Configuración del Administrador de Seguridad en Cisco IOS IPS

Contenido

Introducción

Cisco Security Manager forma parte de Cisco Security Management Suite, que ofrece una administración y aplicación de políticas completas para la red de autodefensa de Cisco. Cisco Security Manager es una aplicación de clase empresarial líder del sector para la gestión de la seguridad. Cisco Security Manager aborda la gestión de la configuración de los servicios de seguridad de firewall, VPN y del sistema de prevención de intrusiones (IPS) en los routers, dispositivos de seguridad y módulos de servicios de seguridad de Cisco.

Para obtener un resumen de las características y ventajas de Cisco Security Manager, así como de las nuevas funciones de la versión 3.1, consulte la hoja de datos de Cisco Security Manager 3.1 en http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html. Puede descargar Cisco Security Manager 3.1 de Cisco.com en http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app (sólo clientes registrados).

Este documento describe cómo utilizar Cisco Security Manager 3.1 para realizar la configuración inicial de IOS IPS. Para los routers ya configurados con IOS IPS, los clientes pueden utilizar directamente Cisco Security Manager 3.1 para las tareas de aprovisionamiento.

Nota: Cisco Security Manager 3.1 soporta solamente las imágenes IOS 12.4(11)T2 y posteriores para configurar IOS IPS.

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 Security Manager 3.1
- Cisco IOS 12.4(11)T2

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.

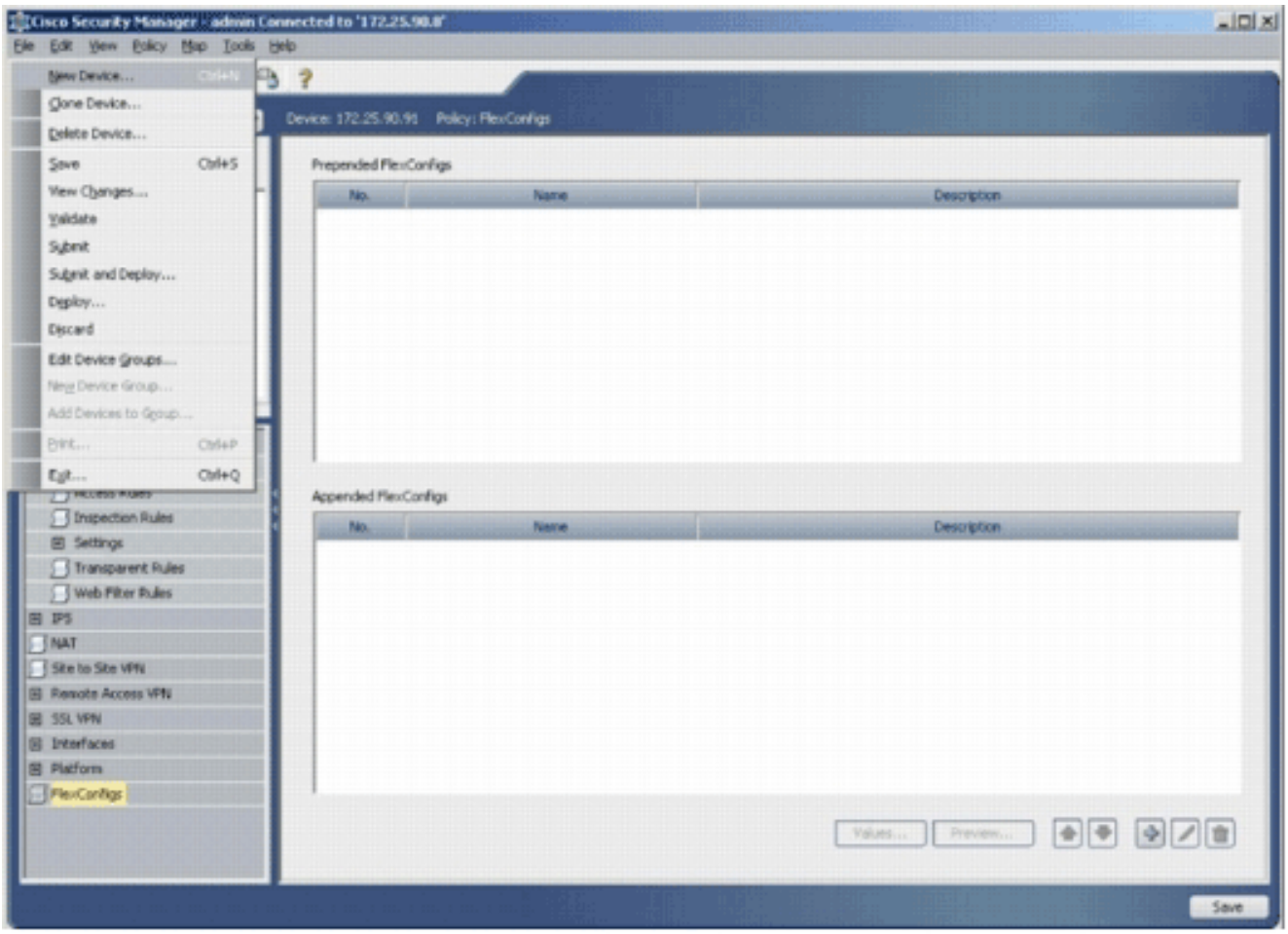
Convenciones

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

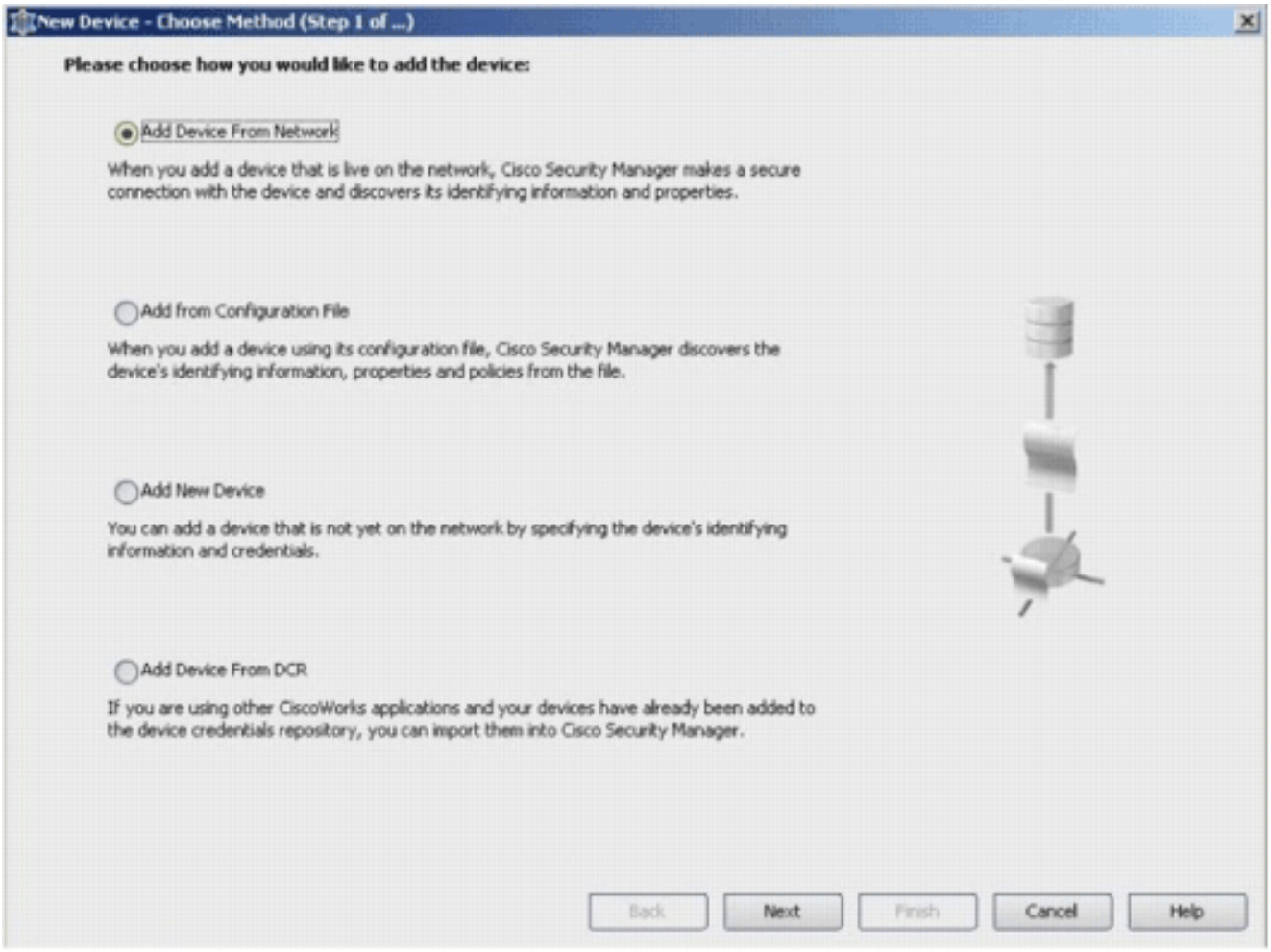
Configurar

Complete estos pasos para configurar IOS IPS:

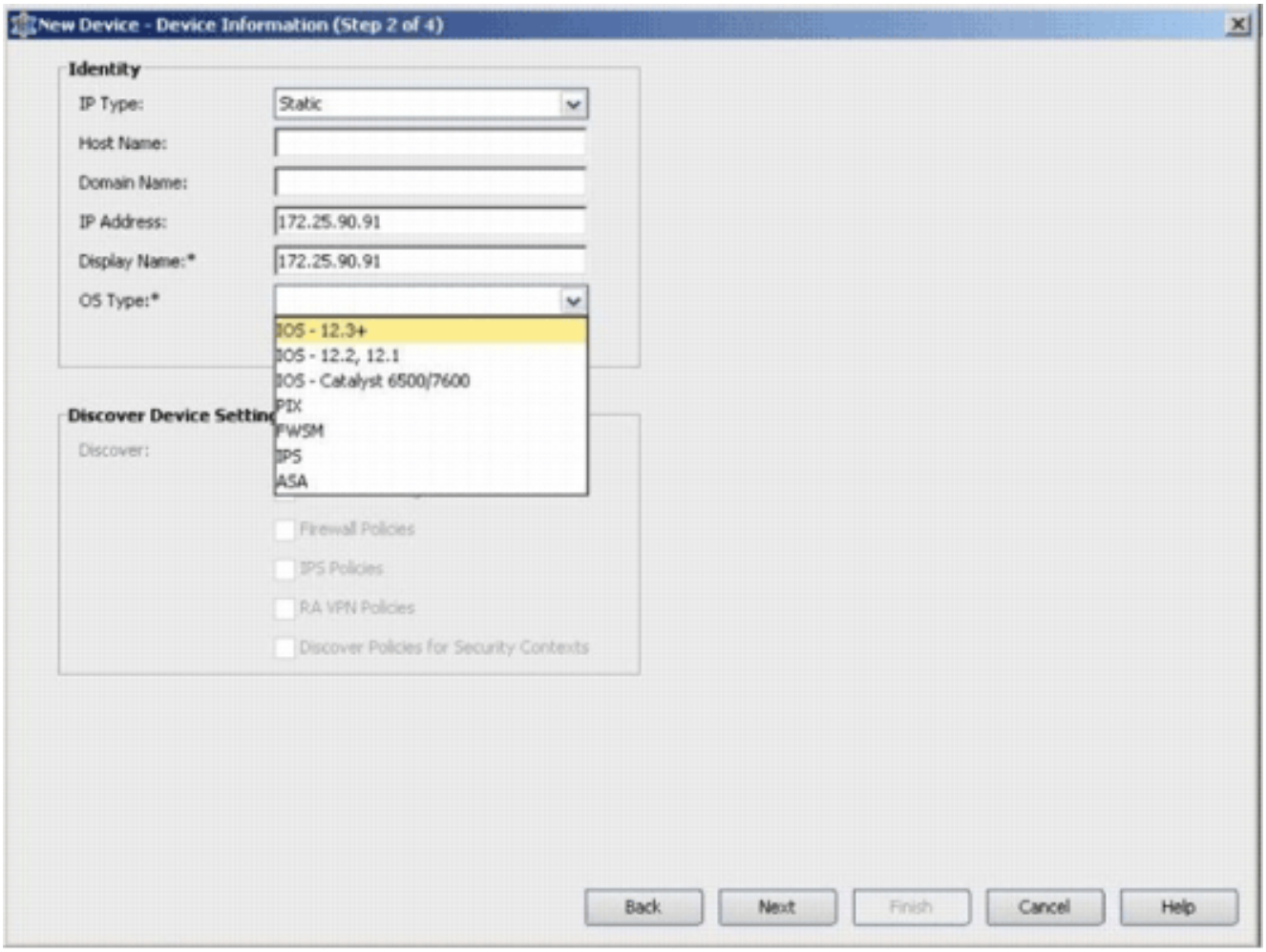
1. Ejecute el cliente Cisco Security Manager 3.1 desde su PC local.
2. Elija **Nuevo dispositivo** en el menú Archivo para agregar un dispositivo a Cisco Security Manager
   3.1.



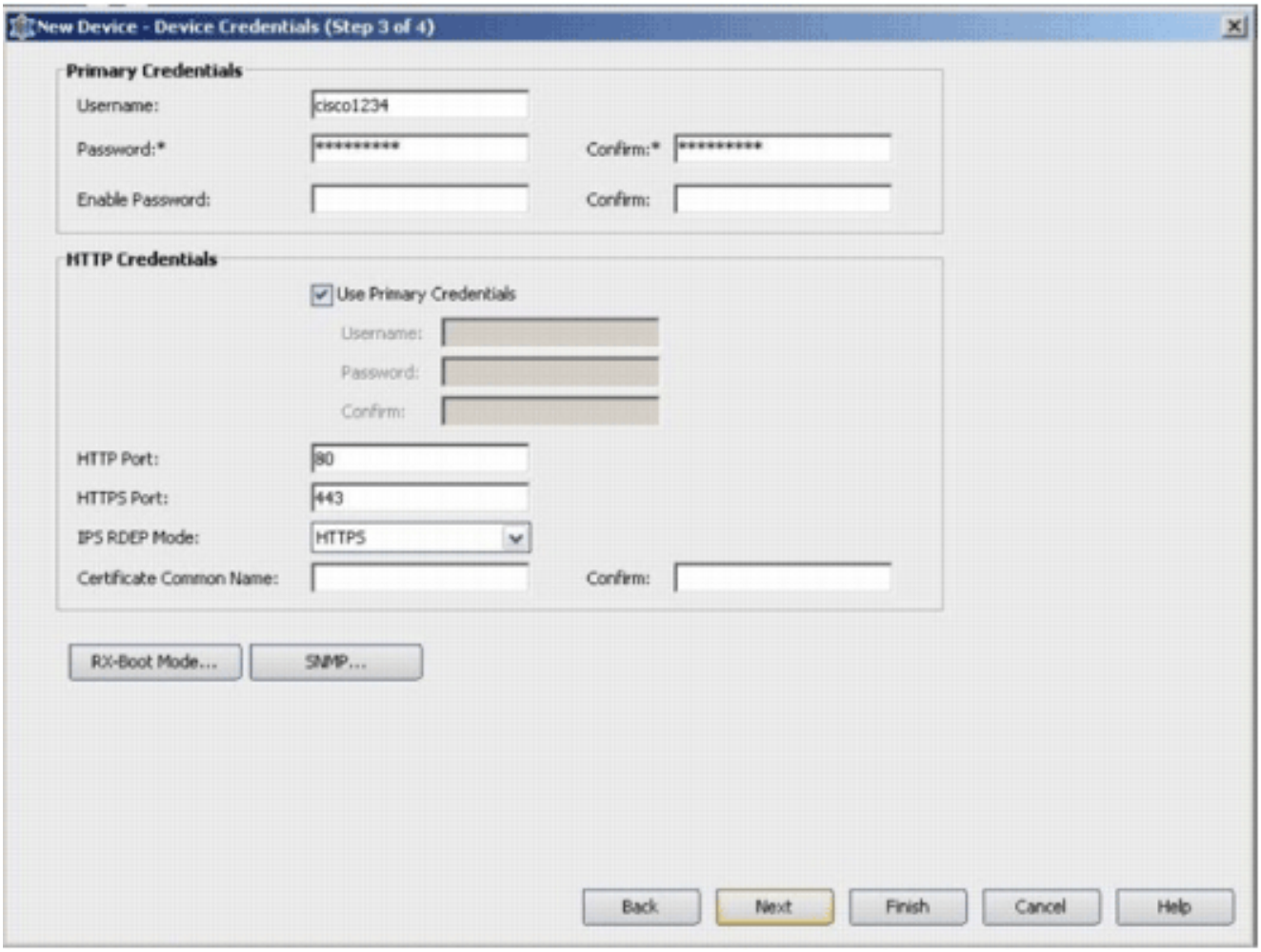
3. En la ventana Nuevo dispositivo, elija cómo desea agregar el dispositivo. Este ejemplo agrega el dispositivo desde la
   red.



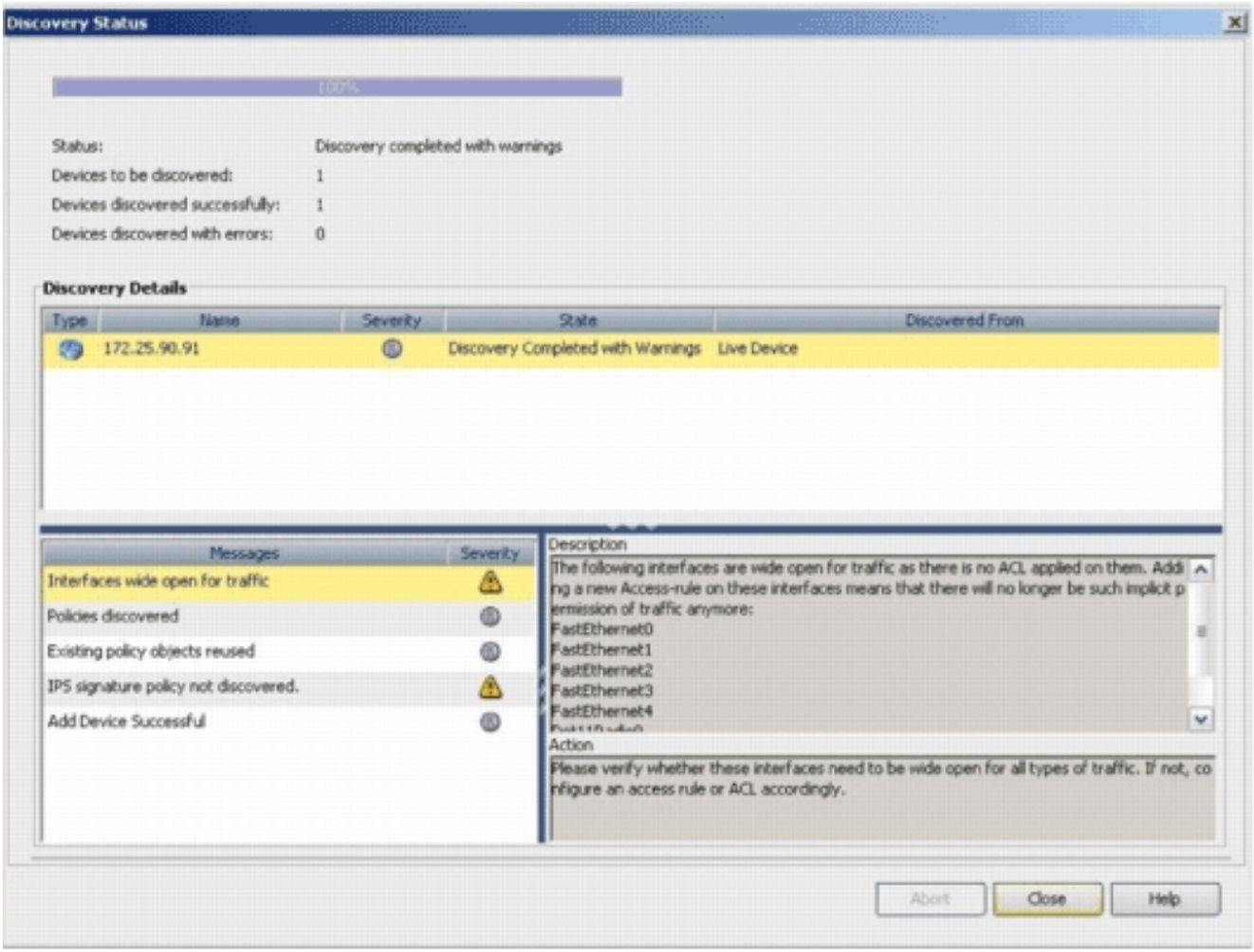
4. Haga clic en Next (Siguiente).
5. Introduzca los detalles de identidad del dispositivo que desea agregar. Por ejemplo, nombre de host y dirección
   IP.



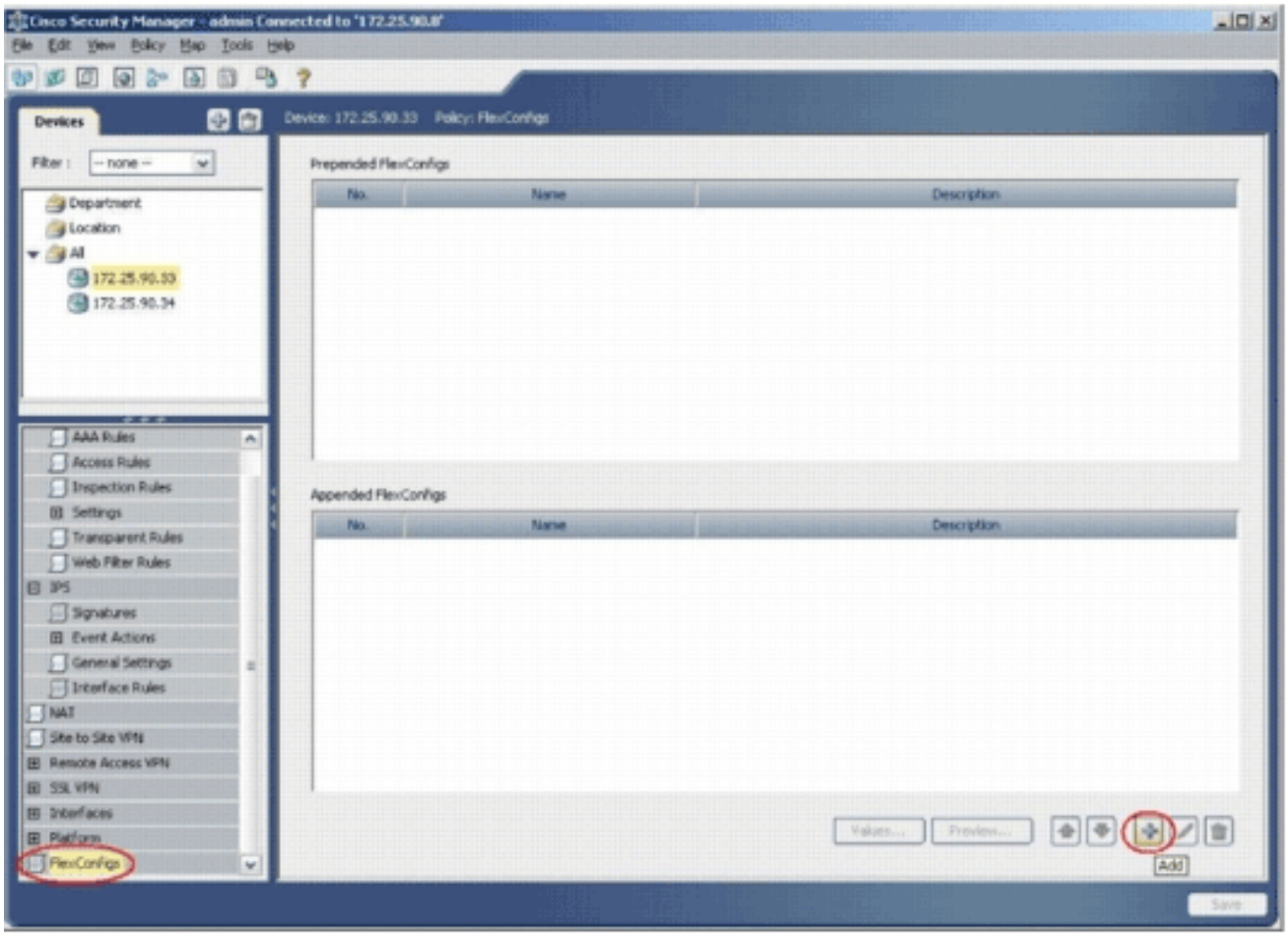
6. Haga clic en Next (Siguiente).
7. Introduzca las credenciales principales, como el nombre de usuario, la contraseña o la contraseña Enable para el router IOS que desea agregar.
8. Haga clic en **Finalizar** para agregar el dispositivo a Cisco Security Manager.**Nota:** En este ejemplo se asume que el usuario ya tiene un router preconfigurado y puede iniciar sesión en el router con las credenciales
adecuadas.



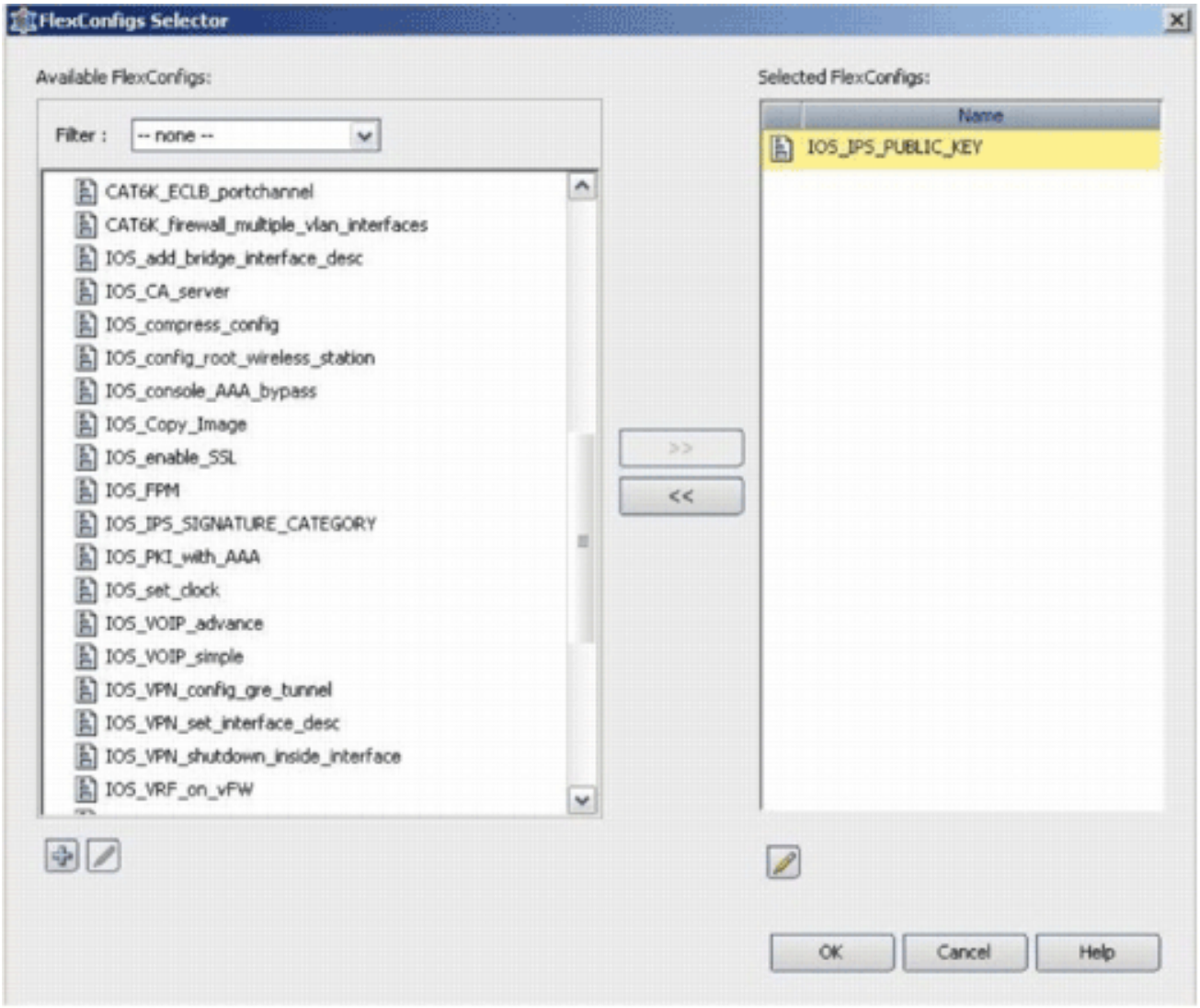
Cuando aparece "Detección finalizada" en la ventana Estado de detección, ha agregado correctamente un dispositivo a Cisco Security Manager. Una vez que haya agregado correctamente un dispositivo en Cisco Security Manager, debe asignar una clave pública para habilitar
IPS.



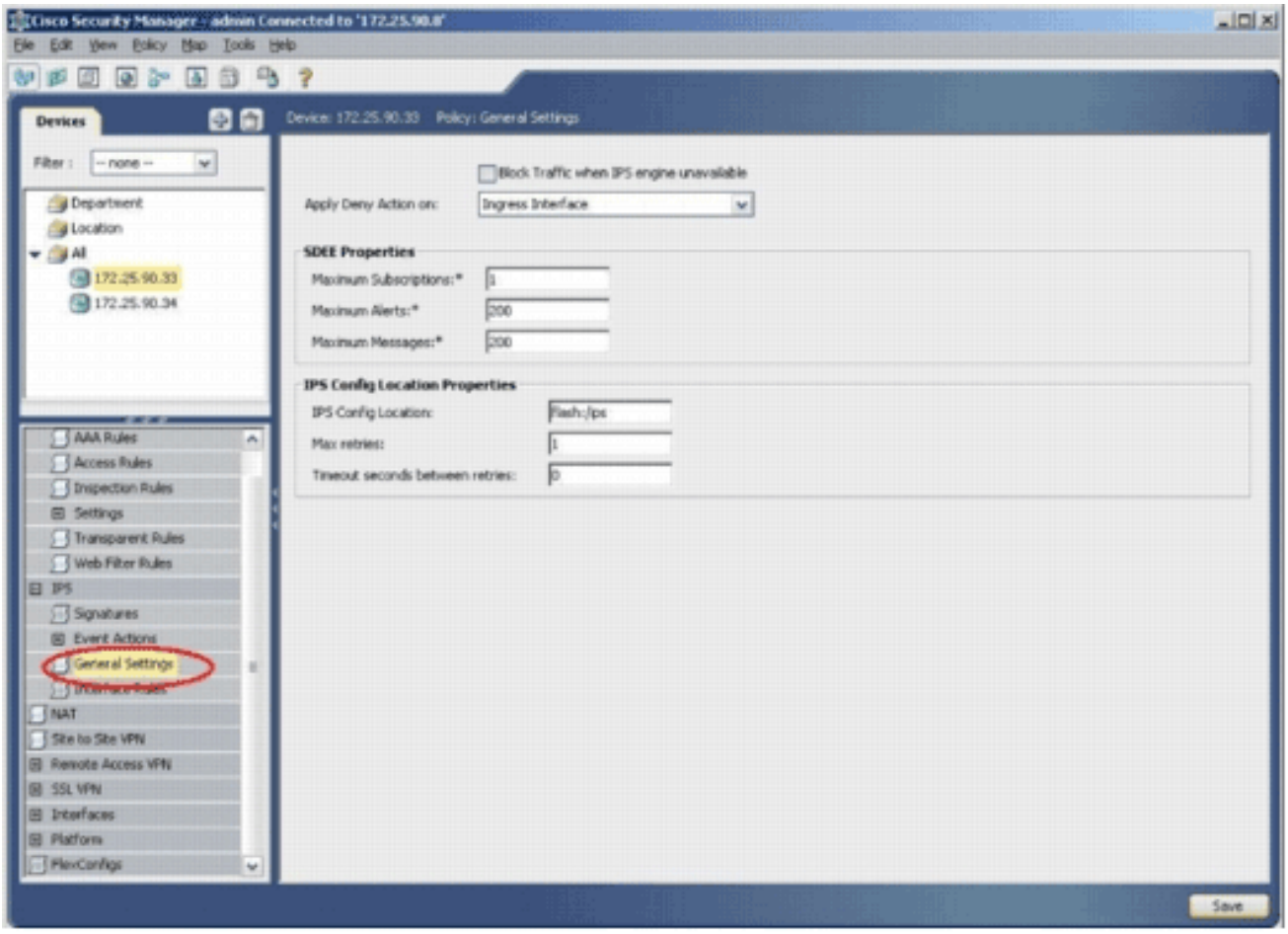
9. En el menú de la izquierda, vaya a la pantalla de configuración de FlexConfigs.
10. Haga clic en la interfaz de usuario de FlexConfigs en el lado derecho de la pantalla y, a continuación, haga clic en el icono
    Agregar.



11. En la lista FlexConfigs seleccionados, elija **IOS_IPS_PUBLIC_KEY** y haga clic en **Aceptar**.

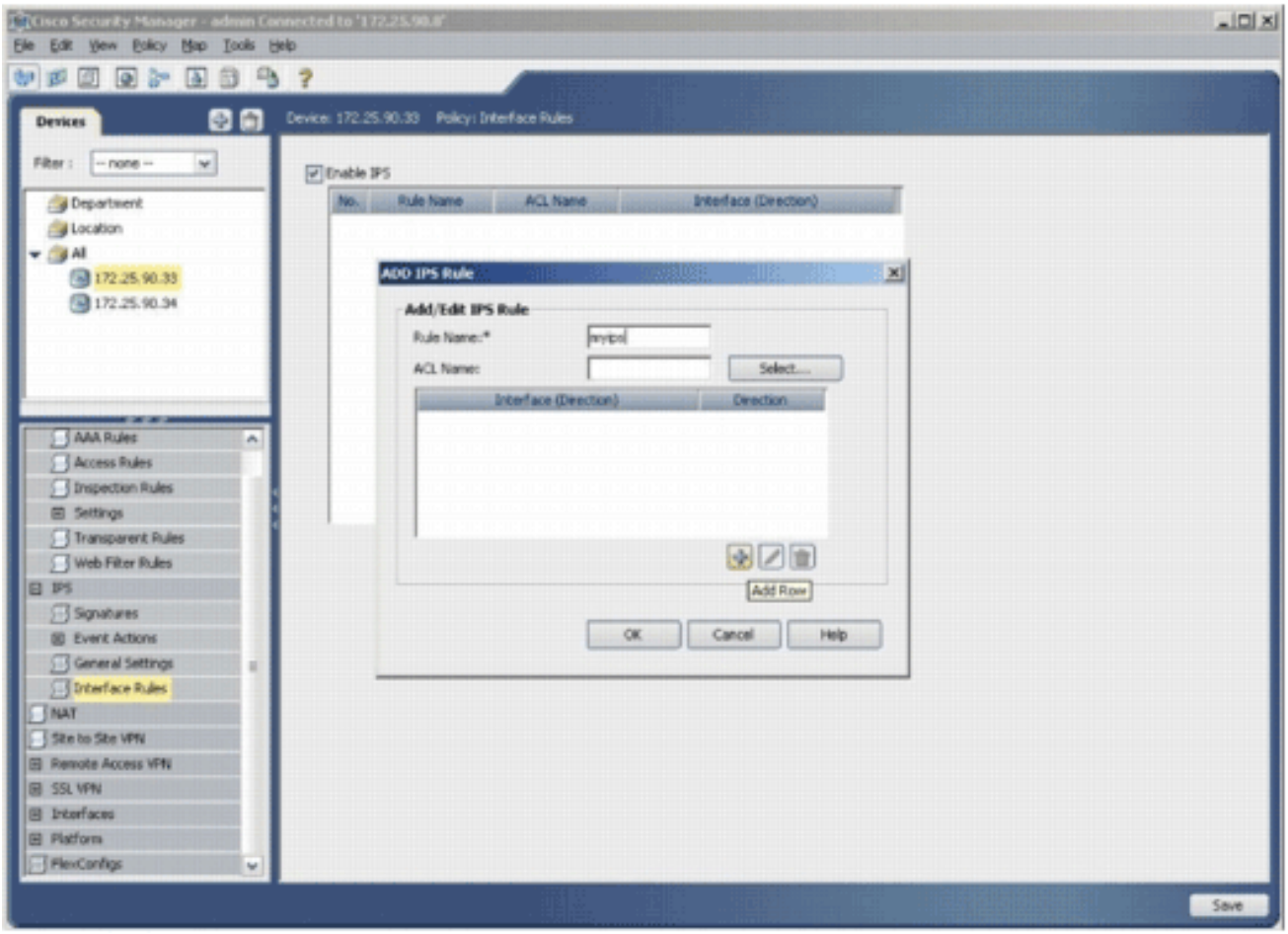


12. Haga clic en **Guardar** para guardar los cambios.**Nota:** La FlexConfig de IOS_IPS_PUBLIC_KEY contiene la configuración para la clave pública.
13. En el menú de la izquierda, elija **General Settings**, situado debajo del encabezado IPS.
14. Introduzca la ubicación de configuración IPS en la memoria flash. Ésta es la ubicación en la que se ubican las configuraciones IPS.
15. Haga clic en **Guardar** para guardar los cambios.

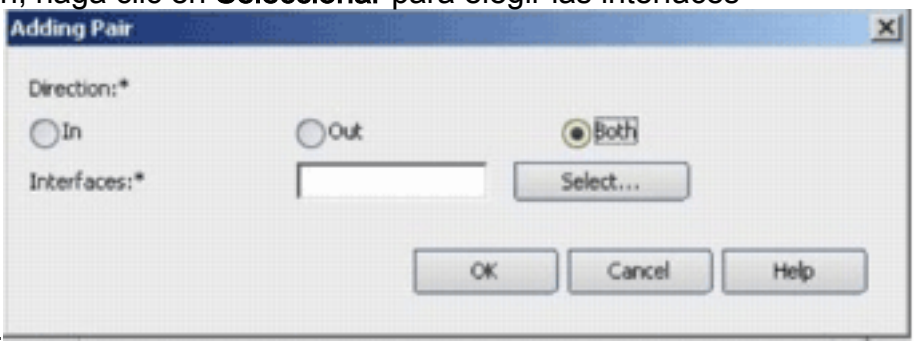


Nota: Asegúrese de que el directorio de ubicación ya se ha creado en la memoria flash del router. Si no es así, utilice el comando **mkdir <directory_name>** para crear el directorio de ubicación.

16. Para habilitar IPS, navegue hasta Reglas de interfaz, marque la casilla de verificación **Enable IPS** y luego haga clic en **Add Row**.
17. En el cuadro de diálogo Agregar regla IPS, introduzca un nombre para la regla IPS en el campo Nombre de regla y, a continuación, haga clic en **Agregar fila** para incluir las interfaces en las que se debe aplicar
IPS.

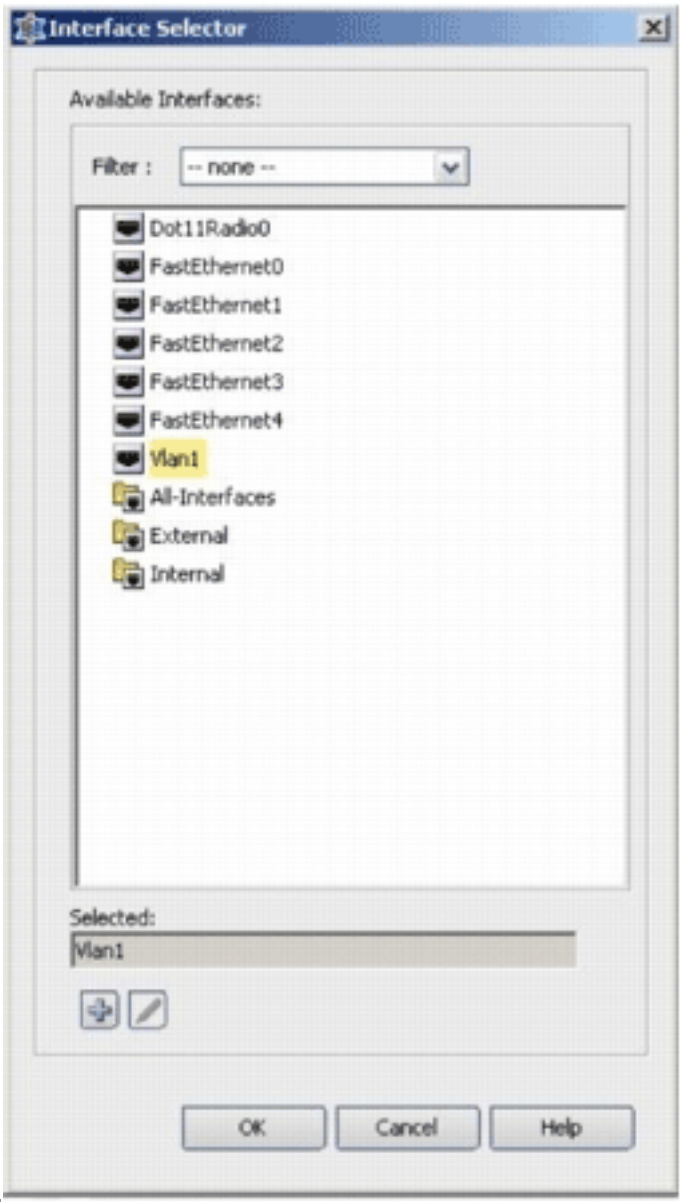


18. Haga clic en el botón de opción que indica en qué dirección debe aplicarse la regla IPS y, a continuación, haga clic en **Seleccionar** para elegir las interfaces



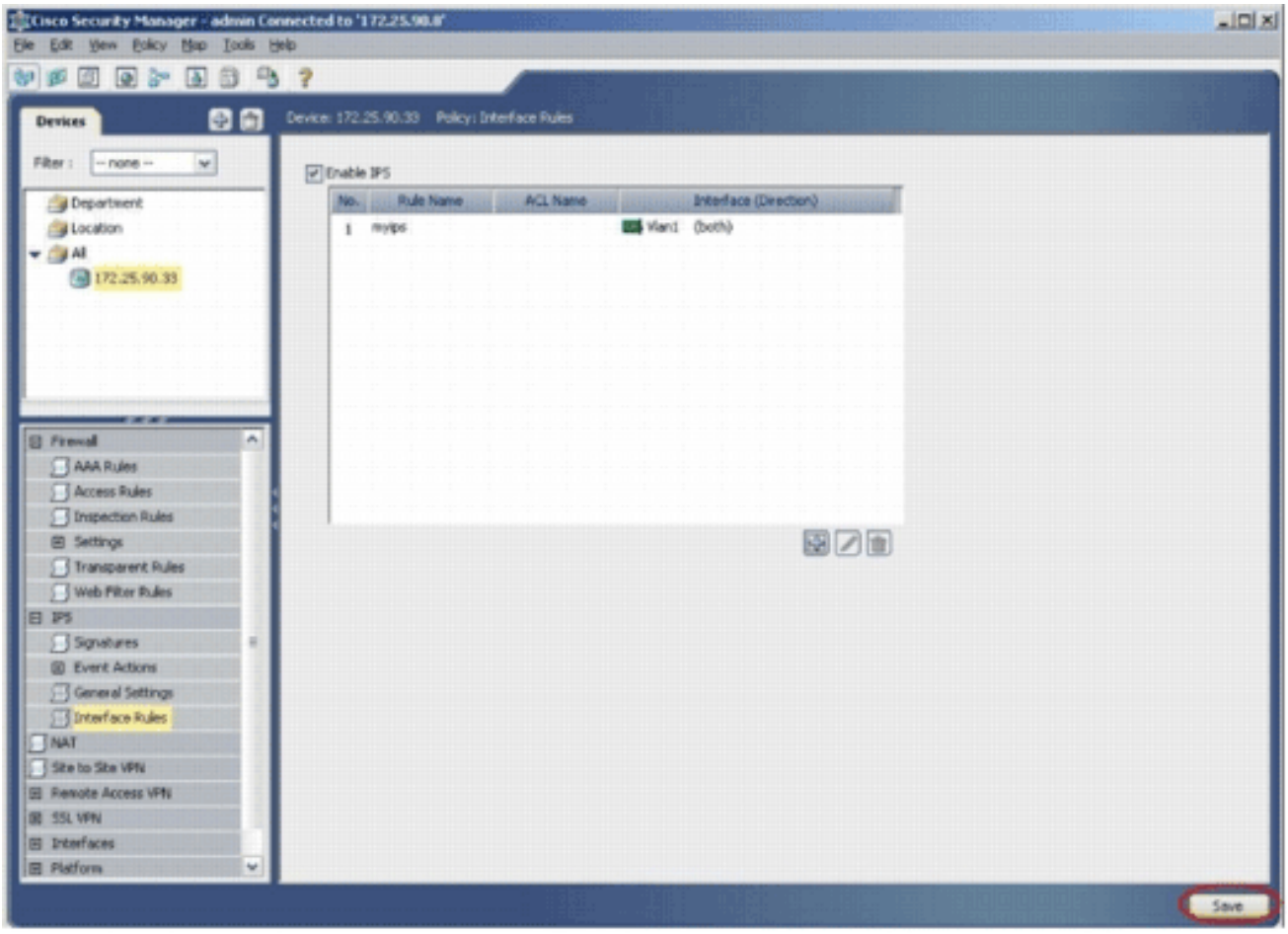
adecuadas.

19. Elija una interfaz de la lista Selector de interfaces y haga clic en

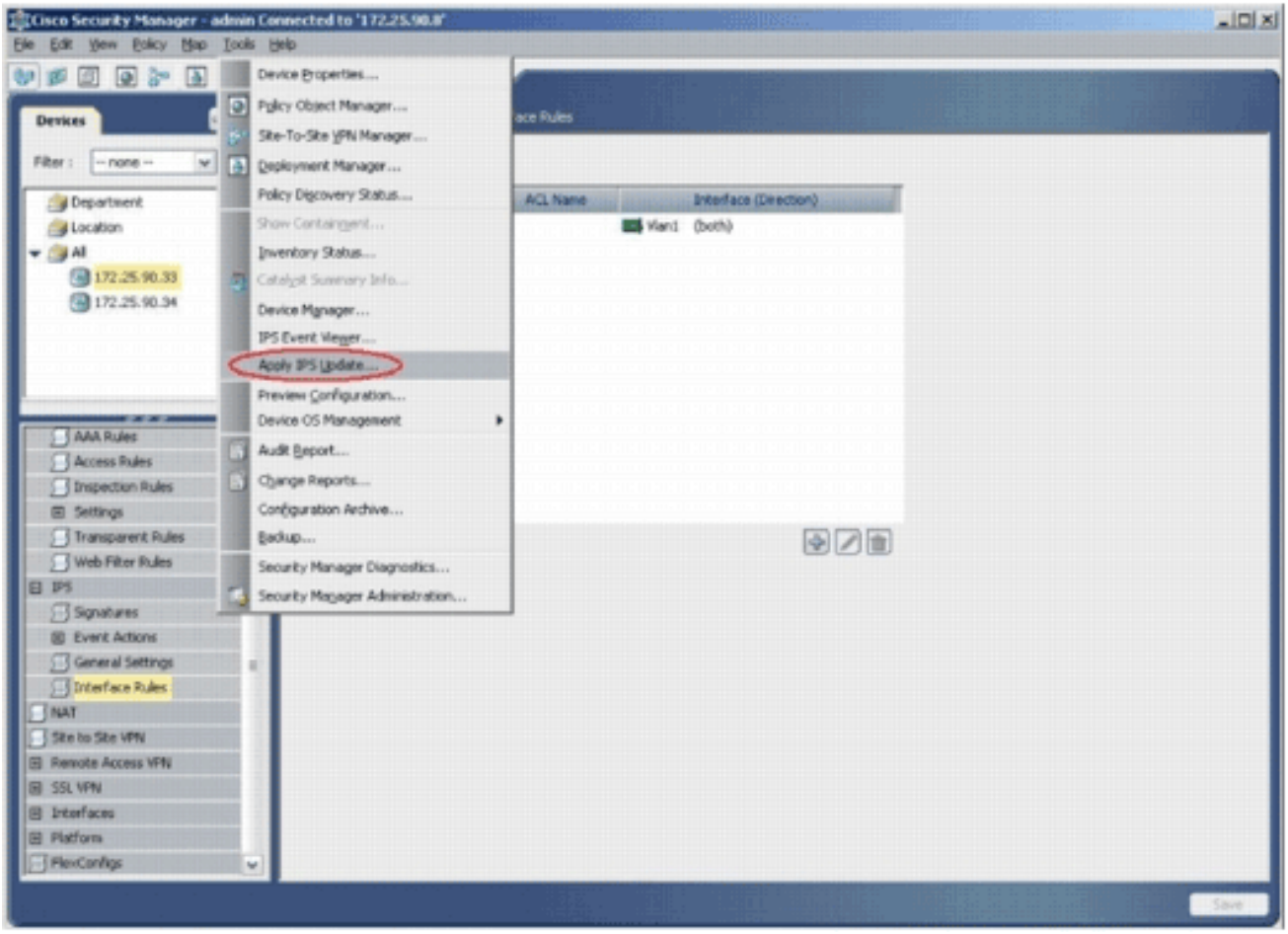


Aceptar.

20. Haga clic en **Guardar** para guardar los cambios.

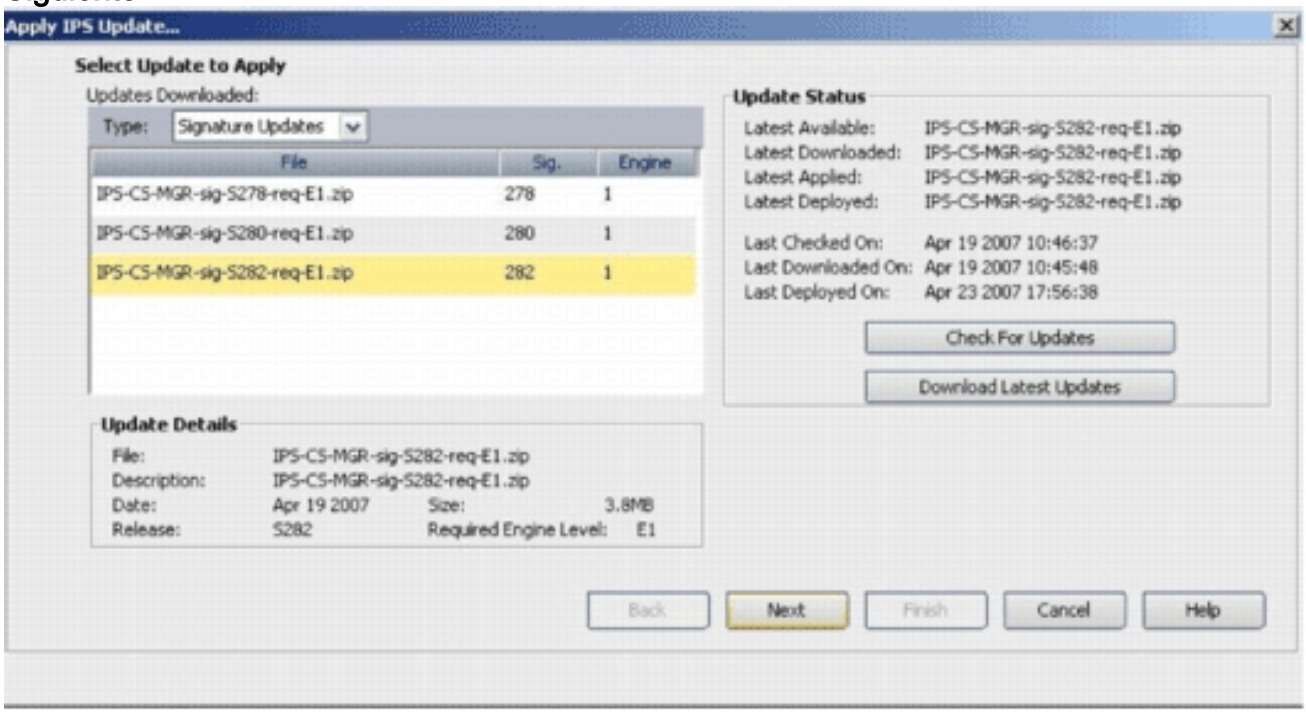


21. Elija **Tools > Apply IPS Update** para instalar las firmas IPS más recientes.

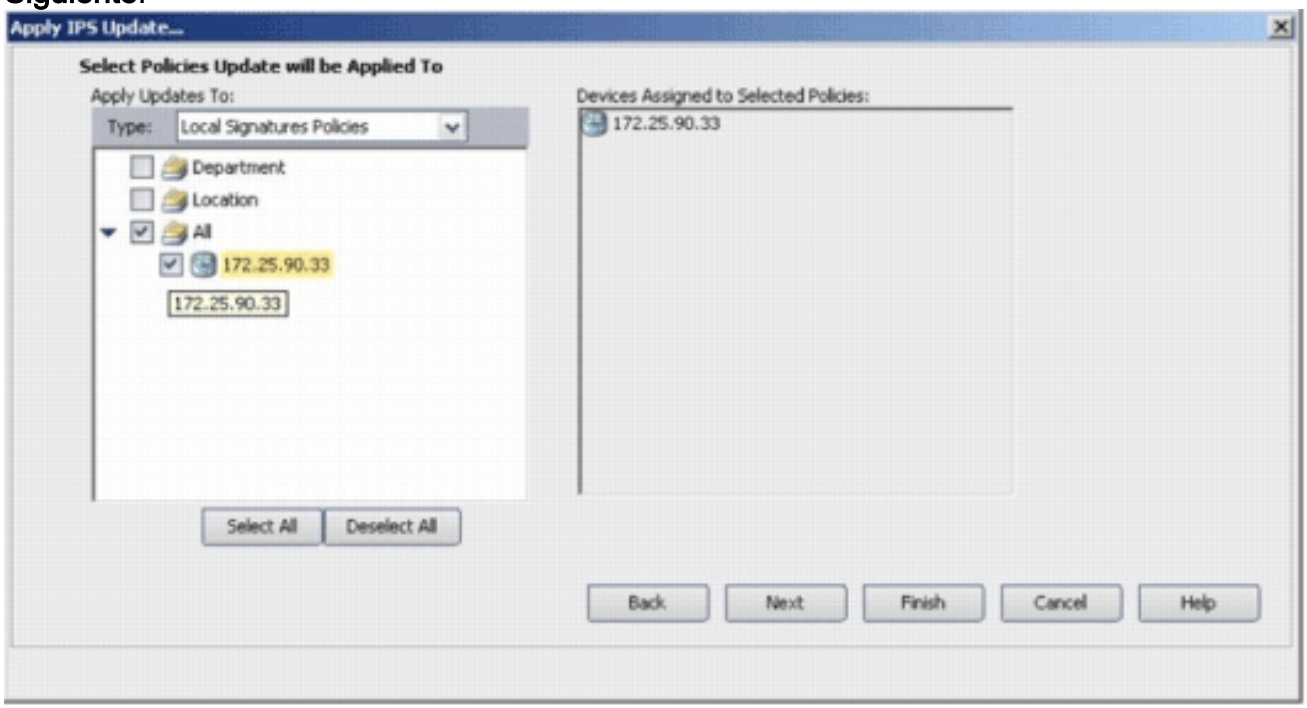


22. Elija el archivo de firma más reciente y haga clic en

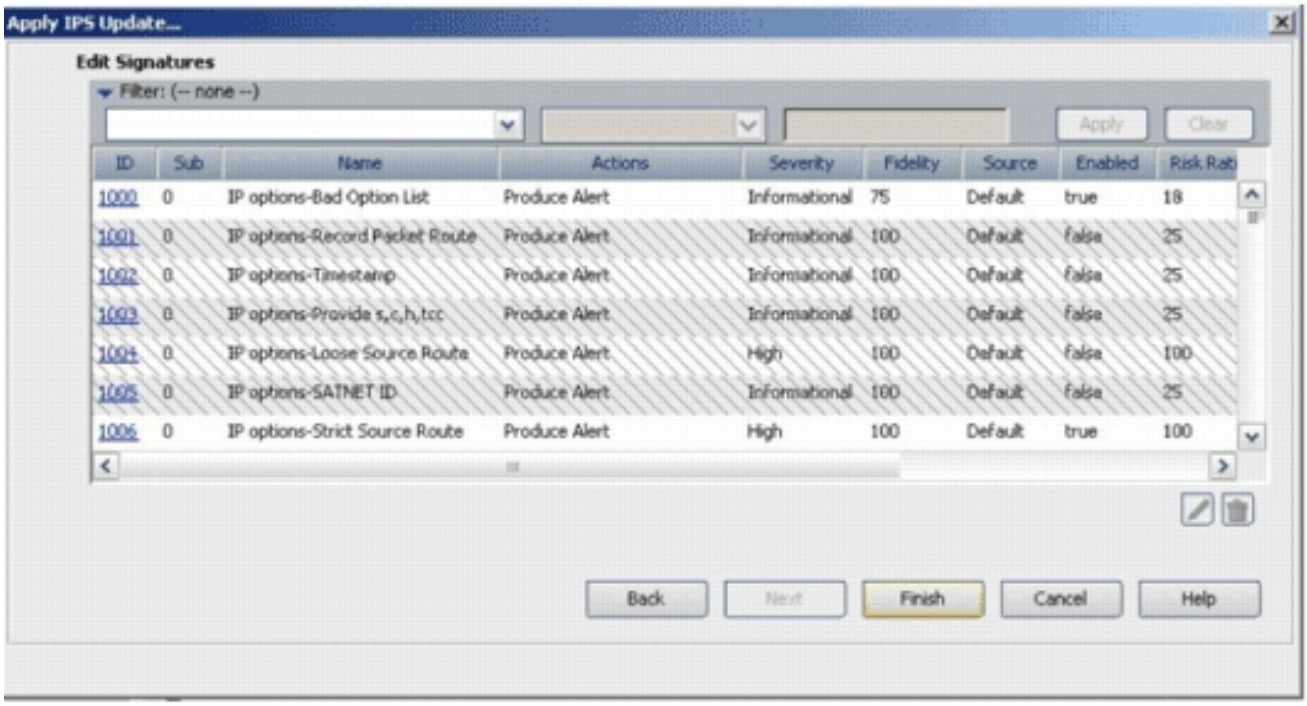
Siguiente.



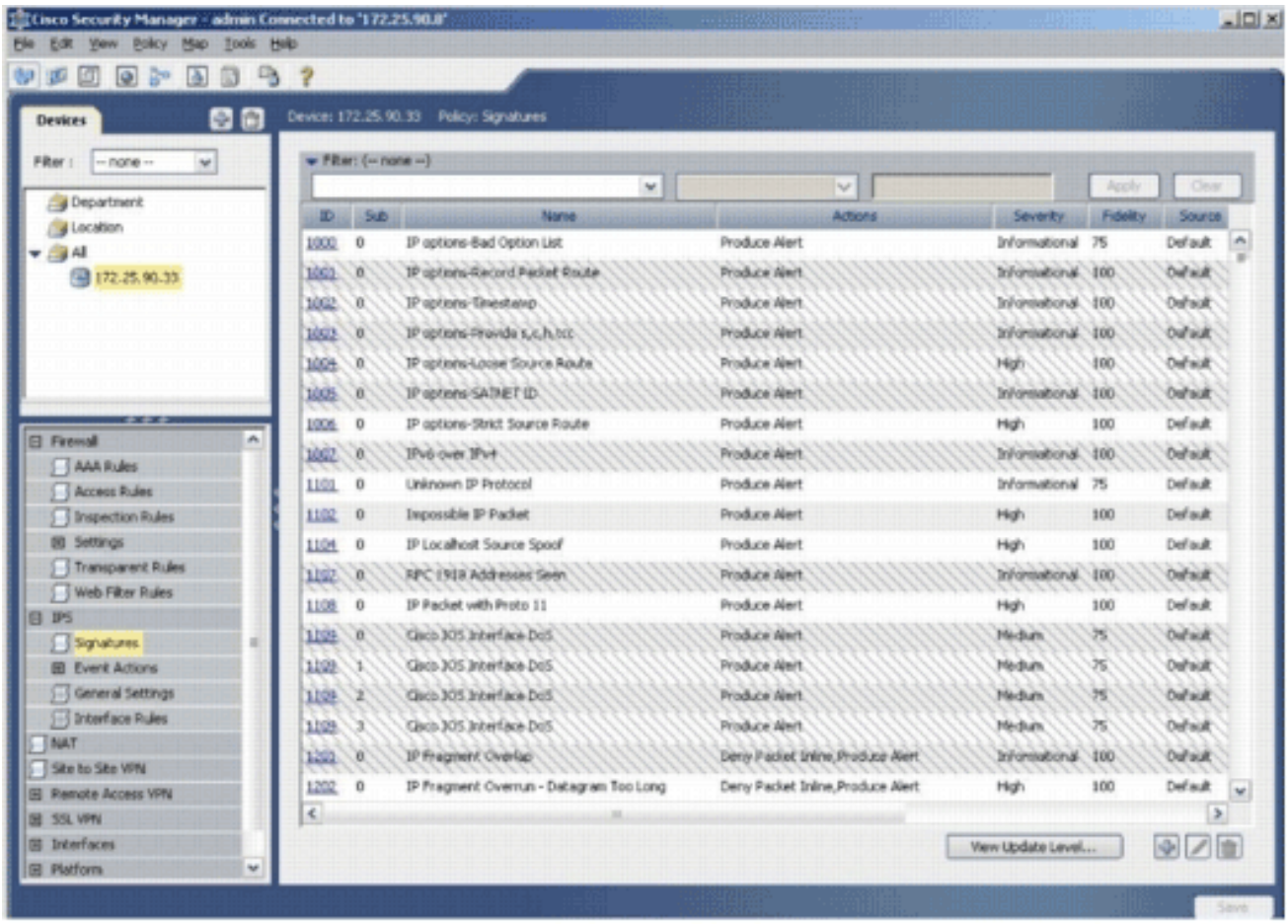
23. Elija los dispositivos en los que se debe aplicar la actualización IPS y haga clic en Siguiente.



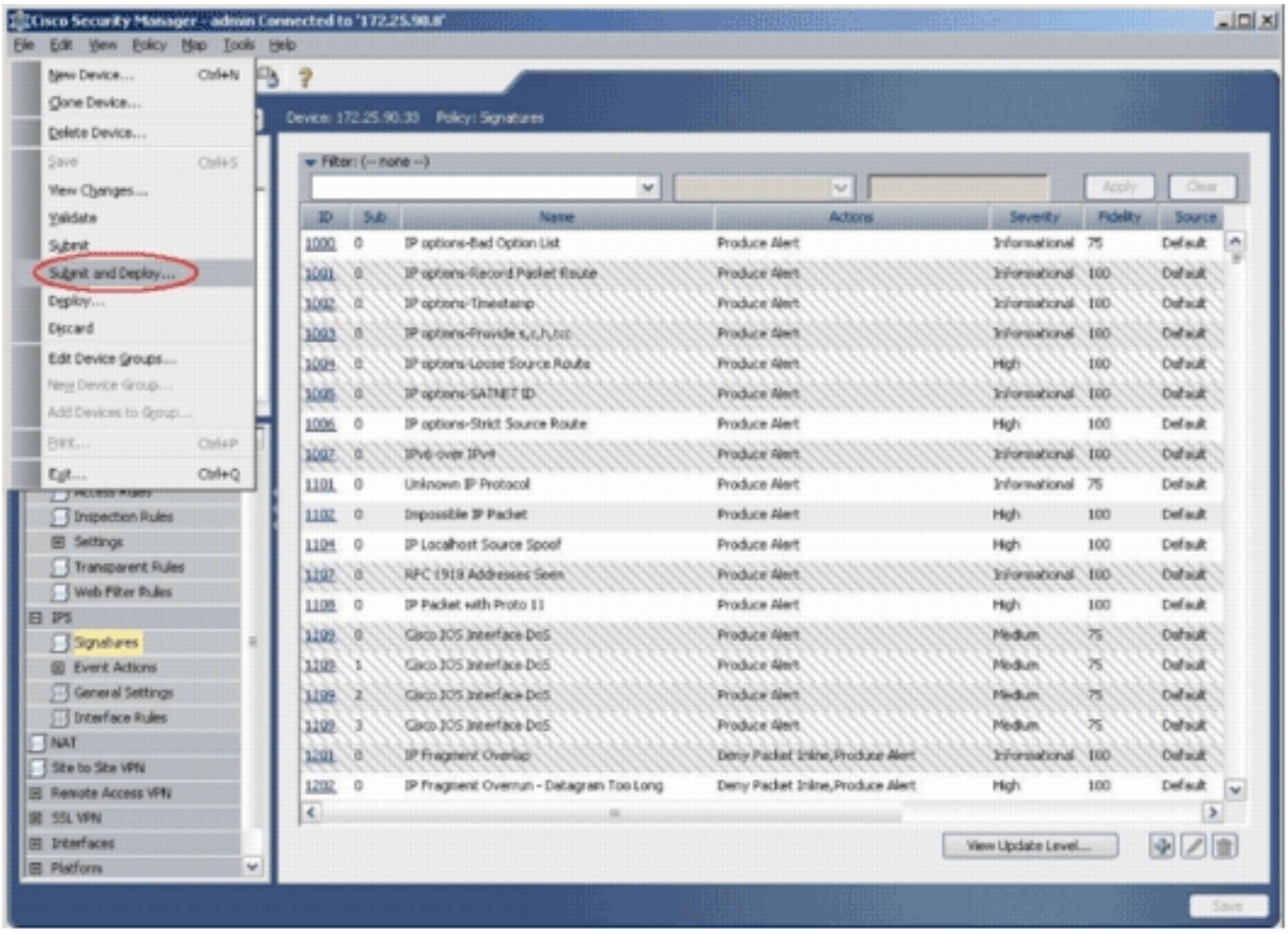
24. Haga clic en **Finalizar** para aplicar las firmas.



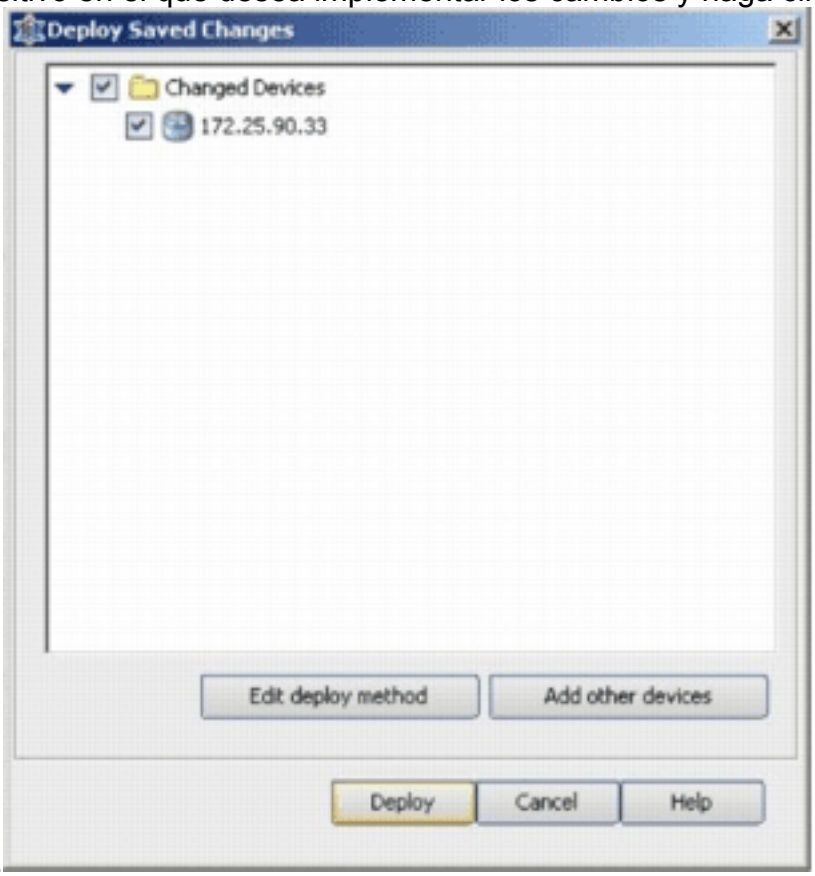
25. Navegue hasta IPS y elija **Firmas** para ver la lista de todas las firmas.



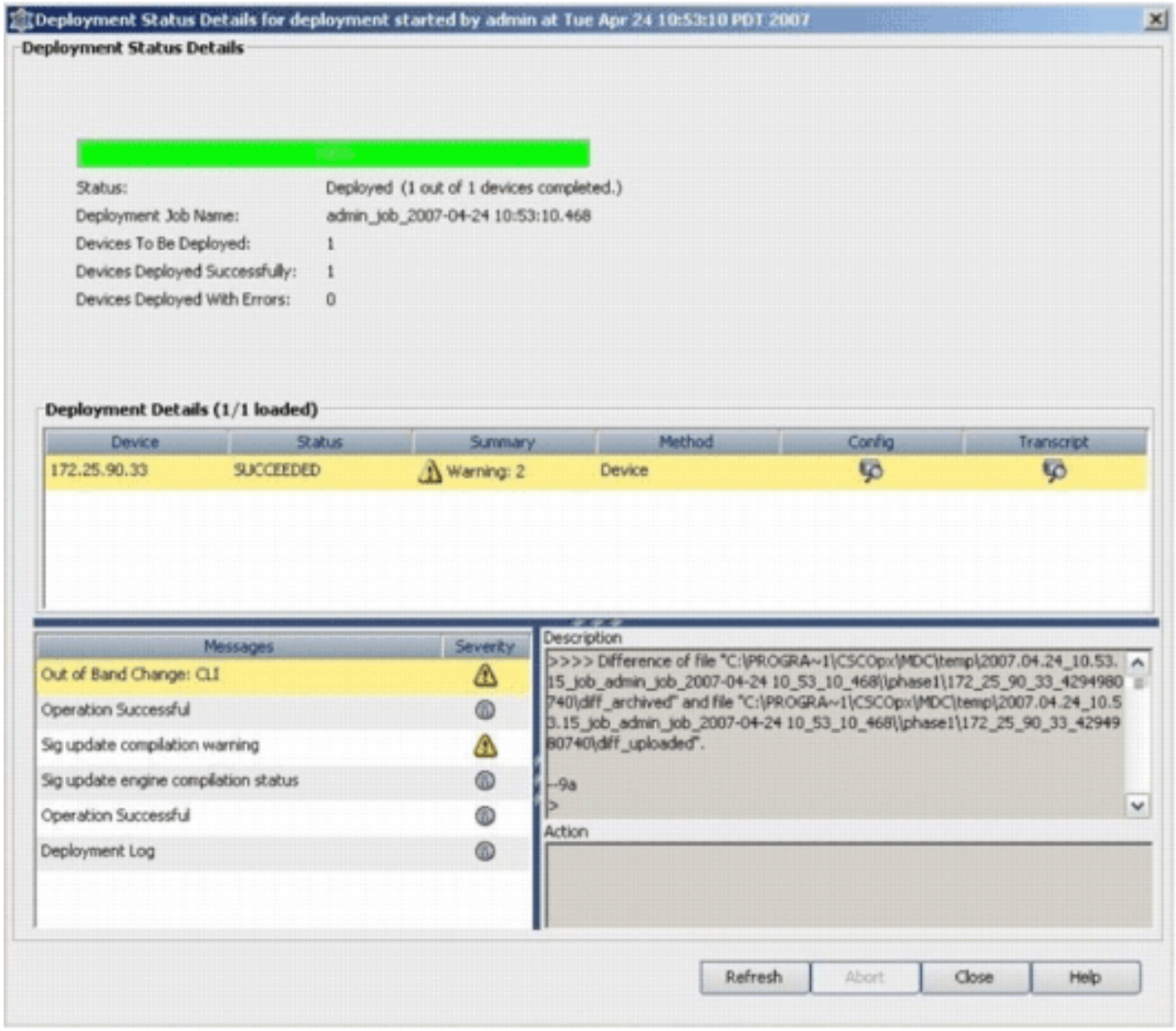
26. Elija **File > Submit and Deploy** para implementar IPS en el router IOS.



27. Elija el dispositivo en el que desea implementar los cambios y haga clic en **Implementar**.



28. Vea el estado de implementación para verificar si hay algún error.



Información Relacionada

- Página de productos y servicios de Cisco IOS Intrusion Prevention System (IPS)
- Introducción a Cisco IOS IPS con formato de firma 5.x
- Compatibilidad con formato de firma IPS 5.x y mejoras de uso
- Cisco Intrusion Prevention System
- Avisos de campo de productos de seguridad (incluida CiscoSecure Intrusion Detection)
- Soporte Técnico - Cisco Systems