IPSシグニチャ形式4.xから5.xへの移行

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[バージョン 4.x SDF ファイルへの移行手順](#)
[Cisco IOS IPS 移行スクリプトの実行](#)
[Cisco IOS ソフトウェア リリース 12.4(11)T の Cisco IOS IPS への、移行したシグニチャのロード](#)
[関連情報](#)

概要

Cisco IOS® リリース 12.4(11)T 以降、Cisco IOS 侵入防御システム（IPS）では、Cisco IPS ソフトウェア バージョン 5.x シグニチャ形式がサポートされます。5.x シグニチャ形式は、Cisco アプライアンス ベースのその他の IPS 製品でも使用されている、バージョン ベースのシグニチャ定義 XML 形式です。Cisco IPS バージョン 4.x のシグニチャおよびシグニチャ定義ファイル（SDF）は、現在のリリース以降の Cisco IOS T トレイン ソフトウェア リリースではサポートされなくなります。

バージョン 4.x シグニチャ形式の SDF で Cisco IOS IPS を実行しているお客様は、事前定義済みの Cisco シグニチャ カテゴリである Basic および Advanced シグニチャ セット、または Cisco IOS IPS 移行ユーティリティを使用して、以前のバージョン 4.x SDF ファイルを Cisco IPS バージョン 5.x 形式のシグニチャ セットに移行できるように、Cisco IOS IPS を再設定できます。

このドキュメントでは、Cisco IPS 4.x 形式の SDF から移行する方法、および移行したシグニチャ セットを Cisco IOS リリース 12.4(11)T 以降で有効にする方法について説明します。Cisco IOS リリース 12.4(11)T 以降の Cisco IOS IPS の設定方法の詳細は、『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』を参照してください。

注：Cisco IOSリリース12.4(11)T以降のイメージにアップグレードする前に、Cisco IOS IPSの移行を実行することを推奨します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS リリース 12.4(11)T 以降に基づくものです。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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。

バージョン 4.x SDF ファイルへの移行手順

移行スクリプトには、Cisco IOS リリース 12.4(11)T より前のリリースが稼働しているルータで使用される Cisco IOS IPS 設定情報を含む Cisco IPS 4.x 形式の SDF ファイルと、（オプションで）CLI 設定ファイルが必要です。

移行スクリプトはルータの設定ファイル内で、「**ip ips signature <sigid> [<sigsubid>] disabled**」を含むコマンドを検索します。設定ファイルにこの CLI コマンドが含まれていない場合、移行スクリプトで CLI 設定ファイルを読み取る必要はありません。シグニチャの変換は、SDF のみに基づいて行われることになります。

Cisco IOS IPS を Cisco IOS リリース 12.4(11)T 以降にアップグレードする前に移行スクリプトを実行する場合は、「Cisco IOS IPS 移行スクリプトの実行」に記載された処理に従ってください。

Cisco IOS IPS を Cisco IOS リリース 12.4(11)T 以降にアップグレードした後で移行スクリプトを実行する場合は、次の手順を実行します。

1. 前述のように、CLI コマンド **ip ips signature <sigid> [<sigsubid>] disabled** を変換する必要がないか確認します。
2. コマンド **copy running-config flash:ipscfg.cfg** を使用して、ルータの CLI 設定をファイルに保存します。このコマンドは、既存のルータ設定を、*ipscfg.cfg* というファイルのフラッシュにバックアップします。移行プロセスはこのファイルを使用して、シグニチャ形式を 4.x から 5.x に完全に変換します。
3. 「Cisco IOS IPS 移行スクリプトの実行」に進みます。

Cisco IOS IPS 移行スクリプトの実行

移行スクリプトは、次の URL の Cisco.com から入手できます：http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup移行スクリプトをルータのフラッシュ、またはルータからアクセス可能な場所（Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）サーバなど）に保存します。

移行スクリプトは SDF を、Cisco IPS バージョン 4.x 形式からバージョン 5.x 形式に変換します。移行スクリプトは、次のシグニチャ パラメータのみをサポートしています。

- severity
- action
- enabled

また、移行スクリプトは IOS IPS 設定ファイルを読み取って、Cisco IOS リリース 12.4(11)T より前のリリースで CLI の **ip ips signature <sigid> <sigsubid> disabled** コマンドで設定された無効化されたシグニチャを移行することもできます。

注：カスタム(シスコ以外の)シグネチャは、このスクリプトでは変換されません。

次の例は、IPS 4.x 形式のファイル *sdmips.sdf* を、Cisco IOS IPS 5.x シグニチャ形式をサポートする Cisco IOS リリース 12.4(11)T の Cisco IOS IPS に移行する方法を示しています。

```
C2821#tclsh flash:ios-ips-migrate.tbc
This migration script will migrate Signature Definition Files
     from 4.x format to 5.x format.
The migration script will migrate only the following signature
     parameters - severity, action, enabled - for Cisco (non-custom) signatures.
Do you want to continue? [y/n] y
Please choose an IOS config file from which to migrate IOS IPS configuration.
Config File: [startup-config]
The following SDF locations were found configured in startup-config:
  flash://sdmips.sdf
Please provide SDF to migrate from the above list or of your own
     choice: flash:// sdmips.sdf
Migrating following SDF file (this will a take few minutes):
  flash://sdmips.sdf
Time Elapsed: 0:02:23
Migration completed successfully. The migrated file is
  C2821-sigdef-delta.xml
C2821#
```

最初に、移行スクリプトは、その関数に関する簡単なテキストを表示します。次に、現在（移行前）の Cisco IOS IPS の設定を読み取る場所を選択するオプションが提供されます。デフォルトでは、スタートアップ コンフィギュレーションから読み取られます。以前に設定を TFTP サーバやルータのフラッシュに保存した場合は、プロンプトでその場所を指定します。

以下に、いくつかの例を示します。

TFTP サーバ 192.168.1.5 から CLI 設定をロードするようにスクリプトに通知する場合は、**tftp://192.168.1.5/<router CLI configuration> を使用します。**

フラッシュ上に保存されたファイルから読み取る場合は、**flash://<saved-configuration> を使用します。**

Cisco IOS ソフトウェア リリース 12.4(11)T の Cisco IOS IPS への、移行したシグニチャのロード

シグニチャの移行が完了したら、まだ行っていない場合は、ルータのイメージを Cisco IOS リリース 12.4(11)T にアップグレードします。ルータをリロードしたら、次の手順を実行します。

1. Cisco IOS IPS を有効にします。次の出力は、Cisco 2821 ルータで Cisco IOS IPS を有効にする方法を示しています。Cisco IOS IPS の設定方法の詳細は、『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』を参照してください。

   ```
   C2821#mkdir ips
   Create directory filename [ips]?
   Created dir flash:ips
   C2821#conf t
   Enter configuration commands, one per line. End with CNTL/Z.
   C2821(config)#ip ips name MYIPS
   ```

```
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
C2821(config)#
```

2. 次のキーをルータにコピー アンド ペーストして、暗号シグニチャの公開キーを設定します。

```
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
 exit
 exit
```

3. 次の例に示すように、インターフェイス上の Cisco IOS IPS を有効にします：

```
C2821(config)#
C2821(config)#interface gigabitEthernet 0/0
C2821(config-if)#ip ips MYIPS in
C2821(config-if)#ip ips MYIPS out
C2821(config-if)#exit
```

4. **copy** コマンドを使用して、最新のシグニチャ パッケージをロードします。

```
C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf
```

このコマンドは、シグニチャ パッケージ *IOS-S253-CLI.pkg* から Cisco IOS IPS にシグニチャをロードします。**注： すべてのシグニチャをリタイアする ios-ips signature category all** は、手順 1 で設定しました。シグニチャ パッケージが正しくロードされても、シグニチャは選択されずコンパイルされません。

5. 次のコマンドを使用して、移行した XML ファイルを Cisco IOS IPS にロードします。**<router-hostname>-sigdef-delta.xml**以下に、いくつかの例を示します。

```
copy flash:C2821-sigdef-delta.xml idconf
```

ルータがバージョン 5.x 形式のシグニチャ ファイルを解析すれば、移行は完了です。

6. **show ip ips signature count** コマンドを使用してシグニチャの要約ステータスをチェックし、**show ip ips signature details** コマンドを使用して、すべてのシグニチャの詳細情報を表示します。

関連情報

- Cisco Intrusion Prevention System
- セキュリティ製品に関する Field Notices (CiscoSecure Intrusion Detection を含む)
- テクニカルサポート - Cisco Systems