Configurar o roteador e o SDM e o Cisco IOS CLI no Cisco IOS IPS

Contents

Introduction

No Cisco Router and Security Device Manager (SDM) 2.2, a configuração do IPS do Cisco IOS® é integrada no aplicativo SDM. Você não precisa mais iniciar uma janela separada para configurar o Cisco IOS IPS.

No Cisco SDM 2.2, um novo assistente de configuração de IPS o orienta pelas etapas necessárias para ativar o Cisco IOS IPS no roteador. Além disso, você ainda pode usar as opções de configuração avançada para habilitar, desabilitar e ajustar o Cisco IOS IPS com o Cisco SDM 2.2.

A Cisco recomenda que você execute o Cisco IOS IPS com os arquivos de definição de assinatura (SDFs) pré-ajustados: ataque-drop.sdf, 128 MB.sdf e 256 MB.sdf. Esses arquivos são criados para roteadores com diferentes quantidades de memória. Os arquivos são agrupados com o Cisco SDM, que recomenda SDFs quando você habilita o Cisco IOS IPS pela primeira vez em um roteador. Esses arquivos também podem ser baixados em http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (somente clientes registrados) .

O processo para habilitar os SDFs padrão é detalhado em Habilitar o Cisco IOS IPS com um SDF padrão de fábrica. Quando os SDFs padrão não forem suficientes ou você quiser adicionar novas assinaturas, poderá usar o procedimento descrito em Acrescentar Assinaturas Adicionais depois de Habilitar o SDF Padrão.

Prerequisites

Requirements

O Java Runtime Environment (JRE) Versão 1.4.2 ou posterior é necessário para usar o Cisco SDM 2.2. Um arquivo de assinatura (baseado na DRAM) recomendado e ajustado pela Cisco é fornecido com o Cisco SDM (carregado na memória flash do roteador com o Cisco SDM).

Componentes Utilizados

As informações neste documento são baseadas no Cisco Router and Security Device Manager (SDM) 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.

Conventions

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

Configurar

Habilitar o Cisco IOS IPS com um SDF padrão de fábrica

Procedimento CLI

Conclua este procedimento para usar a CLI para configurar um Cisco 1800 Series Router com Cisco IOS IPS para carregar 128MB.sdf na memória flash do roteador.

1. Configure o roteador para ativar a notificação de eventos do Security Device Event Exchange (SDEE).
   ```
   yourname#conf t
   ```
2. Insira os comandos de configuração (um por linha) e pressione Cntl+Z para terminar.
   ```
   yourname(config)#ip ips notify sdee
   ```
3. Crie um nome de regra de IPS que seja usado para associar às interfaces.
   ```
   yourname(config)#ip ips name myips
   ```
4. Configurar um comando de localização de IPS para especificar de qual arquivo o sistema de IPS do Cisco IOS lerá as assinaturas.Este exemplo usa o arquivo na flash: 128 MB.sdf A parte da URL do local desse comando pode ser qualquer URL válida que use flash, disco ou protocolos via FTP, HTTP, HTTPS, RTP, SCP e TFTP para apontar para os arquivos.
   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

   Observação: você deve habilitar o comando **terminal monitor** se configurar o roteador através de uma sessão Telnet ou se não verá as mensagens SDEE quando o mecanismo de assinatura estiver sendo criado.
5. Ative o IPS na interface onde você deseja habilitar o Cisco IOS IPS para verificar o tráfego. Nesse caso, ativamos em ambas as direções na interface 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 of15 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 f 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
```

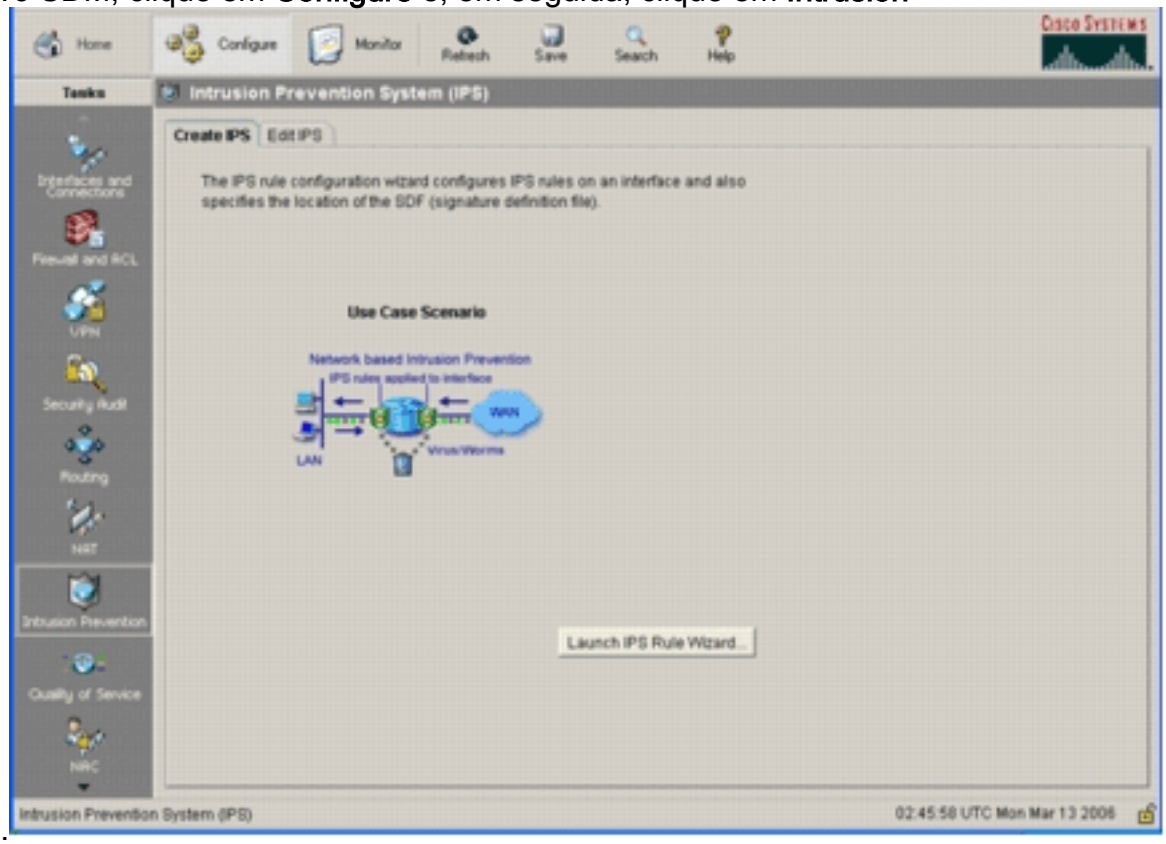
Na primeira vez que uma regra de IPS é aplicada a uma interface, o Cisco IOS IPS inicia assinaturas criadas do arquivo especificado pelo comando SDF locations. As mensagens SDEE são registradas no console e enviadas ao Servidor syslog, se configurado. As mensagens SDEE com <*number*> de <*number*> mecanismos indicam o processo de criação do mecanismo de assinatura. Finalmente, quando os dois números são os mesmos, todos os motores são construídos.**Observação:** a remontagem virtual de IP é um recurso de interface que (quando ativada) reagrupa automaticamente os pacotes fragmentados que entram no roteador através dessa interface. A Cisco recomenda que você habilite o ip virtual-assembly em todas as interfaces onde o tráfego entra no roteador. No exemplo acima, além de ativar "ip virtual-assembly" na interface fastEthernet 0, configuramos na interface interna VLAN 1 também.

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

Procedimento do SDM 2.2

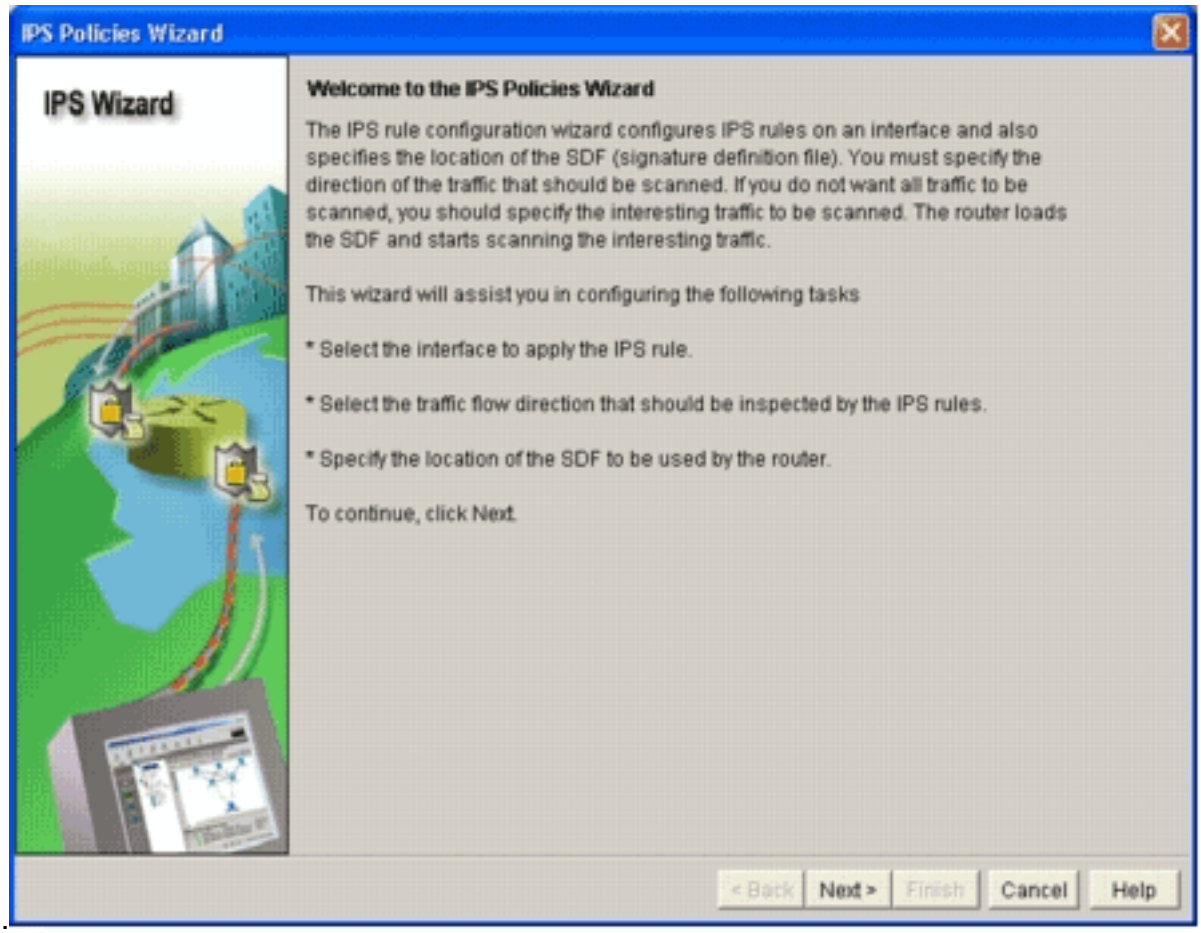
Conclua este procedimento para usar o Cisco SDM 2.2 para configurar um Cisco 1800 Series Router com Cisco IOS IPS.

1. No aplicativo SDM, clique em **Configure** e, em seguida, clique em **Intrusion Prevention**.

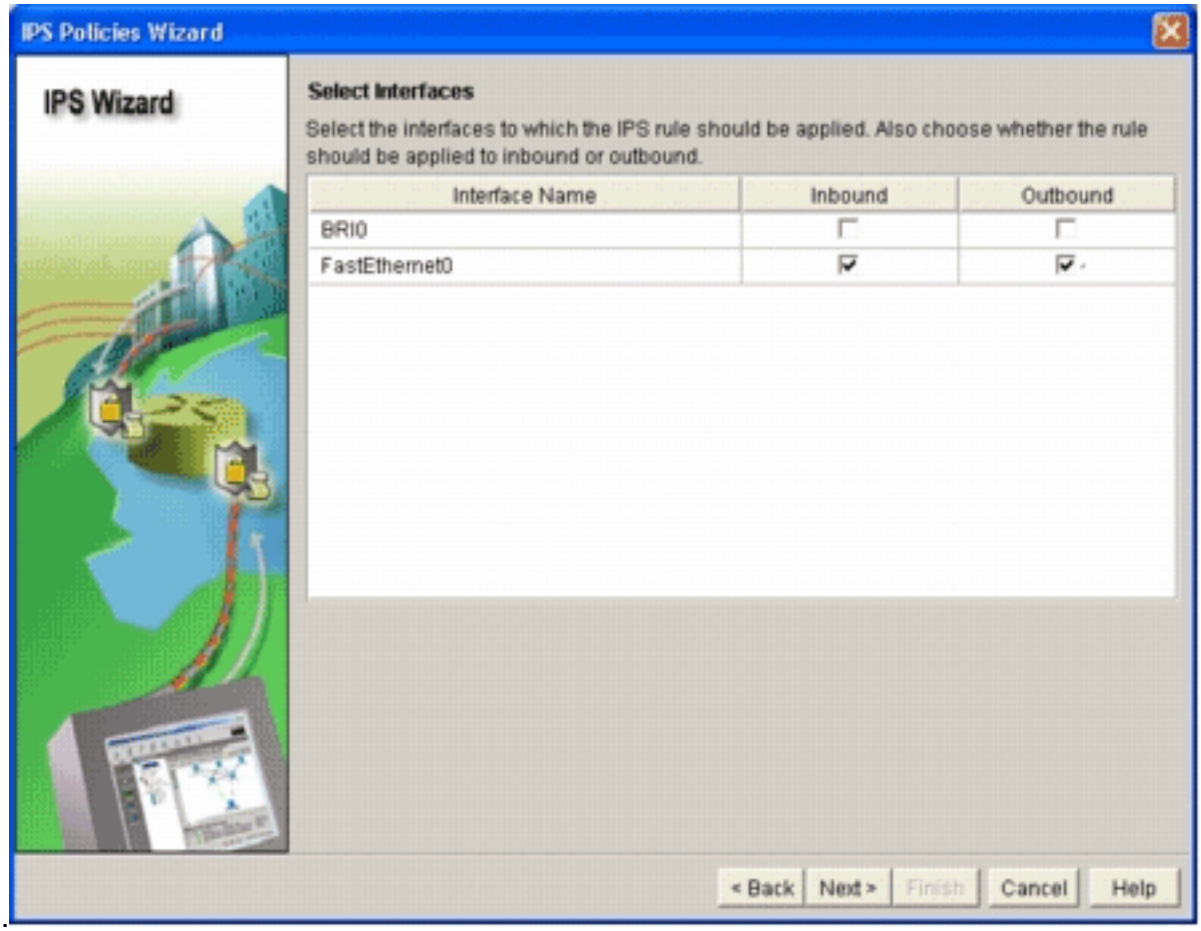


2. Clique na guia **Create IPS** e clique em **Launch IPS Rule Wizard**.O Cisco SDM requer notificação de evento de IPS via SDEE para configurar o recurso IPS do Cisco IOS. Por padrão, a notificação SDEE não está ativada. O Cisco SDM solicita que você habilite a notificação de eventos de IPS via SDEE, como mostrado nesta

imagem: 

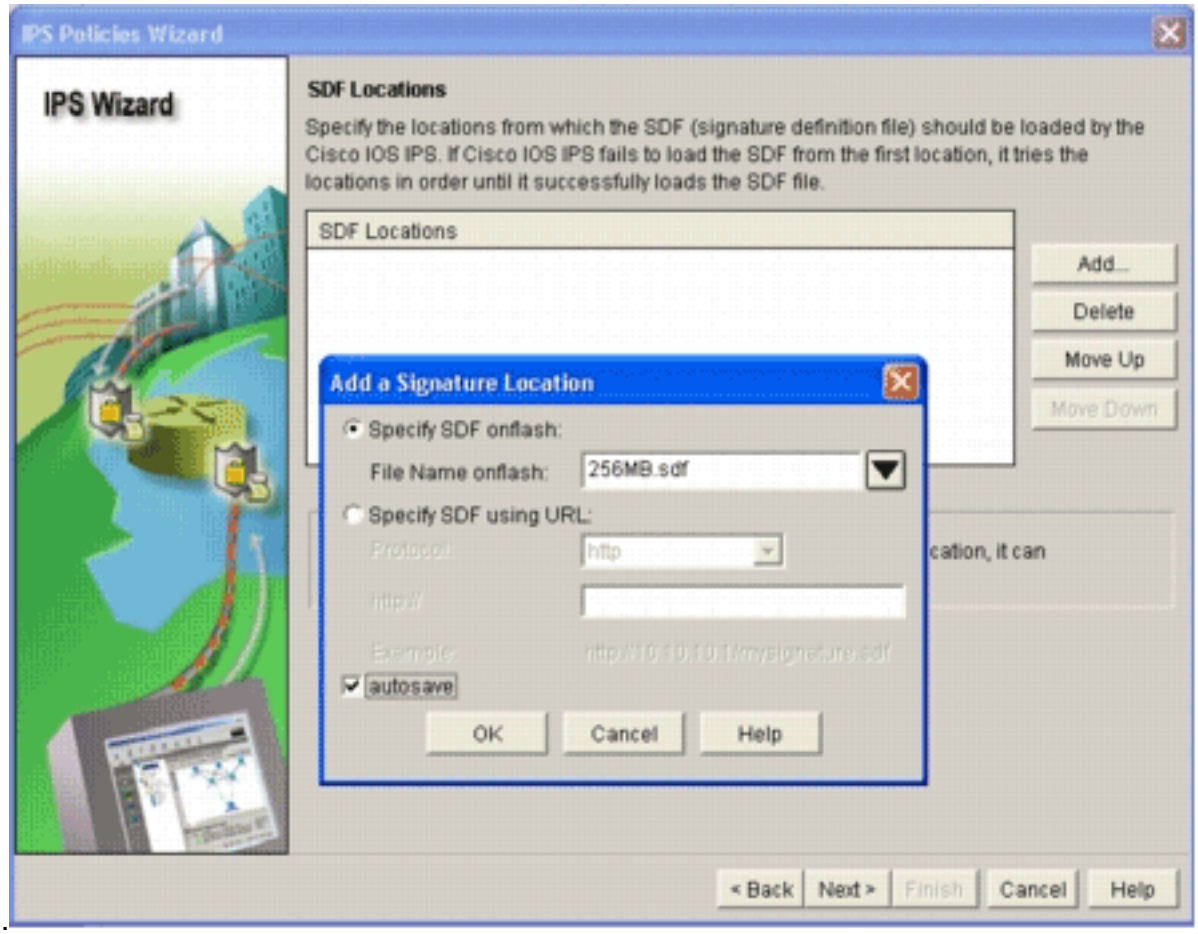
3. Click **OK**.A janela Bem-vindo ao Assistente de Políticas de IPS da caixa de diálogo Assistente de Políticas de IPS é exibida. 

4. Clique em Next.A janela Selecionar interfaces é



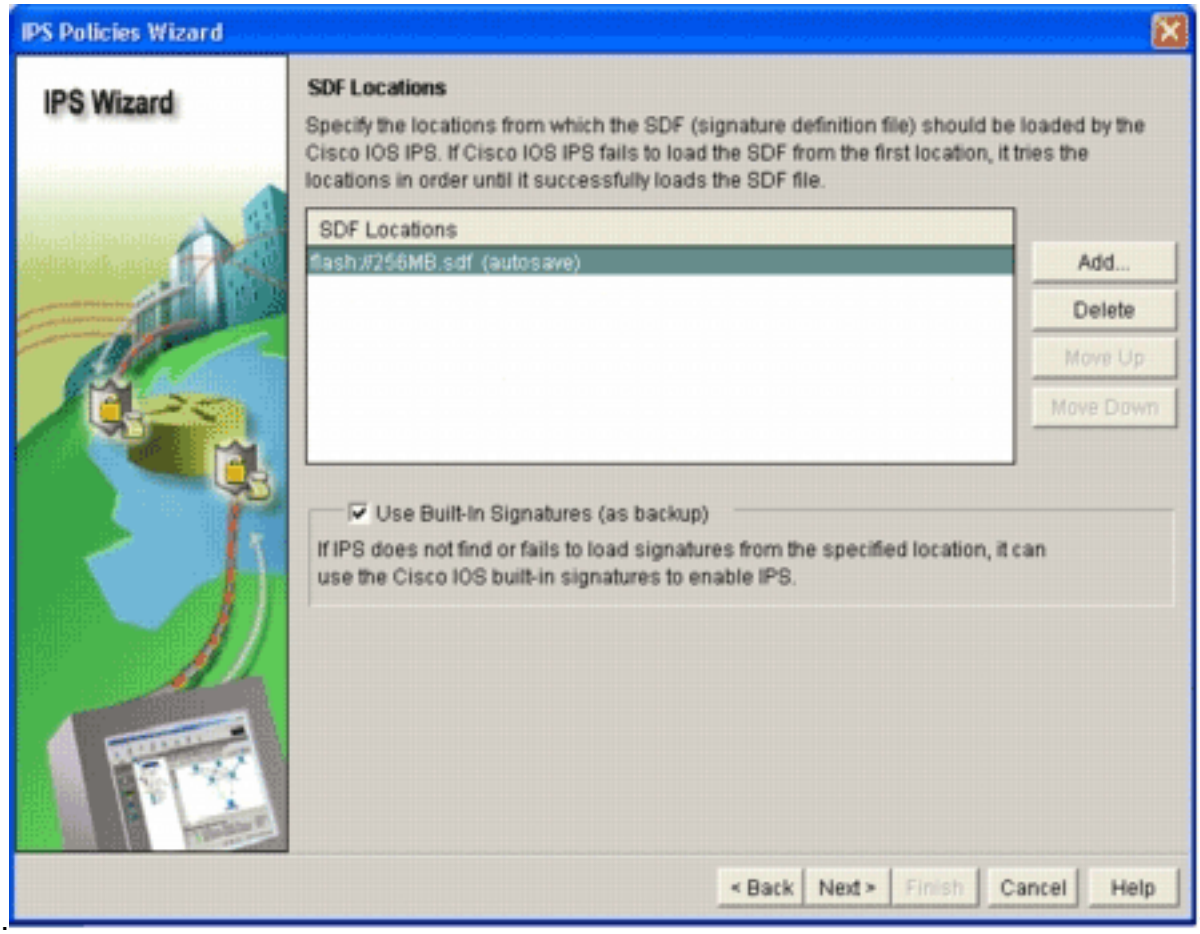
exibida.

5. Escolha as interfaces para as quais deseja habilitar o IPS e clique na caixa de seleção **Entrada** ou **Saída** para indicar a direção dessa interface.**Observação:** a Cisco recomenda que você habilite as direções de entrada e saída ao habilitar o IPS em uma interface.
6. Clique em Next.A janela SDF Locations (Locais SDF) é exibida.
7. Clique em **Adicionar** para configurar um local SDF.A caixa de diálogo Adicionar um local de assinatura é



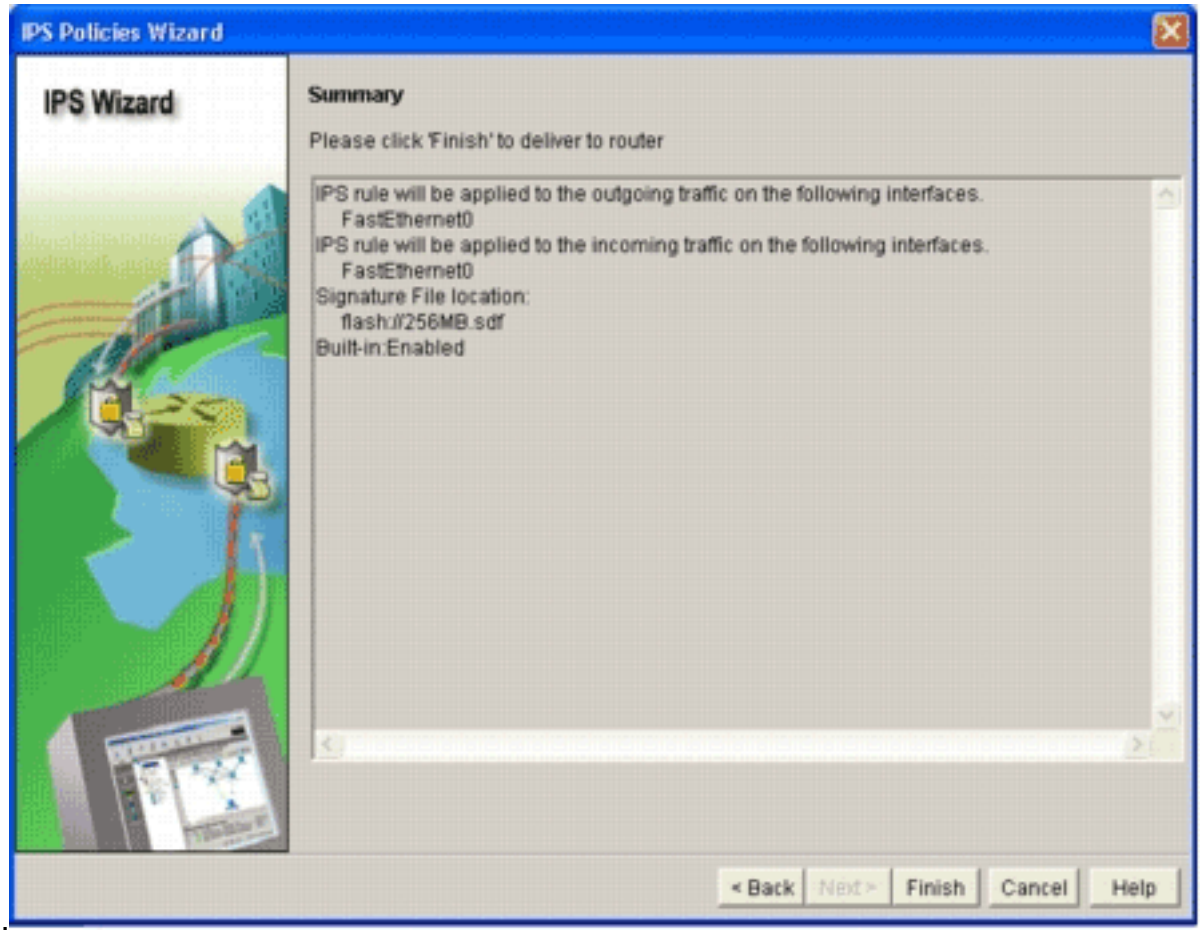
exibida.

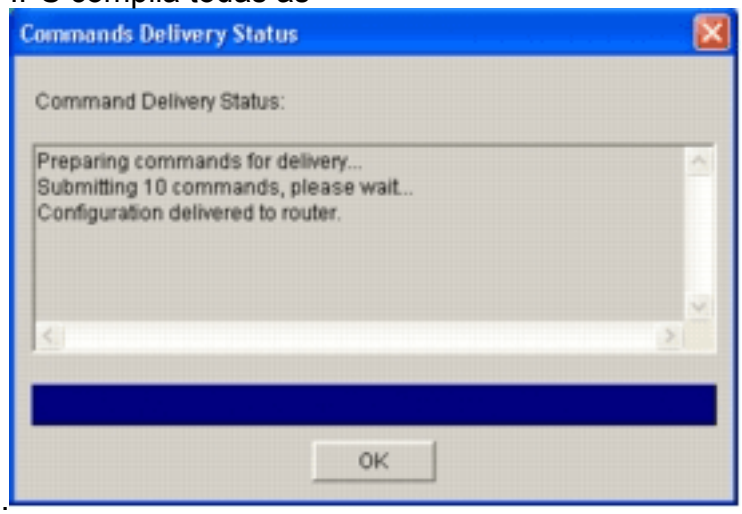
8. Clique no botão de opção **Especificar SDF na flash** e escolha 256MB.sdf na lista suspensa **Nome do arquivo na flash**.
9. Clique na caixa de seleção **salvar automaticamente** e clique em **OK**.**Nota:** a opção de gravação automática salva automaticamente o arquivo de assinatura quando há uma alteração de assinatura.A janela SDF Locations (Locais SDF) exibe o novo local



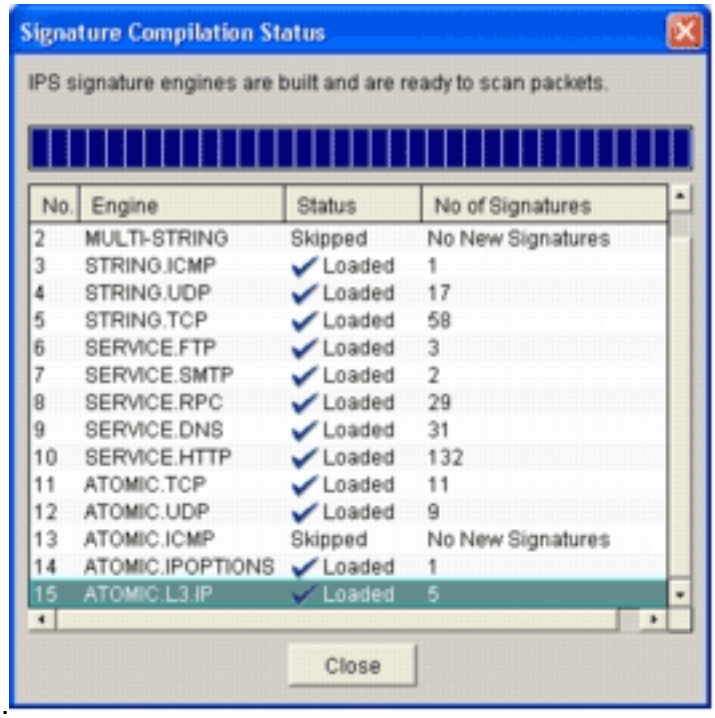
SDF. **Observação:** você pode adicionar outros locais de assinatura para designar um backup.

10. Clique na caixa de seleção **Usar assinaturas incorporadas (como backup)**.**Observação:** a Cisco recomenda que você não use a opção de assinatura integrada, a menos que tenha especificado um ou mais locais.
11. Clique em **Next** para continuar.A janela Resumo é

exibida. 

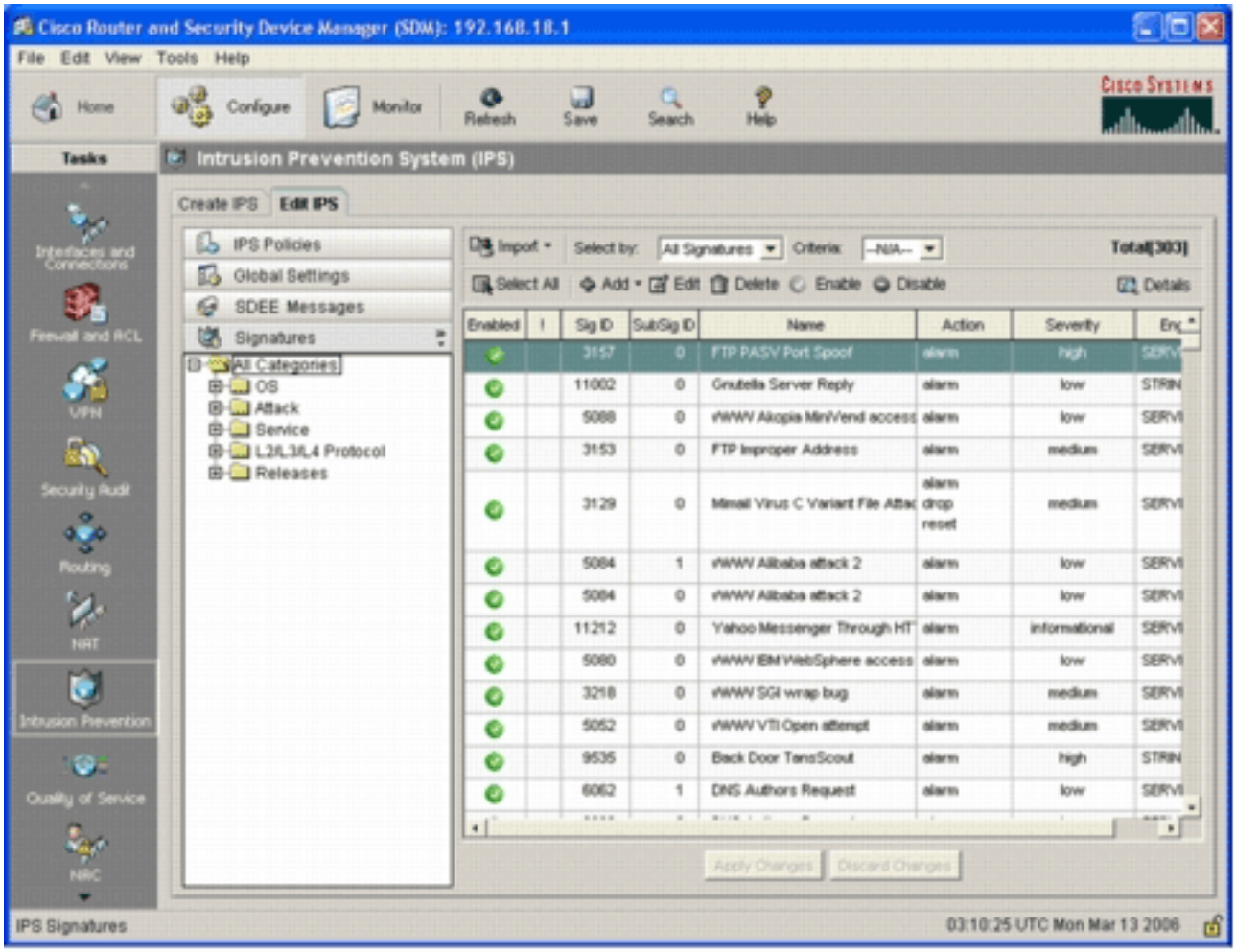
12. Clique em Finish.A caixa de diálogo Commands Delivery Status exibe o status enquanto o mecanismo IPS compila todas as assinaturas. 

13. Quando o processo estiver concluído, clique em **OK**.A caixa de diálogo Status da compilação de assinatura exibe as informações da compilação de



assinatura. Estas informações mostram quais os motores que foram compilados e o número de assinaturas nesse motor. Para mecanismos que exibem *Ignorados* na coluna de status, não há assinatura carregada para esse mecanismo.

14. Clique em **Fechar** para fechar a caixa de diálogo Status da compilação de assinatura.
15. Para verificar quais assinaturas estão carregadas no roteador no momento, clique em **Configurar** e, em seguida, clique em **Prevenção de intrusão**.
16. Clique na guia **Edit IPS** e, em seguida, clique em **Signatures**.A lista de assinaturas IPS é exibida na janela
    Assinaturas.



Acrescentar assinaturas adicionais após ativar o SDF padrão

Procedimento CLI

Não há nenhum comando CLI disponível para criar assinaturas ou ler informações de assinatura do arquivo IOS-Sxxx.zip distribuído. A Cisco recomenda que você use o SDM ou o Management Center for IPS Sensors para gerenciar as assinaturas em sistemas Cisco IOS IPS.

Para clientes que já têm um arquivo de assinatura pronto e desejam mesclar esse arquivo com o SDF executado em um sistema Cisco IOS IPS, você pode usar este comando:

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

O arquivo de assinatura definido pelo comando de local de assinatura é onde o roteador carrega arquivos de assinatura quando é recarregado ou quando o IOS IPS do roteador é reconfigurado. Para que o processo de mesclagem seja bem-sucedido, o arquivo definido pelo comando de localização do arquivo de assinatura também deve ser atualizado.

1. Use o comando **show** para verificar os locais de assinatura configurados no momento.A saída mostra os locais de assinatura configurados. Este comando mostra de onde as assinaturas em execução atuais são carregadas.
   ```
   yourname#show ip ips signatures
   Builtin signatures are configured
   ```
   As assinaturas foram carregadas pela última vez na flash:128MB.sdfVersão do Cisco SDF

S128.0Versão V0.0 do SDF de tendência

2. Use o comando **copy <*url*> ips-sdf**, juntamente com as informações da etapa anterior, para mesclar arquivos de assinatura.

```
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#
```

Depois de emitir o comando **copy**, o roteador carrega o arquivo de assinatura na memória e, em seguida, cria os mecanismos de assinatura. Na saída da mensagem SDEE do console, o status do edifício para cada mecanismo de assinatura é exibido.%IPS-6-ENGINE_BUILD_SKIPPED indica que não há novas assinaturas para este mecanismo.%IPS-6-ENGINE_READY indica que há novas assinaturas e o mecanismo está pronto. Como anteriormente, a mensagem "15 de 15 motores" indica que todos os motores foram construídos.IPS-7-UNSUPPORTED_PARAM indica que um determinado parâmetro não é suportado pelo Cisco IOS IPS. Por exemplo, CapturePacket e ResetAfterIdle.**Observação:** essas mensagens são somente para informação e não terão nenhum efeito no desempenho ou no recurso de assinatura do Cisco IOS IPS. Essas mensagens de registro podem ser desativadas definindo o nível de registro mais alto que a depuração (nível 7).

3. Atualize o SDF definido pelo comando de local de assinatura, de modo que, quando o roteador for recarregado, ele terá a assinatura mesclada definida com assinaturas atualizadas. Este exemplo mostra a diferença de tamanho do arquivo após a assinatura mesclada ser salva no arquivo flash 128MB.sdf.

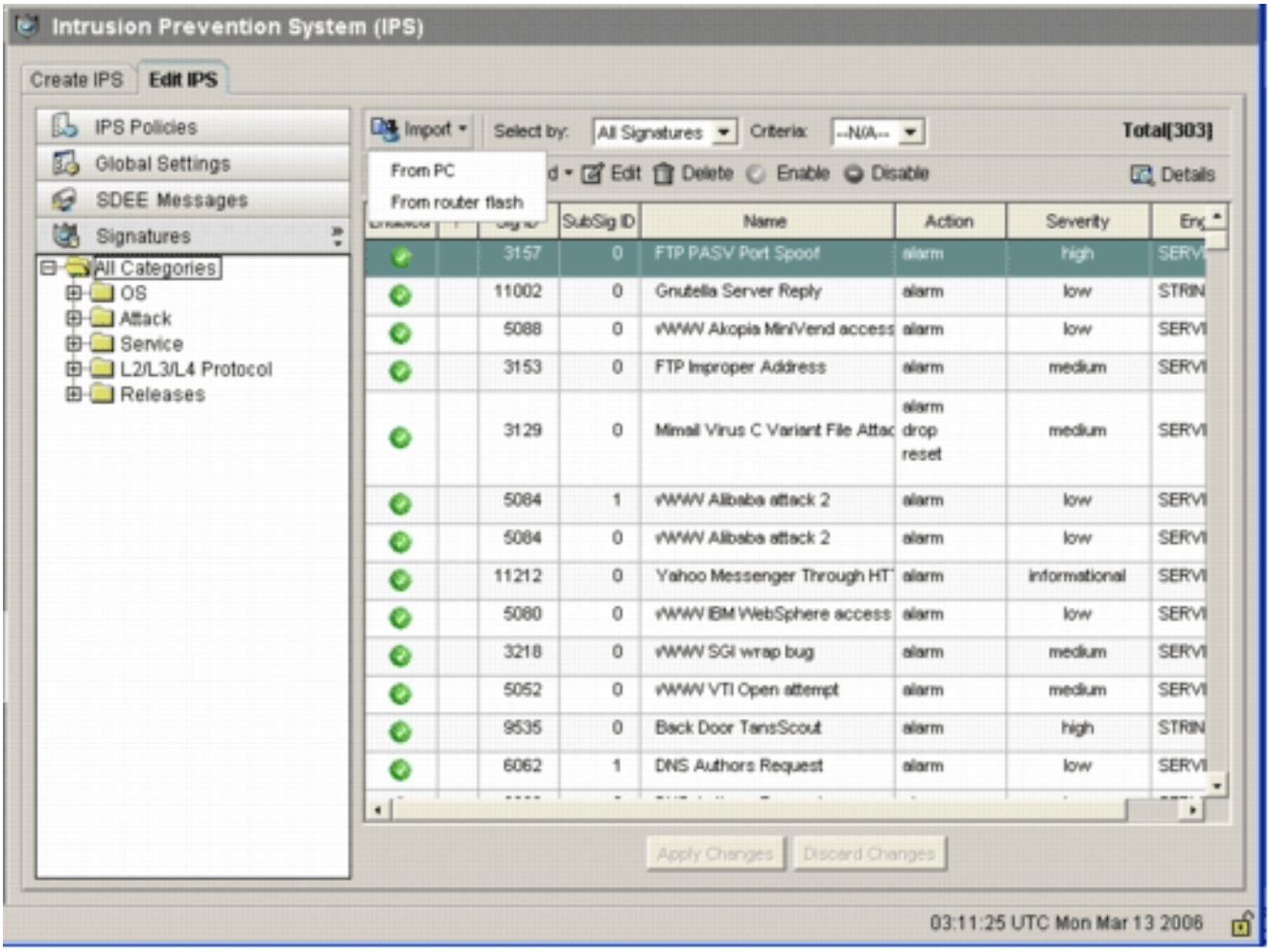
```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

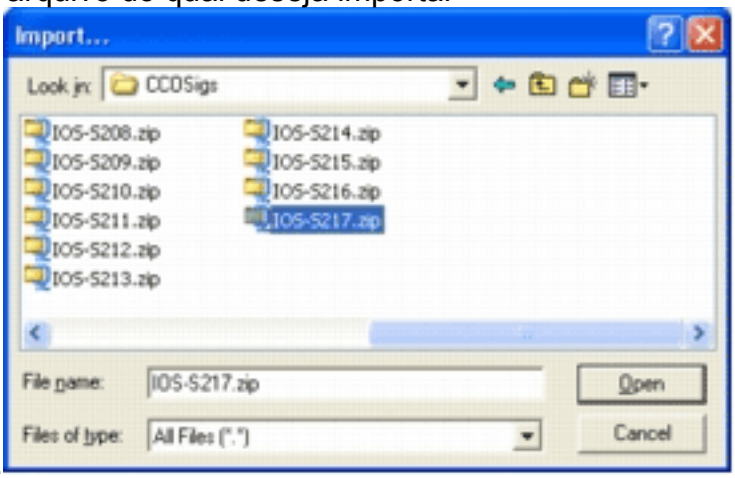
Aviso: o novo 128MB.sdf agora contém assinaturas mescladas pelo cliente. O conteúdo é diferente do arquivo padrão Cisco 128MB.sdf. A Cisco recomenda que você altere esse arquivo para um nome diferente para evitar confusão. Se o nome for alterado, o comando de localização da assinatura também precisará ser alterado.

Procedimento do SDM 2.2

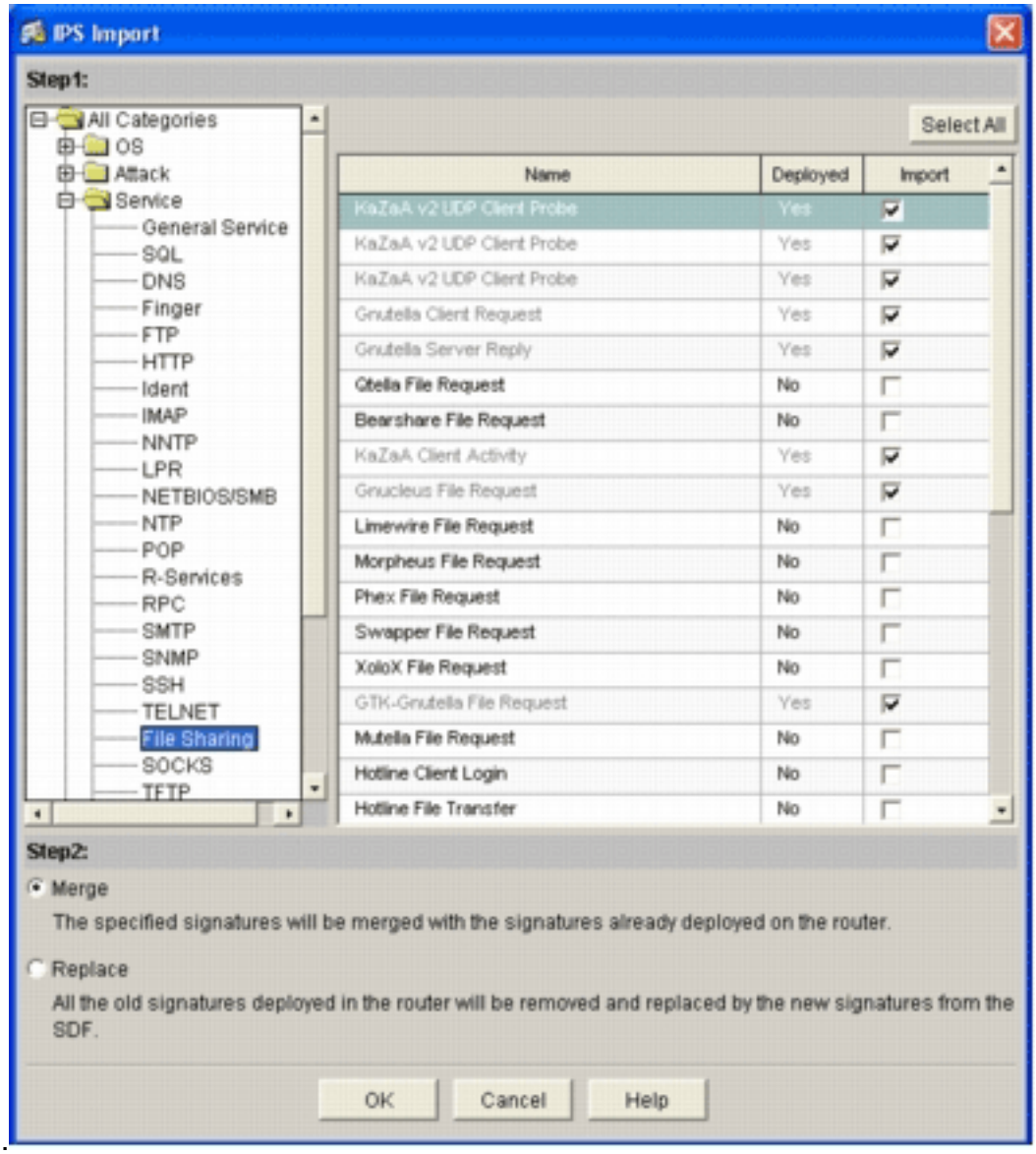
Depois que o Cisco IOS IPS tiver sido ativado, novas assinaturas podem ser adicionadas ao roteador que executa um conjunto de assinaturas com a função de importação do Cisco SDM. Conclua estes passos para importar novas assinaturas:

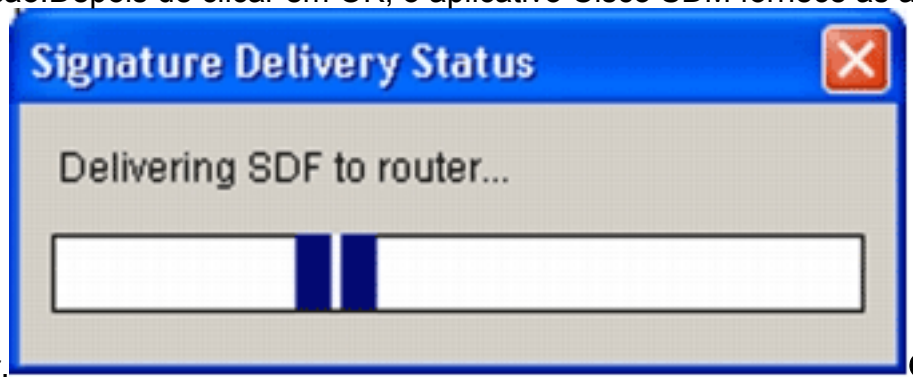
1. Escolha os SDFs padrão ou o arquivo de atualização IOS-Sxxx.zip para importar assinaturas adicionais.
2. Clique em **Configurar** e, em seguida, clique em **Prevenção de intrusão**.
3. Clique na guia **Edit IPS** e clique em **Import**.



4. Escolha **De PC** na lista suspensa Importar.
5. Selecione o arquivo do qual deseja importar assinaturas. 

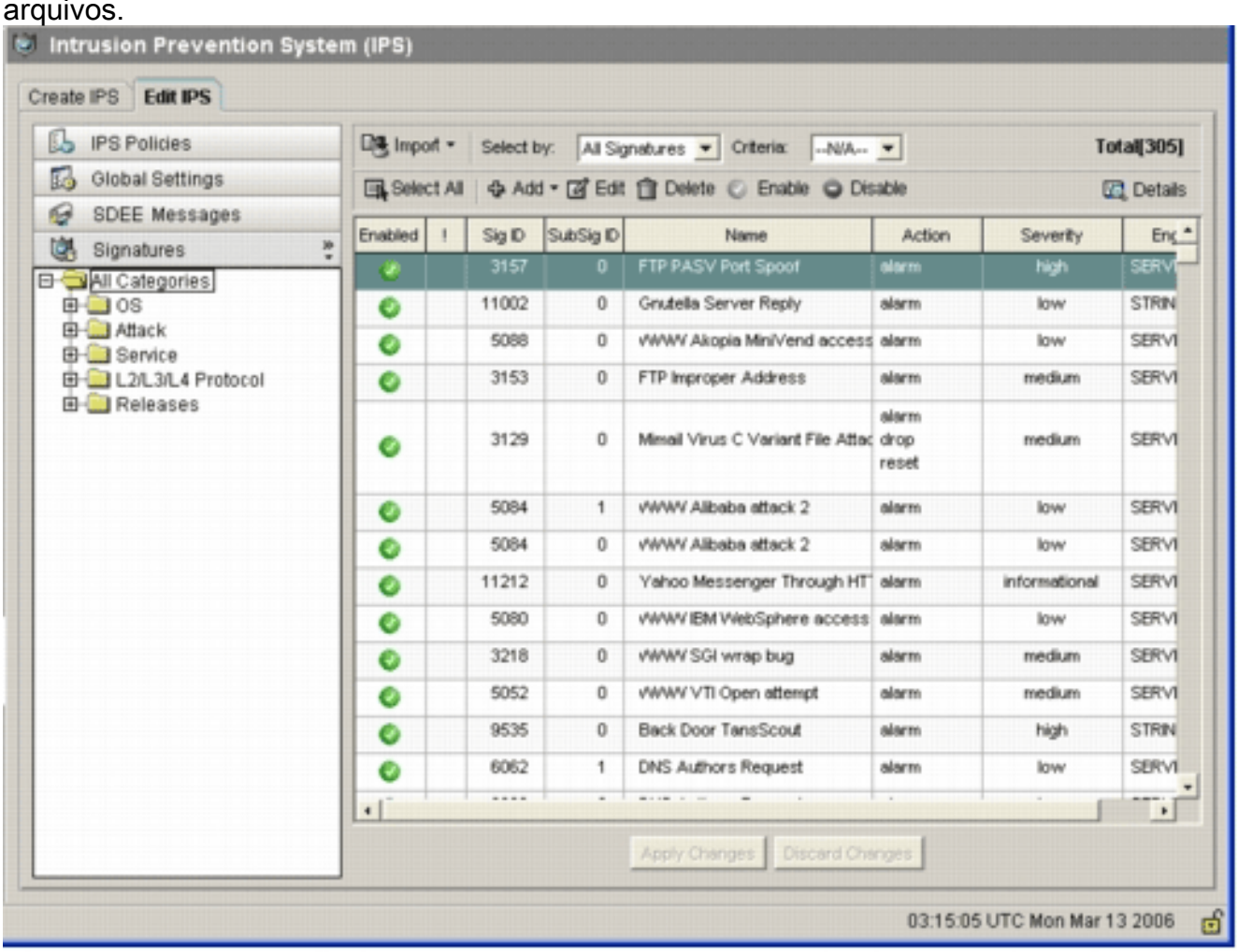
Este exemplo usa a atualização mais recente baixada do Cisco.com e salva no disco rígido local do PC.
6. Clique em **Abrir**.**Aviso:** devido à restrição de memória, apenas um número limitado de novas assinaturas pode ser adicionado no topo das assinaturas que já foram implantadas. Se muitas assinaturas forem selecionadas, o roteador talvez não consiga carregar todas as novas assinaturas devido à falta de memória.Quando o carregamento do arquivo de assinatura for concluído, a caixa de diálogo Importação de IPS será

exibida. 

7. Navegue pela exibição da árvore esquerda e clique na caixa de seleção **Importar** ao lado das assinaturas que deseja importar.
8. Clique no botão de opção **Mesclar** e clique em **OK**.**Observação:** a opção Substituir substitui a assinatura atual definida no roteador pelas assinaturas selecionadas para importação.Depois de clicar em OK, o aplicativo Cisco SDM fornece as assinaturas ao roteador. 

Observação: a utilização elevada da CPU ocorre durante a compilação e o carregamento de assinaturas. Depois que o Cisco IOS IPS é ativado na interface, o arquivo de assinatura começa a ser carregado. O roteador leva aproximadamente cinco minutos para carregar a SDF. Você pode tentar usar o comando **show process cpu** para visualizar a utilização da CPU na CLI do software Cisco IOS. No entanto, não tente usar comandos adicionais ou carregar outros SDFs enquanto o roteador estiver carregando o SDF. Isso pode fazer com que o processo de compilação de assinatura demore mais para ser concluído (já que a utilização da CPU é

de aproximadamente 100% no momento do carregamento da SDF). Talvez seja necessário navegar pela lista de assinaturas e ativar as assinaturas se elas não estiverem no estado *habilitado*.O número total de assinatura aumentou para 519. Esse número inclui todas as assinaturas disponíveis no arquivo IOS-S193.zip que pertencem à subcategoria Compartilhamento de
arquivos.



Para obter tópicos mais avançados sobre como usar o Cisco SDM para gerenciar o recurso Cisco IOS IPS, consulte a documentação do Cisco SDM neste URL:

Selecionar assinaturas e trabalhar com categorias de assinatura

Para determinar como selecionar efetivamente as assinaturas corretas de uma rede, você deve saber algumas coisas sobre a rede que está protegendo. As informações atualizadas da categoria de assinatura no Cisco SDM 2.2 e posterior ajudam os clientes a selecionar o conjunto correto de assinaturas para proteger a rede.

A categoria é uma forma de agrupar assinaturas. Ele ajuda a restringir a seleção de assinaturas a um subconjunto de assinaturas relevantes entre si. Uma assinatura pode pertencer a apenas uma categoria ou pode pertencer a várias categorias.

Estas são as cinco categorias de nível superior:

- SO—categorização de assinatura baseada em sistema operacional
- Ataque—categorização de assinatura baseada em ataque
- Serviço—categorização de assinatura baseada em serviço

- Protocolo de Camada 2-4—categorização de assinatura baseada em protocolo
- Versões—categorização de assinatura baseada em versão

Cada uma destas categorias é ainda dividida em subcategorias.

Como exemplo, considere uma rede residencial com uma conexão de banda larga à Internet e um túnel VPN para a rede corporativa. O roteador de banda larga tem o Cisco IOS Firewall ativado na conexão aberta (não VPN) com a Internet para impedir que qualquer conexão seja originada da Internet e conectada à rede doméstica. Todo o tráfego originado da rede doméstica para a Internet é permitido. Suponha que o usuário use um PC baseado em Windows e use aplicativos como HTTP (navegação na Web) e e-mail.

O firewall pode ser configurado para que somente os aplicativos de que o usuário precisa possam fluir pelo roteador. Isso controlará o fluxo de tráfego indesejado e potencialmente ruim que pode se espalhar pela rede. Considere que o usuário doméstico não precisa ou não usa um serviço específico. Se esse serviço tiver permissão para fluir pelo firewall, há um possível buraco que um ataque pode usar para fluir pela rede. As práticas recomendadas permitem apenas os serviços necessários. Agora, é mais fácil selecionar quais assinaturas ativar. Você precisa habilitar assinaturas somente para os serviços que você permite que fluam pelo firewall. Neste exemplo, os serviços incluem e-mail e HTTP. O Cisco SDM simplifica essa configuração.

Para usar a categoria para selecionar as assinaturas necessárias, escolha **Serviço > HTTP** e ative todas as assinaturas. Esse processo de seleção também funciona na caixa de diálogo de importação de assinatura, na qual você pode selecionar todas as assinaturas HTTP e importá-las no roteador.

As categorias adicionais que precisam ser selecionadas incluem DNS, NETBIOS/SMB, HTTPS e SMTP.

Atualizar assinaturas para arquivos SDF padrão

Os três SDFs por construção (ataque-drop.dsf, 128MB.sdf e 256MB.sdf) estão atualmente publicados no Cisco.com em http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (somente clientes registrados) . Versões mais recentes desses arquivos serão publicadas assim que estiverem disponíveis. Para atualizar os roteadores que executam o Cisco IOS IPS com esses SDFs padrão, acesse o site e baixe as versões mais recentes desses arquivos.

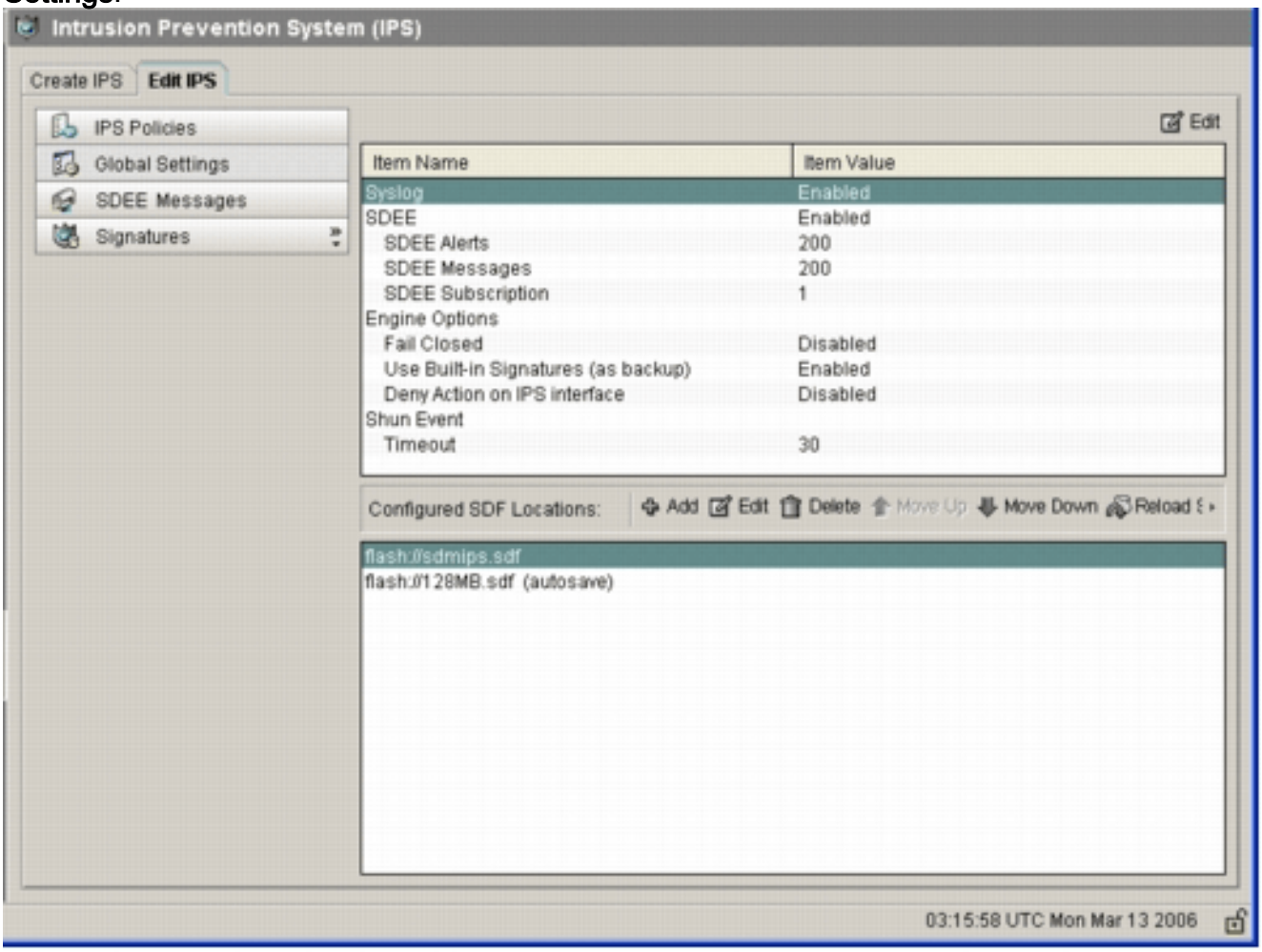
Procedimento CLI

1. Copie os arquivos baixados para o local onde o roteador está configurado para carregar esses arquivos. Para descobrir onde o roteador está configurado no momento, use o comando **show running-config | no** comando **ip ips sdf**.
```
Router#show running-config | in ip ips sdf
ip ips sdf location flash://256MB.sdf autosave
```
   Neste exemplo, o roteador usa 256MB.sdf na memória flash. O arquivo é atualizado quando você copia o novo arquivo baixado 256MB.sdf para a flash do roteador.
2. Recarregue o subsistema Cisco IOS IPS para executar os novos arquivos.Há duas maneiras de recarregar o Cisco IOS IPS: reinicialize o roteador ou reconfigure o Cisco IOS IPS para disparar o subsistema IOS IPS para recarregar assinaturas. Para reconfigurar o Cisco IOS IPS, remova todas as regras de IPS das interfaces configuradas e reaplique as regras de IPS às interfaces. Isso ativará o recarregamento do sistema Cisco IOS IPS.

Procedimento do SDM 2.2

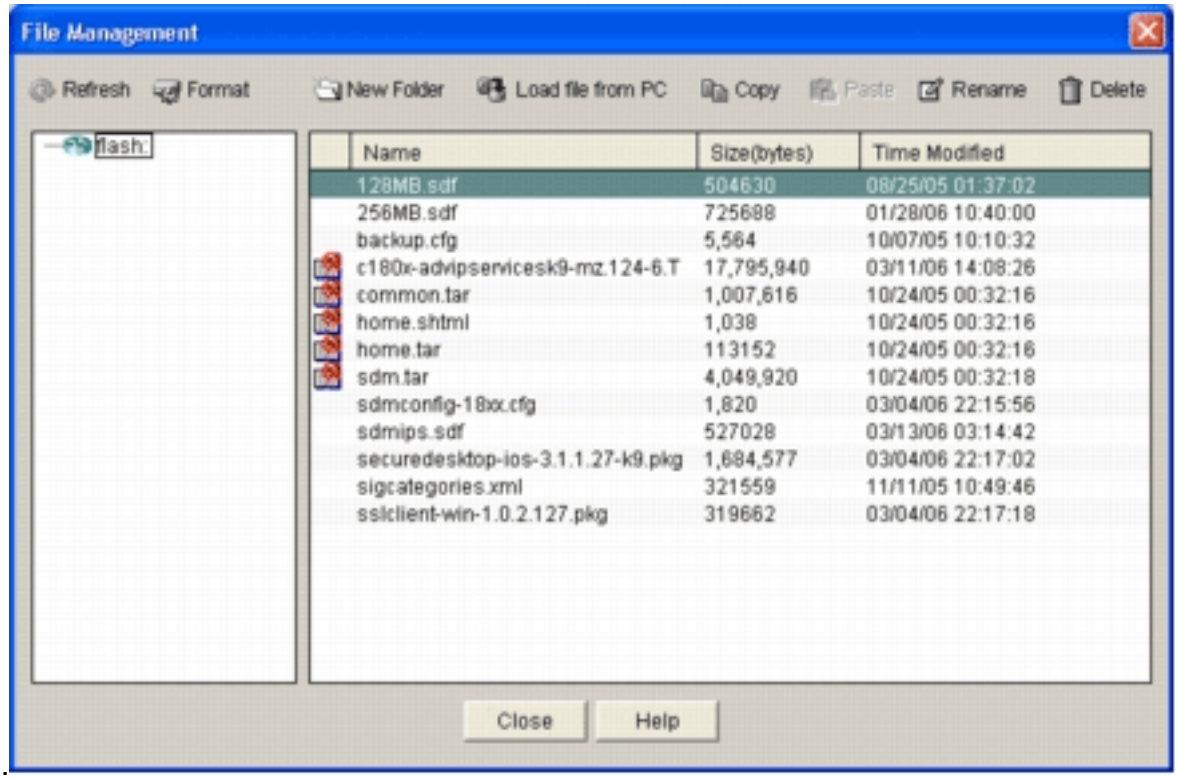
Conclua estes passos para atualizar os SDFs padrão no roteador:

1. Clique em **Configurar** e, em seguida, clique em **Prevenção de intrusão**.
2. Clique na guia **Edit IPS** e clique em **Global Settings**.



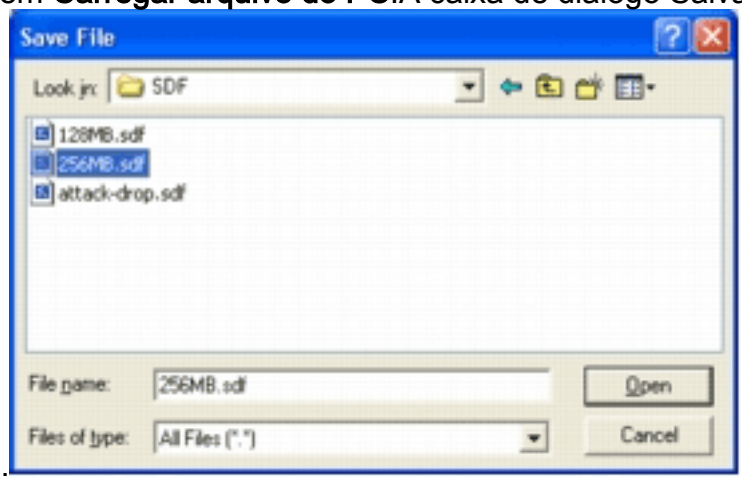
A parte superior da IU mostra as configurações globais. A metade inferior da IU mostra os locais de SDF configurados atualmente. Nesse caso, o arquivo 256MB.sdf da memória flash está configurado.

3. Escolha **Gerenciamento de arquivos** no menu Arquivo.A caixa de diálogo Gerenciamento de arquivos é



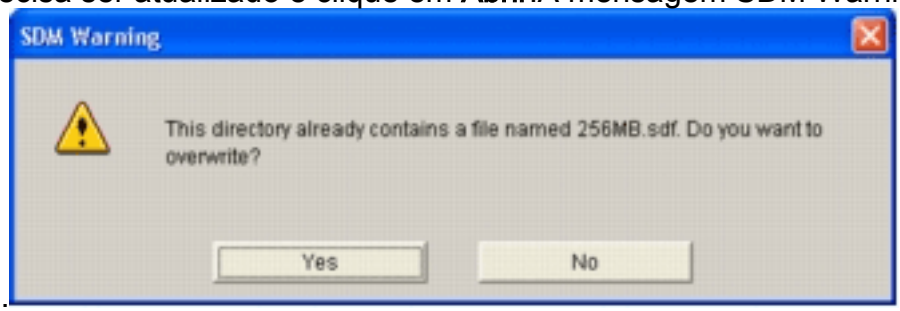
exibida.

4. Clique em **Carregar arquivo do PC**.A caixa de diálogo Salvar arquivo é



exibida.

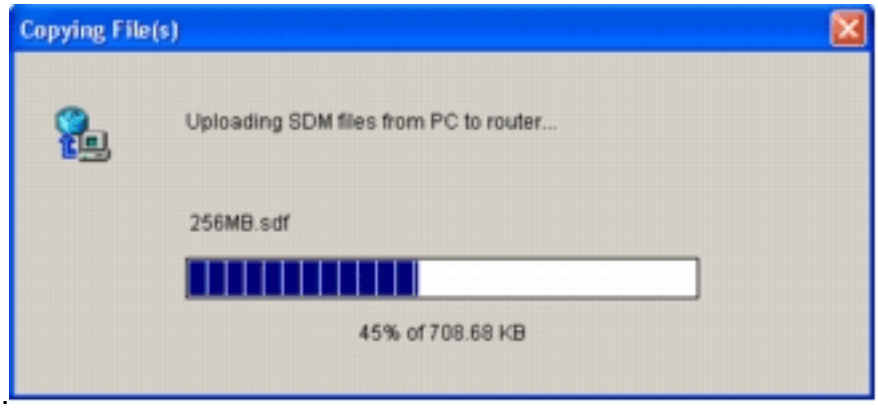
5. Escolha o SDF que precisa ser atualizado e clique em **Abrir**.A mensagem SDM Warning



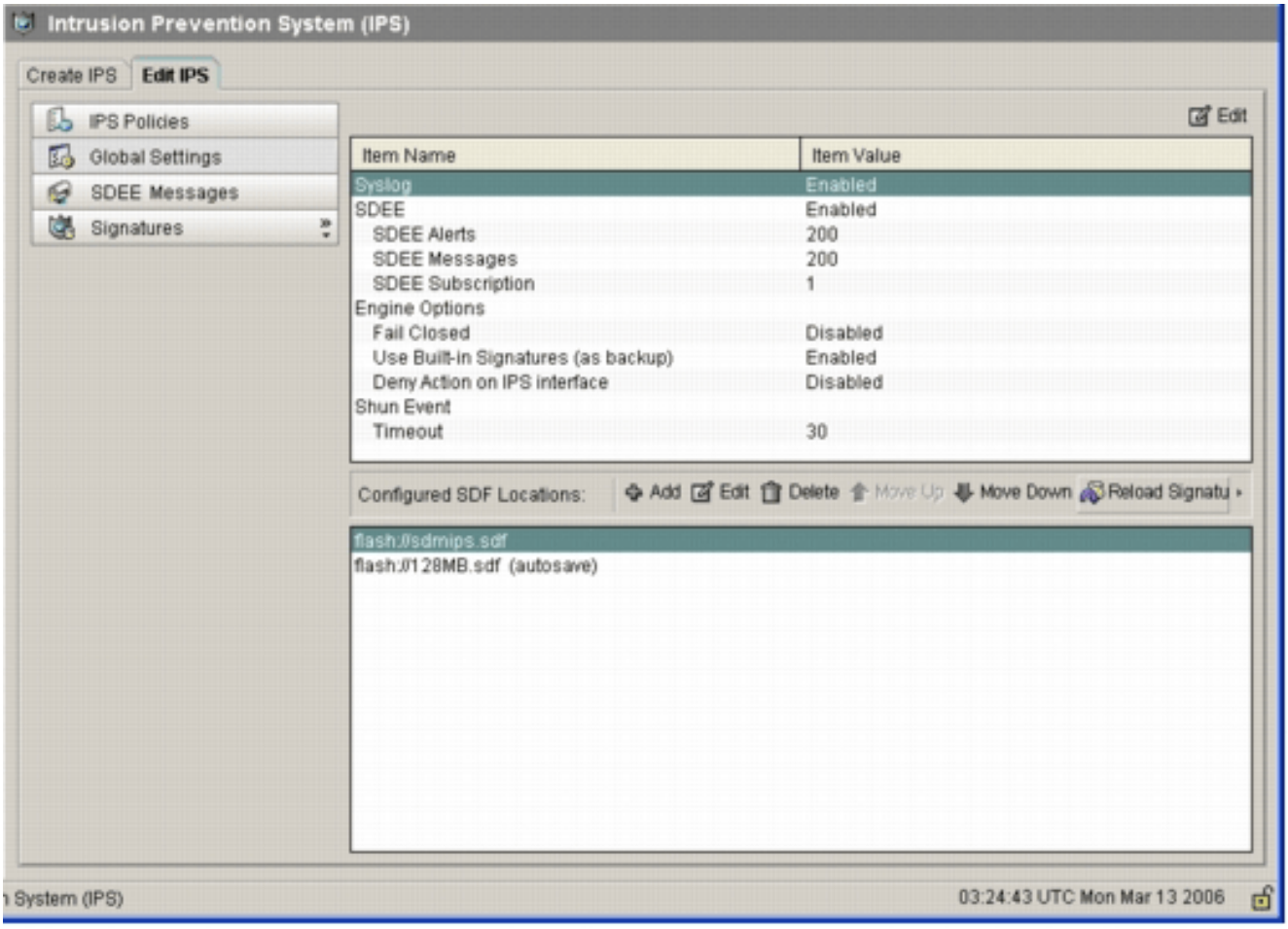
(Aviso SDM) é exibida.

6. Clique em **Sim** para substituir o arquivo existente.Uma caixa de diálogo exibe o progresso do

processo de upload.



7. Quando o processo de carregamento estiver concluído, clique em **Recarregar assinaturas** localizadas na barra de ferramentas de localização do SDF. Esta ação recarrega o Cisco IOS
IPS.



Observação: o pacote IOS-Sxxx.zip contém todas as assinaturas suportadas pelo Cisco IOS IPS. As atualizações para este pacote de assinatura são publicadas no Cisco.com assim que estiverem disponíveis. Para atualizar as assinaturas contidas neste pacote, consulte a Etapa 2.

Informações Relacionadas

- Cisco Intrusion Prevention System
- Avisos de campo do produto de segurança (incluindo CiscoSecure Intrusion Detection)
- Suporte Técnico - Cisco Systems