

Configurer Cisco IOS IPS avec un routeur et SDM

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Informations connexes](#)

Introduction

Ce document décrit comment utiliser Cisco Router and Security Device Manager (SDM) version 2.5 afin de configurer Cisco IOS[®] Intrusion Prevention System (IPS) dans 12.4(15)T3 et versions ultérieures.

Les améliorations de SDM 2.5 liées à IOS IPS sont les suivantes :

- Nombre total de signatures compilées affichées dans l'interface utilisateur graphique de la liste des signatures
- fichiers de signature SDM (format de fichier zip ; par exemple, sigv5-SDM-S307.zip) et packages de signature CLI (format de fichier pkg ; par exemple, IOS-S313-CLI.pkg) peut être téléchargé ensemble en une seule opération
- Les packages de signatures téléchargés peuvent être automatiquement envoyés au routeur en option

Les tâches impliquées dans le processus d'approvisionnement initial sont les suivantes :

1. Téléchargez et installez SDM 2.5.
2. Utilisez SDM Auto Update afin de télécharger le package de signatures IOS IPS sur un PC local.
3. Lancez l'Assistant Stratégies IPS afin de configurer IOS IPS.
4. Vérifier que la configuration et les signatures IOS IPS sont correctement chargées

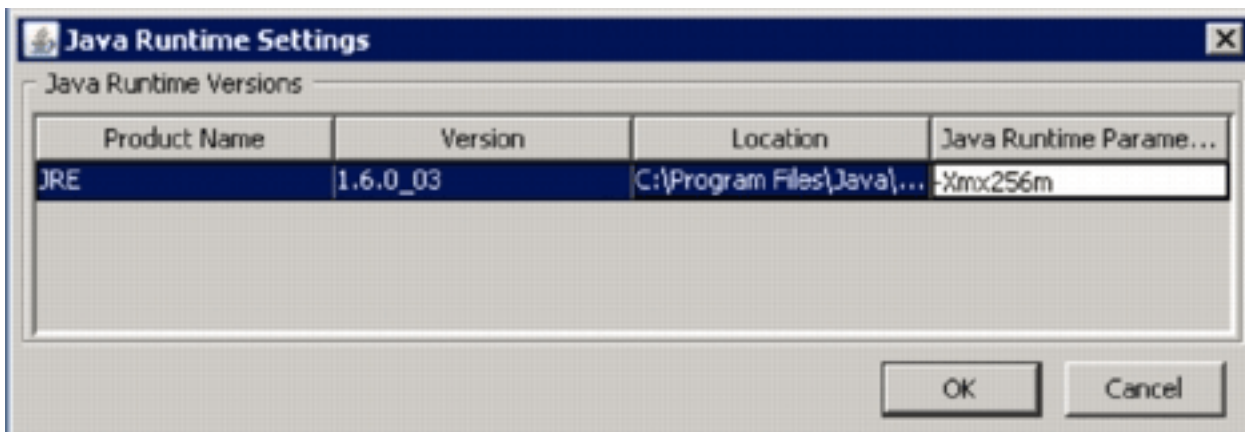
Cisco SDM est un outil de configuration Web qui simplifie la configuration des routeurs et de la sécurité grâce à des assistants intelligents qui aident les clients à déployer, configurer et surveiller rapidement et facilement un routeur Cisco sans avoir besoin de connaître l'interface de ligne de commande (CLI).

SDM version 2.5 peut être téléchargé à partir de Cisco.com à l'adresse <http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm> (clients [enregistrés](#) uniquement). La note de version est disponible à l'adresse

http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr.25.html

Remarque : Cisco SDM nécessite une résolution d'écran d'au moins 1 024 x 768.

Remarque : Cisco SDM nécessite que la taille du segment de mémoire Java ne soit pas inférieure à 256 Mo pour configurer IOS IPS. Afin de modifier la taille du segment de mémoire Java, ouvrez le panneau de configuration Java, cliquez sur l'onglet **Java**, cliquez sur **Affichage** situé sous les paramètres d'exécution de l'applet Java, puis entrez **-Xmx256m** dans la colonne Paramètres d'exécution Java.



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 IOS IPS dans 12.4(15)T3 et versions ultérieures
- Cisco Router and Security Device Manager (SDM) version 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

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

Configuration

Remarque : ouvrez une session console ou telnet sur le routeur (avec le paramètre « term monitor » activé) afin de surveiller les messages lorsque vous utilisez SDM pour provisionner IOS IPS.

1. Téléchargez SDM 2.5 depuis Cisco.com à l'adresse <http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm> (clients [enregistrés](#) uniquement) et installez-le sur un PC local.
2. Exécutez SDM 2.5 à partir du PC local.
3. Lorsque la boîte de dialogue Connexion IPS IOS apparaît, saisissez le même nom d'utilisateur et le même mot de passe que ceux utilisés pour l'authentification SDM sur le

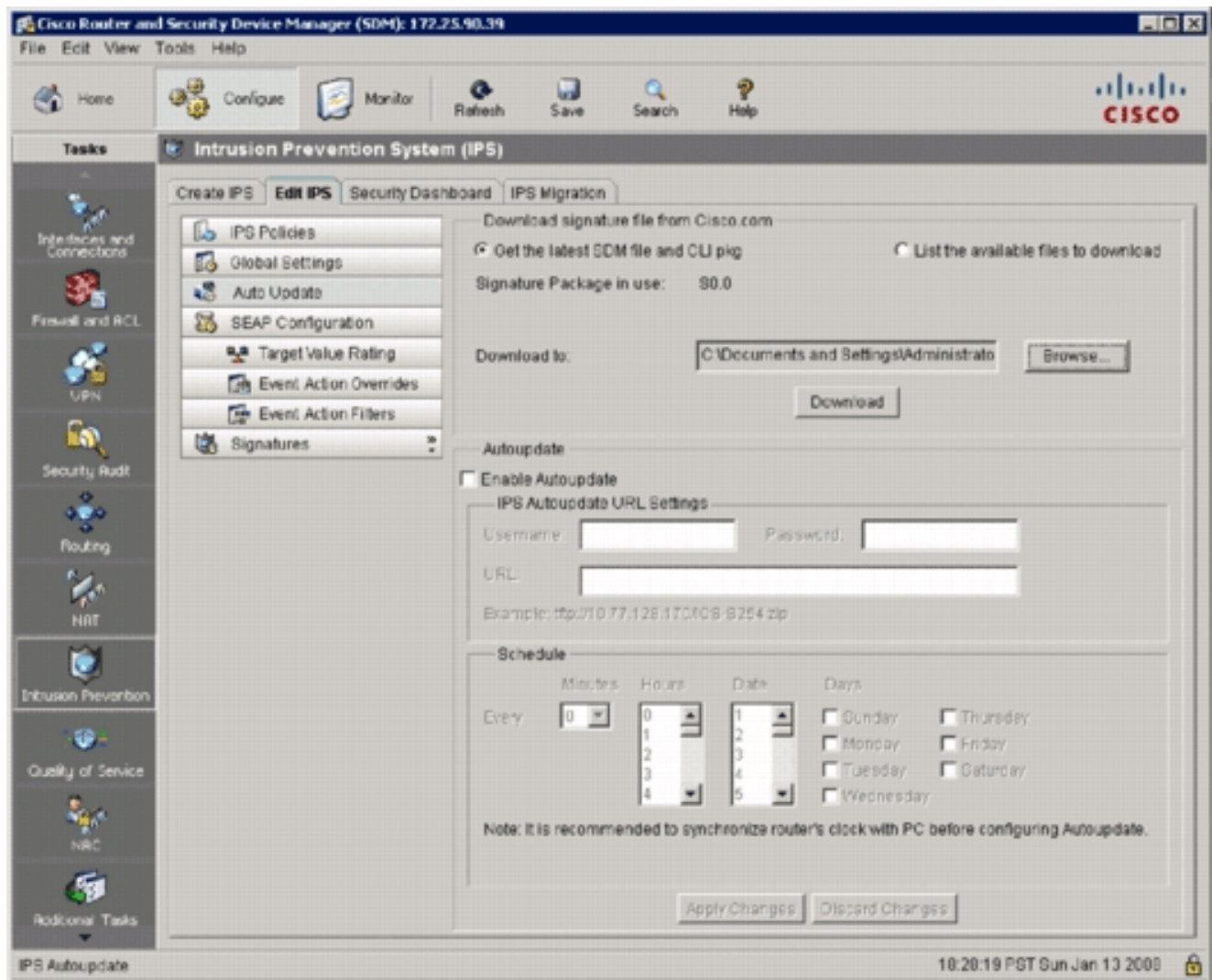


routeur.

4. Dans l'interface utilisateur SDM, cliquez sur **Configurer**, puis sur **Prévention des intrusions**.
5. Cliquez sur l'onglet **Modifier IPS**.
6. Si la notification SDEE n'est pas activée sur le routeur, cliquez sur **OK** afin d'activer la notification SDEE.



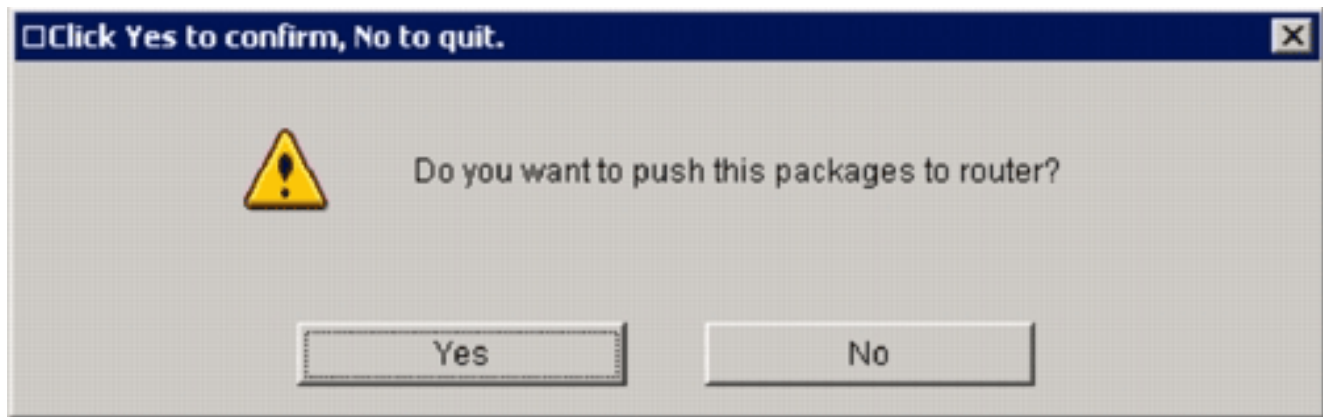
7. Dans la zone Download signature file from Cisco.com de l'onglet Edit IPS, cliquez sur la case d'option **Get the last SDM file and CLI pkg**, puis cliquez sur **Browse** afin de sélectionner un répertoire sur votre ordinateur local dans lequel enregistrer les fichiers téléchargés. Vous pouvez choisir le répertoire racine du serveur TFTP ou FTP, qui sera utilisé ultérieurement lors du déploiement du package de signatures sur le routeur.
8. Cliquez sur **Download**.



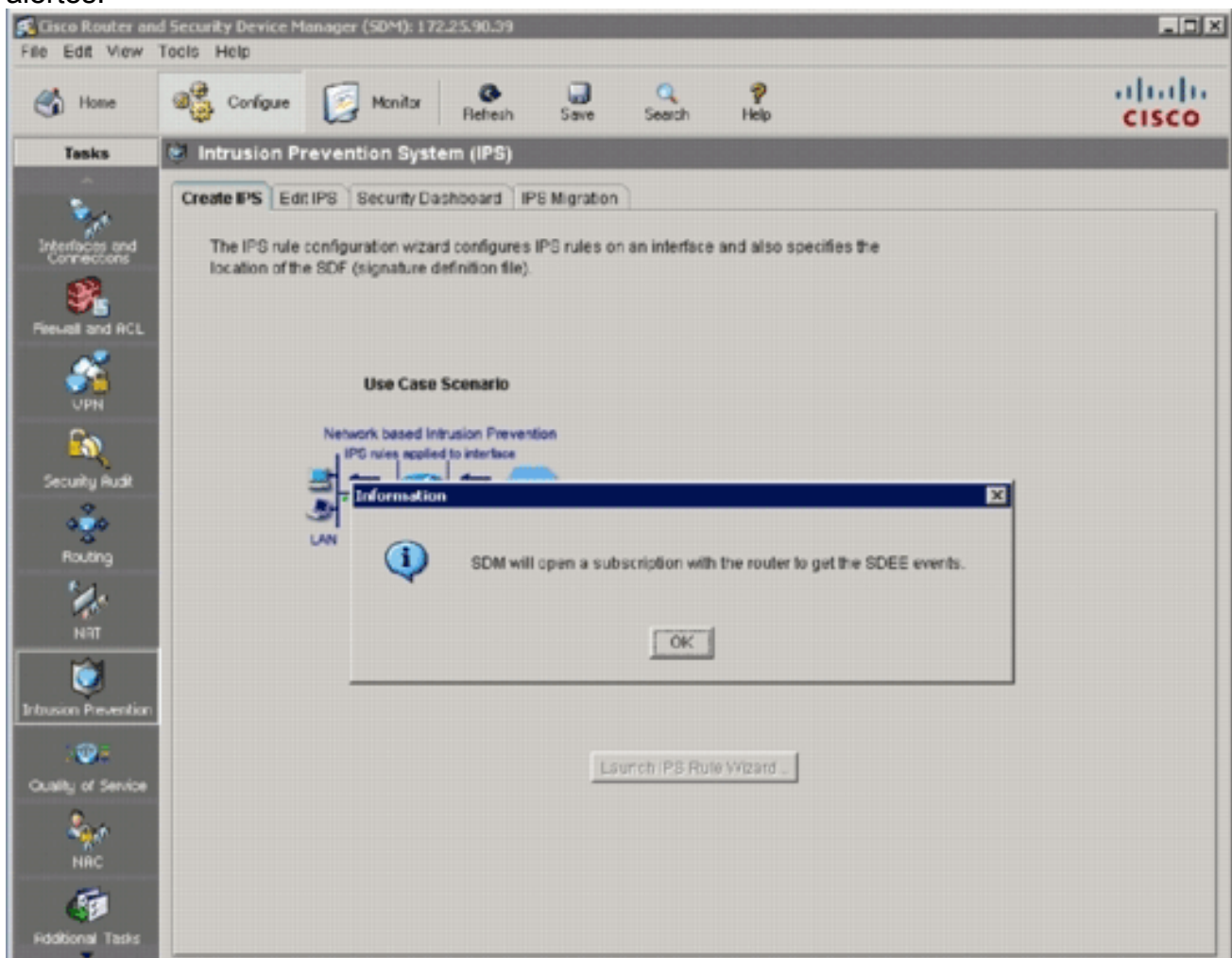
9. Lorsque la boîte de dialogue Connexion CCO apparaît, utilisez votre nom d'utilisateur et votre mot de passe CCO



enregistrés. SDM se connecte à Cisco.com et commence à télécharger le fichier SDM (par exemple, sigv5-SDM-S307.zip) et le fichier pkg CLI (par exemple, IOS-S313-CLI.pkg) dans le répertoire sélectionné à l'étape 7. Une fois les deux fichiers téléchargés, SDM vous invite à envoyer le package de signature téléchargé au routeur.



10. Cliquez sur **Non** car IOS IPS n'a pas encore été configuré sur le routeur.
11. Après avoir téléchargé le dernier package de signatures IOS CLI, cliquez sur l'onglet **Create IPS** afin de créer la configuration IOS IPS initiale.
12. Si vous êtes invité à appliquer des modifications au routeur, cliquez sur **Appliquer les modifications**.
13. Cliquez sur **Lancer l'Assistant Règle IPS**. Une boîte de dialogue apparaît pour vous informer que SDM doit établir un abonnement SDEE au routeur pour récupérer les alertes.



14. Click OK. La boîte de dialogue Authentication requise

Authentication Required [X]

Enter login details to access level_1 or view_access on /172.25.90.39:

User name:

Password:

Save this password in your password list

Authentication scheme: Integrated Windows

s'affiche.

15. Entrez le nom d'utilisateur et le mot de passe que vous avez utilisés pour l'authentification SDM sur le routeur, puis cliquez sur **OK**. La boîte de dialogue Assistant Stratégies IPS s'affiche.

IPS Policies Wizard [X]

IPS Wizard

Welcome to the IPS Policies Wizard

This wizard helps you to configure the IPS rules for an interface and to specify the location of the configuration and the signature file.

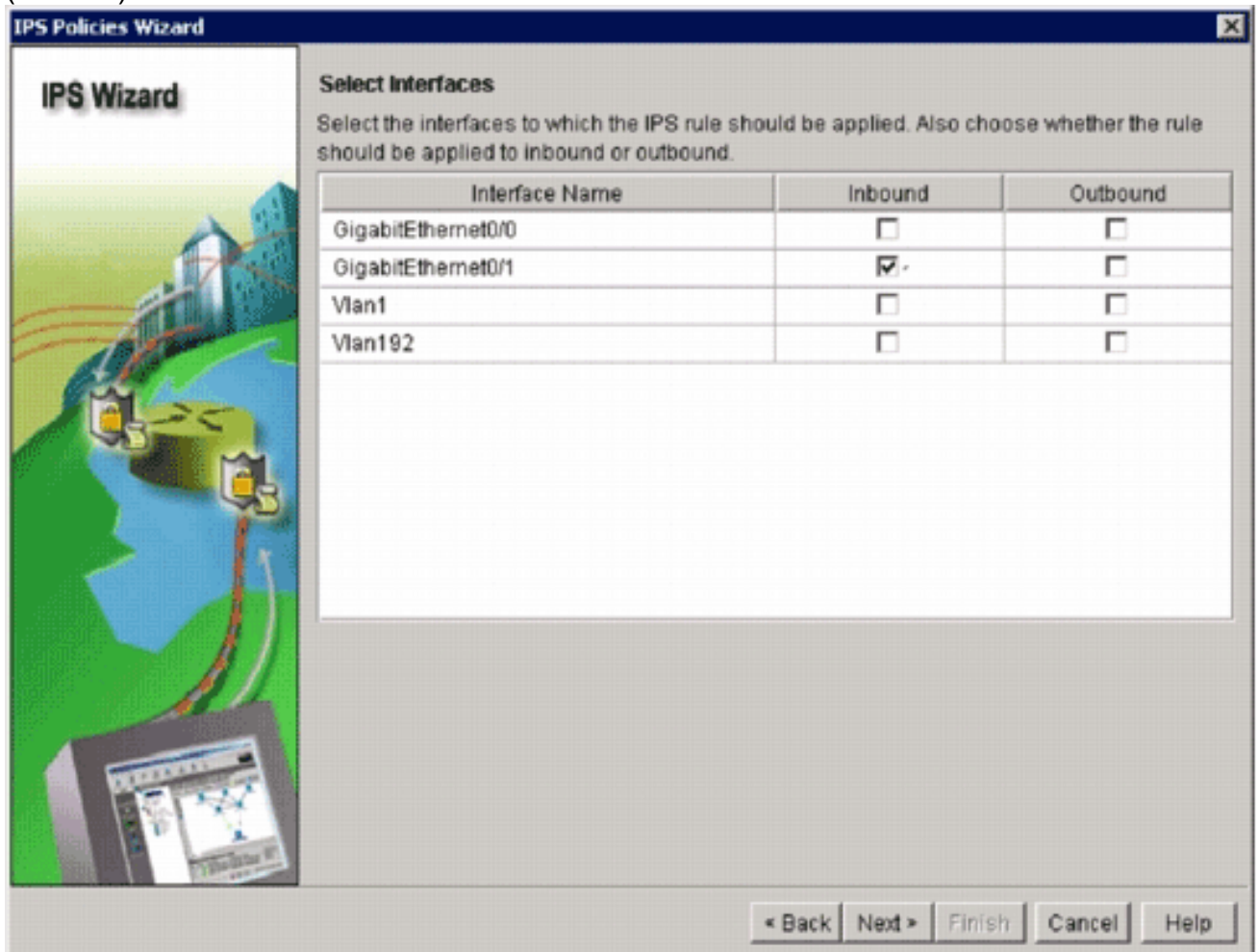
This wizard will assist you in configuring the following tasks:

- * Select the interface to apply the IPS rule.
- * Select the traffic flow direction that should be inspected by the IPS rules.
- * Specify the signature file and public key to be used by the router.
- * Specify the config location and select the category of signatures to be applied to the selected interfaces.

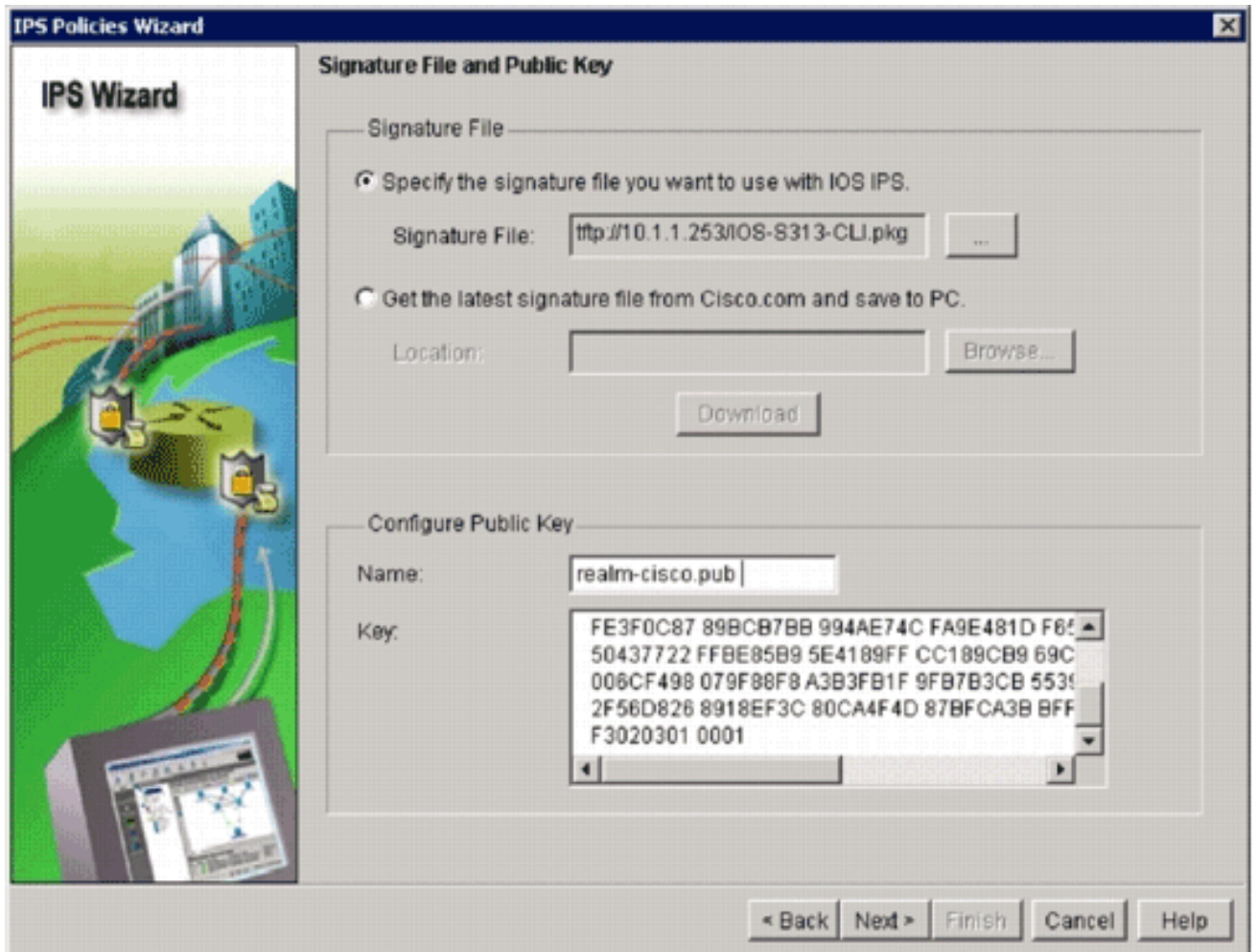
To continue, click Next.

< Back **Next >** Finish Cancel Help

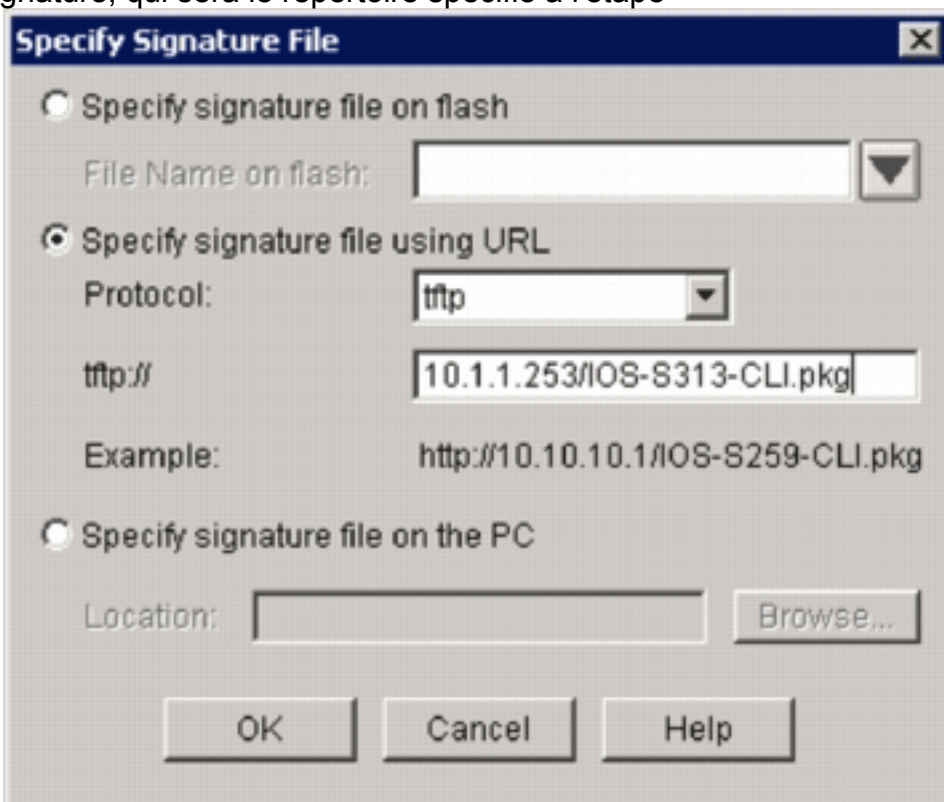
16. Cliquez sur **Next** (Suivant).



17. Dans la fenêtre Interfaces sélectionnées, sélectionnez l'interface et la direction dans laquelle IOS IPS sera appliqué, puis cliquez sur **Suivant** pour continuer.



18. Dans la zone Fichier de signature de la fenêtre Fichier de signature et clé publique, cliquez sur le bouton radio **Spécifier le fichier de signature à utiliser avec IOS IPS**, puis cliquez sur le bouton **Fichier de signature (...)** afin de spécifier l'emplacement du fichier de package de signature, qui sera le répertoire spécifié à l'étape



7.
19. Cliquez sur le bouton radio **Spécifier le fichier de signature à l'aide de l'URL**, puis

sélectionnez un protocole dans la liste déroulante Protocole. **Remarque** : cet exemple utilise TFTP afin de télécharger le package de signature sur le routeur.

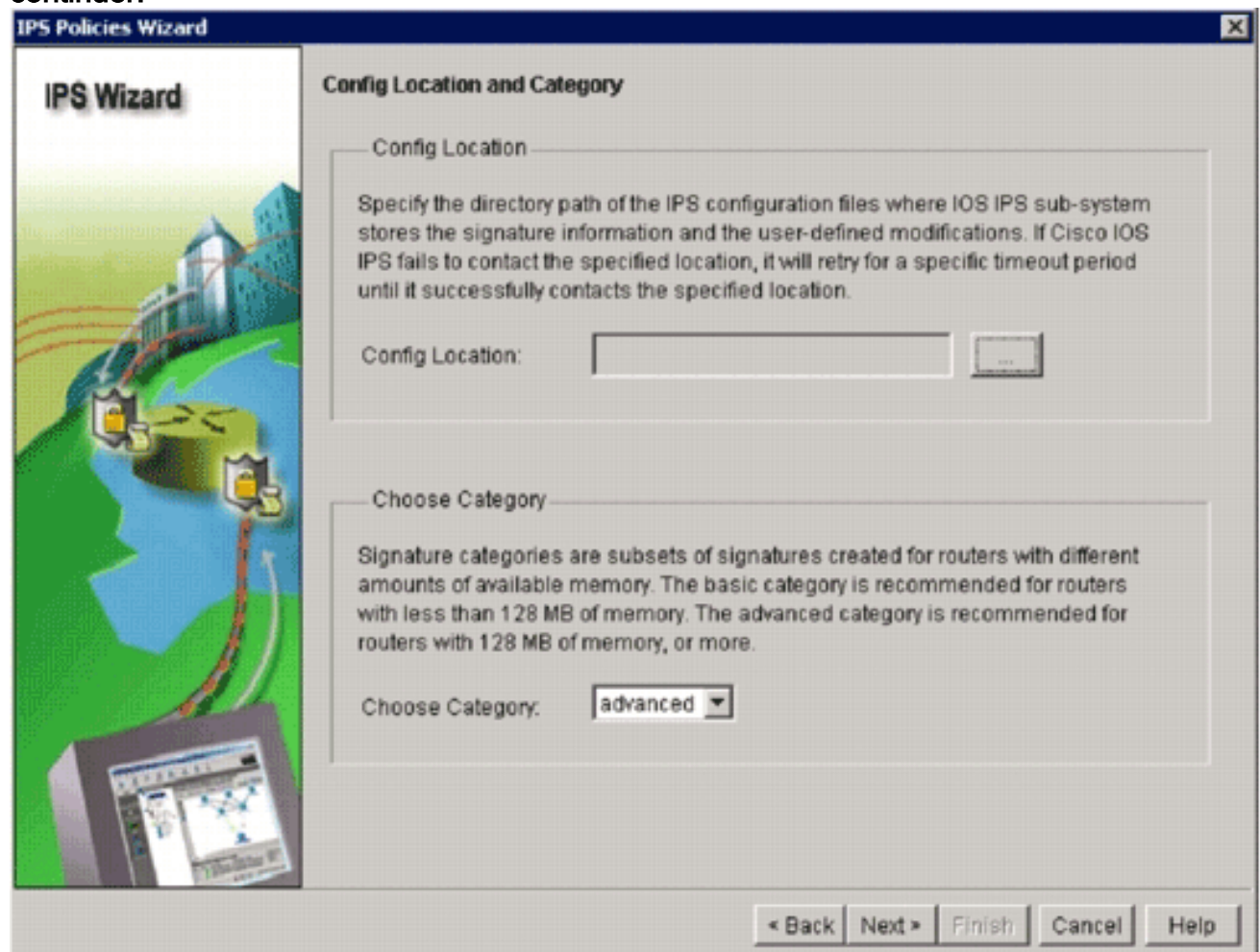
20. Entrez l'URL du fichier de signature, puis cliquez sur **OK**.

21. Dans la zone Configurer la clé publique de la fenêtre Fichier de signature et clé publique, saisissez **realm-cisco.pub** dans le champ Nom, puis copiez cette clé publique et collez-la dans le champ Clé.

```
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
```

Remarque : Cette clé publique peut être téléchargée sur Cisco.com à l'adresse suivante : <http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup> (clients [enregistrés](#) uniquement).

22. Cliquez sur **Next** pour continuer.



The screenshot shows the 'IPS Policies Wizard' window with the 'Config Location and Category' step. On the left is a graphic titled 'IPS Wizard' showing a network diagram with routers and a computer. The main area contains two sections:

- Config Location**: A text box with the instruction: "Specify the directory path of the IPS configuration files where IOS IPS sub-system stores the signature information and the user-defined modifications. If Cisco IOS IPS fails to contact the specified location, it will retry for a specific timeout period until it successfully contacts the specified location." Below this is a text input field labeled 'Config Location:' and a browse button.
- Choose Category**: A text box with the instruction: "Signature categories are subsets of signatures created for routers with different amounts of available memory. The basic category is recommended for routers with less than 128 MB of memory. The advanced category is recommended for routers with 128 MB of memory, or more." Below this is a dropdown menu labeled 'Choose Category:' with 'advanced' selected.

At the bottom of the window are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

23. Dans la fenêtre Emplacement et catégorie de configuration, cliquez sur le bouton **Emplacement de configuration (...)** afin de spécifier un emplacement où seront stockés les fichiers de définition et de configuration des signatures. La boîte de dialogue **Ajouter un emplacement de configuration**

Add Config Location

Specify the config location on this router.

Directory Name: ...

Specify the config location using URL.

Protocol:

http://

Example: http://10.10.10.1/ips5

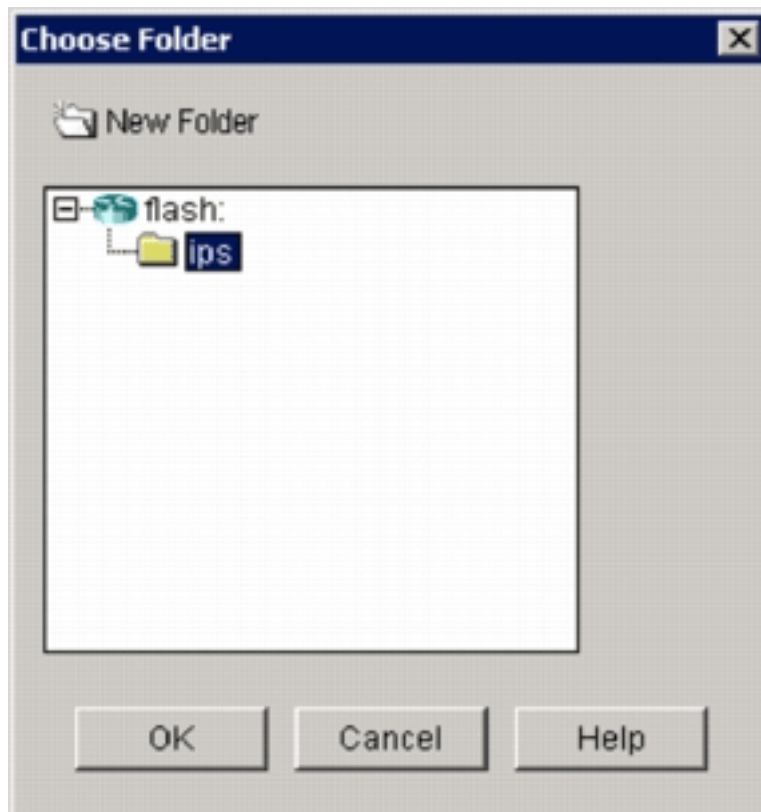
Number of Retries (1-5):

Timeout (1-10): (sec)

OK Cancel Help

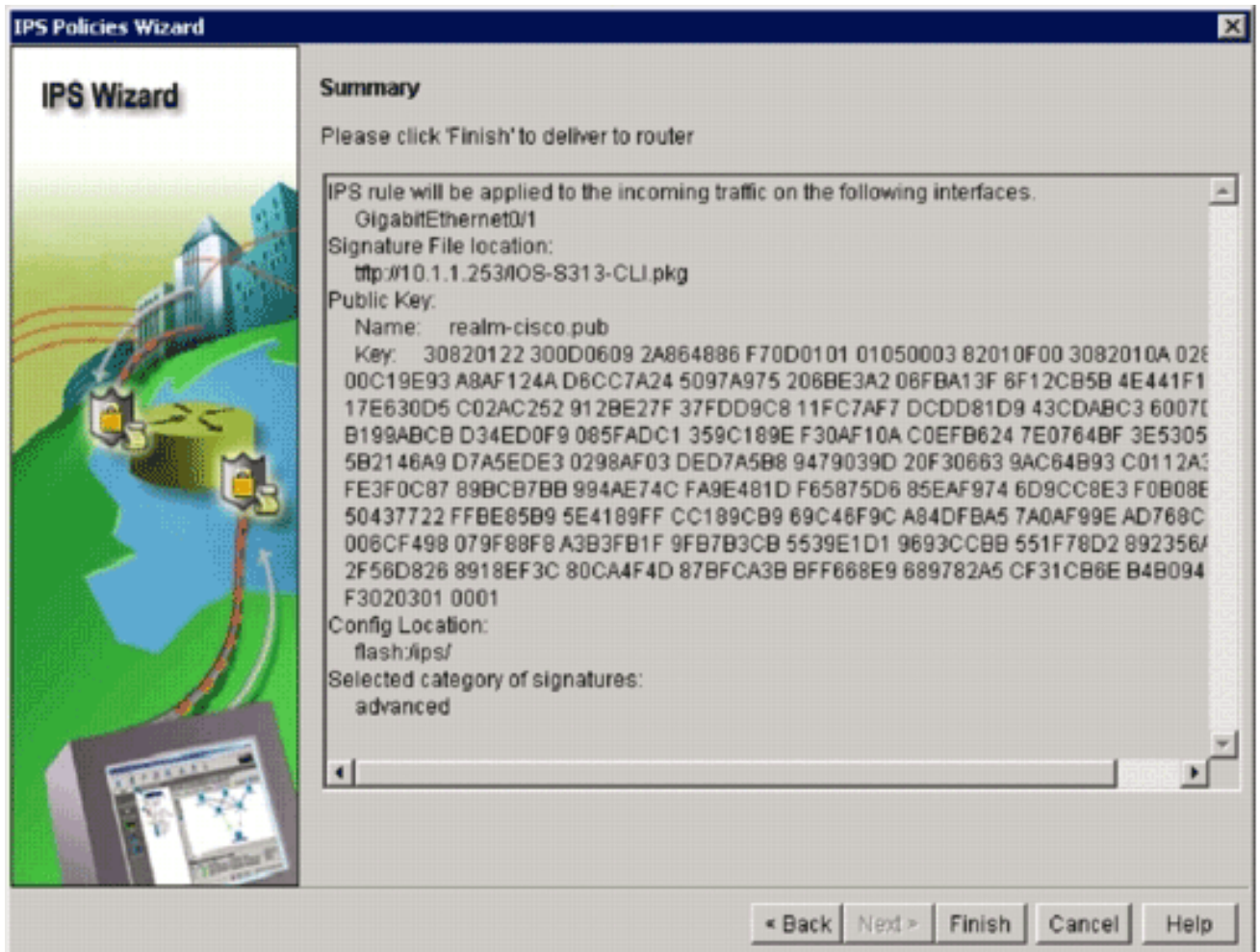
apparaît.

24. Dans la boîte de dialogue Ajouter un emplacement de configuration, cliquez sur le bouton radio **Spécifier l'emplacement de configuration sur ce routeur**, puis cliquez sur le bouton **Nom du répertoire (...)** afin de localiser le fichier de configuration. La boîte de dialogue Choisir un dossier apparaît afin de vous permettre de sélectionner un répertoire existant ou de créer un nouveau répertoire sur la mémoire Flash du routeur pour stocker les fichiers de définition et de configuration de

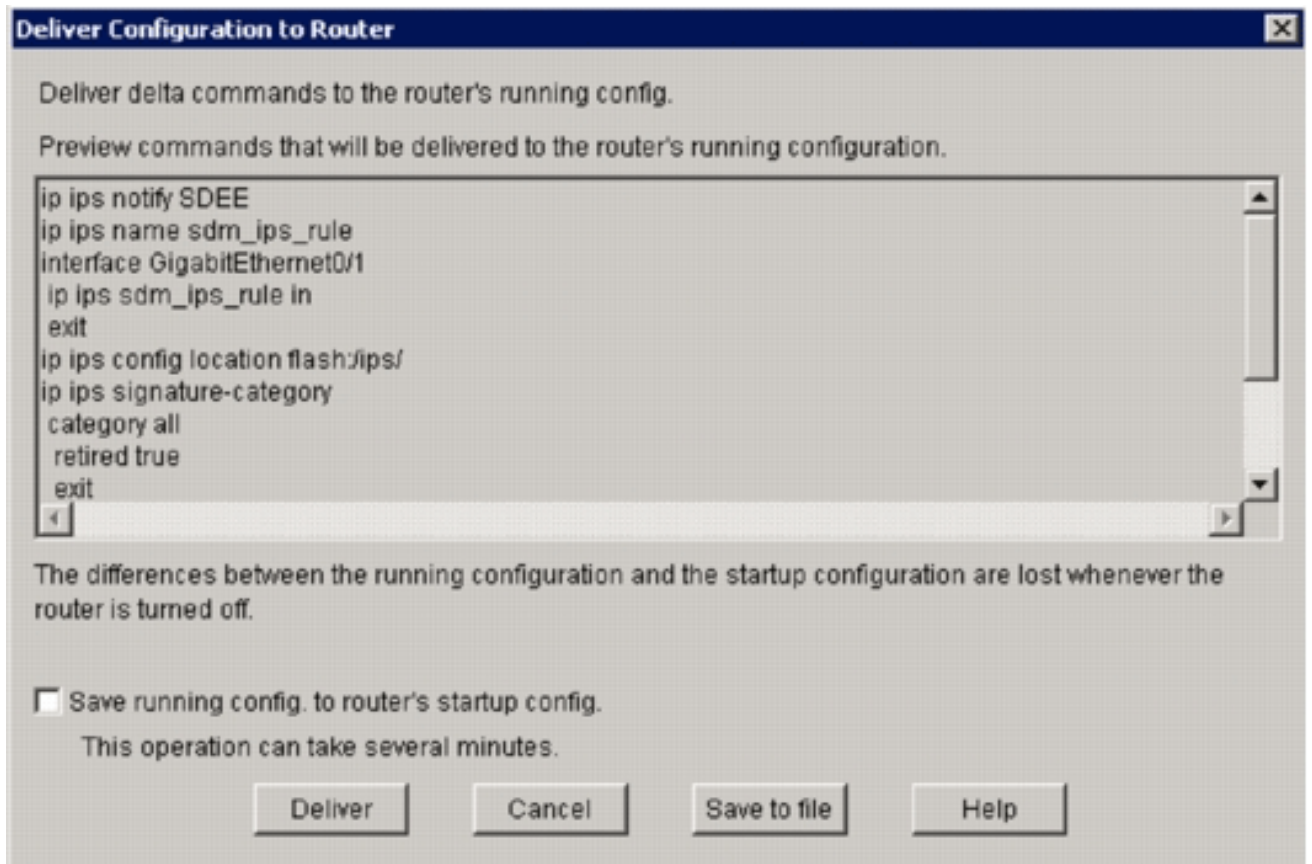


signature.

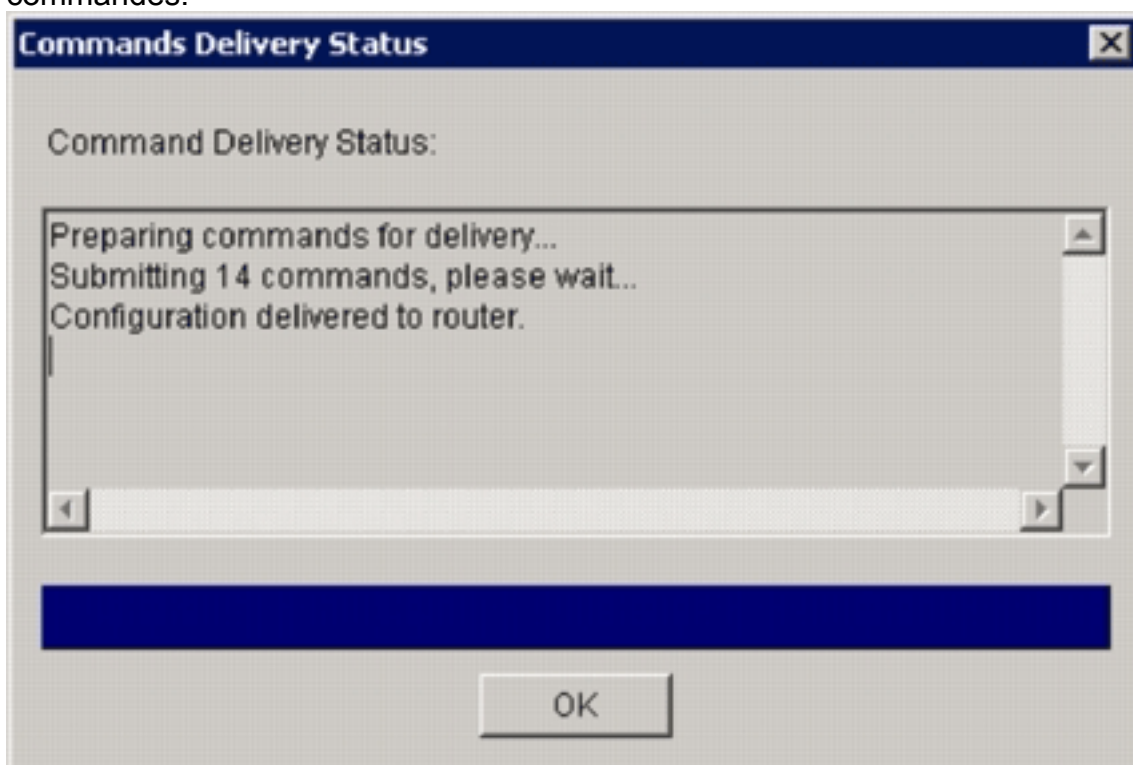
25. Cliquez sur **Nouveau dossier** situé en haut de la boîte de dialogue si vous souhaitez créer un nouveau répertoire.
26. Une fois que vous avez sélectionné le répertoire, cliquez sur **OK** afin d'appliquer les modifications, puis cliquez sur **OK** afin de fermer la boîte de dialogue Ajouter un emplacement de configuration.
27. Dans la boîte de dialogue Assistant Stratégies IPS, sélectionnez la catégorie de signature en fonction de la quantité de mémoire installée sur le routeur. Vous pouvez choisir deux catégories de signatures dans SDM : Basic et Advanced. Si le routeur dispose d'une mémoire DRAM de 128 Mo, Cisco vous recommande de choisir la catégorie Basic afin d'éviter les pannes d'allocation de mémoire. Si le routeur dispose d'une mémoire DRAM de 256 Mo ou plus, vous pouvez choisir l'une ou l'autre catégorie.
28. Une fois que vous avez sélectionné une catégorie à utiliser, cliquez sur **Suivant** afin de continuer à la page de résumé. La page de résumé fournit une brève description des tâches de configuration initiale de l'IPS IOS.



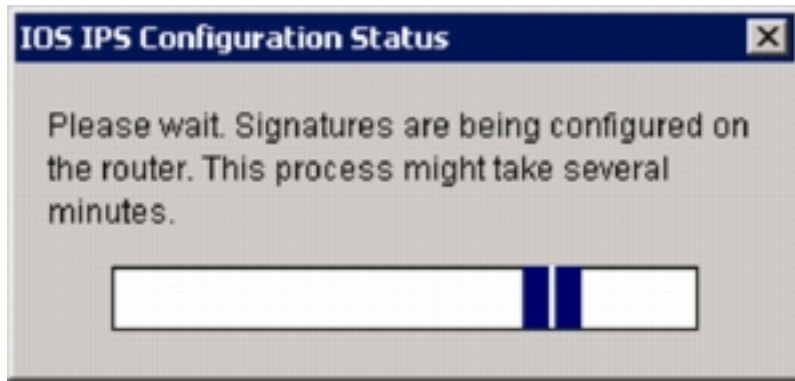
29. Cliquez sur **Terminer** sur la page de résumé afin de remettre les configurations et le package de signatures au routeur. Si l'option de commandes d'aperçu est activée sur les paramètres Préférences dans SDM, SDM affiche la boîte de dialogue Remettre la configuration au routeur qui affiche un résumé des commandes CLI que SDM livre au routeur.



30. Cliquez sur **Livrer** afin de continuer. La boîte de dialogue État de livraison des commandes apparaît pour afficher l'état de livraison des commandes.

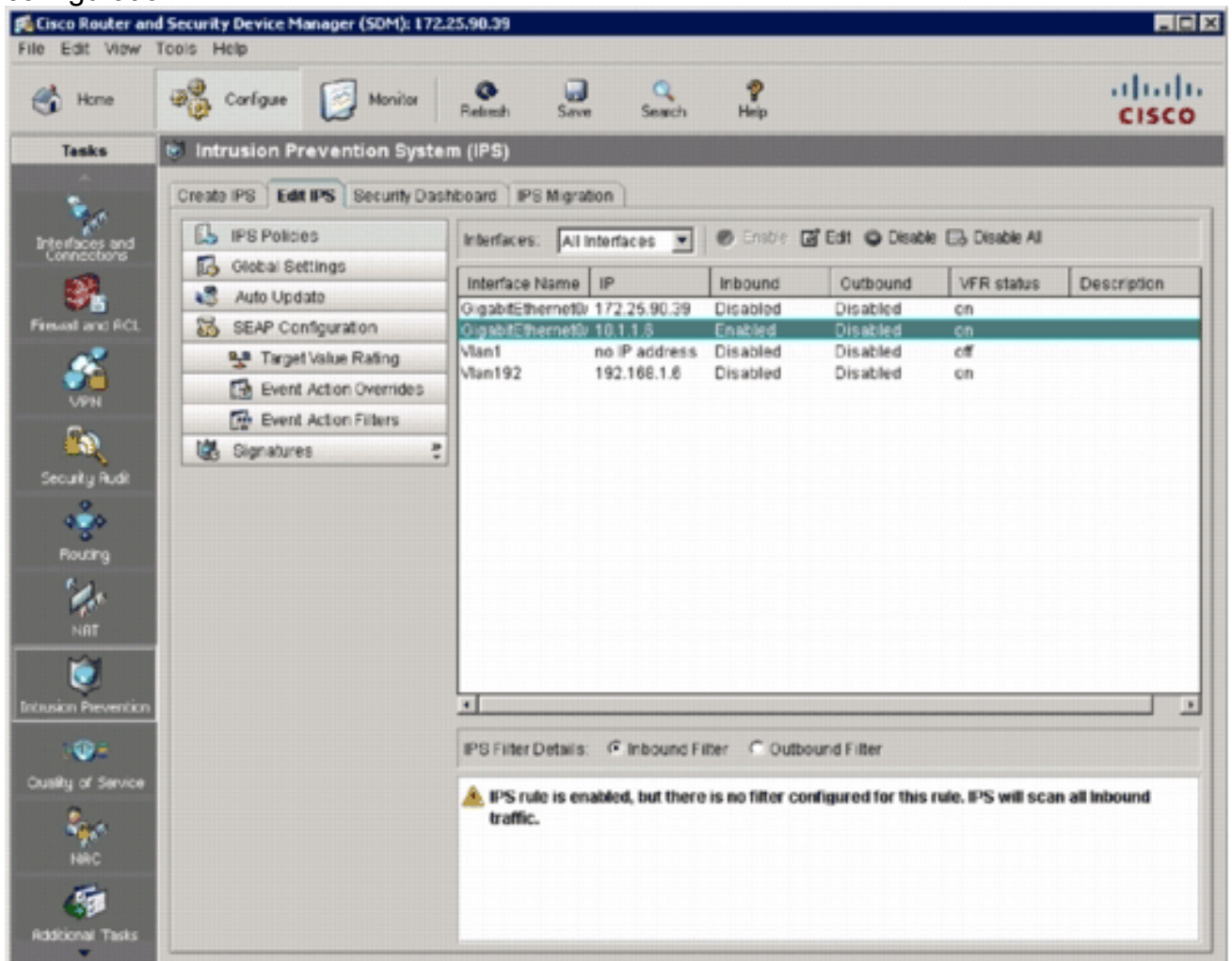


31. Lorsque les commandes sont transmises au routeur, cliquez sur **OK** pour continuer. La boîte de dialogue État de la configuration IOS IPS indique que les signatures sont en cours de



chargement sur le routeur.

32. Lorsque les signatures sont chargées, SDM affiche l'onglet **Edit IPS** avec la configuration actuelle. Vérifiez quelle interface et dans quelle direction l'IPS IOS est activé afin de vérifier la configuration.



La console du routeur indique que les signatures ont été chargées.

```
172.25.90.30 - TTY
ied
*Jan 13 16:41:08 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:41:08 PST Jan 13 2008
*Jan 13 16:41:08 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of 13 engines
*Jan 13 16:41:08 PST: %IPS-6-ENGINE_READY: multi-string - build time 8 ms - packets for this engine
will be scanned
*Jan 13 16:41:00 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures - 2 of 13 engines
*Jan 13 16:41:33 PST: %IPS-6-ENGINE_READY: service-http - build time 24892 ms - packets for this engine
will be scanned
*Jan 13 16:41:33 PST: %IPS-6-ENGINE_BUILDING: string-tcp - 961 signatures - 3 of 13 engines
*Jan 13 16:42:32 PST: %IPS-6-ENGINE_READY: string-tcp - build time 59424 ms - packets for this engine
will be scanned
*Jan 13 16:42:32 PST: %IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines
*Jan 13 16:42:33 PST: %IPS-6-ENGINE_READY: string-udp - build time 948 ms - packets for this engine
will be scanned
*Jan 13 16:42:33 PST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Jan 13 16:42:33 PST: %IPS-6-ENGINE_READY: state - build time 104 ms - packets for this engine will
be scanned
*Jan 13 16:42:33 PST: %IPS-6-ENGINE_BUILDING: atomic-ip - 275 signatures - 6 of 13 engines
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: atomic-ip - build time 572 ms - packets for this engine w
ill be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: string-icmp - build time 32 ms - packets for this engine
will be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-rpc - build time 200 ms - packets for this engine
will be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13 engines
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-dns - build time 36 ms - packets for this engine
will be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for this engine w
ill be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures - 12 of 13 engine
s
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms - packets for thi
s engine will be scanned
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 26 signatures - 13 of 13 engines
*Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 36 ms - packets for this engine
e will be scanned
*Jan 13 16:42:34 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 86304 ms
```

33. Utilisez la commande `show ip ips signatures count` afin de vérifier que les signatures sont chargées correctement.

```
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
```

La mise en service initiale d'IOS IPS à l'aide de SDM 2.5 est terminée.

34. Vérifiez les numéros de signature avec SDM comme illustré dans cette image.

Cisco Router and Security Device Manager (SDM): 172.25.90.39

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

CISCO

Tasks

Intrusion Prevention System (IPS)

Create IPS Edit IPS Security Dashboard IPS Migration

IPS Policies
Global Settings
Auto Update
SEAP Configuration
Target Value Rating
Event Action Overrides
Event Action Filters
Signatures

OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases

Import View by: All Signatures Criteria: --N/A-- Total[2158] Configured[588]

Select All Add Edit Enable Disable Pause Refresh

Enabled	I	Sig ID	SubSig ID	Name	Action	Severity	Fidelity %
+		9423	1	Back Door Psychward	produce-aler	high	85
+		9423	0	Back Door Psychward	produce-aler	high	100
+		5343	0	Apache Host Header Cross Site	produce-aler	high	100
+		3122	0	SMTP EXN root Recon	produce-aler	low	85
+		5099	0	MSN Messenger Webcam Buffer	produce-aler	high	80
+		5537	0	ICQ Client DNS Request	produce-aler	informational	100
+		3316	0	Project DOS	produce-aler	high	75
+		11003	0	Gtella File Request	produce-aler	low	100
+		5196	1	Red Hat Stronghold Recon at	produce-aler	low	100
+		5196	0	Red Hat Stronghold Recon at	produce-aler	low	100
+		5773	1	Simple PHP Blog Unauthorized F	produce-aler	low	70
+		5773	0	Simple PHP Blog Unauthorized F	produce-aler	low	85
+		5411	0	Linksys Hits DoS	produce-aler	high	85
+		12019	0	SideFind Activity	produce-aler	low	85
+		5070	0	VWAV inspace dl Access	produce-aler	medium	100
+		3169	0	FTP SITE EXEC tw	produce-aler	high	85
+		5605	0	Windows Account Locked	produce-aler	informational	85

Apply Changes Discard Changes

IPS Signatures 16:53:02 PST Sun Jan 13 2008

Informations connexes

- [Cisco IOS IPS sur Cisco.com](#)
- [Package de signatures Cisco IOS IPS](#)
- [Fichiers de signature Cisco IOS IPS pour SDM](#)
- [Mise en route de Cisco IOS IPS au format de signature 5.x](#)
- [Guide de configuration de Cisco IOS IPS](#)
- [Observateur d'événements Cisco IDS](#)
- [Support et documentation techniques - Cisco Systems](#)