Exemple de configuration du système de prévention des intrusions avec des signatures au format 5.x

Contenu

Introduction

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

- Étapes de configuration d'I. Getting Started de section — Cette section fournit les étapes nécessaires pour employer l'interface de ligne de commande de Cisco IOS (CLI) afin d'obtenir commencé par des signatures de format de l'IOS IPS 5.x. Cette section décrit ces étapes :Étape 1. Téléchargez les fichiers d'IOS IPS.Étape 2. Créez un répertoire de la configuration d'IOS IPS sur l'éclair.Étape 3. Configurez une crypto clé d'IOS IPS.Étape 4. IOS IPS d'enable.Étape 5. Chargez le module de signature d'IOS IPS au routeur.Chaque étape et commandes de particularité sont décrites en détail, aussi bien que des commandes et des références supplémentaires. Un exemple de configuration est affiché au-dessous de chaque commande.
- Options de configuration avancée de la section II. — Cette section fournit des instructions et des exemples en des options avancées pour l'accord de signature. Il contient ces options :Retirez ou des signatures d'UnretireSignatures d'enable ou de débronchementActions de signature de modification

Conditions préalables

Conditions requises

Assurez que vous avez les composants appropriés (comme décrit dans des composants utilisés) avant que vous vous terminiez les étapes dans ce document.

Composants utilisés

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

- Un Integrated Services Router de Cisco (87x, 18xx, 28xx, ou 38xx)
- 128MB ou plus de mémoire vive dynamique et au moins de mémoire Flash libre 2MB
- Connectivité de console ou de telnet au routeur
- Cisco IOS version 12.4(15)T3 ou ultérieures
- Un nom et un mot de passe valides d'utilisateur de connexion CCO (Cisco.com)
- Un contrat de service en cours de Cisco IPS pour des services autorisés de mise à jour de signature

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Étapes de configuration d'I. Getting Started de section

Étape 1. Fichiers d'IOS IPS de téléchargement

La première étape est de télécharger des fichiers de package de signature d'IOS IPS et la crypto clé publique de Cisco.com.

Téléchargez les fichiers de signatures requis de Cisco.com à votre PC :

- Emplacement : http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (clients enregistrés seulement)
- Fichiers aux télécharger :IOS-Sxxx-CLI.pkg (registeredcustomers seulement) — C'est le dernier module de signature.realm-cisco.pub.key.txt (clients enregistrés seulement) — C'est la crypto clé publique utilisée par IOS IPS.

Étape 2. Créez un répertoire de la configuration d'IOS IPS sur l'éclair

La deuxième étape est de créer un répertoire sur l'éclair de votre routeur où vous enregistrez les

fichiers de signatures et les configurations priés. Alternativement, vous pouvez utiliser un USB Flash Drive de Cisco connecté au port USB du routeur pour enregistrer les fichiers de signatures et les configurations. L'USB Flash Drive doit demeurer connecté au port USB du routeur s'il est utilisé comme emplacement de répertoire de la configuration d'IOS IPS. L'IOS IPS prend en charge également n'importe quel système de fichiers IOS en tant que son emplacement de configuration avec l'accès en écriture approprié.

Afin de créer un répertoire, sélectionnez cette commande à la demande de routeur : *nom* **<directory de mkdir >**

Exemple :

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

Commandes et références supplémentaires

Afin de vérifier le contenu de l'éclair, sélectionnez cette commande à la demande de 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 : **renommez le** *nom* **<current > le** *nom de* **<new >**

Exemple :

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

Étape 3. Configurez une crypto clé d'IOS IPS

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

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

1. Ouvrez le fichier texte, et copiez le contenu du fichier.
2. Employez la commande de **configure terminal** afin de présenter le routeur configurent le mode.
3. Collez le contenu de fichier texte à la demande de `<hostname>(config)#`.
4. Annulez le mode de configuration du routeur.
5. Sélectionnez la commande de **passage d'exposition à la** demande de routeur afin de confirmer que la crypto clé est configurée. Vous devriez voir cette sortie 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. Employez cette commande afin de sauvegarder la configuration :**la copie exécution-configurent startup-configurent**

Commandes et références supplémentaires

Si la clé est configurée inexactement, vous devez retirer la crypto clé d'abord et ensuite la modifier :

1. Afin de retirer la clé, sélectionnez 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. Employez la commande de **passage d'exposition** afin de vérifier que la clé est retirée de la configuration.
3. Remplissez la procédure dans l'étape 3 afin de modifier la clé.

Étape 4. IOS IPS d'enable

La quatrième étape est de configurer l'IOS IPS. Remplissez cette procédure afin de configurer l'IOS IPS :

1. Utilisez le *nom de* **<rule d'ip ips name >** commande **< d'***ACL facultatif* **>** afin de créer un nom de règle. (Ceci sera utilisé sur une interface pour activer l'IPS.)Exemple :`router#`**`configure terminal`** `router(config)#`**`ip ips name iosips`** Vous pouvez spécifier une liste de contrôle d'accès étendue ou standard facultative (ACL) afin de filtrer le trafic qui sera balayé par ce nom de règle. Tout le trafic qui est permis par l'ACL est sujet à l'inspection par l'IPS. Trafiquez qui est refusé par l'ACL n'est pas examiné par l'IPS.`router(config)#`**`ip ips name ips list ?`** `<1-199> Numbered access list WORD Named access list`
2. Utilisez l'**éclair d'ip ips config location :** *nom* **>** commande **<directory** afin de configurer l'emplacement de mémoire de signature IPS. (C'est le répertoire *IPS* créé dans l'étape 2.)Exemple :`router(config)#`**`ip ips config location flash:ips`**
3. Employez la commande de **sdee d'ip ips notify** afin d'activer la notification d'événement IPS SDEE.Exemple :`router(config)#`**`ip ips notify sdee`** Afin d'utiliser SDEE, le serveur HTTP doit être activé (avec la commande d'**ip http server**). Si le serveur HTTP n'est pas activé, le routeur ne peut pas répondre aux clients SDEE parce qu'il ne peut pas voir les demandes. La notification SDEE est désactivée par défaut et doit être explicitement activée.L'IOS IPS prend en charge également l'utilisation du Syslog afin d'envoyer la notification d'événement. SDEE et Syslog peuvent être utilisés indépendamment ou activés en même temps afin d'envoyer la notification d'événement d'IOS IPS. La notification de Syslog est activée par défaut. Si le logging console est activé, vous verrez des messages de Syslog IPS. Afin d'activer le Syslog, utilisez cette commande :`router(config)#`**`ip ips notify log`**
4. Configurez l'IOS IPS pour utiliser une des catégories de signature de prédéfinis.L'IOS IPS avec des signatures de format de Cisco 5.x fonctionne avec des catégories de signature (juste comme des appliances de Cisco IPS). Toutes les signatures sont groupées dans des catégories, et les catégories sont hiérarchiques. Ceci aide à classifier des signatures pour le

groupement et l'accord faciles.**Avertissement :** *La toute la* catégorie de signature contient toutes les signatures dans une release de signature. Puisque l'IOS IPS ne peut pas compiler et utiliser toutes les signatures contenues dans une signature relâchez en même temps, *ne font pas l'unretire la toute la catégorie* ; autrement, le routeur manquera de mémoire.**Remarque:** Quand vous configurez l'IOS IPS, vous devez d'abord retirer toutes les signatures dans la *toute la* catégorie, et puis des catégories de signature sélectionnée d'unretire.**Remarque:** La commande dans laquelle les catégories de signature sont configurées sur le routeur est également importante. L'IOS IPS traite les commandes de catégorie dans l'ordre indiqué dans la configuration. Quelques signatures appartiennent à de plusieurs catégories. Si de plusieurs catégories sont configurées et une signature appartient à plus d'une d'entre elles, les propriétés de la signature (par exemple, retiré, unretired, des actions, etc.) dans la dernière catégorie configurée sont utilisées par IOS IPS.Dans cet exemple, toutes les signatures dans la « toute la » catégorie sont retirées, et alors la catégorie *de base d'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. Employez ces commandes afin d'activer la règle IPS sur l'interface désirée, et spécifiez la direction dans laquelle la règle sera appliquée :*nom de* **<interface d'interface >***nom de* **<rule d'ip ips > [***dans* **/]**Exemple :`router(config)#`**`interface GigabitEthernet 0/1`** `router(config-if)#`**`ip ips iosips in`** `router(config-if)#`**`exit`** `router(config)#`**`exit`** `router#` *Dans l'*argument signifie que seulement le trafic allant dans l'interface est examiné par IPS. L'argument de *sortie* signifie que seulement l'extinction du trafic de l'interface est examinée par IPS.Afin de permettre à l'IPS d'examiner chacun des deux dans et le trafic de l'interface, écrivez séparément le nom de règle IPS pour *dedans* et 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. Chargez le module de signature d'IOS IPS au routeur

La dernière étape est de charger au routeur que le module de signature l'a téléchargé dans l'étape 1.

Remarque: La plupart de manière courante de charger le module de signature au routeur est d'utiliser le FTP ou le TFTP. Cette procédure utilise le FTP. Veuillez se référer à la section *supplémentaire de commandes et de références* dans cette procédure pour qu'une approche alternative charge le module de signature d'IOS IPS. Si vous utilisez une session de telnet, employez la commande de **terminal monitor** afin de visualiser les sorties de console.

Afin de charger le module de signature au routeur, terminez-vous ces étapes :

1. Employez cette commande afin de copier le module téléchargé de signature du ftp server sur le routeur :**<ftp_user de ftp:// de copie** *:* **idconf de** *password@Server_IP_address* **>/<signature_package>Remarque:** Souvenez-vous s'il vous plaît pour utiliser le paramètre d'*idconf à la* fin de la Commande **COPY**.**Remarque:** Exemple :`router#`**`copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf`** `Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK - 7608873/4096 bytes]` Compiler de signature commence juste après que le module de signature est chargé au routeur. Vous pouvez voir les logins le

routeur avec se connecter le niveau 6 ou au-dessus d'activer.*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. Employez la commande de **compte de signature de show ip ips** afin de vérifier le module de signature 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 crypto clé publique est non valide si vous recevez un message d'erreur au moment de la compilation de signature semblable à ce message d'erreur :

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

Référez-vous au pour en savoir plus d'étape 3.

Si vous n'avez pas accès à un serveur de FTP ou TFTP, vous pouvez employer un USB Flash Drive afin de charger le module de signature au routeur. D'abord, copiez le module de signature sur le lecteur USB, connectez le lecteur USB à un des ports USB sur le routeur, et puis employez la Commande **COPY** avec le paramètre d'*idconf* afin de copier le module de signature sur le routeur.

Exemple :

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

Il y a six fichiers dans le répertoire configuré de mémoire d'IOS IPS. Ces fichiers utilisent ce format de nom : **<**router-nom **>**-sigdef-xxx.xml ou **<** routeur-nom *>-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 enregistrés dans le format compressé et ne sont pas directement editable ou visualisables. Le contenu de chaque fichier est décrit ci-dessous :

- *router-sigdef-default.xml contient* toutes les définitions de signature de par défaut d'usine.
- *router-sigdef-delta.xml contient les* définitions de signature qui ont été changées du par défaut.
- *router-sigdef-typedef.xml contient* toutes les définitions de paramètre de signature.
- *router-sigdef-category.xml contient les* informations de catégorie de signature, telles que des ios_ips de catégorie de base et avancés.
- *router-seap-delta.xml contient des* modifications apportées aux paramètres du par défaut SEAP.
- *router-seap-typedef.xml contient* toutes les définitions de paramètre SEAP.

Options de configuration avancée de la section II.

Cette section fournit des instructions et des exemples en des options avancées d'IOS IPS pour l'accord de signature.

Des signatures retirez ou d'Unretire

Pour se retirer ou unretire moyens d'une signature de sélectionner ou désélectionner les signatures qui sont utilisées par IOS IPS afin de balayer le trafic.

- **Le retrait d'une** signature signifie que l'IOS IPS ne compilera pas cette signature dans la mémoire pour le balayage.
- **Unretiring une** signature demande à l'IOS IPS de compiler la signature dans la mémoire et d'employer la signature pour balayer le trafic.

Vous pouvez employer l'interface de ligne de commande IOS (CLI) afin de différentes signatures se retirer ou d'unretire ou un groupe de signatures qui appartiennent à une catégorie de signature. Quand vous vous retirez ou unretire par groupe de signatures, toutes les signatures dans cette catégorie sont retirées ou unretired.

Remarque: Quelques signatures unretired (unretired en tant que signature individuelle ou dans une catégorie unretired) peuvent ne pas compiler en raison de la mémoire insuffisante ou des paramètres non valides ou si la signature obsoleted.

Cet exemple affiche comment retirer différentes signatures. Par exemple, signature 6130 avec l'ID de subsig 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)#
```

Cet exemple affiche comment à l'unretire toutes les signatures qui appartiennent à la catégorie de base d'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
```

Remarque: Quand des signatures dans les catégories autres que l'IOS IPS de base et l'IOS IPS avancé unretired comme catégorie, la compilation de quelques signatures ou engines pourrait échouer parce que certaines signatures dans ces catégories ne sont pas prises en charge par IOS IPS (voir l'exemple ci-dessous). Tout l'autre les signatures (unretired) avec succès compilées sont utilisés par IOS IPS pour balayer 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
```

Signatures d'enable ou de débronchement

Pour activer ou désactiver une signature est d'imposer ou négliger les actions associées avec les signatures par IOS IPS quand le paquet ou l'écoulement de paquet apparie les signatures.

Remarque: L'enable et le débronchement ne sélectionne pas et désélectionne des signatures à utiliser par IOS IPS.

- Pour **activer une** signature signifie qu'une fois déclenchée par un paquet assorti (ou écoulement de paquet), la signature prend la mesure appropriée associée avec elle. Cependant, seulement les signatures unretired ET avec succès compilées prendront la mesure quand elles sont activées. En d'autres termes, si une signature est retirée, quoiqu'il soit activé, il ne sera pas compilé (parce qu'il est retiré) et il ne prendra pas la mesure associée avec lui.
- Pour **désactiver une** signature signifie qu'une fois déclenchée par un paquet assorti (ou écoulement de paquet), la signature ne prend pas la mesure appropriée associée avec elle. En d'autres termes, quand une signature est désactivée, quoiqu'il unretired et soit avec succès compilé, il ne prendra pas la mesure associée avec lui.

Vous pouvez employer l'interface de ligne de commande IOS (CLI) afin d'activer ou désactiver différentes signatures ou un groupe de signatures basées sur des catégories de signature. Cet exemple affiche comment désactiver la signature 6130 avec l'ID de subsig 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)#
```

Cet exemple affiche comment activer toutes les signatures qui appartiennent à la catégorie de base d'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)#
```

Actions de signature de modification

Vous pouvez employer l'interface de ligne de commande IOS (CLI) afin de changer des actions de signature pour une signature ou un groupe de signatures basées sur des catégories de signature. Cet exemple affiche comment changer des actions de signature d'alerter, relâcher, et la remise pour la signature 6130 avec l'ID de subsig 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)#
```

Cet exemple affiche comment changer des actions d'événement pour toutes les signatures qui appartiennent à la catégorie de base d'IOS IPS de signature.

```
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

- Produits de Système de protection contre les intrusions (IPS) Cisco IOS et page de services
- Cisco IOS IPS - Téléchargement logiciel de signatures de version 5
- IPS améliorations de support et de facilité d'utilisation de format de signature 5.x
- Téléchargement logiciel de Cisco Security Device Manager
- Comment employer le CCP pour configurer l'IOS IPS
- Téléchargement logiciel cryptographique du visualisateur d'événements 3DES de Detection System de Cisco Intrusion
- Support et documentation techniques - Cisco Systems