Exemple de migration du format de signature version 4.x du système de prévention des intrusions vers le format de signature version 5.x

Contenu

Introduction

Dans la version 12.4(11)T et ultérieures de Cisco IOS®, le Système de protection contre les intrusions (IPS) Cisco IOS fournit le support pour le format de signature de la version de logiciel 5.x de Cisco IPS. Le format de la signature 5.x est un format XML basé sur version de définition de signature également utilisé par d'autres Produits basés sur appliance de Cisco IPS. Le soutien des signatures et les fichiers de définition de signature (SDF) dans la version 4.x de Cisco IPS sont discontinués en cela et d'autres versions logicielles de T-série de Cisco IOS.

Les clients qui exécutent le Cisco IOS IPS avec le format SDF de signature de version 4.x peuvent modifier le Cisco IOS IPS pour employer des catégories de signature prédéfinies par Cisco, des positionnements de base et avancés de signature, ou l'utilitaire de transfert IPS de Cisco IOS afin de migrer les fichiers SDF précédents de version 4.x dans la version 5.x de Cisco IPS formatent des positionnements de signature.

Ce document décrit comment migrer d'un format SDF du Cisco IPS 4.x et activer la signature migrée réglée dans la Cisco IOS version 12.4(11)T ou ultérieures. Pour plus d'informations sur la façon configurer le Cisco IOS IPS dans la Cisco IOS version 12.4(11)T ou ultérieures, référez-vous aux améliorations de support et de facilité d'utilisation de format de signature IPS 5.x.

Remarque: Cisco recommande que vous exécutiez le transfert IPS de Cisco IOS avant que vous amélioriez à une image de Cisco IOS version 12.4(11)T ou ultérieures.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la Cisco IOS version 12.4(11)T ou ultérieures.

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.

Étapes pour migrer des fichiers SDF de version 4.x

Le script de transfert exige un fichier SDF de format du Cisco IPS 4.x et (sur option) le fichier de configuration CLI qui contient les informations de configuration IPS de Cisco IOS utilisées sur une version de thatrunsa de routeur plus tôt que la Cisco IOS version 12.4(11)T.

Le script de transfert recherche les commandes qui contiennent le **<sigid d'ip ips signature > [<sigsubid >] désactivé** dans le fichier de configuration de routeur. Si le fichier de configuration ne contient pas cette commande CLI, il n'y a aucun besoin du script de transfert de lire le fichier de configuration CLI. La conversion des signatures, en soi, sont basées seulement sur le SDF.

Si vous exécutez le script de transfert avant que vous amélioriez le Cisco IOS IPS à la Cisco IOS version 12.4(11)T ou ultérieures, suivez le processus exécutent dedans le script de transfert IPS de Cisco IOS.

Si vous exécutez le script de transfert après que vous amélioriez le Cisco IOS IPS à la Cisco IOS version 12.4(11)T ou ultérieures, terminez-vous ces étapes :

1. Vérifiez n'importe quel besoin de convertir des commandes CLI, **<sigid d'ip ips signature > [<sigsubid >] a désactivé**, comme mentionné ci-dessus.
2. Utilisez l'**éclair de** commande copy running-config **: ipscfg.cfg afin de** sauvegarder la configuration CLI du routeur à un fichier.Cette commande sauvegarde la configuration de routeur existant pour flasher dans un fichier nommé *ipscfg.cfg.* Le procédé de transfert utilise ce fichier pour plein 4.x à la conversion de format de la signature 5.x.
3. Poursuivez pour exécuter le script de transfert IPS de Cisco IOS.

Exécutez le script de transfert IPS de Cisco IOS

Le script de transfert est fourni par Cisco.com à cet URL : http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. Sauvegardez le script de transfert à l'éclair du routeur ou à un

emplacement routeur-accessible, tel qu'un serveur de Protocole TFTP (Trivial File Transfer Protocol).

Le script de transfert convertit un SDF de format de version 4.x de Cisco IPS en format de version 5.x. Le script de transfert prend en charge seulement ces paramètres de signature :

- sévérité
- action
- activé

En outre, le script de transfert peut également lire d'un fileand de configuration d'IOS IPS migrent les signatures handicapées qui ont été configurées par la commande **désactivée par <sigsubid> de <sigid> d'ip ips signature** CLI dans les versions plus tôt que la Cisco IOS version 12.4(11)T.

Remarque: (Non des signatures faites sur commande de Cisco) ne sont pas converties avec ce script.

Cet exemple affiche comment migrer le fichier formaté par 4.x *sdmips.sdf* IPS *vers le* Cisco IOS IPS dans la Cisco IOS version 12.4(11)T avec le support de format de signature IPS 5.x de Cisco IOS.

```
C2821#tclsh flash:ios-ips-migrate.tbc
This migration script will migrate Signature Definition Files
     from 4.x format to 5.x format.
The migration script will migrate only the following signature
     parameters - severity, action, enabled - for Cisco (non-custom) signatures.
Do you want to continue? [y/n] y
Please choose an IOS config file from which to migrate IOS IPS configuration.
Config File: [startup-config]
The following SDF locations were found configured in startup-config:
  flash://sdmips.sdf
Please provide SDF to migrate from the above list or of your own
     choice: flash:// sdmips.sdf
Migrating following SDF file (this will a take few minutes):
  flash://sdmips.sdf
Time Elapsed: 0:02:23
Migration completed successfully. The migrated file is
  C2821-sigdef-delta.xml
C2821#
```

D'abord, le script de transfert affiche un bref texte au sujet de sa fonction. Ensuite, le script fournit une option de choisir un emplacement d'où lire la configuration en cours (de prémigration) pour le Cisco IOS IPS. Le par défaut lit de la configuration de démarrage. Si vous avez précédemment enregistré une configuration à un serveur TFTP ou à l'éclair du routeur, spécifiez l'emplacement à la demande.

Exemple :

Utilisez la *configuration de* **tftp:// 192.168.1.5/<routeur** *CLI* **>** afin d'informer le script de charger une configuration CLI du serveur 192.168.1.5 TFTP.

Utilisez la <saved-**configuration de flash:// >** afin de lire à partir d'un fichier enregistré sur l'éclair.

Chargez les signatures migrées dans le Cisco IOS IPS dans le Logiciel Cisco IOS version 12.4(11)T

Après que le transfert de signature soit complet, améliorez l'image du routeur au Cisco IOS

Release12.4(11)T si vous n'avez pas déjà fait ainsi. Une fois que le routeur est rechargé, terminez-vous ces étapes.

1. Cisco IOS IPS d'enable.Cette sortie affiche comment activer le Cisco IOS IPS sur un routeur de Cisco 2821. Pour plus d'informations sur la façon configurer le Cisco IOS IPS, référez-vous aux [améliorations de support et de facilité d'utilisation de format de signature IPS 5.x](#).
```
C2821#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
C2821#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
C2821(config)#
```
2. Copiez et collez cette clé dans le routeur afin de configurer la clé publique de crypto signature.
```
C2821#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
C2821#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
C2821(config)#
```
3. Activez le Cisco IOS IPS sur des interfaces suivant les indications de cet exemple :
```
C2821(config)#
C2821(config)#interface gigabitEthernet 0/0
C2821(config-if)#ip ips MYIPS in
C2821(config-if)#ip ips MYIPS out
C2821(config-if)#exit
```
4. Employez la Commande **COPY** afin de charger le dernier module de signature :`C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf`
   Cette commande charge des signatures du module *IOS-S253-CLI.pkg de* signature dans le Cisco IOS IPS.**Remarque: la catégorie toute de la signature IOS-IPS** a été configurée dans l'étape 1, qui retire toutes les signatures. Après que le module de signature soit avec succès chargé, aucune signature n'est sélectionnée et est compilée.
5. Employez cette commande afin de charger le fichier XML migré au Cisco IOS IPS :**<routeur-adresse Internet >-sigdef-delta.xml**Exemple :
   `copy flash:C2821-sigdef-delta.xml idconf`
   Une fois que le routeur analyse le fichier de signatures formaté par version 5.x, le transfert est complet.
6. Employez la commande de **compte de signature de show ip ips** afin de vérifier l'état récapitulatif de signature, et puis utilisez les **détails de signature de show ip ips** commandent afin de visualiser les détails spécifiques sur toutes les signatures.

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