侵入防御システムでの 5.x 形式シグニチャの設定例

目次

概要

このドキュメントでは、Cisco IOS® IPS で 5.x 形式シグニチャを設定する方法について、2 つのセクションに分けて説明します：

- セクション I. 設定手順について：このセクションでは、Cisco IOS コマンドライン インターフェイス（CLI）を使用して IOS IPS 5.x 形式シグニチャを使用するための手順について説明します。 このセクションでは次の手順について説明します。手順 1：IOS IPS ファイルのダウンロード。手順 2：フラッシュでの IOS IPS 設定ディレクトリの作成。手順 3：IOS IPS 暗号キーの設定。手順 4：IOS IPS の有効化。手順 5：ルータへの IOS IPS シグニチャ パッケージのロード。各ステップと固有のコマンドについて詳しく説明し、追加コマンドと参照情報も記載されています。 各コマンドの後に設定例を示します。
- セクション II.高度な設定オプション：このセクションでは、シグニチャ調整の高度なオプションの使用手順と例を示します。 次のオプションについて説明します。シグニチャのリタイアまたはアンリタイアシグニチャの有効化または無効化シグニチャ アクションの変更

前提条件

要件

このドキュメントで説明する手順を実行する前に、（「使用するコンポーネント」で説明されている）適切なコンポーネントを使用していることを確認してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Integrated Services Router（87x、18xx、28xx、または 38xx）
- 128 MB 以上の DRAM および 2 MB 以上の空き容量があるフラッシュ メモリ
- コンソールまたはルータへの telnet 接続
- Cisco IOS Release 12.4(15)T3 以降
- 有効な CCO（Cisco.com）ログイン ユーザ名とパスワード
- ライセンスを購入したシグニチャ更新サービスの現行 Cisco IPS サービス契約

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

セクション I. 設定手順について

手順 1：IOS IPS ファイルのダウンロード

1 番目のステップとして、IOS IPS シグニチャ パッケージ ファイルと公開暗号キーを Cisco.com からダウンロードします。

必要なシグニチャ ファイルを Cisco.com から PC にダウンロードします。

- 場所： http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup（登録ユーザのみ）
- ダウンロードするファイル：IOS-Sxxx-CLI.pkg（登録ユーザのみ）：最新のシグニチャ パッケージです。realm-cisco.pub.key.txt（登録ユーザのみ）：IOS IPS が使用する公開暗号キーです。

手順 2：フラッシュでの IOS IPS 設定ディレクトリの作成

2 番目のステップとして、必要なシグニチャ ファイルと設定を保存するためのディレクトリをルータのフラッシュに作成します。 あるいは Cisco USB フラッシュ ドライブをルータの USB ポートに接続し、このフラッシュ ドライブにシグニチャ ファイルと設定を保存します。 USB フラッシュ ドライブを IOS IPS 設定ディレクトリの作成先として使用する場合、USB フラッシュ ドライブをルータの USB ポートに接続したままにする必要があります。 IOS IPS では、適切な書き込みアクセス権限のある設定の保存先として任意の IOS ファイル システムも使用できます。

ディレクトリを作成するため、ルータのプロンプトで次のコマンドを入力します。 **mkdir <directory name>**

次に、例を示します。

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

追加のコマンドと参照情報

フラッシュの内容を確認するには、ルータのプロンプトで次のコマンドを入力します。 **show flash:**

次に、例を示します。

```
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)
```

ディレクトリ名を変更するには、次のコマンドを使用します。 **rename <current name> <new name>**

次に、例を示します。

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

手順 3：IOS IPS 暗号キーの設定

3 番目のステップとして、IOS IPS が使用する暗号キーを設定します。 このキーは、「ステップ 1」でロードした realm-cisco.pub.key.txt ファイルに格納されています。

暗号キーは、マスター シグニチャ ファイル（sigdef-default.xml）のデジタル署名を検証するために使用されます。マスター シグニチャ ファイルの内容は、すべてのリリースでの真正性および整合性を保証するために、シスコの秘密キーによって署名されています。

1. テキスト ファイルを開いてファイルの内容をコピーします。
2. **configure terminal** コマンドを使用してルータ コンフィギュレーション モードに切り替えます。
3. テキスト ファイルの内容を <hostname>(config)# プロンプトに貼り付けます。
4. ルータ コンフィギュレーション モードを終了します。
5. 暗号キーが設定されていることを確認するため、ルータ プロンプトに **show run** コマンドを入力します。 設定に次のように出力されていることを確認します。
```
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. 次のコマンドを使用して設定を保存します。**copy running-configure startup-configure**

追加のコマンドと参照情報

暗号キーの設定が誤っている場合、暗号キーを最初に削除してから再設定する必要があります。

1. キーを削除するには、次のコマンドを示されている順序で入力します。
```
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. **show run** コマンドを使用して、設定からキーが削除されているかどうかを確認します。
3. 「ステップ 3」の手順を実行してキーを再設定します。

手順 4：IOS IPS の有効化

4 番目のステップとして IOS IPS を設定します。 IOS IPS を設定するには次の手順を実行します。

1. **ip ips name <rule name> < optional ACL>** コマンドを使用してルール名を作成します。（これは IPS を有効にするためにインターフェイスで使用されます）次に、例を示します。`router#configure terminal router(config)#ip ips name iosips` このルール名によってスキャンされるトラフィックをフィルタリングするため、オプションで拡張アクセス コントロール リスト（ACL）または標準アクセス コントロール リストを指定できます。 ACL により許可されるトラフィックはすべて IPS により検査されます。 ACL により拒否されるトラフィックは IPS の検査対象ではありません。`router(config)#ip ips name ips list ? <1-199> Numbered access list WORD Named access list`
2. **ip ips config location flash: <directory name>** コマンドを使用して、IPS シグニチャの保存場所を設定します。（これは「*ステップ 2*」で作成した ips ディレクトリです）次に、例を示します。`router(config)#ip ips config location flash:ips`
3. **ip ips notify sdee** コマンドを使用して IPS SDEE イベント通知を有効にします。次に、例を示します。`router(config)#ip ips notify sdee` SDEE を使用するには、HTTP サーバが（**ip http server** コマンドを使用して）有効にされている必要があります。 HTTP サーバが有効でないと、ルータは要求を認識できないため SDEE クライアントに対して応答できません。デフォルトでは SDEE 通知は無効になっているため、明示的に有効にする必要があります。IOS IPS では syslog を使用してイベント通知を送信することもできます。 IOS IPS イベント通知を送信するために、SDEE と syslog はそれぞれ個別に使用するか、または同時に有効に設定することができます。 デフォルトでは syslog 通知は有効になっています。 コンソールのロギングが有効になっている場合は IPS syslog メッセージが表示されます。 syslog を有効にするには次のコマンドを使用します。`router(config)#ip ips notify log`
4. 事前に定義されているシグニチャ カテゴリの 1 つを使用するように IOS IPS を設定します。Cisco 5.x 形式のシグニチャを使用する IOS IPS は（Cisco IPS アプライアンスと同様に）シグニチャ カテゴリを使用して動作します。 すべてのシグニチャは階層型のカテゴリに分類されます。 これにより、シグニチャを分類してグループ化と調整を容易に実行できます。**警告：** すべてのシグニチャ カテゴリにシグニチャ リリースのすべてのシグニチャが含まれています。 シグニチャ リリースに含まれているすべてのシグニチャを IOS IPS が一括でコンパイルおよび使用できない場合、*すべてのカテゴリをアンリタイアしないでください*。 このようにすると、ルータのメモリが不足します。**注:** IOS IPS を設定するときには、最初に すべてのカテゴリのすべてのシグニチャをリタイアしてから、選択したシグニチャ カテゴリをアンリタイアする必要があります。**注:** ルータでのシグニチャ カテゴリの設定順序も重要です。 IOS IPS は設定にリストされている順序でカテゴリ コマンドを処理します。 複数のカテゴリに属しているシグニチャがあります。 複数のカテゴリを設定しており、1 つのシグニチャが 2 つ以上のカテゴリに属している場合、最後に設定したカテゴリのシグニチャのプロパティ（リタイア、アンリタイア、アクションなど）が IOS IPS によって使用されます。次の例では、「all」カテゴリのすべてのシグニチャをリタイアした後に、*IOS IPS Basic* カテゴリがアンリタイアされます。`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. 次のコマンドを使用して、使用するインターフェイスで IPS ルールを有効にし、ルールの適用方向を指定します。**interface <interface name>ip ips <rule name> [in / out]**次に、例を示します。`router(config)#interface GigabitEthernet 0/1 router(config-if)#ip ips iosips in router(config-if)#exit router(config)#exit router#` **in** 引数は、インターフェイスに入るトラフィックだけが IPS により検査されることを意味します。 **out** 引数は、インターフェイスから出るトラフィックだけが IPS により検査されることを意味します。IPS でインターフェイスの両方向のトラフィックの検査を有効にするには、同じインターフェイスで **in** と **out** の IPS ルール名を個別に入力します。`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#`

手順 5：ルータへの IOS IPS シグニチャ パッケージのロード

最後のステップとして、「手順 1」でダウンロードしたシグニチャ パッケージをルータにロードします。

注: シグニチャ パッケージをルータにロードする最も一般的な方法は、FTP または TFTP を使用する方法です。 この手順では FTP を使用します。 IOS IPS シグニチャ パッケージをロードする他の方法については、この手順の「*追加コマンドと参照情報*」を参照してください。 telnet セッションを使用する場合は、**terminal monitor** コマンドを使用してコンソール出力を表示します。

シグニチャパッケージをルータにロードするには、次の手順を実行します。

1. 次のコマンドを使用して、FTP サーバからダウンロードしたシグニチャ パッケージをルータにコピーします。**copy ftp://<ftp_user: password@Server_IP_address>/<signature_package> idconf注: copy** コマンドの終わりに必ず **idconf** パラメータを指定してください。**注:** 次に、例を示します。`router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK - 7608873/4096 bytes]` シグニチャ パッケージがルートにロードされた直後にシグニチャ コンパイルが開始されます。 ログ レベル 6 以上が有効に設定されているルータではログを確認できます。`*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. **show ip ips signature count** コマンドを使用してシグニチャ パッケージが適切にコンパイル

されているかどうかを確認します。次に、例を示します。`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#`

追加のコマンドと参照情報

シグニチャ コンパイル時に次のようなエラー メッセージが表示される場合は、公開暗号キーが無効です。

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

詳細については「ステップ 3」を参照してください。

FTP サーバまたは TFTP サーバにアクセスできない場合は、USB フラッシュ ドライブを使用してルータをシグニチャ パッケージにロードできます。 最初にシグニチャ パッケージを USB ドライブにコピーし、USB ドライブをルータの USB ポートの 1 つに接続し、**idconf** パラメータを指定した **copy** コマンドを使用してシグニチャ パッケージをルータにコピーします。

次に、例を示します。

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

設定された IOS IPS 保管ディレクトリに 6 つのファイルがあります。 これらのファイルの名前の形式は <router-name>-sigdef-xxx.xml or < 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#
```

これらのファイルは圧縮形式で保存されており、直接編集または表示することはできません。 次に各ファイルの内容について説明します。

- *router-sigdef-default.xml* には、工場出荷時のデフォルト シグニチャ定義が含まれています。
- *router-sigdef-delta.xml* には、デフォルトから変更されたシグニチャ定義が含まれています。
- *router-sigdef-typedef.xml* には、すべてのシグニチャ パラメータ定義が含まれています。
- *router-sigdef-category.xml* には、シグニチャ カテゴリ情報（カテゴリ ios_ips basic や advanced など）が含まれています。
- *router-seap-delta.xml* には、デフォルト SEAP パラメータの変更内容が含まれています。
- *router-seap-typedef.xml* には、すべての SEAP パラメータ定義が含まれています。

セクション II.高度な設定オプション

このセクションでは、シグニチャを調整するための高度な IOS IPS オプションの手順と例を説明します。

シグニチャのリタイアまたはアンリタイア

シグニチャのリタイアまたはアンリタイアとは、トラフィックをスキャンするために IOS IPS により使用されるシグニチャを選択または選択解除することです。

- シグニチャの**リタイア**では、IOS IPS はスキャンのためにそのシグニチャをコンパイルしてメモリに格納しません。
- シグニチャの**アンリタイア**では、IOS IPS に対しシグニチャをコンパイルしてメモリに格納し、トラフィックのスキャンにそのシグニチャを使用するよう指示します。

個々のシグニチャ、または特定のシグニチャ カテゴリに属するシグニチャのグループをリタイアまたはアンリタイアするには、IOS コマンドライン インターフェイス（CLI）を使用します。 シグニチャ グループをリタイアまたはアンリタイアすると、そのカテゴリのすべてのシグニチャがリタイアまたはアンリタイアされます。

注: アンリタイアされたシグニチャ（個別にアンリタイアされているか、またはアンリタイアされたカテゴリに属しているシグニチャ）は、メモリ不足または誤ったパラメータが原因でコンパイルされないことがあります。また、シグニチャが古い場合にもコンパイルされません。

次の例に、個々のシグニチャのリタイア手順を示します。 たとえば、subsig ID が 10 のシグニチャ 6130 の場合は次のようになります。

```
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)#
```

次の例に、IOS IPS Basic カテゴリに属するすべてのシグニチャをアンリタイアする手順を示します。

```
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
```

注: IOS IPS Basic または IOS IPS Advanced 以外のカテゴリのシグニチャがカテゴリ単位でアンリタイアされると、一部のシグニチャまたはエンジンのコンパイルが失敗することがあります。これは、このようなカテゴリの一部のシグニチャが IOS IPS でサポートされていないためです（次の例を参照）。 正常にコンパイル（アンリタイア）されたその他のシグニチャはすべて IOS IPS がトラフィックをスキャンするために使用します。

```
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
```

シグニチャの有効化または無効化

シグニチャを有効または無効にすることで、パケットまたはパケット フローがシグニチャに一致するときに IOS IPS によりシグニチャに関連付けられているアクションが施行または無視されます。

注: 有効または無効にする操作は、IOS IPS が使用するシグニチャを選択または選択解除する操作ではありません。

- シグニチャを**有効にする**と、一致するパケット（またはパケット フロー）によってトリガーされた場合に、シグニチャに関連付けられている適切なアクションが実行されます。 ただし、シグニチャが有効に設定されている場合、アンリタイアされておりかつ正常にコンパイルされているシグニチャだけがアクションを実行します。 つまりシグニチャをリタイアすると、そのシグニチャが有効な場合でも（リタイアされているため）コンパイルされず、関連付けられているアクションが実行されません。
- シグニチャを**無効にする**と、一致するパケット（またはパケット フロー）によってトリガーされた場合に、シグニチャに関連付けられている適切なアクションが実行されません。 つまりシグニチャが無効にされると、そのシグニチャがアンリタイアされ正常にコンパイルされている場合でも、関連付けられているアクションが実行されません。

IOS コマンドライン インターフェイス（CLI）を使用して、シグニチャ カテゴリに基づいて個別のシグニチャまたはシグニチャ グループを有効または無効にできます。 次の例に、subsig ID が 10 のシグニチャ 6130 を無効にする方法を示します。

```
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)#
```

次の例に、IOS IPS Basic カテゴリに属するすべてのシグニチャを有効にする方法を示します。

```
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)#
```

シグニチャ アクションの変更

IOS コマンドライン インターフェイス（CLI）を使用して、1 つのシグニチャまたはシグニチャ グループのシグニチャ アクションを、シグニチャのカテゴリに基づいて変更できます。 次の例に、subsig ID が 10 のシグニチャ 6130 のシグニチャ アクションをアラート、ドロップ、リセットに変更する方法を示します。

```
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)#
```

次の例に、シグニチャ IOS IPS Basic カテゴリに属するすべてのシグニチャのイベント アクションを変更する方法を示します。

```
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)#
```

関連情報

- Cisco IOS 侵入防御システム（IPS）製品 & サービス ページ
- Cisco IOS IPS - バージョン 5 シグニチャ ソフトウェアのダウンロード
- IPS 5.x シグニチャ形式のサポートおよびユーザビリティ拡張
- Cisco Security Device Manager ソフトウェアのダウンロード
- CCP を使用した IOS IPS の設定方法
- Cisco Intrusion Detection System Event Viewer 3DES 暗号化ソフトウェアのダウンロード
- テクニカルサポートとドキュメント - Cisco Systems