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

Contenu

Introduction

Le Cisco Security Manager fait partie de la suite logicielle de gestion de sécurité Cisco, qui fournit la gestion et l'application complètes de stratégie pour le Cisco Self-Defending Network. Le Cisco Security Manager est une demande de classe entreprise de leader de gérer la Sécurité. Le Cisco Security Manager s'adresse à la gestion de la configuration du Pare-feu, du VPN, et des Services de sécurité de Système de prévention d'intrusion (IPS) à travers des Routeurs de Cisco, des dispositifs de sécurité, et des modules de Services de sécurité.

Pour un résumé des caractéristiques et des avantages de Cisco Security Manager, aussi bien que de nouvelles caractéristiques dans la version 3.1, référez-vous à la fiche technique de Cisco Security Manager 3.1 chez http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html. Vous pouvez télécharger le Cisco Security Manager 3.1 de Cisco.com chez http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app (clients enregistrés seulement).

Ce document décrit comment employer le Cisco Security Manager 3.1 afin d'exécuter la configuration initiale de l'IOS IPS. Pour des Routeurs déjà configurés avec l'IOS IPS, les clients peuvent directement utiliser le Cisco Security Manager 3.1 pour des tâches de ravitaillement.

Remarque: Le Cisco Security Manager 3.1 prend en charge seulement IOS 12.4(11)T2 et images postérieures IOS afin de configurer l'IOS IPS.

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 Security Manager 3.1
- Cisco IOS 12.4(11)T2

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

Terminez-vous ces étapes afin de configurer l'IOS IPS :

1. Exécutez le client de Cisco Security Manager 3.1 de votre ordinateur local.
2. Choisissez le **nouveau périphérique du** menu File afin d'ajouter un périphérique sur le Cisco Security Manager 3.1.
3. Dans la nouvelle fenêtre de périphérique, choisissez comment vous voudriez ajouter le périphérique. Cet exemple ajoute le périphérique du réseau.
4. Cliquez sur **Next** (Suivant).
5. Écrivez les détails d'identité pour le périphérique que vous voulez ajouter. Par exemple, nom d'hôte et adresse IP.
6. Cliquez sur **Next** (Suivant).
7. Entrez dans les qualifications primaires, telles que le nom d'utilisateur, mot de passe, mot de passe d'enable pour le routeur IOS que vous voulez ajouter.
8. Cliquez sur Finish afin d'ajouter le périphérique sur le Cisco Security Manager.**Remarque:** Cet exemple supposent que l'utilisateur déjà a un routeur préconfiguré et peut ouvrir une session au routeur avec les qualifications appropriées.Quand la « détection terminée » apparaît dans la fenêtre d'état de détection, vous avez avec succès ajouté un périphérique sur le Cisco Security Manager. Une fois que vous avez avec succès ajouté un périphérique sur le Cisco Security Manager, vous devez assigner une clé publique afin d'activer l'IPS.
9. Du menu du côté gauche, naviguez vers l'écran de configuration de FlexConfigs.
10. Cliquez sur l'interface utilisateur de FlexConfigs du côté droit de l'écran, et puis cliquez sur l'icône d'**ajouter**.
11. Dans la liste sélectionnée de FlexConfigs, choisissez **IOS_IPS_PUBLIC_KEY**, et cliquez sur OK.
12. **Sauvegarde de** clic afin de sauvegarder les modifications.**Remarque:** L'IOS_IPS_PUBLIC_KEY FlexConfig tient la configuration pour la clé publique.
13. Du menu du côté gauche, choisissez les **paramètres généraux** situés sous le titre IPS.

14. Entrez l'emplacement de configuration IPS sur l'éclair. C'est l'emplacement dans lequel les configurations IPS sont placées.
15. **Sauvegarde de** clic afin de sauvegarder les modifications.**Remarque:** Assurez-vous que le répertoire d'emplacement a été déjà créé sur le flash du routeur. Sinon, employez la commande de **<directory_name> de mkdir** afin de créer le répertoire d'emplacement.
16. Afin d'activer l'IPS, naviguez pour relier des règles, cochez la case **IPS d'enable**, et puis cliquez sur Add la **ligne**.
17. Dans la boîte de dialogue de règle IPS d'ajouter, écrivez un nom pour la règle IPS dans la zone d'identification de règle, et puis cliquez sur Add la **ligne** afin d'inclure les interfaces sur lesquelles l'IPS doit être appliqué.
18. Cliquez sur la case d'option qui indique dans quelle direction la règle IPS doit être appliquée, et puis clique sur **choisi** afin de choisir les interfaces appropriées.
19. Choisissez une interface de la liste de sélecteur d'interface, et cliquez sur OK.
20. **Sauvegarde de** clic afin de sauvegarder les modifications.
21. Choisissez les **outils > appliquent la mise à jour IPS** afin d'installer les plus défuntes signatures IPS.
22. Choisissez le dernier fichier de signatures, et cliquez sur Next.
23. Choisissez les périphériques sur lesquels la mise à jour IPS doit être appliquée, et cliquez sur Next.
24. Cliquez sur Finish afin d'appliquer les signatures.
25. Naviguez vers l'IPS, et choisissez les **signatures** afin de visualiser la liste de toutes les signatures.
26. Choisissez le **fichier > soumettent et se déploient** afin de déployer l'IPS sur le routeur IOS.
27. Choisissez le périphérique sur lequel vous voulez déployer les modifications, et le clic **se déploient**.
28. Visualisez l'état de déployer afin de vérifier s'il y a des erreurs.

Informations connexes

- Produits de Système de protection contre les intrusions (IPS) Cisco IOS et page de services
- Obtenir commencé par le Cisco IOS IPS avec le format de la signature 5.x
- IPS améliorations de support et de facilité d'utilisation de format de signature 5.x
- 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