Migrar el formato de firma IPS 4.x a 5.x

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Pasos para migrar archivos SDF de la versión 4.x](#)
[Ejecutar el script de migración de Cisco IOS IPS](#)
[Carga de las Firmas Migradas en Cisco IOS IPS en Cisco IOS Software Release 12.4(11)T](#)
[Información Relacionada](#)

Introducción

En Cisco IOS® versión 12.4(11)T y posteriores, Cisco IOS Intrusion Prevention System (IPS) proporciona compatibilidad con el formato de firma de la versión 5.x del software Cisco IPS. El formato de firma 5.x es un formato XML de definición de firma basado en versión que también utilizan otros productos IPS basados en dispositivos de Cisco. La compatibilidad con las firmas y los archivos de definición de firma (SDF) de la versión 4.x de Cisco IPS se ha interrumpido en esta y otras versiones del software T-Train del IOS de Cisco.

Los clientes que ejecutan Cisco IOS IPS con el formato de firma SDF de la versión 4.x pueden reconfigurar Cisco IOS IPS para utilizar las categorías de firma predefinidas de Cisco, los conjuntos de firma básicos y avanzados o la utilidad de migración de Cisco IOS IPS para migrar los archivos SDF de la versión anterior 4.x a los conjuntos de firmas de formato Cisco IPS versión 5.x.

Este documento describe cómo migrar desde un SDF con formato Cisco IPS 4.x y habilitar la firma migrada establecida en Cisco IOS Release 12.4(11)T o posterior. Para obtener más información sobre cómo configurar Cisco IOS IPS en Cisco IOS Release 12.4(11)T o posterior, refiérase a Soporte de Formato de Firma IPS 5.x y Mejoras de Usabilidad.

Nota: Cisco recomienda que ejecute la migración de Cisco IOS IPS antes de actualizar a una imagen de Cisco IOS Release 12.4(11)T o posterior.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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.

Convenciones

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

Pasos para migrar archivos SDF de la versión 4.x

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

El script de migración busca los comandos que contienen **ip ips Signature <*sigid*> [<*sigsubid*>] inhabilitados** dentro del archivo de configuración del router. Si el archivo de configuración no contiene este comando CLI, no es necesario que el script de migración lea el archivo de configuración CLI. La conversión de firmas, como tal, se basa únicamente en las FAD.

Si ejecuta la secuencia de comandos de migración antes de actualizar Cisco IOS IPS a Cisco IOS Release 12.4(11)T o posterior, siga el proceso en Ejecutar la secuencia de comandos de migración de Cisco IOS IPS.

Si ejecuta la secuencia de comandos de migración después de actualizar Cisco IOS IPS a Cisco IOS Release 12.4(11)T o posterior, complete estos pasos:

1. Verifique la necesidad de convertir los comandos CLI, **ip ips Signature <*sigid*> [<*sigsubid*>] inhabilitados**, como se mencionó anteriormente.
2. Utilice el comando **copy running-config flash:ipscfg.cfg** para guardar la configuración CLI del router en un archivo.Este comando realiza una copia de seguridad de la configuración del router existente para que parpadee en un archivo denominado *ipscfg.cfg*. El proceso de migración utiliza este archivo para la conversión completa del formato de firma 4.x a 5.x.
3. Continúe con la ejecución del script de migración de Cisco IOS IPS.

Ejecutar el script de migración de Cisco IOS IPS

El script de migración está disponible en Cisco.com en esta URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. Guarde la secuencia de comandos de migración en la memoria flash del router o en una ubicación accesible al router, como un servidor de protocolo de transferencia de archivos trivial (TFTP).

El script de migración convierte un SDF del formato Cisco IPS versión 4.x al formato versión 5.x. La secuencia de comandos de migración sólo admite estos parámetros de firma:

- gravedad
- acción
- habilitado

Además, la secuencia de comandos de migración también puede leer de un archivo de configuración de IOS IPS y migrar firmas inhabilitadas que fueron configuradas por el comando CLI **ip ips Signature <sigid> <sigsubid> disabled** en versiones anteriores a Cisco IOS Release 12.4(11)T.

Nota: Las firmas personalizadas (que no son de Cisco) no se convierten con este script.

Este ejemplo muestra cómo migrar el archivo con formato IPS 4.x *sdmips.sdf* a Cisco IOS IPS en Cisco IOS Release 12.4(11)T con soporte de formato de firma 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#
```

En primer lugar, el script de migración muestra un texto breve sobre su función. A continuación, el script proporciona una opción para elegir una ubicación desde la que leer la configuración actual (previa a la migración) para Cisco IOS IPS. El valor predeterminado se lee desde la configuración de inicio. Si previamente ha guardado una configuración en un servidor TFTP o en la memoria flash del router, especifique la ubicación en el mensaje.

Por ejemplo:

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

Utilice **flash://<*save-configuration*>** para leer un archivo guardado en la memoria flash.

Carga de las Firmas Migradas en Cisco IOS IPS en Cisco IOS Software Release 12.4(11)T

Una vez finalizada la migración de la firma, actualice la imagen del router a Cisco IOS Release12.4(11)T si aún no lo ha hecho. Una vez que se recarga el router, complete estos pasos.

1. Habilite Cisco IOS IPS.Este resultado muestra cómo habilitar Cisco IOS IPS en un Cisco 2821 Router. Para obtener más información sobre cómo configurar Cisco IOS IPS, refiérase a Soporte de Formato de Firma IPS 5.x y Mejoras de Usabilidad.

   ```
   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. Copie y pegue esta clave en el router para configurar la clave pública de firma criptográfica.

```
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. Habilite Cisco IOS IPS en las interfaces como se muestra en 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 paquete de firma más reciente:

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

   Este comando carga las firmas del paquete de firma *IOS-S253-CLI.pkg* en Cisco IOS IPS.**Nota: la categoría de firma ios-ips** se configuró en el paso 1, que retira todas las firmas. Una vez que el paquete de firma se ha cargado correctamente, no se seleccionan ni compilan firmas.
5. Utilice este comando para cargar el archivo XML migrado a Cisco IOS IPS:***<router-hostname>*-sigdef-delta.xml**Por ejemplo:

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

   Una vez que el router analiza el archivo de firma con formato de la versión 5.x, se completa la migración.
6. Utilice el comando **show ip ips Signature count** para verificar el estado de resumen de la firma, y luego use el comando **show ip ips Signature details** para ver detalles específicos de todas las firmas.

Información Relacionada

- Cisco Intrusion Prevention System
- Avisos de campo de productos de seguridad (incluida CiscoSecure Intrusion Detection)

- Soporte Técnico - Cisco Systems