# Router y Administrador de dispositivos de seguridad en el ejemplo de configuración del sistema de prevención de intrusiones del Cisco IOS

## Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Configurar](#)
[Información Relacionada](#)

## Introducción

Este documento describe cómo utilizar la versión 2.5 del (SDM) de Router de Cisco y Administrador de dispositivo de seguridad para configurar el Sistema de prevención de intrusiones (IPS) del ® del Cisco IOS en y posterior las versiones 12.4(15)T3.

Las mejoras en el SDM 2.5 relacionado a IOS IPS son:

- Sume el número compilado de la firma visualizado en la lista de firma GUI
- Archivos de firma del SDM (archivo zip formato; por ejemplo, sigv5-SDM-S307.zip) y paquetes de la firma CLI (formato de archivo de paquete; por ejemplo, IOS-S313-CLI.pkg) se puede descargar junto en una operación
- Los paquetes descargados de la firma se pueden avanzar automáticamente al router como opción

Las tareas implicadas en el proceso de abastecimiento inicial son:

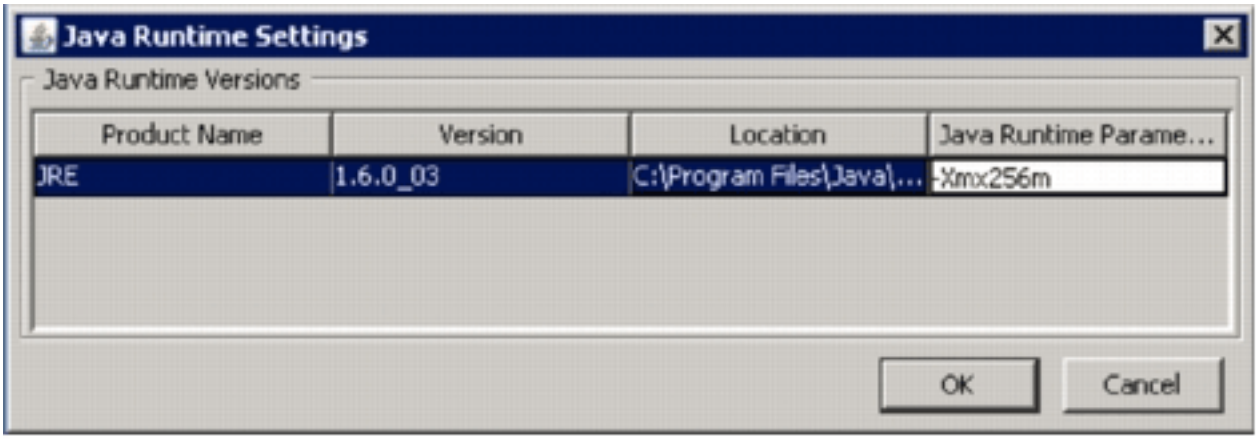
1. Descargue y instale el SDM 2.5.
2. Utilice la actualización auto del SDM para descargar el paquete de la firma IOS IPS a PC local.
3. Inicie al Asisitente de las directivas IPS para configurar IOS IPS.
4. Verifique que la configuración y las firmas IOS IPS estén cargadas correctamente

El SDM de Cisco es una herramienta de configuración basada en web que simplifica el router y la Configuración de seguridad a través de los Asisitente elegantes que ayudan a los clientes de manera rápida y fácil a desplegar, a configurar, y a monitorear a un router Cisco sin requerir el conocimiento del comando line interface(cli).

La versión 2.5 del SDM se puede descargar de Cisco.com en http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (clientes registrados solamente). El Release Note se puede encontrar en http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

**Note**: El SDM de Cisco requiere una resolución de la pantalla de por lo menos 1024 x 768.

**Note**: El SDM de Cisco requiere el tamaño del almacenamiento dinámico de memoria de las Javas estar ningún menos que 256MB para configurar IOS IPS. Para cambiar el tamaño del almacenamiento dinámico de memoria de las Javas, abra el panel de control Java, haga clic la lengueta de las **Javas**, haga clic la **visión** situada bajo configuraciones del Runtime de la Java Applet, y después ingrese **-Xmx256m** en el motor de ejecución Java columna parameter (parámetro).




# prerrequisitos

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS IPS en y posterior las versiones 12.4(15)T3
- Versión 2.5 del (SDM) de Router de Cisco y Administrador de dispositivo de seguridad

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

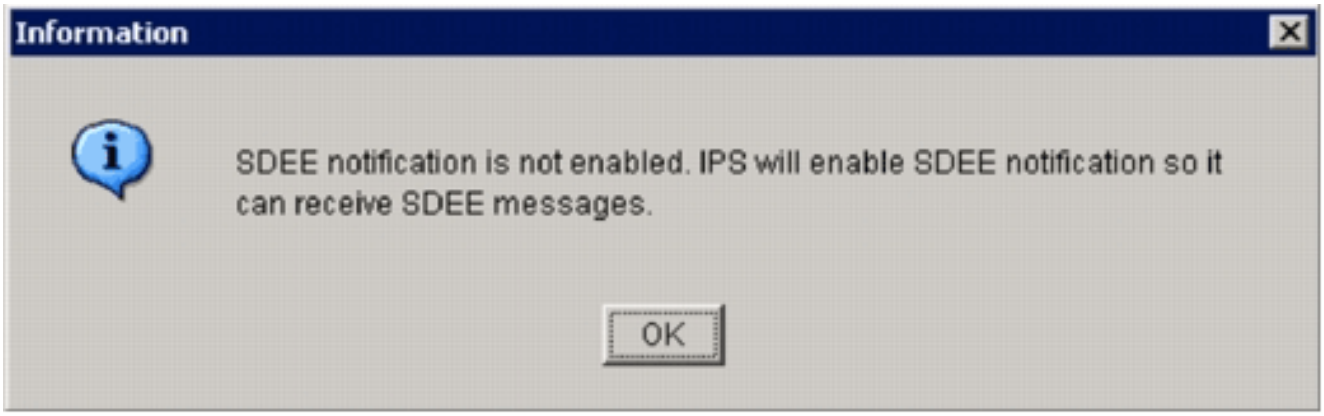
Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

# Configurar

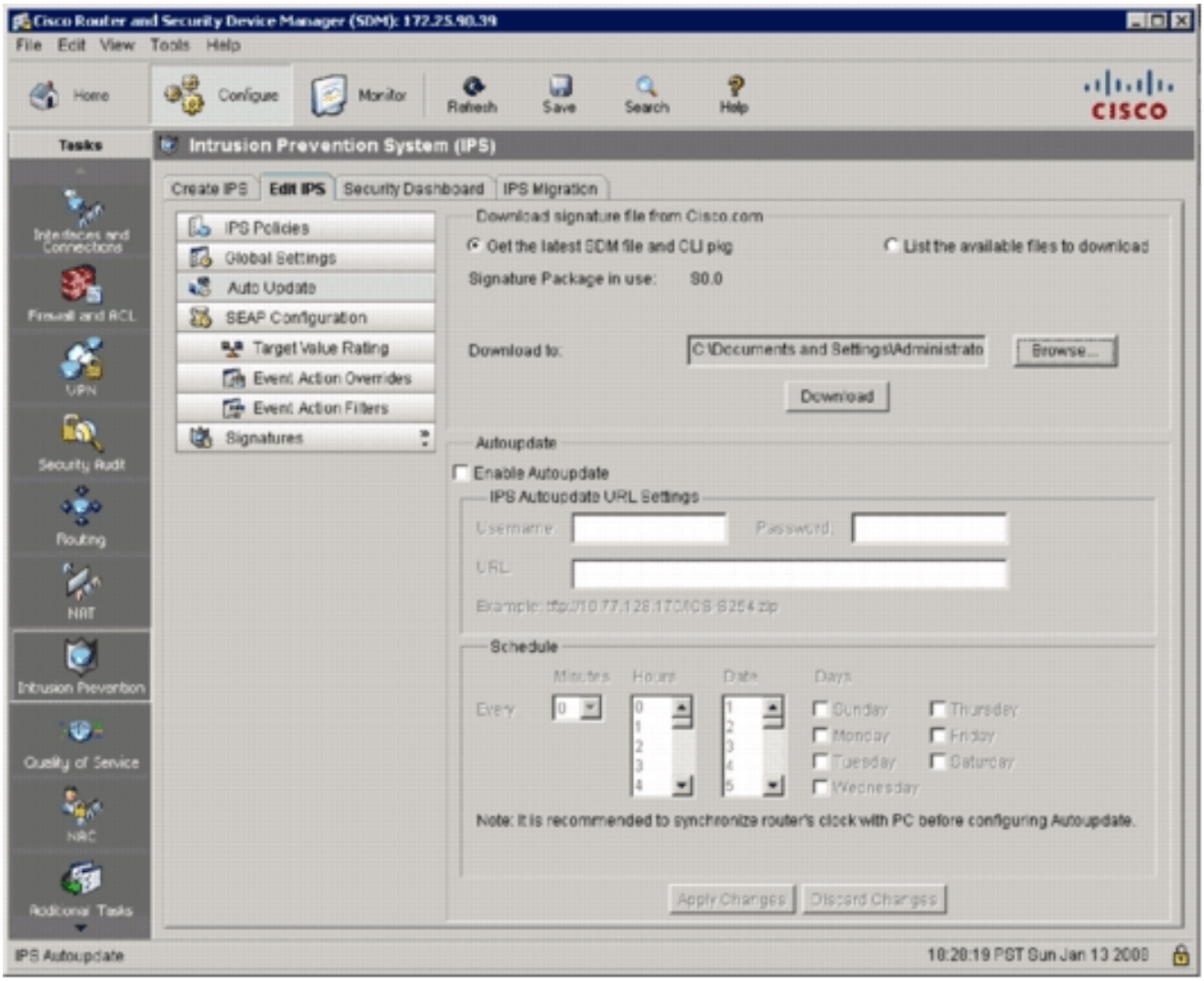
**Note**: Abra una consola o sesión Telnet en el router (con el “monitor del término” encendido) para monitorear los mensajes cuando usted utiliza el SDM para provision IOS IPS.

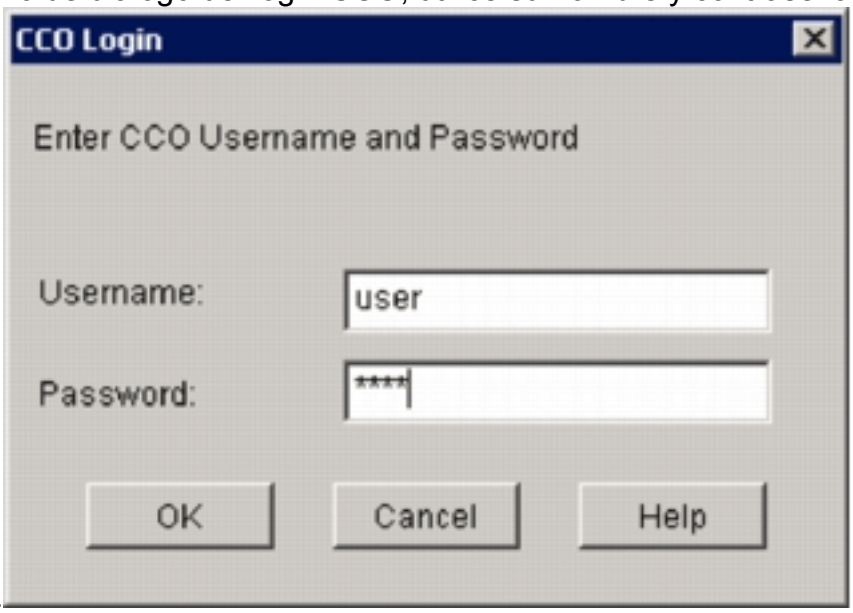
1. Descargue el SDM 2.5 del cisco.com en http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (clientes registrados solamente) y instalelo en a PC local.
2. Ejecute el SDM 2.5 del PC local.
3. Cuando aparece el cuadro de diálogo del login IOS IPS, ingrese el mismo Nombre de usuario y contraseña que usted utiliza para la autenticación del SDM al router.


4. De la interfaz de usuario del SDM, haga clic la **configuración**, y después haga clic la **prevención de intrusiones**.
5. Haga clic la lengueta **IPS del editar**.
6. Si la notificación SDEE no se habilita en el router, haga clic la **AUTORIZACIÓN** para habilitar la notificación SDEE.

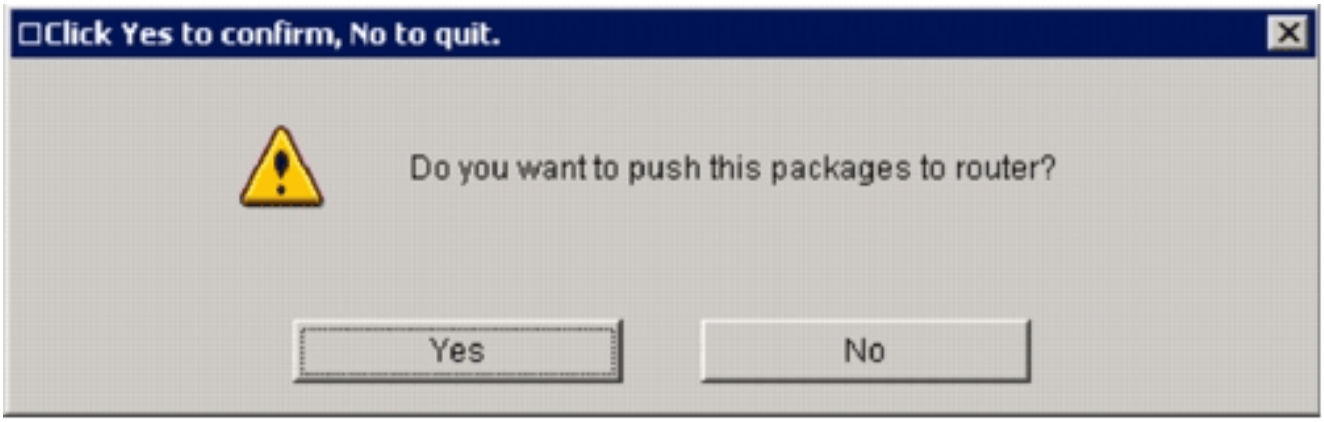



7. En el archivo de firma de la descarga del área del cisco.com de la lengueta IPS del editar, haga clic el **conseguir el último archivo del SDM y** botón de radio del **paquete CLI**, y después haga clic **hojean** para seleccionar un directorio en su PC local adentro que salvar los archivos descargados.Usted puede elegir el directorio raíz TFTP o del servidor FTP, que será utilizado más adelante cuando usted despliega el paquete de la firma al router.
8. Haga clic en **Descarga**.

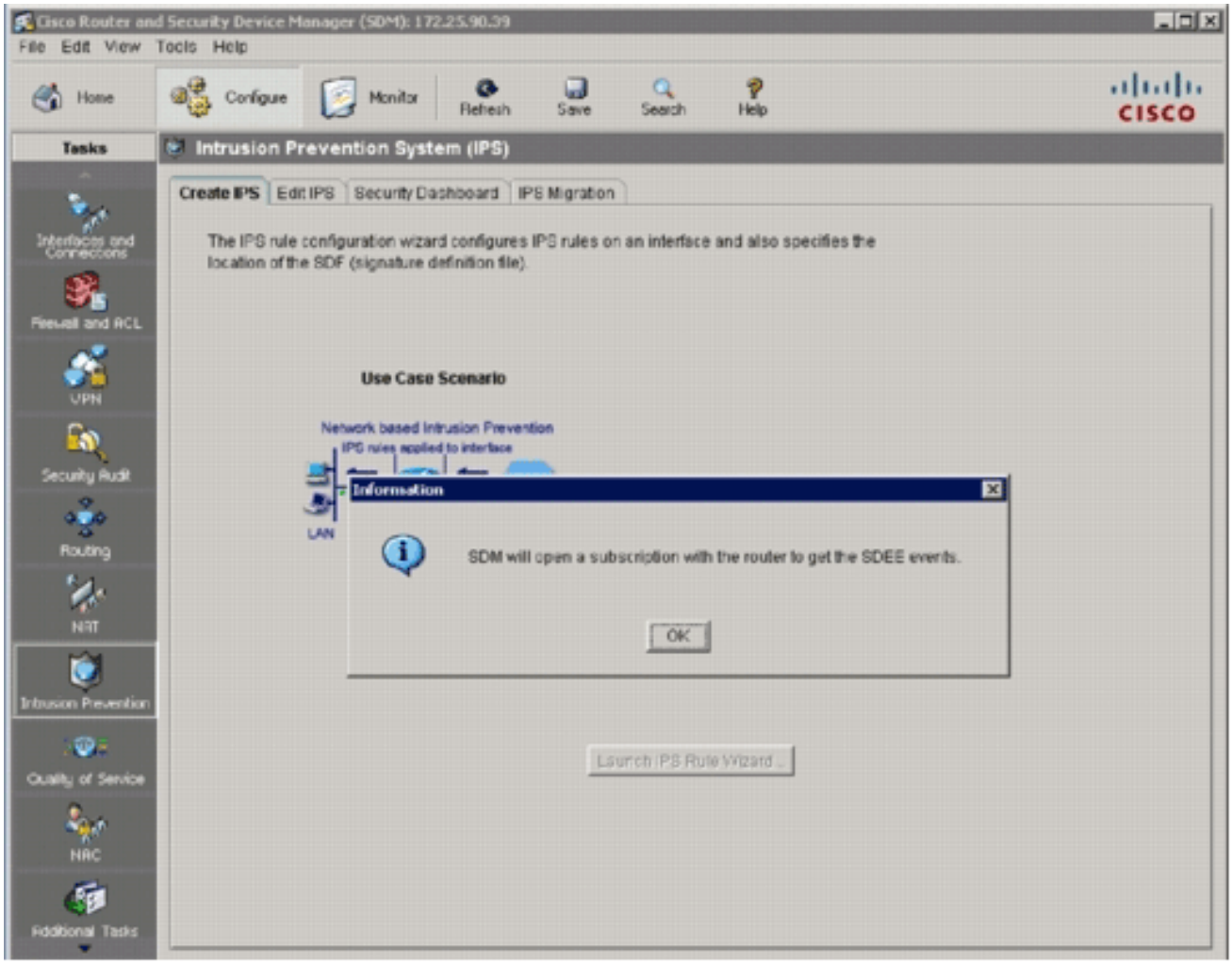



9. Cuando aparece el cuadro de diálogo del login CCO, utilice su nombre y contraseña de usuario registrado CCO. 

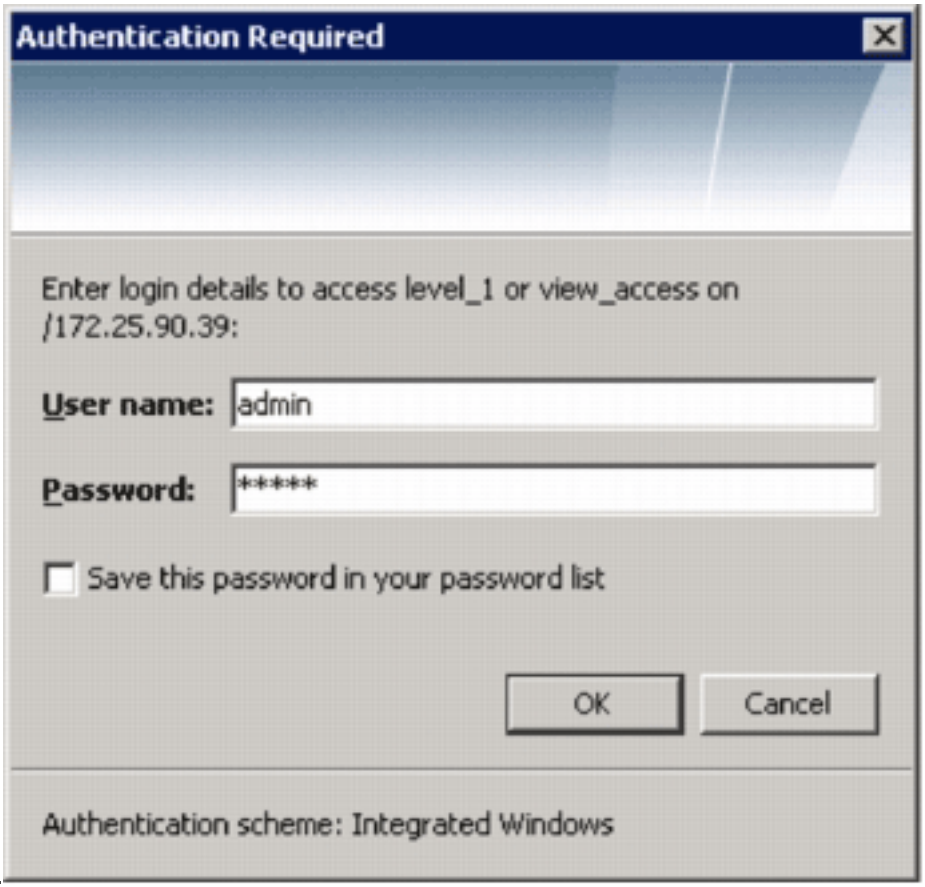
El SDM conecta con el cisco.com y comienza a descargar ambos el archivo del SDM (por ejemplo, sigv5-SDM-S307.zip) y el archivo de paquete CLI (por ejemplo, IOS-S313-CLI.pkg) al directorio seleccionado en el paso 7.Una vez que se descargan ambos archivos, el SDM le indica a que avance el paquete descargado de la firma al router.




10. Haga clic **ningún** puesto que el IOS IPS no se ha configurado en el router todavía.
11. Después de que el SDM descargue el último IOS CLI paquete de la firma, haga clic la lengueta **IPS del crear** para crear la configuración inicial IOS IPS.
12. Si a le indican que aplique los cambios al router, el tecleo **aplica los cambios**.
13. **Asisitente de la regla IPS del lanzamiento del** tecleo.Un cuadro de diálogo aparece informarle que las necesidades del SDM de establecer una suscripción SDEE al router para extraer las
    alertas.

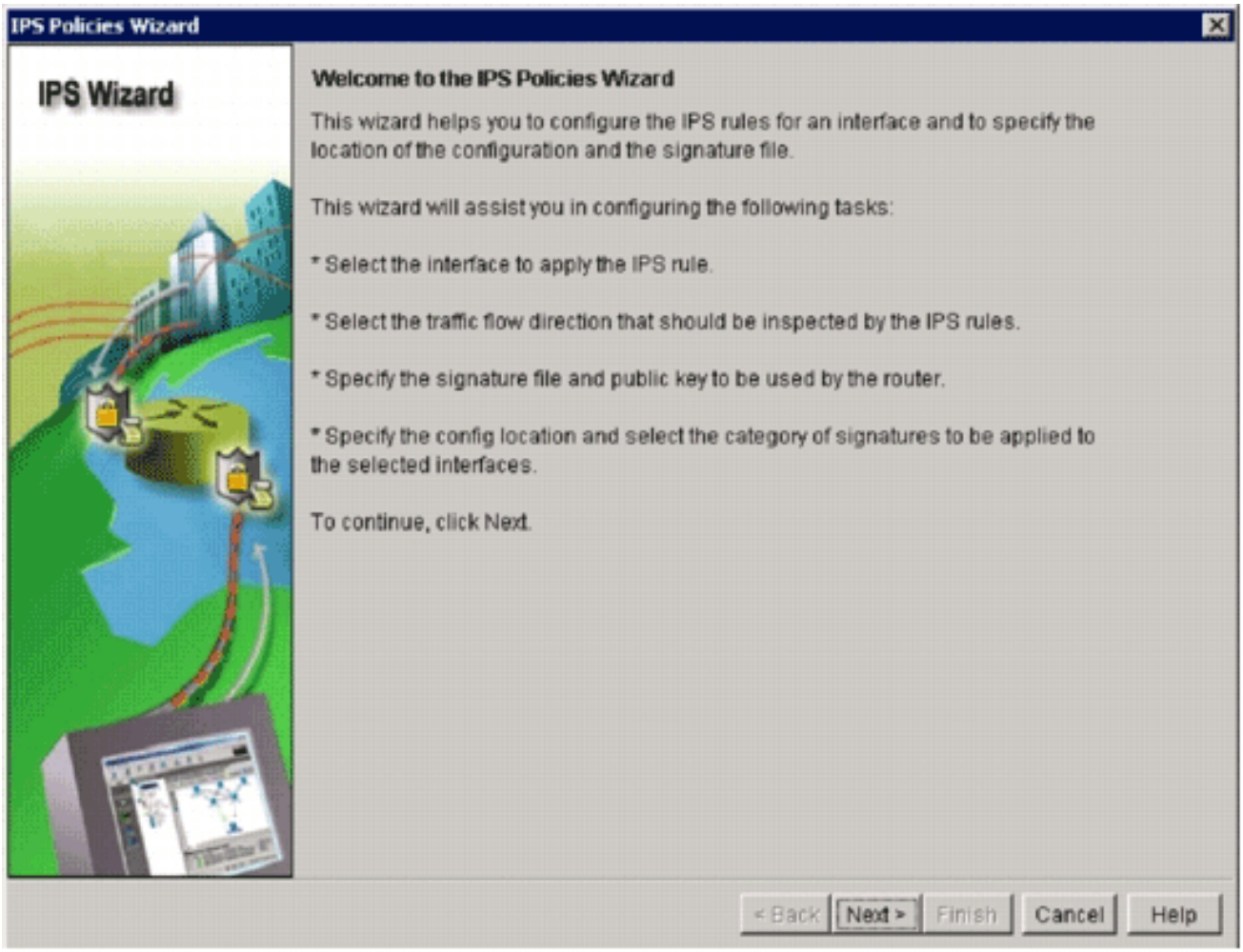



14. Click OK.La autenticación requirió el cuadro de diálogo

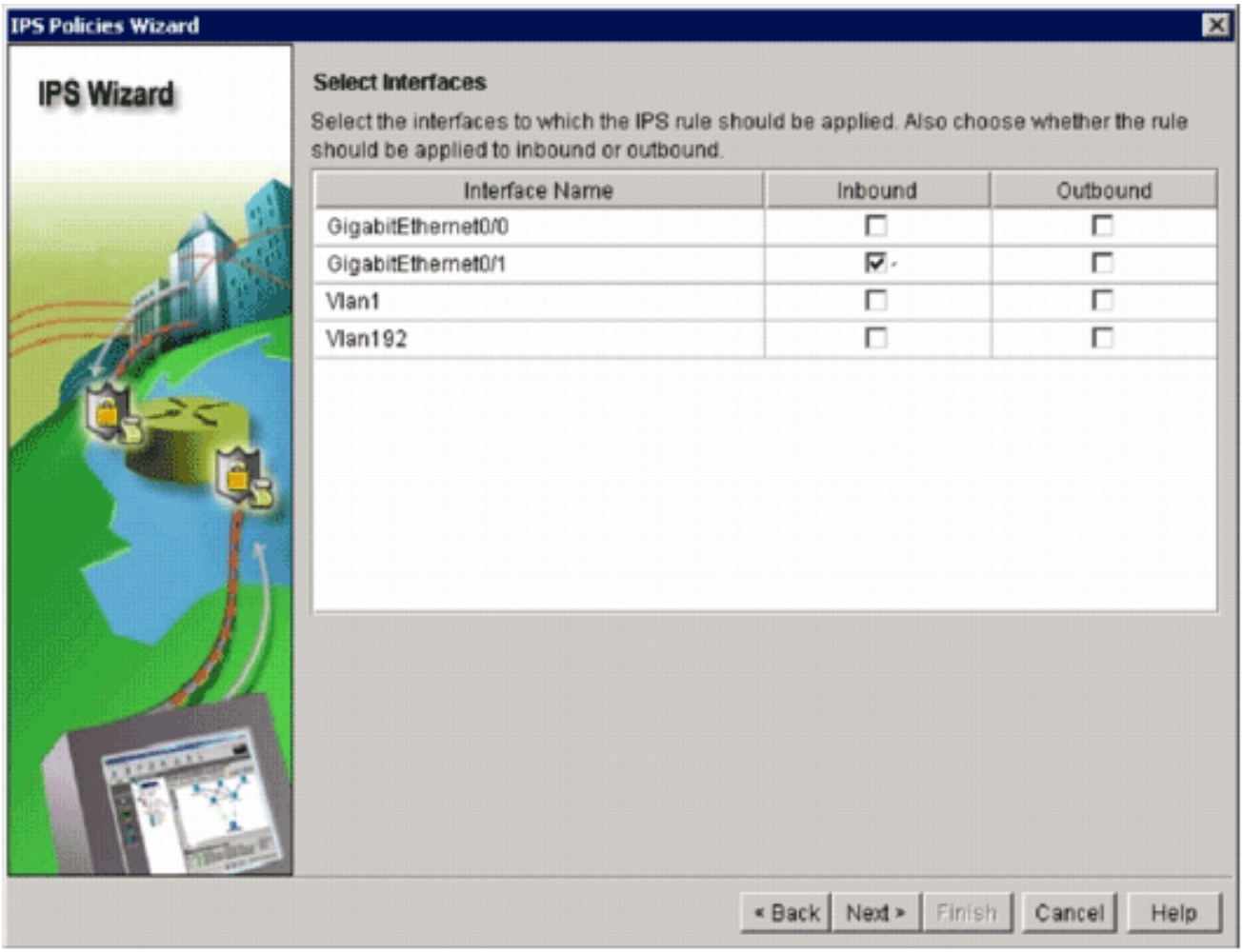



aparece.

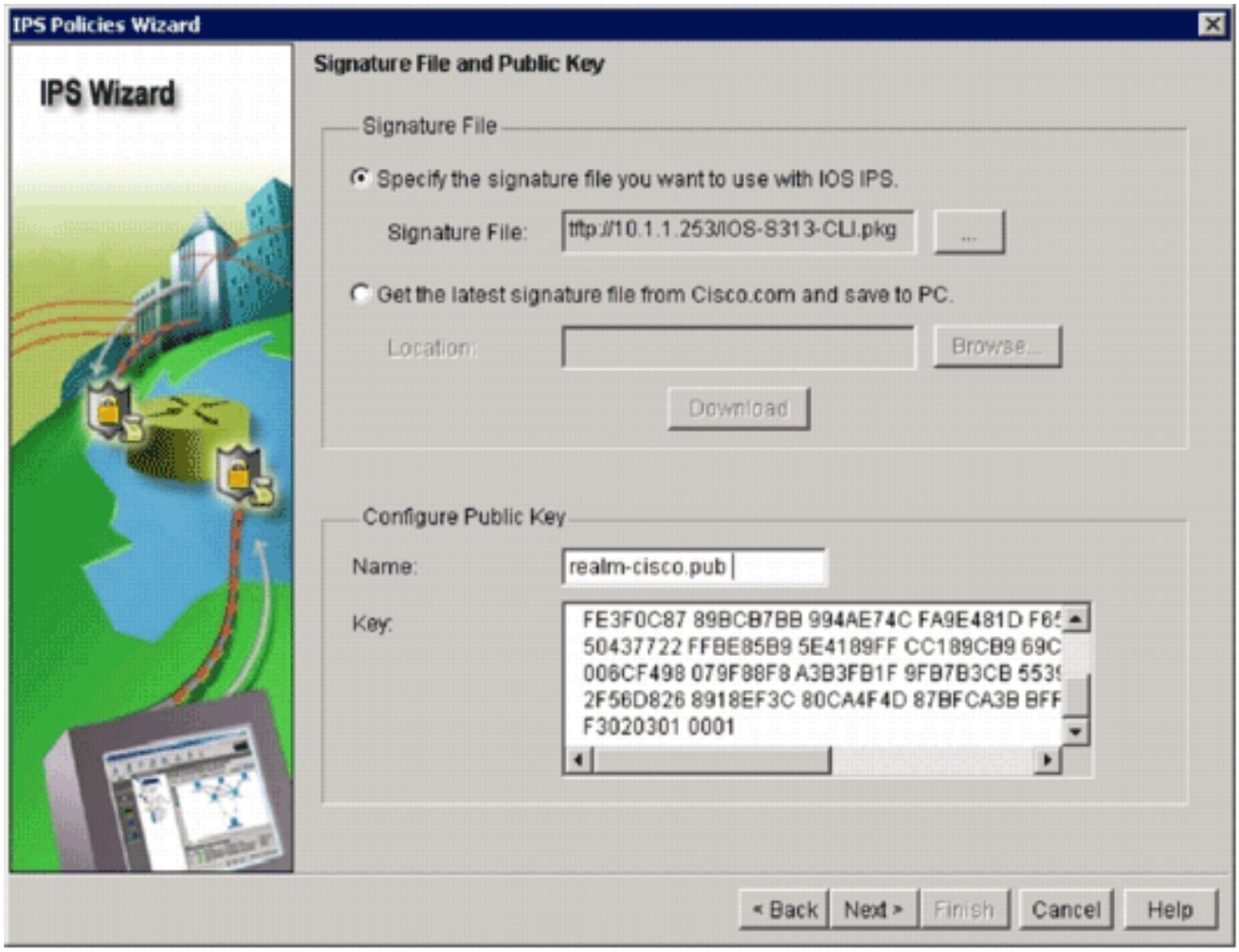
15. Ingrese el Nombre de usuario y la contraseña que usted utilizó para el SDM para autenticar al router, y haga clic la **AUTORIZACIÓN**.El cuadro de diálogo del Asisitente de las directivas IPS
    aparece.



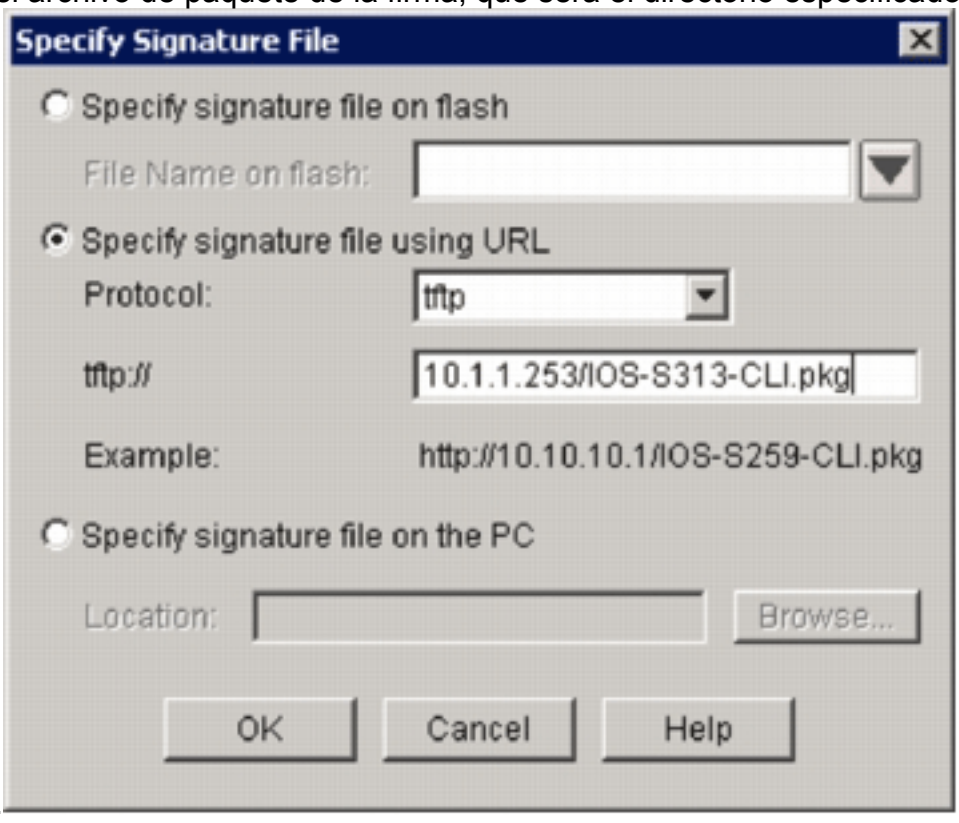

16. Haga clic en Next (Siguiente).




17. En la ventana de las interfaces seleccionadas, elija la interfaz y la dirección a las cuales ese IOS IPS será aplicado, y después haga clic **al lado de** continúan.




18. En el área del archivo de firma de la ventana del archivo de firma y de la clave pública, haga clic el **especificar el archivo de firma que usted quiere utilizar con el** botón de radio **IOS IPS**, y después haga clic el botón del **archivo de firma** (...) para especificar la ubicación del archivo de paquete de la firma, que será el directorio especificado en el paso




7.

19. Haga clic el **archivo de firma del especificar usando el** botón de radio **URL**, y elija un

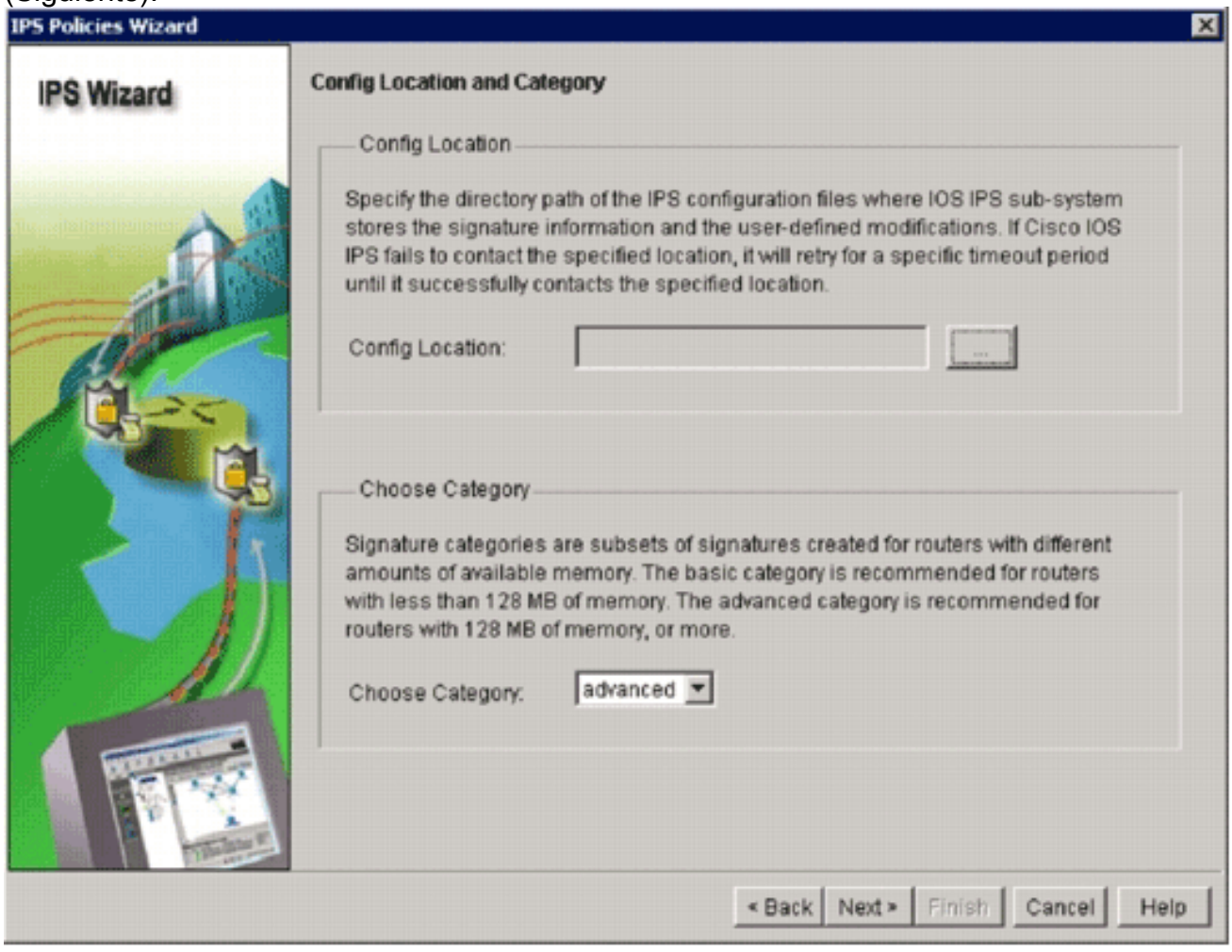
protocolo de la lista desplegable del protocolo.**Note**: Este ejemplo utiliza el TFTP para descargar el paquete de la firma al router.

20. Ingrese el URL para el archivo de firma, y haga clic la **AUTORIZACIÓN**.
21. En el área de la clave pública de la configuración de la ventana del archivo de firma y de la clave pública, ingrese **realm-cisco.pub en el** campo de nombre, y entonces copie esta clave pública y pegúela en el campo clave.

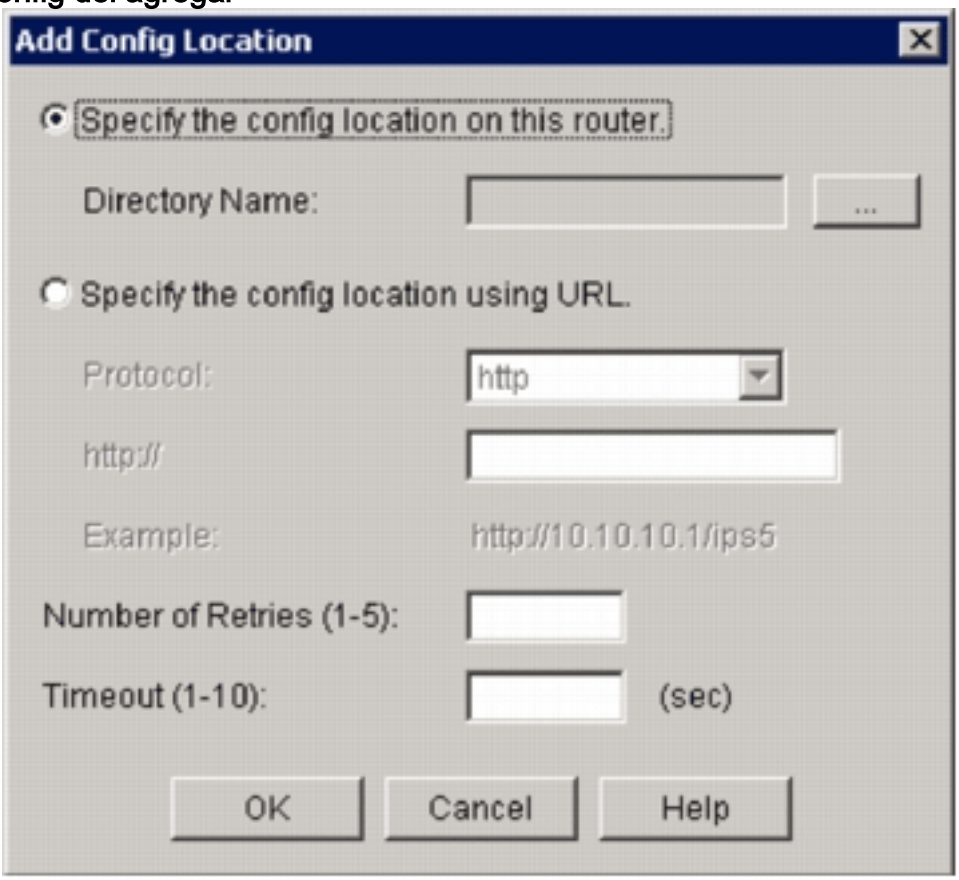
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001
```

**Note**: Esta clave pública puede ser descarga del cisco.com en: [http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup](http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup) (clientes registrados solamente).

22. Para continuar, haga clic en Next (Siguiente).

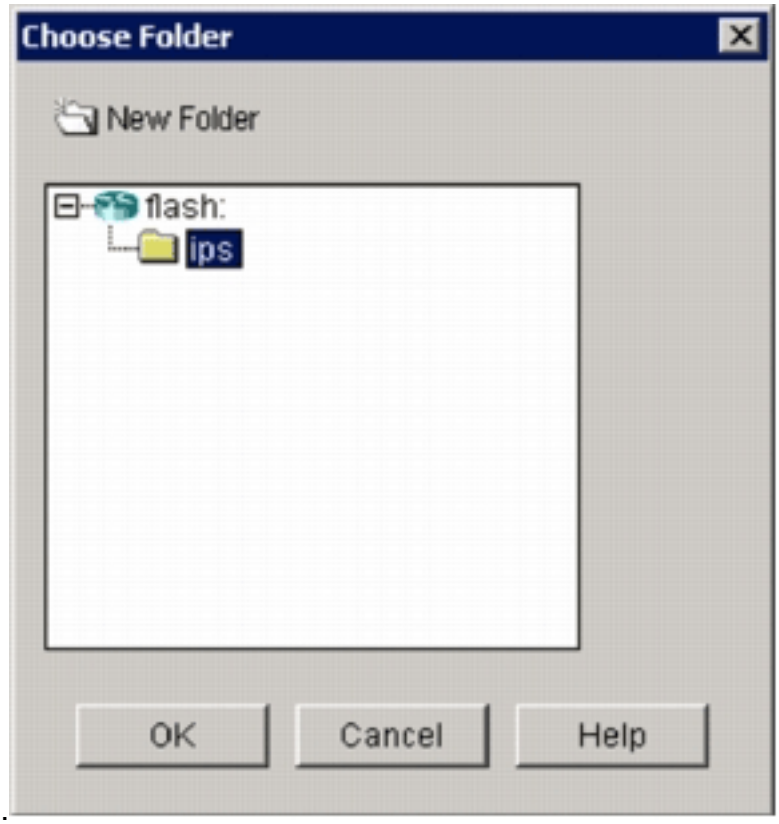


23. En la ventana de la ubicación y de la categoría de los Config, haga clic el botón de la **ubicación de los Config** (...) para especificar una ubicación en donde la definición y los archivos de configuración de las firmas serán salvados.El cuadro de diálogo de la **ubicación de los Config del agregar**



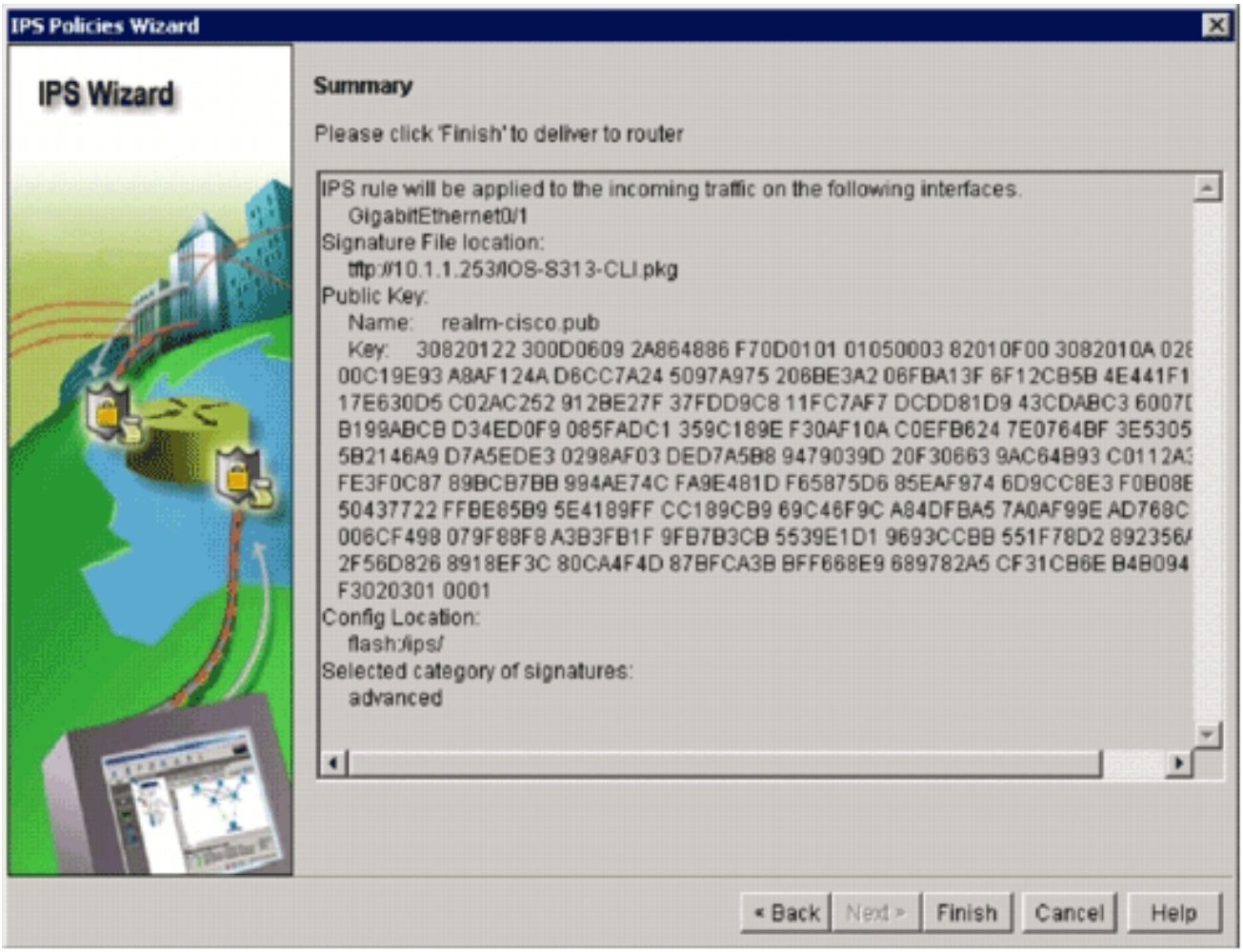

aparece.

24. En el cuadro de diálogo de la ubicación de los Config del agregar, haga clic el **especificar la ubicación de los config en este** botón de radio del **router**, y después haga clic **Directory Name (Nombre de directorio) el** botón (...) para localizar el archivo de configuración.El cuadro de diálogo de la carpeta del elegir aparece para permitir que usted seleccione un directorio existente o que cree un nuevo directorio en memoria Flash del router para salvar la definición y los archivos de configuración de la

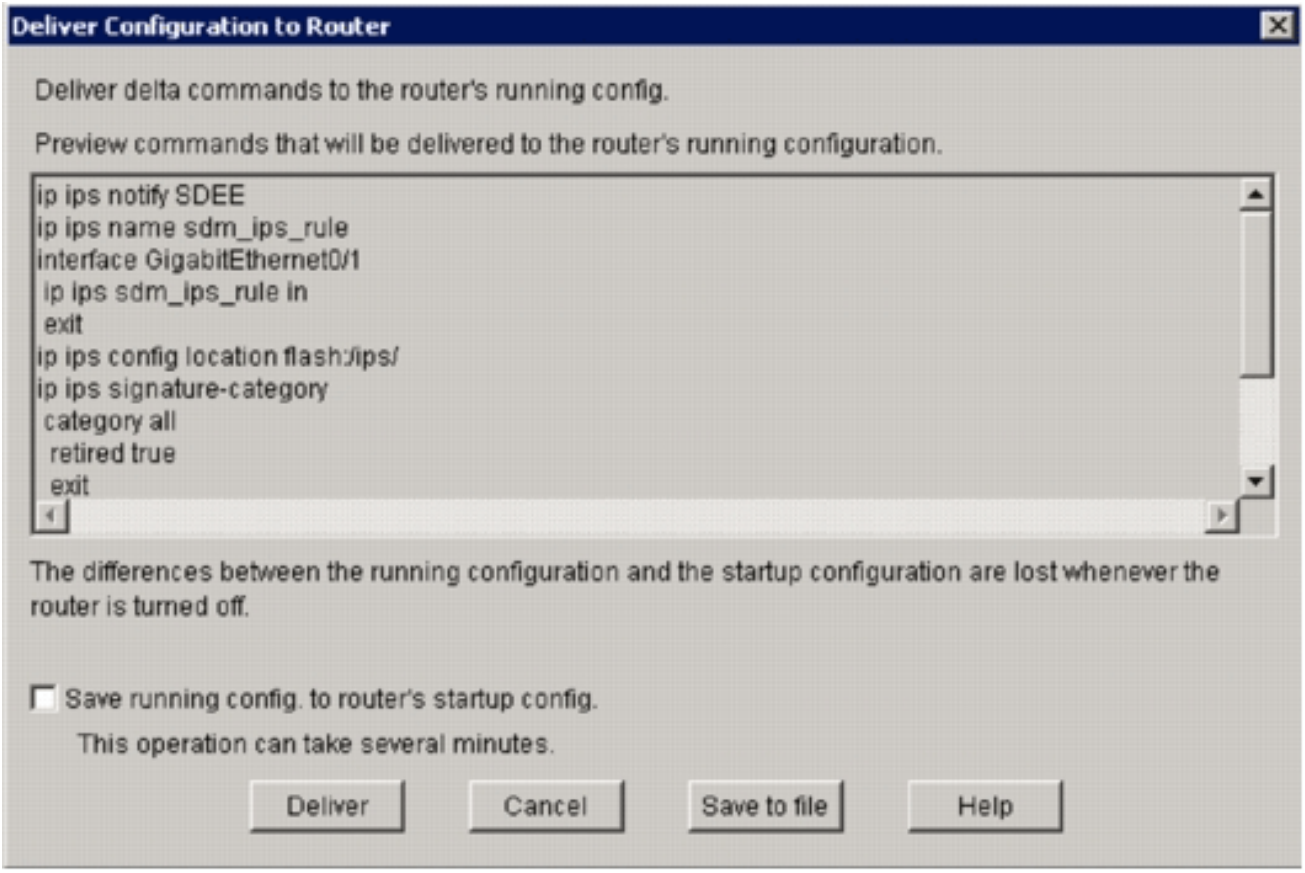


firma.

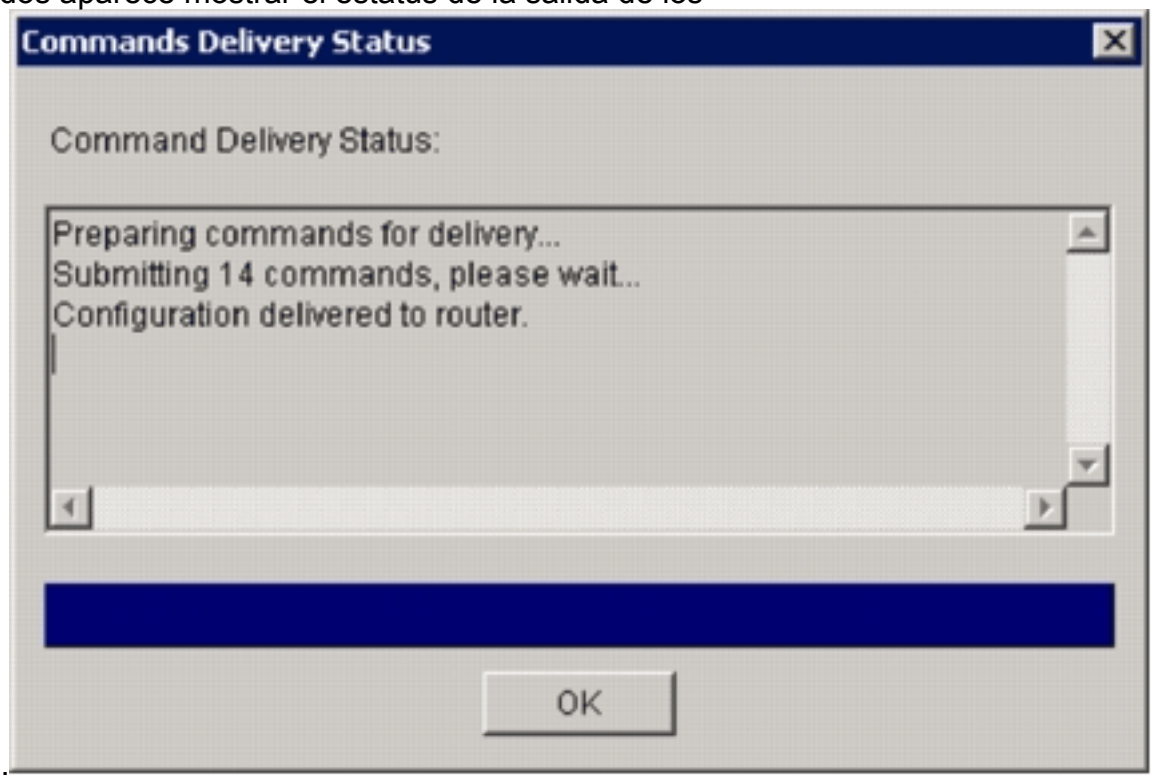
25. Haga clic la **nueva carpeta** situada en la cima del cuadro de diálogo si usted quiere crear un nuevo directorio.
26. Una vez que usted selecciona el directorio, haga clic la **AUTORIZACIÓN** para aplicar los cambios, y después haga clic la **AUTORIZACIÓN** para cerrar el cuadro de diálogo de la ubicación de los Config del agregar.
27. En el cuadro de diálogo del Asisitente de las directivas IPS, seleccione la categoría de la firma según la cantidad de memoria instalada en el router. Hay dos categorías de la firma que usted puede elegir en el SDM: Básico y avanzado.Si el router hace 128MB DRAM instalar, Cisco recomienda que usted elige la categoría básica para evitar las fallas de asignación de memoria. Si el router hace 256MB o más DRAM instalar, usted puede elegir cualquier categoría.
28. Una vez que usted selecciona una categoría para utilizar, hacer clic **después** para continuar a la página de resumen.La página de resumen proporciona una Breve descripción sobre la configuración inicial IOS IPS de las
tareas.




29. Clic en Finalizar en la página de resumen para entregar las configuraciones y el paquete de la firma al router.Si habilitan a los comandos option del avance en las configuraciones de las preferencias en el SDM, el SDM visualiza la configuración de la entrega al cuadro de diálogo del router que muestra un resumen de comandos CLI que el SDM entregue al router.

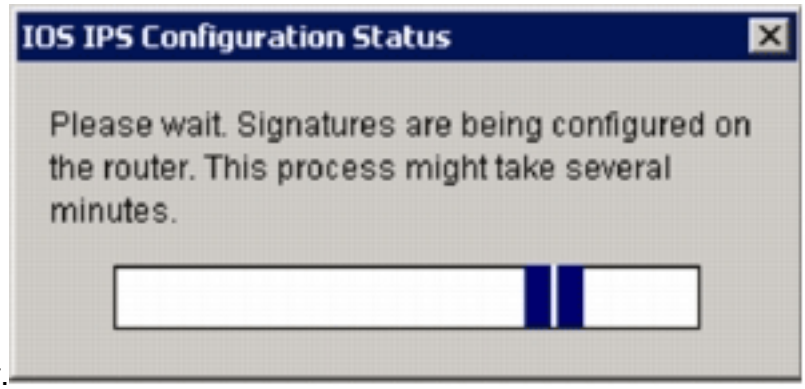



30. El tecleo **entrega** para proceder.El cuadro del cuadro de diálogo de estado de la salida de los comandos aparece mostrar el estatus de la salida de los



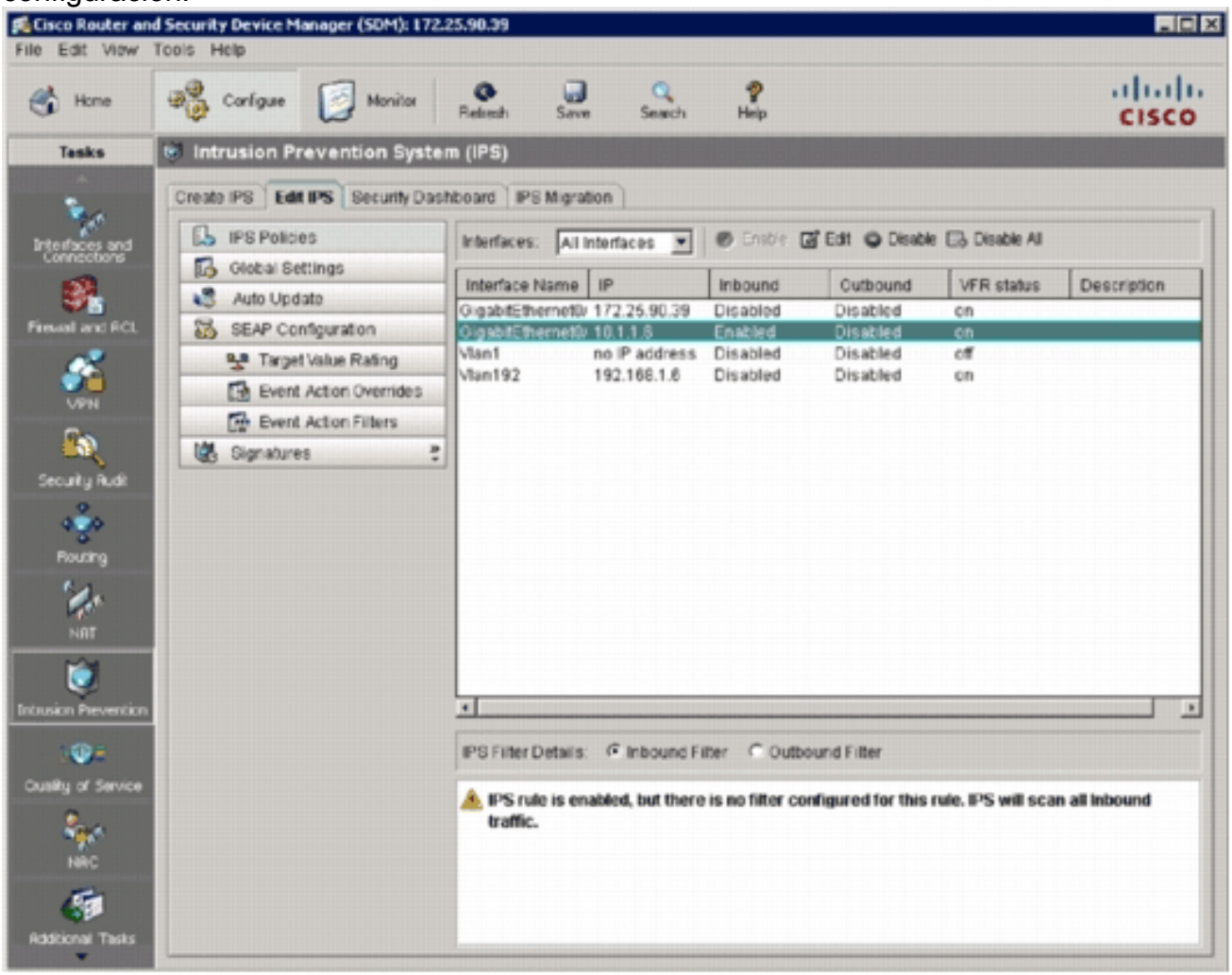

comandos.

31. Cuando los comandos se entregan al router, haga clic la **AUTORIZACIÓN** para continuar.El cuadro de diálogo del estado de la configuración IOS IPS muestra que las firmas se están

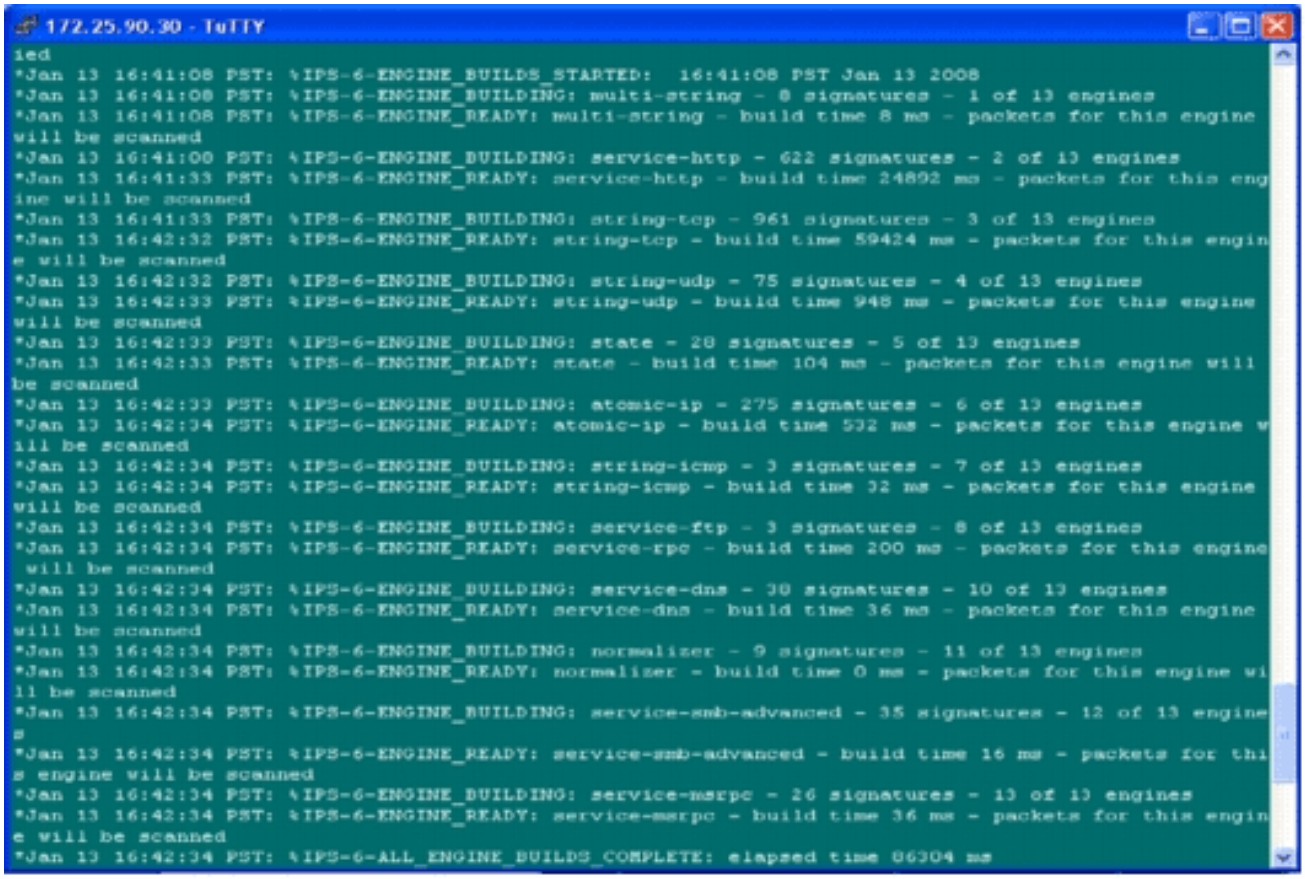



cargando en el router.

32. Cuando se cargan las firmas, el SDM visualiza la lengueta **IPS del editar** con la configuración actual. Marque que interconectan y en qué dirección se habilita el IOS IPS para verificar la
configuración.




La consola del router muestra que se han cargado las
firmas.

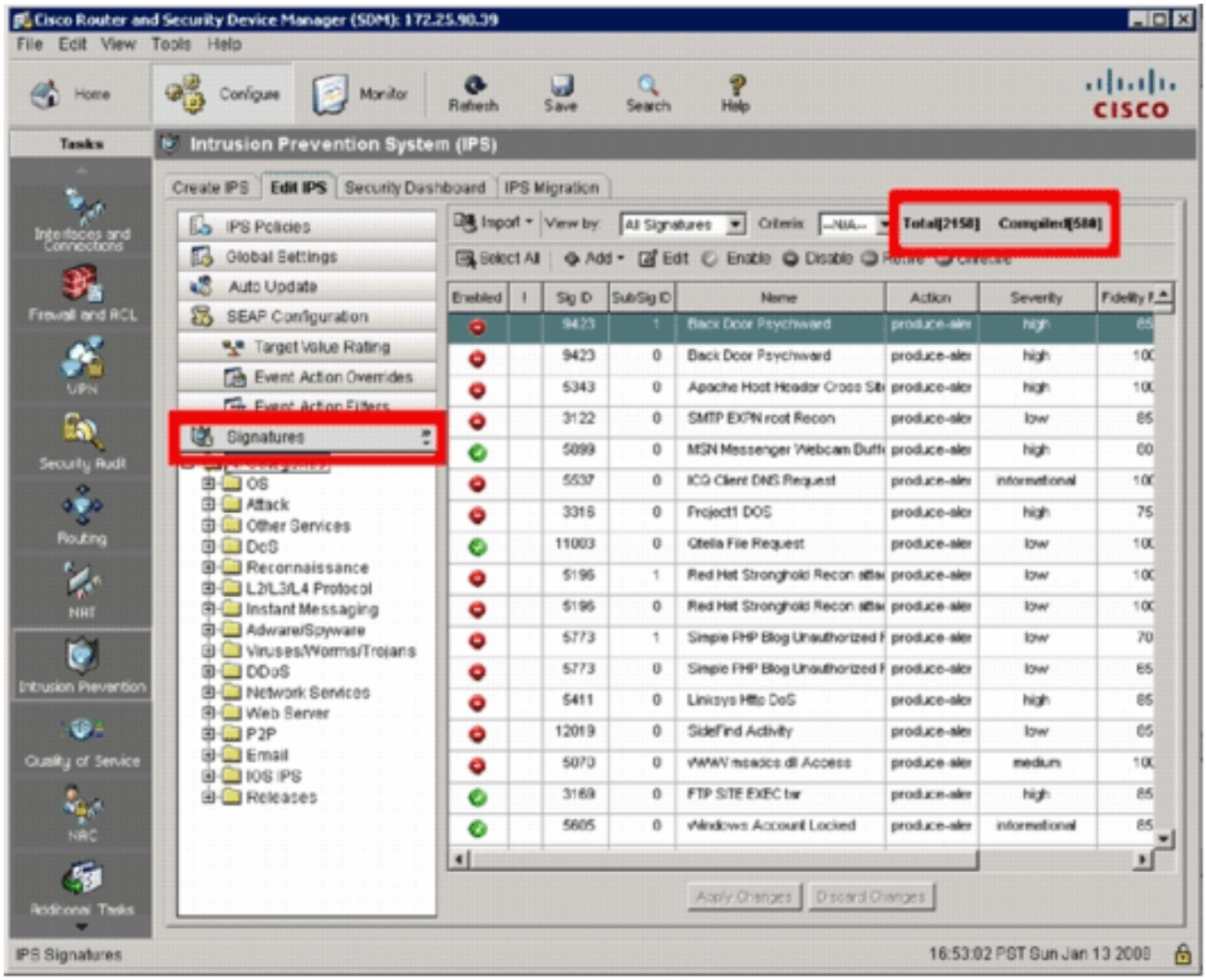



33. Utilice el **comando count de las firmas IPS del IP de la demostración** para verificar las firmas se cargan correctamente.

```
router#show ip ips signatures count
Cisco SDF release version S313.0
Trend SDF release version V0.0
|
snip
|
Total Signatures: 2158
 Total Enabled Signatures: 829
 Total Retired Signatures: 1572
 Total Compiled Signatures: 580
 Total Signatures with invalid parameters: 6
         Total Obsoleted Signatures: 11
```

El aprovisionamiento inicial de IOS IPS usando el SDM 2.5 es completo.

34. Verifique los números de la firma con el SDM tal y como se muestra en de esta imagen.




# Información Relacionada

- Cisco IOS IPS en el cisco.com
- Paquete de la firma IPS del Cisco IOS
- Archivos de firma IPS del Cisco IOS para el SDM
- Introducción con el Cisco IOS IPS con el formato de la firma 5.x
- Guía de configuración IPS del Cisco IOS
- Visor de eventos del Cisco IDS
- Soporte Técnico y Documentación - Cisco Systems