Configuración de Cisco IOS IPS con un router y SDM

Contenido

Introducción

Este documento describe cómo utilizar Cisco Router and Security Device Manager (SDM) versión 2.5 para configurar Cisco IOS® Intrusion Prevention System (IPS) en 12.4(15)T3 y versiones posteriores.

Las mejoras en SDM 2.5 relacionadas con IOS IPS son:

- Número total de firma compilada que se muestra en la GUI de la lista de firmas
- Archivos de firma SDM (formato de archivo zip; por ejemplo, sigv5-SDM-S307.zip) y paquetes de firma CLI (formato de archivo pkg; por ejemplo, IOS-S313-CLI.pkg) se puede descargar juntos en una operación
- Los paquetes de firma descargados se pueden enviar automáticamente al router como opción

Las tareas involucradas en el proceso de aprovisionamiento inicial son:

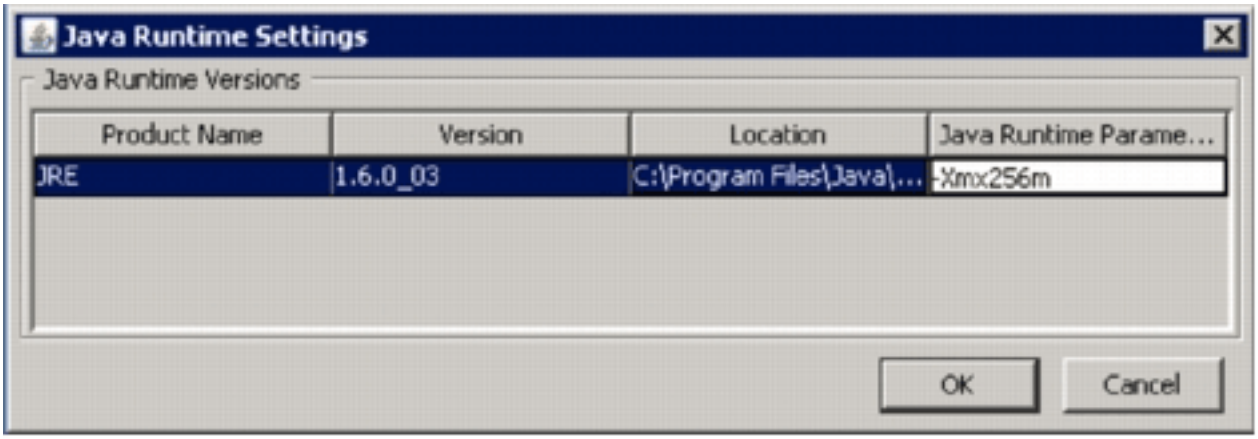
1. Descargue e instale SDM 2.5.
2. Utilice SDM Auto Update para descargar el paquete de firma IPS de IOS en un equipo local.
3. Inicie el asistente de políticas IPS para configurar IOS IPS.
4. Verifique que la configuración y las firmas de IOS IPS estén correctamente cargadas

Cisco SDM es una herramienta de configuración basada en Web que simplifica la configuración de router y seguridad mediante asistentes inteligentes que ayudan a los clientes a implementar, configurar y supervisar de forma rápida y sencilla un router de Cisco sin necesidad de conocer la interfaz de línea de comandos (CLI).

SDM versión 2.5 se puede descargar de Cisco.com en http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (sólo clientes registrados). La nota de la versión se puede encontrar en http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr.25.html

Nota: Cisco SDM requiere una resolución de pantalla de al menos 1024 x 768.

Nota: Cisco SDM requiere que el tamaño del montón de memoria Java no sea inferior a 256 MB para configurar IOS IPS. Para cambiar el tamaño del montón de memoria Java, abra el panel de control Java, haga clic en la pestaña **Java**, haga clic en **View** ubicado en Java Applet Runtime Settings y, a continuación, introduzca **-Xmx256m** en la columna Java Runtime Parameter.



Prerequisites

Requirements

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 las versiones 12.4(15)T3 y posteriores
- Router de Cisco y Security Device Manager (SDM) versión 2.5

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.

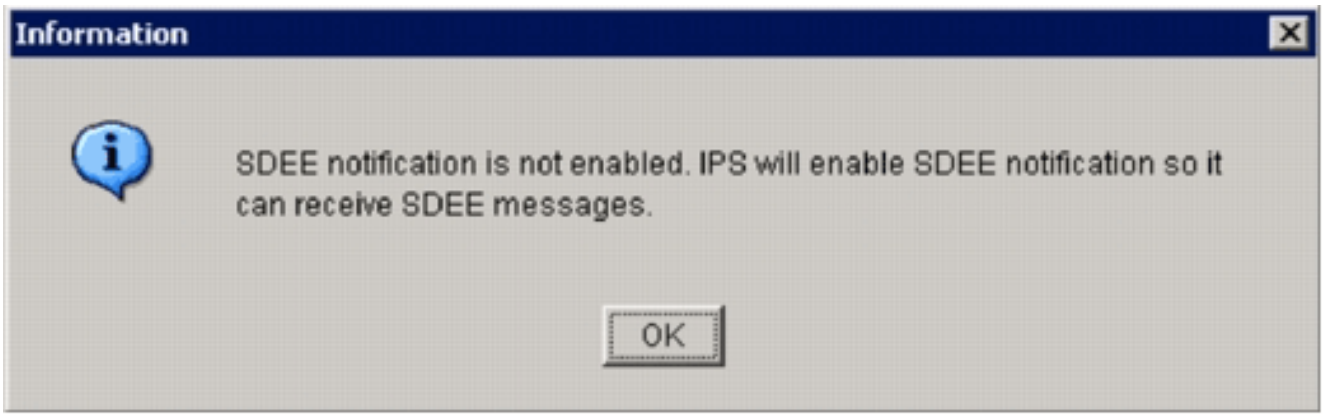
Configurar

Nota: Abra una sesión de consola o telnet al router (con "monitor de término" activado) para monitorear los mensajes cuando utilice SDM para aprovisionar IPS de IOS.

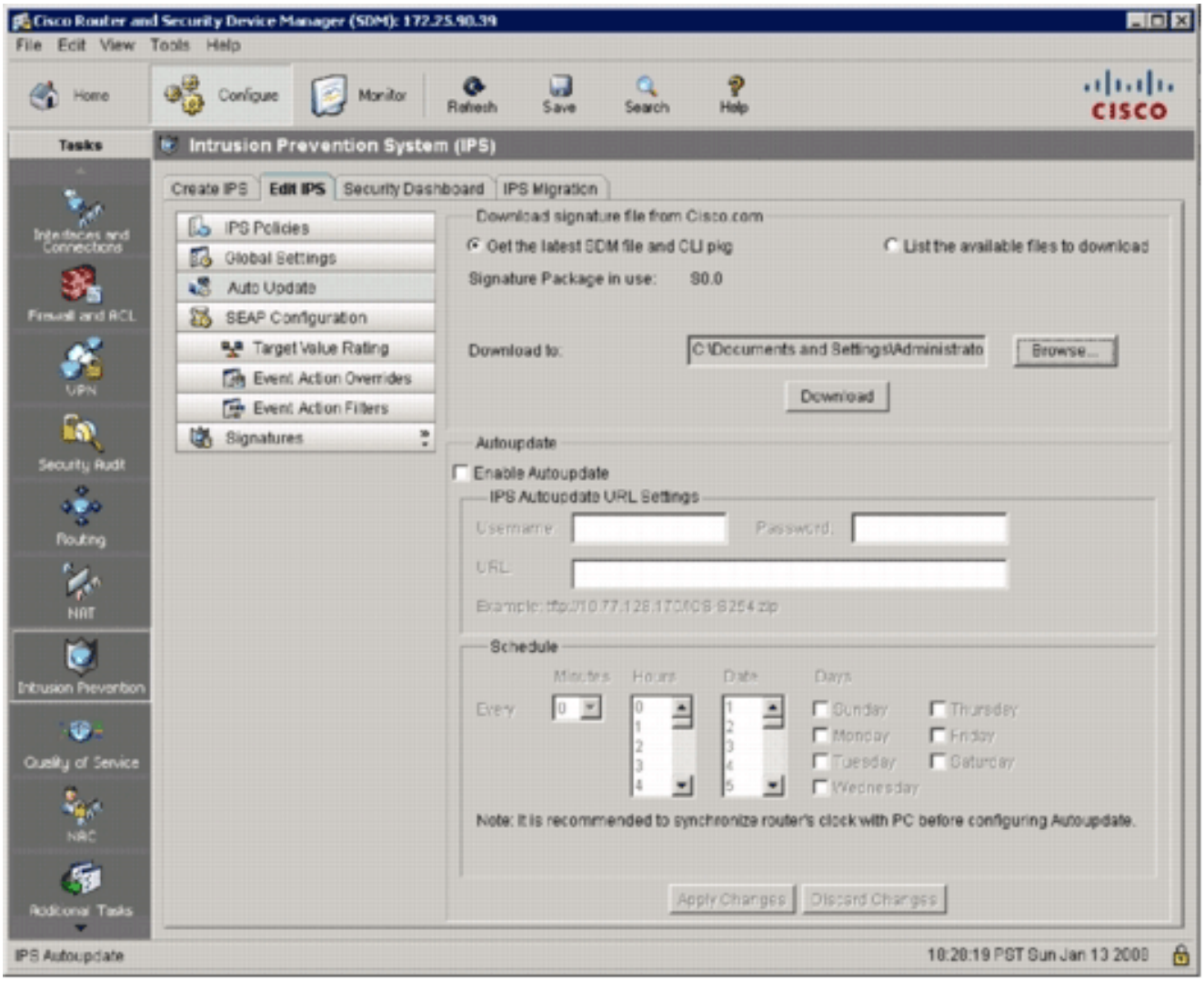
1. Descargue SDM 2.5 de Cisco.com en http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (sólo clientes registrados) e instálelo en un equipo local.
2. Ejecute SDM 2.5 desde el PC local.
3. Cuando aparezca el cuadro de diálogo Inicio de sesión de IOS IPS, introduzca el mismo

nombre de usuario y contraseña que utiliza para la autenticación de SDM en el router.

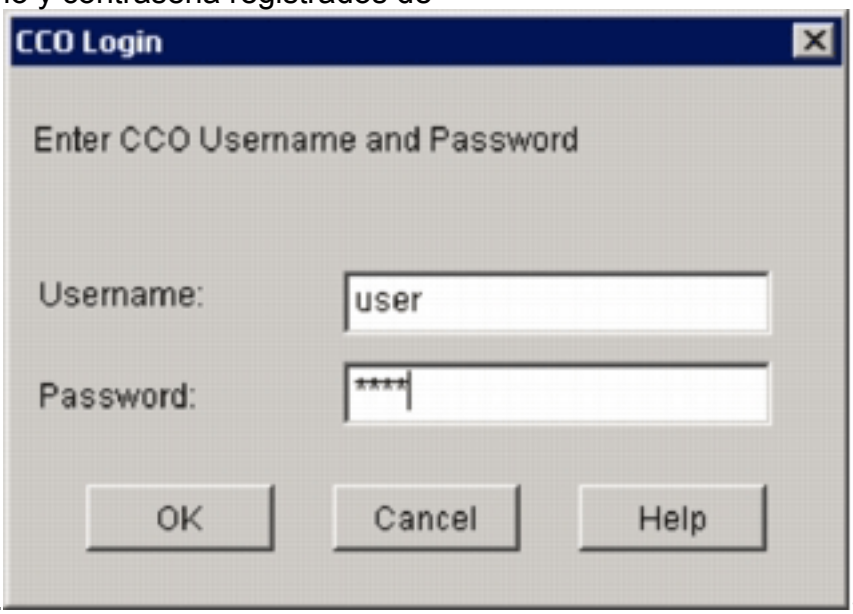
4. En la interfaz de usuario de SDM, haga clic en **Configurar** y, a continuación, haga clic en **Prevención de intrusiones**.
5. Haga clic en la pestaña **Edit IPS**.
6. Si la notificación SDEE no está habilitada en el router, haga clic en **Aceptar** para habilitar la notificación SDEE.



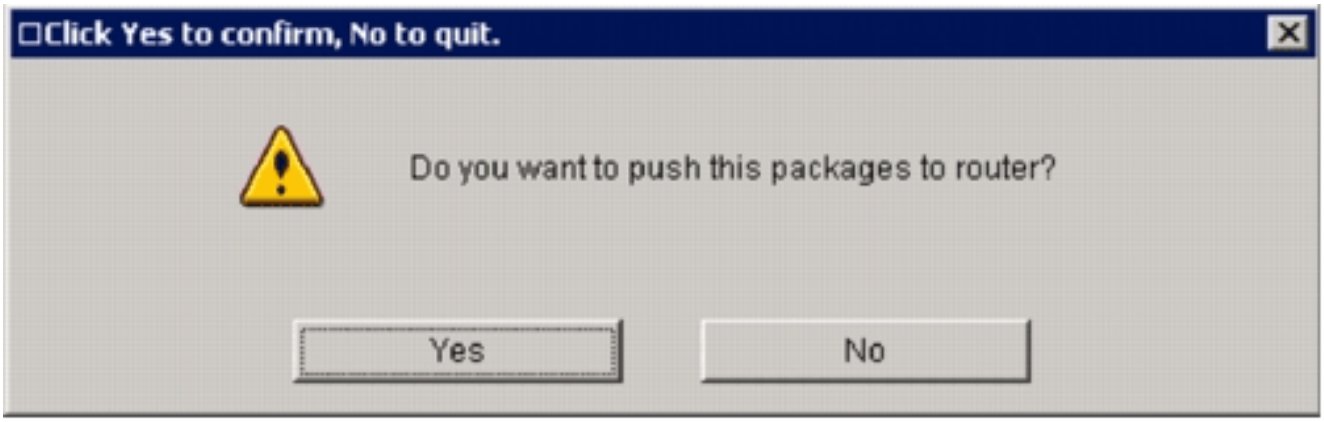
7. En el área Descargar archivo de firma de Cisco.com de la ficha Editar IPS, haga clic en el botón de opción **Obtener el archivo SDM más reciente y el** botón de opción **CLI pkg** y, a continuación, haga clic en **Examinar** para seleccionar un directorio en su equipo local en el que guardar los archivos descargados.Puede elegir el directorio raíz del servidor TFTP o FTP, que se utilizará más adelante cuando implemente el paquete de firma en el router.
8. Haga clic en **Descarga**.



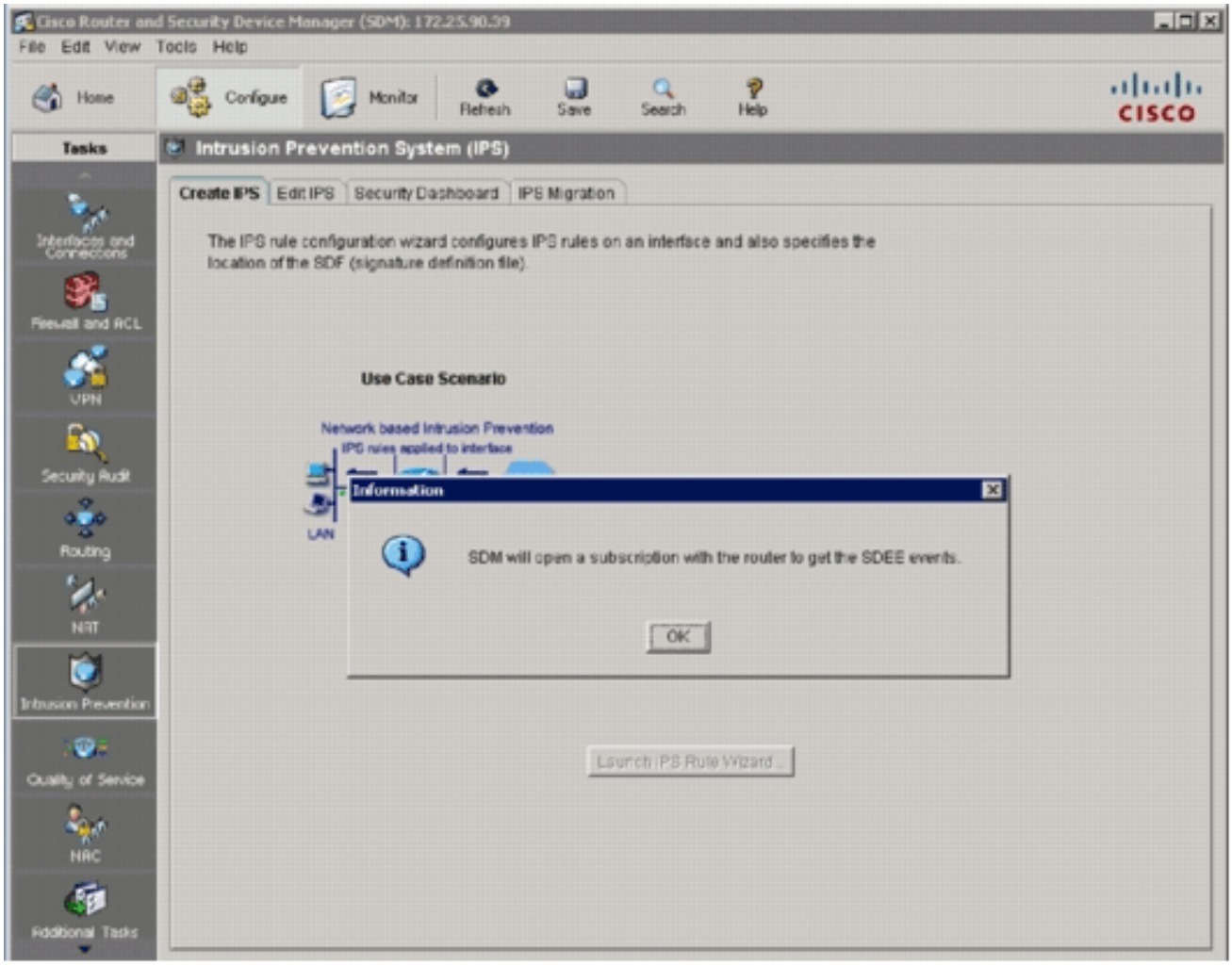
9. Cuando aparezca el cuadro de diálogo Inicio de sesión de CCO, utilice su nombre de usuario y contraseña registrados de



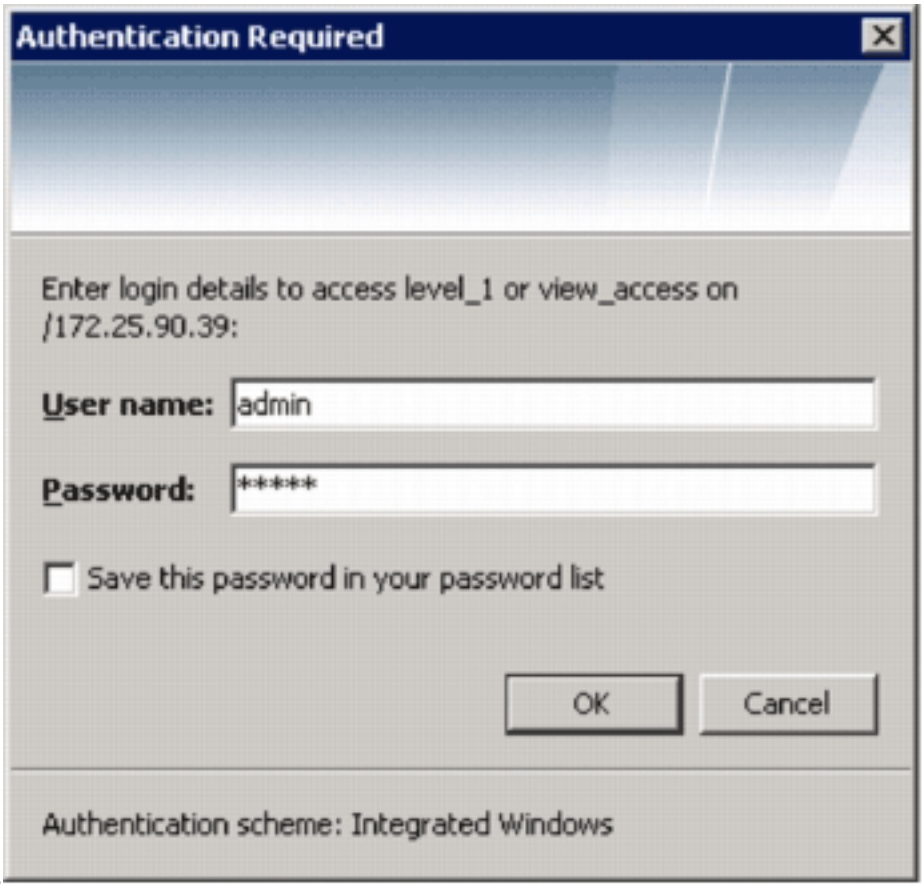
CCO. SDM se conecta a Cisco.com y comienza a descargar el archivo SDM (por ejemplo, sigv5-SDM-S307.zip) y el archivo pkg de CLI (por ejemplo, IOS-S313-CLI.pkg) en el directorio seleccionado en el paso 7.Una vez descargados ambos archivos, SDM le solicita que envíe el paquete de firma descargado al
router.



10. Haga clic en **No** porque el IPS del IOS todavía no se ha configurado en el router.
11. Después de que SDM descargue el paquete de firma IOS CLI más reciente, haga clic en la pestaña **Create IPS** para crear la configuración IPS de IOS inicial.
12. Si se le solicita que aplique cambios al router, haga clic en **Aplicar cambios**.
13. Haga clic en **Iniciar Asistente para reglas IPS**.Aparece un cuadro de diálogo para informarle de que SDM necesita establecer una suscripción SDEE al router para recuperar alertas.

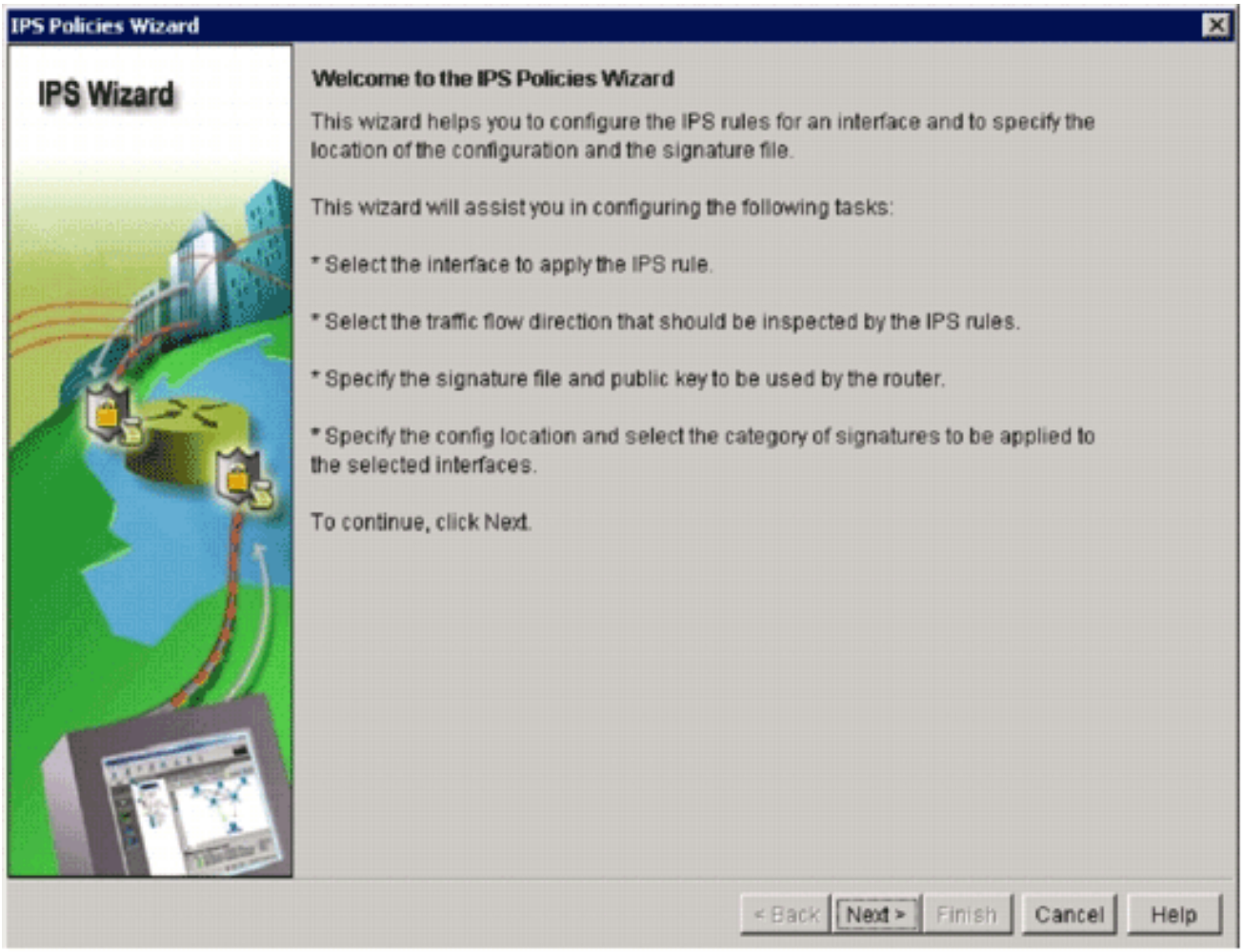


14. Click OK.Aparecerá el cuadro de diálogo Authentication Required (Autenticación

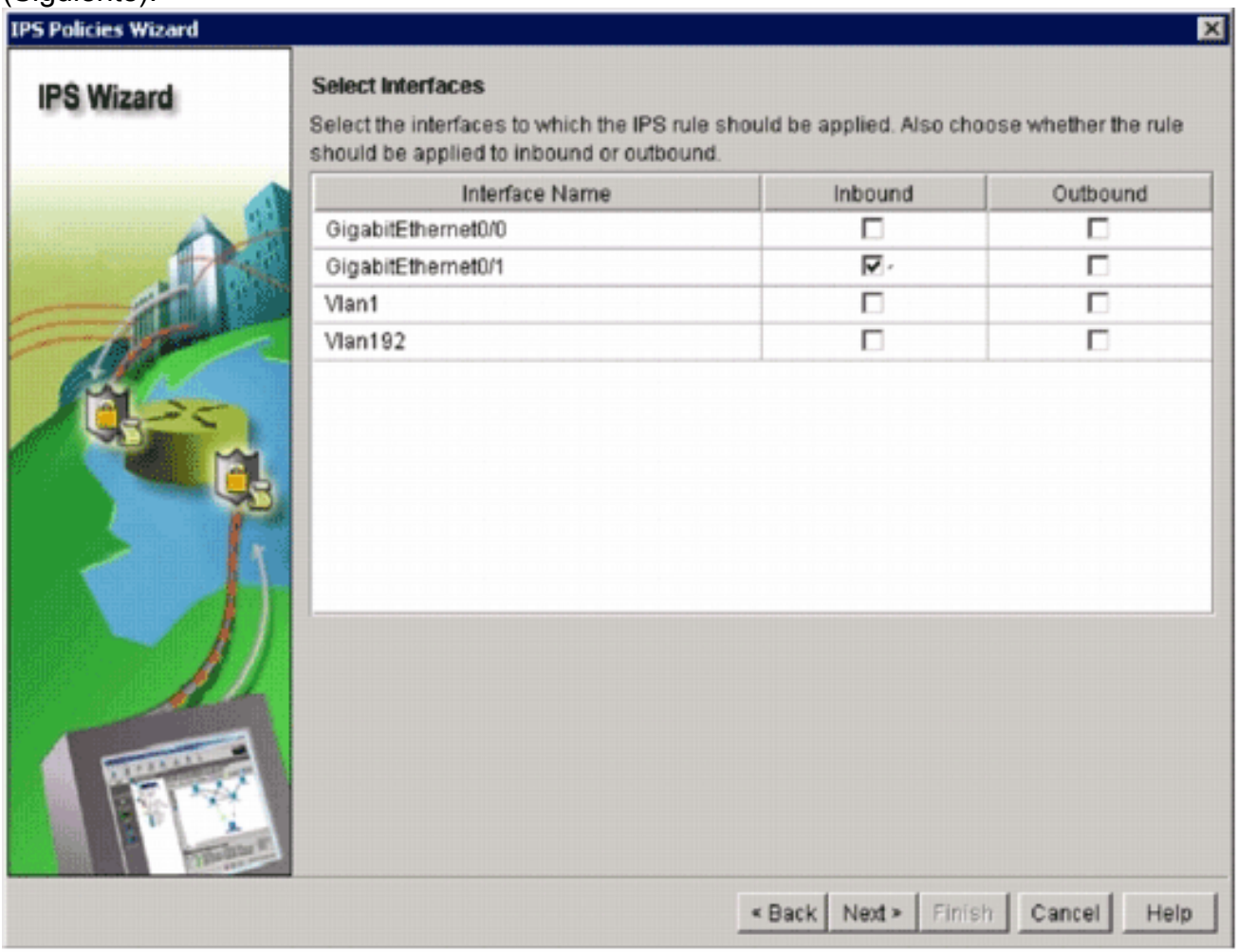


requerida).

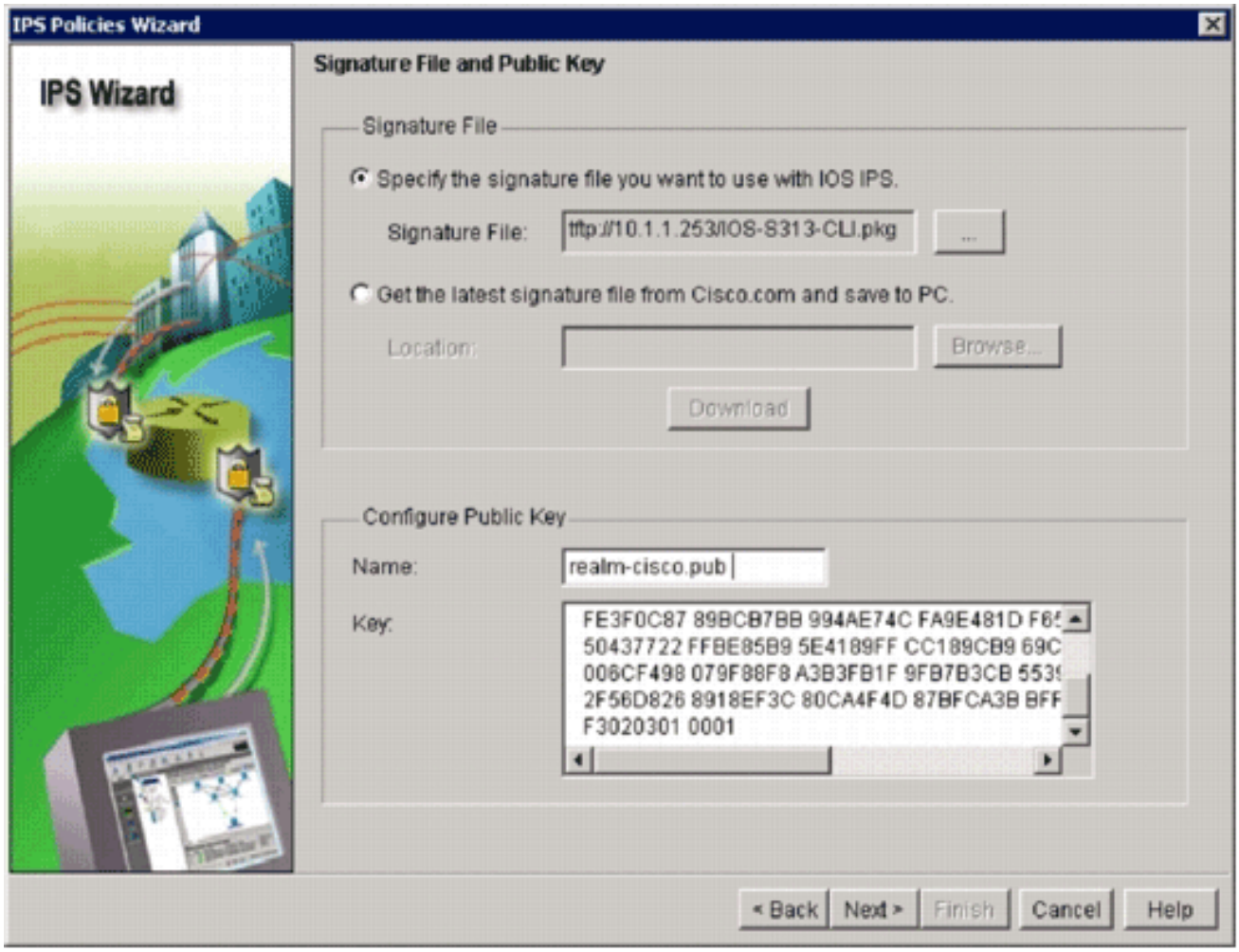
15. Ingrese el nombre de usuario y la contraseña que utilizó para SDM para autenticarse en el router y haga clic en **Aceptar**.Aparecerá el cuadro de diálogo Asistente para políticas IPS.



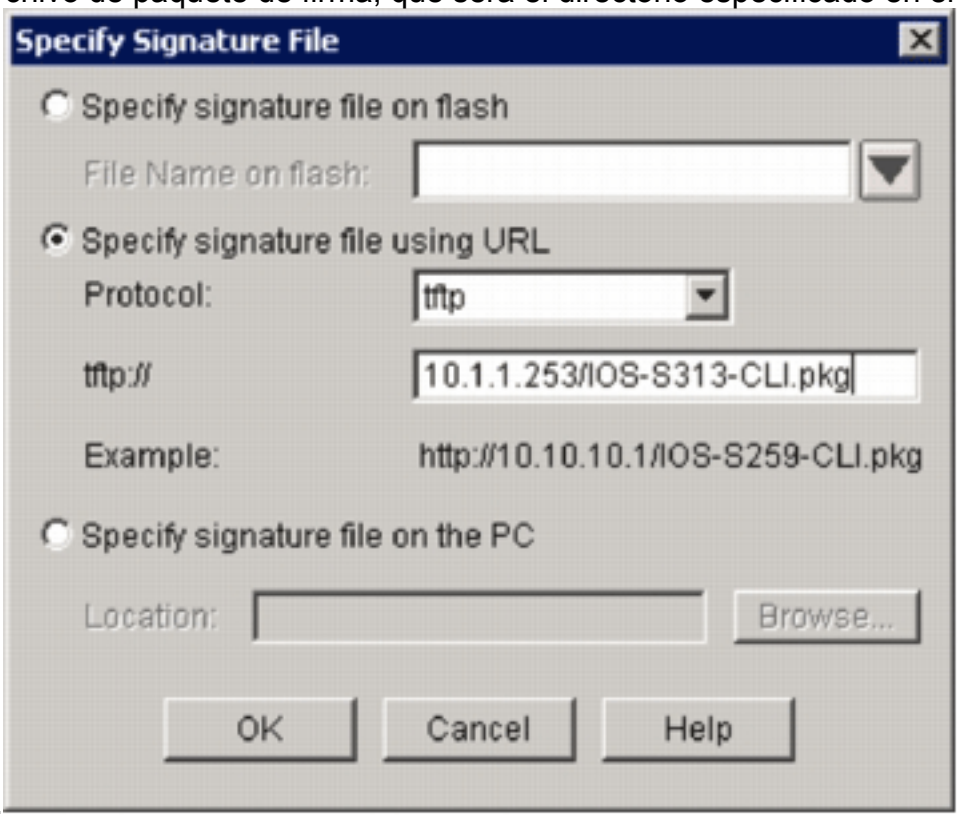
16. Haga clic en Next (Siguiente).



17. En la ventana Interfaces seleccionadas, elija la interfaz y la dirección a la que se aplicará el IPS de IOS y, a continuación, haga clic en **Siguiente** para continuar.



18. En el área Archivo de firma de la ventana Archivo de firma y Clave pública, haga clic en el botón de opción **Especificar el archivo de firma que desea utilizar con IOS IPS** y, a continuación, haga clic en el **botón Archivo de firma** (...) para especificar la ubicación del archivo de paquete de firma, que será el directorio especificado en el paso



7.

19. Haga clic en el botón de opción **Especificar archivo de firma mediante URL** y elija un

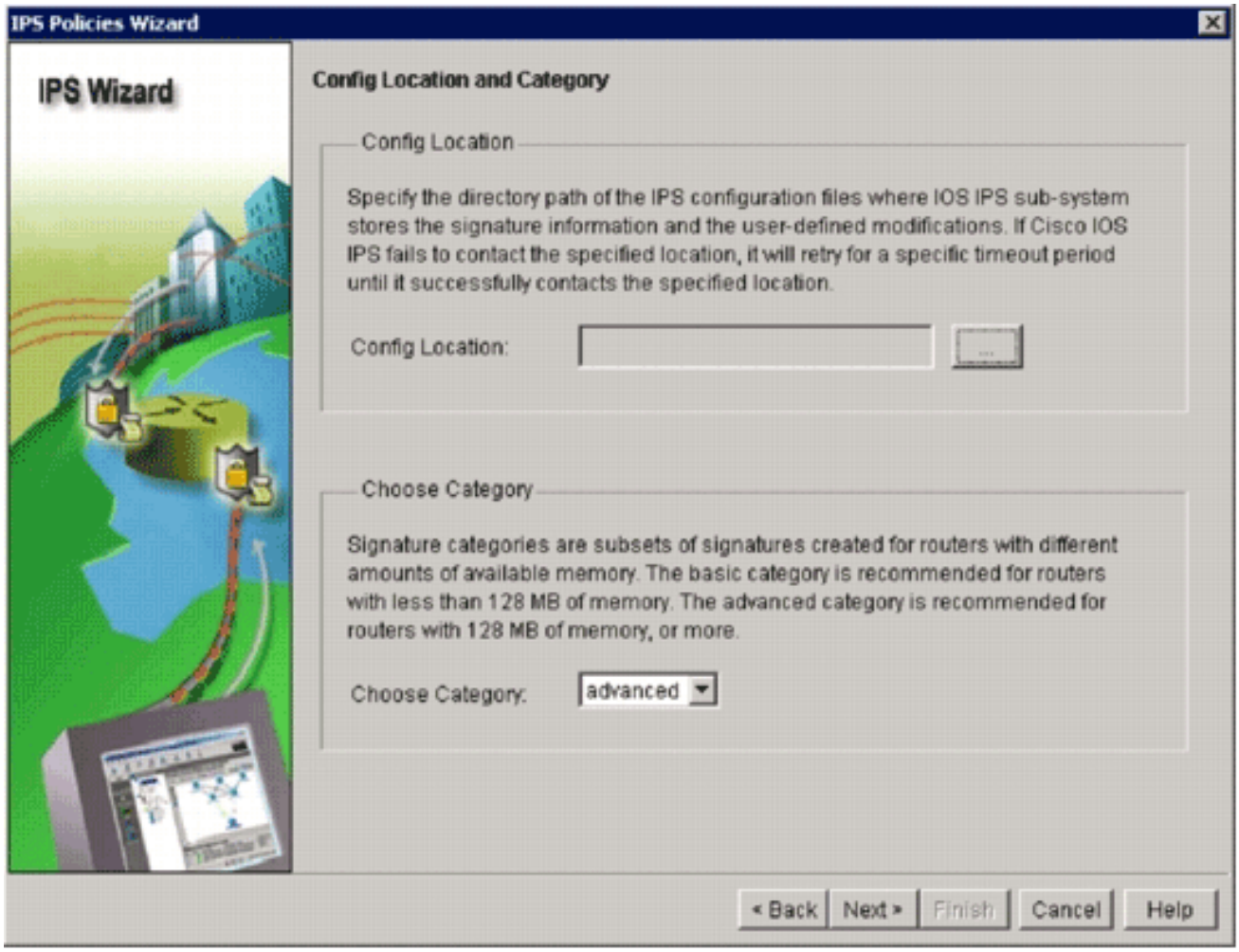
protocolo de la lista desplegable Protocolo.**Nota:** Este ejemplo utiliza TFTP para descargar el paquete de firma al router.

20. Ingrese la URL para el archivo de firma y haga clic en **Aceptar**.
21. En el área Configure Public Key (Configurar clave pública) de la ventana Signature File (Archivo de firma) y Public Key (Clave pública), introduzca **realm-cisco.pub** en el campo Name (Nombre) y, a continuación, copie esta clave pública y péguela en el campo Key (Clave).

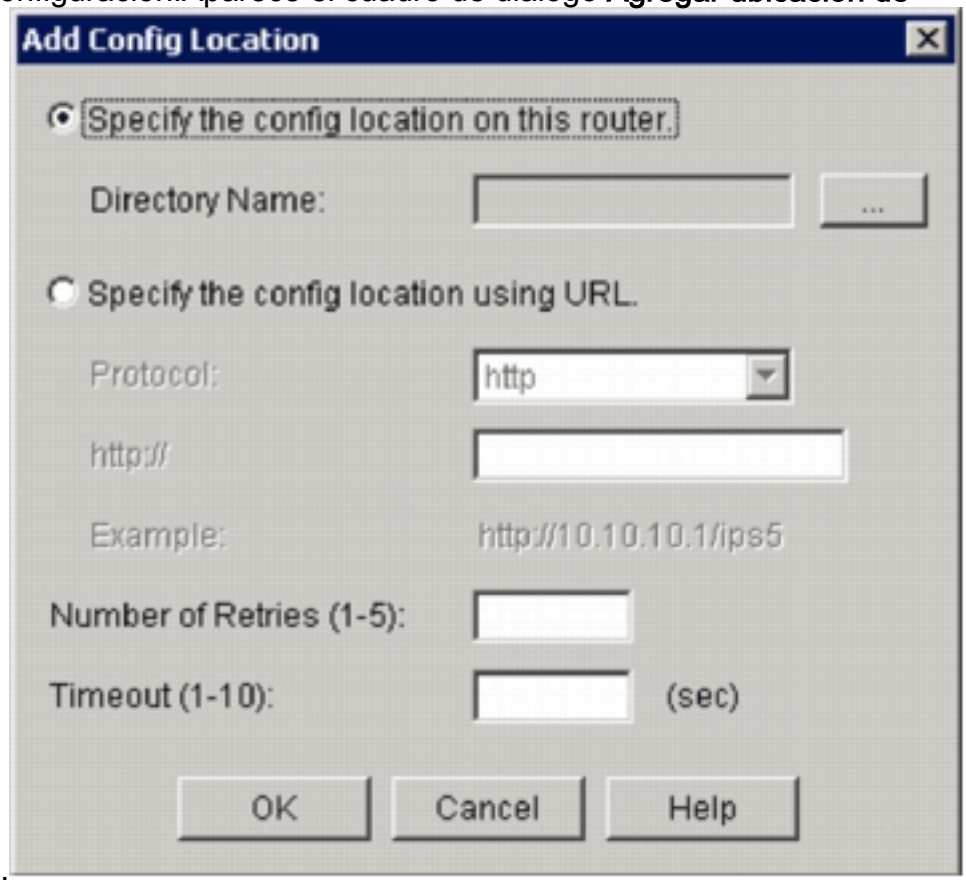
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

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
```

Nota: Esta clave pública se puede descargar de Cisco.com en: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (sólo clientes registrados) .

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

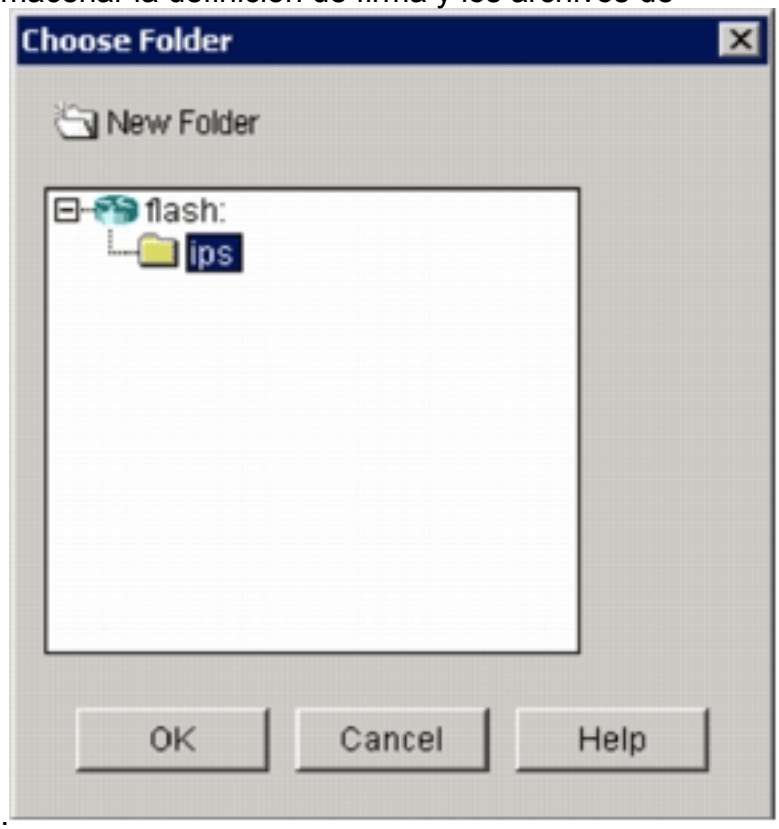


23. En la ventana Config Location and Category , haga clic en el botón **Config Location** (...) para especificar una ubicación en la que se almacenarán la definición de firmas y los archivos de configuración.Aparece el cuadro de diálogo **Agregar ubicación de configuración**.

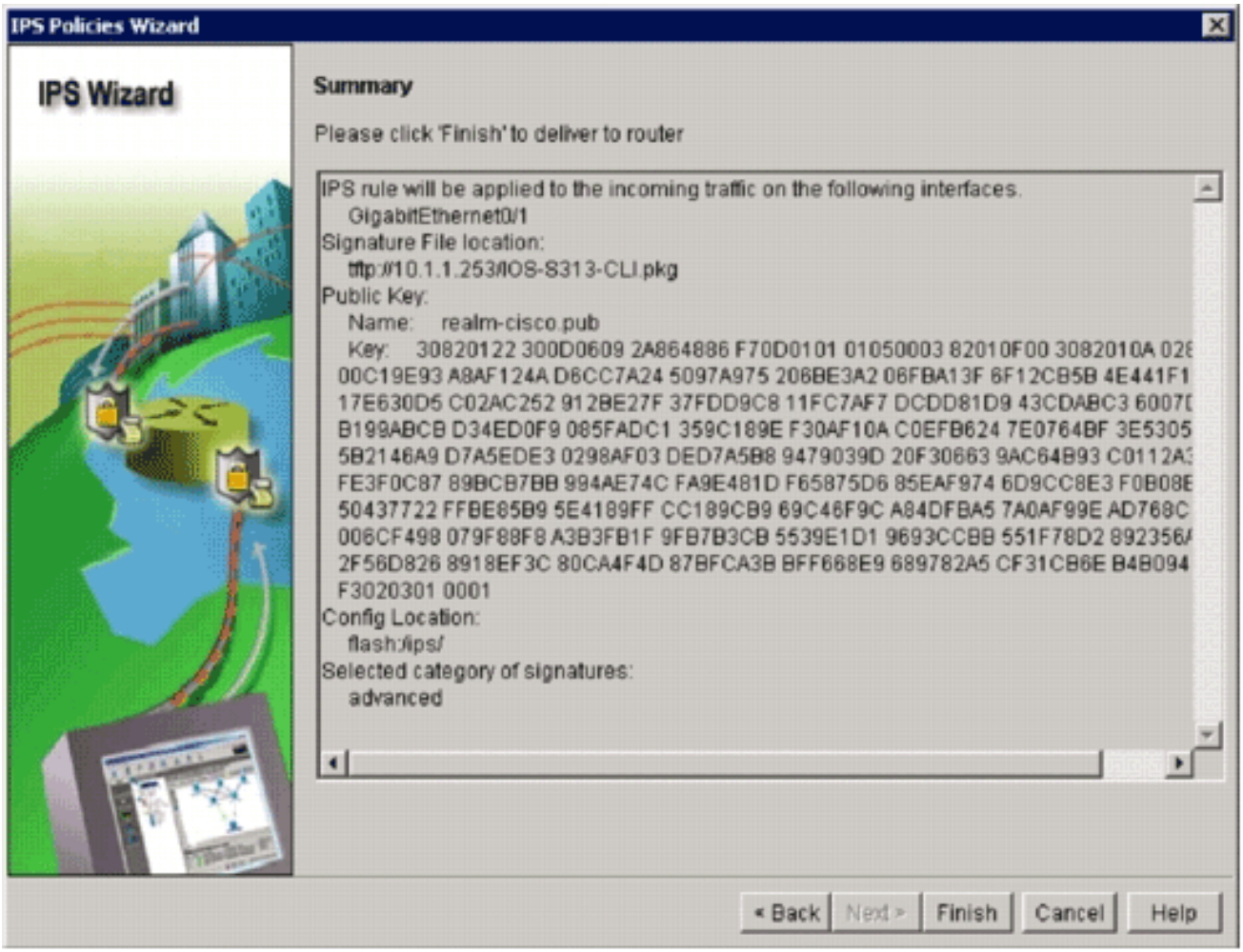


24. En el cuadro de diálogo Add Config Location, haga clic en el botón de opción **Specify the**

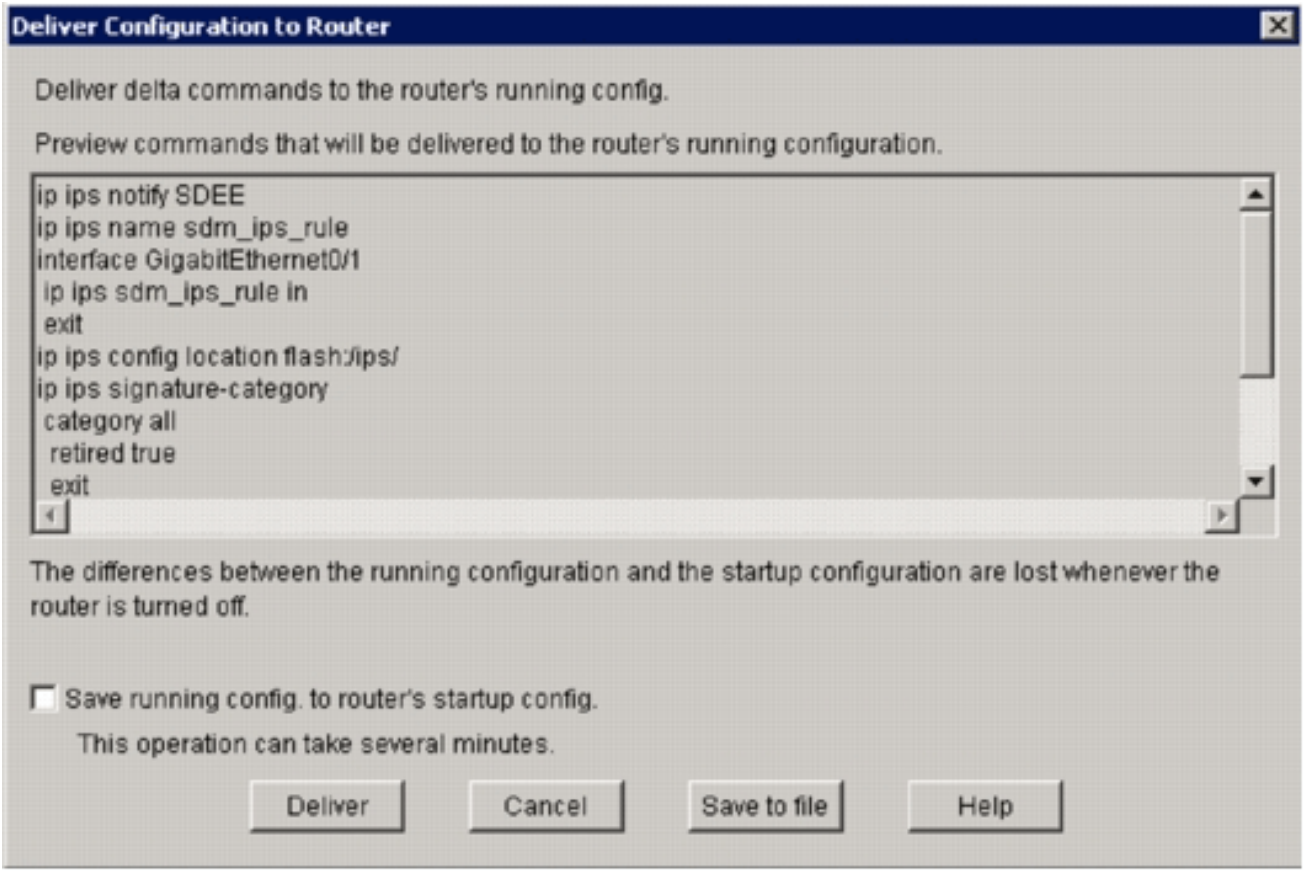
config location on this router y luego haga clic en el **botón Directory Name** (...) para localizar el archivo de configuración.Aparece el cuadro de diálogo Elegir carpeta para permitirle seleccionar un directorio existente o crear un nuevo directorio en la memoria flash del router para almacenar la definición de firma y los archivos de configuración.



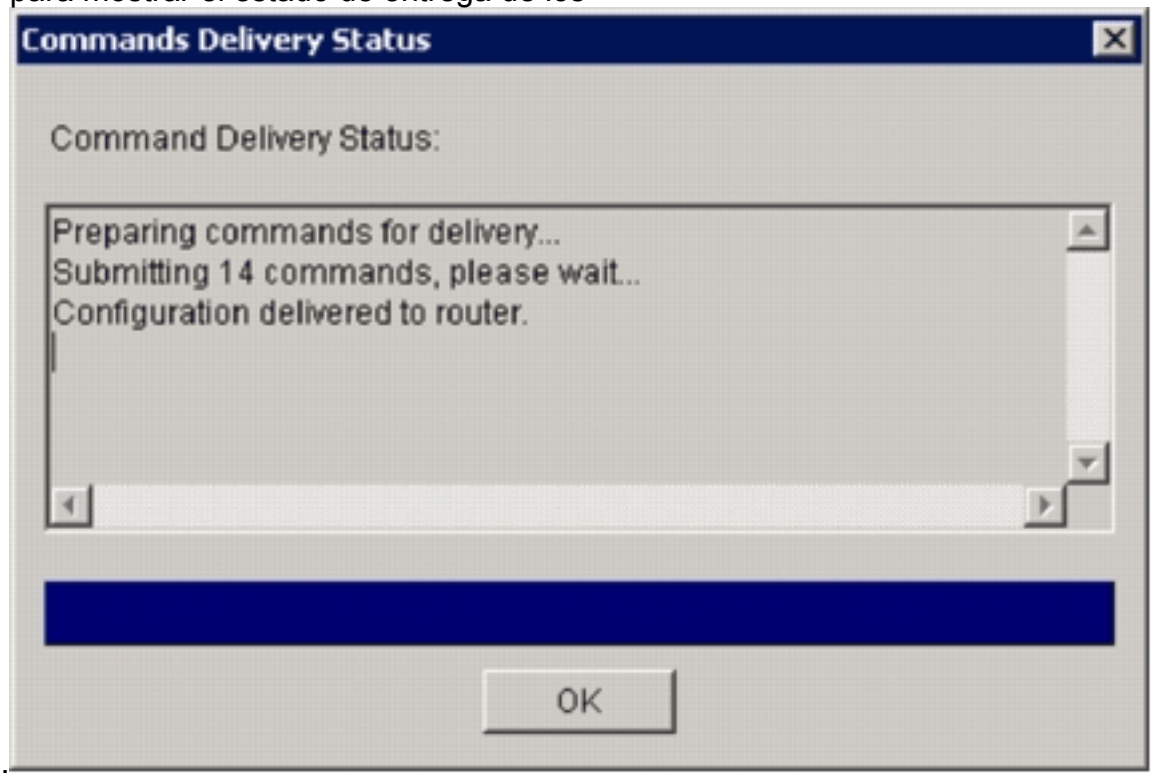
25. Haga clic en **Nueva carpeta** situada en la parte superior del cuadro de diálogo si desea crear un nuevo directorio.
26. Una vez que seleccione el directorio, haga clic en **Aceptar** para aplicar los cambios y luego haga clic en **Aceptar** para cerrar el cuadro de diálogo Agregar ubicación de configuración.
27. En el cuadro de diálogo Asistente para políticas IPS, seleccione la categoría de firma según la cantidad de memoria instalada en el router. Existen dos categorías de firma que puede elegir en SDM: Basic y Advanced.Si el router tiene instalada una DRAM de 128 MB, Cisco recomienda que elija la categoría Basic para evitar fallas de asignación de memoria. Si el router tiene instalada una DRAM de 256 MB o más, puede elegir cualquiera de las categorías.
28. Una vez que seleccione una categoría a utilizar, haga clic en **Siguiente** para continuar con la página de resumen.La página de resumen proporciona una breve descripción de las tareas de configuración inicial de IOS
    IPS.



29. Haga clic en **Finalizar** en la página de resumen para entregar las configuraciones y el paquete de firma al router.Si la opción de comandos de vista previa está activada en la configuración Preferencias de SDM, SDM muestra el cuadro de diálogo Enviar configuración al router que muestra un resumen de los comandos CLI que SDM envía al router.

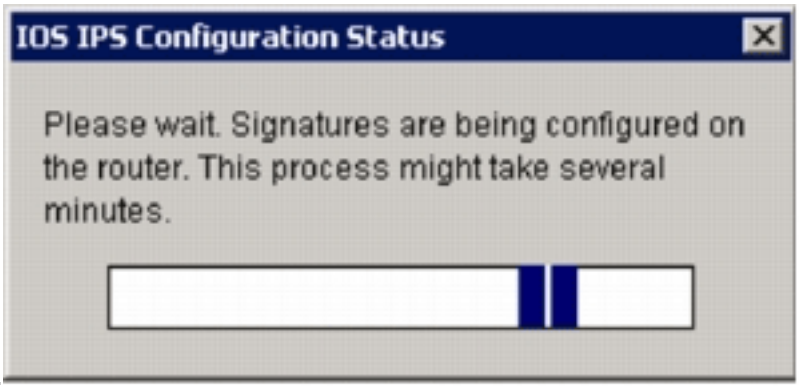


30. Haga clic en **Entregar** para continuar.Aparece el cuadro de diálogo Estado de entrega de comandos para mostrar el estado de entrega de los



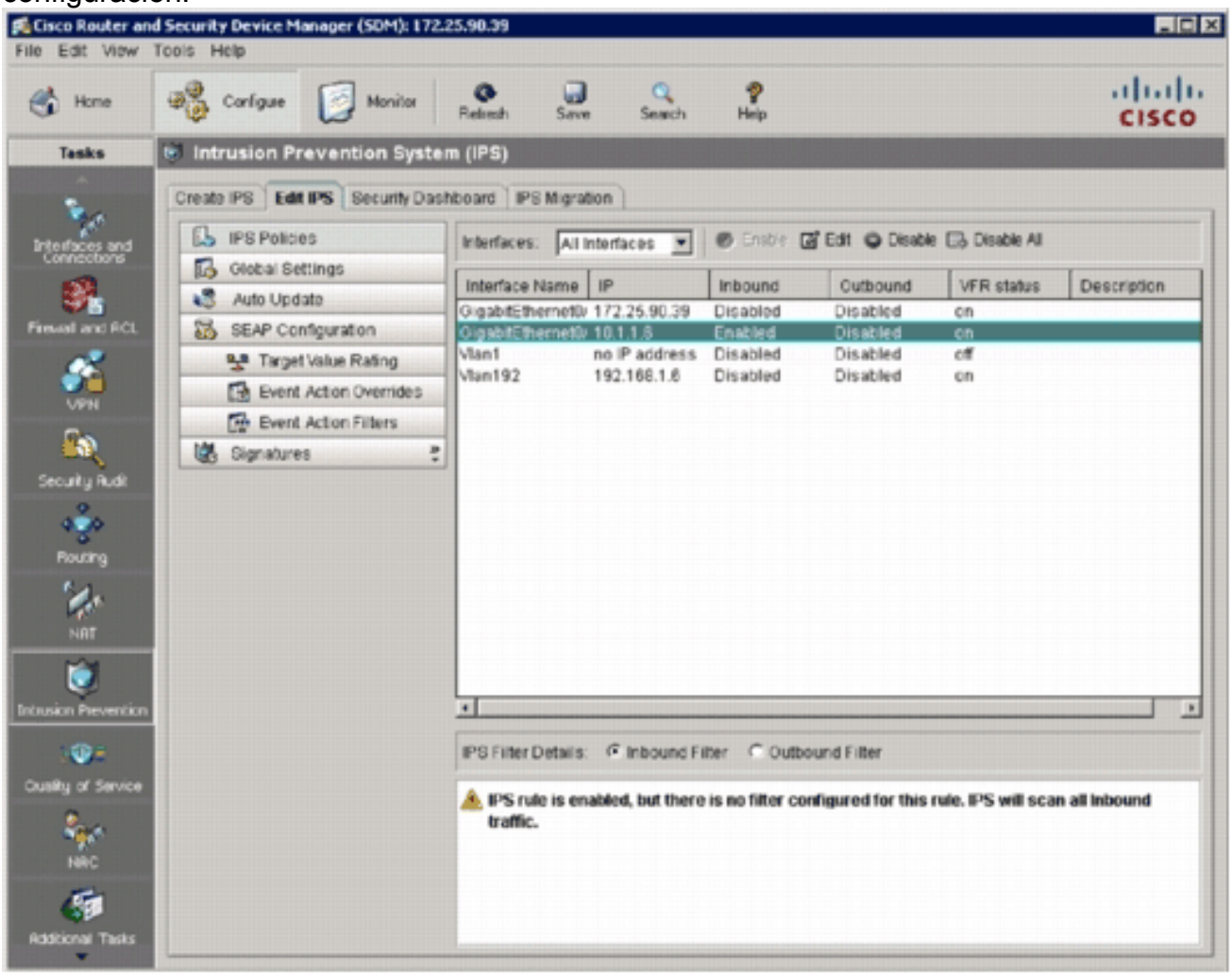
comandos.

31. Cuando los comandos se envían al router, haga clic en **Aceptar** para continuar.El cuadro de diálogo Estado de la configuración de IOS IPS muestra que las firmas se están cargando

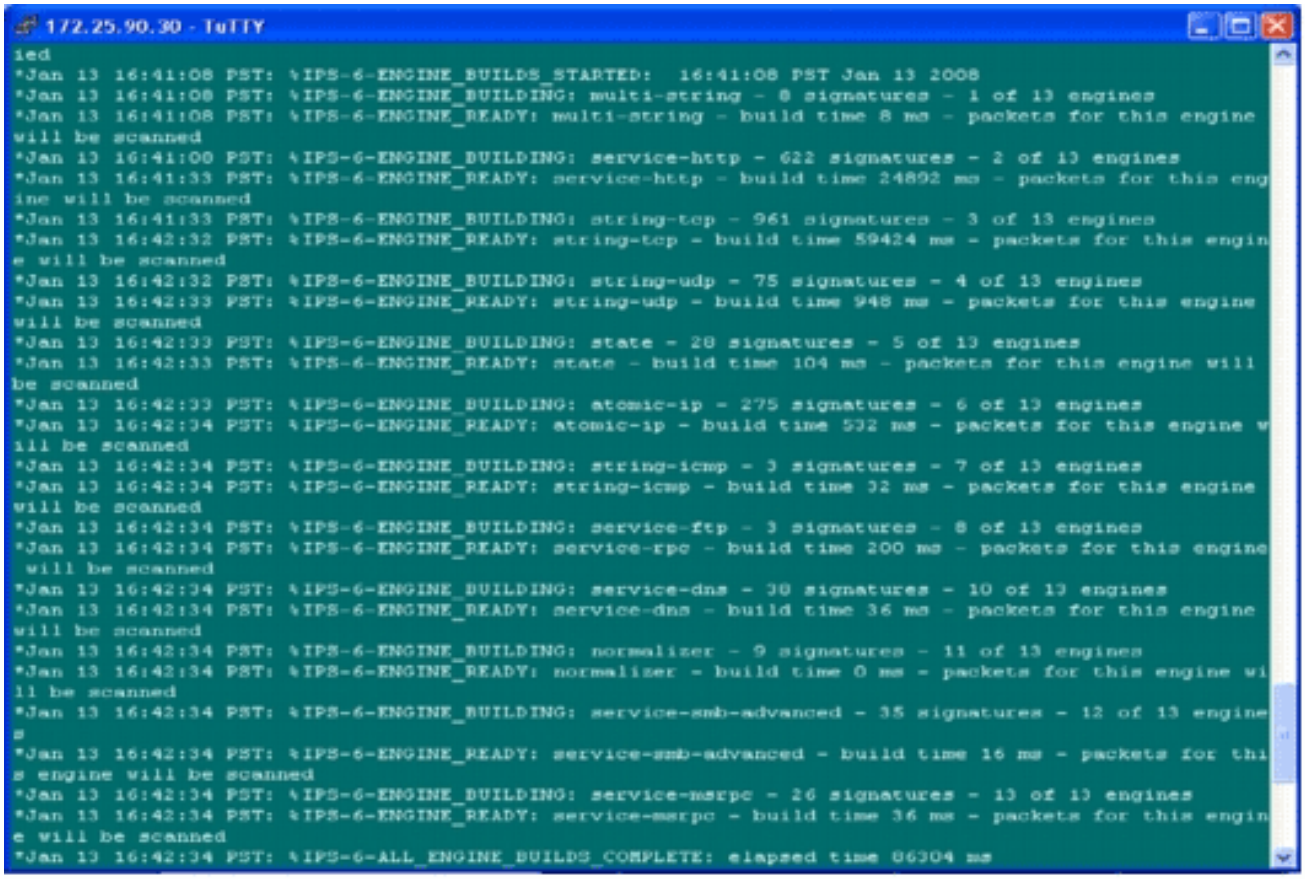


en el router.

32. Cuando se cargan las firmas, SDM muestra la ficha **Editar IPS** con la configuración actual. Verifique qué interfaz y en qué dirección está habilitado el IPS del IOS para verificar la configuración.



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

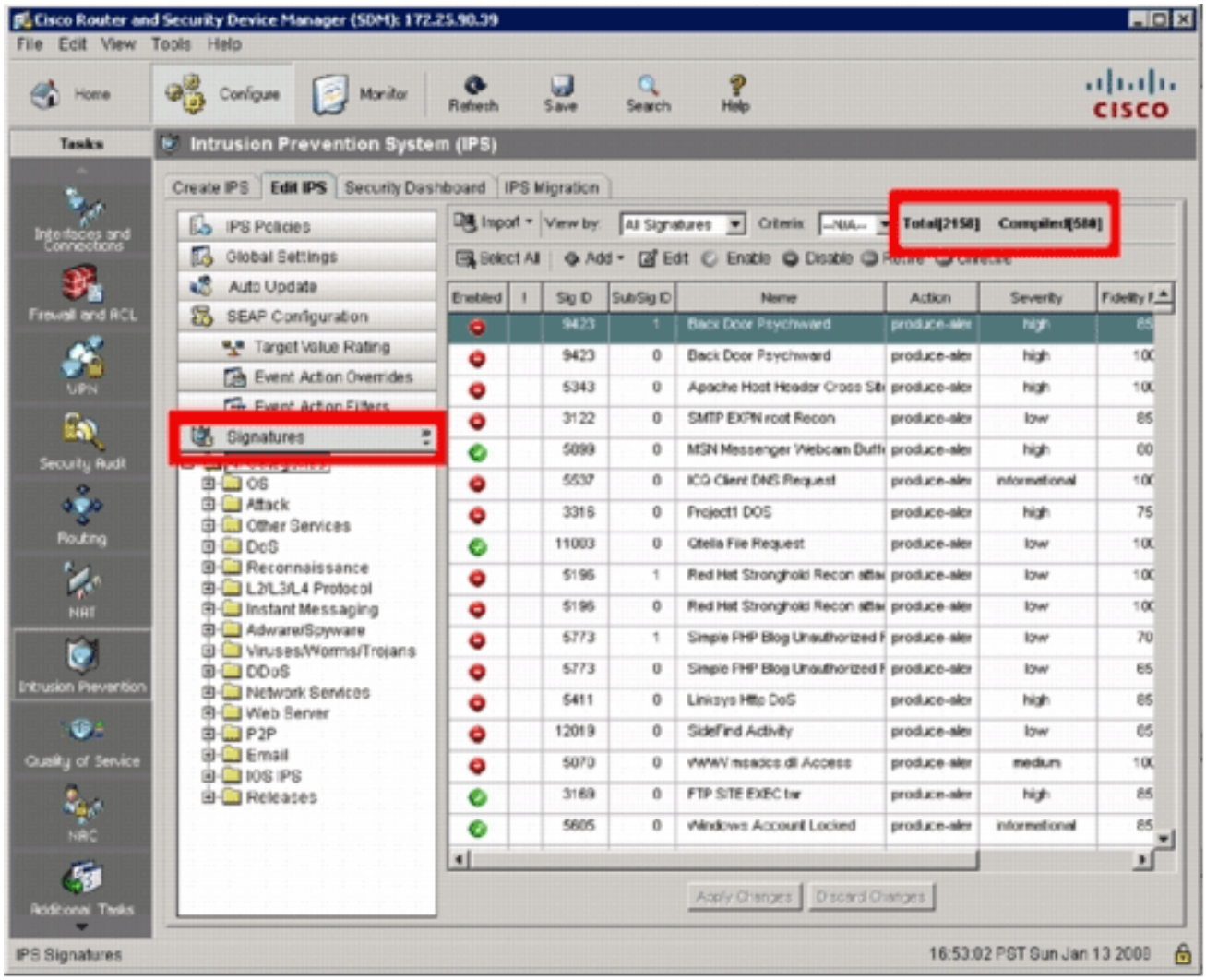


33. Utilice el comando **show ip ips Signature count** para verificar que las firmas se carguen correctamente.

```
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 con SDM 2.5 ha finalizado.

34. Verifique los números de firma con SDM como se muestra en esta imagen.



Información Relacionada

- Cisco IOS IPS en Cisco.com
- Paquete de firma IPS de Cisco IOS
- Archivos de firma IPS de Cisco IOS para SDM
- Introducción a Cisco IOS IPS con formato de firma 5.x
- Guía de Configuración de Cisco IOS IPS
- Visor de eventos de Cisco IDS
- Soporte Técnico y Documentación - Cisco Systems