Configurer IPS avec des signatures au format 5.x

Contenu

Introduction

Ce document décrit comment configurer les signatures au format 5.x dans Cisco IOS® IPS et est organisé en deux sections :

- Section I. Étapes de configuration initiale - Cette section décrit les étapes nécessaires à l'utilisation de l'interface de ligne de commande (CLI) de Cisco IOS afin de commencer à utiliser les signatures au format IOS IPS 5.x. Cette section décrit les étapes suivantes :Étape 1. Téléchargez les fichiers IPS IOS.Étape 2. Créez un répertoire de configuration IOS IPS sur Flash.Étape 3. Configurez une clé de chiffrement IOS IPS.Étape 4. Activez IOS IPS.Étape 5. Chargez le package de signatures IOS IPS sur le routeur.Chaque étape et chaque commande spécifique sont décrites en détail, ainsi que des commandes et références supplémentaires. Un exemple de configuration est affiché sous chaque commande.
- Section II. Options de configuration avancées : cette section fournit des instructions et des exemples sur les options avancées pour le réglage des signatures. Il contient les options suivantes :Retirer ou annuler les signaturesActiver ou désactiver les signaturesModifier les actions de signature

Conditions préalables

Conditions requises

Vérifiez que vous disposez des composants appropriés (comme décrit dans Composants utilisés) avant de terminer les étapes de ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Un routeur à services intégrés Cisco (87x, 18xx, 28xx ou 38xx)
- DRAM : 128 Mo ou plus et mémoire flash disponible : 2 Mo minimum
- Connectivité console ou telnet au routeur
- Cisco IOS version 12.4(15)T3 ou ultérieure
- Nom d'utilisateur et mot de passe de connexion CCO (Cisco.com) valides
- Contrat de service Cisco IPS actuel pour les services de mise à jour des signatures sous licence

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Section I. Étapes de configuration de démarrage

Étape 1. Télécharger les fichiers IPS IOS

La première étape consiste à télécharger les fichiers de package de signatures IPS IOS et la clé de chiffrement publique à partir de Cisco.com.

Téléchargez les fichiers de signature requis depuis Cisco.com vers votre PC :

- Emplacement: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (clients enregistrés uniquement)
- Fichiers à télécharger :IOS-Sxxx-CLI.pkg (clients enregistrés uniquement) : il s'agit du dernier package de signatures.realm-cisco.pub.key.txt (clients enregistrés uniquement) : il s'agit de la clé de chiffrement publique utilisée par IOS IPS.

Étape 2. Créer un répertoire de configuration IPS IOS sur Flash

La deuxième étape consiste à créer un répertoire sur la mémoire Flash de votre routeur, dans lequel vous stockerez les fichiers de signature et les configurations requis. Vous pouvez également utiliser un lecteur flash USB Cisco connecté au port USB du routeur pour stocker les fichiers de signature et les configurations. Le lecteur flash USB doit rester connecté au port USB du routeur s'il est utilisé comme emplacement du répertoire de configuration IPS IOS. IOS IPS

prend également en charge tout système de fichiers IOS comme emplacement de configuration avec un accès en écriture approprié.

Afin de créer un répertoire, entrez cette commande à l'invite du routeur : **mkdir <*nom du répertoire*>**

Exemple :

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

Commandes et références supplémentaires

Afin de vérifier le contenu de la mémoire Flash, entrez cette commande à l'invite du routeur : **show flash:**

Exemple :

```
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)
```

Afin de renommer le nom du répertoire, utilisez cette commande : **renommer <*nom actuel*> <*nouveau nom*>**

Exemple :

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

Étape 3. Configurer une clé de chiffrement IOS IPS

La troisième étape consiste à configurer la clé de chiffrement utilisée par IOS IPS. Cette clé se trouve dans le fichier realm-cisco.pub.key.txt qui a été téléchargé à l'étape 1.

La clé de chiffrement est utilisée pour vérifier la signature numérique du fichier de signature principal (sigdef-default.xml) dont le contenu est signé par une clé privée Cisco afin de garantir son authenticité et son intégrité à chaque version.

1. Ouvrez le fichier texte et copiez le contenu du fichier.
2. Utilisez la commande **configure terminal** afin de passer en mode de configuration de routeur.
3. Collez le contenu du fichier texte à l'invite `<hostname>(config)#`.
4. Quittez le mode de configuration du routeur.
5. Entrez la commande **show run** à l'invite du routeur afin de confirmer que la clé de chiffrement est configurée. Vous devriez voir ce résultat dans la configuration :

```
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. Utilisez cette commande afin d'enregistrer la configuration :**copy running-configure startup-configure**

Commandes et références supplémentaires

Si la clé n'est pas configurée correctement, vous devez d'abord supprimer la clé de chiffrement, puis la reconfigurer :

1. Afin de supprimer la clé, entrez ces commandes dans l'ordre indiqué ci-dessous :
```
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. Utilisez la commande **show run** afin de vérifier que la clé est supprimée de la configuration.
3. Suivez la procédure de l'étape 3 afin de reconfigurer la clé.

Étape 4. Activer IOS IPS

La quatrième étape consiste à configurer IOS IPS. Suivez cette procédure afin de configurer IOS IPS :

1. Utilisez la commande **ip ips name <*rule name*> < *facultatif ACL*>** afin de créer un nom de règle. (Ceci sera utilisé sur une interface pour activer IPS.)Exemple :
```
router#configure terminal
router(config)#ip ips name iosips
```

   Vous pouvez spécifier une liste de contrôle d'accès étendue ou standard (ACL) facultative afin de filtrer le trafic qui sera analysé par ce nom de règle. Tout le trafic autorisé par la liste de contrôle d'accès est soumis à l'inspection de l'IPS. Le trafic refusé par la liste de contrôle d'accès n'est pas inspecté par le système de prévention des intrusions.
```
router(config)#ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
```
2. Utilisez la commande **ip ips config location flash:<*directory name*>** afin de configurer l'emplacement de stockage des signatures IPS. (Il s'agit du répertoire *ips* créé à l'étape 2.)Exemple :
```
router(config)#ip ips config location flash:ips
```

3. Utilisez la commande **ip ips notification sdee** afin d'activer la notification d'événement IPS SDEE.Exemple :
```
router(config)#ip ips notify sdee
```

   Pour utiliser SDEE, le serveur HTTP doit être activé (avec la commande **ip http server**). Si le

serveur HTTP n'est pas activé, le routeur ne peut pas répondre aux clients SDEE car il ne peut pas voir les requêtes. La notification SDEE est désactivée par défaut et doit être explicitement activée.IOS IPS prend également en charge l'utilisation de syslog afin d'envoyer une notification d'événement. SDEE et syslog peuvent être utilisés indépendamment ou activés en même temps afin d'envoyer une notification d'événement IOS IPS. La notification Syslog est activée par défaut. Si la console de journalisation est activée, les messages syslog IPS s'affichent. Afin d'activer syslog, utilisez cette commande :

```
router(config)#ip ips notify log
```

4. Configurez IOS IPS pour utiliser l'une des catégories de signatures prédéfinies.IOS IPS avec signatures au format Cisco 5.x fonctionne avec des catégories de signatures (tout comme les appliances Cisco IPS). Toutes les signatures sont regroupées en catégories et les catégories sont hiérarchiques. Cela permet de classer les signatures pour faciliter le regroupement et le réglage.**Avertissement :** La catégorie de *toutes les* signatures contient toutes les signatures dans une version de signature. Puisque IOS IPS ne peut pas compiler et utiliser toutes les signatures contenues dans une version de signature à la fois, *ne retirez pas la catégorie all* ; sinon, la mémoire du routeur est insuffisante.**Remarque :** lorsque vous configurez IOS IPS, vous devez d'abord retirer toutes les signatures de la catégorie *all*, puis annuler les catégories de signatures sélectionnées.**Remarque :** L'ordre dans lequel les catégories de signature sont configurées sur le routeur est également important. IOS IPS traite les commandes de catégorie dans l'ordre indiqué dans la configuration. Certaines signatures appartiennent à plusieurs catégories. Si plusieurs catégories sont configurées et qu'une signature appartient à plusieurs d'entre elles, les propriétés de la signature (par exemple, les actions retirées, non retirées, etc.) de la dernière catégorie configurée sont utilisées par IOS IPS.Dans cet exemple, toutes les signatures de la catégorie « all » sont retirées, puis la catégorie *IOS IPS Basic* n'est pas supprimée.

```
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. Utilisez ces commandes afin d'activer la règle IPS sur l'interface souhaitée, et spécifiez la direction dans laquelle la règle sera appliquée :**interface <***nom de l'interface***>ip ips <***nom de la règle***> [***dans | sortant***]**Exemple :

```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#exit
router(config)#exit
router#
```

L'argument *in* signifie que seul le trafic entrant dans l'interface est inspecté par IPS. L'argument *out* signifie que seul le trafic sortant de l'interface est inspecté par IPS.Afin de permettre à IPS d'inspecter le trafic entrant et sortant de l'interface, entrez séparément le nom de la règle IPS pour *les entrées* et *sorties* sur la même interface :

```
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#
```

Étape 5. Charger le package de signatures IPS IOS sur le routeur

La dernière étape consiste à charger sur le routeur le package de signatures téléchargé à l'étape 1.

Remarque : La façon la plus courante de charger le package de signature sur le routeur est d'utiliser FTP ou TFTP. Cette procédure utilise FTP. Reportez-vous à la section *Commandes et références supplémentaires* de cette procédure pour obtenir une autre méthode de chargement du package de signature IOS IPS. Si vous utilisez une session telnet, utilisez la commande **terminal monitor** afin d'afficher les sorties de la console.

Afin de charger le package de signature sur le routeur, procédez comme suit :

1. Utilisez cette commande afin de copier le package de signature téléchargé à partir du serveur FTP vers le routeur :**copy ftp://*<ftp_user:password@Server_IP_address>*/*<signature_package>* idconf****Remarque :*** N'oubliez pas d'utiliser le *paramètre idconf* à la fin de la commande **copy**.**Remarque :** Par exemple :
   ```
   router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
   Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   [OK - 7608873/4096 bytes]
   ```
   La compilation des signatures commence immédiatement après le chargement du package de signatures sur le routeur. Vous pouvez voir les journaux sur le routeur avec le niveau de journalisation 6 ou supérieur activé.
   ```
   *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. Utilisez la commande **show ip ips signature count** afin de vérifier que le paquet de signatures est correctement compilé.Exemple :
   ```
   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#
```

Commandes et références supplémentaires

La clé de chiffrement publique n'est pas valide si vous recevez un message d'erreur au moment de la compilation des signatures, similaire à ce message d'erreur :

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

Référez-vous à Étape 3 pour plus d'informations.

Si vous n'avez pas accès à un serveur FTP ou TFTP, vous pouvez utiliser un lecteur flash USB afin de charger le package de signature sur le routeur. D'abord, copiez le package de signature sur le lecteur USB, connectez le lecteur USB à l'un des ports USB du routeur, puis utilisez la commande **copy** avec le paramètre *idconf* afin de copier le package de signature sur le routeur.

Exemple :

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

Le répertoire de stockage IOS IPS configuré comporte six fichiers. Ces fichiers utilisent le format de nom suivant : <*nom-routeur*>-sigdef-xxx.xml ou <*nom-routeur*>-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#
```

Ces fichiers sont stockés au format compressé et ne sont ni directement modifiables ni visualisables. Le contenu de chaque fichier est décrit ci-dessous :

- *router-sigdef-default.xml* contient toutes les définitions de signature par défaut d'usine.
- *router-sigdef-delta.xml* contient des définitions de signature qui ont été modifiées par défaut.
- *router-sigdef-typedef.xml* contient toutes les définitions de paramètres de signature.
- *router-sigdef-category.xml* contient les informations de catégorie de signature, telles que category ios_ips basic et advanced.

- *router-seap-delta.xml* contient les modifications apportées aux paramètres SEAP par défaut.
- *router-seap-typedef.xml* contient toutes les définitions de paramètres SEAP.

Section II. Options de configuration avancées

Cette section fournit des instructions et des exemples sur les options IOS IPS avancées pour le réglage des signatures.

Retirer ou annuler des signatures

Retirer ou annuler une signature signifie sélectionner ou désélectionner les signatures utilisées par IOS IPS pour analyser le trafic.

- **La suppression** d'une signature signifie qu'IOS IPS *NE* compile *PAS* cette signature en mémoire pour analyse.
- **Le retrait** d'une signature indique à IOS IPS de compiler la signature en mémoire et d'utiliser la signature pour analyser le trafic.

Vous pouvez utiliser l'interface de ligne de commande (CLI) d'IOS afin de retirer ou d'annuler des signatures individuelles ou un groupe de signatures appartenant à une catégorie de signatures. Lorsque vous retirez ou annulez un groupe de signatures, toutes les signatures de cette catégorie sont retirées ou non.

Note : Certaines signatures non retirées (non retirées en tant que signature individuelle ou dans une catégorie non retirée) peuvent ne pas être compilées en raison d'une mémoire insuffisante ou de paramètres non valides ou si la signature a été obsolète.

Cet exemple montre comment retirer des signatures individuelles. Par exemple, la signature 6130 avec l'ID de subvention 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)#
```

Cet exemple montre comment annuler toutes les signatures appartenant à la catégorie 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
```

Remarque : lorsque les signatures de catégories autres que IOS IPS Basic et IOS IPS Advanced ne sont pas retirées en tant que catégorie, la compilation de certaines signatures ou de certains moteurs peut échouer car certaines signatures de ces catégories ne sont pas prises en charge par IOS IPS (voir l'exemple ci-dessous). Toutes les autres signatures correctement compilées (non retirées) sont utilisées par IOS IPS pour analyser le trafic.

```
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
```

Activer ou désactiver les signatures

Pour activer ou désactiver une signature, vous devez appliquer ou ignorer les actions associées aux signatures par IOS IPS lorsque le flux de paquets ou de paquets correspond aux signatures.

Remarque : Activer et désactiver ne sélectionne PAS et ne désélectionne pas les signatures à utiliser par IOS IPS.

- Pour **activer** une signature, cela signifie que lorsqu'elle est déclenchée par un paquet correspondant (ou un flux de paquets), la signature prend l'action appropriée qui lui est associée. Cependant, seules les signatures NON retirées ET compilées avec succès prendront l'action lorsqu'elles sont activées. En d'autres termes, si une signature est retirée, même si elle est activée, elle ne sera pas compilée (parce qu'elle est retirée) et elle n'exécutera pas l'action qui lui est associée.
- Pour **désactiver** une signature, cela signifie que lorsqu'elle est déclenchée par un paquet correspondant (ou un flux de paquets), la signature NE prend PAS l'action appropriée qui lui est associée. En d'autres termes, lorsqu'une signature est désactivée, même si elle n'est pas retirée et compilée avec succès, elle n'exécute pas l'action qui lui est associée.

Vous pouvez utiliser l'interface de ligne de commande IOS afin d'activer ou de désactiver des signatures individuelles ou un groupe de signatures basé sur des catégories de signatures. Cet exemple montre comment désactiver la signature 6130 avec l'ID de subvention 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)#
```

Cet exemple montre comment activer toutes les signatures appartenant à la catégorie 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)#
```

Modifier les actions de signature

Vous pouvez utiliser l'interface de ligne de commande (CLI) IOS afin de modifier les actions de signature pour une signature ou un groupe de signatures basé sur des catégories de signatures. Cet exemple montre comment modifier les actions de signature pour alerter, supprimer et réinitialiser la signature 6130 avec l'ID de subvention 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)#
```

Cet exemple montre comment modifier les actions d'événement pour toutes les signatures appartenant à la catégorie de signature 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)#
```

Informations connexes

- Page Produits et services de Cisco IOS Intrusion Prevention System (IPS)
- Cisco IOS IPS - Téléchargement du logiciel des signatures de la version 5
- Prise en charge du format de signature IPS 5.x et amélioration de l'utilisation
- Téléchargement du logiciel Cisco Security Device Manager
- Comment utiliser CCP pour configurer IOS IPS
- Téléchargement du logiciel cryptographique 3DES de Cisco Intrusion Detection System Event Viewer
- Support et documentation techniques - Cisco Systems