将IPS签名格式4.x迁移到5.x

目录

简介

在Cisco IOS® 12.4(11)T版及更高版本中，Cisco IOS入侵防御系统(IPS)支持Cisco IPS软件版本5.x签名格式。5.x签名格式是基于版本的签名定义XML格式，其他基于思科设备的IPS产品也使用该格式。在本版和更多Cisco IOS T系列软件版本中，不再支持Cisco IPS版本4.x中的签名和签名定义文件(SDF)。

运行Cisco IOS IPS和4.x版签名格式SDF的客户可以重新配置Cisco IOS IPS，使其使用思科预定义的签名类别、基本和高级签名集或Cisco IOS IPS迁移实用程序，以便将之前版本4.x SDF文件迁移到Cisco IPS 5.x版格式签名集。

本文档介绍如何从Cisco IPS 4.x格式SDF迁移并启用Cisco IOS版本12.4(11)T或更高版本中迁移的签名集。有关如何在Cisco IOS版本12.4(11)T或更高版本中配置Cisco IOS IPS的详细信息，请参阅IPS 5.x签名格式支持和可用性增强。

注意：Cisco建议您在升级到Cisco IOS版本12.4(11)T或更高版本映像之前运行Cisco IOS IPS迁移。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco IOS版本12.4(11)T或更高版本。

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。

迁移版本4.x SDF文件的步骤

迁移脚本需要Cisco IPS 4.x格式的SDF文件和（可选）CLI配置文件，该文件包含运行Cisco IOS 12.4(11)T之前版本的路由器上使用的Cisco IOS IPS配置信息。

迁移脚本搜索在路由器配置文**件中包含ip ips signature <*sigid*> [<*sigsubid*>] disabled的**命令。如果配置文件不包含此CLI命令，则无需迁移脚本读取CLI配置文件。这样，签名的转换仅基于SDF。

如果在将Cisco IOS IPS升级到Cisco IOS版本12.4(11)T或更高版本之前运行迁移脚本，请遵循执行Cisco IOS IPS迁移脚本中的过程。

如果在将Cisco IOS IPS升级到Cisco IOS版本12.4(11)T或更高版本后运行迁移脚本，请完成以下步骤：

1. 验证是否需要转换CLI命令，**如上所述，ip ips signature <*sigid*> [<*sigsubid*>]已禁用。**
2. 使用命令**copy running-config flash:ipscfg.cfg**将路由器的CLI配置保存到文件。此命令将现有路由器配置备份到名为ipscfg.cfg的文*件中的闪存*。迁移过程使用此文件进行4.x到5.x签名格式的完全转换。
3. 继续执行Cisco IOS IPS迁移脚本。

执行Cisco IOS IPS迁移脚本

迁移脚本可从Cisco.com的以下URL获取：http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup。将迁移脚本保存到路由器的闪存或路由器可访问的位置，例如简单文件传输协议(TFTP)服务器。

迁移脚本将SDF从Cisco IPS版本4.x格式转换为版本5.x格式。迁移脚本仅支持以下签名参数：

- 严重级
- 动作
- 启用

此外，迁移脚本还可以从IOS IPS配置文件读取，并迁移在Cisco IOS版本12.4(11)T之前的版本中通过CLI **ip ips signature <sigid> <sigsubid> disabled命令配置的禁用签名。**

注意：自定义（非思科）签名不使用此脚本转换。

本示例展示如何在Cisco IOS 12.4(11)T版本中，通过Cisco IOS IPS 5.x签名格式支持将IPS 4.x格式化文件*sdmips.sdf*迁移到Cisco IOS IPS。

```
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，迁移脚本显示有关其功能的简短文本。接下来，脚本提供了一个选项，用于选择从何处读取Cisco IOS IPS的当前（迁移前）配置。默认从启动配置读取。如果之前已将配置保存到TFTP服务器或路由器的闪存中，请在提示符处指定位置。

例如：

使用**tftp:// 192.168.1.5/*<路由器CLI配置>***通知脚本从TFTP服务器192.168.1.5加载CLI配置。

使用**flash://*<saved-configuration>***从闪存中保存的文件中读取。

在思科IOS软件版本12.4(11)T中将迁移的签名加载到思科IOS IPS

签名迁移完成后，如果尚未将路由器映像升级到Cisco IOS版本12.4(11)T。重新加载路由器后，请完成以下步骤。

1. 启用Cisco IOS IPS。此输出显示如何在Cisco 2821路由器上启用Cisco IOS IPS。有关如何配置Cisco IOS IPS的详细信息，请参阅IPS 5.x签名格式支持和可用性增强。

```
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. 将此密钥复制并粘贴到路由器中以配置加密签名公钥。

```
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. 在接口上启用Cisco IOS IPS，如以下示例所示：

```
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. 使用**copy**命令加载最新的签名包：
   ```
   C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf
   ```

   此命令将签名从签名包*IOS-S253-CLI.pkg加载*到Cisco IOS IPS中。**注意： 在步骤1中配置了**ios-ips签名类别，该类别将停用所有签名。成功加载签名包后，不会选择并编译签名。
5. 使用以下命令将迁移的XML文件加载到Cisco IOS IPS:**<*router-hostname* >-sigdef-delta.xml**例如：

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

   路由器解析5.x版格式签名文件后，迁移即完成。
6. 使用**show ip ips signature count**命令检查签名摘要状态，然后使用**show ip ips signature details**命令查看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