Formato de la firma de la versión 4.x del sistema de prevención de intrusiones a los ejemplos de migración del formato de la firma de la versión 5.x

Contenido

Introducción

En la versión 12.4(11)T del ® del Cisco IOS y posterior, el Cisco IOS Intrusion Prevention System (IPS) proporciona el soporte para el formato de la firma de la versión de software 5.x del IPS de Cisco. El formato de la firma 5.x es un formato XML versión-basado de la definición de la firma también usado por otros Productos dispositivo-basados Cisco IPS. El soporte para las firmas y los archivos de definición de la firma (SDFs) en la versión 4.x del IPS de Cisco se interrumpe en este y versiones de software más futuras del T-tren del Cisco IOS.

Los clientes que funcionan con el Cisco IOS IPS con el formato SDFs de la firma de la versión 4.x pueden configurar de nuevo el Cisco IOS IPS para utilizar las categorías predefinidas Cisco de la firma, los conjuntos de firmas básicos y avanzados, o la utilidad de la migración IPS del Cisco IOS para emigrar los archivos de la versión anterior 4.x SDF en la versión 5.x del IPS de Cisco formatan los conjuntos de firmas.

Este documento describe cómo emigrar de un formato SDF del IPS de Cisco 4.x y habilitar el conjunto de firmas emigrado en el Cisco IOS Release 12.4(11)T o Posterior. Para más información sobre cómo configurar el Cisco IOS IPS en el Cisco IOS Release 12.4(11)T o Posterior, refiera a las mejoras del soporte y de la utilidad del formato de la firma IPS 5.x.

Nota: Cisco recomienda que usted ejecuta la migración IPS del Cisco IOS antes de que usted actualice a una imagen del Cisco IOS Release 12.4(11)T o Posterior.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Cisco IOS Release 12.4(11)T o Posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Pasos para emigrar los archivos de la versión 4.x SDF

El script de la migración requiere un archivo del formato SDF del IPS de Cisco 4.x y (opcionalmente) el archivo de configuración CLI que contiene la información de la configuración IPS del Cisco IOS usada en una versión del thatrunsa del router anterior que el Cisco IOS Release 12.4(11)T.

El script de la migración busca para los comandos que contienen el **<sigid > el [<sigsubid>] de la firma IPS del IP inhabilitados** dentro del archivo de configuración del router. Si el archivo de configuración no contiene este comando CLI, no hay necesidad del script de la migración de leer el archivo de configuración CLI. La conversión de las firmas, como tal, se basa solamente en el SDF.

Si usted ejecuta el script de la migración antes de que usted actualice el Cisco IOS IPS al Cisco IOS Release 12.4(11)T o Posterior, siga el proceso adentro ejecutan el script de la migración IPS del Cisco IOS.

Si usted ejecuta el script de la migración después de que usted actualice el Cisco IOS IPS al Cisco IOS Release 12.4(11)T o Posterior, complete estos pasos:

1. Verifique cualquier necesidad de convertir los comandos CLI, **<sigid de la firma IPS del IP > [<sigsubid>] inhabilitado**, como se mencionó anteriormente.
2. Utilice el **flash de los ejecutar-config del** comando copy**: ipscfg.cfg para** salvar la configuración CLI del router a un archivo.Este comando sostiene la configuración del router existente para contellear en un archivo nombrado *ipscfg.cfg.* El proceso de migración utiliza este archivo para 4.x lleno a la conversión del formato de la firma 5.x.
3. Proceda a ejecutar el script de la migración IPS del Cisco IOS.

Ejecute el script de la migración IPS del Cisco IOS

El script de la migración es disponible desde Cisco.com en este URL: http://www.cisco.com/cgi-

bin/tablebuild.pl/ios-v5sigup. Salve el script de la migración al flash del router o a una ubicación router-accesible, tal como un servidor del Trivial File Transfer Protocol (TFTP).

El script de la migración convierte un SDF del formato de la versión 4.x del IPS de Cisco al formato de la versión 5.x. El script de la migración soporta solamente estos parámetros de la firma:

- gravedad
- acción
- habilitado

Además, el script de la migración puede también leer en un fileand de la configuración IOS IPS emigra las firmas discapacitadas que fueron configuradas por el comando **inhabilitado <sigsubid> del <sigid> de la firma IPS del IP** CLI en las versiones anterior que el Cisco IOS Release 12.4(11)T.

Nota: (No las firmas de encargo de Cisco) no se convierten con este script.

Este ejemplo muestra cómo emigrar el archivo formatado 4.x *sdmips.sdf* IPS al Cisco IOS IPS en el Cisco IOS Release 12.4(11)T con el soporte del formato de la firma IPS 5.x del 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#
```

Primero, el script de la migración visualiza un texto abreviado sobre su función. Después, el script proporciona una opción para elegir una ubicación de donde leer la configuración actual (de la premigración) para el Cisco IOS IPS. El valor por defecto lee en la configuración de inicio. Si usted ha guardado previamente una configuración a un servidor TFTP o al flash del router, especifique la ubicación en el prompt.

Por ejemplo:

Utilice la *configuración CLI de* **tftp:// 192.168.1.5/<router >** para notificar el script para cargar una configuración CLI del servidor TFTP 192.168.1.5.

Utilice la <saved-**configuración de flash:// >** para leer en un archivo guardado en el flash.

Cargue las firmas emigradas en el Cisco IOS IPS en el Cisco IOS Software Release 12.4(11)T

Después de que la migración de la firma sea completa, actualice la imagen del router al Cisco IOS

Release12.4(11)T si usted no ha hecho ya tan. Una vez que recargan al router, complete estos pasos.

1. Habilite el Cisco IOS IPS.Esta salida muestra cómo habilitar el Cisco IOS IPS en un Cisco 2821 Router. Para más información sobre cómo configurar el Cisco IOS IPS, refiera a las mejoras del soporte y de la utilidad del formato de la firma 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. La copia y pega esta clave en el router para configurar la clave pública crypto de la firma.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. Habilite el Cisco IOS IPS en las interfaces tal y como se muestra en de este ejemplo: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. Utilice el **comando copy** para cargar el último paquete de la firma:C2821#**copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf**
   Este comando carga las firmas del paquete *IOS-S253-CLI.pkg de la* firma en el Cisco IOS IPS.**Nota: la categoría toda de la firma IOS-IPS** fue configurada en el paso 1, que retira todas las firmas. Después de que el paquete de la firma se cargue con éxito, no se selecciona y se compila ningunas firmas.
5. Utilice este comando para cargar el archivo XML emigrado al Cisco IOS IPS:**<router-nombre de host >-sigdef-delta.xml**Por ejemplo:
   copy flash:C2821-sigdef-delta.xml idconf
   Una vez que el router analiza el archivo de firma formatado versión 5.x, la migración es completa.
6. Utilice el **comando count de la firma IPS del IP de la demostración** para marcar el estado resumido de la firma, y después utilice los **detalles de la firma IPS del IP de la demostración** ordenan para ver los detalles específicos en todas las firmas.

Información Relacionada

- Cisco Intrusion Prevention System
- Field Notice de seguridad del producto (CiscoSecure Intrusion Detection incluyendo)
- Soporte Técnico - Cisco Systems