Exemple de configuration de Router and Security Device Manager dans le système de prévention des intrusions Cisco IOS

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Configurez](#)
[Informations connexes](#)

Introduction

Ce document décrit comment employer la version 2.5 du Cisco Router and Security Device Manager (SDM) afin de configurer le Système de prévention d'intrusion (IPS) de Cisco IOS® dans 12.4(15)T3 et des versions ultérieures.

Les améliorations dans SDM 2.5 connexe à l'IOS IPS sont :

- Montez-vous au numéro affiché compilé de signature dans le GUI de liste de signature
- Fichiers de signatures SDM (format de fichier zip ; par exemple, sigv5-SDM-S307.zip) et modules de signature CLI (format de fichier de package ; par exemple, IOS-S313-CLI.pkg) peut être téléchargé ensemble dans une exécution
- Des modules téléchargés de signature peuvent être poussés automatiquement au routeur comme option

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

1. Téléchargez et installez SDM 2.5.
2. Employez la mise à jour automatique SDM afin de télécharger le module de signature d'IOS IPS à un ordinateur local.
3. Lancez l'assistant de stratégies IPS afin de configurer l'IOS IPS.
4. Vérifiez que la configuration et les signatures d'IOS IPS sont correctement chargées

Le Cisco SDM est un outil de configuration par le Web qui simplifie le routeur et la configuration de sécurité par les assistants intelligents qui aident des clients rapidement et facilement déploient, configurent, et surveillent un routeur de Cisco sans exiger la connaissance de l'interface de ligne de commande (CLI).

La version 2.5 SDM peut être téléchargée de Cisco.com chez http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (clients enregistrés seulement). La note de mise à jour peut être trouvée

chez
http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

Note: Le Cisco SDM exige une résolution d'écran au moins de 1024 x de 768.

Note: Le Cisco SDM exige de la taille de segment de mémoire de mémoire de Javas d'être aucune moins que 256MB afin de configurer l'IOS IPS. Afin de changer la taille de segment de mémoire de mémoire de Javas, ouvrez le panneau de contrôle Java, cliquez sur l'onglet de **Javas**, cliquez sur la **vue** située sous les configurations d'exécution d'applet Java, et puis écrivez **-Xmx256m** dans la colonne de paramètre d'exécution de Javas.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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 des versions ultérieures
- Version 2.5 du Cisco Router and Security Device Manager (SDM)

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

Note: Ouvrez une console ou une session de telnet au routeur (avec le « moniteur de terme » en fonction) afin de surveiller des messages quand vous employez SDM pour provision l'IOS IPS.

1. Téléchargez SDM 2.5 de Cisco.com chez http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (clients enregistrés seulement) et installez-le sur un ordinateur local.
2. Exécutez SDM 2.5 de l'ordinateur local.
3. Quand la boîte de dialogue de connexion d'IOS IPS apparaît, entrez le mêmes nom d'utilisateur et mot de passe que vous utilisez pour l'authentification SDM au routeur.
4. De l'interface utilisateur SDM, cliquez sur Configure, et puis cliquez sur la **prévention des intrusions**.
5. Cliquez sur l'onglet **IPS d'éditer**.

6. Si la notification SDEE n'est pas activée sur le routeur, cliquez sur OK afin d'activer la notification SDEE.
7. Dans le fichier de signatures de téléchargement de la région de Cisco.com de l'onglet IPS d'éditer, cliquez sur l'**obtenir la dernière** case d'option de **fichier SDM et de module CLI**, et puis cliquez sur **parcourent** afin de sélectionner un répertoire sur votre ordinateur local en lequel pour sauvegarder les fichiers téléchargés.Vous pouvez choisir le TFTP ou le répertoire racine serveur ftp, qui seront utilisés plus tard quand vous déployez le module de signature vers le routeur.
8. Cliquez sur **Download**.
9. Quand la boîte de dialogue de connexion CCO apparaît, utilisez votre nom et mot de passe d'utilisateur enregistré CCO.SDM se connecte à Cisco.com et aux débuts pour télécharger le fichier SDM (par exemple, sigv5-SDM-S307.zip) et le fichier de package CLI (par exemple, IOS-S313-CLI.pkg) au répertoire sélectionné dans l'étape 7.Une fois que les deux fichiers sont téléchargés, SDM vous incite à pousser le module téléchargé de signature au routeur.
10. Cliquez sur l'**aucun** puisque l'IOS IPS n'a pas été configuré sur le routeur encore.
11. Après que SDM télécharge le dernier module de signature IOS CLI, cliquez sur l'onglet **IPS de création** afin de créer la configuration initiale d'IOS IPS.
12. Si vous êtes incité à appliquer des modifications au routeur, cliquez sur Apply les **modifications**.
13. **Assistant de règle IPS de lancement de** clic.Une boîte de dialogue semble vous informer que SDM doit établir un abonnement SDEE au routeur pour récupérer des alertes.
14. Cliquez sur **OK**.L'authentification a exigé la boîte de dialogue apparaît.
15. Entrez le nom d'utilisateur et le mot de passe que vous avez utilisé pour SDM pour authentifier au routeur, et cliquez sur OK.La boîte de dialogue d'assistant de stratégies IPS apparaît.
16. Cliquez sur **Next** (Suivant).
17. Dans la fenêtre d'interfaces sélectionnées, choisissez l'interface et la direction auxquelles cet IOS IPS sera appliqué, et puis cliquez sur **à côté de** continuent.
18. Dans la région de fichier de signatures de la fenêtre de fichier de signatures et de clé publique, cliquez sur le **spécifier le fichier de signatures que vous voulez utiliser avec la** case d'option d'**IOS IPS**, et puis cliquez sur le bouton de **fichier de signatures** (...) afin de spécifier l'emplacement du fichier de package de signature, qui sera le répertoire spécifié dans l'étape 7.
19. Cliquez sur le **fichier de signatures de spécifier utilisant la** case d'option **URL**, et choisissez un protocole de la liste déroulante de Protocol.**Note**: Cet exemple emploie le TFTP afin de télécharger le module de signature au routeur.
20. Écrivez l'URL pour le fichier de signatures, et cliquez sur OK.
21. Dans la zone clé publique de configurer de la fenêtre de fichier de signatures et de clé publique, écrivez **realm-cisco.pub dans la** zone d'identification, et puis copiez cette clé publique et collez-la dans la zone de tri.

```
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
```

Note: Cette clé publique peut être téléchargement de Cisco.com à : http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (clients enregistrés seulement).

22. Cliquez sur **Next** pour continuer.
23. Dans la fenêtre de config location et de catégorie, cliquez sur le bouton de **config location** (...) afin de spécifier un emplacement où la définition et les fichiers de configuration de signatures seront enregistrés.La boîte de dialogue de **config location d'ajouter** apparaît.
24. Dans la boîte de dialogue de config location d'ajouter, cliquez sur le **spécifier le config location sur cette** case d'option de **routeur**, et puis cliquez sur le bouton de **nom du répertoire** (...) afin de localiser le fichier de configuration.La boîte de dialogue de répertoire de choisir apparaît afin de te permettre pour sélectionner un répertoire existant ou pour créer un nouveau répertoire sur le flash du routeur pour enregistrer la définition et les fichiers de configuration de signature.
25. Cliquez sur New le **répertoire** situé en haut de la boîte de dialogue si vous voulez créer un nouveau répertoire.
26. Une fois que vous sélectionnez le répertoire, cliquez sur OK afin d'appliquer des modifications, et puis cliquez sur OK afin de fermer la boîte de dialogue de config location d'ajouter.
27. Sur la boîte de dialogue d'assistant de stratégies IPS, sélectionnez la catégorie de signature selon la quantité de mémoire installée sur le routeur. Il y a deux catégories de signature que vous pouvez choisir dans SDM : De base et avancé.Si le routeur fait installer la mémoire vive dynamique 128MB, Cisco recommande que vous choisissiez la catégorie de base afin d'éviter des défaillances d'allocation de mémoire. Si le routeur fait installer 256MB ou plus de mémoire vive dynamique, vous pouvez choisir l'un ou l'autre de catégorie.
28. Une fois que vous sélectionnez une catégorie pour utiliser, cliquez sur Next afin de continuer à la page récapitulative.La page récapitulative fournit une brève description au sujet de la configuration initiale d'IOS IPS de tâches.
29. Cliquez sur Finish à la page récapitulative afin de fournir les configurations et le module de signature au routeur.Si l'option de commandes d'aperçu est activée sur les configurations de préférences dans SDM, SDM affiche la configuration de livraison dans la boîte de dialogue de routeur qui affiche qu'un résumé de CLI commande que SDM livrent au routeur.
30. Le clic **livrent** afin de poursuivre.La boîte de dialogue d'état de la livraison de commandes semble afficher l'état de la livraison de commandes.
31. Quand les commandes sont fournies au routeur, cliquez sur OK afin de continuer.La boîte de dialogue d'état de configuration d'IOS IPS prouve que les signatures sont chargées sur le routeur.
32. Quand les signatures sont chargées, SDM affiche l'onglet **IPS d'éditer** avec la configuration en cours. Vérifiez qui relient et dans au quel direction l'IOS IPS est permis afin de vérifier la configuration.La console du routeur prouve que les signatures ont été chargées.
33. Employez la commande de **compte de signatures de show ip ips** afin de vérifier les

signatures sont chargés 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
```

Le ravitaillement initial de l'IOS IPS utilisant SDM 2.5 est complet.

34. Vérifiez les nombres de signature avec SDM suivant les indications de cette image.

Informations connexes

- Cisco IOS IPS sur Cisco.com
- Module de signature IPS de Cisco IOS
- Fichiers de signature IPS de Cisco IOS pour SDM
- Obtenir commencé par le Cisco IOS IPS avec le format de la signature 5.x
- Guide de configuration IPS de Cisco IOS
- Visualisateur d'événements d'ID de Cisco
- Support et documentation techniques - Cisco Systems