Configurar o Cisco IOS IPS com um roteador e um SDM

Contents

Introduction

Este documento descreve como usar o Cisco Router and Security Device Manager (SDM) versão 2.5 para configurar o Cisco IOS® Intrusion Prevention System (IPS) em 12.4(15)T3 e versões posteriores.

As melhorias no SDM 2.5 relacionadas ao IOS IPS são:

- Número total de assinatura compilada exibido na GUI da lista de assinaturas
- Arquivos de assinatura SDM (formato de arquivo zip; por exemplo, sigv5-SDM-S307.zip) e pacotes de assinatura CLI (formato de arquivo pkg; por exemplo, IOS-S313-CLI.pkg) podem ser baixados juntos em uma operação
- Os pacotes de assinatura baixados podem ser enviados automaticamente para o roteador como uma opção

As tarefas envolvidas no processo de provisionamento inicial são:

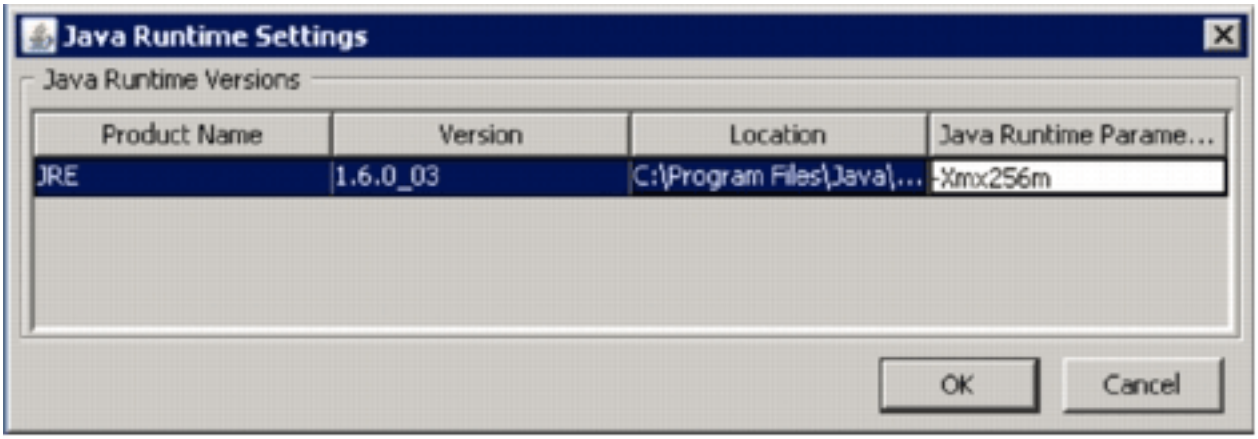
1. Baixe e instale o SDM 2.5.
2. Use a Atualização automática do SDM para fazer o download do pacote de assinatura do IOS IPS para um PC local.
3. Inicie o Assistente de políticas de IPS para configurar o IPS do IOS.
4. Verifique se a configuração e as assinaturas do IOS IPS estão carregadas corretamente

O Cisco SDM é uma ferramenta de configuração baseada na Web que simplifica a configuração de roteador e segurança por meio de assistentes inteligentes que ajudam os clientes a implantar, configurar e monitorar um roteador Cisco de forma rápida e fácil, sem exigir conhecimento da interface de linha de comando (CLI).

O SDM versão 2.5 pode ser baixado do Cisco.com em http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (somente clientes registrados) . A nota de versão pode ser encontrada em http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr.25.html

Observação: o Cisco SDM exige uma resolução de tela de pelo menos 1024 x 768.

Observação: o Cisco SDM exige que o tamanho do heap da memória Java não seja inferior a 256 MB para configurar o IOS IPS. Para alterar o tamanho do heap da memória Java, abra o painel de controle Java, clique na guia **Java**, clique em **View** localizado em Java Applet Runtime Settings e digite **-Xmx256m** na coluna Java Runtime Parameter.



Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS IPS em 12.4(15)T3 e versões posteriores
- Cisco Router and Security Device Manager (SDM) versão 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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

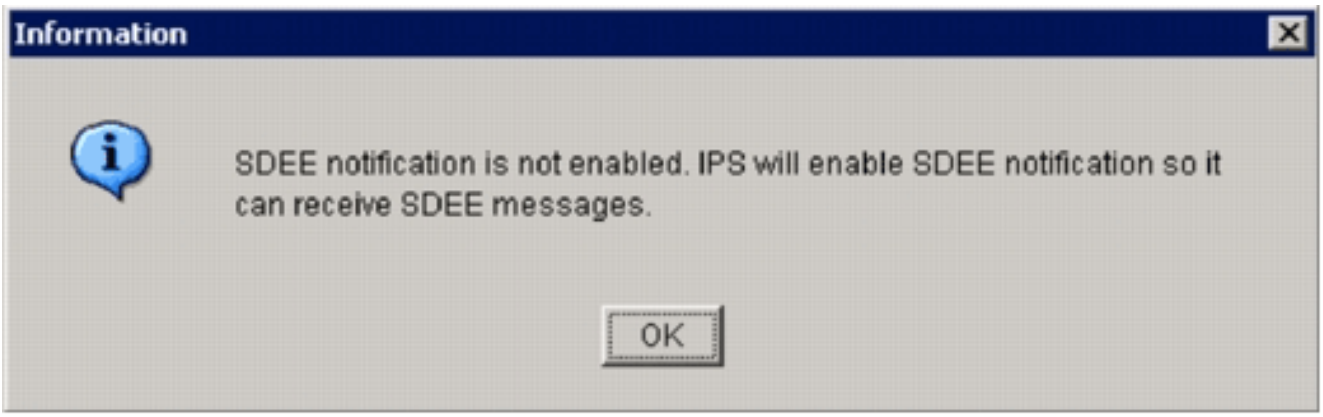
Observação: abra um console ou uma sessão telnet para o roteador (com o 'monitor de prazo' ativado) para monitorar mensagens quando você usa o SDM para provisionar o IOS IPS.

1. Baixe o SDM 2.5 do Cisco.com em http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (somente clientes registrados) e instale-o em um PC local.
2. Execute o SDM 2.5 do PC local.
3. Quando a caixa de diálogo IOS IPS Login for exibida, digite o mesmo nome de usuário e

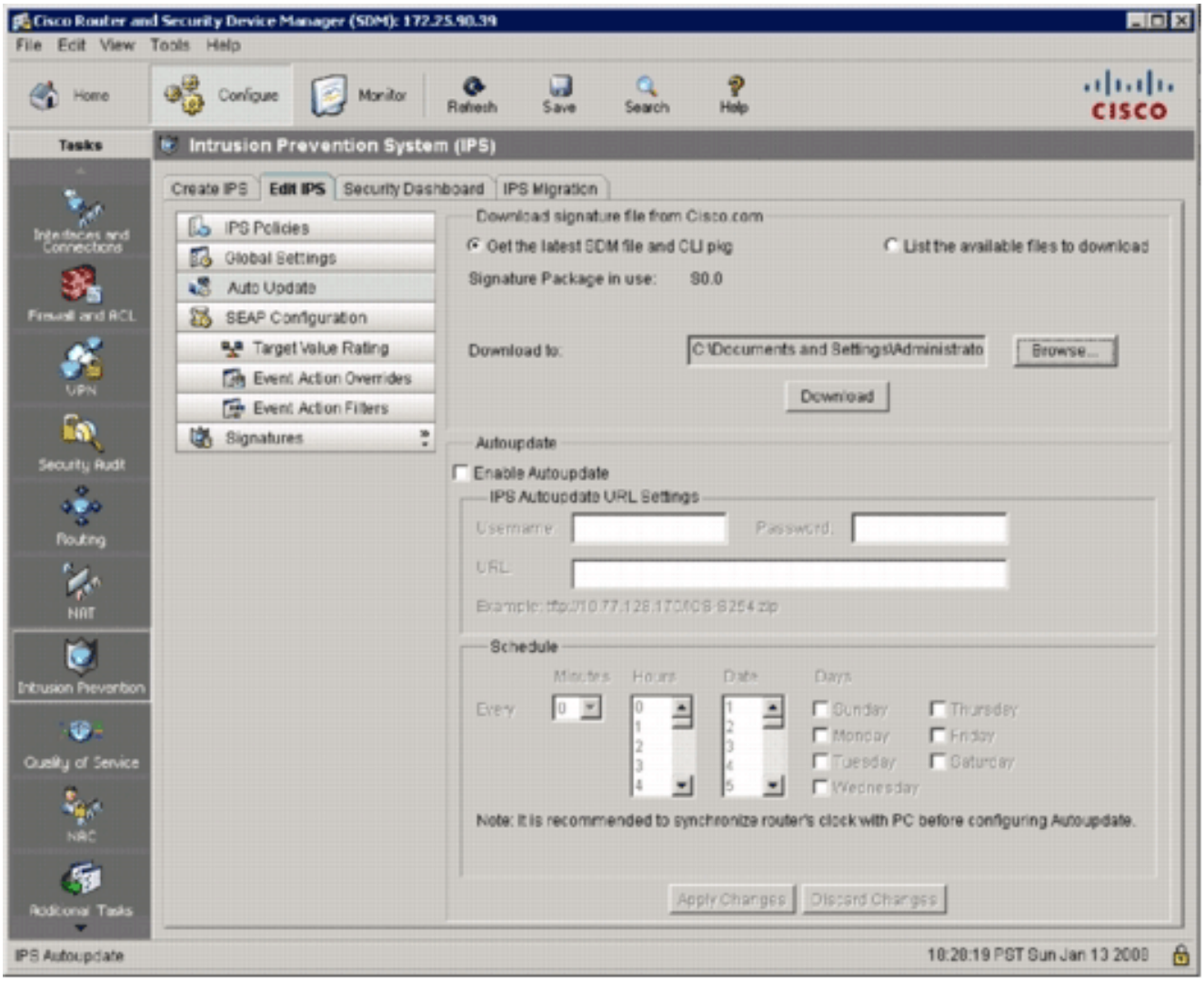
senha que você usa para autenticação SDM no

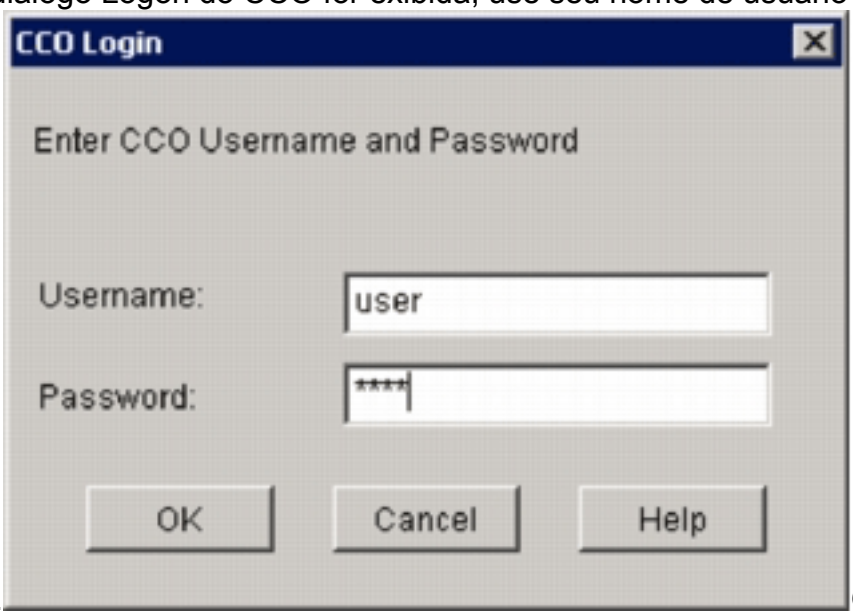

roteador.

4. Na interface de usuário SDM, clique em **Configure** e, em seguida, clique em **Intrusion Prevention**.
5. Clique na guia **Editar IPS**.
6. Se a notificação SDEE não estiver habilitada no roteador, clique em **OK** para habilitar a notificação
   SDEE.

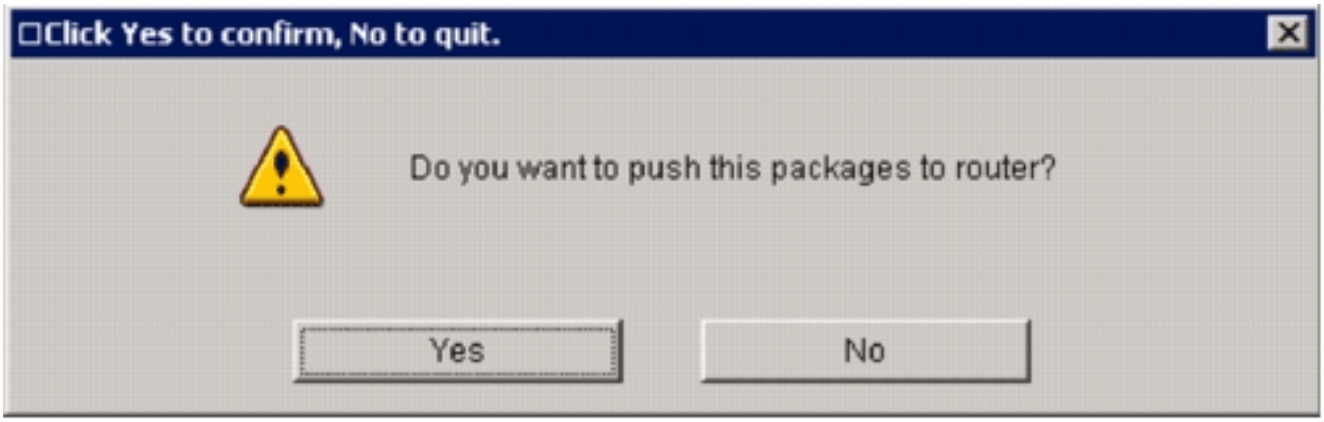


7. No arquivo de assinatura Download da área Cisco.com da guia Edit IPS, clique no botão de opção **Get the latest SDM file and CLI pkg e, em seguida, clique em Browse** para selecionar um diretório no PC local no qual salvar os arquivos baixados.Você pode escolher o diretório raiz do servidor TFTP ou FTP, que será usado posteriormente ao implantar o pacote de assinatura no roteador.
8. Clique em
   Download.

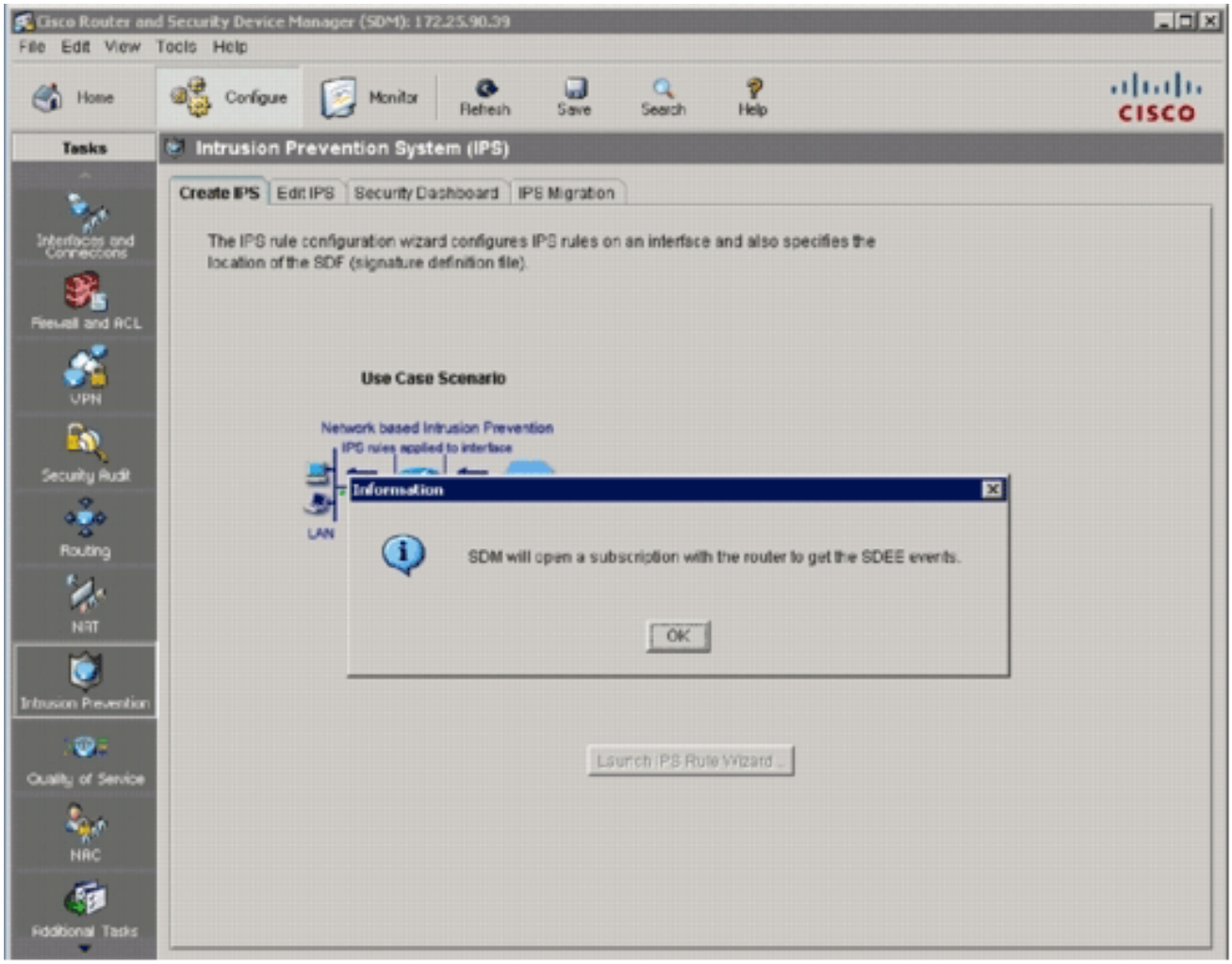


9. Quando a caixa de diálogo Logon do CCO for exibida, use seu nome de usuário e senha registrados do CCO. 

O SDM se conecta ao Cisco.com e começa a fazer o download do arquivo SDM (por exemplo, sigv5-SDM-S307.zip) e do arquivo pkg CLI (por exemplo, IOS-S313-CLI.pkg) para o diretório selecionado na etapa 7.Quando ambos os arquivos forem baixados, o SDM solicitará que você envie o pacote de assinatura baixado para o roteador.



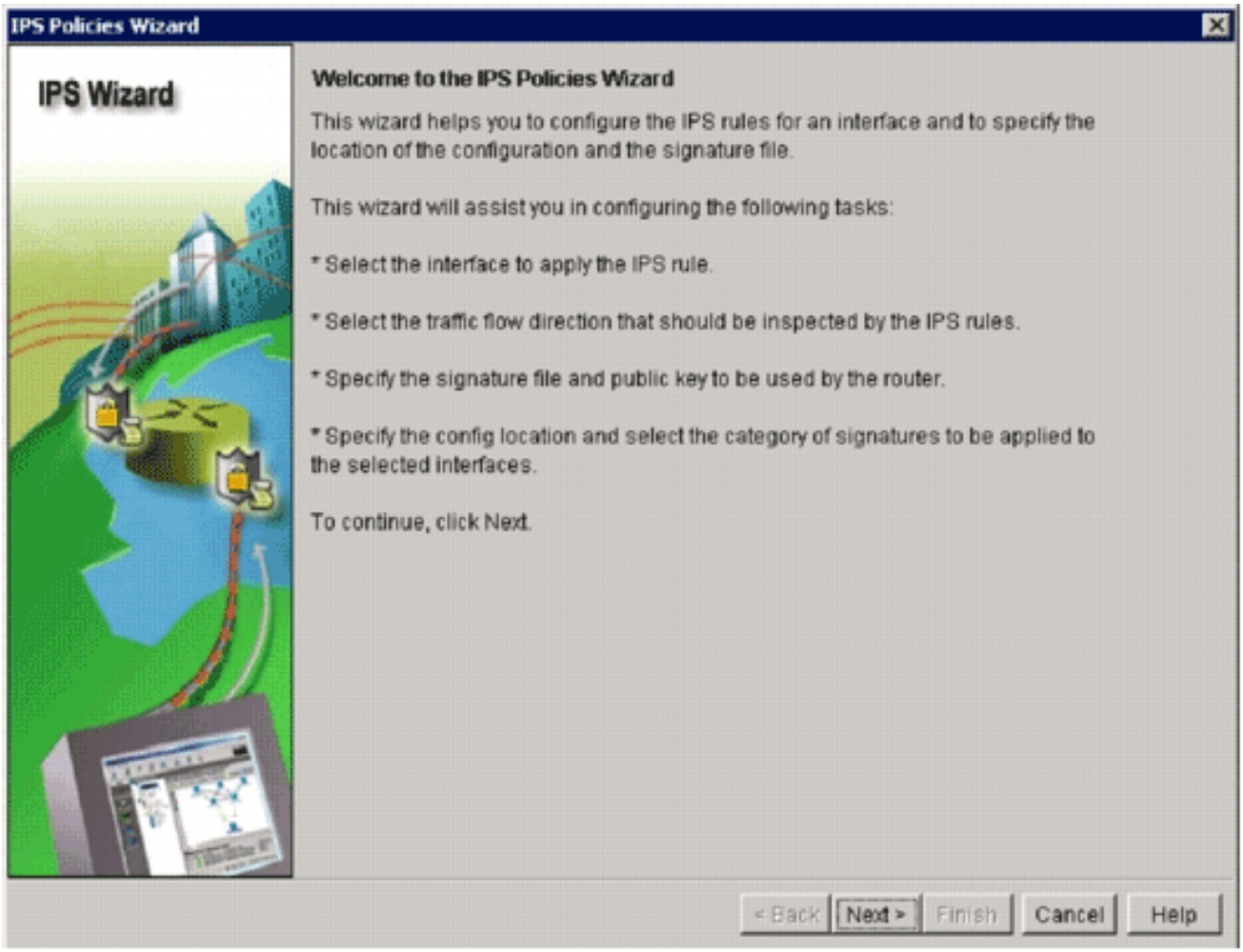
10. Clique em **Não**, pois o IOS IPS ainda não foi configurado no roteador.
11. Depois que o SDM baixar o pacote de assinatura da CLI do IOS mais recente, clique na guia **Create IPS** para criar a configuração inicial do IPS do IOS.
12. Se for solicitado que você aplique alterações no roteador, clique em **Apply Changes (Aplicar alterações)**.
13. Clique em **Iniciar Assistente de regra de IPS**.Uma caixa de diálogo é exibida para informá-lo de que o SDM precisa estabelecer uma assinatura SDEE no roteador para recuperar alertas.



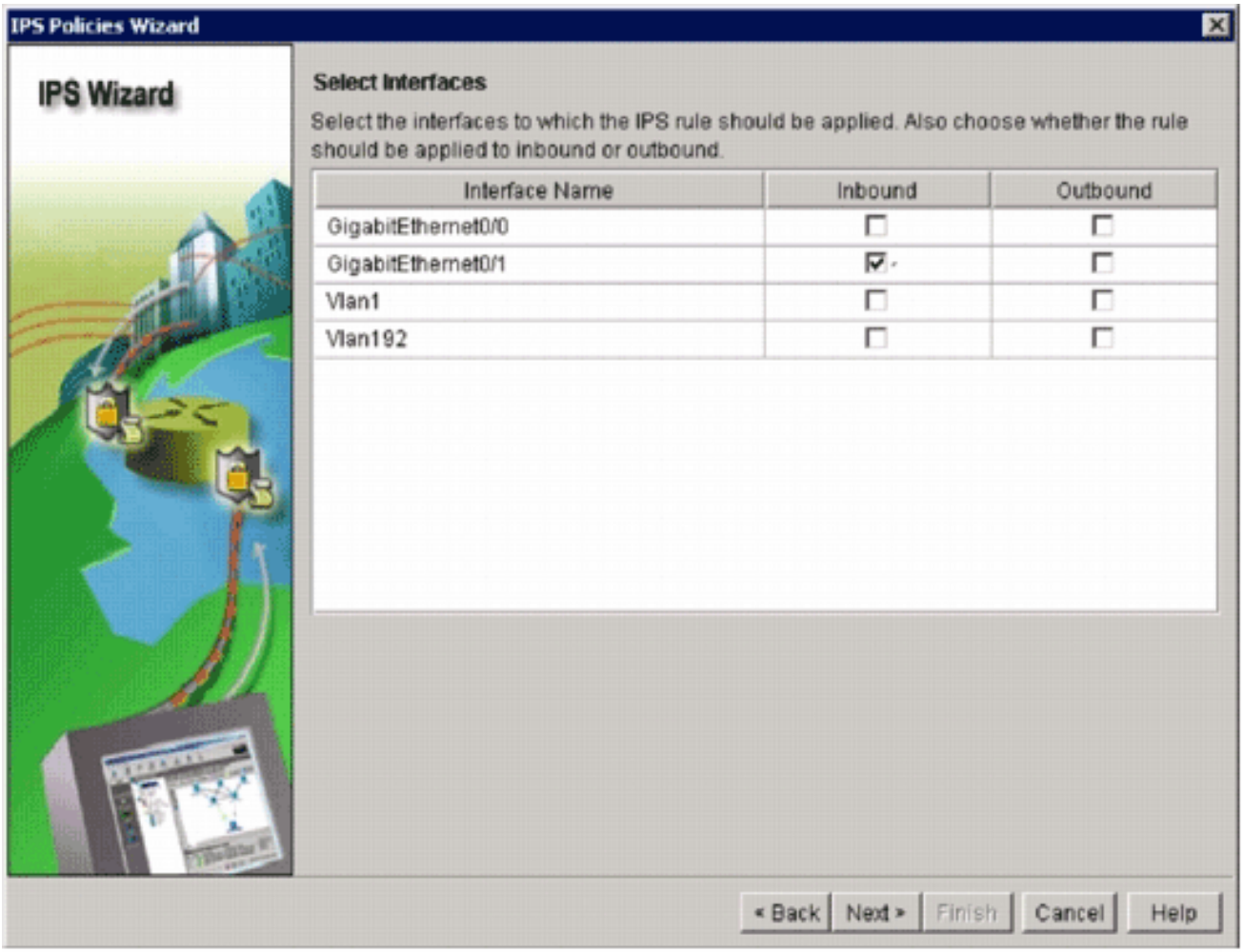
14. Click **OK**.A caixa de diálogo Autenticação necessária é

exibida.

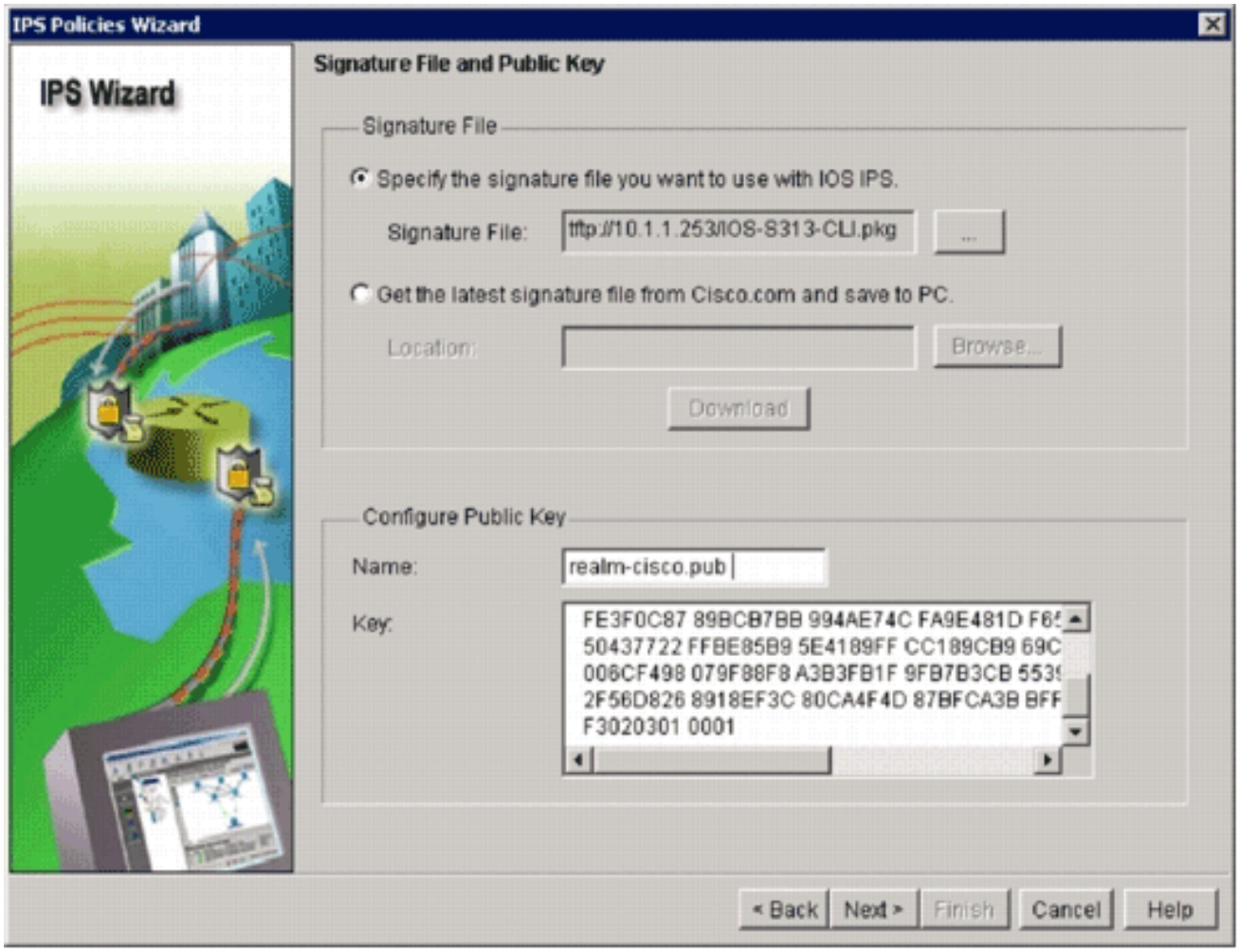
15. Insira o nome de usuário e a senha usados para que o SDM se autentique no roteador e clique em **OK**.A caixa de diálogo Assistente de políticas de IPS é exibida.



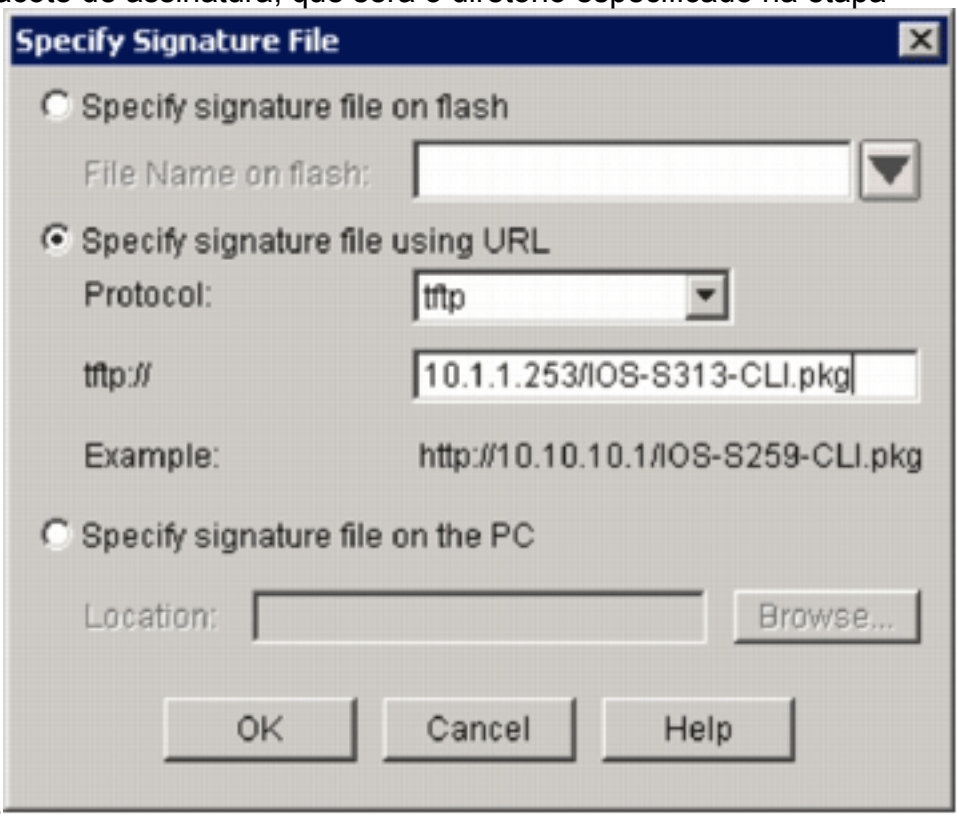
16. Clique em
    Next.



17. Na janela Interfaces selecionadas, escolha a interface e a direção para a qual o IOS IPS será aplicado e clique em **Avançar** para
    continuar.



18. Na área Arquivo de assinatura da janela Arquivo de assinatura e chave pública, clique no botão de opção **Especificar o arquivo de assinatura que deseja usar com o IOS IPS** e clique no botão de **Arquivo de assinatura** (...) para especificar a localização do arquivo de pacote de assinatura, que será o diretório especificado na etapa



7.

19. Clique no botão de opção **Especificar arquivo de assinatura usando URL** e escolha um

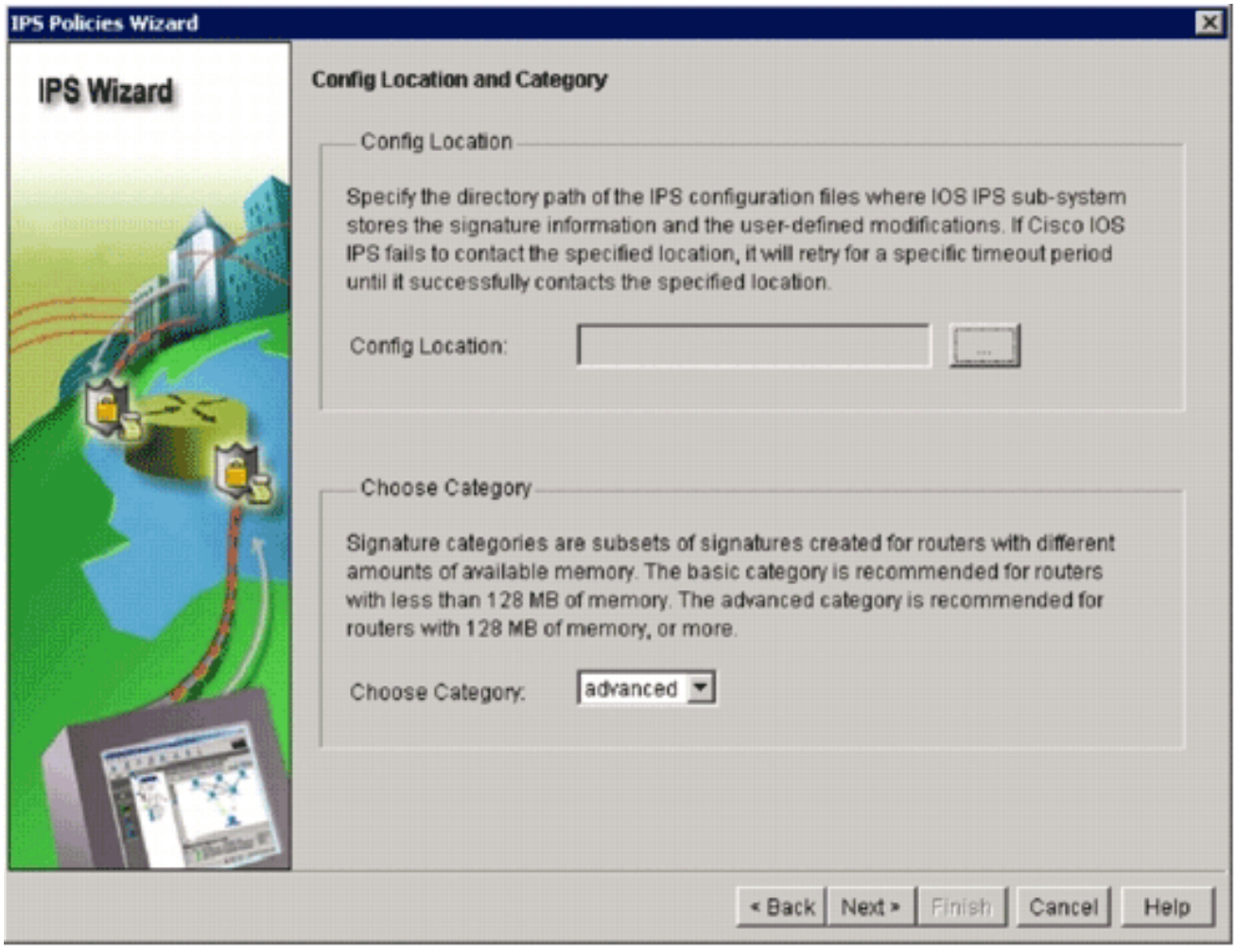
protocolo na lista suspensa Protocolo.**Observação:** este exemplo usa TFTP para baixar o pacote de assinatura para o roteador.

20. Digite o URL do arquivo de assinatura e clique em **OK**.
21. Na área Configurar chave pública da janela Arquivo de assinatura e chave pública, insira **realm-cisco.pub** no campo Nome e, em seguida, copie essa chave pública e cole-a no campo Chave.

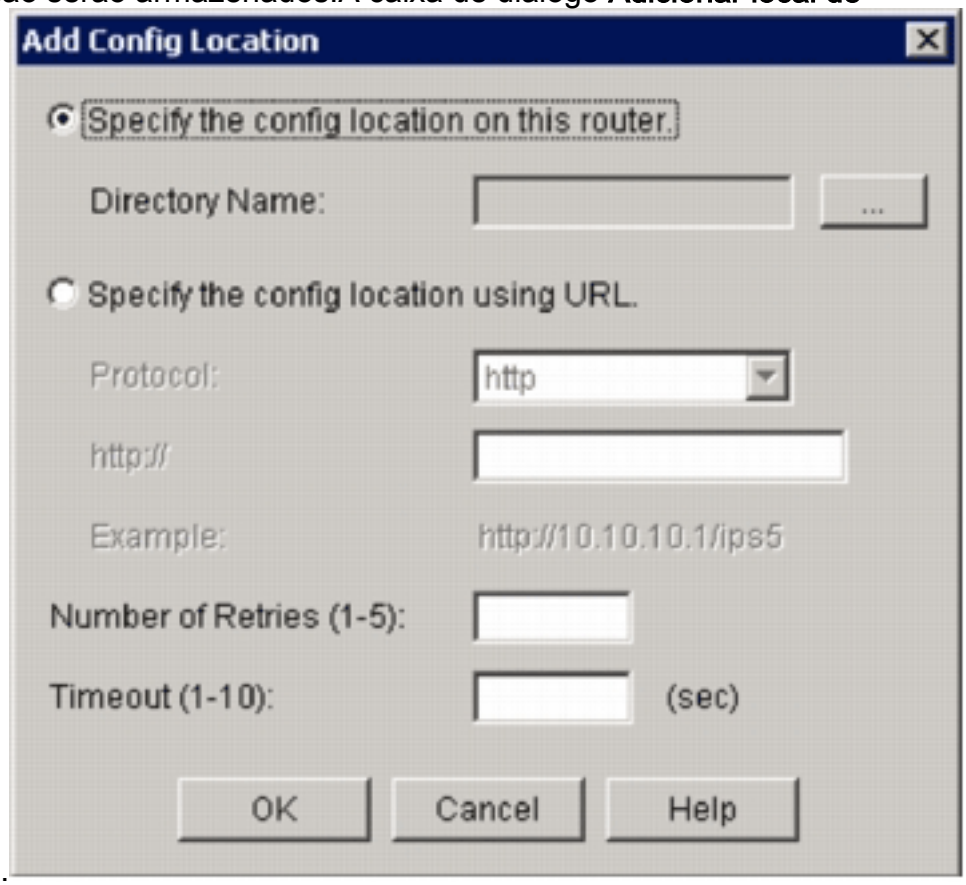
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

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
```

Observação: esta chave pública pode ser baixada do Cisco.com em: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (apenas clientes registrados) .

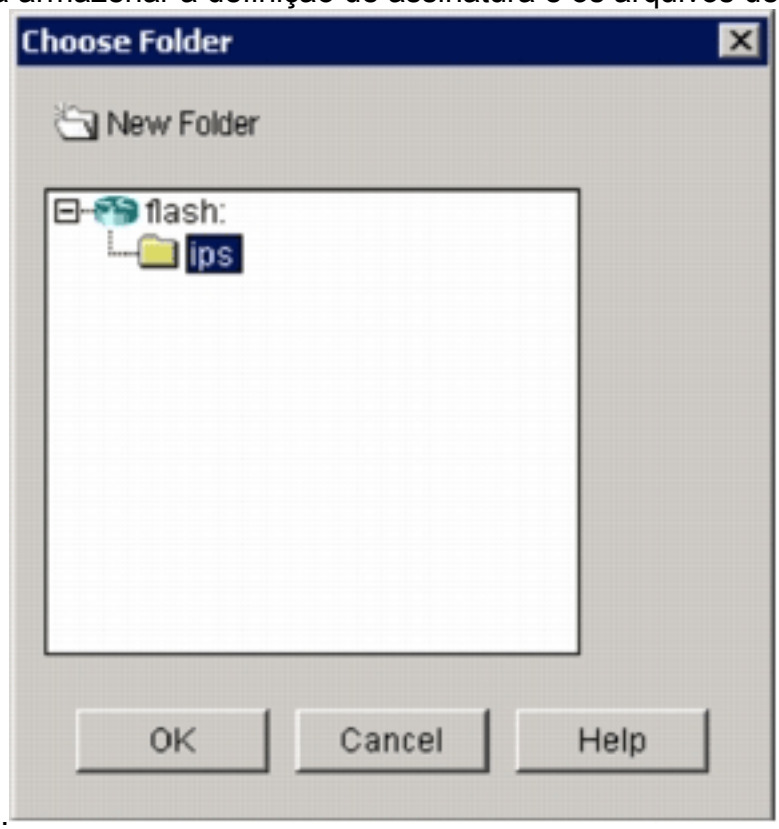
22. Clique em Avançar para continuar.



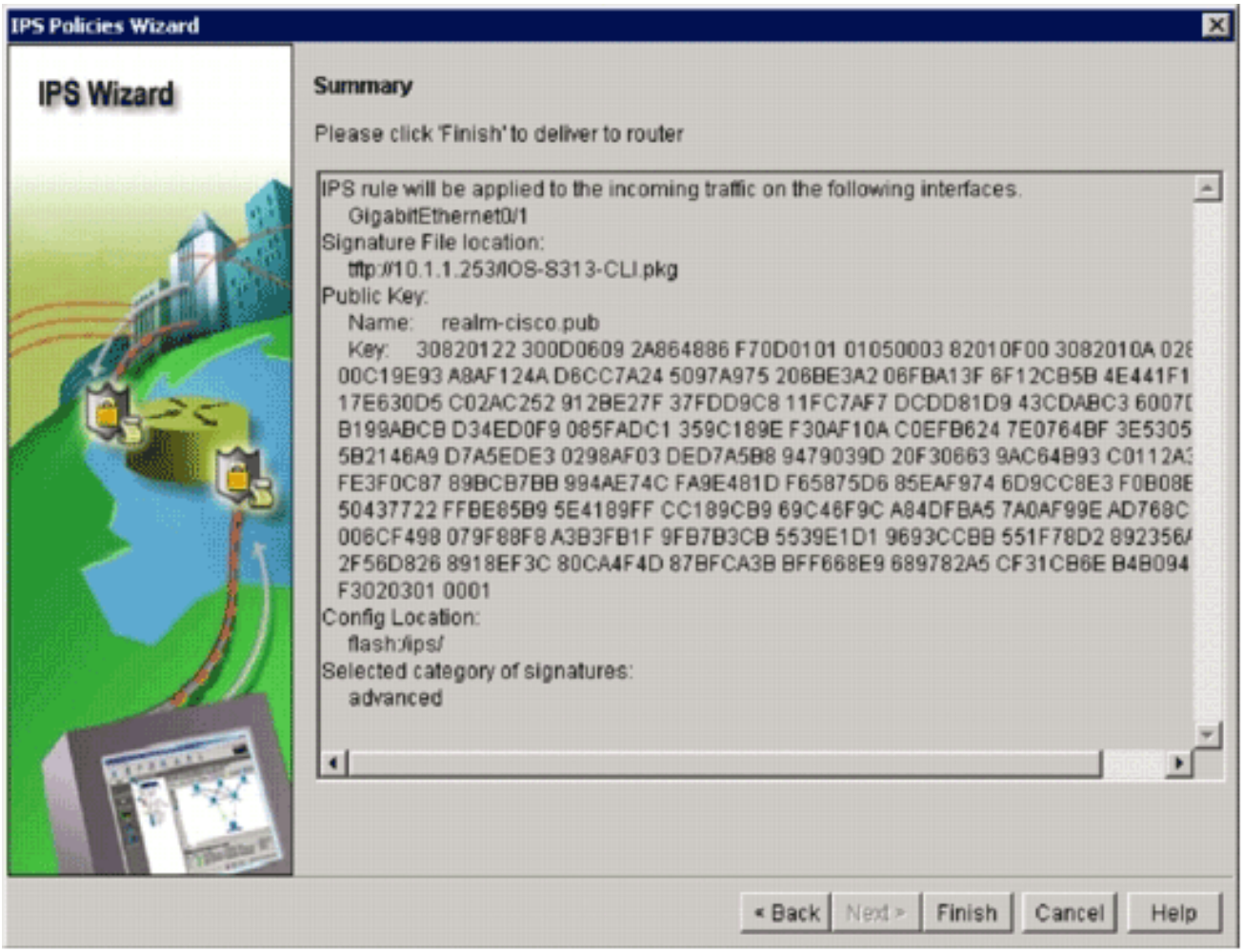
23. Na janela Config Location and Category (Local de configuração e Categoria), clique no botão **Config Location** (..) para especificar um local onde a definição de assinaturas e os arquivos de configuração serão armazenados.A caixa de diálogo **Adicionar local de configuração** é exibida.



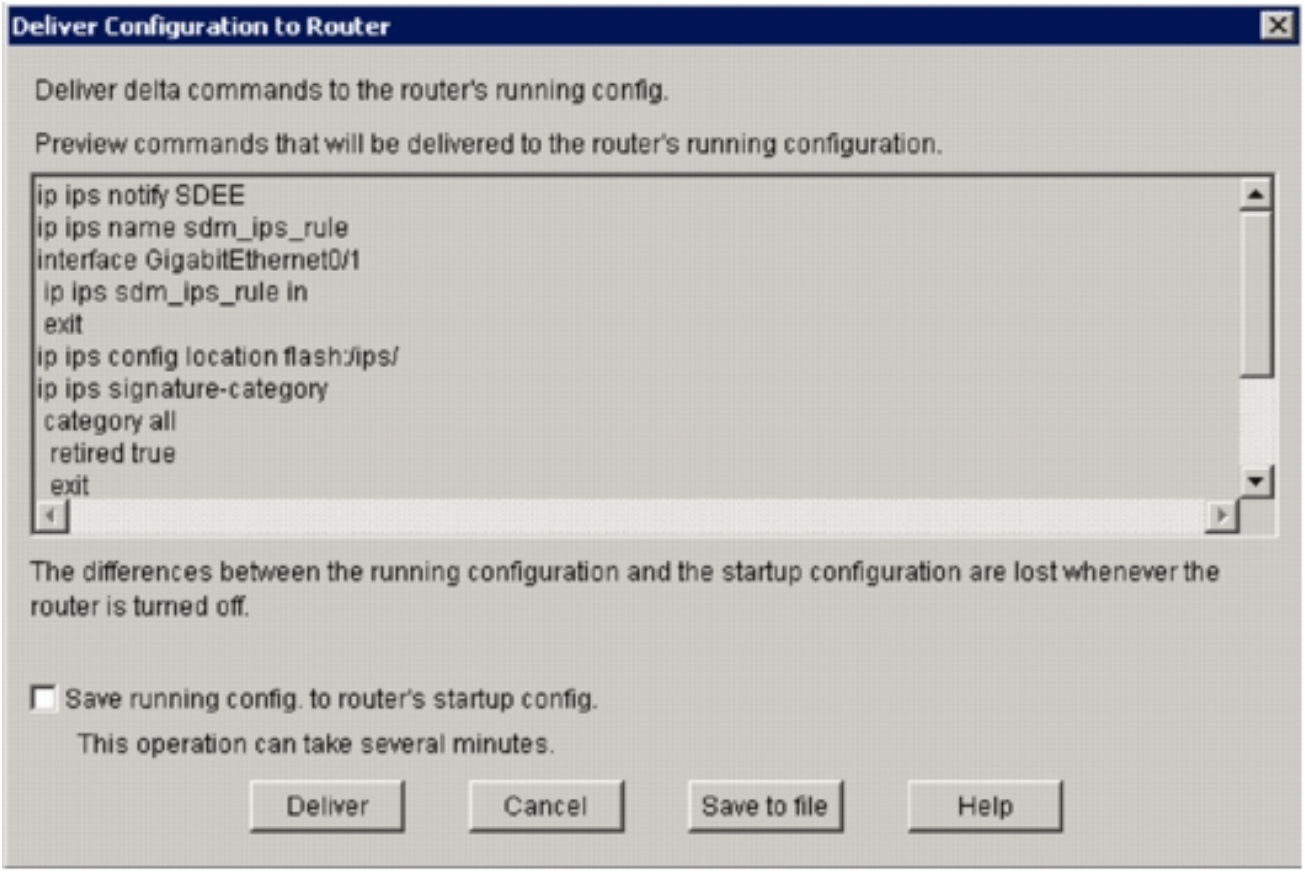
24. Na caixa de diálogo Add Config Location (Adicionar local de configuração), clique no botão de opção **Specify the config location on this router** e clique no botão **Diretory Name** (...) para localizar o arquivo de configuração.A caixa de diálogo Escolher pasta é exibida para permitir que você selecione um diretório existente ou crie um novo diretório na flash do roteador para armazenar a definição de assinatura e os arquivos de configuração.



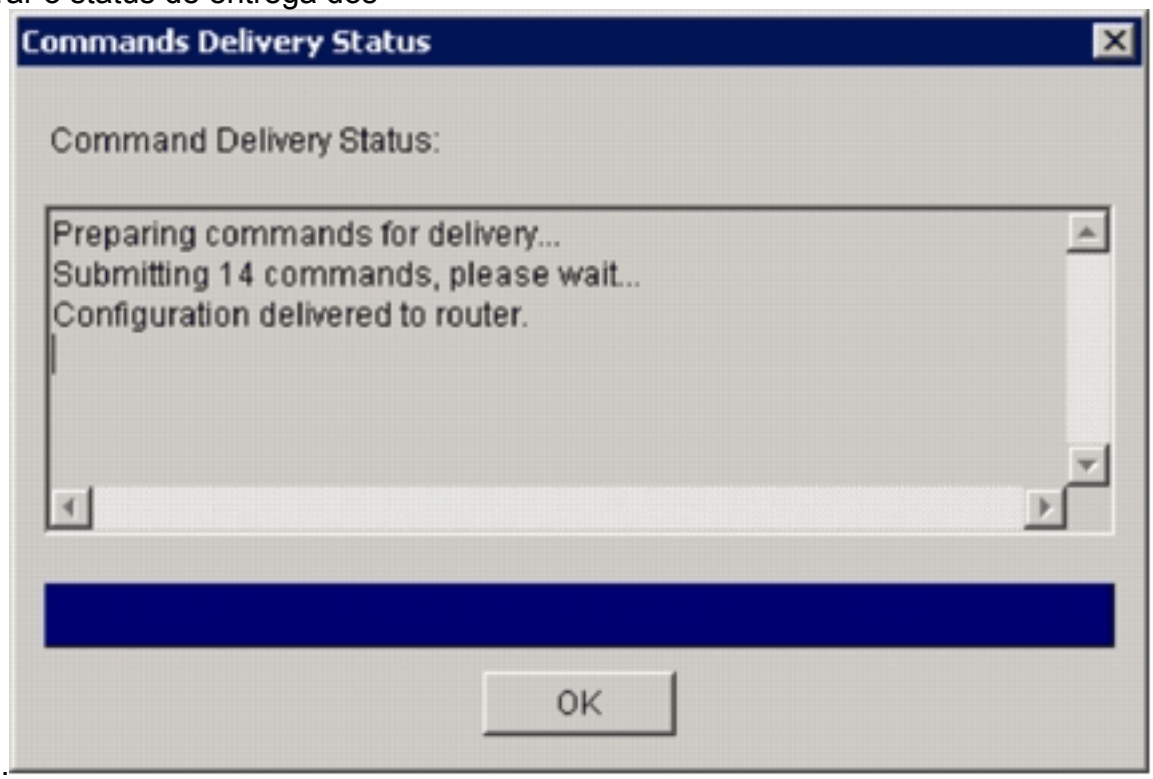
25. Clique em **Nova pasta** localizada na parte superior da caixa de diálogo se quiser criar um novo diretório.
26. Depois de selecionar o diretório, clique em **OK** para aplicar as alterações e, em seguida, clique em **OK** para fechar a caixa de diálogo Adicionar local de configuração.
27. Na caixa de diálogo Assistente de políticas de IPS, selecione a categoria de assinatura de acordo com a quantidade de memória instalada no roteador. Há duas categorias de assinatura que você pode escolher no SDM: Básico e Avançado.Se o roteador tiver DRAM de 128 MB instalada, a Cisco recomenda que você escolha a categoria Basic para evitar falhas na alocação de memória. Se o roteador tiver 256 MB ou mais de DRAM instalados, você poderá escolher qualquer categoria.
28. Depois de selecionar uma categoria a ser usada, clique em **Avançar** para continuar para a página de resumo.A página de resumo fornece uma breve descrição sobre as tarefas da configuração inicial do IOS
    IPS.



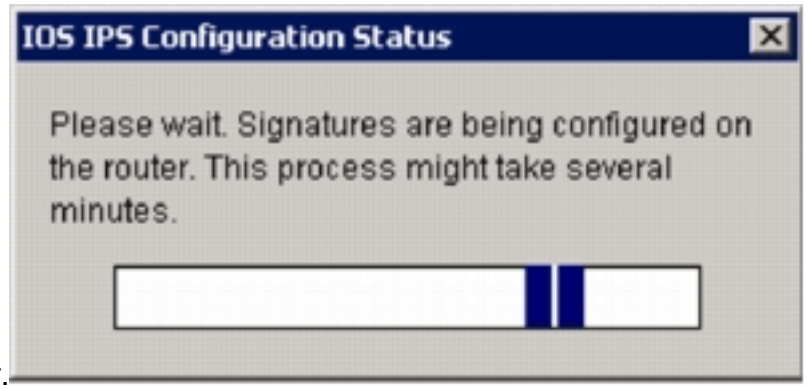
29. Clique em **Finish** na página de resumo para entregar as configurações e o pacote de assinatura ao roteador.Se a opção de comandos de visualização estiver ativada nas configurações de Preferências no SDM, o SDM exibirá a caixa de diálogo Deliver Configuration to Router que mostra um resumo dos comandos CLI que o SDM fornece ao roteador.



30. Clique em **Deliver** para continuar.A caixa de diálogo Commands Delivery Status é exibida para mostrar o status de entrega dos comandos.

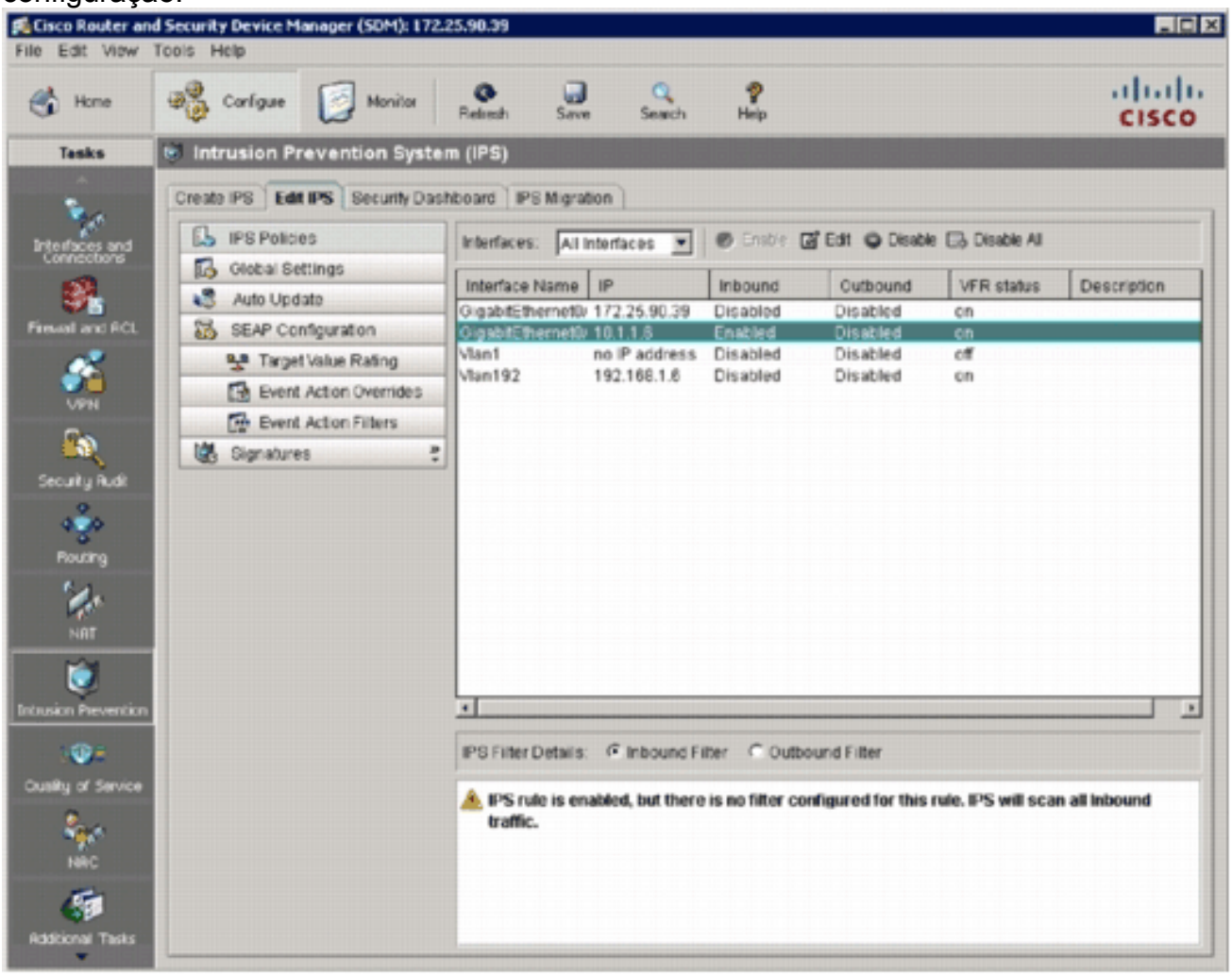


31. Quando os comandos forem entregues ao roteador, clique em **OK** para continuar.A caixa de diálogo Status da configuração do IOS IPS mostra que as assinaturas estão sendo

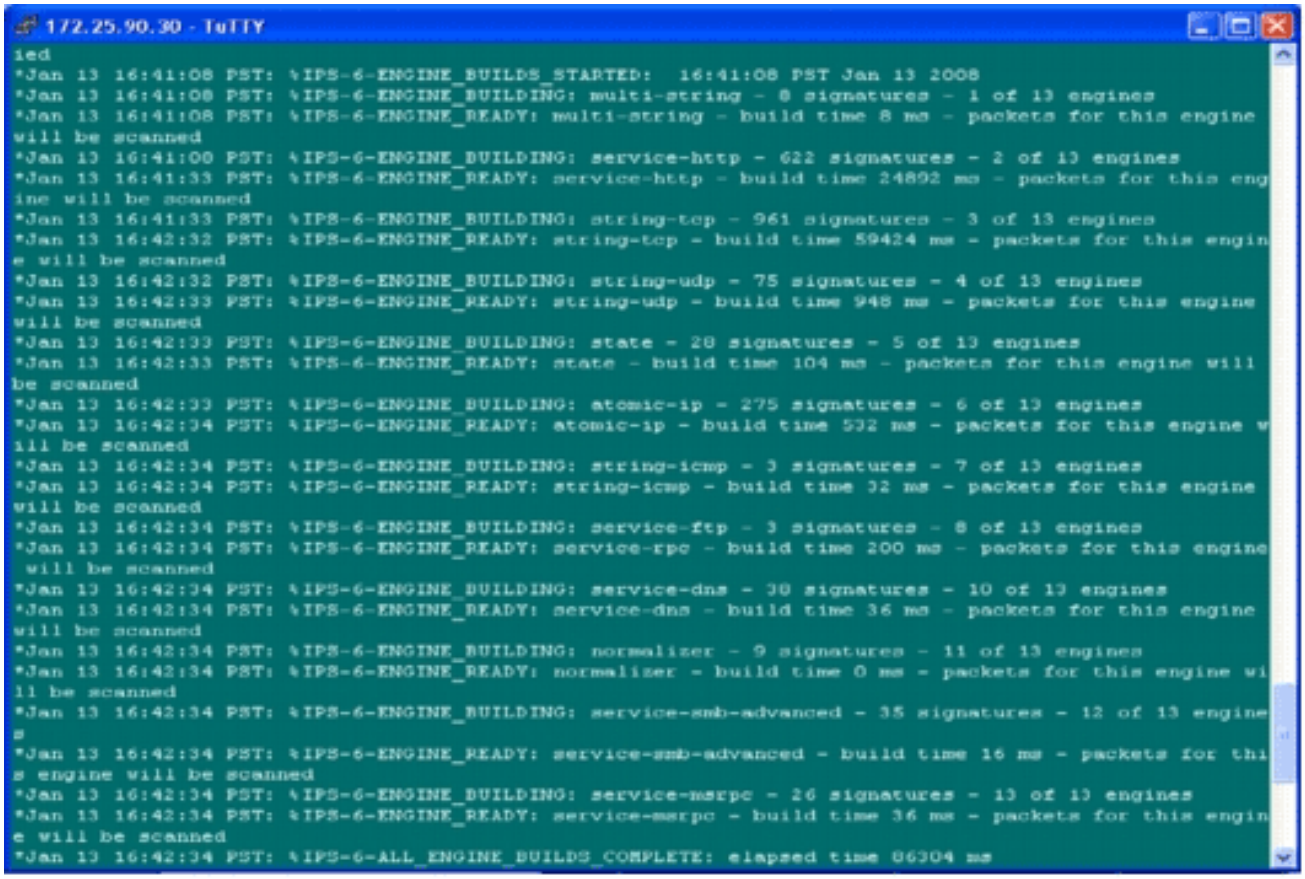


carregadas no roteador.

32. Quando as assinaturas são carregadas, o SDM exibe a guia **Editar IPS** com a configuração atual. Verifique qual interface e em que direção o IOS IPS está ativado para verificar a configuração.



O console do roteador mostra que as assinaturas foram carregadas.

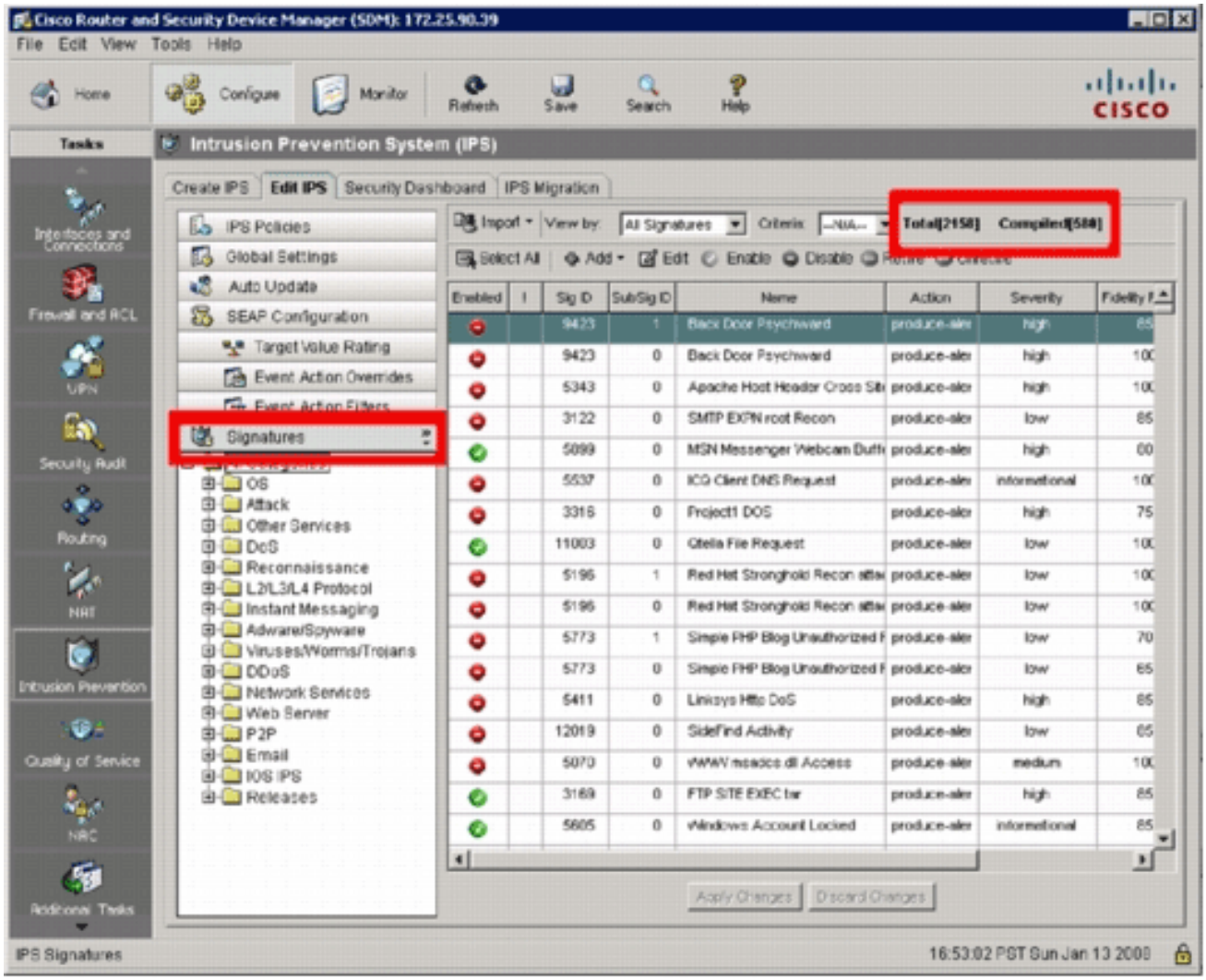


33. Use o comando **show ip ips subscription count** para verificar se as assinaturas foram carregadas corretamente.

```
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
```

O provisionamento inicial do IOS IPS usando o SDM 2.5 está concluído.

34. Verifique os números de assinatura com SDM como mostrado nesta imagem.



Informações Relacionadas

- Cisco IOS IPS em Cisco.com
- Pacote de assinatura do Cisco IOS IPS
- Arquivos de assinatura do Cisco IOS IPS para SDM
- Introdução ao Cisco IOS IPS com formato de assinatura 5.x
- Guia de configuração do Cisco IOS IPS
- Cisco IDS Event Viewer
- Suporte Técnico e Documentação - Cisco Systems