Konfigurationsbeispiel für ein Intrusion Prevention System mit Signaturen im 5.x-Format

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Signaturen im 5.x-Format in Cisco IOS® IPS konfiguriert werden. Das Dokument ist in zwei Abschnitte unterteilt:

- Abschnitt I. Erste Schritte zur Konfiguration - In diesem Abschnitt werden die Schritte beschrieben, die zur Verwendung der Cisco IOS-Befehlszeilenschnittstelle (CLI) erforderlich sind, um mit Signaturen im IOS IPS 5.x-Format zu beginnen. In diesem Abschnitt werden die folgenden Schritte beschrieben:Schritt 1: Laden Sie die IOS IPS-Dateien herunter.Schritt 2: Erstellen Sie ein IOS IPS-Konfigurationsverzeichnis auf Flash.Schritt 3: Konfigurieren eines IOS IPS-VerschlüsselungsschlüsselsSchritt 4: Aktivieren Sie IOS IPS.Schritt 5: Laden Sie das IOS IPS-Signaturpaket in den Router.Jeder Schritt und bestimmte Befehle werden detailliert beschrieben sowie zusätzliche Befehle und Verweise. Unter jedem Befehl wird eine Beispielkonfiguration angezeigt.
- Abschnitt II. Erweiterte Konfigurationsoptionen - Dieser Abschnitt enthält Anweisungen und Beispiele zu erweiterten Optionen für die Signaturanpassung. Sie umfasst folgende Optionen:Signaturen aufheben oder außer Betrieb nehmenSignaturen aktivieren oder deaktivierenSignaturaktionen ändern

Voraussetzungen

Anforderungen

Vergewissern Sie sich, dass die richtigen Komponenten vorhanden sind (wie unter Verwendete Komponenten beschrieben), bevor Sie die Schritte in diesem Dokument durchführen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Ein Cisco Integrated Services Router (87x, 18xx, 28xx oder 38xx)
- 128 MB oder mehr DRAM und mindestens 2 MB freier Flash-Speicher
- Konsolen- oder Telnet-Verbindung zum Router
- Cisco IOS Release 12.4(15)T3 oder höher
- Ein gültiger Benutzername und ein gültiges Kennwort für die CCO-Anmeldung (Cisco.com)
- Aktueller Cisco IPS-Servicevertrag für lizenzierte Signatur-Update-Services

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Abschnitt I. Erste Schritte zur Konfiguration

Schritt 1: IOS IPS-Dateien herunterladen

Der erste Schritt besteht darin, die IOS IPS-Signaturpaket-Dateien und den öffentlichen Kryptoschlüssel von Cisco.com herunterzuladen.

Laden Sie die erforderlichen Signaturdateien von Cisco.com auf Ihren PC herunter:

- Standort: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (nur registrierte Kunden)
- Dateien zum Herunterladen:IOS-Sxxx-CLI.pkg (nur registrierte Kunden) - Dies ist das neueste Signaturpaket.realm-cisco.pub.key.txt (nur registrierte Kunden) - Dies ist der öffentliche Verschlüsselungsschlüssel, der von IOS IPS verwendet wird.

Schritt 2: Erstellen Sie ein IOS IPS-Konfigurationsverzeichnis auf Flash.

Im zweiten Schritt erstellen Sie ein Verzeichnis auf dem Flash-Speicher des Routers, in dem Sie die erforderlichen Signaturdateien und -konfigurationen speichern. Alternativ können Sie ein Cisco USB-Flash-Laufwerk verwenden, das an den USB-Port des Routers angeschlossen ist, um die Signaturdateien und -konfigurationen zu speichern. Das USB-Flash-Laufwerk muss mit dem USB-

Port des Routers verbunden bleiben, wenn es als Speicherort für das IOS IPS-Konfigurationsverzeichnis verwendet wird. IOS IPS unterstützt darüber hinaus jedes IOS-Dateisystem als Konfigurationsspeicherort mit entsprechendem Schreibzugriff.

Geben Sie den folgenden Befehl an der Router-Eingabeaufforderung ein, um ein Verzeichnis zu erstellen: **mkdir <*Verzeichnisname*>**

Beispiele:

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

Zusätzliche Befehle und Verweise

Um den Inhalt des Flash-Laufwerks zu überprüfen, geben Sie diesen Befehl an der Router-Eingabeaufforderung ein: **Flash anzeigen:**

Beispiele:

```
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)
```

Um den Verzeichnisnamen umzubenennen, verwenden Sie den folgenden Befehl: **umbenennen <*aktueller Name*> <*neuer Name*>**

Beispiele:

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

Schritt 3: Konfigurieren eines IOS IPS-Verschlüsselungsschlüssels

Der dritte Schritt besteht in der Konfiguration des vom IOS IPS verwendeten Verschlüsselungsschlüssels. Dieser Schlüssel befindet sich in der Datei realm-cisco.pub.key.txt, die in Schritt 1 heruntergeladen wurde.

Der Verschlüsselungsschlüssel wird verwendet, um die digitale Signatur für die Master-Signaturdatei (sigdef-default.xml) zu überprüfen, deren Inhalt von einem privaten Cisco Schlüssel signiert wird, um bei jeder Version ihre Authentizität und Integrität zu gewährleisten.

1. Öffnen Sie die Textdatei, und kopieren Sie den Inhalt der Datei.
2. Wechseln Sie mit dem Befehl **configure terminal** in den Router-Konfigurationsmodus.
3. Fügen Sie den Inhalt der Textdatei an der Eingabeaufforderung `<hostname>(config)#` ein.
4. Beenden Sie den Router-Konfigurationsmodus.
5. Geben Sie den Befehl **show run** an der Router-Eingabeaufforderung ein, um die Konfiguration des Verschlüsselungsschlüssels zu bestätigen. Diese Ausgabe sollte in der Konfiguration angezeigt werden:
   ```
   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. Verwenden Sie diesen Befehl, um die Konfiguration zu speichern:**Kopieren der ausgeführten Konfiguration des Startkonfigurators**

Zusätzliche Befehle und Verweise

Wenn der Schlüssel falsch konfiguriert ist, müssen Sie zuerst den Verschlüsselungsschlüssel entfernen und ihn dann neu konfigurieren:

1. Um den Schlüssel zu entfernen, geben Sie diese Befehle in der unten aufgeführten Reihenfolge ein:

```
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. Verwenden Sie den Befehl **show run**, um zu überprüfen, ob der Schlüssel aus der Konfiguration entfernt wurde.
3. Führen Sie das Verfahren in Schritt 3 aus, um den Schlüssel neu zu konfigurieren.

Schritt 4: IOS IPS aktivieren

Der vierte Schritt ist die Konfiguration von IOS IPS. Führen Sie dieses Verfahren aus, um IOS IPS zu konfigurieren:

1. Verwenden Sie den Befehl **ip ips name <*Regelname*> < *optionale ACL*>**, um einen Regelnamen zu erstellen. (Diese wird auf einer Schnittstelle verwendet, um IPS zu aktivieren.)Beispiele:

```
router#configure terminal
router(config)#ip ips name iosips
```

   Sie können eine erweiterte oder standardmäßige Zugriffskontrollliste (ACL) angeben, um den Datenverkehr, der mit diesem Regelnamen gescannt wird, zu filtern. Der gesamte von der ACL zugelassene Datenverkehr wird vom IPS überprüft. Von der ACL abgelehnter Datenverkehr wird vom IPS nicht überprüft.

```
router(config)#ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
```

2. Verwenden Sie den Befehl **ip ips config location flash:<*directory name*>**, um den Speicherort für das Speichern der IPS-Signatur zu konfigurieren. (Dies ist das in Schritt 2 erstellte *ips*-Verzeichnis.)Beispiele:

```
router(config)#ip ips config location flash:ips
```

3. Verwenden Sie den Befehl **ip ips notify sdee**, um die IPS SDEE-Ereignisbenachrichtigung zu aktivieren.Beispiele:
```
router(config)#ip ips notify sdee
```

   Um SDEE verwenden zu können, muss der HTTP-Server aktiviert sein (mit dem Befehl **ip http server**). Wenn der HTTP-Server nicht aktiviert ist, kann der Router nicht auf die SDEE-Clients reagieren, da er die Anfragen nicht sehen kann. Die SDEE-Benachrichtigung ist standardmäßig deaktiviert und muss explizit aktiviert werden.IOS IPS unterstützt auch die Verwendung von Syslog, um Ereignisbenachrichtigungen zu senden. SDEE und Syslog können unabhängig voneinander verwendet oder gleichzeitig aktiviert werden, um IOS IPS-Ereignisbenachrichtigungen zu senden. Die Syslog-Benachrichtigung ist standardmäßig aktiviert. Wenn die Protokollkonsole aktiviert ist, werden IPS-Syslog-Meldungen angezeigt. Verwenden Sie den folgenden Befehl, um Syslog zu aktivieren:
```
router(config)#ip ips notify log
```

4. Konfigurieren Sie IOS IPS so, dass eine der vordefinierten Signaturkategorien verwendet wird.IOS IPS mit Signaturen im Cisco 5.x-Format wird mit Signaturkategorien betrieben (genau wie Cisco IPS-Appliances). Alle Signaturen sind in Kategorien gruppiert, und die Kategorien sind hierarchisch. So können Signaturen einfacher gruppiert und angepasst werden.**Warnung:** Die Kategorie Alle Signaturen enthält alle Signaturen in einer Signaturversion. Da IOS IPS nicht alle in einer Signaturversion enthaltenen Signaturen gleichzeitig kompilieren und verwenden kann, *sollten nicht alle Kategorien außer Kraft gesetzt werden*. Andernfalls ist der Arbeitsspeicher des Routers nicht mehr verfügbar.**Hinweis:** Wenn Sie IOS IPS konfigurieren, müssen Sie zunächst alle Signaturen in der Kategorie "*Alle*" außer Kraft setzen und anschließend ausgewählte Signaturkategorien aufheben.**Hinweis:** Die Reihenfolge, in der die Signaturkategorien auf dem Router konfiguriert werden, ist ebenfalls wichtig. IOS IPS verarbeitet die Kategoriebefehle in der in der Konfiguration angegebenen Reihenfolge. Einige Signaturen gehören mehreren Kategorien an. Wenn mehrere Kategorien konfiguriert werden und eine Signatur zu mehr als einer von ihnen gehört, werden die Eigenschaften der Signatur (z. B. außer Betrieb genommen, nicht eingestellt, Aktionen usw.) in der zuletzt konfigurierten Kategorie von IOS IPS verwendet.In diesem Beispiel werden alle Signaturen in der Kategorie "all" (Alle) außer Kraft gesetzt. Anschließend wird die Kategorie *IOS IPS Basic* nicht mehr eingestellt.
```
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. Verwenden Sie diese Befehle, um die IPS-Regel auf der gewünschten Schnittstelle zu aktivieren, und geben Sie die Richtung an, in der die Regel angewendet wird:**interface <*Schnittstellenname*>ip ips <*Regelname*> [*in | out*]**Beispiele:
```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#exit
router(config)#exit
router#
```

Das *in*-Argument bedeutet, dass nur der Datenverkehr, der in die Schnittstelle geleitet wird, vom IPS überprüft wird. Das *out*-**Argument** bedeutet, dass nur Datenverkehr, der die Schnittstelle verlässt, vom IPS überprüft wird.Damit IPS sowohl den ein- als auch den ausgehenden Datenverkehr der Schnittstelle überprüfen kann, geben Sie den IPS-Regelnamen für *ein* und **aus** derselben Schnittstelle separat ein:

```
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#
```

Schritt 5: Laden des IOS IPS-Signaturpakets auf den Router

Der letzte Schritt besteht darin, das in Schritt 1 heruntergeladene Signaturpaket auf den Router zu laden.

Hinweis: Die häufigste Methode zum Laden des Signaturpakets auf den Router ist die Verwendung von FTP oder TFTP. Diese Prozedur verwendet FTP. Eine alternative Methode zum Laden des IOS IPS-Signaturpakets finden Sie im Abschnitt *Zusätzliche Befehle und Verweise* in diesem Verfahren. Wenn Sie eine Telnet-Sitzung verwenden, verwenden Sie den Befehl **terminal monitor**, um die Konsolenausgaben anzuzeigen.

Führen Sie die folgenden Schritte aus, um das Signaturpaket auf den Router zu laden:

1. Verwenden Sie diesen Befehl, um das heruntergeladene Signaturpaket vom FTP-Server auf den Router zu kopieren:**copy ftp://<*ftp_user:password@Server_IP_address*>/<*signatur_package*> idconfHinweis:** Denken Sie daran, den *idconf*-***Parameter am Ende des copy***-Befehls zu verwenden.**Hinweis:** Beispiel:

   ```
   router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
   Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   [OK - 7608873/4096 bytes]
   ```

   Die Signaturkompilierung beginnt unmittelbar nach dem Laden des Signaturpakets auf den Router. Sie können die Protokolle auf dem Router sehen, bei denen die Protokollierungsebene 6 oder höher aktiviert ist.

   ```
   *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. Verwenden Sie den Befehl **show ip ips signature count**, um zu überprüfen, ob das Signaturpaket korrekt kompiliert wurde.Beispiele:

```
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#
```

Zusätzliche Befehle und Verweise

Der öffentliche Kryptografieschlüssel ist ungültig, wenn Sie bei der Signaturkompilierung eine Fehlermeldung ähnlich der folgenden Fehlermeldung erhalten:

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

Weitere Informationen finden Sie in Schritt 3.

Wenn Sie keinen Zugriff auf einen FTP- oder TFTP-Server haben, können Sie ein USB-Flash-Laufwerk verwenden, um das Signaturpaket auf den Router zu laden. Kopieren Sie zunächst das Signaturpaket auf das USB-Laufwerk, verbinden Sie das USB-Laufwerk mit einem der USB-Ports am Router, und verwenden Sie dann den Befehl **copy** mit dem **Parameter *idconf***, um das Signaturpaket auf den Router zu kopieren.

Beispiele:

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

Das konfigurierte IOS IPS-Speicherverzeichnis enthält sechs Dateien. Diese Dateien verwenden das folgende Namensformat: <*router-name*>-sigdef-xxx.xml oder <*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#
```

Diese Dateien werden im komprimierten Format gespeichert und können nicht direkt bearbeitet oder angezeigt werden. Der Inhalt jeder Datei wird nachfolgend beschrieben:

- *router-sigdef-default.xml* enthält alle standardmäßigen Signaturdefinitionen.
- *router-sigdef-delta.xml* enthält Signaturdefinitionen, die vom Standardwert geändert wurden.
- *router-sigdef-typedef.xml* enthält alle Definitionen der Signaturparameter.
- *router-sigdef-category.xml* enthält Informationen zur Signaturkategorie, z. B. Kategorie ios_ips basic und advanced.
- *router-seap-delta.xml* enthält Änderungen an den Standard-SEAP-Parametern.
- *router-seap-typedef.xml* enthält alle SEAP-Parameterdefinitionen.

Abschnitt II. Erweiterte Konfigurationsoptionen

Dieser Abschnitt enthält Anweisungen und Beispiele zu erweiterten IOS IPS-Optionen für die Signaturanpassung.

Signaturen aufheben oder aufheben

Signaturen außer Kraft zu setzen oder außer Kraft zu setzen, bedeutet, die Signaturen auszuwählen oder zu deaktivieren, die von IOS IPS zum Scannen von Datenverkehr verwendet werden.

- **Das Zurücksetzen** einer Signatur bedeutet, dass IOS IPS diese Signatur *NICHT* zum Scannen in den Speicher kompiliert.
- **Durch das Auslösen** einer Signatur wird IOS IPS angewiesen, die Signatur in den Speicher zu kompilieren und die Signatur zum Prüfen des Datenverkehrs zu verwenden.

Sie können die IOS-Befehlszeilenschnittstelle (CLI) verwenden, um einzelne Signaturen oder eine Gruppe von Signaturen, die zu einer Signaturkategorie gehören, außer Kraft zu setzen bzw. zu entfernen. Wenn Sie eine Gruppe von Signaturen aus dem Ruhestand setzen oder aus dem Ruhestand treten, werden alle Signaturen dieser Kategorie entfernt oder nicht mehr in den Ruhestand gesetzt.

Hinweis: Einige nicht pensionierte Signaturen (entweder nicht als einzelne Signatur oder in einer nicht pensionierten Kategorie) werden möglicherweise nicht kompiliert, da der Speicher nicht ausreicht oder die Parameter ungültig sind oder die Signatur veraltet ist.

In diesem Beispiel wird veranschaulicht, wie einzelne Signaturen entfernt werden. Signatur 6130 mit Submit-ID 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)#
```

In diesem Beispiel wird veranschaulicht, wie alle Signaturen aus der Kategorie IOS IPS Basic entfernt werden:

```
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
```

Hinweis: Wenn Signaturen in anderen Kategorien als IOS IPS Basic und IOS IPS Advanced nicht als Kategorie eingestellt werden, kann die Kompilierung einiger Signaturen oder Engines fehlschlagen, da bestimmte Signaturen in diesen Kategorien nicht von IOS IPS unterstützt werden (siehe Beispiel unten). Alle anderen erfolgreich kompilierten (nicht pensionierten) Signaturen werden von IOS IPS zum Durchsuchen des Datenverkehrs verwendet.

```
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
```

Signaturen aktivieren oder deaktivieren

Um eine Signatur zu aktivieren oder zu deaktivieren, müssen die den Signaturen von IOS IPS zugeordneten Aktionen durchgesetzt oder ignoriert werden, wenn Paket- oder Paketfluss mit den Signaturen übereinstimmt.

Hinweis: Bei Aktivierung und Deaktivierung werden KEINE Signaturen für IOS IPS ausgewählt und deaktiviert.

- Die **Aktivierung** einer Signatur bedeutet, dass die Signatur, wenn sie durch ein übereinstimmendes Paket (oder Paketfluss) ausgelöst wird, die ihr zugeordnete entsprechende Aktion ausführt. Wenn sie aktiviert sind, werden jedoch nur nicht pensionierte UND erfolgreich kompilierte Signaturen ausgeführt. Mit anderen Worten: Wenn eine Signatur zurückgestellt wird, obwohl sie aktiviert ist, wird sie nicht kompiliert (weil sie entfernt wird) und nicht die ihr zugeordnete Aktion ausgeführt.

- Die **Deaktivierung** einer Signatur bedeutet, dass die Signatur, wenn sie durch ein übereinstimmendes Paket (oder einen übereinstimmenden Paketfluss) ausgelöst wird, NICHT die entsprechende Aktion durchführt, die ihr zugeordnet ist. Mit anderen Worten: Wenn eine Signatur deaktiviert ist, obwohl sie nicht eingestellt und erfolgreich kompiliert wurde, wird sie nicht die ihr zugeordnete Aktion ausführen.

Sie können die IOS-Befehlszeilenschnittstelle (CLI) verwenden, um einzelne Signaturen oder eine Gruppe von Signaturen auf der Grundlage von Signaturkategorien zu aktivieren oder zu deaktivieren. In diesem Beispiel wird veranschaulicht, wie die Signatur 6130 mit der Submit-ID 10 deaktiviert wird.

```
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)#
```

In diesem Beispiel wird veranschaulicht, wie alle Signaturen aktiviert werden, die der Kategorie IOS IPS Basic angehören.

```
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)#
```

Signaturaktionen ändern

Sie können die IOS-Befehlszeilenschnittstelle (CLI) verwenden, um Signaturaktionen für eine Signatur oder eine Gruppe von Signaturen auf der Grundlage von Signaturkategorien zu ändern. In diesem Beispiel wird veranschaulicht, wie Signaturaktionen geändert werden, um Warnungen, Löschvorgänge und Rücksetzvorgänge für Signatur 6130 mit der Submit-ID 10 auszugeben.

```
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)#
```

In diesem Beispiel wird veranschaulicht, wie Ereignisaktionen für alle Signaturen geändert

werden, die der Kategorie IOS IPS Basic angehören.

```
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)#
```

Zugehörige Informationen

- Cisco IOS Intrusion Prevention System (IPS) - Produkte und Services-Seite
- Cisco IOS IPS - Version 5 Signatures Software-Download
- Unterstützung für IPS 5.x-Signaturformat und verbesserte Benutzerfreundlichkeit
- Cisco Security Device Manager-Software herunterladen
- Konfigurieren von IOS IPS mithilfe von CCP
- Cisco Intrusion Detection System Event Viewer 3DES Cryptographic Software Download
- Technischer Support und Dokumentation für Cisco Systeme