IPS met 5.x bestandsindelingen configureren

Inhoud

Inleiding

Dit document beschrijft hoe u 5.x-handtekeningen in Cisco IOS® IPS kunt configureren en is georganiseerd in twee secties:

- Sectie I. Introducted Configuration Stappen-Deze sectie verschaft de stappen die nodig zijn om de Cisco IOS opdrachtregel-interface (CLI) te gebruiken om te beginnen met IOS IPS 5.x-indelingen. In dit gedeelte worden de volgende stappen beschreven:Stap 1. Download de IOS IPS-bestanden.Stap 2. Maak een IOS IPS-configuratiemap in Flash.Stap 3. Configuratie van een IOS IPS-encryptie.Stap 4. Schakel IOS IPS in.Stap 5. Laad het IOS IPS-pakket voor handtekeningen in de router.Elke stap en specifieke opdrachten worden uitvoerig beschreven, evenals extra opdrachten en referenties. Onder elke opdracht wordt een voorbeeldconfiguratie weergegeven.
- Deel II. Geavanceerde Configuration-opties - Deze sectie verschaft instructies en voorbeelden voor geavanceerde opties voor het stemmen van handtekeningen. Dit programma bevat de volgende opties:Handtekeningen makenHandtekeningen inschakelen of uitschakelenHandelingen wijzigen

Voorwaarden

Vereisten

Zorg ervoor dat u de juiste onderdelen hebt (zoals beschreven in Gebruikte componenten) voordat u de stappen in dit document uitvoert.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Een Cisco geïntegreerde services router (870x, 18xx, 28xx of 38xx)
- 128 MB of meer DRAM en ten minste 2 MB vrij flash-geheugen
- Console of telnet connectiviteit op de router
- Cisco IOS-softwarerelease 12.4(15)T3 of hoger
- Een geldige inlognaam en wachtwoord voor CCO (Cisco.com)
- Een huidig Cisco IPS-servicecontract voor gelicentieerde update-services

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Sectie I. Stappen configuratie aan het begin

Stap 1. Download IOS IPS-bestanden

De eerste stap is het downloaden van IOS IPS-pakketbestanden met handtekeningen en openbare cryptosleutel van Cisco.com.

Download de vereiste signaalbestanden van Cisco.com naar uw PC:

- Plaats: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (alleen geregistreerde klanten)
- Bestanden te downloaden:IOS-Sxxx-CLI.pkg (alleen geregistreerde klanten) — Dit is het nieuwste pakket voor handtekeningen.Realm-cisco.pub.key.txt (alleen geregistreerde klanten) — Dit is de openbare sleutel voor crypto die door IOS IPS wordt gebruikt.

Stap 2. Maak een IOS IPS-Configuration-map op Flash

De tweede stap is om een folder op de flitser van uw router te maken waar u de vereiste signatuurbestanden en configuraties opslaat. In plaats hiervan kunt u ook een Cisco USB-flitser gebruiken die op de USB-poort van de router is aangesloten om de bestanden en configuraties met de handtekening op te slaan. Het USB-flitsstation moet op de USB-poort van de router worden aangesloten als het gebruikt wordt als de IOS IPS-configuratielocatie. IOS IPS ondersteunt ook elk IOS-bestandssysteem als zijn configuratielocatie met juiste schrijftoegang.

Om een folder te maken, voer deze opdracht in de routerprompt: **mkdir <*directory name*>**

Bijvoorbeeld:

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

Aanvullende opdrachten en referenties

Om de inhoud van de flitser te verifiëren, voer dit bevel in bij de routerherinnering: **flitser tonen:**

Bijvoorbeeld:

```
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)
```

Gebruik deze opdracht om de naam van de map een andere naam te geven: **Hernoemen <*huidige naam*> <*nieuwe naam*>**

Bijvoorbeeld:

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

Stap 3. Configuratie van een IOS IPS-encryptie

De derde stap is de configuratie van de crypto-toets die door IOS IPS wordt gebruikt. Deze toets bevindt zich in het bestand realm-cisco.pub.key.txt dat in Stap 1 is gedownload.

De crypto-toets wordt gebruikt om de digitale handtekening voor het hoofdbestand voor de handtekening (sigdef-default.xml) te controleren waarvan de inhoud door een particuliere sleutel van Cisco wordt ondertekend om de authenticiteit en integriteit van het bestand bij elke release te garanderen.

1. Open het tekstbestand en kopieer de inhoud van het bestand.
2. Gebruik de opdracht **aanpasterminal** om router in te stellen en modus te configureren.
3. Plakt de inhoud van het tekstbestand bij de `<hostname>(configuratie)#`prompt.
4. Routerconfiguratie afsluiten.
5. Voer de opdracht **Show run** in op de routermelding om te bevestigen dat de crypto-toets is geconfigureerd. U dient deze uitvoer in de configuratie te zien:
   ```
   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. Gebruik deze opdracht om de configuratie op te slaan:**kopieer het beheer van het apparaat**

Aanvullende opdrachten en referenties

Als de toets niet correct is ingesteld, moet u eerst de crypto-toets verwijderen en hem vervolgens opnieuw configureren:

1. Geef deze opdrachten in de onderstaande volgorde op om de toets te verwijderen:
```
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. Gebruik de opdracht **Show run** om te controleren of de toets uit de configuratie is verwijderd.
3. Volg de procedure in Stap 3 om de toets te configureren.

Stap 4. Schakel IOS IPS in

De vierde stap is om IOS IPS te configureren. Voltooi deze procedure om IOS IPS te configureren:

1. Gebruik de **IP IPS-naam <*regelnaam*> < *optioneel ACL*>**-opdracht om een regelnaam te maken. (Dit zal op een interface worden gebruikt om IPS mogelijk te maken.)Bijvoorbeeld:
```
router#configure terminal
router(config)#ip ips name iosips
```

   U kunt een optionele uitgebreide of standaard toegangscontrolelijst (ACL) instellen om het verkeer te filteren dat gescand wordt met deze regelnaam. Alle verkeer dat door de ACL is toegestaan, wordt door IPS geïnspecteerd. Het verkeer dat door ACL wordt ontkend wordt niet door IPS geïnspecteerd.
```
router(config)#ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
```
2. Gebruik de **flitser** van de **ip**. **de** plaats van de **opstelling van een** IP-***directory*:** opdracht om de opslaglocatie van IPS-handtekeningen te configureren. (Dit is de map *ips* die in Stap 2 is gemaakt.)Bijvoorbeeld:
```
router(config)#ip ips config location flash:ips
```

3. Gebruik de **ip** s **om het** bevel **van de** sdee te melden **om** IPS SDEE-gebeurtenis in te schakelen.Bijvoorbeeld:
```
router(config)#ip ips notify sdee
```

   Om SDEE te kunnen gebruiken, moet de HTTP server ingeschakeld zijn (met de opdracht **ip http server**). Als de HTTP server niet is ingeschakeld, kan de router niet reageren op de SDEE-clients omdat deze de verzoeken niet kunnen zien. SDEE-melding wordt standaard uitgeschakeld en moet expliciet worden ingeschakeld.IOS IPS ondersteunt ook het gebruik van syslog om melding van gebeurtenissen te verzenden. SDEE en SLOG kunnen onafhankelijk of op het zelfde moment worden gebruikt om IOS IPS gebeurtenis bericht te verzenden. Automatische melding is standaard ingeschakeld. Als de logconsole is ingeschakeld, ziet u IPS-syslig-berichten. Gebruik deze opdracht om syslog in te schakelen:
```
router(config)#ip ips notify log
```

4. Configureer IOS IPS om een van de vooraf gedefinieerde kenmerkcategorieën te

gebruiken.IOS IPS met Cisco 5.x-handtekeningen voor handtekeningen werkt met categorieën handtekeningen (net zoals Cisco IPS-apparaten). Alle handtekeningen zijn gegroepeerd in categorieën, en de categorieën zijn hiërarchisch. Hierdoor kunnen handtekeningen worden geclassificeerd zodat ze gemakkelijk kunnen worden gegroepeerd en afgestemd.**Waarschuwing:** de *hele* categorie handtekeningen bevat alle handtekeningen in een handtekeningen. Aangezien IOS IPS niet alle handtekeningen in een handmatige release tegelijk kan samenstellen en gebruiken, *moet u de alle categorie niet opheffen*. anders raakt de router niet meer in het geheugen gegrift.**Opmerking:** Wanneer u IOS IPS configureren moet u eerst alle handtekeningen in de *hele* categorie intrekken en vervolgens geselecteerde ondertekencategorieën verwijderen.**Opmerking:** De volgorde waarin de categorieën handtekeningen op de router zijn geconfigureerd is ook belangrijk. IOS IPS verwerkt de groepopdrachten in de volgorde die in de configuratie is opgesomd. Sommige handtekeningen behoren tot meerdere categorieën. Als meerdere categorieën worden geconfigureerd en een handtekening van meer dan één categorie behoort, worden de eigenschappen van de handtekening (bijvoorbeeld beëindigd, niet-beëindigd, acties, enz.) in de laatste geconfigureerde categorie gebruikt door IOS IPS.In dit voorbeeld, worden alle handtekeningen in de "all" categorie teruggetrokken, en dan is de *IOS IPS Basic* categorie niet teruggetrokken.

```
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. Gebruik deze opdrachten om IPS-regels op de gewenste interface in te schakelen en specificeer de richting waarin de regel wordt toegepast:**interface <*interfacenaam*>ip IPS <*regelnaam*> [*in | uit*]**Bijvoorbeeld:

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

Het in argument betekent dat alleen verkeer dat de interface ingaat, door IPS geïnspecteerd wordt. Het out argument betekent dat alleen verkeer dat de interface verlaat, door IPS geïnspecteerd wordt.Om IPS in staat te stellen om zowel in- als uitverkeer van de interface te inspecteren, voert u **op dezelfde interface** afzonderlijk de IPS-regelnaam voor *in* **-** en *buiten in:*

```
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#
```

Stap 5. Laad het IOS IPS-signaalpakket naar de router

De laatste stap is om het pakket voor de handtekening te laden dat in Stap 1 is gedownload naar de router.

Opmerking: de meest gebruikelijke manier om het pakket voor handtekeningen aan de router te laden is door FTP of TFTP te gebruiken. Deze procedure gebruikt FTP. Raadpleeg het gedeelte *Aanvullende opdrachten en verwijzingen* in deze procedure voor een alternatieve methode om het IOS IPS-handboekingspakket te laden. Als u een telnet sessie gebruikt, gebruik de opdracht van de **eindmonitor** om de console output te bekijken.

Om het pakket van de handtekening aan de router te laden, voltooien deze stappen:

1. Gebruik deze opdracht om het gedownload signatuur pakket van de FTP server naar de router te kopiëren:**Kopie ftp://<*ftp_user:password@Server_IP_address*>/<*signatuur_Package*> idconfOpmerking:** Denk eraan om de *idconf*-parameter te gebruiken aan het einde van de opdracht kopiëren.**Opmerking:** Bijvoorbeeld:
   ```
   router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
   Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   [OK - 7608873/4096 bytes]
   ```
   De compilatie van de handtekening begint onmiddellijk nadat het pakket met de handtekening is geladen naar de router. U kunt de logbestanden op de router zien met houtkapniveau 6 of hoger ingeschakeld.
   ```
   *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. Gebruik de opdracht **toonaangevende IP IPS-handtekeningen** om te controleren of het pakket handtekeningen goed is samengesteld.Bijvoorbeeld:
   ```
   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#
```

Aanvullende opdrachten en referenties

De openbare sleutel van crypto is ongeldig als u een foutbericht op het tijdstip van de signatuur ontvangt gelijkend aan deze foutmelding:

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

Raadpleeg Stap 3 voor meer informatie.

Als u geen toegang tot een FTP- of TFTP-server hebt, kunt u een USB-flitser gebruiken om het pakket handtekeningen aan de router te laden. Kopieer eerst het signatuur-pakket naar de USB-schijf, sluit de USB-schijf aan op een van de USB-poorten op de router, en gebruik vervolgens de kopie-opdracht met de DICOM-parameter om het signatuur-pakket naar de router te kopiëren.

Bijvoorbeeld:

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

Er zijn zes bestanden in de geconfigureerde IOS IPS-opslagmap. Deze bestanden gebruiken deze naamindeling: <*router-name*>-sigdef-xxx.xml of <*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#
```

Deze bestanden worden in gecomprimeerde indeling opgeslagen en zijn niet rechtstreeks bewerkbaar of zichtbaar. De inhoud van elk bestand wordt hieronder beschreven:

- *router-sigdef-default.xml* bevat alle standaardinstellingen van de standaard fabriek voor de kenmerking.
- *router-sigdef-delta.xml* bevat kenmerkende definities die van de standaard zijn gewijzigd.
- *router-gesigneerd-type-xml* bevat alle definities van de kenmerkende parameter.
- *router-sigdef-Category.xml* bevat de informatie over de kenmerkcategorie, zoals elementair en geavanceerd voor categorie ios_ips.
- *router-seap-delta.xml* bevat wijzigingen die in de standaard MAP-parameters zijn aangebracht.
- *router-seap-typdef.xml* bevat alle MAP-parameterdefinities.

Deel II. Geavanceerde configuratieopties

Deze sectie verschaft instructies en voorbeelden van geavanceerde IOS IPS-opties voor het afstemmen van handtekeningen.

Ondertekeningen van Retire of Unpensioenar

Om met pensioen te gaan of ongedaan te maken betekent het het selecteren of deselecteren van de handtekeningen die door IOS IPS worden gebruikt om verkeer te scannen.

- **Het intrekken van** een handtekening betekent dat IOS IPS *deze* handtekening *NIET* in het geheugen *zal* samenstellen om te scannen.
- **Ontkoppelt** een handtekening instructies IOS IPS om de handtekening in geheugen te compileren en de handtekening te gebruiken om verkeer te scannen.

U kunt IOS commando-line interface (CLI) gebruiken om individuele handtekeningen of een groep handtekeningen die tot een signatuur behoren, terug te trekken of uit te sluiten. Als je een groep handtekeningen loslaat of uittrekt, worden alle handtekeningen in die categorie teruggetrokken of niet teruggetrokken.

Opmerking: Sommige niet-gepensioneerde handtekeningen (ofwel niet teruggetrokken als individuele handtekening of in een niet-teruggetrokken categorie) kunnen niet compileren vanwege onvoldoende geheugen of ongeldige parameters of als de handtekening is achterhaald.

Dit voorbeeld laat zien hoe je individuele handtekeningen moet intrekken. Bijvoorbeeld handtekening 6130 met subsidie-ID van 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)#
```

Dit voorbeeld toont hoe te om alle handtekeningen die tot de IOS Basis categorie behoren uit te schakelen:

```
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
```

Opmerking: Wanneer handtekeningen in andere categorieën dan IOS IPS Basic en IOS IPS Advanced niet als categorie worden beëindigd, kan de compilatie van sommige handtekeningen of motoren falen omdat bepaalde handtekeningen in die categorieën niet door IOS IPS worden ondersteund (zie voorbeeld hieronder). Alle andere succesvolle gecompileerde (niet-gepensioneerde) handtekeningen worden door IOS IPS gebruikt om verkeer te scannen.

```
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
```

Handtekeningen inschakelen of uitschakelen

Om een handtekening in te schakelen of uit te schakelen is of om de actie(s) die aan de handtekeningen door IOS IPS is gekoppeld, af te dwingen of te negeren wanneer de pakketstroom overeenkomt met de handtekeningen.

Opmerking: Schakel en uit (NIET selecteren en deselecteren) van handtekeningen die door IOS IPS gebruikt moeten worden.

- Om een handtekening **in** te **schakelen** betekent dit dat, wanneer de handtekening wordt geactiveerd door een bijpassend pakje (of pakketstroom), de betreffende handeling wordt uitgevoerd. Maar alleen niet gepensioneerde en succesvol gecompileerde handtekeningen kunnen de actie uitvoeren als ze zijn ingeschakeld. Met andere woorden, als een handtekening wordt teruggetrokken, ook al is hij ingeschakeld, zal hij niet worden samengesteld (omdat hij wordt teruggetrokken) en zal hij niet de daarmee samenhangende actie ondernemen.
- Om een handtekening **uit** te **schakelen** betekent dit dat wanneer de handtekening wordt geactiveerd door een bijpassend pakje (of pakketstroom), de handtekening NIET de juiste actie uitvoert die eraan is gekoppeld. Met andere woorden, wanneer een handtekening wordt uitgeschakeld, ook al is hij niet gepensioneerd en succesvol samengesteld, zal hij niet de daarmee samenhangende actie ondernemen.

U kunt IOS commando-line interface (CLI) gebruiken om individuele handtekeningen of een groep handtekeningen in te schakelen of uit te schakelen op basis van ondertekeningscategorieën. Dit voorbeeld toont hoe te om handtekening 6130 met subsidie-ID van 10 uit te schakelen.

```
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)#
```

Dit voorbeeld toont hoe te om alle handtekeningen toe te laten die tot de IOS IPS Basis categorie behoren.

```
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)#
```

Handelingen wijzigen

U kunt IOS commando-line interface (CLI) gebruiken om signatuur acties voor één handtekening of een groep handtekeningen te wijzigen op basis van signatuurcategorieën. Dit voorbeeld laat zien hoe u acties voor handtekening kunt wijzigen om te waarschuwen, te laten vallen en terug te zetten voor handtekening 6130 met subsidie-ID van 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)#
```

Dit voorbeeld toont hoe om gebeurtenis acties voor alle handtekeningen te veranderen die tot de kenmerkende IOS IPS Basis categorie behoren.

```
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)#
```

Gerelateerde informatie

- Cisco IOS IPS-pagina (Inbraakpreventiesysteem) voor producten en services
- Cisco IOS IPS - versie 5 Handtekeningen en softwaredownloads
- Verbeteringen in IPS 5.x-signaalindeling en bruikbaarheid

- Cisco Security Appliance Manager-software downloaden
- Gebruik CTP om IOS IPS te configureren
- Cisco Inbraakdetectiesysteem, Event Viewer 3DES-cryptografische softwaredownloads
- Technische ondersteuning en documentatie – Cisco Systems