Configurazione di IPS con firme di formato 5.x

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Sezione I. Fasi preliminari della configurazione](#)
[Passaggio 1. Scaricare i file IPS di IOS](#)
[Passaggio 2. Creare una directory di configurazione IPS IOS su Flash](#)
[Passaggio 3. Configurare una chiave di crittografia IPS IOS](#)
[Passaggio 4. Abilitare IPS IOS](#)
[Passaggio 5. Caricare il pacchetto della firma IPS IOS sul router](#)
[Sezione II. Opzioni di configurazione avanzate](#)
[Ritira o Annulla ritiro firme](#)
[Attivare o disattivare le firme](#)
[Modifica azioni firma](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare le firme in formato 5.x in Cisco IOS® IPS ed è suddiviso in due sezioni:

- Sezione I. Fasi della configurazione iniziale: in questa sezione vengono illustrati i passaggi necessari per utilizzare l'interfaccia della riga di comando (CLI) di Cisco IOS e iniziare a utilizzare le firme del formato IPS 5.x di IOS. In questa sezione vengono descritti i passaggi seguenti:Passaggio 1. Scaricare i file IPS di IOS.Passaggio 2. Creare una directory di configurazione IPS IOS su Flash.Passaggio 3. Configurare una chiave di crittografia IPS IOS.Passaggio 4. Abilitare IPS IOS.Passaggio 5. Caricare il pacchetto di firma IPS IOS sul router.Ogni passo e i comandi specifici sono descritti in dettaglio, insieme a comandi e riferimenti aggiuntivi. Sotto ciascun comando viene visualizzato un esempio di configurazione.
- Sezione II. Opzioni di configurazione avanzate: in questa sezione vengono fornite istruzioni ed esempi sulle opzioni avanzate per il tuning delle firme. Contiene le opzioni seguenti:Ritira o Annulla ritiro firmeAttivare o disattivare le firmeModifica azioni firma

Prerequisiti

Requisiti

Assicurarsi di disporre dei componenti corretti (come descritto in Componenti usati) prima di completare la procedura descritta in questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Un router di servizi integrati Cisco (87x, 18xx, 28xx o 38xx)
- almeno 128 MB di DRAM e almeno 2 MB di memoria flash libera
- Connettività console o telnet al router
- Cisco IOS release 12.4(15)T3 o successive
- Nome utente e password di accesso CCO (Cisco.com) validi
- Contratto di servizio IPS Cisco corrente per servizi di aggiornamento della firma con licenza

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Sezione I. Fasi preliminari della configurazione

Passaggio 1. Scaricare i file IPS di IOS

Il primo passaggio consiste nel scaricare i file del pacchetto della firma IPS di IOS e la chiave di crittografia pubblica da Cisco.com.

Scaricare i file della firma richiesti da Cisco.com sul PC:

- Percorso: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (solo utenti registrati)
- File da scaricare:IOS-Sxxx-CLI.pkg (solo utenti registrati): è l'ultimo pacchetto di firme.realm-cisco.pub.key.txt (solo utenti registrati): chiave crittografica pubblica utilizzata da IOS IPS.

Passaggio 2. Creare una directory di configurazione IPS IOS su Flash

Il secondo passaggio consiste nel creare una directory sul flash del router in cui memorizzare i file della firma e le configurazioni richieste. In alternativa, è possibile utilizzare un'unità flash USB Cisco collegata alla porta USB del router per archiviare i file di firma e le configurazioni. L'unità flash USB deve rimanere collegata alla porta USB del router se viene utilizzata come percorso della directory di configurazione IPS di IOS. IOS IPS supporta inoltre qualsiasi file system IOS come posizione di configurazione con accesso in scrittura appropriato.

Per creare una directory, immettere questo comando al prompt del router: **mkdir <*nome directory*>**

Ad esempio:

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

Ulteriori comandi e riferimenti

Per verificare il contenuto della memoria flash, immettere questo comando al prompt del router: **show flash:**

Ad esempio:

```
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)
```

Per rinominare la directory, utilizzare questo comando: **rename <*nome corrente*> <*nuovo nome*>**

Ad esempio:

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

Passaggio 3. Configurare una chiave di crittografia IPS IOS

Il terzo passaggio consiste nella configurazione della chiave crittografica utilizzata da IOS IPS. Questa chiave si trova nel file realm-cisco.pub.key.txt scaricato nel passaggio 1.

La chiave crittografica viene utilizzata per verificare la firma digitale del file della firma master (sigdef-default.xml) il cui contenuto è firmato da una chiave privata Cisco per garantirne l'autenticità e l'integrità in ogni versione.

1. Aprire il file di testo e copiare il contenuto del file.
2. Usare il comando **configure terminal** per accedere alla modalità di configurazione del router.
3. Incollare il contenuto del file di testo al prompt `<hostname>(config)#`.
4. Uscire dalla modalità di configurazione del router.
5. Immettere il comando **show run** al prompt del router per confermare che la chiave crittografica è configurata. Nella configurazione dovrebbe essere visualizzato questo output:
   ```
   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. Per salvare la configurazione, usare questo comando:**copy running-configure startup-**

configure

Ulteriori comandi e riferimenti

Se la chiave non è configurata correttamente, è necessario rimuovere prima la chiave crittografica e quindi riconfigurarla:

1. Per rimuovere la chiave, immettere questi comandi nell'ordine indicato di seguito:
```
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. Per verificare che la chiave sia stata rimossa dalla configurazione, usare il comando **show run**.
3. Completare la procedura descritta nel passaggio 3 per riconfigurare la chiave.

Passaggio 4. Abilitare IPS IOS

Il quarto passaggio consiste nella configurazione di IPS IOS. Completare questa procedura per configurare IOS IPS:

1. Per creare un nome di regola, usare il comando **ip ips name <*nome regola*> < *ACL facoltativo*>**. (da utilizzare su un'interfaccia per abilitare IPS).Ad esempio:
```
router#configure terminal
router(config)#ip ips name iosips
```

   Èpossibile specificare un elenco di controllo di accesso (ACL) standard o esteso facoltativo per filtrare il traffico che verrà analizzato in base a questo nome di regola. Tutto il traffico autorizzato dall'ACL è soggetto a ispezione da parte dell'IPS. Il traffico negato dall'ACL non viene ispezionato dall'IPS.
```
router(config)#ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
```
2. Per configurare il percorso di archiviazione delle firme IPS, usare il comando **ip ips config location flash:<*directory name*>**. Questa è la directory *ips* creata nel passo 2.Ad esempio:
```
router(config)#ip ips config location flash:ips
```

3. Per abilitare la notifica degli eventi IPS SDEE, usare il comando **ip ips ify side**.Ad esempio:
```
router(config)#ip ips notify sdee
```

   Per utilizzare SDEE, il server HTTP deve essere abilitato (con il comando **ip http server**). Se il server HTTP non è abilitato, il router non può rispondere ai client SDEE perché non può visualizzare le richieste. La notifica SDEE è disattivata per impostazione predefinita e deve essere attivata in modo esplicito.IOS IPS supporta anche l'uso di syslog per inviare la notifica degli eventi. SDEE e syslog possono essere utilizzati in modo indipendente o abilitati contemporaneamente per inviare la notifica degli eventi IPS IOS. La notifica Syslog è attivata per impostazione predefinita. Se la console di registrazione è abilitata, verranno visualizzati messaggi syslog IPS. Per abilitare syslog, utilizzare questo comando:
```
router(config)#ip ips notify log
```

4. Configurare IPS IOS per l'utilizzo di una delle categorie di firma predefinite.IOS IPS con firme di formato Cisco 5.x funziona con categorie di firma (proprio come le appliance Cisco IPS). Tutte le firme sono raggruppate in categorie gerarchiche. In questo modo è possibile classificare le firme per semplificare il raggruppamento e l'ottimizzazione.**Avviso:** la categoria *Tutte le* firme contiene tutte le firme di una versione di firma. Poiché IOS IPS non è in grado di compilare e utilizzare contemporaneamente tutte le firme contenute in una versione di firma, *non ritirare la categoria all*; in caso contrario, la memoria del router si esaurisce.**Nota:** quando si configura IPS IOS, è necessario prima ritirare tutte le firme nella categoria *all* e quindi annullare il ritiro delle categorie di firma selezionate.**Nota:** anche l'ordine in cui vengono configurate le categorie di firma sul router è importante. IOS IPS elabora i comandi delle categorie nell'ordine elencato nella configurazione. Alcune firme appartengono a più categorie. Se sono configurate più categorie e una firma appartiene a più di una di esse, le proprietà della firma (ad esempio, ritirata, non ritirata, azioni e così via) nell'ultima categoria configurata vengono utilizzate da IPS IOS.In questo esempio, tutte le firme della categoria "all" vengono ritirate, quindi la categoria *IOS IPS Basic* viene annullata.
```
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. Utilizzare questi comandi per abilitare la regola IPS sull'interfaccia desiderata e specificare la direzione di applicazione della regola:**interface <*nome interfaccia*>ip ips <*nome regola*> [*in | fuori*]**Ad esempio:
```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#exit
router(config)#exit
router#
```
L'argomento *in* indica che solo il traffico che entra nell'interfaccia viene ispezionato da IPS. L'argomento *out* indica che solo il traffico in uscita dall'interfaccia viene ispezionato da IPS.Per consentire all'IPS di ispezionare sia il traffico in entrata che in uscita dall'interfaccia, immettere separatamente il nome della regola IPS per *in* entrata e *in uscita* sulla stessa interfaccia:
```
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#
```

Passaggio 5. Caricare il pacchetto della firma IPS IOS sul router

L'ultimo passaggio consiste nel caricare sul router il pacchetto di firma scaricato nel passaggio 1.

Nota: il modo più comune per caricare il pacchetto di firma sul router è usare l'FTP o il TFTP. In questa procedura viene utilizzato il protocollo FTP. Per un metodo alternativo per caricare il pacchetto della firma IPS di IOS, consultare la sezione *Altri comandi e riferimenti* di questa procedura. Se si usa una sessione telnet, usare il comando **terminal monitor** per visualizzare gli

output della console.

Per caricare il pacchetto di firma sul router, attenersi alla seguente procedura:

1. Per copiare il pacchetto della firma scaricato dal server FTP al router, usare questo comando:**copy ftp://<*ftp_user:password@Server_IP_address*>/<*signature_package*> idconfNota:** utilizzare il parametro *idconf* alla fine del comando **copy**.**Nota:** ad esempio:
```
router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```
La compilazione della firma inizia immediatamente dopo il caricamento del pacchetto di firma sul router. È possibile visualizzare i log sul router con il livello di log 6 o superiore abilitato.
```
*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. Per verificare che il pacchetto della firma sia compilato correttamente, usare il comando **show ip ips signature count**.Ad esempio:
```
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#
```

Ulteriori comandi e riferimenti

La chiave crittografica pubblica non è valida se si riceve un messaggio di errore simile al seguente

al momento della compilazione della firma:

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

Per ulteriori informazioni, fare riferimento al passo 3.

Se non si dispone dell'accesso a un server FTP o TFTP, è possibile utilizzare un'unità flash USB per caricare il pacchetto della firma sul router. Copiare innanzitutto il pacchetto della firma nell'unità USB, collegare l'unità USB a una delle porte USB sul router e quindi utilizzare il comando **copy** con il parametro *idconf* per copiare il pacchetto della firma sul router.

Ad esempio:

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

La directory di archiviazione IPS IOS configurata contiene sei file. Questi file utilizzano questo formato nome: <*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#
```

Questi file vengono memorizzati in formato compresso e non sono direttamente modificabili o visualizzabili. Di seguito è descritto il contenuto di ciascun file:

- *router-sigdef-default.xml* contiene tutte le definizioni di firma predefinite in fabbrica.
- *router-sigdef-delta.xml* contiene le definizioni di firma modificate rispetto a quelle predefinite.
- *router-sigdef-typedef.xml* contiene tutte le definizioni dei parametri di firma.
- *router-sigdef-category.xml* contiene le informazioni relative alla categoria della firma, ad esempio la categoria ios_ips basic e advanced.
- *router-seap-delta.xml* contiene le modifiche apportate ai parametri SEAP predefiniti.
- *router-seap-typedef.xml* contiene tutte le definizioni dei parametri SEAP.

Sezione II. Opzioni di configurazione avanzate

In questa sezione vengono fornite istruzioni ed esempi sulle opzioni IPS IOS avanzate per il tuning delle firme.

Ritira o Annulla ritiro firme

Ritirare o annullare il ritiro di una firma significa selezionare o deselezionare le firme utilizzate da IPS IOS per analizzare il traffico.

- **Se si ritira** una firma, IOS IPS *NON* compilerà tale firma in memoria per la scansione.
- **Se si ritira** una firma, IOS IPS compila la firma in memoria e la utilizza per analizzare il traffico.

Èpossibile utilizzare l'interfaccia della riga di comando (CLI) di IOS per ritirare o annullare il ritiro di singole firme o di un gruppo di firme appartenenti a una categoria di firme. Quando si ritira o non si ritira un gruppo di firme, tutte le firme della categoria vengono ritirate o non ritirate.

Nota: alcune firme non ritirate (non ritirate come firme singole o all'interno di una categoria non ritirate) potrebbero non essere compilate a causa di memoria insufficiente o parametri non validi oppure se la firma è obsoleta.

In questo esempio viene illustrato come ritirare singole firme. Ad esempio, firma 6130 con ID di subnet 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)#
```

Nell'esempio viene mostrato come annullare il ritiro di tutte le firme appartenenti alla categoria 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: quando le firme in categorie diverse da IOS IPS Basic e IOS IPS Advanced non vengono ritirate come categoria, la compilazione di alcune firme o motori potrebbe non riuscire perché alcune firme in tali categorie non sono supportate da IOS IPS (vedere l'esempio seguente). Tutte le altre firme compilate correttamente (non ritirate) vengono utilizzate da IPS IOS per analizzare il traffico.

```
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
```

Attivare o disattivare le firme

Abilitare o disabilitare una firma significa applicare o ignorare le azioni associate alle firme da parte di IPS IOS quando il pacchetto o il flusso del pacchetto corrisponde alle firme.

Nota: l'opzione Abilita e disabilita NON seleziona né deseleziona le firme che devono essere utilizzate da IPS IOS.

- Per **abilitare** una firma si intende che quando viene attivata da un pacchetto (o flusso di pacchetto) corrispondente, la firma esegue l'azione appropriata associata. Tuttavia, solo le firme non ritirate e compilate correttamente eseguiranno l'azione quando sono attivate. In altre parole, se una firma viene ritirata, anche se è abilitata, non verrà compilata (perché è ritirata) e non eseguirà l'azione associata.
- Per **disabilitare** una firma si intende che quando viene attivata da un pacchetto (o flusso di pacchetto) corrispondente, la firma NON esegue l'azione appropriata associata. In altre parole, quando una firma viene disattivata, anche se non viene ritirata e compilata correttamente, non eseguirà l'azione associata.

Èpossibile utilizzare l'interfaccia della riga di comando (CLI) di IOS per abilitare o disabilitare singole firme o un gruppo di firme basate su categorie di firme. Nell'esempio viene mostrato come disabilitare la firma 6130 con ID di subnet 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)#
```

Nell'esempio viene mostrato come abilitare tutte le firme appartenenti alla categoria 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)#
```

Modifica azioni firma

Èpossibile utilizzare l'interfaccia della riga di comando (CLI) di IOS per modificare le azioni di firma per una firma o un gruppo di firme in base alle categorie di firma. In questo esempio viene illustrato come modificare le azioni relative alla firma in modo da avvisare, eliminare e reimpostare la firma 6130 con ID di subnet 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)#
```

Nell'esempio viene mostrato come modificare le azioni evento per tutte le firme appartenenti alla categoria 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)#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)#
```

Informazioni correlate

- Pagina Prodotti e servizi Cisco IOS Intrusion Prevention System (IPS)
- Cisco IOS IPS - Download del software con firme versione 5
- Miglioramenti utilizzabilità e supporto del formato della firma IPS 5.x
- Download del software Cisco Security Device Manager
- Come utilizzare CCP per configurare IOS IPS
- Software di crittografia 3DES per il Visualizzatore eventi di sistema per il rilevamento delle intrusioni di Cisco
- Documentazione e supporto tecnico – Cisco Systems