

# Configurer Security Manager dans Cisco IOS IPS

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Informations connexes](#)

## [Introduction](#)

Cisco Security Manager fait partie de la suite de gestion de la sécurité Cisco, qui assure une administration et une application complètes des politiques pour le réseau Cisco Self-Defending Network. Cisco Security Manager est une application d'entreprise de pointe pour la gestion de la sécurité. Cisco Security Manager traite de la gestion de la configuration des services de sécurité de pare-feu, VPN et IPS (Intrusion Prevention System) sur les routeurs, les appliances de sécurité et les modules de services de sécurité Cisco.

Pour un résumé des fonctionnalités et avantages de Cisco Security Manager, ainsi que des nouvelles fonctionnalités de la version 3.1, reportez-vous à la fiche technique de Cisco Security Manager 3.1 à l'adresse

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product\\_data\\_sheet0900aecd8062bf6e.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html). Vous pouvez télécharger Cisco Security Manager 3.1 depuis Cisco.com à l'adresse <http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app> (clients [enregistrés](#) uniquement).

Ce document décrit comment utiliser Cisco Security Manager 3.1 afin d'effectuer la configuration initiale d'IOS IPS. Pour les routeurs déjà configurés avec IOS IPS, les clients peuvent directement utiliser Cisco Security Manager 3.1 pour les tâches de provisionnement.

**Remarque** : Cisco Security Manager 3.1 prend uniquement en charge les images IOS 12.4(11)T2 et ultérieures afin de configurer IOS IPS.

## [Conditions préalables](#)

### [Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

### [Components Used](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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.

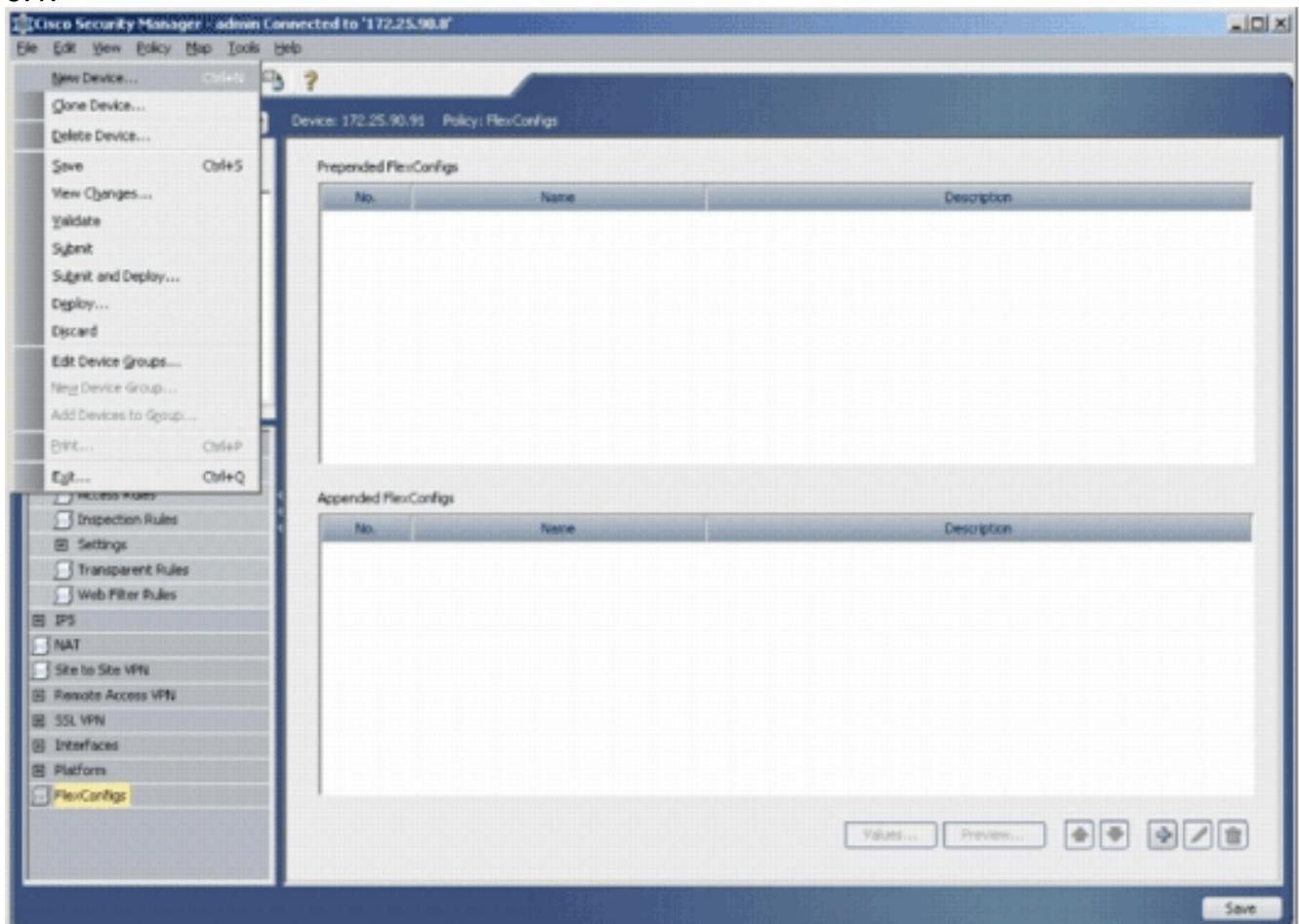
## Conventions

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

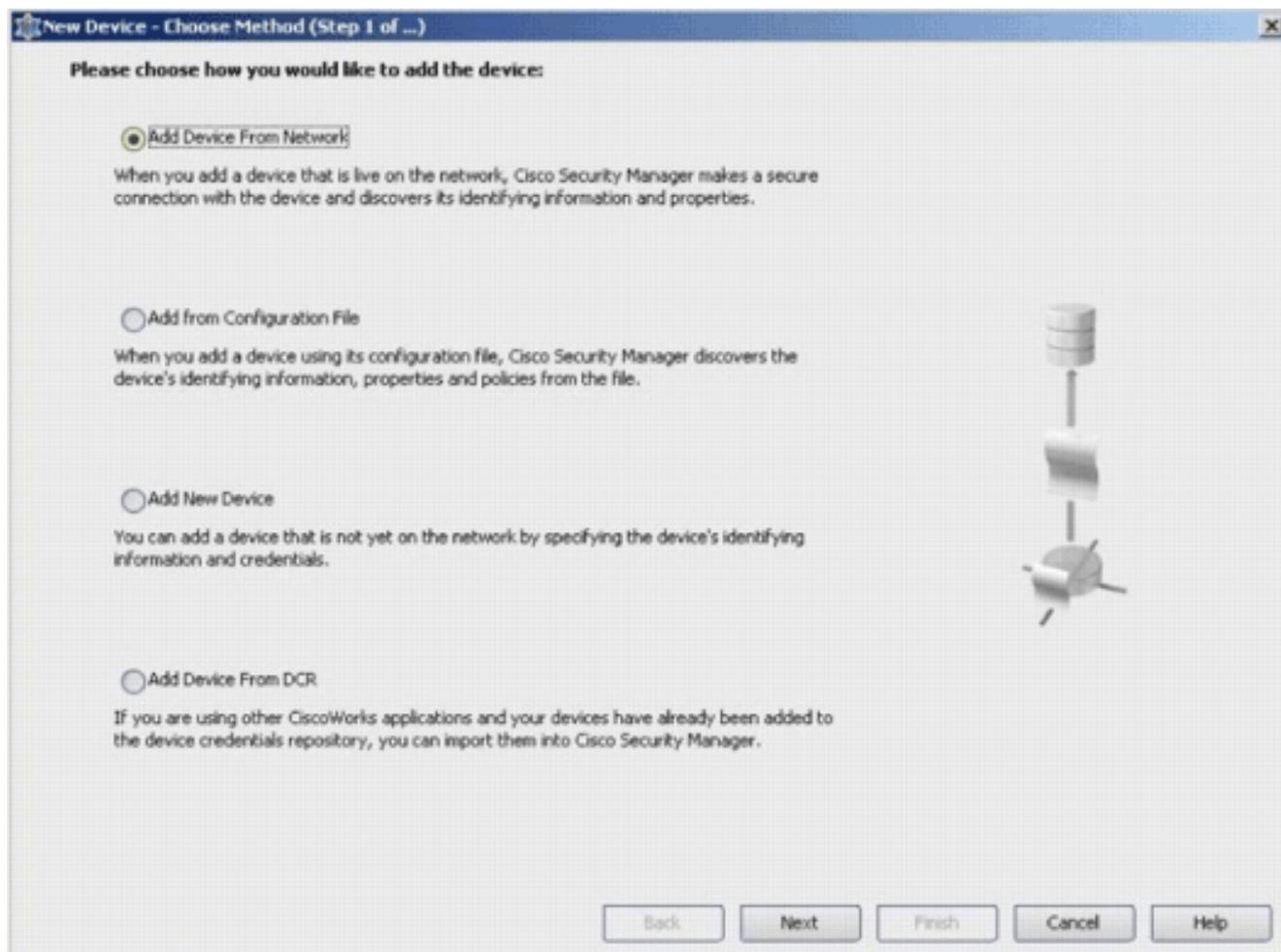
## Configuration

Complétez ces étapes afin de configurer IOS IPS :

1. Exécutez le client Cisco Security Manager 3.1 à partir de votre ordinateur local.
2. Choisissez **New Device** dans le menu File afin d'ajouter un périphérique à Cisco Security Manager
- 3.1.



3. Dans la fenêtre Nouveau périphérique, sélectionnez la manière dont vous souhaitez ajouter le périphérique. Cet exemple montre comment ajouter le périphérique du réseau.



4. Cliquez sur **Next** (Suivant).

5. Saisissez les détails d'identité du périphérique que vous souhaitez ajouter. Par exemple, le nom d'hôte et l'adresse IP.

**New Device - Device Information (Step 2 of 4)**

**Identity**

IP Type: Static

Host Name:

Domain Name:

IP Address: 172.25.90.91

Display Name:\* 172.25.90.91

OS Type:\*

- IOS - 12.3+
- IOS - 12.2, 12.1
- IOS - Catalyst 6500/7600
- PIX
- FW5M
- IPS
- ASA

**Discover Device Settings**

Discover:

- Firewall Policies
- IPS Policies
- RA VPN Policies
- Discover Policies for Security Contexts

Back Next Finish Cancel Help

6. Cliquez sur **Next** (Suivant).
7. Saisissez les informations d'identification principales, telles que le nom d'utilisateur, le mot de passe et le mot de passe Enable pour le routeur IOS que vous souhaitez ajouter.
8. Cliquez sur **Terminer** afin d'ajouter le périphérique à Cisco Security Manager. **Remarque** : Cet exemple suppose que l'utilisateur dispose déjà d'un routeur préconfiguré et peut se connecter au routeur avec les informations d'identification appropriées.

New Device - Device Credentials (Step 3 of 4)

**Primary Credentials**

Username:

Password:\*  Confirm:\*

Enable Password:  Confirm:

**HTTP Credentials**

Use Primary Credentials

Username:

Password:

Confirm:

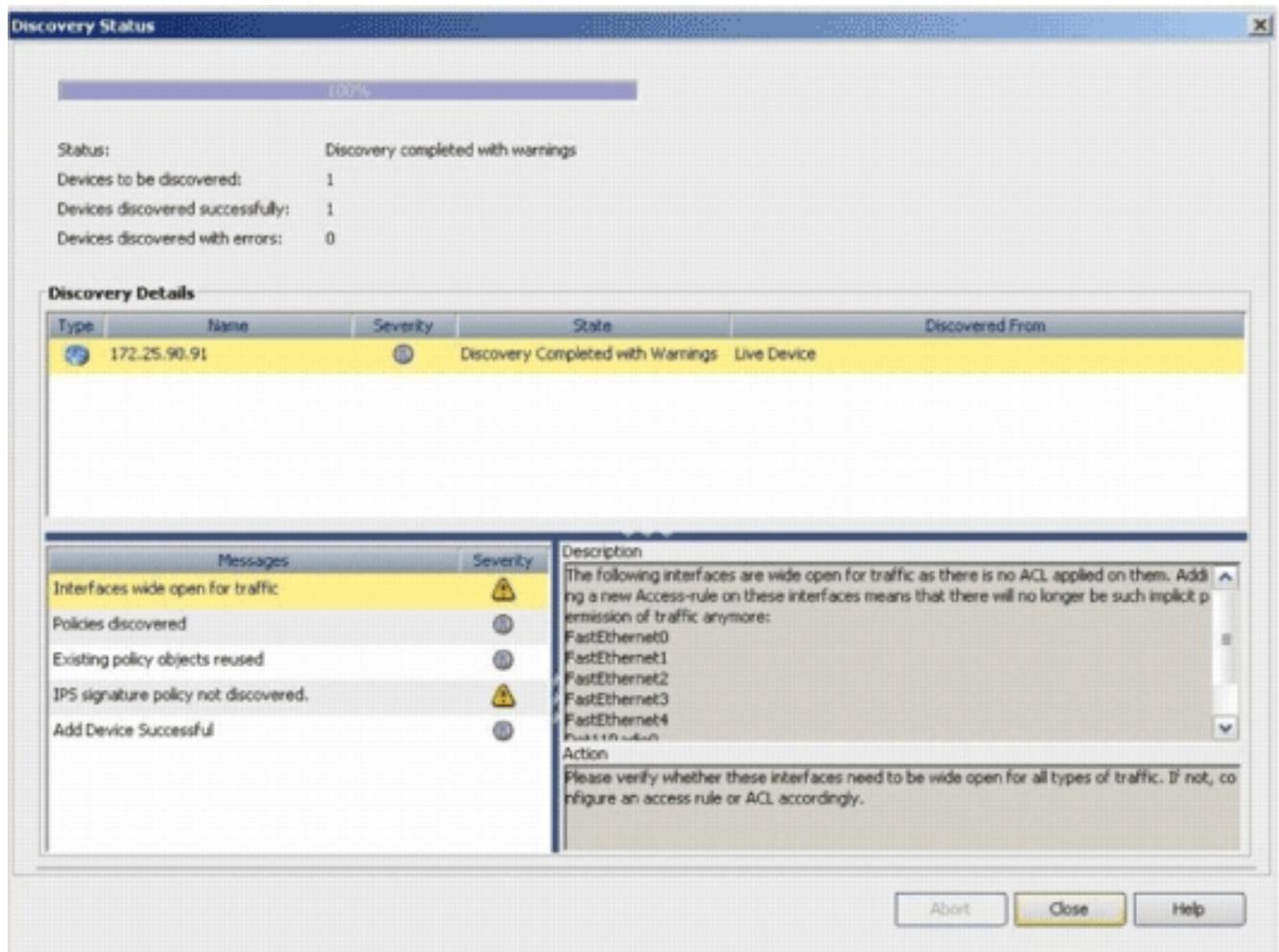
HTTP Port:

HTTPS Port:

IPS RDEP Mode:

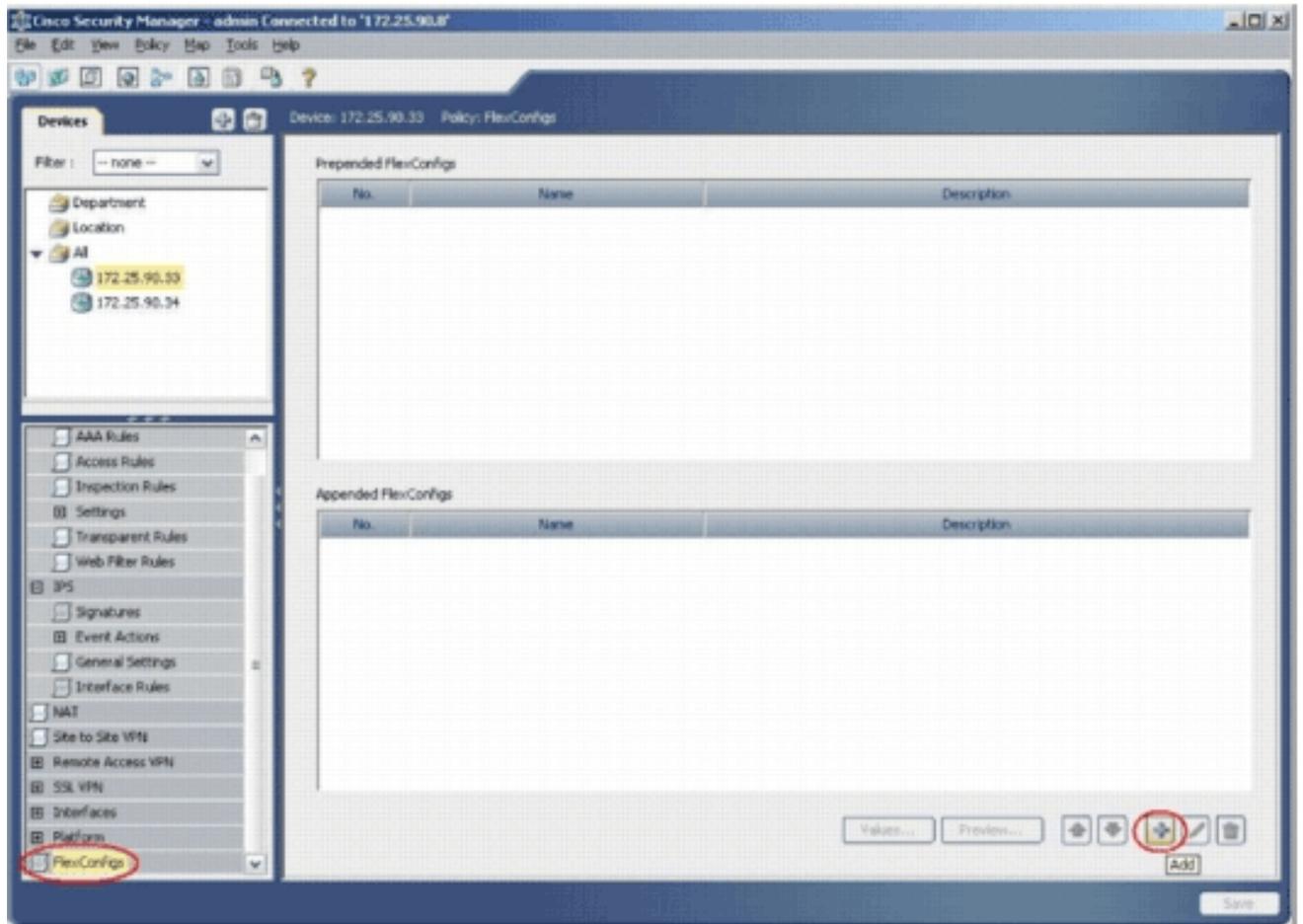
Certificate Common Name:  Confirm:

Une fois la détection terminée, vous avez ajouté un périphérique à Cisco Security Manager. Une fois que vous avez correctement ajouté un périphérique à Cisco Security Manager, vous devez attribuer une clé publique afin d'activer IPS.

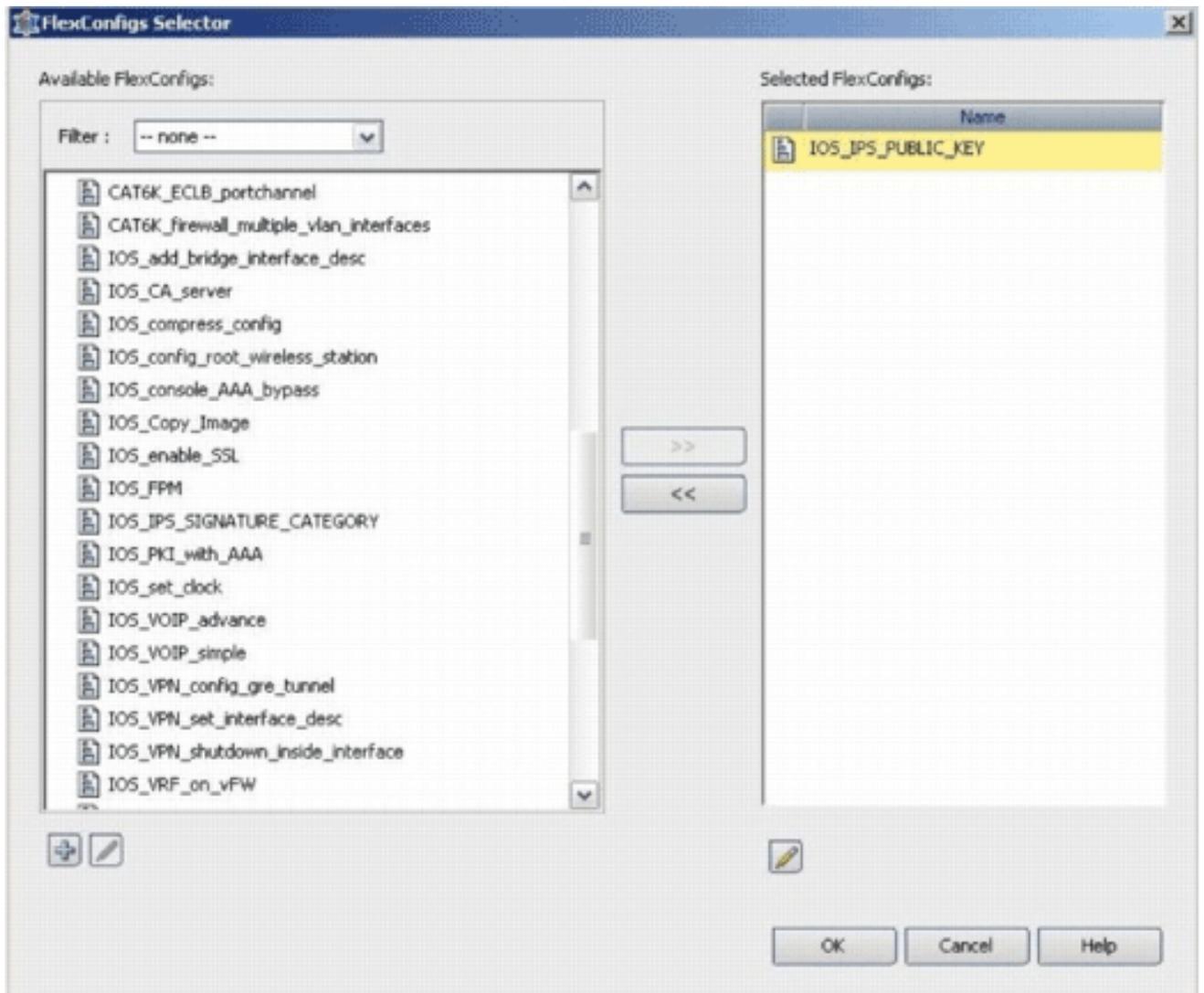


9. Dans le menu de gauche, accédez à l'écran de configuration FlexConfigs.

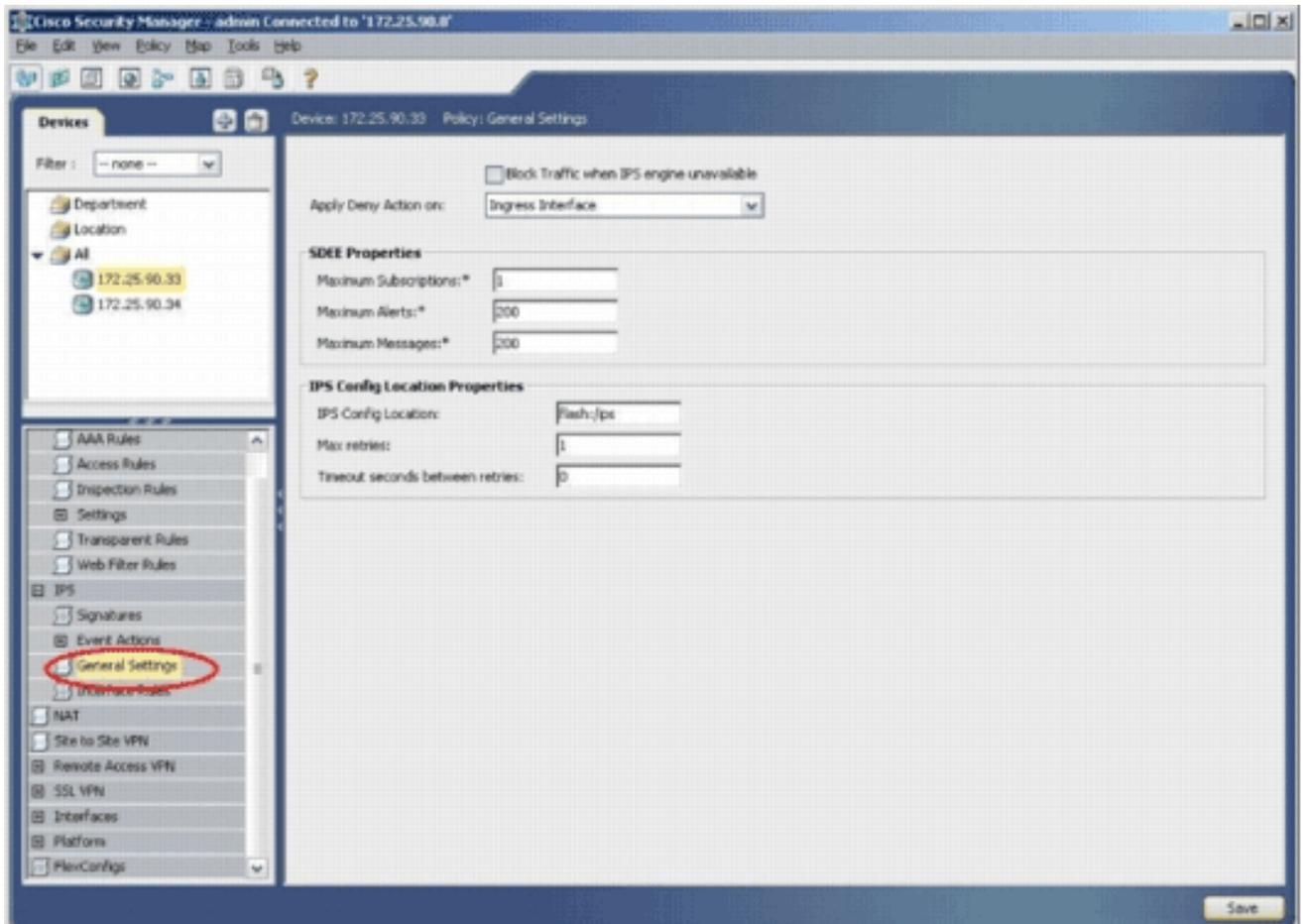
10. Cliquez sur l'interface utilisateur FlexConfigs située sur le côté droit de l'écran, puis cliquez sur l'icône **Ajouter**.



11. Dans la liste Configurations flexibles sélectionnées, sélectionnez `IOS_IPS_PUBLIC_KEY`, puis cliquez sur **OK**.

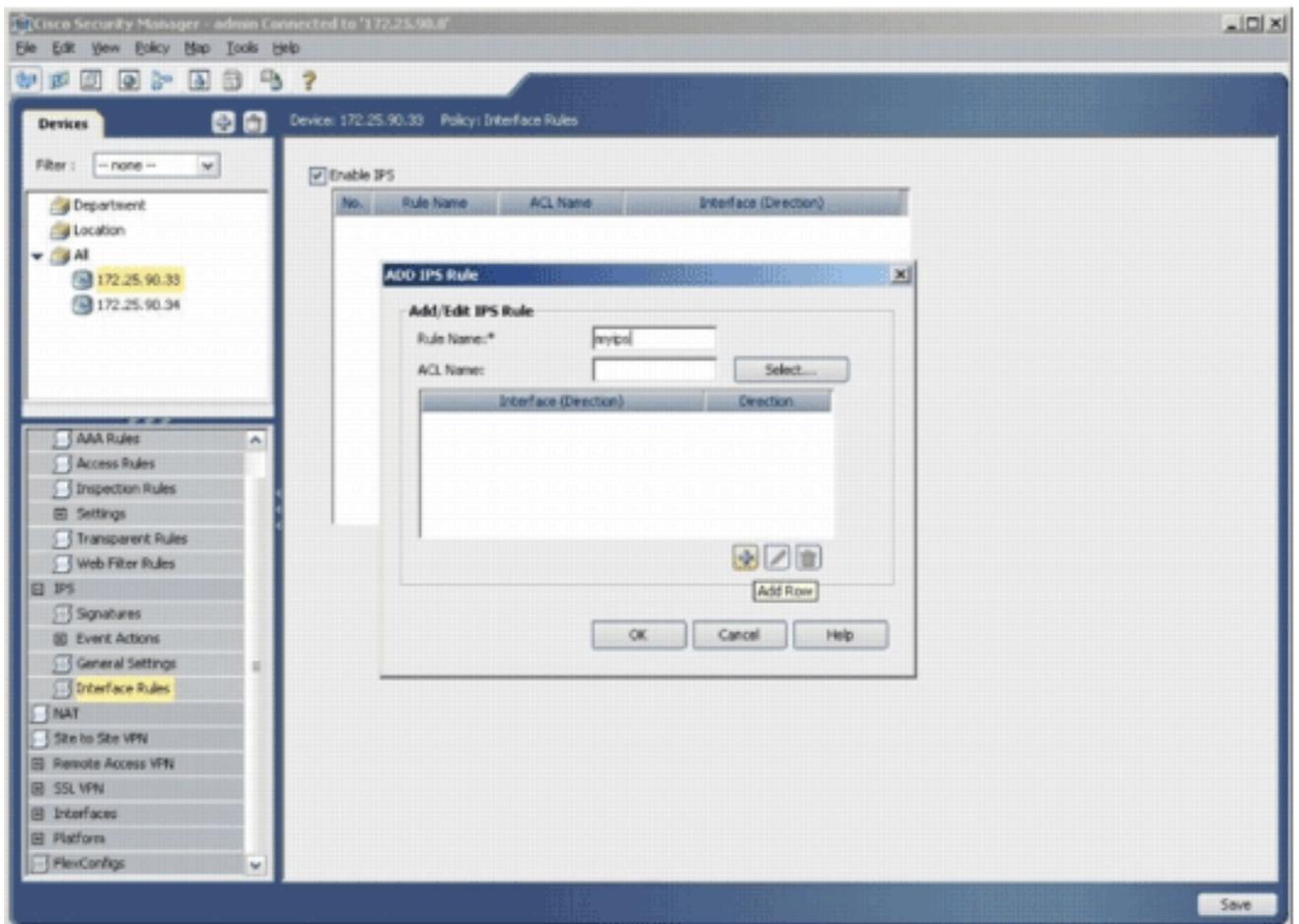


12. Cliquez sur **Enregistrer** afin d'enregistrer les modifications. **Remarque :**  
IOS\_IPS\_PUBLIC\_KEY FlexConfig contient la configuration de la clé publique.
13. Dans le menu de gauche, sélectionnez **General Settings** situé sous l'en-tête IPS.
14. Entrez l'emplacement de configuration IPS sur la mémoire Flash. Il s'agit de l'emplacement où sont placées les configurations IPS.
15. Cliquez sur **Enregistrer** afin d'enregistrer les modifications.

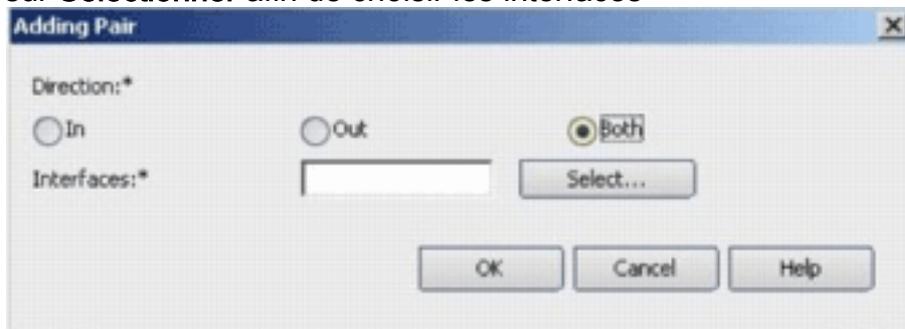


**Remarque :** Vérifiez que le répertoire d'emplacement a déjà été créé sur la mémoire Flash du routeur. Sinon, utilisez la commande `mkdir <nom_répertoire>` afin de créer le répertoire d'emplacement.

16. Afin d'activer IPS, accédez à Règles d'interface, cochez la case **Activer IPS**, puis cliquez sur **Ajouter une ligne**.
17. Dans la boîte de dialogue Ajouter une règle IPS, entrez un nom pour la règle IPS dans le champ Nom de la règle, puis cliquez sur **Ajouter une ligne** afin d'inclure les interfaces sur lesquelles IPS doit être appliqué.

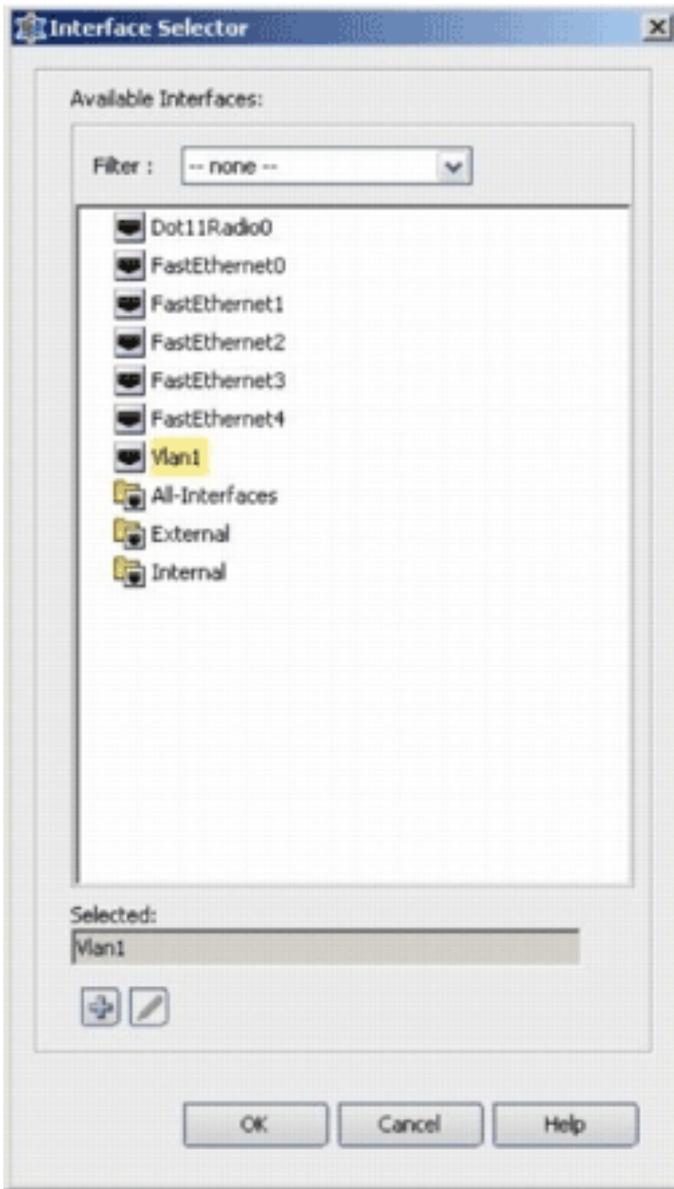


18. Activez la case d'option qui indique dans quelle direction la règle IPS doit être appliquée, puis cliquez sur **Sélectionner** afin de choisir les interfaces



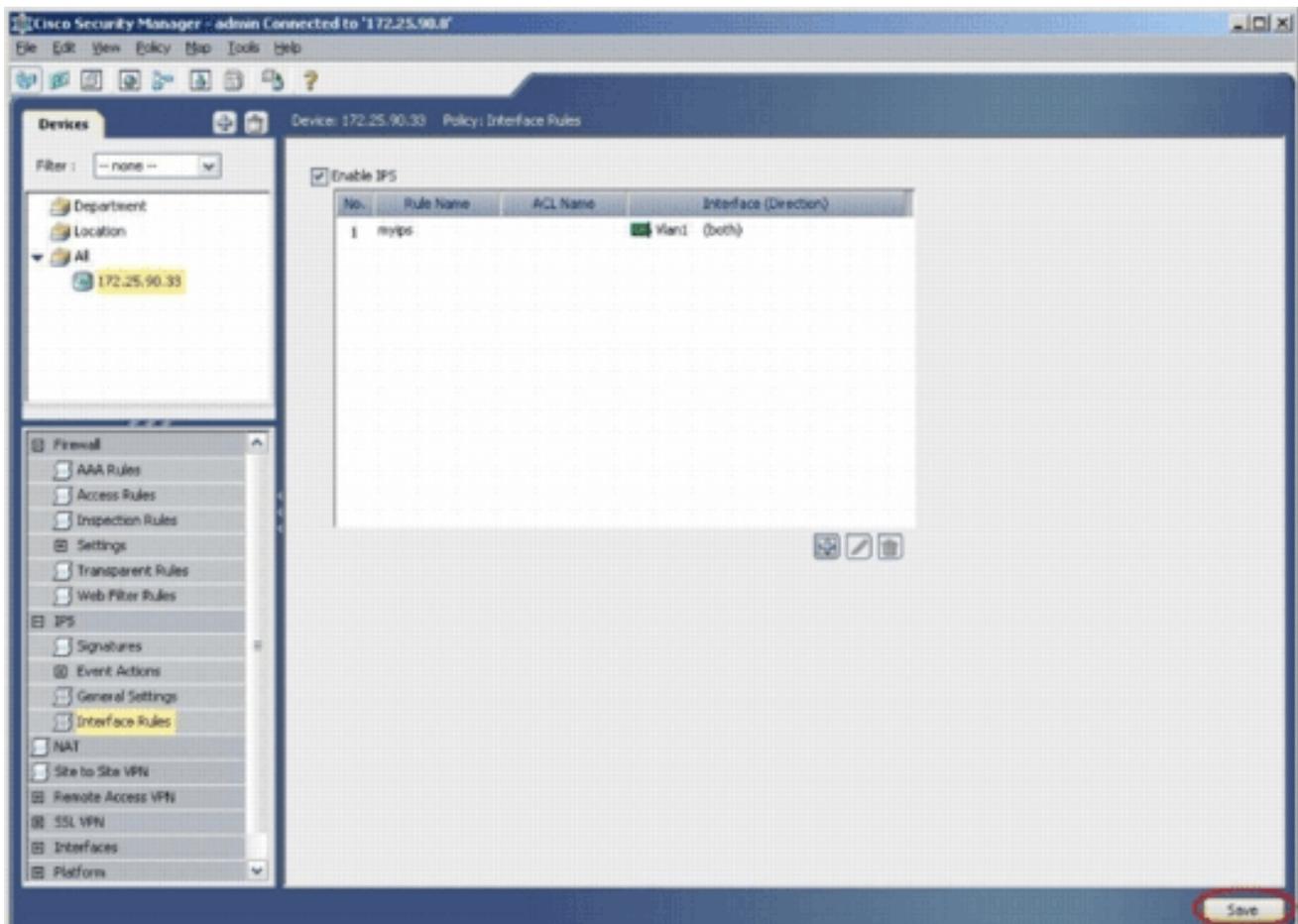
appropriées.

19. Choisissez une interface dans la liste Sélecteur d'interface, puis cliquez sur

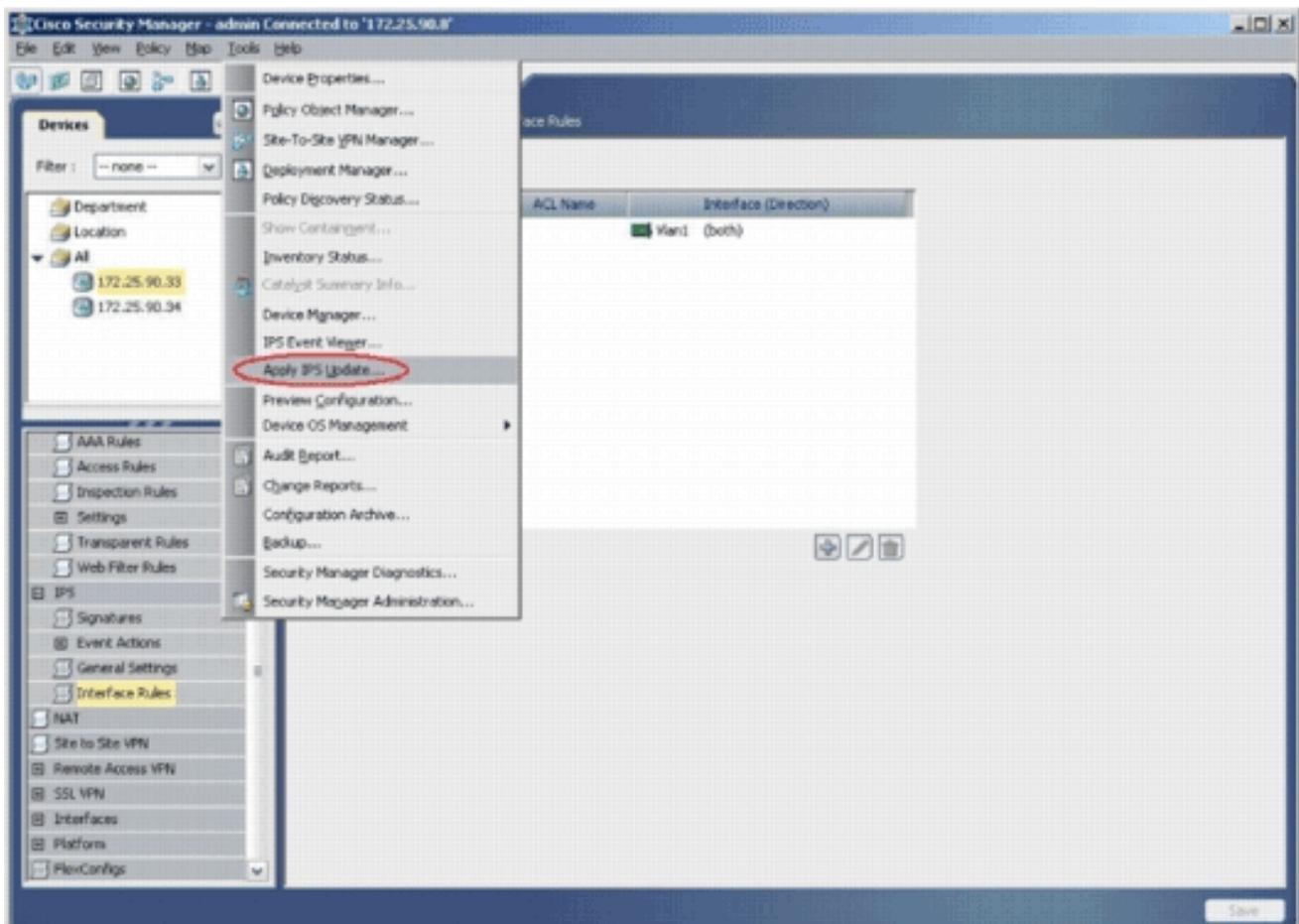


OK.

20. Cliquez sur **Enregistrer** afin d'enregistrer les modifications.

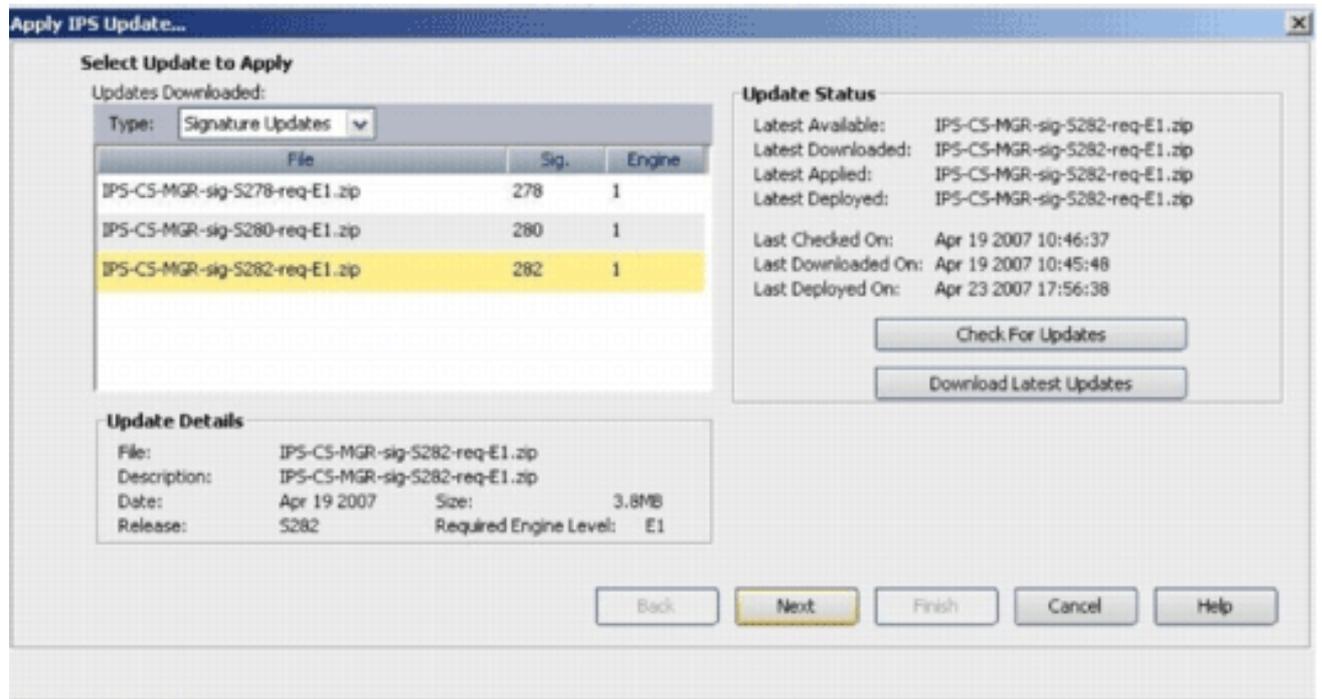


21. Choisissez **Tools > Apply IPS Update** afin d'installer les dernières signatures IPS.

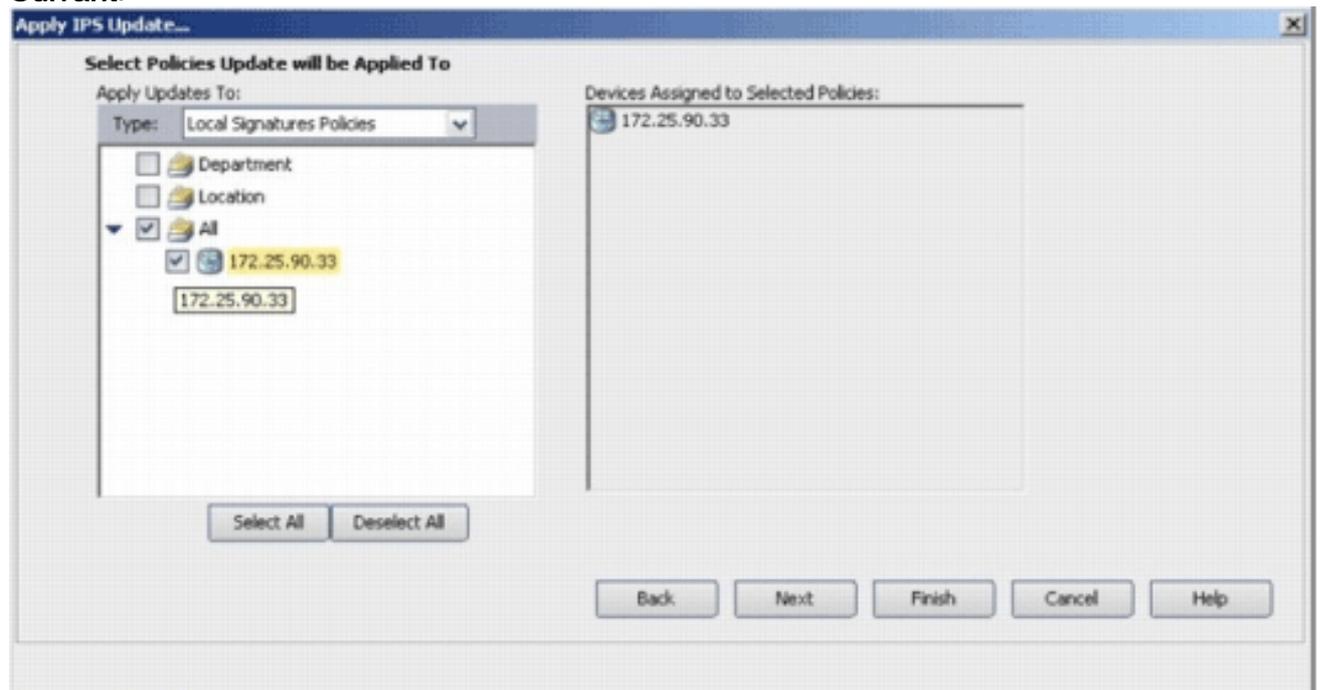


22. Choisissez le dernier fichier de signature, puis cliquez sur

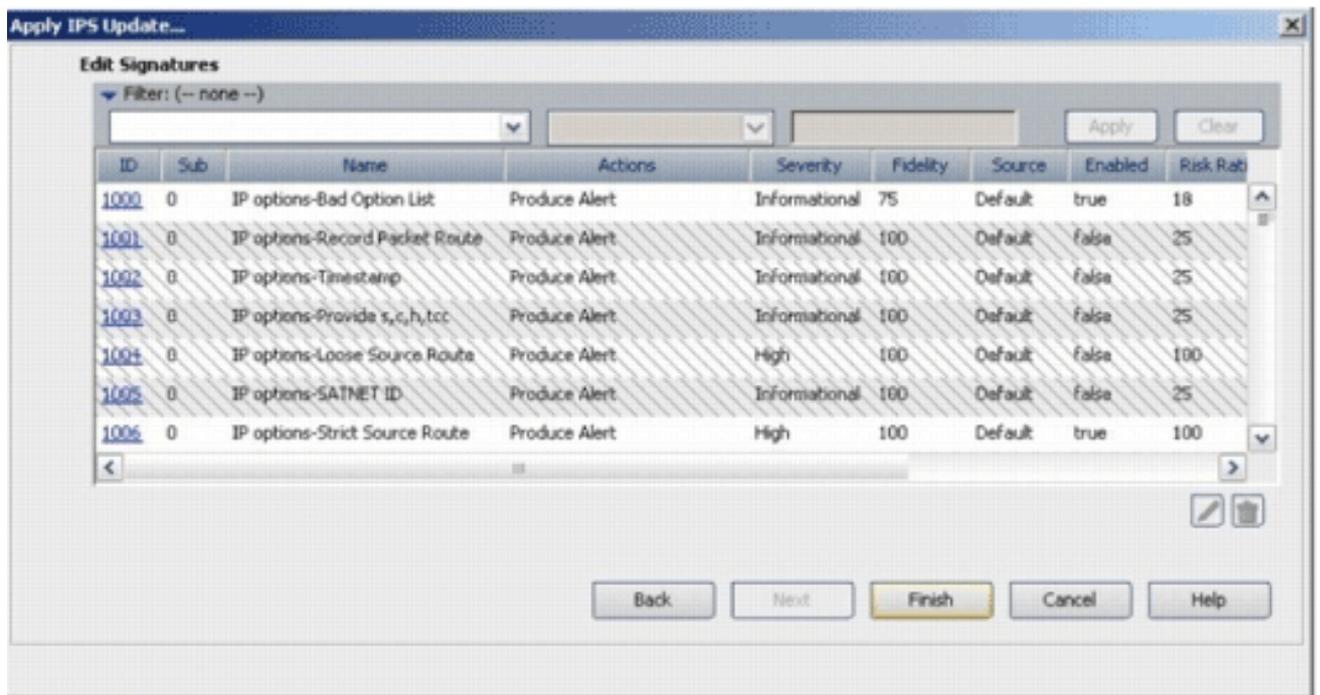
Suivant.



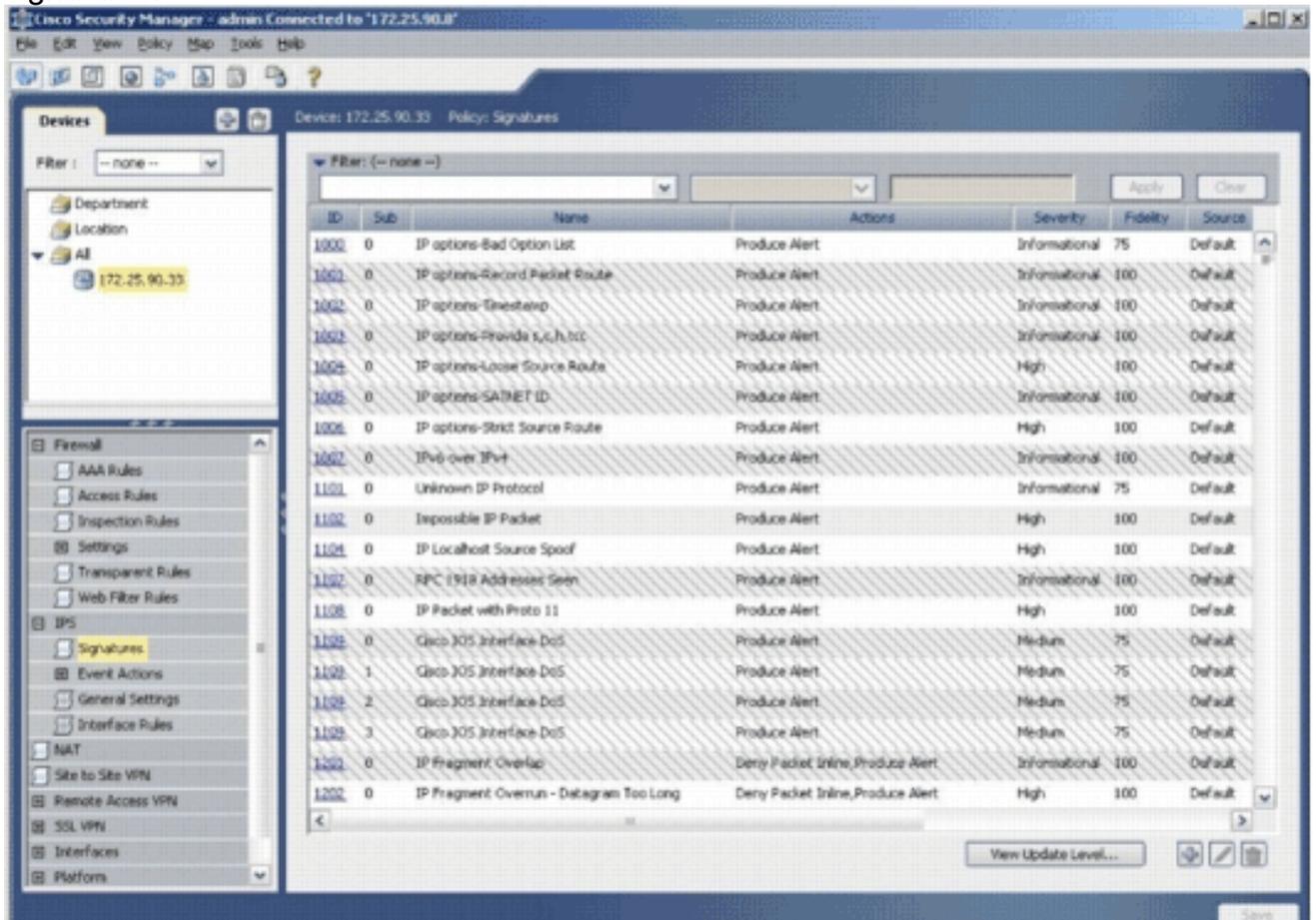
23. Choisissez les périphériques sur lesquels la mise à jour IPS doit être appliquée, puis cliquez sur **Suivant**.



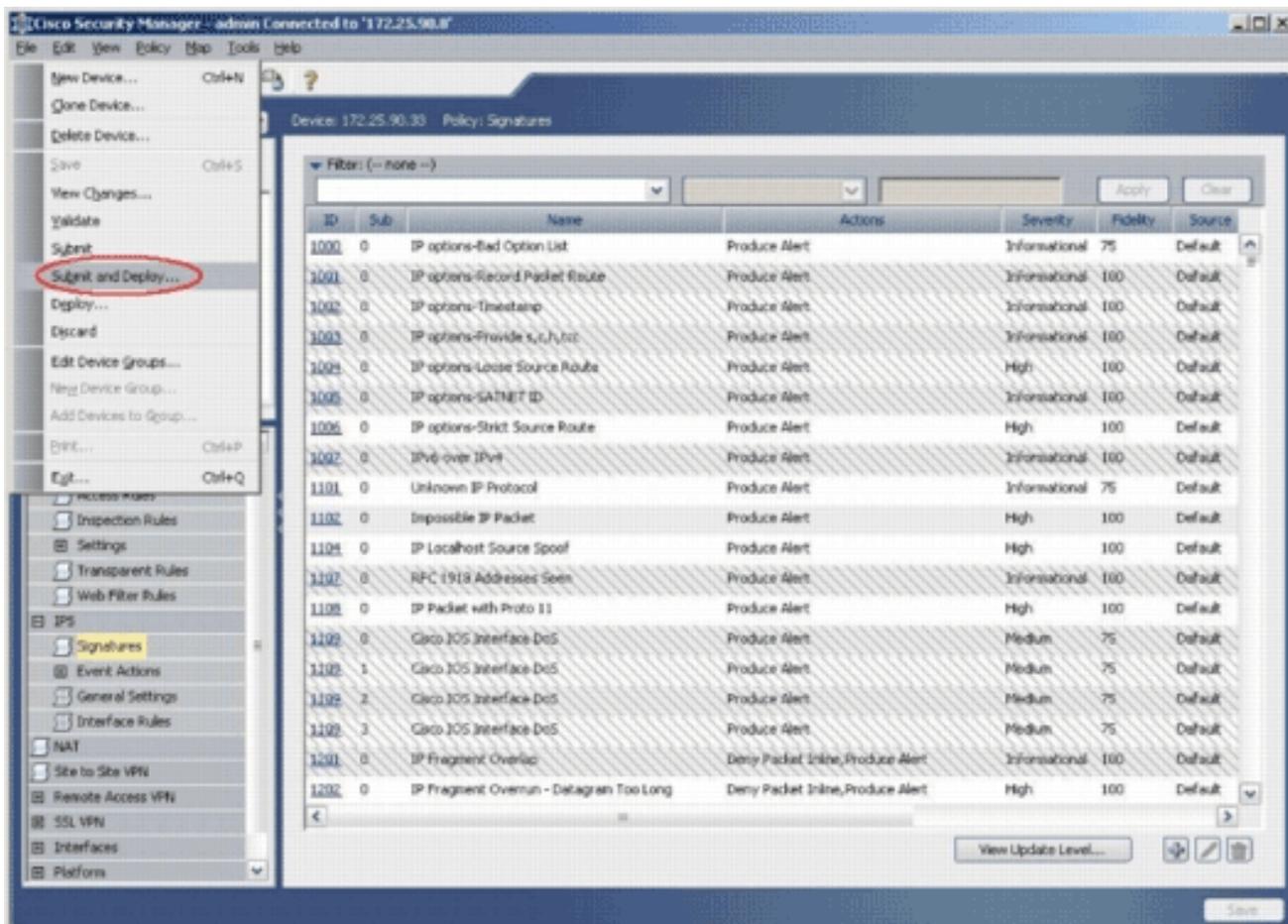
24. Cliquez sur **Terminer** afin d'appliquer les signatures.



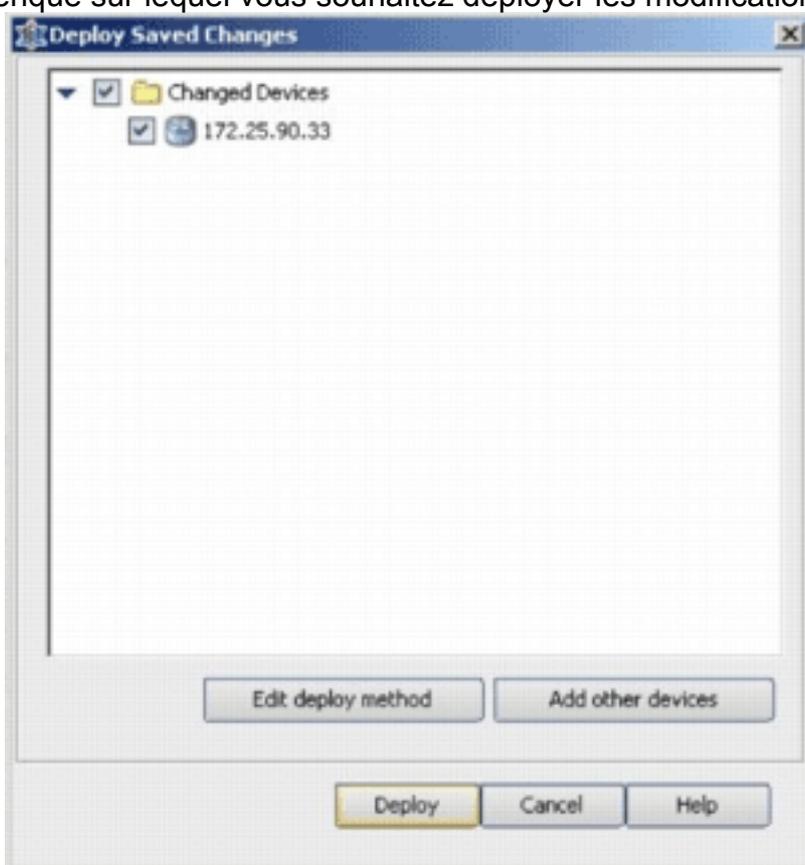
25. Accédez à IPS, puis sélectionnez **Signatures** afin d'afficher la liste de toutes les signatures.



26. Choisissez **File > Submit and Deploy** afin de déployer IPS sur le routeur IOS.

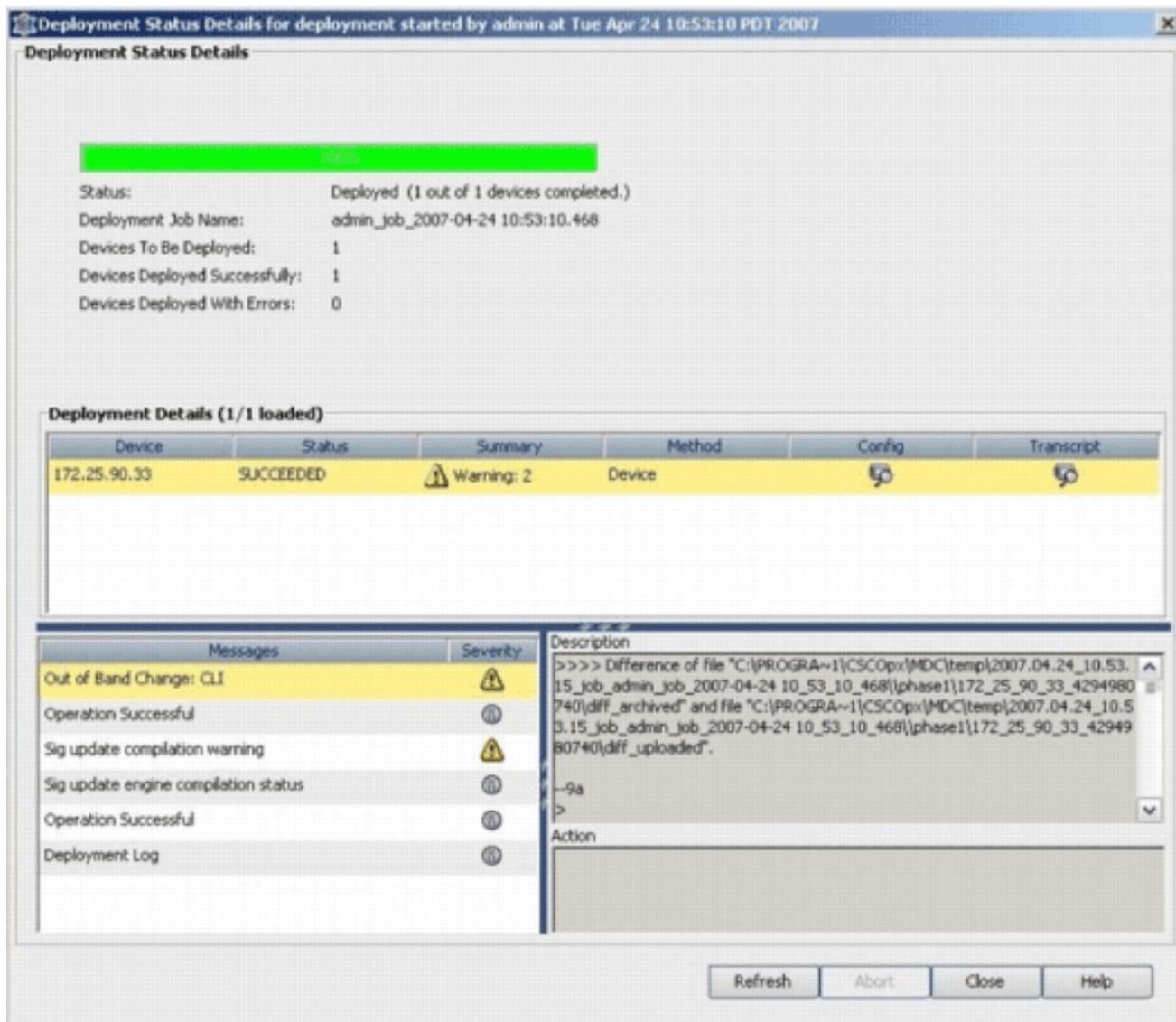


27. Choisissez le périphérique sur lequel vous souhaitez déployer les modifications, puis



cliquez sur **Déployer**.

28. Affichez l'état du déploiement afin de vérifier s'il y a des erreurs.



## Informations connexes

- [Page Produits et services de Cisco IOS Intrusion Prevention System \(IPS\)](#)
- [Mise en route de Cisco IOS IPS au format de signature 5.x](#)
- [Prise en charge du format de signature IPS 5.x et amélioration de l'utilisation](#)
- [Système de prévention des intrusions Cisco](#)
- [Avis de champs relatifs aux produits de sécurité \(y compris CiscoSecure Intrusion Detection\)](#)
- [Support technique - Cisco Systems](#)