入侵防御系统版本4.x签名格式到版本5.x签名格式的迁移示例

目录

简介

在Cisco IOS版本12.4(11)T和以上中， Cisco IOS入侵防御系统(IPS) Cisco IPS软件版本5.x签名格式的提供支持。5.x签名格式是其他思科基于设备的IPS产品也使用的一个基于版本的签名定义XML格式。签名和签名定义文件的(SDFs)支持在Cisco IPS版本4.x在这和更加进一步的Cisco IOS T系列软件版本中被中断。

运行Cisco IOS IPS以版本4.x签名格式SDFs的客户能重新配置Cisco IOS IPS使用Cisco预定义的签名类别、基本和先进的签名集或者Cisco IOS IPS迁移工具为了移植以前版本4.x SDF文件到Cisco IPS版本5.x格式化签名集。

本文描述如何从Cisco IPS 4.x格式SDF移植和启用在Cisco IOS版本12.4(11)T或以上设置的被移植的签名。关于如何配置在Cisco IOS版本12.4(11)T或以上、参考的IPS 5.x签名格式支持和可用性增强的Cisco IOS IPS的更多信息。

注意： Cisco建议您运行Cisco IOS IPS迁移，在您升级对Cisco IOS版本12.4(11)T或以上镜像前。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco IOS版本12.4(11)T或以上。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

移植版本4.x SDF文件的步骤

迁移脚本要求Cisco IPS 4.x格式SDF文件和(或者)早于Cisco IOS版本12.4(11)T包含Cisco IOS IPS配置信息使用在路由器thatrunsa版本的CLI配置文件。

迁移脚本搜索包含**ip ips**在路由器配置文件内**> [<sigsubid>]禁用的签名<sigid的**命令。如果配置文件不包含此CLI命令，没有需要对于迁移脚本读CLI配置文件。签名转换根据自卫队独自地，同样地。

如果运行迁移脚本，在您升级Cisco IOS IPS到Cisco IOS版本12.4(11)T或以上前，请按照进程执行Cisco IOS IPS迁移脚本。

如果运行迁移脚本，在您升级Cisco IOS IPS到Cisco IOS版本12.4(11)T或以上后，请完成这些步骤：

1. 验证所有需要转换CLI命令， **ip ips签名禁用的<sigid > [<sigsubid>]**，如上所述。
2. 请使用copy命令**running-config flash: ipscfg.cfg为了**保存路由器的CLI配置到文件。此命令备份闪烁的现有的路由器配置在文件命名了*ipscfg.cfg*。迁移进程使用此文件全双工4.x对5.x签名格式转换。
3. 继续执行Cisco IOS IPS迁移脚本。

执行Cisco IOS IPS迁移脚本

迁移脚本从Cisco.com是可得到在此URL ：http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup。保存迁移脚本对路由器闪存或到一个路由器可访问位置，例如简单文件传输协议(TFTP)服务器。

迁移脚本转换SDF从Cisco IPS版本4.x格式到版本5.x格式。迁移脚本支持仅这些签名参数：

- 严重性
- 操作
- 已启用

另外，迁移脚本能也读从由CLI **ip ips签名<sigid> <sigsubid>禁用的**in命令版本早于Cisco IOS版本12.4(11)T配置的IOS IPS配置fileand迁移禁用的签名。

注意： 自定义(非思科)签名没有转换与此脚本。

此示例显示如何移植IPS 4.x格式文件*sdmips.sdf到*在Cisco IOS版本12.4(11)T的Cisco IOS IPS有Cisco IOS IPS 5.x签名格式支持的。

```
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#
```

首先，迁移脚本显示关于其功能的一个简要文本。其次，脚本在哪里的提供一选择的选项一个位置从读Cisco IOS IPS的当前(预先移植)配置。默认读从启动配置。如果以前保存配置对TFTP server或路由器闪存，请指定位置在提示符。

例如：

请使用**tftp:// 192.168.1.5/<router** *CLI配置***>**为了通知脚本装载从TFTP server 192.168.1.5的一CLI配置。

请使用**flash:// <saved配置>**为了从保存的文件读在闪存。

装载已迁移签名到在Cisco IOS软件版本12.4(11)T的Cisco IOS IPS

在签名迁移完成后，请升级路由器镜像对Cisco IOS Release12.4(11)T，如果不如此已经执行。一旦路由器重新加载，请完成这些步骤。

1. 启用Cisco IOS IPS。此输出显示如何启用在思科2821路由器的Cisco IOS IPS。关于如何配置Cisco IOS IPS、参考的IPS 5.x签名格式支持和可用性增强的更多信息。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. 复制和插入此密钥到路由器为了配置crypto签名公共密钥。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)#
   ```
3. 如此示例所显示，启用在接口的Cisco IOS IPS ：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. 请使用**copy命令**为了装载最新的签名包：`C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf`
   此命令装载从签名包*IOS-S253-CLI.pkg的*签名到Cisco IOS IPS。**注意： IOS IPS签名类别全部**在step1配置，退休所有签名。在签名包顺利地装载后，签名没有选择并且被编译。
5. 请使用此命令为了装载被移植的XML文件到Cisco IOS IPS ：**<router主机名>-sigdef-delta.xml**例如：
   `copy flash:C2821-sigdef-delta.xml idconf`
   一旦路由器解析版本5.x被格式化的签名文件，迁移完成。
6. 请使用**count命令显示ip ips的签名**为了检查签名汇总状态，然后请使用**显示ip ips签名详细信息**命令为了查看在所有签名的特定详细信息。

相关信息

- Cisco Intrusion Prevention System
- 安全产品的问题信息通告（Field Notice）(包括CiscoSecure Intrusion Detection)
- 技术支持 - Cisco Systems