將IPS特徵碼格式4.x遷移到5.x

目錄

簡介

在Cisco IOS®版本12.4(11)T和更新版本中，Cisco IOS入侵防禦系統(IPS)為Cisco IPS軟體版本5.x簽名格式提供支援。5.x特徵碼格式是基於版本的特徵碼定義XML格式，其他基於Cisco裝置的IPS產品也會使用這種格式。Cisco IPS 4.x版不再支援簽名和簽名定義檔案(SDF)，此版本及其他Cisco IOS T-Train軟體版本也停止了支援。

運行4.x版特徵碼格式SDF的Cisco IOS IPS的客戶可以重新配置Cisco IOS IPS，以使用思科預定義的特徵碼類別、基本和高級特徵碼集或Cisco IOS IPS遷移實用程式，以便將先前版本4.x SDF檔案遷移到Cisco IPS 5.x版格式特徵碼集。

本文說明如何從Cisco IPS 4.x格式SDF遷移，以及如何啟用Cisco IOS版本12.4(11)T或更高版本中的遷移簽名集。有關如何在Cisco IOS版本12.4(11)T或更高版本中配置Cisco IOS IPS的詳細資訊，請參閱IPS 5.x簽名格式支援和可用性增強。

注意：Cisco建議在升級到Cisco IOS版本12.4(11)T或更高版本映像之前運行Cisco IOS IPS遷移。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco IOS版本12.4(11)T或更新版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

遷移4.x SDF版本檔案的步驟

遷移指令碼需要Cisco IPS 4.x格式的SDF檔案和（可選）CLI配置檔案，後者包含運行早於Cisco IOS版本12.4(11)T的路由器上使用的Cisco IOS IPS配置資訊。

遷移指令碼搜尋路由器配置檔案中包含**ip ips signature <*sigid*> [<*sigsubid*>] disabled**的命令。如果配置檔案不包含此CLI命令，則無需遷移指令碼來讀取CLI配置檔案。對簽名的轉換僅基於SDF。

如果在將Cisco IOS IPS升級到Cisco IOS版本12.4(11)T或更高版本之前運行遷移指令碼，請按照執行Cisco IOS IPS遷移指令碼中的過程操作。

如果您在將Cisco IOS IPS升級到Cisco IOS版本12.4(11)T或更高版本後運行遷移指令碼，請完成以下步驟：

1. 如上所述，驗證是否需要轉換CLI命令，**ip ips signature <*sigid*> [<*sigsubid*>] disabled**。
2. 使用命令**copy running-config flash:ipscfg.cfg**將路由器的CLI配置儲存到檔案。此命令將現有路由器配置備份到名為*ipscfg.cfg*的檔案中的快閃記憶體中。遷移過程使用此檔案進行4.x到5.x的完整簽名格式轉換。
3. 繼續執行Cisco IOS IPS遷移指令碼。

執行Cisco IOS IPS遷移指令碼

遷移指令碼可從以下URL的Cisco.com獲得：http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup。將遷移指令碼儲存到路由器的快閃記憶體或路由器可訪問的位置，如簡單式檔案傳輸協定(TFTP)伺服器。

遷移指令碼將SDF從Cisco IPS 4.x版格式轉換為5.x版格式。遷移指令碼僅支援以下簽名引數：

- 嚴重性
- 動作
- 已啟用

此外，遷移指令碼還可以從IOS IPS配置檔案進行讀取，並遷移由CLI **ip ips signature <sigid> <sigsubid> disabled**命令在低於Cisco IOS版本12.4(11)T的版本中配置的禁用簽名。

注意：自定義（非思科）簽名不會與此指令碼轉換。

此示例說明如何使用Cisco IOS IPS 5.x簽名格式支援將IPS 4.x格式檔案*sdmips.sdf*遷移到Cisco IOS版本12.4(11)T中的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，遷移指令碼顯示有關其功能的簡短文本。接下來，該指令碼提供了用於選擇從何處讀取Cisco IOS IPS的當前（遷移前）配置的選項。預設值會從啟動組態讀取。如果之前已將配置儲存到TFTP伺服器或路由器的快閃記憶體中，請在提示符處指定位置。

例如：

使用**tftp:// 192.168.1.5/<*router CLI configuration*>**通知指令碼從TFTP伺服器192.168.1.5載入CLI配置。

使用**flash://<*saved-configuration*>**從快閃記憶體中儲存的檔案進行讀取。

在Cisco IOS軟體版本12.4(11)T中將遷移的簽名載入到Cisco IOS IPS中

完成特徵碼遷移後，如果尚未將路由器的映像升級到Cisco IOS版本12.4(11)T。重新載入路由器後，請完成以下步驟。

1. 啟用Cisco IOS IPS。此輸出顯示了如何在Cisco 2821路由器上啟用Cisco IOS IPS。有關如何配置Cisco IOS IPS的詳細資訊，請參閱IPS 5.x簽名格式支援和可用性增強。

```
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. 將此金鑰複製貼上到路由器中，以設定密碼編譯簽名的公鑰。

```
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. 如以下示例所示，在介面上啟用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. 使用**copy**命令以載入最新的簽名包：

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

此命令將簽名包*IOS-S253-CLI.pkg*中的簽名載入到Cisco IOS IPS。**附註： ios-ips簽名類別all在步驟**1中配置，該步驟將保留所有簽名。成功載入簽名包後，不會選擇和編譯任何簽名。

5. 使用以下命令將遷移的XML檔案載入到Cisco IOS IPS:**<*router-hostname*>-sigdef-delta.xml**例如：

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

一旦路由器解析版本5.x格式化的簽名檔案，遷移完成。

6. 使用**show ip ips signature count**命令檢查特徵碼摘要狀態，然後使用**show ip ips signature details**命令檢視有關所有特徵碼的特定詳細資訊。

相關資訊

- 思科入侵防禦系統
- 安全產品現場通知（包括CiscoSecure Intrusion Detection）
- 技術支援 - Cisco Systems