Sistema de prevención de intrusiones con el ejemplo de configuración de las firmas del formato 5.x

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Pasos para la configuración de la introducción de la sección I.
Paso 1. Archivos IOS IPS de la descarga
Paso 2. Cree un directorio de configuración IOS IPS en el Flash
Paso 3. Configure un crypto key IOS IPS
Paso 4. IOS IPS del permiso
Paso 5. Cargue el paquete de la firma IOS IPS al router
Opciones de configuración avanzada de la sección II.
Las firmas retírese o de Unretire
Firmas del permiso o de la neutralización
Cambie las acciones de la firma
Información Relacionada

Introducción

Este documento describe cómo configurar las firmas del formato 5.x en el ® IPS del Cisco IOS y se ordena en dos secciones:

- Pasos para la configuración de la introducción de la sección I. — Esta sección proporciona los pasos necesarios utilizar el comando line interface(cli) del Cisco IOS para conseguir comenzada con las firmas del formato IOS IPS 5.x. Esta sección describe estos pasos:Paso 1. Descargue los archivos IOS IPS.Paso 2. Cree un directorio de configuración IOS IPS en el Flash.Paso 3. Configure un crypto key IOS IPS.Paso 4. IOS IPS del permiso.Paso 5. Cargue el paquete de la firma IOS IPS al router.Cada paso y comandos específicos se describen detalladamente, así como los comandos adicionales y las referencias. Un ejemplo de configuración se visualiza debajo de cada comando.
- Opciones de configuración avanzada de la sección II. — Esta sección proporciona las instrucciones y los ejemplos en las opciones avanzadas para ajustar de la firma. Contiene estas opciones:Retírese o las firmas de UnretireHabilite o inhabilite las firmasCambie las acciones de la firma

prerrequisitos

Requisitos

Asegúrese que usted tenga los componentes apropiados (según lo descrito en los componentes usados) antes de que usted complete los pasos en este documento.

Componentes Utilizados

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

- Un router de los Servicios integrados de Cisco (87x, 18xx, 28xx, o 38xx)
- 128MB o más memoria Flash libre DRAM y por lo menos 2MB
- Conectividad de la consola o telnet al router
- Cisco IOS Release 12.4(15)T3 o Posterior
- Un nombre y una contraseña válidos de usuario que ingresa al sistema CCO (cisco.com)
- Un contrato de servicio actual del IPS de Cisco para los servicios autorizados de la actualización de firma

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.

Seccione los pasos para la configuración de la introducción I.

Paso 1. Archivos IOS IPS de la descarga

El primer paso es descargar los archivos de paquete de la firma IOS IPS y el crypto key público del cisco.com.

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

- Ubicación: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (clientes registrados solamente)
- Archivos a descargar:IOS-Sxxx-CLI.pkg (registeredcustomers solamente) — Éste es el último paquete de la firma.realm-cisco.pub.key.txt (clientes registrados solamente) — Éste es el crypto key público usado por IOS IPS.

Paso 2. Cree un directorio de configuración IOS IPS en el Flash

El segundo paso es crear un directorio en el flash de su router donde usted salva los archivos de

firma y las configuraciones requeridos. Alternativamente, usted puede utilizar memoria USB de Cisco conectada con el puerto USB del router para salvar los archivos de firma y las configuraciones. Memoria USB debe seguir conectada con el puerto USB del router si se utiliza como la ubicación del directorio de configuración IOS IPS. El IOS IPS también soporta cualquier archivo de sistema de IOS como su ubicación de la configuración con el acceso de escritura apropiado.

Para crear un directorio, ingrese este comando en el prompt de router: *name*> **<directory del mkdir**

Por ejemplo:

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

Comandos adicionales y referencias

Para verificar el contenido del flash, ingrese este comando en el prompt de router: **flash de la demostración:**

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 retitular Directory Name (Nombre de directorio), utilice este comando: **retitule el** *name*> **<current del <new del** *name*>

Por ejemplo:

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

Paso 3. Configure un crypto key IOS IPS

El tercer paso es configurar el crypto key usado por IOS IPS. Esta clave está situada en el archivo de realm-cisco.pub.key.txt que fue descargado en el paso 1.

El crypto key se utiliza para verificar la firma digital para el archivo de firma principal (sigdef-default.xml) cuyo contenido es firmado por una clave privada de Cisco para garantizar su autenticidad y integridad en cada versión.

1. Abra el archivo de texto, y copie el contenido del archivo.
2. Utilice el **comando configure terminal** para ingresar el modo de la configuración del router.
3. Pegue el contenido del archivo de texto en el prompt del `<hostname>(config)#`.
4. Dé salida al modo de configuración del router.
5. Ingrese el **comando show run** en el prompt de router para confirmar que el crypto key está configurado. Usted debe ver esta salida 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:**copie la lanzamiento-configuración de la ejecutar-configuración**

Comandos adicionales y referencias

Si la clave se configura incorrectamente, usted debe quitar el crypto key primero y en seguida configurarlo de nuevo:

1. Para quitar la clave, ingrese estos comandos en la orden enumerada abajo:`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 está quitada de la configuración.
3. Complete el procedimiento en el paso 3 para configurar de nuevo la clave.

Paso 4. IOS IPS del permiso

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

1. Utilice el comando del *name>* **<** *ACL opcional* **> del <rule del nombre IPS del IP** para crear un nombre de la regla. (Esto será utilizada en una interfaz para habilitar el IPS.)Por ejemplo:`router#`**`configure terminal`** `router(config)#`**`ip ips name iosips`** Usted puede especificar un Access Control List extendido o estándar opcional (ACL) para filtrar el tráfico que será analizado por este nombre de la regla. Todo el tráfico que es permitido por el ACL está conforme al examen por el IPS. Trafique que es negado por el ACL no es examinado por el IPS.`router(config)#`**`ip ips name ips list ?`** `<1-199> Numbered access list WORD Named access list`
2. Utilice el **flash de la ubicación de los config IPS del IP:** comando **<directory del** *name>* para configurar la ubicación de almacenamiento de la firma IPS. (Éste es el directorio *IPS* creado en el paso 2.)Por ejemplo:`router(config)#`**`ip ips config location flash:ips`**
3. Utilice el **IP IPS notifican el** comando del **sdee** para habilitar la notificación de evento IPS SDEE.Por ejemplo:`router(config)#`**`ip ips notify sdee`** Para utilizar SDEE, el servidor HTTP debe ser habilitado (con el **comando ip http server**). Si no habilitan al servidor HTTP, el router no puede responder a los clientes SDEE porque no puede ver las peticiones. La notificación SDEE se inhabilita por abandono y debe ser habilitada explícitamente.El IOS IPS también soporta el uso del Syslog para enviar la notificación de evento. SDEE y el Syslog se pueden utilizar independientemente o habilitar al mismo tiempo para enviar la notificación de evento IOS IPS. La notificación de Syslog se habilita por abandono. Si se habilita la consola de registro, usted verá los mensajes de Syslog IPS. Para habilitar el Syslog, utilice este comando:`router(config)#`**`ip ips notify log`**
4. Configure IOS IPS para utilizar una de las categorías predefinidas de la firma.El IOS IPS con las firmas del formato de Cisco 5.x actúa con las categorías de la firma (apenas como los dispositivos del IPS de Cisco). Todas las firmas se agrupan en las categorías, y las categorías son jerárquicas. Esto ayuda a clasificar las firmas para agrupar y ajustar fáciles.**Advertencia:** *Toda la* categoría de la firma contiene todas las firmas en una versión de la firma. Puesto que el IOS IPS no puede compilar y utilizar todas las firmas contenidas en una firma libere al mismo tiempo, *no hace el unretire toda la categoría*; si no, el router se ejecutará de la memoria.**Nota:** Cuando usted configura IOS IPS, usted debe primero retirar

todas las firmas en *toda la* categoría, y entonces el unretire seleccionó las categorías de la firma.**Nota:** La orden en la cual las categorías de la firma se configuran en el router es también importante. El IOS IPS procesa los comandos de la categoría en la orden enumerada en la configuración. Algunas firmas pertenecen a las categorías múltiples. Si se configuran las categorías múltiples y una firma pertenece a más de una de ellas, las propiedades de la firma (por ejemplo, retirado, unretired, las acciones, etc.) en la categoría configurada último son utilizadas por IOS IPS.En este ejemplo, todas las firmas en “toda la” categoría se retiran, y entonces la *categoría básica IOS IPS* unretired.`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 cual la regla será aplicada:**interfaz <interface name>***name> del* **<rule IPS del IP [***en | hacia fuera***]**Por ejemplo:`router(config)#interface GigabitEthernet 0/1 router(config-if)#ip ips iosips in router(config-if)#exit router(config)#exit router#` *En el* argumento significa que solamente el tráfico que entra la interfaz es examinado por el IPS. El argumento de la *salida* significa que solamente la salida del tráfico de la interfaz es examinada por el IPS.Para permitir al IPS para examinar ambos en y hacia fuera el tráfico de la interfaz, ingrese por separado el nombre de la regla IPS para *adentro* y *hacia fuera* en lo mismo interconecte:`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. Cargue el paquete de la firma IOS IPS al router

El paso más reciente es cargar al router que el paquete de la firma descargó en el paso 1.

Nota: La mayoría de la manera común de cargar el paquete de la firma al router es utilizar el FTP o el TFTP. Este procedimiento utiliza el FTP. Refiera por favor a la sección de los *comandos adicionales y de referencias* en este procedimiento para que un método alternativo cargue el paquete de la firma IOS IPS. Si usted utiliza a una sesión telnet, utilice el **comando terminal monitor** para ver las salidas de la consola.

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

1. Utilice este comando para copiar el paquete descargado de la firma del servidor FTP al router:**copie el <ftp_user de ftp://***: idconf de password@Server_IP_address* **>/<signature_package>Nota:** Recuerde por favor utilizar el parámetro del *idconf* en el extremo 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 firma que compila comienza inmediatamente después que el paquete de la firma se carga al router. Usted puede ver que abre una sesión al router con el nivel de registro 6 o habilitado antedicho.`*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 count de la firma IPS del IP de la demostración** para verificar el paquete de la firma se compila correctamente.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 adicionales y referencias

El crypto key público es inválido si usted recibe un mensaje de error a la hora de la compilación de la firma similar a este mensaje de error:

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

Refiera al paso 3 para más información.

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

Por ejemplo:

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

Hay seis archivos en el directorio configurado del almacenamiento IOS IPS. Estos archivos utilizan este formato del nombre: <router-nombre >-sigdef-xxx.xml o < nombre del router *>-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 salvan en el formato comprimido y no son directamente editable o viewable. El contenido de cada archivo es descrito más abajo:

- *router-sigdef-default.xml contiene* todas las definiciones de la firma del valor predeterminado de fábrica.
- *router-sigdef-delta.xml contiene las* definiciones de la firma que se han cambiado del valor por defecto.

- *router-sigdef-typedef.xml contiene* todas las Definiciones del parámetro de la firma.
- *router-sigdef-category.xml contiene la* información de la categoría de la firma, tal como ios_ips de la categoría básicos y avanzados.
- *router-seap-delta.xml contiene los* cambios realizados a los parámetros del valor por defecto SEAP.
- *router-seap-typedef.xml contiene* todas las Definiciones del parámetro SEAP.

Opciones de configuración avanzada de la sección II.

Esta sección proporciona las instrucciones y los ejemplos en las opciones avanzadas IOS IPS para ajustar de la firma.

Las firmas retírese o de Unretire

Para retirarse o unretire medios de una firma de seleccionar o de no reelegir como candidato las firmas que son utilizadas por IOS IPS para analizar el tráfico.

- **Retirar una** firma significa que el IOS IPS no compilará esa firma en la memoria para analizar.
- **Unretiring una** firma da instrucciones IOS IPS para compilar la firma en la memoria y para utilizar la firma para analizar el tráfico.

Usted puede utilizar el comando line interface(cli) IOS para las firmas individuales retirarse o de unretire o un grupo de firmas que pertenezcan a una categoría de la firma. Cuando usted se retira o unretire al grupo de firmas, todas las firmas en esa categoría se retiran o unretired.

Nota: Algunas firmas unretired (unretired como firma individual o dentro de una categoría unretired) pueden no compilar debido a memoria insuficiente o a los parámetros inválidos o si la firma obsoleted.

Este ejemplo muestra cómo retirar las firmas individuales. Por ejemplo, firma 6130 con el subsig ID 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 al unretire todas las firmas que pertenecen a la categoría básica IOS IPS:

```
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 las categorías con excepción de IOS IPS básico y de IOS IPS avanzado unretired como categoría, la compilación de algunas firmas o motores podría fallar porque ciertas firmas en esas categorías no son soportadas por IOS IPS (véase el ejemplo abajo). Todo el otro las firmas (unretired) con éxito compiladas es utilizado por IOS IPS 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
```

Firmas del permiso o de la neutralización

Para habilitar o inhabilitar una firma es aplicar o desatender las acciones asociadas a las firmas por IOS IPS cuando el paquete o el flujo de paquetes hace juego las firmas.

Nota: El permiso y la neutralización no selecciona y no reelige como candidato las firmas para ser utilizado por IOS IPS.

- Para **habilitar una** firma significa que cuando es accionada por un paquete que corresponde con (o el flujo de paquetes), la firma toma la acción apropiada asociada a ella. Sin embargo, solamente las firmas unretired Y con éxito compiladas tomarán medidas cuando se habilitan. Es decir si se retira una firma, aunque se habilita, no serán compiladas (porque se retiran) y no tomarán medidas asociadas a ellas.
- Para **inhabilitar una** firma significa que cuando es accionada por un paquete que corresponde con (o el flujo de paquetes), la firma no toma la acción apropiada asociada a ella. Es decir cuando se inhabilita una firma, aunque unretired y se compila con éxito, no tomará medidas asociadas a él.

Usted puede utilizar el comando line interface(cli) IOS para habilitar o inhabilitar las firmas individuales o un grupo de firmas basadas en las categorías de la firma. Este ejemplo muestra cómo inhabilitar la firma 6130 con el subsig ID 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 pertenezcan a la categoría básica IOS IPS.

```
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)#
```

Cambie las acciones de la firma

Usted puede utilizar el comando line interface(cli) IOS para cambiar las acciones de la firma para una firma o un grupo de firmas basadas en las categorías de la firma. Este ejemplo muestra cómo cambiar las acciones de la firma para alertar, para caer, y la restauración para la firma 6130 con el subsig ID 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 del evento para todas las firmas que pertenezcan a la categoría básica IOS IPS 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 los Productos y de los servicios del Cisco IOS Intrusion Prevention System (IPS)
- Cisco IOS IPS - Descarga del software de las firmas de la versión 5
- IPS mejoras de soporte y de la utilidad del formato de la firma 5.x
- Descarga del software del administrador de dispositivo Security de Cisco
- Cómo utilizar el CCP para configurar IOS IPS
- Descarga de Software criptográfico del visor de eventos 3DES del Sistema de detección de intrusos de Cisco
- Soporte Técnico y Documentación - Cisco Systems