Configurar IPS con firmas de formato 5.x

Contenido

Introducción

Este documento describe cómo configurar las firmas de formato 5.x en Cisco IOS® IPS y está organizado en dos secciones:

- Sección I. Pasos de configuración iniciales: esta sección proporciona los pasos necesarios para utilizar la interfaz de línea de comandos (CLI) de Cisco IOS para comenzar con las firmas de formato IOS IPS 5.x. Esta sección describe estos pasos:Paso 1. Descargue los archivos IOS IPS.Paso 2. Cree un directorio de configuración de IOS IPS en Flash.Paso 3. Configure una clave de cifrado IPS de IOS.Paso 4. Habilite IOS IPS.Paso 5. Cargue el paquete de firma IOS IPS al router.Cada paso y cada comando específico se describen en detalle, así como comandos y referencias adicionales. Debajo de cada comando se muestra un ejemplo de configuración.
- Sección II. Opciones de configuración avanzadas: esta sección proporciona instrucciones y ejemplos de opciones avanzadas para el ajuste de firmas. Contiene las siguientes opciones:Retirar o anular la jubilación de firmasActivar o desactivar firmasCambiar acciones de firma

Prerequisites

Requirements

Asegúrese de que dispone de los componentes adecuados (como se describe en Componentes utilizados) antes de completar los pasos de este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Un router de servicios integrados de Cisco (87x, 18xx, 28xx o 38xx)
- 128 MB o más de DRAM y al menos 2 MB de memoria flash libre
- Conectividad Telnet o de consola al router
- Cisco IOS Release 12.4(15)T3 o posterior
- Nombre de usuario y contraseña de inicio de sesión de CCO (Cisco.com) válidos
- Contrato de servicio Cisco IPS actual para servicios de actualización de firmas con licencia

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.

Sección I. Pasos de configuración de inicio

Paso 1. Descargar archivos IPS de IOS

El primer paso es descargar los archivos del paquete de firma IOS IPS y la clave criptográfica pública de Cisco.com.

Descargue los archivos de firma requeridos de Cisco.com a su PC:

- Ubicación: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (sólo clientes registrados)
- Archivos a descargar:IOS-Sxxx-CLI.pkg (sólo clientes registrados): este es el último paquete de firma.realm-cisco.pub.key.txt (sólo clientes registrados): es la clave criptográfica pública utilizada por IOS IPS.

Paso 2. Creación de un Directorio de Configuración IPS de IOS en Flash

El segundo paso consiste en crear un directorio en la memoria flash del router donde almacenará los archivos de firma y las configuraciones necesarias. También puede utilizar una unidad flash USB de Cisco conectada al puerto USB del router para almacenar los archivos de firma y las configuraciones. La unidad flash USB debe permanecer conectada al puerto USB del router si se utiliza como ubicación del directorio de configuración de IOS IPS. IOS IPS también soporta cualquier sistema de archivos IOS como su ubicación de configuración con acceso de escritura adecuado.

Para crear un directorio, ingrese este comando en la indicación del router: **mkdir <*nombre del directorio*>**

Por ejemplo:

```
router#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
```

Comandos y referencias adicionales

Para verificar el contenido de la memoria flash, ingrese este comando en la indicación del router: **show flash:**

Por ejemplo:

```
router#dir flash:
Directory of flash:/
   5 -rw-   51054864 Feb 8 2008 15:46:14 -08:00
                    c2800nm-advipservicesk9-mz.124-15.T3.bin
   6 drw-       0 Feb 14 2008 11:36:36 -08:00 ips
64016384 bytes total (12693504 bytes free)
```

Para cambiar el nombre del directorio, utilice este comando: **cambiar el nombre <*nombre actual*> <*nuevo nombre*>**

Por ejemplo:

```
router#rename ips ips_new
Destination filename [ips_new]?
```

Paso 3. Configuración de una Clave Criptográfica IPS de IOS

El tercer paso es configurar la clave de criptografía utilizada por IOS IPS. Esta clave se encuentra en el archivo realm-cisco.pub.key.txt que se descargó en el Paso 1.

La clave crypto se utiliza para verificar la firma digital del archivo de firma principal (sigdef-default.xml) cuyo contenido está firmado por una clave privada de Cisco para garantizar su autenticidad e integridad en cada versión.

1. Abra el archivo de texto y copie el contenido del archivo.
2. Utilice el comando **configure terminal** para ingresar al modo de configuración del router.
3. Pegue el contenido del archivo de texto en el mensaje `<hostname>(config)#`.
4. Salga del modo de configuración del router.
5. Ingrese el comando **show run** en el mensaje del router para confirmar que la clave crypto está configurada. Debería ver este resultado en la configuración:

```
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
```

6. Use este comando para guardar la configuración:**copy running-configure startup-configure**

Comandos y referencias adicionales

Si la clave está configurada incorrectamente, primero debe quitar la clave crypto y luego reconfigurarla:

1. Para quitar la clave, ingrese estos comandos en el orden que se muestra a continuación:
```
router#configure terminal
router(config)#no crypto key pubkey-chain rsa
router(config-pubkey-chain)#no named-key realm-cisco.pub signature
router(config-pubkey-chain)#exit
router(config)#exit
```

2. Utilice el comando **show run** para verificar que la clave se quita de la configuración.
3. Complete el procedimiento del Paso 3 para reconfigurar la clave.

Paso 4. Activar IPS de IOS

El cuarto paso es configurar IOS IPS. Complete este procedimiento para configurar IOS IPS:

1. Utilice el comando **ip ips name <*rule name*> < *opcional ACL*>** para crear un nombre de regla. (Esto se utilizará en una interfaz para activar IPS.)Por ejemplo:
```
router#configure terminal
router(config)#ip ips name iosips
```

   Puede especificar una lista de control de acceso (ACL) extendida o estándar opcional para filtrar el tráfico que analizará este nombre de regla. Todo el tráfico permitido por la ACL está sujeto a inspección por el IPS. El IPS no inspecciona el tráfico denegado por la ACL.
```
router(config)#ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
```
2. Utilice el comando **ip ips config location flash:<*directory name*>** para configurar la ubicación de almacenamiento de firma IPS. (Este es el directorio *ips* creado en el Paso 2.)Por ejemplo:
```
router(config)#ip ips config location flash:ips
```

3. Utilice el comando **ip ips notify sdee** para habilitar la notificación de eventos IPS SDEE.Por ejemplo:
```
router(config)#ip ips notify sdee
```

   Para utilizar SDEE, el servidor HTTP debe estar habilitado (con el comando **ip http server**). Si el servidor HTTP no está habilitado, el router no puede responder a los clientes SDEE porque no puede ver las solicitudes. La notificación SDEE está desactivada de forma predeterminada y debe estar habilitada explícitamente.IOS IPS también soporta el uso de syslog para enviar la notificación de eventos. SDEE y syslog se pueden utilizar de forma independiente o habilitada al mismo tiempo para enviar la notificación de eventos IPS de IOS. La notificación Syslog está habilitada de forma predeterminada. Si la consola de registro está habilitada, verá los mensajes de syslog IPS. Para habilitar syslog, utilice este comando:
```
router(config)#ip ips notify log
```

4. Configure IOS IPS para utilizar una de las categorías de firma predefinidas.IOS IPS con firmas de formato Cisco 5.x funciona con categorías de firmas (al igual que los dispositivos Cisco IPS). Todas las firmas se agrupan en categorías y las categorías son jerárquicas. Esto ayuda a clasificar las firmas para facilitar la agrupación y el ajuste.**Advertencia:** La categoría *de* firma contiene todas las firmas en una versión de firma. Dado que IOS IPS no puede compilar y utilizar todas las firmas contenidas en una versión de firma al mismo tiempo, *no anule la eliminación de todas las categorías*; de lo contrario, el router se quedará sin memoria.**Nota:** Al configurar IOS IPS, primero debe retirar todas las firmas de la categoría *all* y, a continuación, anular la retirada de las categorías de firma seleccionadas.**Nota:** El orden en que se configuran las categorías de firma en el router también es importante. IOS IPS procesa los comandos de categoría en el orden indicado en la configuración. Algunas firmas pertenecen a varias categorías. Si se configuran varias categorías y una firma pertenece a más de una de ellas, las propiedades de la firma (por ejemplo, retiradas, no retiradas, acciones, etc.) en la última categoría configurada son utilizadas por IOS IPS.En este ejemplo, todas las firmas de la categoría "all" se retiran y, a continuación, la categoría *IOS IPS Basic* no se retira.
```
router(config)#ip ips signature-category
router(config-ips-category)#category all
router(config-ips-category-action)#retired true
router(config-ips-category-action)#exit
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```
5. Utilice estos comandos para habilitar la regla IPS en la interfaz deseada y especifique la dirección en la que se aplicará la regla:**interface <*interface name*>ip ips <*rule name*> [*in* | *out*]**Por ejemplo:
```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#exit
router(config)#exit
router#
```
El argumento *in* significa que el IPS sólo inspecciona el tráfico que entra en la interfaz. El argumento *out* significa que el IPS sólo inspecciona el tráfico que sale de la interfaz.Para permitir que IPS inspeccione tanto el tráfico de entrada como de salida de la interfaz, ingrese separadamente el nombre de regla IPS para *el* entrada y *salida* en la misma interfaz:
```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#ip ips iosips out
router(config-if)#exit
router(config)#exit
router#
```

Paso 5. Carga del Paquete de Firma IPS de IOS al Router

El último paso es cargar al router el paquete de firma descargado en el Paso 1.

Nota: La forma más común de cargar el paquete de firma al router es utilizar FTP o TFTP. Este procedimiento utiliza FTP. Consulte la sección *Comandos y Referencias Adicionales* en este procedimiento para ver un método alternativo para cargar el paquete de firma IPS de IOS. Si utiliza una sesión telnet, utilice el comando **terminal monitor** para ver los resultados de la consola.

Para cargar el paquete de firma en el router, complete estos pasos:

1. Utilice este comando para copiar el paquete de firma descargado del servidor FTP al router:**copy ftp://<*ftp_user:password@Server_IP_address* >/<*Signature_package*> idconfNota:** Recuerde utilizar el parámetro *idconf al final del comando copy*.**Nota:** Por ejemplo:
```
router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```
La compilación de firmas comienza inmediatamente después de que el paquete de firmas se cargue en el router. Puede ver los registros en el router con el nivel de registro 6 o superior habilitado.
```
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Feb 14 2008
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures -
                      1 of 13 engines
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms -
                      packets for this engine will be scanned
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures -
                      2 of 13 engines
*Feb 14 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms -
                      packets for this engine will be scanned
|
output snipped
|
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures -
                      12 of 13 engines
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms -
                      packets for this engine will be scanned
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures -
                      13 of 13 engines
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms -
                      packets for this engine will be scanned
*Feb 14 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```
2. Utilice el comando **show ip ips Signature count** para verificar que el paquete de firma esté correctamente compilado.Por ejemplo:
```
router#show ip ips signature count
Cisco SDF release version S310.0  signature package release version
Trend SDF release version V0.0
Signature Micro-Engine: multi-string: Total Signatures 8
multi-string enabled signatures: 8
multi-string retired signatures: 8
|
outpt snipped
|
Signature Micro-Engine: service-msrpc: Total Signatures 25
service-msrpc enabled signatures: 25
service-msrpc retired signatures: 18
service-msrpc compiled signatures: 1
service-msrpc inactive signatures - invalid params: 6
Total Signatures: 2136
Total Enabled Signatures: 807
Total Retired Signatures: 1779
Total Compiled Signatures:
      351  total compiled signatures for the IOS IPS Basic category
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
router#
```

Comandos y referencias adicionales

La clave criptográfica pública no es válida si recibe un mensaje de error en el momento de la

compilación de la firma similar a este mensaje de error:

```
%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)
```

Consulte Paso 3 para obtener más información.

Si no tiene acceso a un servidor FTP o TFTP, puede utilizar una unidad flash USB para cargar el paquete de firma al router. Primero, copie el paquete de firma en la unidad USB, conecte la unidad USB a uno de los puertos USB del router y luego use el comando **copy** con el parámetro *idconf* para copiar el paquete de firma al router.

Por ejemplo:

```
router#copy usbflash1:IOS-S310-CLI.pkg idconf
```

Hay seis archivos en el directorio de almacenamiento IOS IPS configurado. Estos archivos utilizan este formato de nombre: <*router-name*>-sigdef-xxx.xml o <*router-name*>-seap-xxx.xml.

```
router#dir ips
Directory of flash:/ips/
7 -rw- 203419 Feb 14 2008 16:45:24 -08:00 router-sigdef-default.xml
8 -rw- 271 Feb 14 2008 16:43:36 -08:00 router-sigdef-delta.xml
9 -rw- 6159 Feb 14 2008 16:44:24 -08:00 router-sigdef-typedef.xml
10 -rw- 22873 Feb 14 2008 16:44:26 -08:00 router-sigdef-category.xml
11 -rw- 257 Feb 14 2008 16:43:36 -08:00 router-seap-delta.xml
12 -rw- 491 Feb 14 2008 16:43:36 -08:00 router-seap-typedef.xml
64016384 bytes total (12693504 bytes free)
router#
```

Estos archivos se almacenan en formato comprimido y no se pueden editar ni ver directamente. A continuación se describe el contenido de cada archivo:

- *router-sigdef-default.xml* contiene todas las definiciones de firma predeterminadas de fábrica.
- *router-sigdef-delta.xml* contiene definiciones de firma que se han cambiado desde el valor predeterminado.
- *router-sigdef-typedef.xml* contiene todas las definiciones de parámetros de firma.
- *router-sigdef-category.xml* contiene la información de la categoría de firma, como category ios_ips basic y advanced.
- *router-seap-delta.xml* contiene los cambios realizados a los parámetros SEAP predeterminados.
- *router-seap-typedef.xml* contiene todas las definiciones de parámetros SEAP.

Sección II. Opciones de configuración avanzadas

Esta sección proporciona instrucciones y ejemplos sobre las opciones IPS de IOS avanzadas para el ajuste de firmas.

Retirar o anular la retirada de las firmas

Para retirar o anular la retirada de una firma, significa seleccionar o anular la selección de las

firmas que utiliza IOS IPS para analizar el tráfico.

- **Retirando** una firma significa que IOS IPS *NO* compilará esa firma en la memoria para el escaneo.
- **Al retirar** una firma, se indica a IOS IPS que compile la firma en la memoria y que utilice la firma para analizar el tráfico.

Puede utilizar la interfaz de línea de comandos (CLI) de IOS para retirar o anular la retirada de firmas individuales o de un grupo de firmas que pertenecen a una categoría de firma. Cuando se retira o se retira un grupo de firmas, todas las firmas de esa categoría se retiran o se retiran.

Nota: Es posible que algunas firmas no retiradas (ya sea no retiradas como firma individual o dentro de una categoría no jubilada) no se compilen debido a la memoria insuficiente o a parámetros no válidos o si la firma ha quedado obsoleta.

Este ejemplo muestra cómo retirar firmas individuales. Por ejemplo, firma 6130 con ID de brote de 10:

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status
router(config-sigdef-sig-status)#retired true
router(config-sigdef-sig-status)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

Este ejemplo muestra cómo retirar todas las firmas que pertenecen a la categoría IOS IPS Basic:

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
```

Nota: Cuando las firmas en categorías distintas de IOS IPS Basic e IOS IPS Advanced no se retiran como categoría, la compilación de algunas firmas o motores podría fallar porque ciertas firmas en esas categorías no son compatibles con IOS IPS (consulte el ejemplo a continuación). El IPS de IOS utiliza todas las demás firmas compiladas correctamente (no retiradas) para analizar el tráfico.

```
Router(config)#ip ips signature-category
router(config-ips-category)#category os
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
*Feb 14 18:10:46 PST: Applying Category configuration to signatures ...
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDS_STARTED: 08:10:49 PST Feb 18 2008
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures -
```

```
                      1 of 13 engines
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_READY: multi-string - build time 136 ms -
                      packets for this engine will be scanned
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures -
                      2 of 13 engines
*Feb 14 18:10:50 PST: %IPS-4-META_ENGINE_UNSUPPORTED: service-http 5903:1 -
                      this signature is a component of the unsupported META engine
*Feb 14 18:24:42 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5754:0 -
                      compilation of regular expression failed
*Feb 14 18:24:49 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5729:1 -
                      compilation of regular expression failed
```

Activar o desactivar firmas

Para habilitar o inhabilitar una firma es aplicar o ignorar las acciones asociadas con las firmas por el IPS de IOS cuando el flujo de paquetes o paquetes coincide con las firmas.

Nota: Enable and disable NO selecciona y anula la selección de las firmas que utilizará IOS IPS.

- Para **Habilitar** una firma significa que cuando se activa por un paquete coincidente (o flujo de paquetes), la firma toma la acción apropiada asociada con ella. Sin embargo, solo las firmas sin retirar Y compiladas correctamente tomarán la acción cuando estén habilitadas. En otras palabras, si se retira una firma, aunque esté habilitada, no se compilará (porque se retira) y no realizará la acción asociada con ella.
- Para **Deshabilitar** una firma significa que cuando se activa por un paquete coincidente (o flujo de paquetes), la firma NO realiza la acción adecuada asociada con ella. En otras palabras, cuando una firma se inhabilita, aunque no se retira y se compila correctamente, no realiza la acción asociada.

Puede utilizar la interfaz de línea de comandos (CLI) de IOS para habilitar o deshabilitar firmas individuales o un grupo de firmas basado en categorías de firma. Este ejemplo muestra cómo inhabilitar la firma 6130 con el ID de seguimiento de 10.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status
router(config-sigdef-sig-status)#enabled false
router(config-sigdef-sig-status)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

Este ejemplo muestra cómo habilitar todas las firmas que pertenecen a la categoría IOS IPS Basic.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#enabled true
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

Cambiar acciones de firma

Puede utilizar la interfaz de línea de comandos (CLI) de IOS para cambiar las acciones de firma para una firma o un grupo de firmas basándose en las categorías de firma. Este ejemplo muestra cómo cambiar las acciones de firma para alertar, descartar y restablecer para la firma 6130 con ID de sondeo de 10.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#engine
router(config-sigdef-sig-engine)#event-action produce-alert
router(config-sigdef-sig-engine)#event-action deny-packet-inline
router(config-sigdef-sig-engine)#event-action reset-tcp-connection
router(config-sigdef-sig-engine)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

Este ejemplo muestra cómo cambiar las acciones de evento para todas las firmas que pertenecen a la categoría IOS IPS Basic de la firma.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#event-action produce-alert
router(config-ips-category-action)#event-action deny-packet-inline
router(config-ips-category-action)#event-action reset-tcp-connection
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

Información Relacionada

- Página de productos y servicios de Cisco IOS Intrusion Prevention System (IPS)
- Descarga de software de Cisco IOS IPS - Versión 5
- Compatibilidad con formato de firma IPS 5.x y mejoras de uso
- Descarga de software del administrador de dispositivos de seguridad de Cisco
- Cómo Utilizar CCP para Configurar IOS IPS
- Descarga de software criptográfico 3DES del Visor de eventos del sistema de detección de intrusiones de Cisco
- Soporte Técnico y Documentación - Cisco Systems