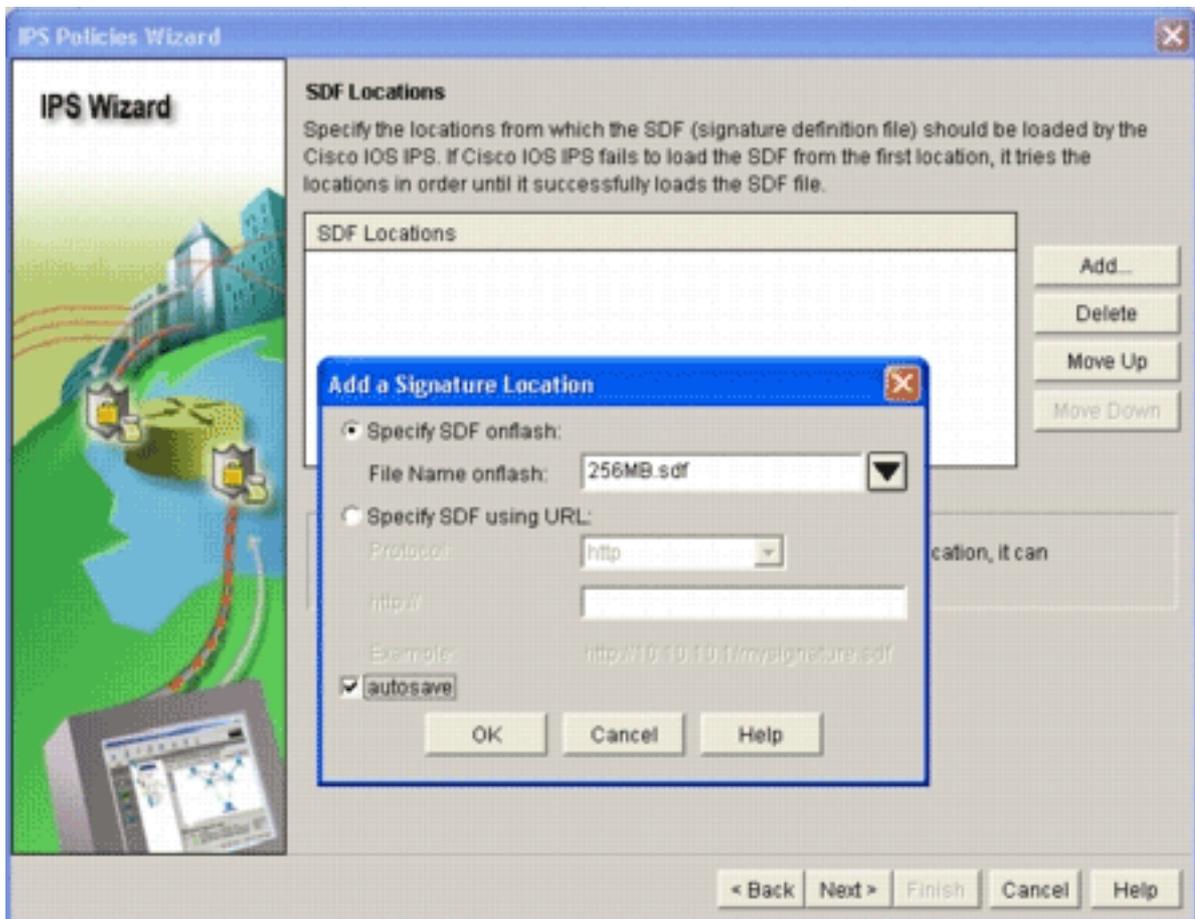


IPS).

4. Haga clic en Next (Siguiete). Aparecerá la ventana Seleccionar interfaces.

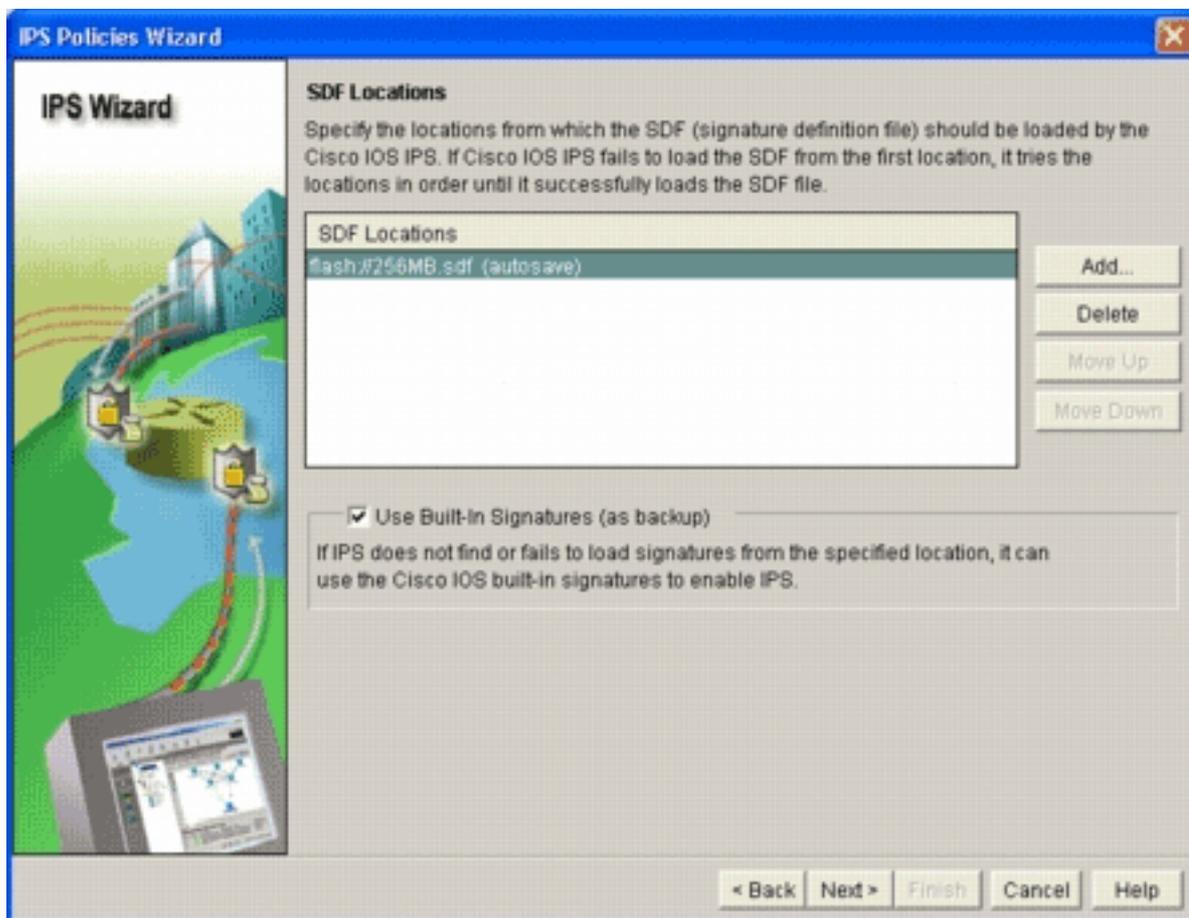


5. Elija las interfaces para las que desea habilitar IPS, y haga clic en la casilla de verificación **Entrante** o **Saliente** para indicar la dirección de esa interfaz. **Nota:** Cisco recomienda que habilite tanto las direcciones entrantes como las salientes cuando habilite IPS en una interfaz.
6. Haga clic en Next (Siguiete). Aparecerá la ventana Ubicaciones de SDF.
7. Haga clic en **Agregar** para configurar una ubicación SDF. Aparecerá el cuadro de diálogo Agregar una ubicación de



firma.

8. Haga clic en el botón de opción **Especificar SDF en flash** y elija 256MB.sdf en la lista desplegable **Nombre de archivo en flash**.
9. Haga clic en la casilla de verificación **Autosave** y haga clic en **OK**.**Nota:** La opción Autosave guarda automáticamente el archivo de firma cuando hay un cambio de firma.La ventana Ubicaciones de SDF muestra la nueva ubicación de



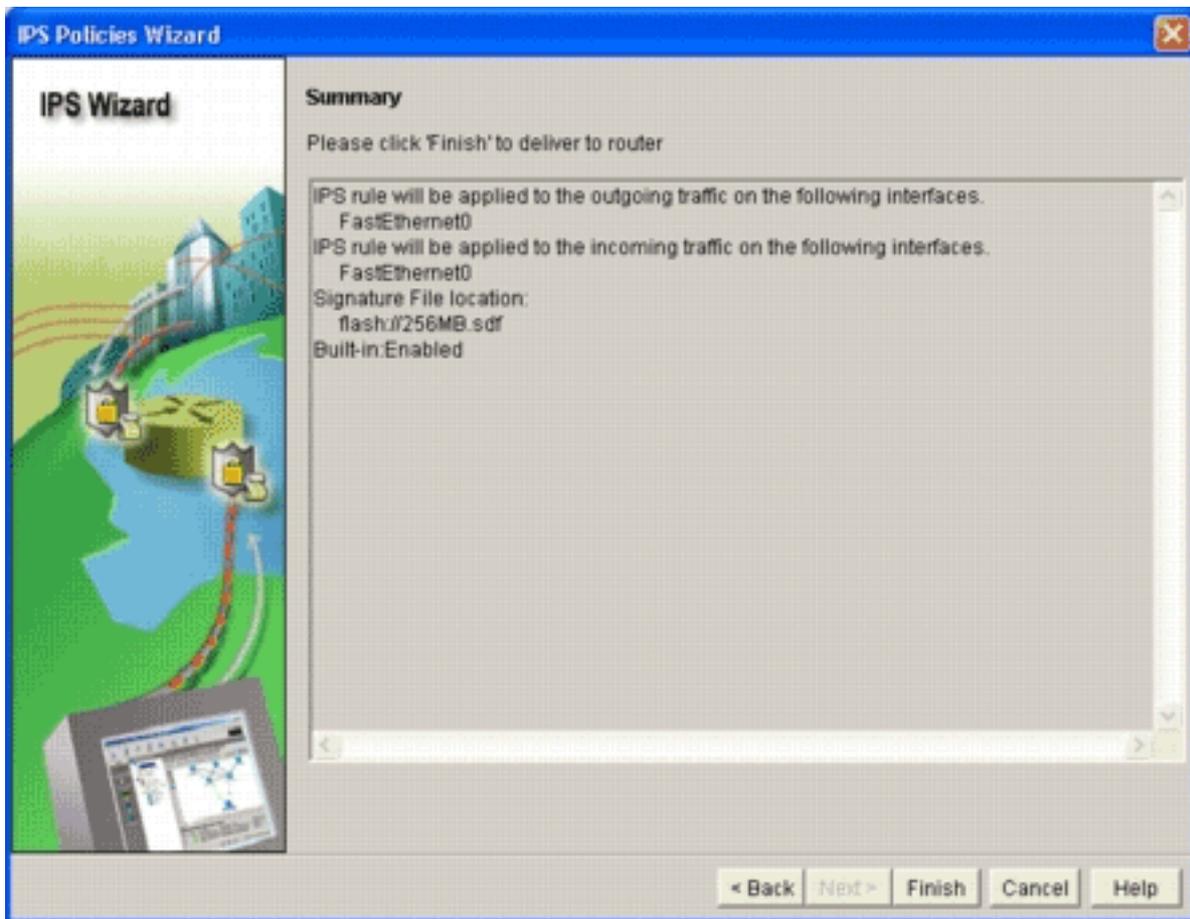
SDF.

Not

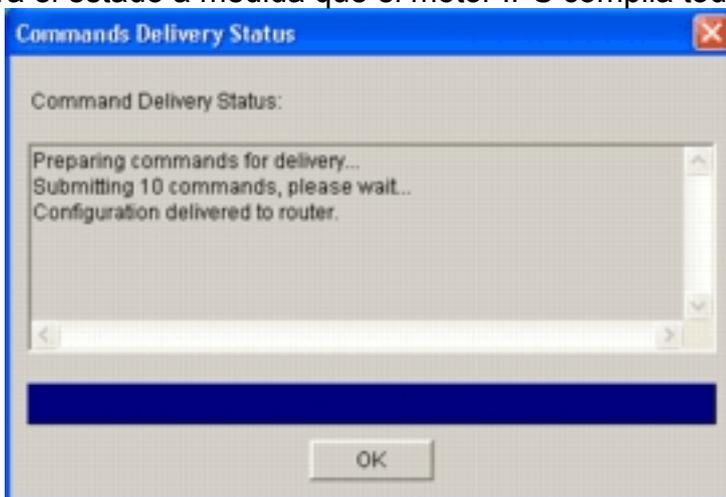
a: Puede agregar ubicaciones de firma adicionales para designar una copia de seguridad.

10. Haga clic en la casilla de verificación **Usar firmas integradas (como copia de seguridad)**.**Nota:** Cisco recomienda que no utilice la opción de firma integrada a menos que haya especificado una o más ubicaciones.

11. Haga clic en **Next** para continuar. Aparecerá la ventana Resumen.



12. Haga clic en Finish (Finalizar).El cuadro de diálogo Estado de entrega de comandos muestra el estado a medida que el motor IPS compila todas las



firmas.

13. Una vez que el proceso haya finalizado, haga clic en **Aceptar**.El cuadro de diálogo Estado de compilación de firmas muestra la información de compilación de

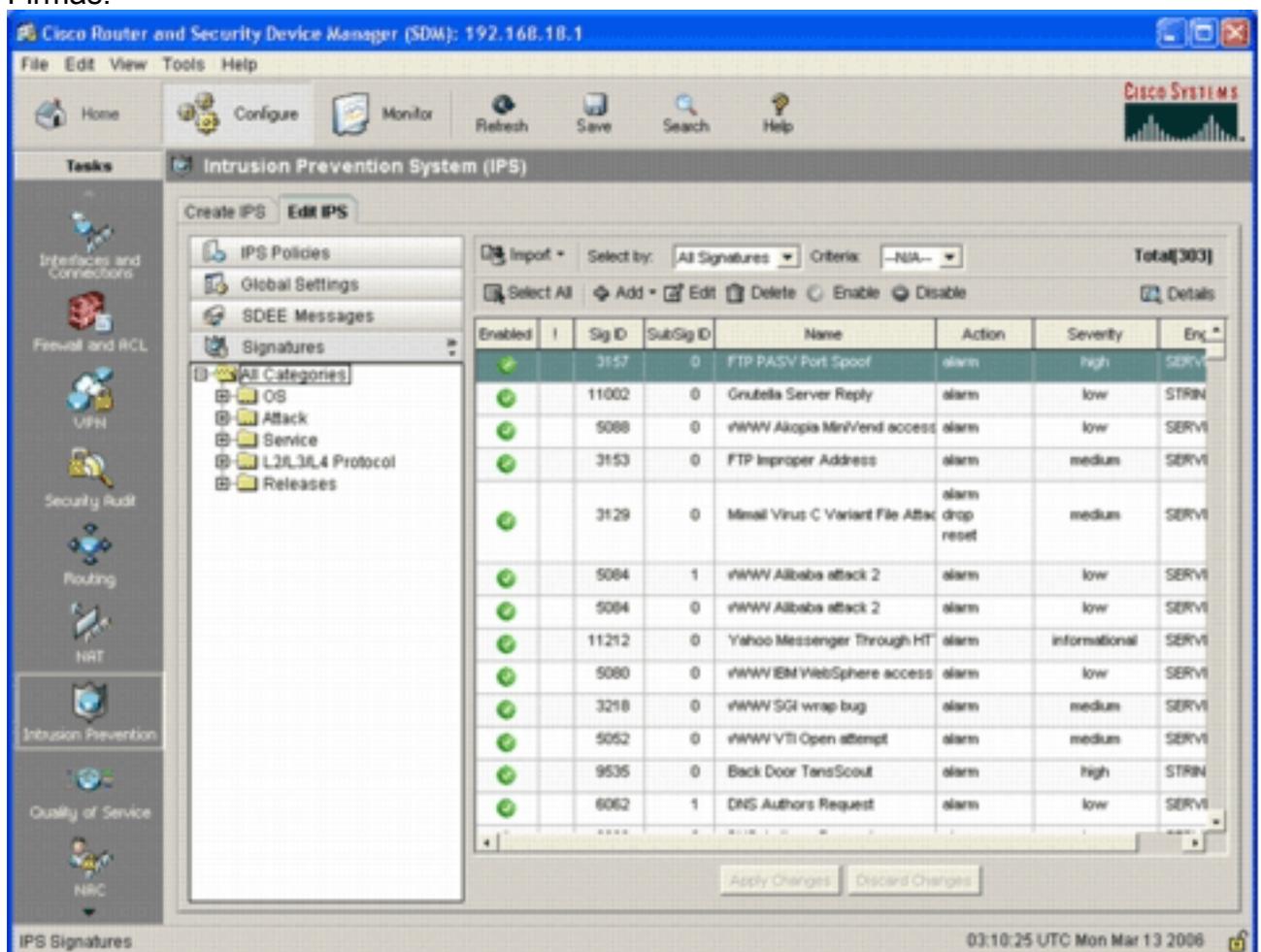


firmas.

Esta información muestra qué

motores se han compilado y el número de firmas en ese motor. Para los motores que muestran *Omitido* en la columna de estado, no hay ninguna firma cargada para ese motor.

14. Haga clic en **Cerrar** para cerrar el cuadro de diálogo Estado de compilación de firmas.
15. Para verificar qué firmas están cargadas actualmente en el router, haga clic en **Configurar** y luego haga clic en **Prevención de intrusiones**.
16. Haga clic en la ficha **Edit IPS** y, a continuación, haga clic en **Firmas**. La lista de firmas IPS aparece en la ventana Firmas.



[Agregar firmas adicionales después de habilitar el SDF predeterminado](#)

Procedimiento CLI

No hay ningún comando CLI disponible para crear firmas o leer información de firma del archivo IOS-Sxxx.zip distribuido. Cisco recomienda que utilice SDM o Management Center for IPS Sensors para administrar las firmas en los sistemas IPS de Cisco IOS.

Para los clientes que ya tienen un archivo de firma preparado y desean fusionar este archivo con el SDF que se ejecuta en un sistema IPS de Cisco IOS, puede utilizar este comando:

```
yourname#show running-config | include ip ips sdf
ip ips sdf location flash:128MB.sdf
yourname#
```

El archivo de firma definido por el comando de ubicación de firma es donde el router carga los archivos de firmas cuando se recarga o cuando se reconfigura el IPS del IOS del router. Para que el proceso de fusión sea exitoso, también se debe actualizar el archivo definido por el comando de ubicación del archivo de firma.

1. Utilice el comando **show** para verificar las ubicaciones de firma configuradas actualmente. El resultado muestra las ubicaciones de firma configuradas. Este comando muestra desde dónde se cargan las firmas actuales en ejecución.

```
yourname#show ip ips signatures
Builtin signatures are configured
```

Las firmas se cargaron por última vez desde flash:128MB.sdf Versión S128.0 de Cisco SDF Versión V0.0 de Trend SDF

2. Utilice el comando **copy <url> ips-sdf**, junto con la información del paso anterior, para fusionar archivos de firma.

```
yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf
Loading mysignatures.xml from 10.10.10.5 (via Vlan1): !
[OK - 1612 bytes]
*Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl
No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport
4715
*Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from
tftp://10.10.10.5/mysignatures.xml
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature
definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures -
2 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are
no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures -
3 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are
no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures -
4 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are
no new signature definitions for this engine
*Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures -
5 of 15 engines
*Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False -
This parameter is not supported
*Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this
```

```

engine will be scanned
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures -
6 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are
no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures -
7 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are
no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures -
8 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are
no new signature definitions for this engine
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures -
9 of 15 engines
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are
no new signature definitions for this engine
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures -
10 of 15 engines
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are
no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures -
11 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are
no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures -
12 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are
no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures -
13 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are
no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures -
14 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are
no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures -
15 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are
no new signature definitions for this engine

```

yourname#

Después de ejecutar el comando **copy**, el router carga el archivo de firma en la memoria y luego genera los motores de firma. En la salida del mensaje SDEE de la consola, se muestra el estado de construcción de cada motor de firma. %IPS-6-ENGINE_BUILD_SKIPPED indica que no hay nuevas firmas para este motor. %IPS-6-ENGINE_READY indica que hay nuevas firmas y que el motor está listo. Como antes, el mensaje "15 de 15 motores" indica que todos los motores han sido construidos. IPS-7-UNSUPPORTED_PARAM indica que un parámetro determinado no es soportado por Cisco IOS IPS. Por ejemplo, CapturePacket y ResetAfterIdle. **Nota:** Estos mensajes son sólo para información y no afectarán a la capacidad o el rendimiento de la firma IPS de Cisco IOS. Estos mensajes de registro se pueden desactivar estableciendo el nivel de registro más alto que la depuración (nivel 7).

- Actualice el SDF definido por el comando de ubicación de firma, de modo que cuando el router se recargue, tenga la firma combinada configurada con firmas actualizadas. Este ejemplo muestra la diferencia de tamaño de archivo después de guardar la firma combinada en el archivo flash 128MB.sdf.

yourname#**show flash:**

```

-#- --length-- -----date/time----- path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf

```

```

yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time----- path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf

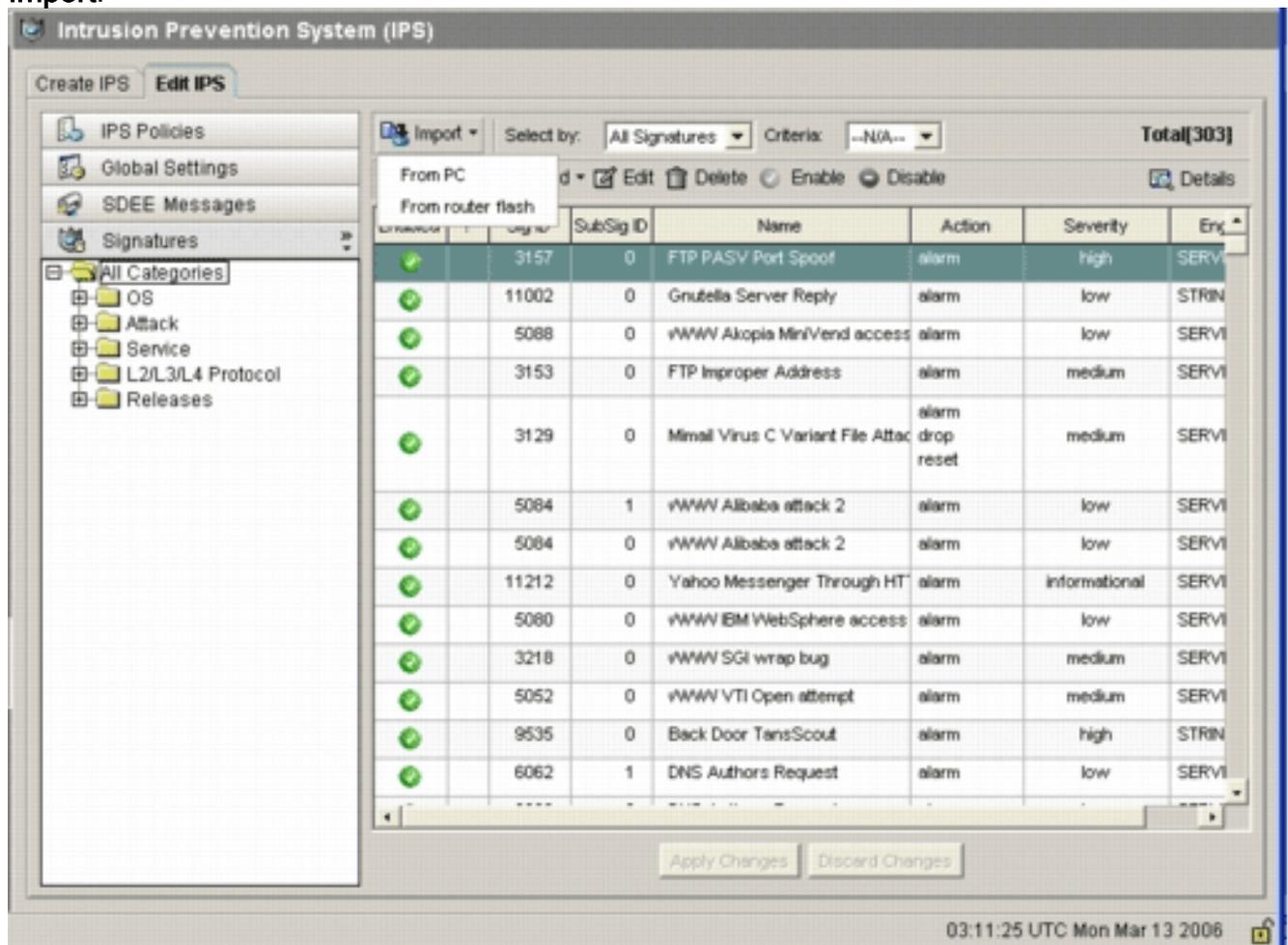
```

Advertencia: El nuevo archivo 128MB.sdf ahora contiene firmas combinadas con el cliente. El contenido es diferente del archivo 128MB.sdf predeterminado de Cisco. Cisco recomienda que cambie este archivo a un nombre diferente para evitar confusiones. Si se cambia el nombre, también se debe cambiar el comando de ubicación de firma.

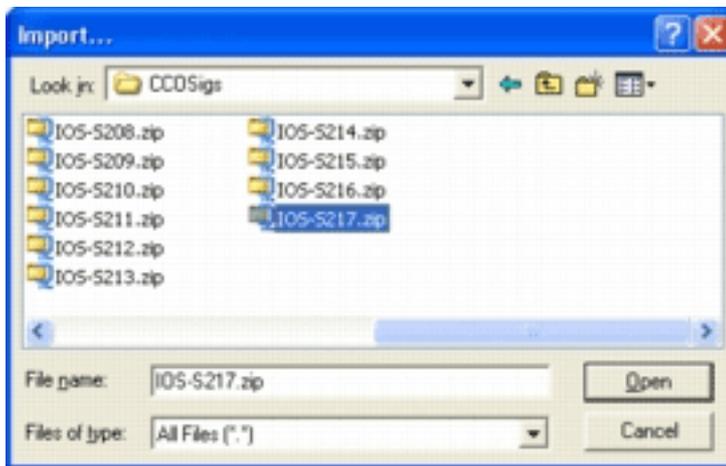
Procedimiento SDM 2.2

Después de que Cisco IOS IPS se haya habilitado, se pueden agregar nuevas firmas al router que ejecuta un conjunto de firmas con la función de importación de Cisco SDM. Complete estos pasos para importar nuevas firmas:

1. Elija los SDF predeterminados o el archivo de actualización IOS-Sxxx.zip para importar firmas adicionales.
2. Haga clic en **Configurar** y, a continuación, haga clic en **Prevención de intrusiones**.
3. Haga clic en la ficha **Edit IPS** y, a continuación, haga clic en **Import**.



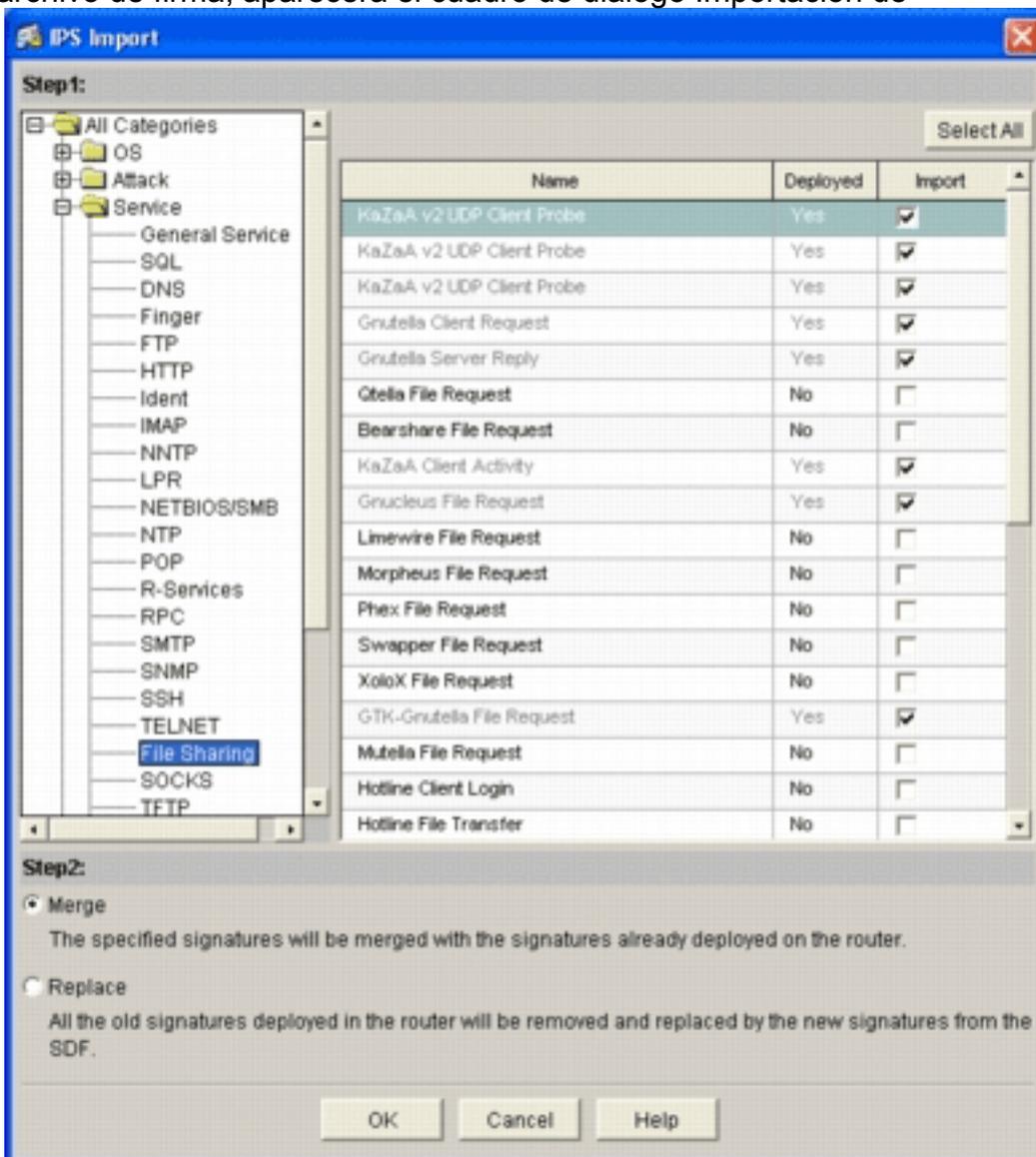
4. Elija **Desde PC** en la lista desplegable Importar.
5. Seleccione el archivo desde el que desea importar las



firmas.

En este ejemplo se utiliza la última actualización descargada de Cisco.com y guardada en el disco duro del equipo local.

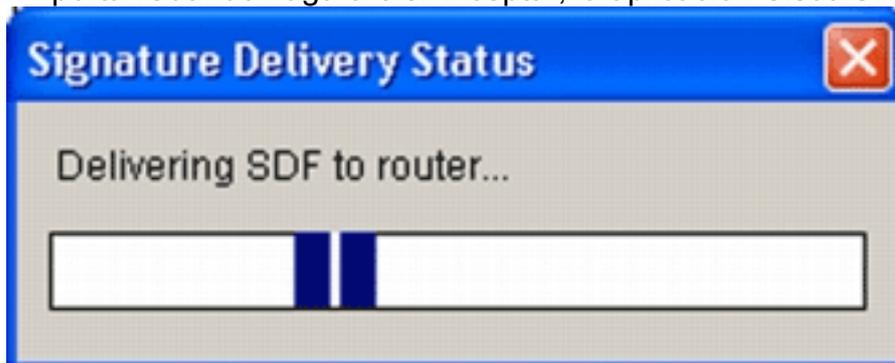
- Haga clic en **Abrir**. **Advertencia:** Debido a la restricción de memoria, sólo se puede agregar un número limitado de firmas nuevas a la parte superior de las firmas que ya se han implementado. Si se seleccionan demasiadas firmas, es posible que el router no pueda cargar todas las firmas nuevas debido a la falta de memoria. Cuando se complete la carga del archivo de firma, aparecerá el cuadro de diálogo Importación de



IPS.

- Desplácese por la vista de árbol izquierda y haga clic en la casilla de verificación **Importar** junto a las firmas que desea importar.
- Haga clic en el botón de opción **Combinar** y, a continuación, haga clic en **Aceptar**. **Nota:** La

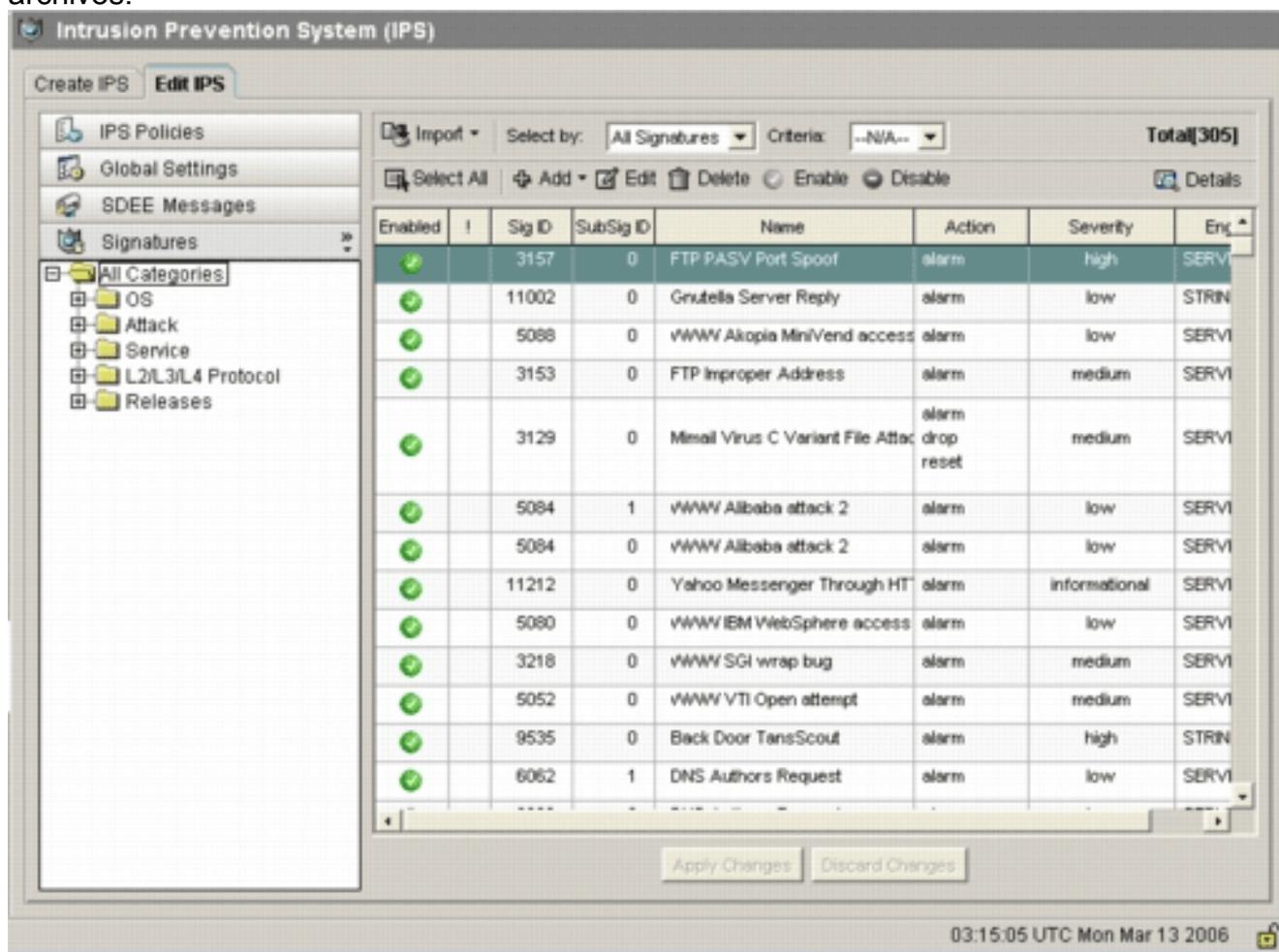
opción Reemplazar reemplaza el conjunto de firmas actual en el router con las firmas que seleccione para importar. Cuando haga clic en Aceptar, la aplicación Cisco SDM enviará las



firmas al router.

Nota:

Durante la compilación y la carga de firmas se produce un uso elevado de la CPU. Después de que Cisco IOS IPS esté habilitado en la interfaz, el archivo de firma comienza a cargarse. El router tarda unos cinco minutos en cargar el SDF. Puede intentar utilizar el comando **show process cpu** para ver la utilización de la CPU desde la CLI del software Cisco IOS. Sin embargo, no intente utilizar comandos adicionales ni cargar otros SDF mientras el router carga el SDF. Esto puede hacer que el proceso de compilación de la firma tarde más en completarse (ya que la utilización de la CPU se acerca al 100% en el momento de cargar el SDF). Es posible que deba examinar la lista de firmas y habilitarlas si no están en estado *habilitado*. El número total de firma ha aumentado a 519. Este número incluye todas las firmas disponibles en el archivo IOS-S193.zip que pertenecen a la subcategoría Compartir archivos.



Para obtener información sobre temas más avanzados sobre cómo utilizar Cisco SDM para administrar la función Cisco IOS IPS, consulte la documentación de Cisco SDM en esta URL:

Seleccionar firmas y trabajar con categorías de firmas

Para determinar cómo seleccionar de forma efectiva las firmas correctas para una red, debe saber algunas cosas sobre la red que está protegiendo. La información actualizada de la categoría de firma en Cisco SDM 2.2 y posteriores ayuda a los clientes a seleccionar el conjunto correcto de firmas para proteger la red.

La categoría es una forma de agrupar firmas. Ayuda a restringir la selección de firmas a un subconjunto de firmas que son relevantes entre sí. Una firma sólo puede pertenecer a una categoría o puede pertenecer a varias categorías.

Estas son las cinco categorías principales:

- SO: categorización de firmas basada en el sistema de operaciones
- Ataque: categorización de firma basada en ataques
- Servicio: categorización de firma basada en servicios
- Protocolo de capa 2-4: categorización de firma basada en protocolo
- Versiones: categorización de firmas basada en versiones

Cada una de estas categorías se divide en subcategorías.

Por ejemplo, considere una red doméstica con una conexión de banda ancha a Internet y un túnel VPN a la red corporativa. El router de banda ancha tiene Cisco IOS Firewall activado en la conexión abierta (no VPN) a Internet para evitar que cualquier conexión se origine desde Internet y se conecte a la red doméstica. Se permite todo el tráfico que se origina desde la red doméstica a Internet. Suponga que el usuario utiliza un PC basado en Windows y aplicaciones como HTTP (exploración web) y correo electrónico.

El firewall se puede configurar de modo que sólo las aplicaciones que necesita el usuario puedan fluir a través del router. Esto controlará el flujo de tráfico no deseado y potencialmente malo que puede propagarse por la red. Tenga en cuenta que el usuario de inicio no necesita ni utiliza un servicio específico. Si se permite que ese servicio fluya a través del firewall, existe un agujero potencial que un ataque puede utilizar para fluir por la red. Las prácticas recomendadas solo permiten los servicios necesarios. Ahora, es más fácil seleccionar qué firmas se van a habilitar. Debe activar las firmas sólo para los servicios que permita que fluyan a través del firewall. En este ejemplo, los servicios incluyen correo electrónico y HTTP. Cisco SDM simplifica esta configuración.

Para utilizar la categoría para seleccionar las firmas requeridas, elija **Service > HTTP**, y habilite todas las firmas. Este proceso de selección también funciona en el diálogo de importación de firmas, donde puede seleccionar todas las firmas HTTP e importarlas al router.

Las categorías adicionales que deben seleccionarse incluyen DNS, NETBIOS/SMB, HTTPS y SMTP.

Actualizar firmas para archivos SDF predeterminados

Los tres SDFs por construcción (attack-drop.dsF, 128MB.sdf y 256MB.sdf) se encuentran actualmente disponibles en Cisco.com en <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup> (sólo clientes [registrados](#)). Las versiones más recientes de estos archivos se publicarán tan pronto como estén disponibles. Para actualizar los routers que ejecutan Cisco IOS IPS con estos SDF predeterminados, vaya al sitio web y descargue las últimas versiones de estos archivos.

Procedimiento CLI

1. Copie los archivos descargados en la ubicación desde la que se ha configurado el router para cargar estos archivos. Para averiguar dónde está configurado actualmente el router, utilice el comando **show running-config | in ip ips sdf**.

```
Router#show running-config | in ip ips sdf
ip ips sdf location flash://256MB.sdf autosave
```

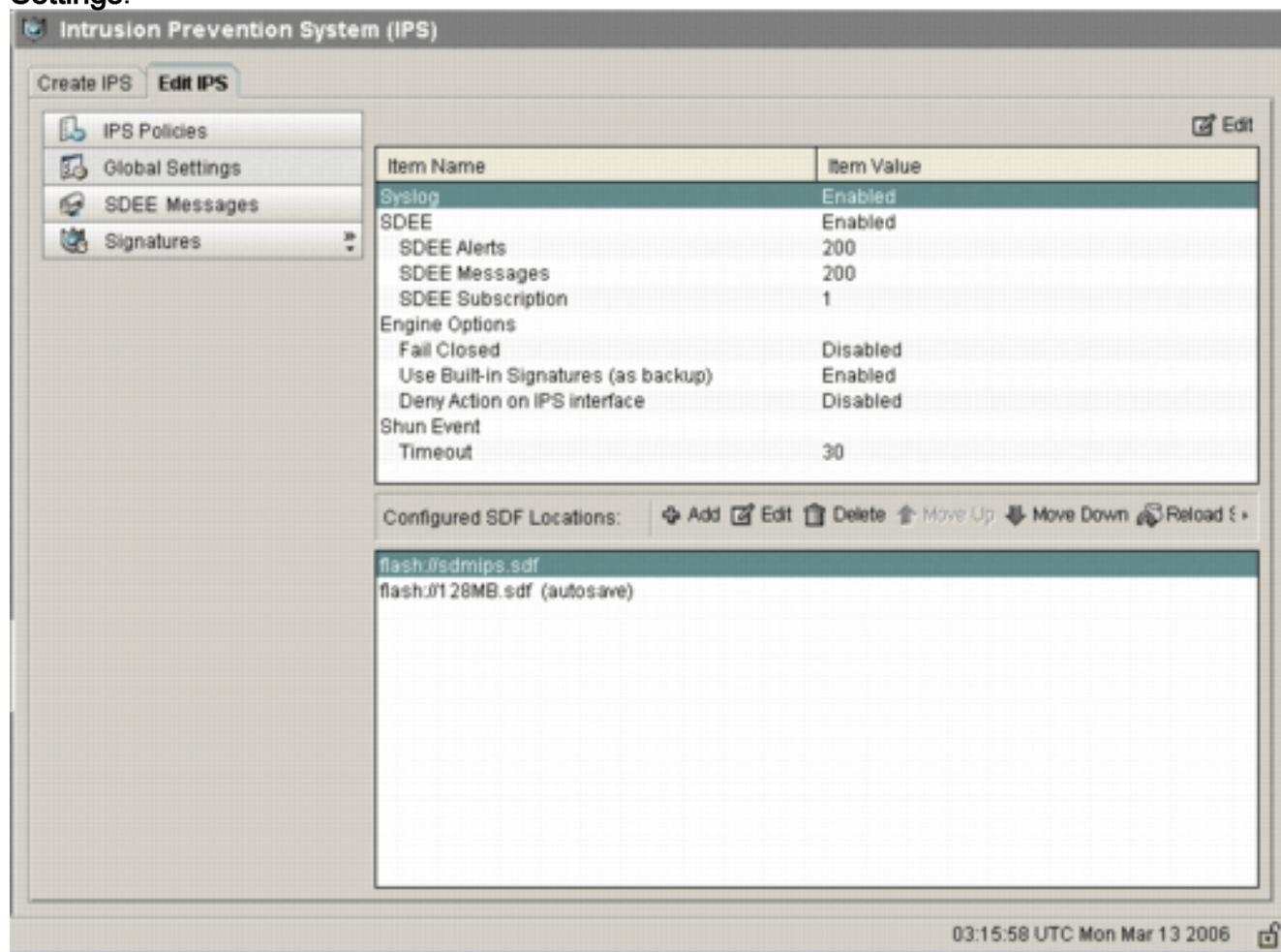
En este ejemplo, el router utiliza 256MB.sdf en la memoria flash. El archivo se actualiza cuando copia el nuevo archivo descargado 256MB.sdf en la memoria flash del router.

2. Recargue el subsistema IPS de Cisco IOS para ejecutar los nuevos archivos. Hay dos maneras de recargar Cisco IOS IPS: recargue el router o vuelva a configurar Cisco IOS IPS para activar el subsistema IOS IPS para recargar las firmas. Para reconfigurar Cisco IOS IPS, quite todas las reglas IPS de las interfaces configuradas y luego vuelva a aplicar las reglas IPS a las interfaces. Esto activará la recarga del sistema IPS de Cisco IOS.

Procedimiento SDM 2.2

Complete estos pasos para actualizar los SDF predeterminados en el router:

1. Haga clic en **Configurar** y, a continuación, haga clic en **Prevención de intrusiones**.
2. Haga clic en la ficha **Edit IPS** y, a continuación, haga clic en **Global Settings**.



The screenshot displays the 'Intrusion Prevention System (IPS)' configuration page. The 'Edit IPS' tab is active, and the 'Global Settings' section is selected in the left-hand navigation pane. The main area shows a table of configuration items and a list of SDF locations.

Item Name	Item Value
syslog	Enabled
SDEE	Enabled
SDEE Alerts	200
SDEE Messages	200
SDEE Subscription	1
Engine Options	
Fail Closed	Disabled
Use Built-in Signatures (as backup)	Enabled
Deny Action on IPS interface	Disabled
Shun Event	
Timeout	30

Configured SDF Locations: Add Edit Delete Move Up Move Down Reload

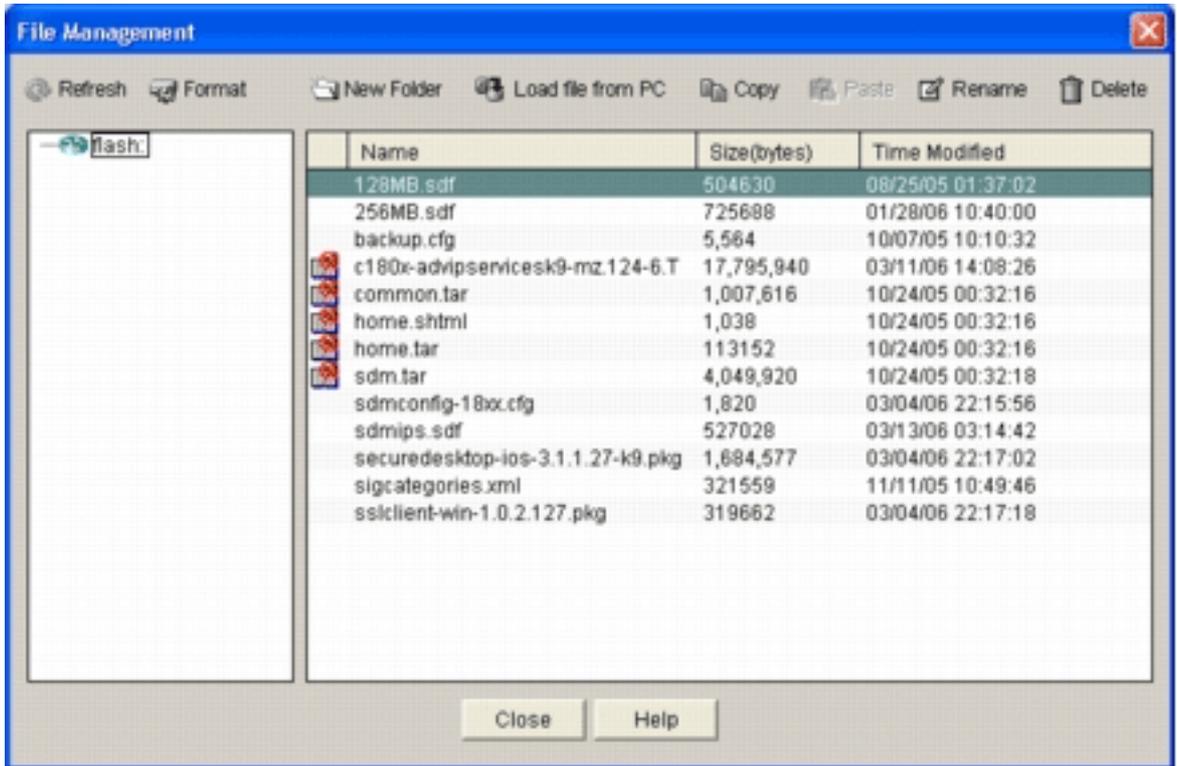
- flash://sdmips.sdf
- flash://128MB.sdf (autosave)

03:15:58 UTC Mon Mar 13 2006

La parte superior de la interfaz de usuario muestra la configuración global. La mitad inferior de la interfaz de usuario muestra las ubicaciones SDF configuradas actualmente. En este caso, se configura el archivo 256MB.sdf de la memoria flash.

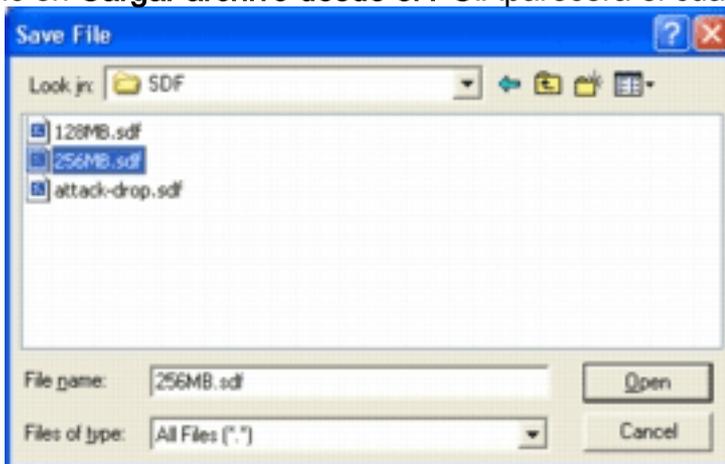
3. Elija **Administración de archivos** en el menú Archivo. Aparecerá el cuadro de diálogo

Administración de



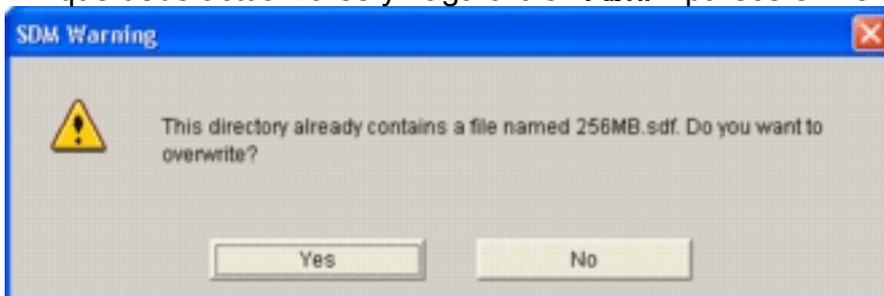
archivos.

4. Haga clic en **Cargar archivo desde el PC**. Aparecerá el cuadro de diálogo Guardar



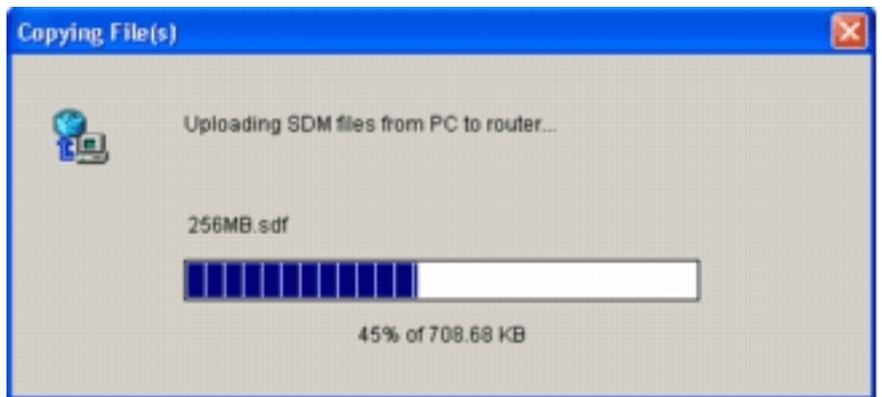
archivo.

5. Elija el SDF que debe actualizarse y haga clic en **Abrir**. Aparece el mensaje de advertencia



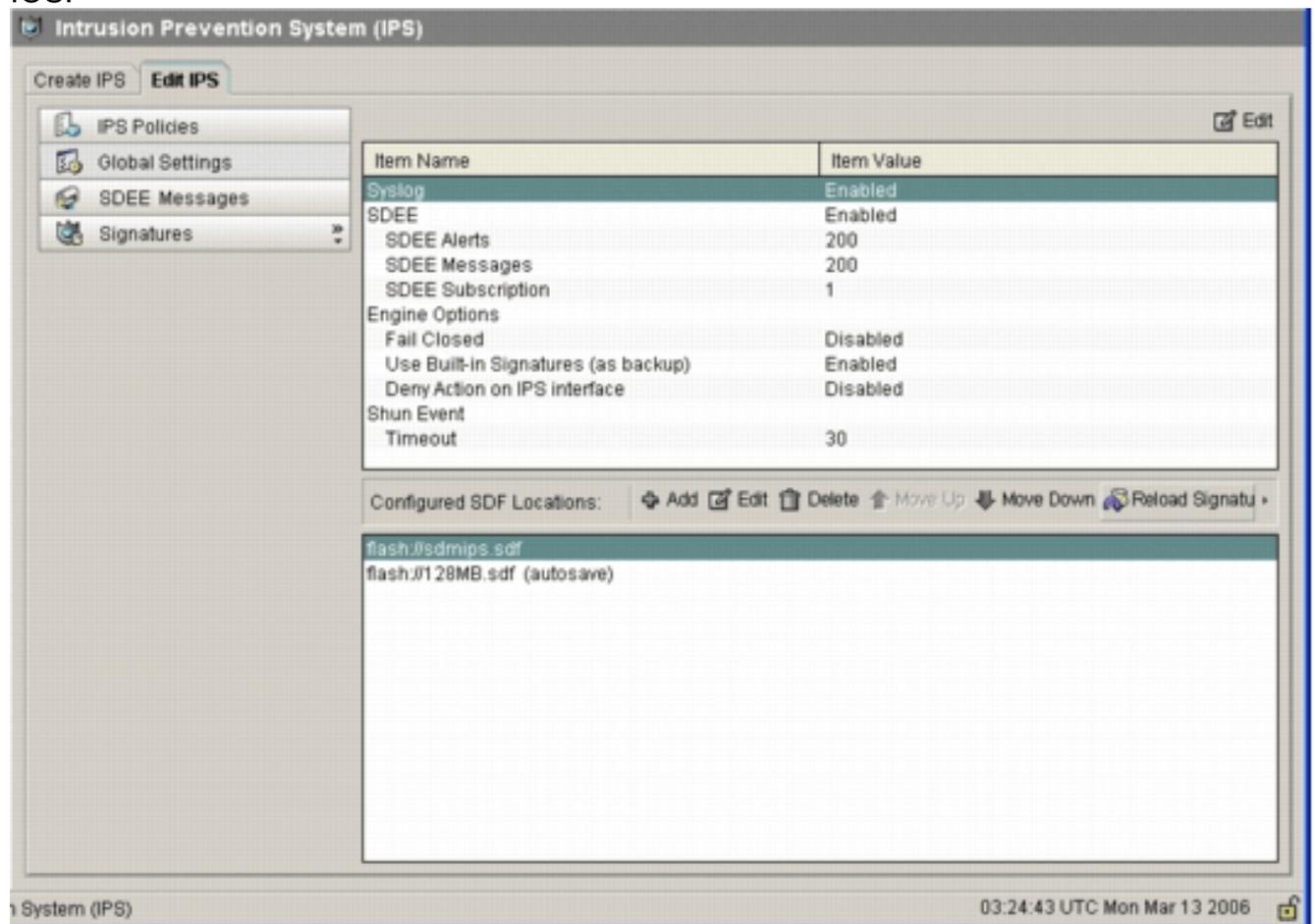
de SDM.

6. Haga clic en **Yes** para reemplazar el archivo existente. Un cuadro de diálogo muestra el



progreso del proceso de carga.

- Una vez que el proceso de carga haya finalizado, haga clic en **Recargar firmas** en la barra de herramientas de ubicación de SDF. Esta acción recarga el IPS de Cisco IOS.



Nota: El paquete IOS-Sxxx.zip contiene todas las firmas que admite Cisco IOS IPS. Las actualizaciones de este paquete de firma se publican en Cisco.com en cuanto estén disponibles. Para actualizar las firmas contenidas en este paquete, vea el [Paso 2](#).

[Información Relacionada](#)

- [Cisco Intrusion Prevention System](#)
- [Avisos de campo de productos de seguridad \(incluida CiscoSecure Intrusion Detection\)](#)
- [Soporte Técnico - Cisco Systems](#)