Exemple de configuration de Router and Security Device Manager (SDM) et de l'interface CLI de Cisco IOS dans le système de prévention des intrusions (IPS) de Cisco IOS

Contenu

Introduction

Dans le Cisco Router and Security Device Manager (SDM) 2.2, la configuration IPS de Cisco IOS® est intégrée dans l'application SDM. Vous n'êtes plus requis de lancer une fenêtre séparée afin de configurer le Cisco IOS IPS.

Dans le Cisco SDM 2.2, un nouvel assistant de configuration IPS vous guide par le Cisco IOS nécessaire IPS d'enable d'étapes sur le routeur. En outre, vous pouvez encore utiliser les options de configuration avancée d'activer, désactiver, et accorder le Cisco IOS IPS avec le Cisco SDM 2.2.

Cisco recommande que vous exécutiez le Cisco IOS IPS avec les fichiers de définition de signature pretuned (SDF) : attack-drop.sdf, 128MB.sdf, et 256MB.sdf. Ces fichiers sont créés pour des Routeurs avec différentes quantités de mémoire. Les fichiers sont empaquetés avec le Cisco SDM, qui recommande des SDF quand vous activez d'abord le Cisco IOS IPS sur un routeur. Ces fichiers peuvent également être téléchargés de http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (registeredcustomers seulement).

Le processus pour activer le par défaut SDF est détaillé dans le Cisco IOS IPS d'enable avec un par défaut SDF d'usine. Quand le par défaut SDF ne sont pas suffisant ou vous voulez ajouter de nouvelles signatures, vous pouvez utiliser la procédure décrite dedans ajoutez les signatures supplémentaires après l'activation du par défaut SDF.

Conditions préalables

Conditions requises

La version 1.4.2 ou ultérieures de Java Runtime Environment (JRE) est exigée pour utiliser le Cisco SDM 2.2. Un fichier de signatures Cisco-recommandé et accordé (basé sur la mémoire vive dynamique) est empaqueté avec le Cisco SDM (chargé sur la mémoire de flash du routeur avec le Cisco SDM).

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Router and Security Device Manager (SDM) 2.2.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cisco IOS IPS d'enable avec un par défaut SDF d'usine

Procédure CLI

Remplissez cette procédure afin d'employer le CLI pour configurer un routeur de gamme Cisco 1800 avec le Cisco IOS IPS charger 128MB.sdf sur le flash du routeur.

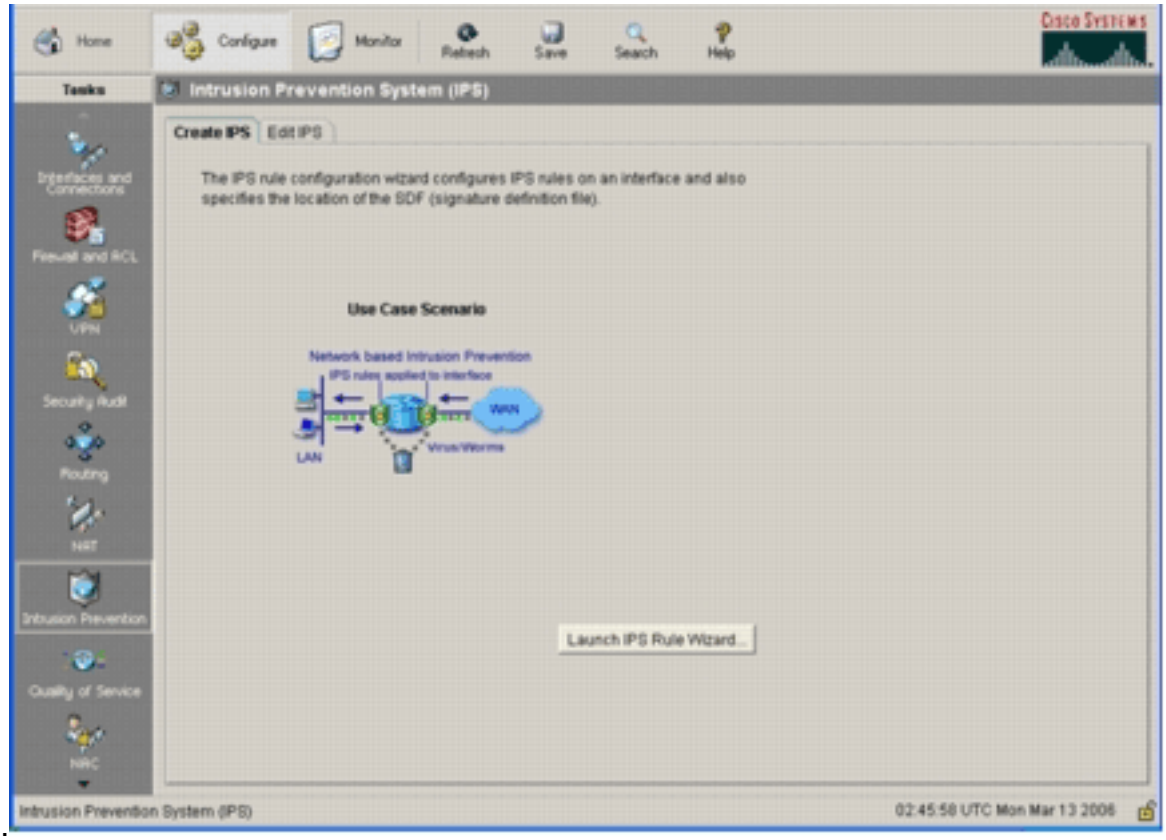
1. Configurez le routeur pour activer la notification d'événement de l'échange d'événement de périphérique de sécurité (SDEE).`yourname#`**`conf t`**
2. Sélectionnez les commandes de configuration (une par la ligne), et puis appuyez sur Cntl+Z pour finir.`yourname(config)#`**`ip ips notify sdee`**
3. Créez un nom de règle IPS qui est utilisé pour s'associer aux interfaces.`yourname(config)#`**`ip ips name myips`**
4. Configurez une commande d'emplacement IPS de spécifier à partir de quel fichier le système IPS de Cisco IOS indiquera des signatures.Cet exemple utilise le fichier sur l'éclair : 128MB.sdf. La partie URL d'emplacement de cette commande peut être n'importe quel URL valide qui emploie l'éclair, le disque, ou les protocoles par l'intermédiaire du FTP, du HTTP, du HTTPS, du RTP, du SCP, et du TFTP afin d'indiquer les fichiers.`yourname(config)#`**`ip ips sdf location flash:128MB.sdf`** **Remarque:** Vous devez activer la commande de **terminal monitor** si vous configurez le routeur par l'intermédiaire d'une session de telnet ou vous ne verrez pas les messages SDEE quand l'engine de signature construit.
5. Activez l'IPS sur l'interface où vous voulez permettre au Cisco IOS IPS de balayer le trafic.

Dans ce cas, nous avons activé sur les deux directions sur les interfaces 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** La première fois qu'une règle IPS est appliquée à une interface, le Cisco IOS IPS commence les signatures construites à partir du fichier spécifié par la commande d'emplacements SDF. Les messages SDEE sont enregistré à la console et envoyé au serveur de Syslog si configurés. Les messages SDEE avec le **<**number **>** du **<**number **>** des engines indique le processus de mise en place d'engine de signature. En conclusion, quand les deux nombres sont identiques, toutes les engines sont construites.**Remarque:** Le réassemblage virtuel IP est une caractéristique d'interface que (une fois activé) rassemble automatiquement les paquets fragmentés qui entrent dans le routeur par cette interface. Cisco recommande que vous activiez le virtuel-assemblage d'IP sur toutes les interfaces où le trafic entre dans le routeur. Dans l'exemple ci-dessus, sans compter qu'activer le « virtuel-assemblage d'IP » sur les interfaces fastethernet 0, nous le configurons sur l'interface interne VLAN 1 aussi bien.yourname(config)#**int vlan 1** yourname(config-if)#**ip virtual-reassembly**

Procédure SDM 2.2

Remplissez cette procédure afin d'employer le Cisco SDM 2.2 pour configurer un routeur de gamme Cisco 1800 avec le Cisco IOS IPS.

1. Dans l'application SDM, cliquez sur Configure, et puis cliquez sur la **prévention des**

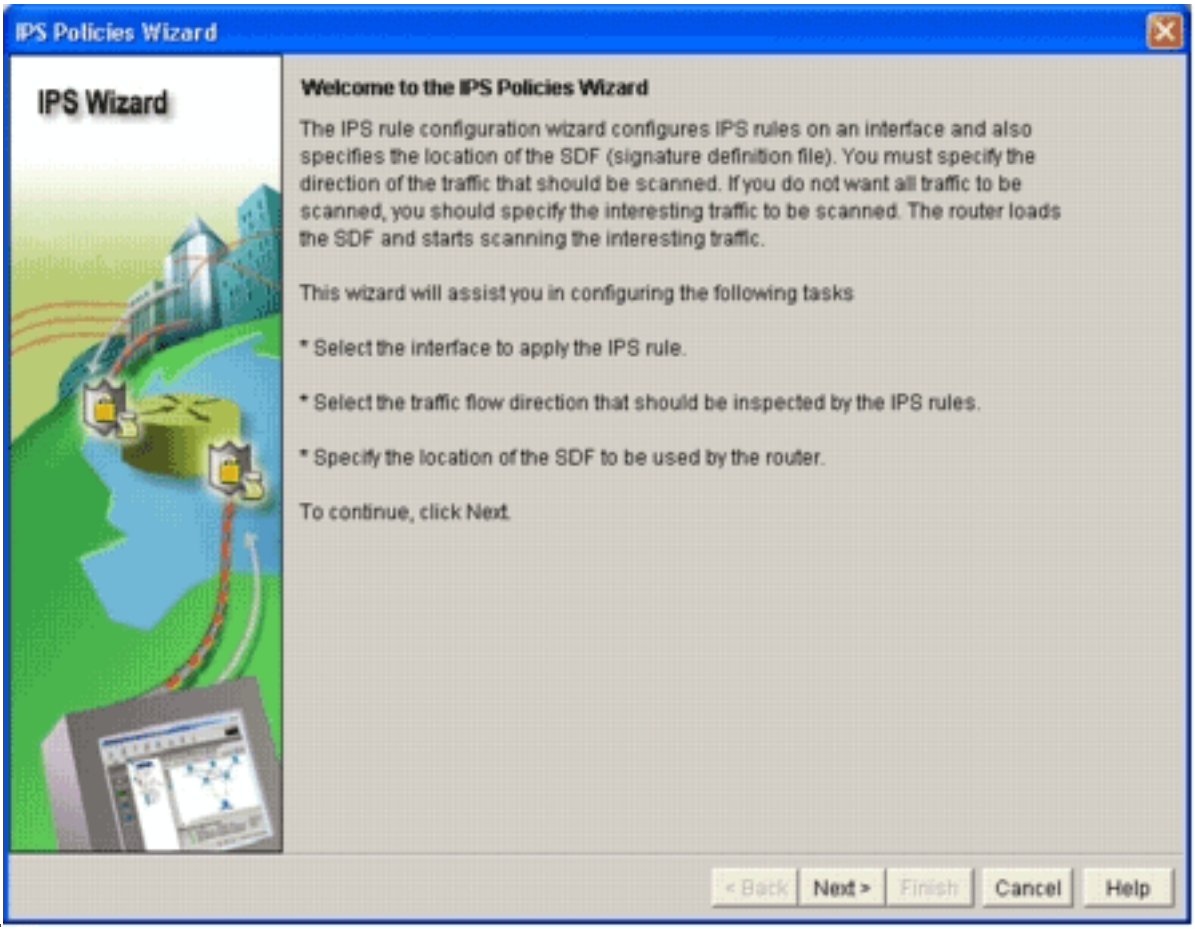


intrusions.

2. Cliquez sur l'onglet **IPS de création**, et puis cliquez sur l'**assistant de règle IPS de lancement**.Le Cisco SDM exige de la notification d'événement IPS par l'intermédiaire de SDEE afin de configurer la caractéristique IPS de Cisco IOS. Par défaut, la notification SDEE n'est pas activée. Le Cisco SDM vous incite à activer la notification d'événement IPS par l'intermédiaire de SDEE suivant les indications de cette image

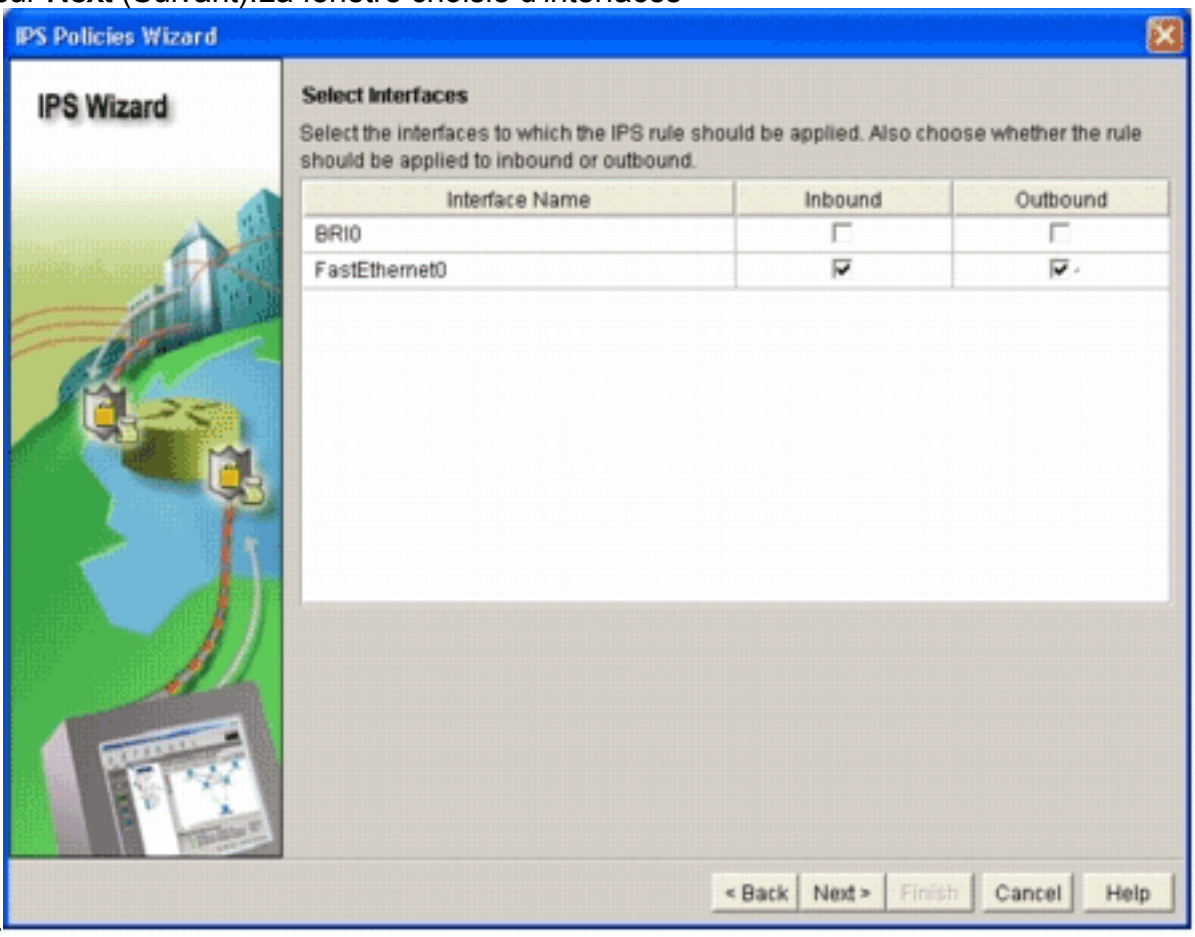
:

3. Cliquez sur **OK**.L'accueil à la fenêtre d'assistant de stratégies IPS de la boîte de dialogue d'assistant de stratégies IPS



apparaît.

4. Cliquez sur **Next** (Suivant).La fenêtre choisie d'interfaces

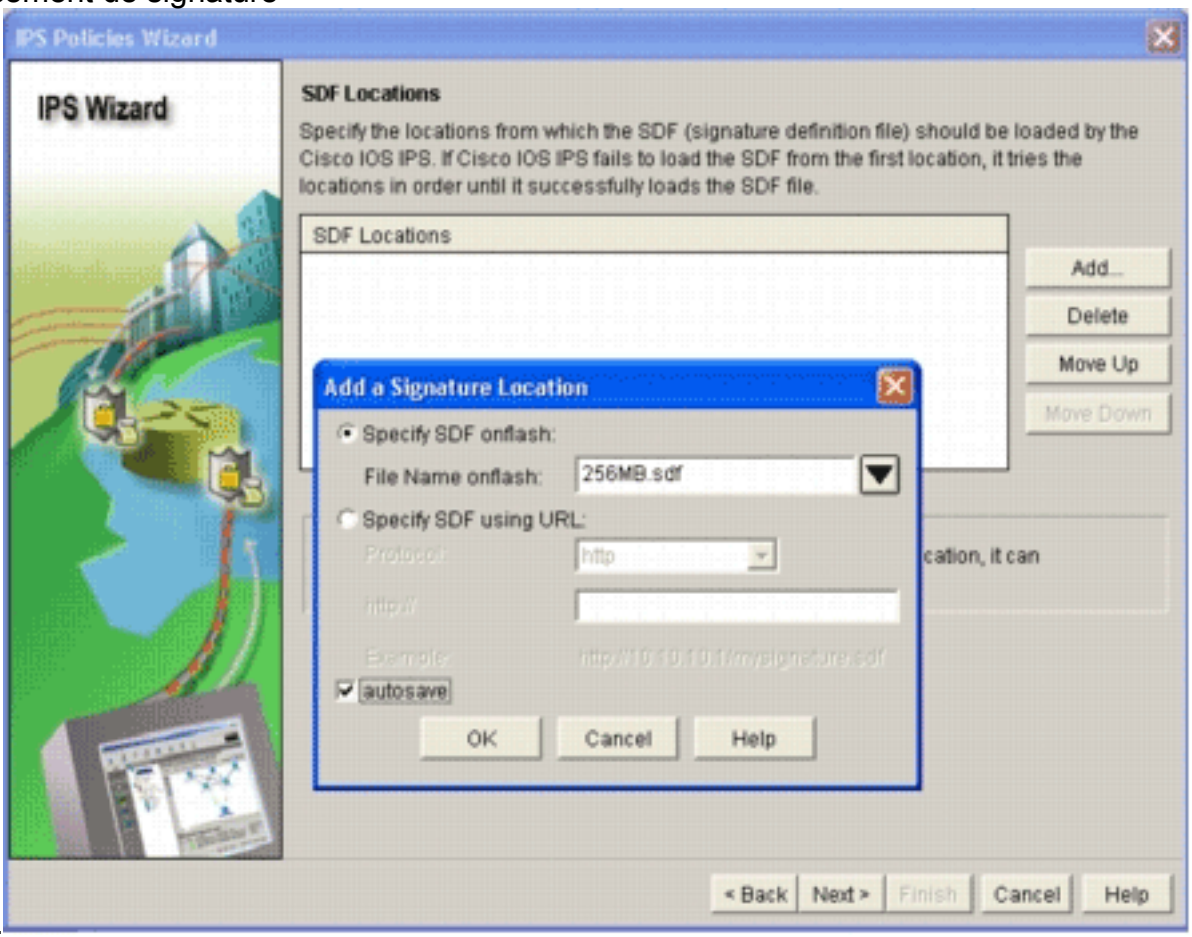


apparaît.

5. Choisissez les interfaces pour lesquelles vous voulez activer l'IPS, et cliquez sur la case à cocher **d'arrivée** ou **sortante** afin d'indiquer la direction de cette interface.**Remarque:** Cisco recommande que vous activiez d'arrivée et des directions sortantes quand vous activez l'IPS

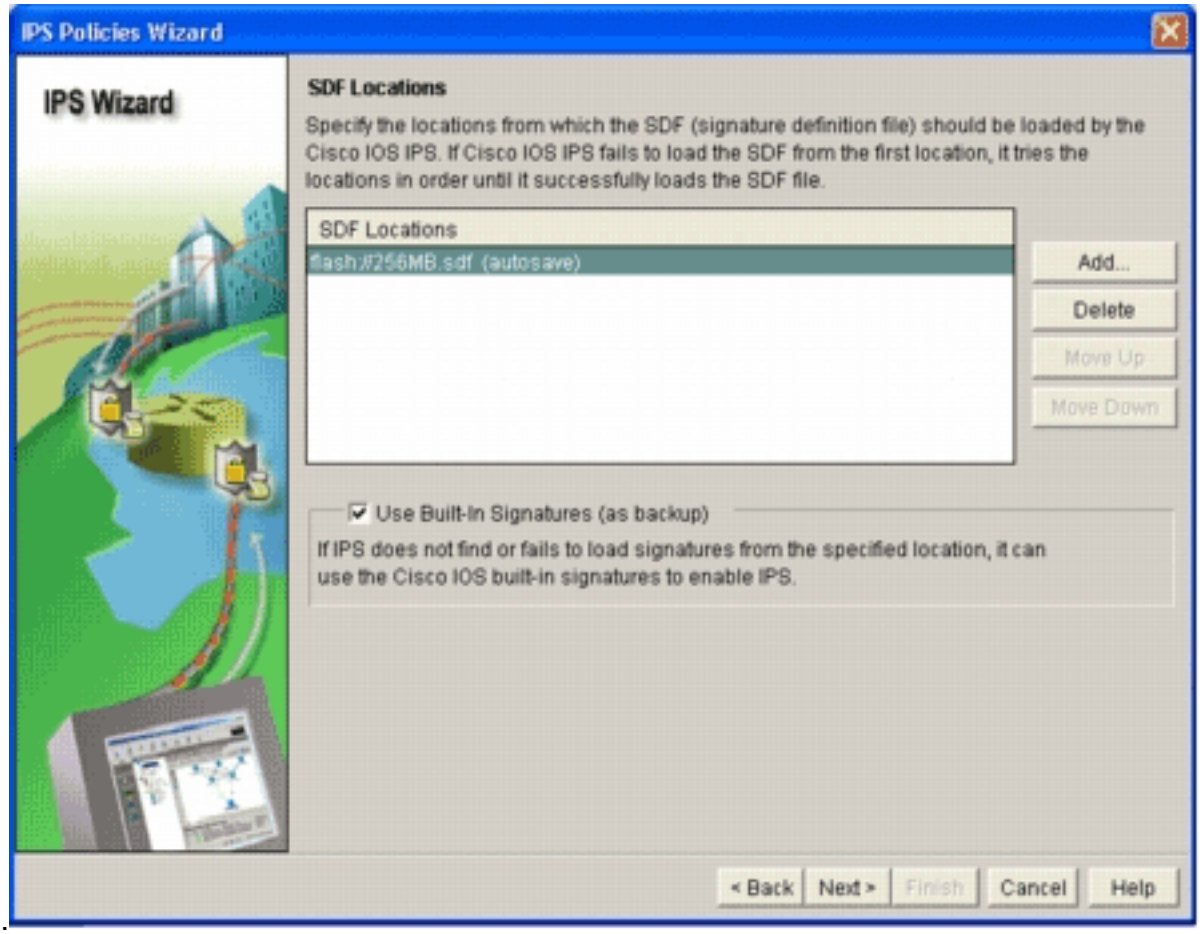
sur une interface.

6. Cliquez sur **Next** (Suivant).La fenêtre d'emplacements SDF apparaît.
7. Cliquez sur Add afin de configurer un emplacement SDF.L'ajouter une boîte de dialogue d'emplacement de signature



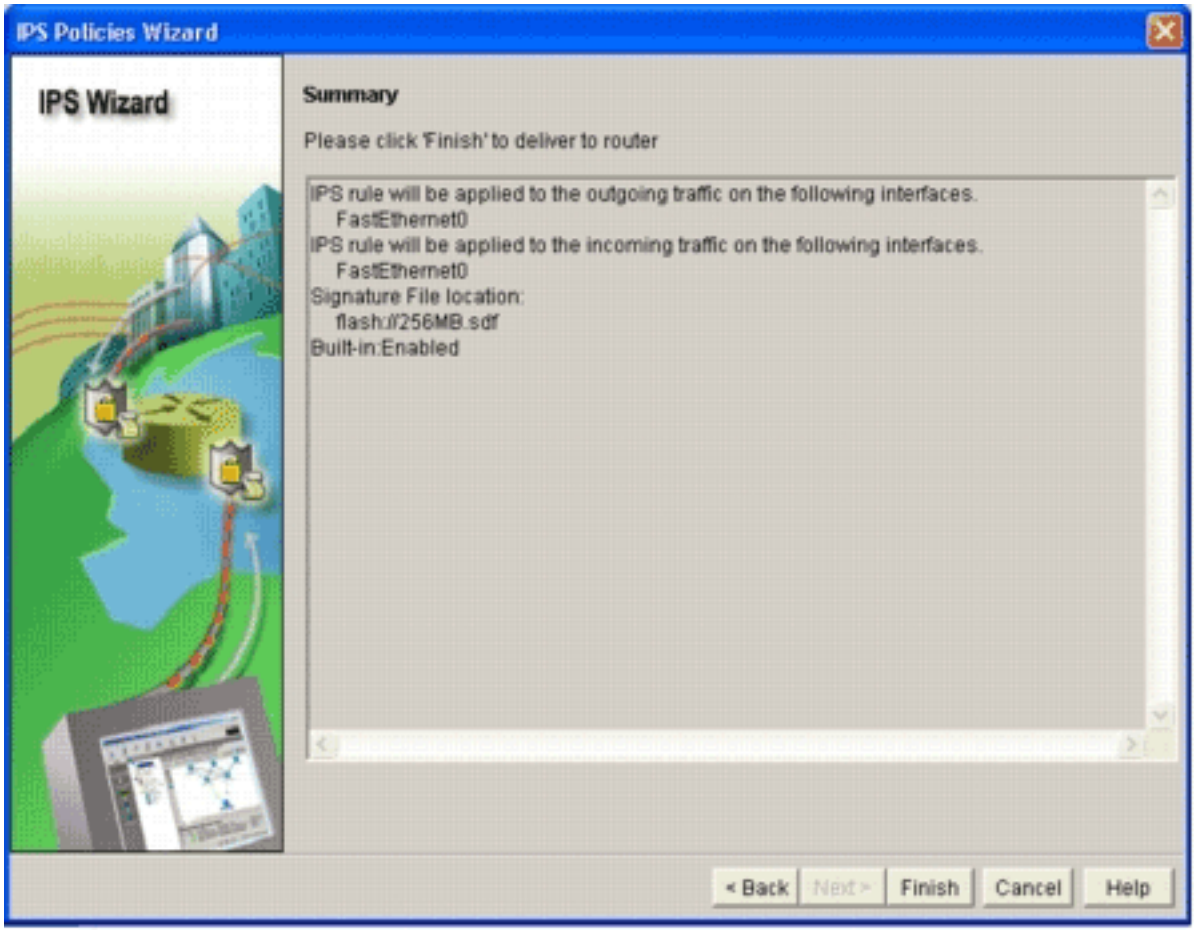
apparaît.

8. Cliquez sur le **spécifier SDF sur la** case d'option **instantanée**, et choisissez 256MB.sdf du **nom du fichier sur la** liste déroulante **instantanée**.
9. Cliquez sur la case à cocher de **sauvegarde automatique**, et cliquez sur OK.**Remarque:** L'option de sauvegarde automatique enregistre automatiquement le fichier de signatures quand il y a une modification de signature.La fenêtre d'emplacements SDF affiche le nouvel emplacement

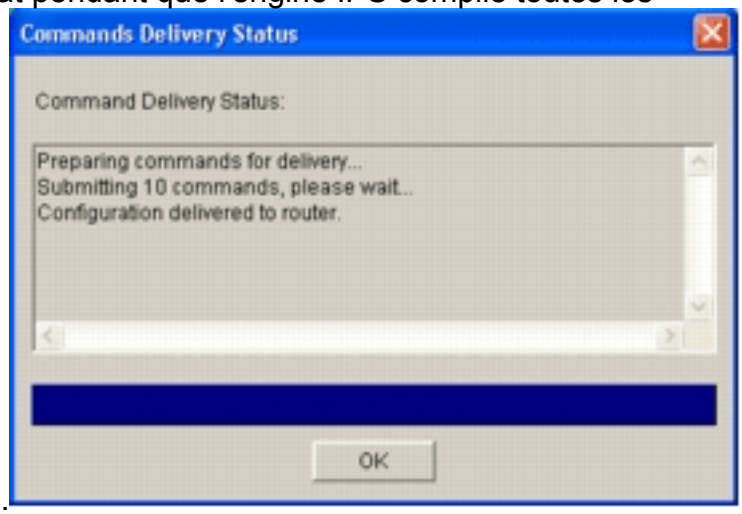


SDF.**Remarque:** Vous pouvez ajouter des emplacements supplémentaires de signature afin d'indiquer une sauvegarde.

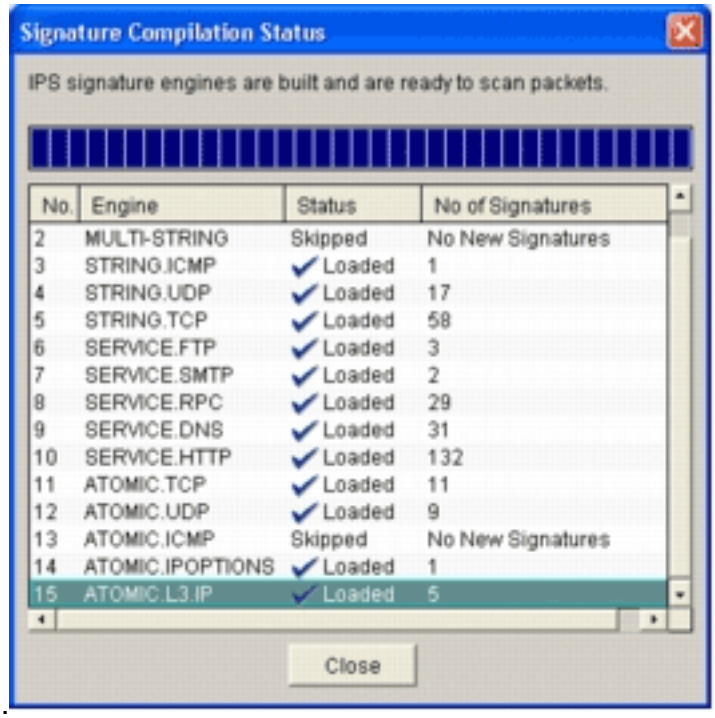
10. Cliquez sur la case **intégrée de signatures d'utilisation (comme sauvegarde)**.**Remarque:** Cisco recommande que vous n'utilisiez pas l'option intégrée de signature à moins que vous ayez spécifié un ou plusieurs emplacements.
11. Cliquez sur Next afin de continuer.La fenêtre récapitulative apparaît.



12. Cliquez sur **Finish** (Terminer).La boîte de dialogue d'état de la livraison de commandes affiche l'état pendant que l'engine IPS compile toutes les signatures.

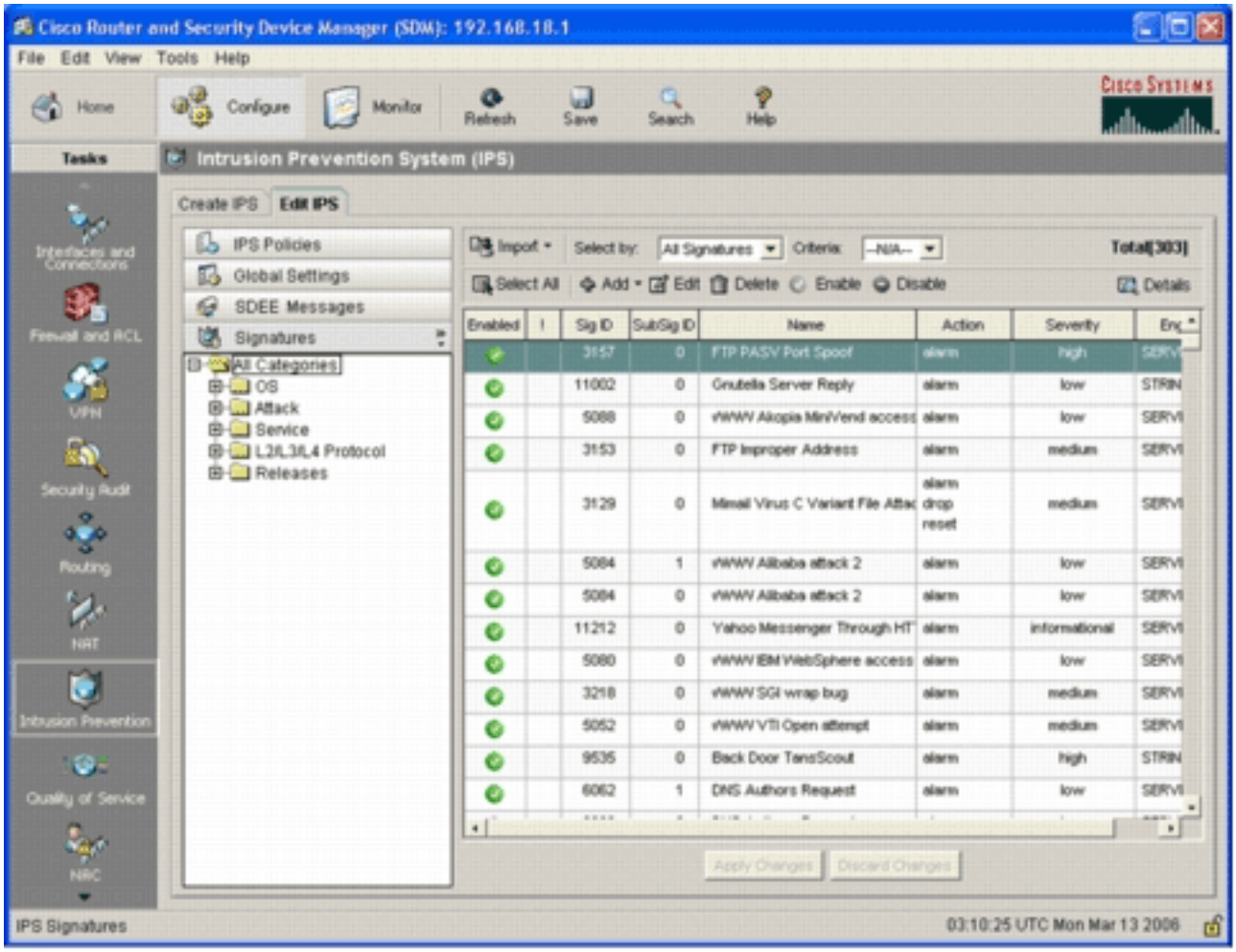


13. Une fois que le processus est complet, cliquez sur OK.La boîte de dialogue d'état de compilation de signature affiche les informations de compilation de



signature.Ces informations affichent quelles engines ont été compilées et le nombre de signatures dans cette engine. Pour les engines qui affichent *ignoré* dans la colonne d'état, il n'y a aucune signature chargée pour cette engine.

14. Clic **étroit** afin de fermer la boîte de dialogue d'état de compilation de signature.
15. Afin de vérifier quelles signatures sont actuellement chargées sur le routeur, cliquez sur Configure, et puis cliquez sur la **prévention des intrusions**.
16. Cliquez sur l'onglet **IPS d'éditer**, et puis cliquez sur les **signatures**.La liste de signature IPS apparaît dans la fenêtre de
    signatures.



Ajoutez les signatures supplémentaires après l'activation du par défaut SDF

Procédure CLI

Il n'y a aucune commande CLI disponible pour créer des signatures ou lire les informations de signature à partir du fichier distribué IOS-Sxxx.zip. Cisco recommande que vous employiez SDM ou le centre de Gestion pour des capteurs IPS pour gérer les signatures sur des systèmes IPS de Cisco IOS.

Pour les clients qui déjà ont un fichier de signatures prêt et veulent fusionner ce fichier avec le SDF qui exécute sur le Cisco IOS système IPS, vous pouvez utiliser cette commande :

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

Le fichier de signatures défini par la commande d'emplacement de signature est où le routeur charge des fichiers de signatures quand elle recharge ou quand l'IOS du routeur IPS est modifié. Pour que le processus de fusionnement soit réussi, le fichier défini par la commande d'emplacement de fichier de signatures doit également être mis à jour.

1. Employez la **commande show** afin de vérifier les emplacements actuellement configurés de signature.La sortie affiche les emplacements configurés de signature. Cette commande montre d'où les signatures courantes en cours sont chargées.`yourname#show ip ips signatures Builtin signatures are configured` Des signatures ont été pour la dernière fois chargées de flash:128MB.sdfVersion S128.0 de Cisco SDFVersion V0.0 de la tendance SDF
2. Employez le **<url de copie > la** commande **IPS-sdf**, avec les informations de l'étape précédente, afin de fusionner des fichiers de signatures.`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# Après que vous émettiez la Commande **COPY**, le routeur charge le fichier de signatures dans la mémoire et puis construit les engines de signature. Dans la sortie de message de la console SDEE, l'état de bâtiment pour chaque engine de signature est affiché.%IPS-6-ENGINE_BUILD_SKIPPED indique qu'il n'y a aucune nouvelle signature pour cette engine.%IPS-6-ENGINE_READY indique qu'il y a de nouvelles signatures et l'engine est prête. Comme avant, le "15 message de 15 engines » indique que toutes les engines ont été construites.IPS-7-UNSUPPORTED_PARAM indique qu'un certain paramètre n'est pas pris en charge par le Cisco IOS IPS. Par exemple, CapturePacket et ResetAfterIdle.**Remarque:** Ces messages sont pour information seulement et n'auront aucun affect sur la capacité ou la représentation de signature IPS de Cisco IOS. Ces messages de journalisation peuvent être arrêtés en plaçant le débogage de niveau se connectant de supérieur à (niveau 7).

3. Mettez à jour le SDF défini par la commande d'emplacement de signature, tels que quand les routeurs rechargés, il auront la signature fusionnée réglée avec les signatures mises à jour. Cet exemple affiche la différence de taille de fichier après que la signature fusionnée soit enregistrée au fichier Flash 128MB.sdf.yourname#**show flash:** -#- --length-- -----

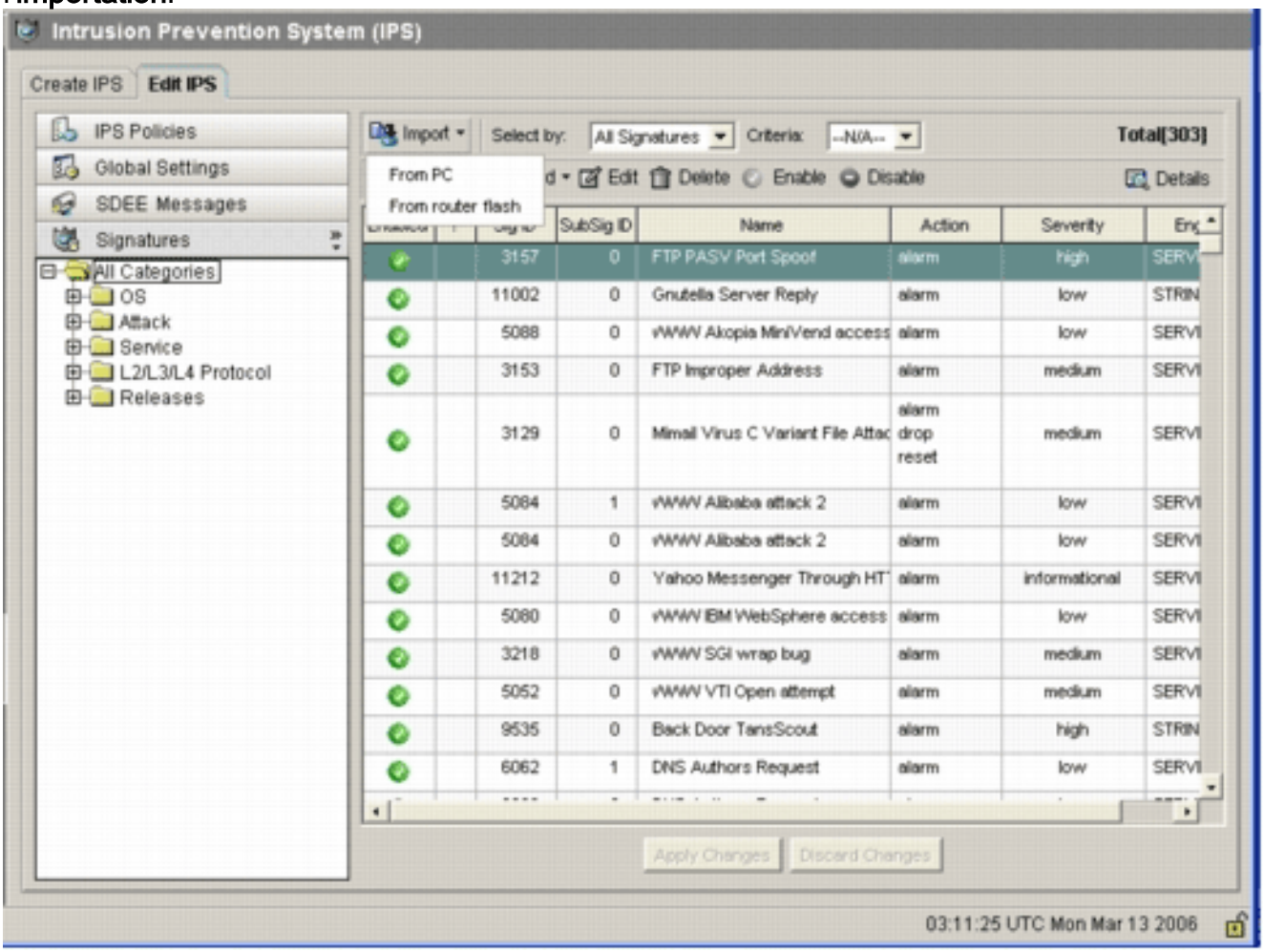
```
date/time------ path 4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf yourname#copy ips-sdf
flash:128MB.sdf yourname#show flash: -#- --length-- -----date/time------ path 4 522656 Oct
26 2005 02:51:32 +00:00 128MB.sdf
```

Avertissement : Le nouveau 128MB.sdf contient maintenant les signatures client-fusionnées. Le contenu est différent à partir du fichier de la valeur par défaut de Cisco 128MB.sdf. Cisco recommande que vous changiez ce fichier à un nom différent pour éviter la confusion. Si le nom est changé, la commande d'emplacement de signature doit être aussi bien changée.

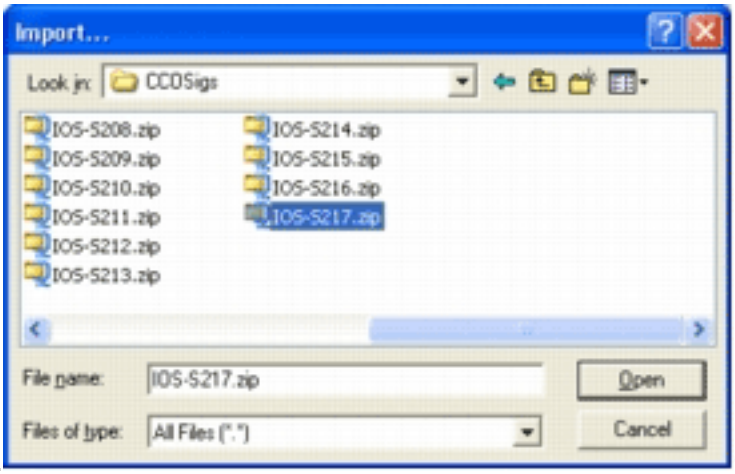
Procédure SDM 2.2

Après que le Cisco IOS IPS ait été activé, de nouvelles signatures peuvent être ajoutées dans le routeur qui exécute un positionnement de signature avec la fonction d'importation de Cisco SDM. Terminez-vous ces étapes afin d'importer de nouvelles signatures :

1. Choisissez le par défaut SDF ou le fichier de mise à jour IOS-Sxxx.zip pour importer les signatures supplémentaires.
2. Cliquez sur Configure, et puis cliquez sur la **prévention des intrusions**.
3. Cliquez sur l'onglet **IPS d'éditer**, et puis cliquez sur l'**importation**.

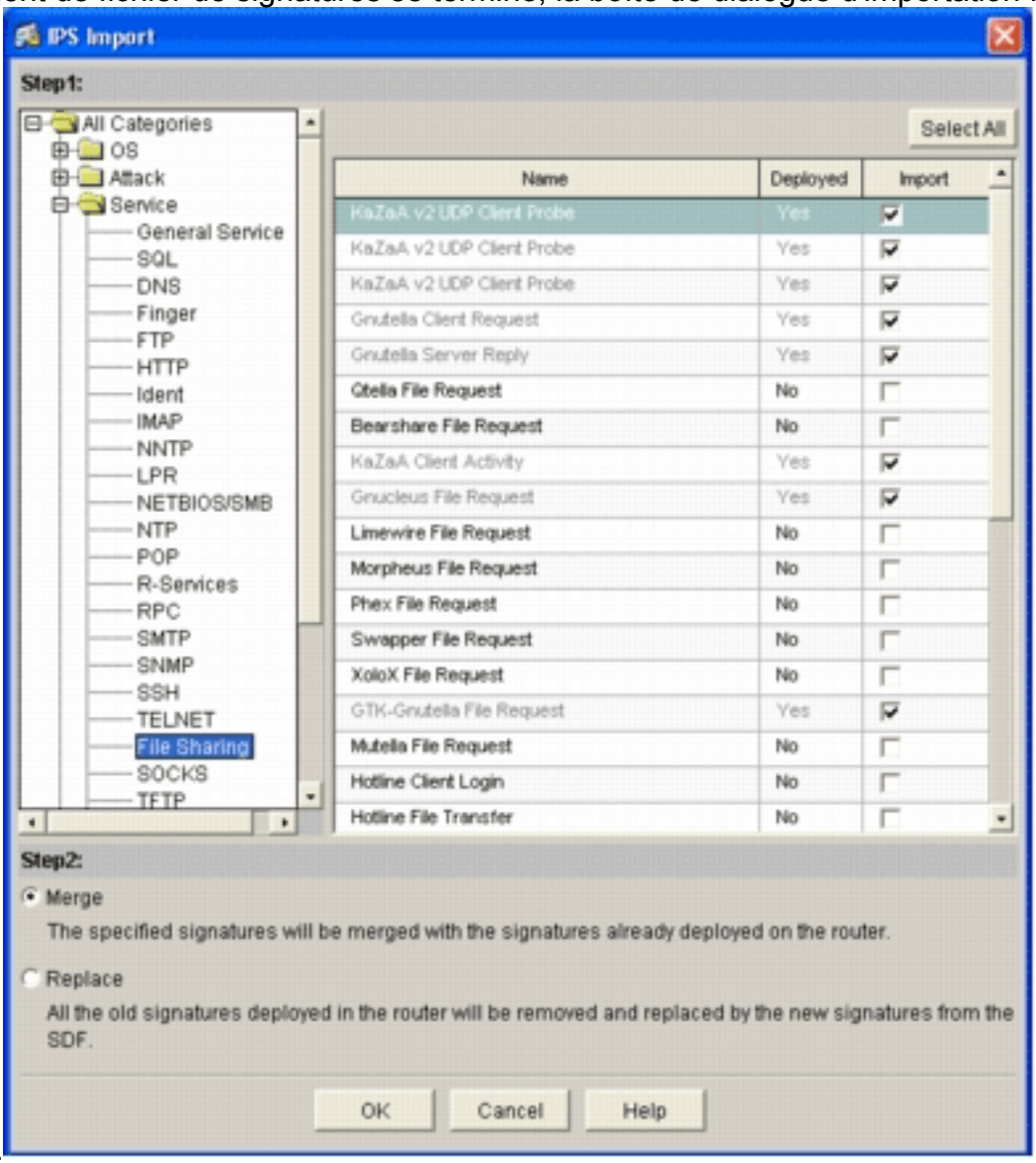


4. Choisissez du **PC de la** liste déroulante d'importation.
5. Sélectionnez le fichier dont vous voulez importer des



signatures.Cet exemple utilise la dernière mise à jour téléchargée de Cisco.com et enregistrée sur le disque dur d'ordinateur local.

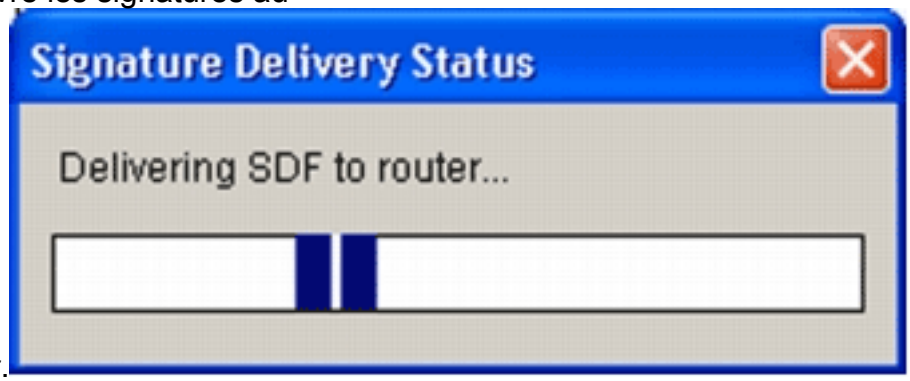
6. Cliquez sur **Open**.**Avertissement :** En raison de la contrainte de mémoire, seulement un nombre limité de nouvelles signatures peut être ajouté sur les signatures qui ont été déjà déployées. Si trop de signatures sont sélectionnées, le routeur ne pourrait pas pouvoir charger toutes les nouvelles signatures en raison du manque de mémoire.Une fois que le chargement de fichier de signatures se termine, la boîte de dialogue d'importation IPS



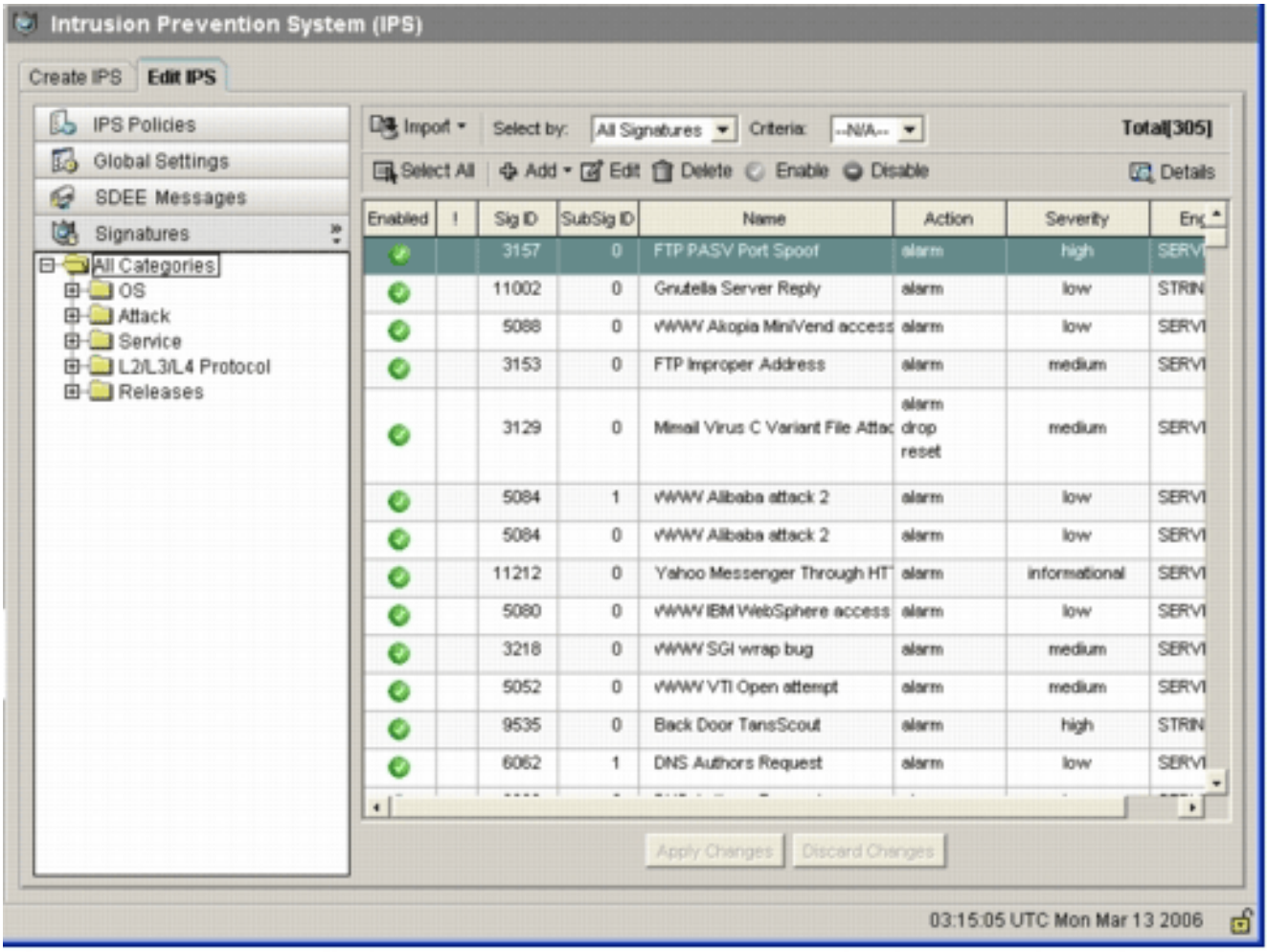
apparaît.

7. Naviguez par la vue d'arborescence gauche, et cliquez sur la case d'**importation** à côté des signatures que vous voulez importer.
8. Cliquez sur la case d'option de **fusion**, et puis cliquez sur OK.**Remarque:** L'option de

remplacer remplace le positionnement en cours de signature sur le routeur par les signatures que vous sélectionnez pour importer.Une fois que vous cliquez sur OK, l'application de Cisco SDM livre les signatures au



routeur.**Remarque:** L'utilisation du CPU élevé se produit pendant la compilation et le chargement des signatures. Après que le Cisco IOS IPS soit activé sur l'interface, les débuts de fichier de signatures à charger. Le routeur prend environ cinq minutes pour charger le SDF. Vous pouvez tenter d'employer la commande **CPU de processus d'exposition** afin de visualiser l'utilisation du processeur du logiciel CLI de Cisco IOS. Cependant, ne tentez pas d'utiliser des commandes supplémentaires ou de charger d'autres SDF tandis que le routeur charge le SDF. Ceci peut faire prendre le processus de compilation de signature plus long pour se terminer (puisque l'utilisation du processeur est proche de l'utilisation 100-percent au moment de charger le SDF). Vous pourriez devoir parcourir par la liste de signatures et activer les signatures si elles ne sont pas état dedans *activé*.Tout le nombre de signature a grimpé jusqu'à 519. Ce nombre inclut toutes les signatures disponibles dans le fichier IOS-S193.zip qui appartiennent à la sous-catégorie de partage de
fichier.



Pour plus de sujets avancés au sujet de la façon employer le Cisco SDM pour gérer la caractéristique IPS de Cisco IOS, référez-vous à la documentation de Cisco SDM à cet URL :

Signatures et travail choisis avec des catégories de signature

Afin de déterminer comment sélectionner efficacement les signatures correctes pour un réseau, vous devez connaître quelques choses au sujet du réseau que vous protégez. Les informations mises à jour de catégorie de signature dans le Cisco SDM 2.2 et les plus défunts autres clients d'aide pour sélectionner l'ensemble correct de signatures pour protéger le réseau.

La catégorie est une manière de grouper des signatures. Il aide à rétrécir vers le bas la sélection de signature à un sous-ensemble de signatures qui sont appropriées entre eux. Une signature pourrait appartenir à seulement une catégorie ou elle pourrait appartenir à de plusieurs catégories.

Ce sont les cinq catégories supérieures :

- SYSTÈME D'EXPLOITATION — catégorisation exécution Exécution système de signature
- Attaque — catégorisation basée sur attaque de signature
- Service — Catégorisation de signature de service en fonction
- Couche 2-4 Protocol — catégorisation basée sur Protocol de signature
- Releases — catégorisation basée sur release de signature

Chacune de ces catégories est encore divisée en sous-catégories.

Comme exemple, considérez un réseau domestique avec une connexion haut débit à l'Internet et un tunnel VPN au réseau d'entreprise. Le routeur haut débit a le Pare-feu Cisco IOS activé sur la connexion à Internet (non-VPN) ouverte empêcher n'importe quelle connexion d'être provenu de

l'Internet et être connecté au réseau domestique. On permet tout le trafic qui provient du réseau domestique à l'Internet. Supposez que l'utilisateur utilise un PC sous Windows et utilise des applications comme le HTTP (navigation web) et le courrier électronique.

Le Pare-feu peut être configuré de sorte que seulement les applications qu'on permet les besoins de l'utilisateur de traverser le routeur. Ceci contrôlera l'écoulement du trafic non désiré et potentiellement mauvais qui peut se propager dans tout le réseau. Considérez que l'utilisateur privé n'a pas besoin ou utilise d'un service spécifique. Si on permet à ce service pour traverser le Pare-feu, il y a un trou potentiel qu'une attaque peut employer pour circuler dans tout le réseau. Les pratiques recommandées permettent seulement des services qui sont nécessaires. Maintenant, il est plus facile de sélectionner quelles signatures à activer. Vous devez activer des signatures seulement pour les services que vous laissez traverser le Pare-feu. Dans cet exemple, les services incluent le courrier électronique et le HTTP. Le Cisco SDM simplifie cette configuration.

Afin d'employer la catégorie pour sélectionner les signatures requises, choisissez le **service > le HTTP**, et activez toutes les signatures. Ce processus de sélection fonctionne également dans le dialogue d'importation de signature, où vous pouvez sélectionner toutes les signatures de HTTP et les importer dans votre routeur.

Les catégories supplémentaires qui doivent être sélectionnées incluent des DN, NETBIOS/SMB, HTTPS, et SMTP.

Signatures de mise à jour pour les fichiers SDF par défaut

Les trois SDF de construction par (attack-drop.dsf, 128MB.sdf, et 256MB.sdf) sont actuellement signalés sur Cisco.com chez http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (registeredcustomers seulement). De plus nouvelles versions de ces fichiers seront signalées dès qu'elles seront disponibles. Afin de mettre à jour les Routeurs qui exécutent le Cisco IOS IPS avec des ces le par défaut SDF, vont au site Web et téléchargent les dernières versions de ces fichiers.

Procédure CLI

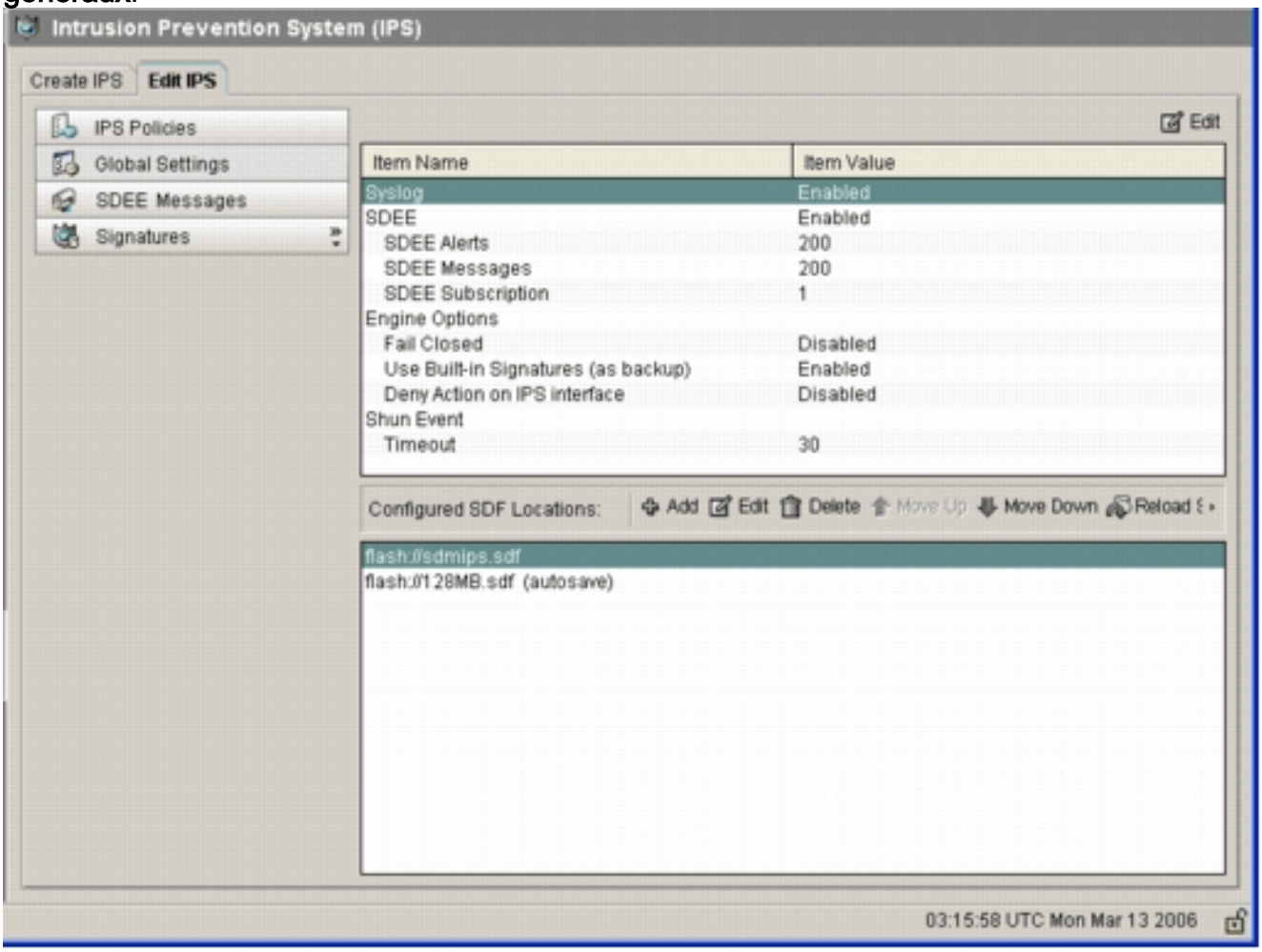
1. Copiez les fichiers téléchargés sur l'emplacement d'où le routeur est configuré pour charger ces fichiers. Pour découvrir où le routeur est actuellement configuré, utilisez le **show running-config | dans la** commande de **sdf d'ip ips**.`Router#show running-config | in ip ips sdf ip ips sdf location flash://256MB.sdf autosave` Dans cet exemple, le routeur utilise 256MB.sdf sur l'éclair. Le fichier est mis à jour quand vous copiez le nouveau 256MB.sdf téléchargé sur le flash du routeur.
2. Rechargez le sous-système IPS de Cisco IOS pour exécuter les nouveaux fichiers.Il y a deux manières de recharger le Cisco IOS IPS : rechargez le routeur ou modifiez le Cisco IOS IPS pour déclencher le sous-système d'IOS IPS pour recharger des signatures. Afin de modifier le Cisco IOS IPS, retirez toutes les règles IPS des interfaces configurées, et puis réappliquez les règles IPS de nouveau aux interfaces. Ceci déclenchera le système IPS de Cisco IOS pour recharger.

Procédure SDM 2.2

Terminez-vous ces étapes afin de mettre à jour le par défaut SDF sur le routeur :

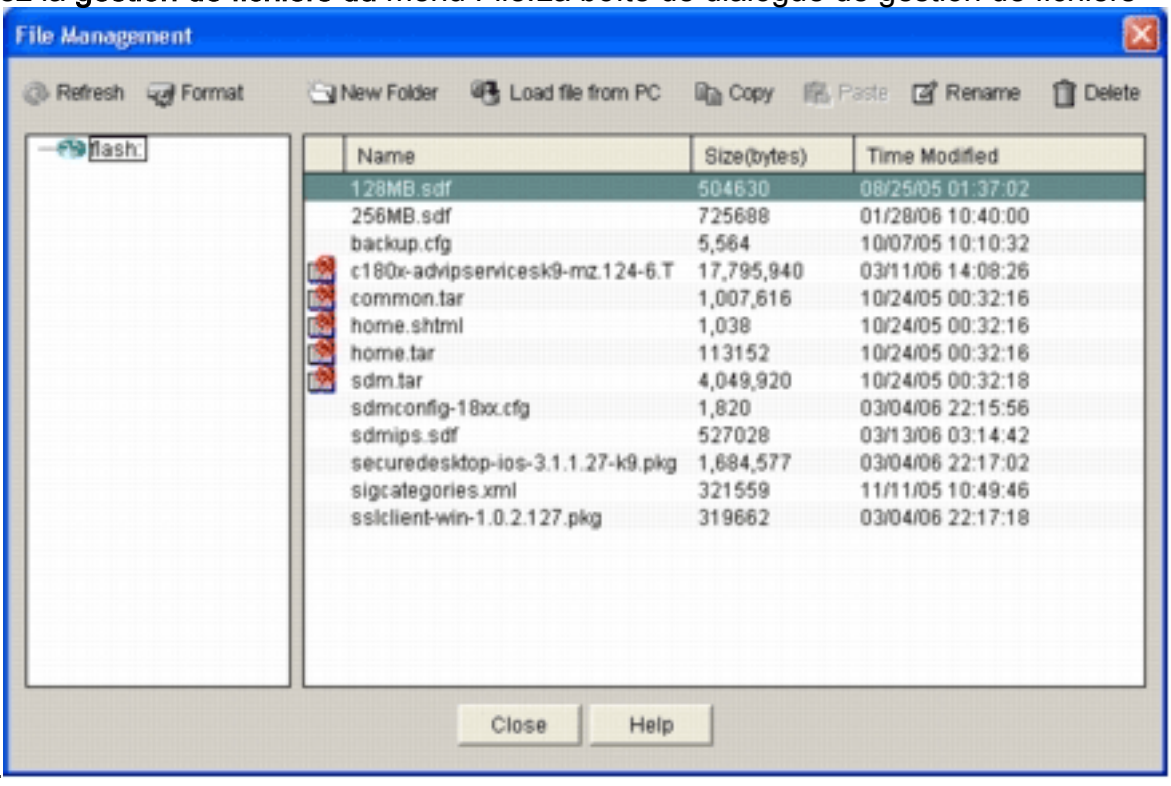
1. Cliquez sur Configure, et puis cliquez sur la **prévention des intrusions**.
2. Cliquez sur l'onglet **IPS d'éditer**, et puis cliquez sur les **paramètres**

généraux.

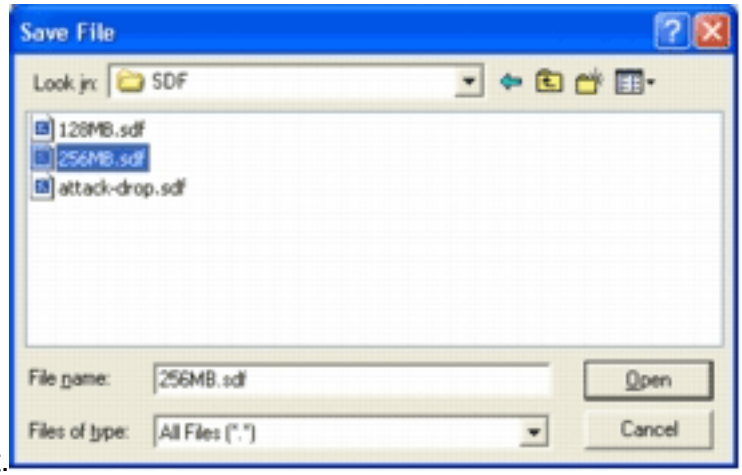


Le dessus de l'UI affiche les paramètres généraux. La moitié inférieure de l'UI affiche des emplacements SDF actuellement configurés. Dans ce cas, le fichier 256MB.sdf de la mémoire flash est configuré.

3. Choisissez la **gestion de fichiers du** menu File.La boîte de dialogue de gestion de fichiers apparaît.

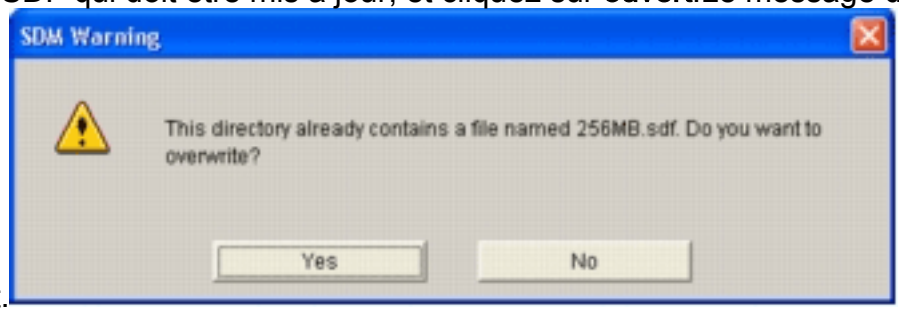


4. **Fichier de chargement de** clic de **PC**.La boîte de dialogue de fichier de sauvegarde

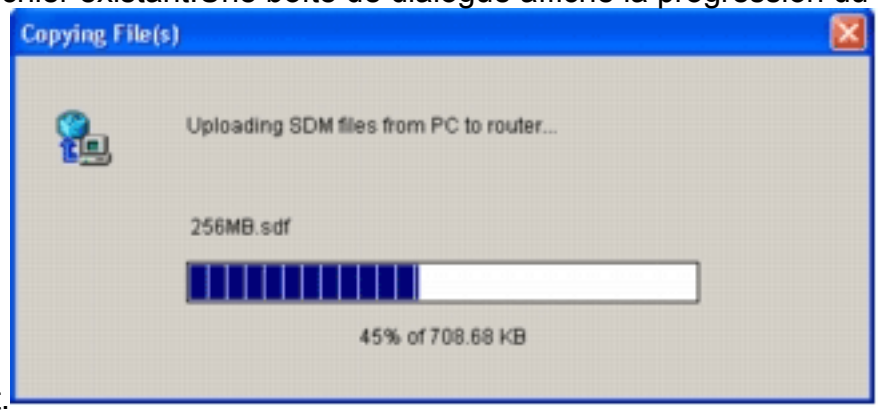


apparaît.

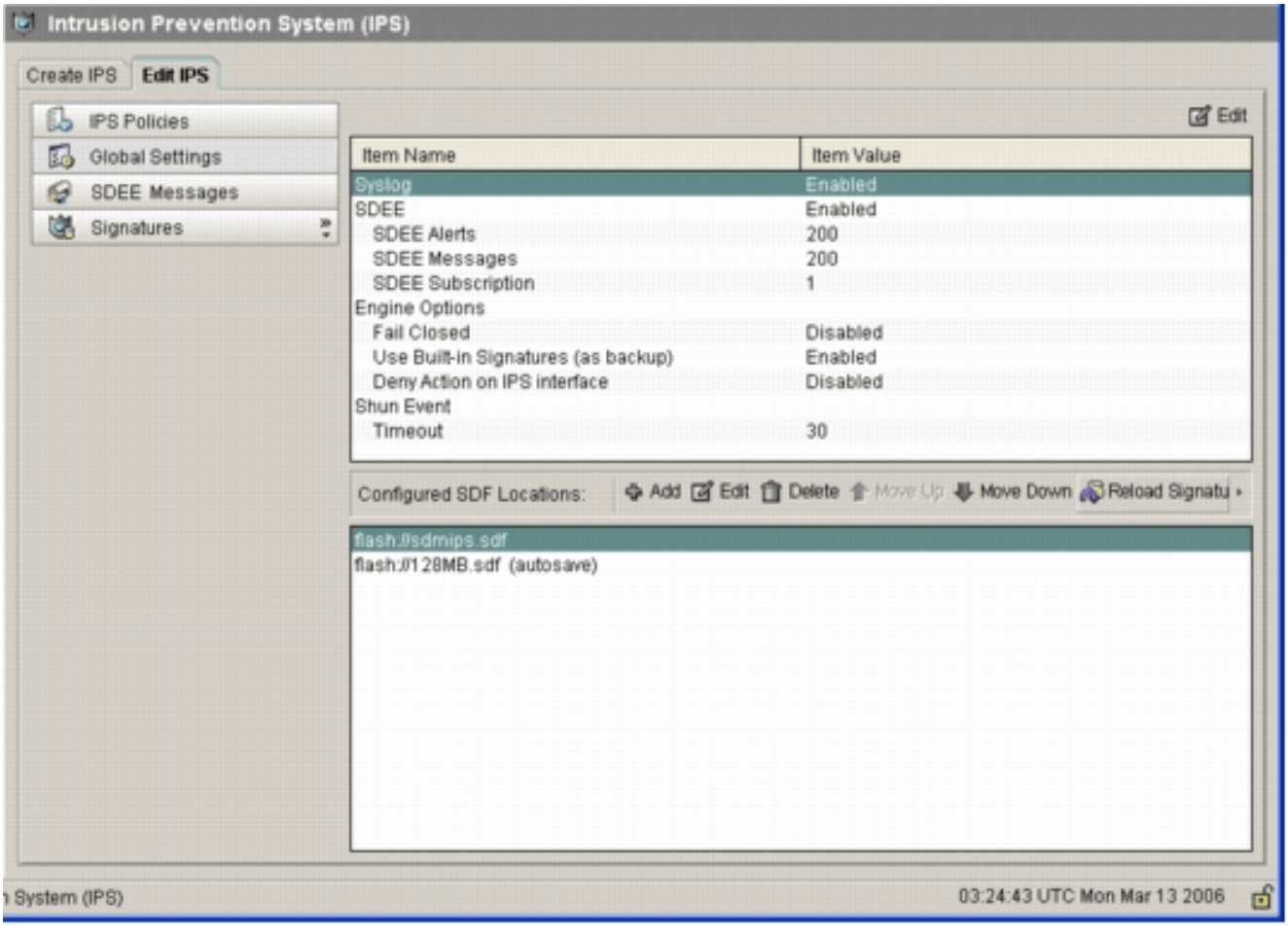
5. Choisissez le SDF qui doit être mis à jour, et cliquez sur **ouvert**.Le message d'avertissement SDM apparaît.



6. Clic **oui** afin de remplacer le fichier existant.Une boîte de dialogue affiche la progression du processus de téléchargement.



7. Une fois le processus de téléchargement est complet, des **signatures de recharge de** clic situées sur la barre d'outils d'emplacement SDF. Ce actions reload le Cisco IOS IPS.



Remarque: Le module IOS-Sxxx.zip contient toutes les signatures que le Cisco IOS IPS prend en charge. Des mises à jour à ce module de signature sont signalées sur Cisco.com dès qu'elles deviendront disponibles. Afin de mettre à jour des signatures contenues en ce module, voir le Step2.

Informations connexes

- Système de protection contre les intrusions Cisco
- Notes de terrain relatives aux produits de sécurité (détection y compris d'intrusion de CiscoSecure)
- Support technique - Cisco Systems