Migration du format de signature IPS 4.x vers 5.x

Contenu

Introduction

Dans Cisco IOS® version 12.4(11)T et ultérieure, Cisco IOS Intrusion Prevention System (IPS) prend en charge le format de signature du logiciel Cisco IPS version 5.x. Le format de signature 5.x est un format XML de définition de signature basé sur la version, également utilisé par d'autres produits IPS basés sur des appliances Cisco. La prise en charge des signatures et des fichiers de définition de signature (SDF) dans Cisco IPS version 4.x est interrompue dans cette version et dans les autres versions du logiciel Cisco IOS T-Train.

Les clients qui exécutent Cisco IOS IPS avec SDF au format de signature version 4.x peuvent reconfigurer Cisco IOS IPS pour utiliser les catégories de signatures prédéfinies Cisco, les jeux de signatures de base et avancés ou l'utilitaire de migration Cisco IOS IPS afin de migrer les fichiers SDF de la version 4.x précédente vers des jeux de signatures au format Cisco IPS version 5.x.

Ce document décrit comment migrer à partir d'un SDF au format Cisco IPS 4.x et activer le jeu de signatures migrées dans Cisco IOS version 12.4(11)T ou ultérieure. Pour plus d'informations sur la configuration de Cisco IOS IPS dans Cisco IOS version 12.4(11)T ou ultérieure, référez-vous à Prise en charge du format de signature IPS 5.x et améliorations de l'utilisation.

Remarque : Cisco vous recommande d'exécuter la migration de Cisco IOS IPS avant de passer à une image Cisco IOS version 12.4(11)T ou ultérieure.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

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.

Étapes de migration des fichiers SDF version 4.x

Le script de migration nécessite un fichier SDF au format Cisco IPS 4.x et (éventuellement) le fichier de configuration CLI qui contient les informations de configuration IPS de Cisco IOS utilisées sur un routeur qui a une version antérieure à la version 12.4(11)T de Cisco IOS.

Le script de migration recherche les commandes qui contiennent la **signature ip ips <*sigid*> [<*sigsubid*>] désactivée** dans le fichier de configuration du routeur. Si le fichier de configuration ne contient pas cette commande CLI, il n'est pas nécessaire que le script de migration lise le fichier de configuration CLI. La conversion des signatures, en tant que telle, est basée uniquement sur le SDF.

Si vous exécutez le script de migration avant de mettre à niveau Cisco IOS IPS vers Cisco IOS version 12.4(11)T ou ultérieure, suivez le processus dans Exécuter le script de migration Cisco IOS IPS.

Si vous exécutez le script de migration après avoir mis à niveau Cisco IOS IPS vers Cisco IOS version 12.4(11)T ou ultérieure, procédez comme suit :

1. Vérifiez si vous avez besoin de convertir les commandes CLI, **ip ips signature <*sigid*> [<*sigsubid*>] désactivée**, comme indiqué ci-dessus.
2. Utilisez la commande **copy running-config flash:ipscfg.cfg** afin d'enregistrer la configuration CLI du routeur dans un fichier.Cette commande sauvegarde la configuration existante du routeur en mémoire flash dans un fichier nommé *ipscfg.cfg*. Le processus de migration utilise ce fichier pour la conversion complète du format de signature 4.x vers 5.x.
3. Passez à l'exécution du script de migration de Cisco IOS IPS.

Exécuter le script de migration de Cisco IOS IPS

Le script de migration est disponible sur Cisco.com à l'adresse suivante : http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. Enregistrez le script de migration dans la mémoire Flash du routeur ou à un emplacement accessible au routeur, tel qu'un serveur TFTP (Trivial File Transfer Protocol).

Le script de migration convertit un fichier SDF du format Cisco IPS version 4.x en format version 5.x. Le script de migration prend uniquement en charge les paramètres de signature suivants :

- severity (gravité)
- action

- activée

En outre, le script de migration peut également lire à partir d'un fichier de configuration IOS IPS et migrer les signatures désactivées qui ont été configurées par la commande **CLI ip ips signature <sigid> <sigsubid> disabled** dans les versions antérieures à la version 12.4(11)T de Cisco IOS.

Remarque : les signatures personnalisées (non Cisco) ne sont pas converties avec ce script.

Cet exemple montre comment migrer le fichier formaté IPS 4.x *sdmips.sdf* vers Cisco IOS IPS dans Cisco IOS Version 12.4(11)T avec prise en charge du format de signature Cisco IOS IPS 5.x.

```
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#
```

Tout d'abord, le script de migration affiche un bref texte sur sa fonction. Ensuite, le script fournit une option permettant de choisir un emplacement à partir duquel lire la configuration actuelle (pré-migration) de Cisco IOS IPS. La valeur par défaut est lue à partir de la configuration de démarrage. Si vous avez précédemment enregistré une configuration sur un serveur TFTP ou sur la mémoire Flash du routeur, spécifiez l'emplacement à l'invite.

Exemple :

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

Utilisez **flash://<*save-configuration*>** afin de lire à partir d'un fichier enregistré sur la mémoire Flash.

Charger les signatures migrées dans Cisco IOS IPS dans le logiciel Cisco IOS Version 12.4(11)T

Une fois la migration des signatures terminée, mettez à niveau l'image du routeur vers Cisco IOS version 12.4(11)T si vous ne l'avez pas déjà fait. Une fois le routeur rechargé, procédez comme suit.

1. Activez Cisco IOS IPS.Ce résultat montre comment activer Cisco IOS IPS sur un routeur Cisco 2821. Pour plus d'informations sur la configuration de Cisco IOS IPS, référez-vous à Prise en charge du format de signature IPS 5.x et améliorations de l'utilisation.
   ```
   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 signature de chiffrement.

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
 key-string
 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
 quit
 exit
 exit
```

3. Activez Cisco IOS IPS sur les interfaces comme indiqué dans 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. Utilisez la commande **copy** afin de charger le dernier package de signatures :

```
C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf
```

Cette commande charge les signatures du package de signatures *IOS-S253-CLI.pkg* dans Cisco IOS IPS.**Remarque : la catégorie de signatures ios-ips** a été configurée à l'étape 1, qui supprime toutes les signatures. Une fois le package de signatures chargé, aucune signature n'est sélectionnée et compilée.

5. Utilisez cette commande afin de charger le fichier XML migré vers Cisco IOS IPS :**<*routeur-hostname*>-sigdef-delta.xml**Exemple :

```
copy flash:C2821-sigdef-delta.xml idconf
```

Une fois que le routeur analyse le fichier de signature formaté version 5.x, la migration est terminée.

6. Utilisez la commande **show ip ips signature count** afin de vérifier l'état récapitulatif des signatures, puis utilisez la commande **show ip ips signature details** afin d'afficher des détails spécifiques sur toutes les signatures.

Informations connexes

- Système de prévention des intrusions Cisco
- Avis de champs relatifs aux produits de sécurité (y compris CiscoSecure Intrusion Detection)
- Support technique - Cisco Systems