目次

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。

注シスコでは、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ています。

前提条件

要件

このドキュメントに関する固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。

バージョン 4.x SDF ファイルの移行手順

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. コマンドの **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。 移行プロセスでは 4.x から 5.x への完全な署名形式変換にこのファイルが使用されます。
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）のシグニチャは、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.tbcThis 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]
yPlease 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.sdfPlease
provide SDF to migrate from the above list or of your own     choice: flash:// sdmips.sdfMigrating
following SDF file (this will a take few minutes):  flash://sdmips.sdfTime Elapsed: 0:02:23Migration
completed successfully. The migrated file is  C2821-sigdef-delta.xmlC2821#
```

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。

次に、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 での Cisco IOS IPS への移行された署名のロード

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 ipsCreate directory filename [ips]?Created dir flash:ipsC2821#conf tEnter configuration commands, one per line. End with CNTL/Z.C2821(config)#ip ips name MYIPSC2821(config)#ip ips config location ipsC2821(config)#ip ips signature-categoryC2821(config-ips-category)#category allC2821(config-ips-category-action)#retired trueC2821(config-ips-category-action)#exitC2821(config-ips-category)#exitDo you want to accept these changes? [confirm]yC2821(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。
```
C2821#mkdir ipsCreate directory filename [ips]?Created dir flash:ipsC2821#conf tEnter configuration commands, one per line. End with CNTL/Z.C2821(config)#ip ips name MYIPSC2821(config)#ip ips config location ipsC2821(config)#ip ips signature-categoryC2821(config-ips-category)#category allC2821(config-ips-category-action)#retired trueC2821(config-ips-category-action)#exitC2821(config-ips-category)#exitDo you want to accept these changes? [confirm]yC2821(config)#
```
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 0/0C2821(config-if)#ip ips MYIPS inC2821(config-if)#ip ips MYIPS outC2821(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**次に、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 Notice (CiscoSecure Intrusion Detection を含む)
- テクニカルサポート - Cisco Systems