使用5.x格式簽名配置IPS

目錄

簡介

本文檔介紹如何在Cisco IOS® IPS中配置5.x格式簽名，分為兩部分：

- I部分。入門配置步驟 — 本節提供使用Cisco IOS命令列介面(CLI)開始使用IOS IPS 5.x格式簽名所需的步驟。本節介紹以下步驟：步驟1.下載IOS IPS檔案。步驟2.在快閃記憶體上建立IOS IPS配置目錄。步驟3.配置IOS IPS加密金鑰。步驟4.啟用IOS IPS。步驟5.將IOS IPS簽名軟體包載入到路由器。詳細描述了每個步驟和特定命令，以及其他命令和參考。每個命令下方都顯示了示例配置。
- 第二節 。高級配置選項 — 本節提供有關用於特徵碼調整的高級選項的說明和示例。它包含以下選項：停用或取消停用簽名啟用或禁用簽名更改簽名操作

必要條件

需求

完成本文檔中的步驟之前，請確保您具有正確的元件(如使用的元件中所述)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科整合多業務路由器（87x、18xx、28xx或38xx）
- 128MB或更大DRAM和至少2MB可用快閃記憶體
- 通過控制檯或telnet連線到路由器
- Cisco IOS版本12.4(15)T3或更高版本
- 有效的CCO(Cisco.com)登入使用者名稱和密碼
- 當前思科IPS服務合約，用於授權簽名更新服務

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。

第I部分。配置入門步驟

步驟1.下載IOS IPS檔案

第一步是從Cisco.com下載IOS IPS簽名包檔案和公共加密金鑰。

將所需的簽名檔案從Cisco.com下載到您的PC:

- 位置：http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup(僅限註冊客戶)
- 要下載的檔案：IOS-Sxxx-CLI.pkg(僅供註冊客戶) — 這是最新的特徵包。realm-cisco.pub.key.txt(僅限註冊客戶) — 這是IOS IPS使用的公共加密金鑰。

步驟2.在快閃記憶體上建立IOS IPS配置目錄

第二步是在路由器的快閃記憶體上建立儲存所需簽名檔案和配置的目錄。或者，您可以使用連線到路由器USB埠的Cisco USB快閃記憶體驅動器來儲存特徵碼檔案和配置。如果將USB快閃記憶體驅動器用作IOS IPS配置目錄位置，則該驅動器必須保持與路由器的USB埠連線。IOS IPS還支援任何IOS檔案系統作為其配置位置，並具有適當的寫入訪問許可權。

要建立目錄，請在路由器提示符下輸入以下命令：**mkdir <*directory name*>**

例如：

```
router#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
```

其他命令和參考

若要確認快閃記憶體的內容，請在路由器提示時輸入以下命令：**show flash:**

例如：

```
router#dir flash:
Directory of flash:/
   5 -rw-   51054864 Feb 8 2008 15:46:14 -08:00
```

```
                    c2800nm-advipservicesk9-mz.124-15.T3.bin
   6 drw-      0 Feb 14 2008 11:36:36 -08:00 ips
64016384 bytes total (12693504 bytes free)
```

若要重新命名目錄名稱，請使用以下命令：**rename <*current name*> <*new name*>**

例如：

```
router#rename ips ips_new
Destination filename [ips_new]?
```

步驟3.配置IOS IPS加密金鑰

第三步是配置IOS IPS使用的加密金鑰。此金鑰位於步驟1中下載的領域 — cisco.pub.key.txt檔案中。

加密金鑰用於驗證主簽名檔案(sigdef-default.xml)的數位簽章，其內容由思科私有金鑰簽名，以確保其在每個版本中的真實性和完整性。

1. 開啟文本檔案，然後複製檔案的內容。
2. 使用**configure terminal**命令以進入路由器配置模式。
3. 在<hostname>(config)#內容。
4. 退出路由器配置模式。
5. 在路由器提示時輸入**show run**命令，以確認已配置加密金鑰。您應該會在設定中看到以下輸出：

```
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
```

6. 使用以下命令以儲存組態：**copy running-configure startup-configure**

其他命令和參考

如果金鑰配置不正確，必須先刪除加密金鑰，然後重新配置它：

1. 若要移除金鑰，請按下列順序輸入以下命令：

```
router#configure terminal
router(config)#no crypto key pubkey-chain rsa
router(config-pubkey-chain)#no named-key realm-cisco.pub signature
router(config-pubkey-chain)#exit
router(config)#exit
```

2. 使用**show run**命令以驗證是否已從配置中刪除該金鑰。
3. 完成步驟3中的程式以重新設定金鑰。

步驟4.啟用IOS IPS

第四步是配置IOS IPS。完成以下步驟即可設定IOS IPS:

1. 使用**ip ips name <*rule name*> < *optional ACL*>**命令以建立規則名稱。（這將在介面上用於啟用IPS。）例如：
```
router#configure terminal
router(config)#ip ips name iosips
```

   您可以指定可選的擴展或標準訪問控制清單(ACL)，以過濾將由此規則名稱掃描的流量。ACL允許的所有流量都須由IPS檢查。IPS不會檢查ACL拒絕的流量。
```
router(config)#ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
```
2. 使用**ip ips config location flash:<*directory name*>**命令配置IPS簽名儲存位置。(這是步驟2中建立的*ips*目錄。)例如：
```
router(config)#ip ips config location flash:ips
```

3. 使用**ip ips notify sdee**命令啟用IPS SDEE事件通知。例如：
```
router(config)#ip ips notify sdee
```

   要使用SDEE，必須啟用HTTP伺服器(使用**ip http server**命令)。 如果未啟用HTTP伺服器，則路由器無法響應SDEE客戶端，因為它看不到請求。SDEE通知預設處於禁用狀態，必須顯式啟用。IOS IPS還支援使用syslog傳送事件通知。可以單獨使用SDEE和系統日誌，也可以同時啟用SDEE和系統日誌以傳送IOS IPS事件通知。預設情況下啟用系統日誌通知。如果啟用了日誌控制檯，您將看到IPS系統日誌消息。若要啟用系統日誌，請使用以下命令：
```
router(config)#ip ips notify log
```

4. 配置IOS IPS以使用預定義簽名類別之一。採用Cisco 5.x格式簽名的IOS IPS使用簽名類別（與Cisco IPS裝置一樣）。 所有特徵碼都按類別分組，類別分層。這有助於對特徵碼進行分類，以便於進行分組和調整。**警告：**all*簽名*類別包含簽名發行版中的所有簽名。由於IOS IPS無法一次編譯和使用特徵碼版本中包含的所有特徵碼，*請不要取消所有類別*;否則，路由器將耗盡記憶體。**注意：**配置IOS IPS時，必須首先註銷all類別中的所有*簽名*，然後取消註銷選定的簽名類別。**注意：**在路由器上配置簽名類別的順序也很重要。IOS IPS按照配置中列出的順序處理category命令。某些簽名屬於多個類別。如果配置了多個類別，並且簽名屬於多個類別，則IOS IPS會使用最後一個配置類別中的簽名屬性（例如，已停用、未停用、操作等）。在本示例中，「all」類別中的所有簽名都已失效，然後*IOS IPS Basic類別*未停用。
```
router(config)#ip ips signature-category
router(config-ips-category)#category all
router(config-ips-category-action)#retired true
router(config-ips-category-action)#exit
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```
5. 使用以下命令以在所需介面上啟用IPS規則，並指定應用規則的方向：**interface <*interface name*>ip ips <*rule name*> [*in |出*]**例如：
```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#exit
router(config)#exit
router#
```
   *in*參數列示IPS僅檢查進入介面的流量。*out*參數列示IPS僅檢查流出介面的流量。要啟用IPS檢查介面的傳入和傳出流量，請分別輸入同一介面上*傳入*和*傳出*的IPS規則名稱：

```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#ip ips iosips out
router(config-if)#exit
router(config)#exit
router#
```

步驟5.將IOS IPS簽名軟體包載入到路由器

最後一步是將步驟1中下載的簽名軟體包載入到路由器。

注意：將特徵碼包載入到路由器的最常見方法是使用FTP或TFTP。此程式使用FTP。請參閱本過程的*其他命令和參考*部分，瞭解載入IOS IPS特徵碼包的替代方法。如果使用telnet會話，請使用terminal monitor命令檢視控制檯輸出。

若要將特徵碼包載入到路由器，請完成以下步驟：

1. 使用以下命令將下載的簽署套件從FTP伺服器複製到路由器：copy ftp://*<ftp_user:password@Server_IP_address>*/*<signature_package>* idconf**註**：請記得在copy命令末尾使用*idconf*參**數**。**註**：例如：
```
router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```
在將特徵碼包載入到路由器之後，特徵碼編譯立即開始。您可以檢視已啟用日誌記錄級別6或以上級別的路由器上的日誌。
```
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Feb 14 2008
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures -
                      1 of 13 engines
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms -
                      packets for this engine will be scanned
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures -
                      2 of 13 engines
*Feb 14 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms -
                      packets for this engine will be scanned
|
output snipped
|
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures -
                      12 of 13 engines
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms -
                      packets for this engine will be scanned
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures -
                      13 of 13 engines
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms -
                      packets for this engine will be scanned
*Feb 14 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```
2. 使用show ip ips signature count命令驗證特徵碼包是否已正確編譯。例如：
```
router#show ip ips signature count
Cisco SDF release version S310.0  signature package release version
Trend SDF release version V0.0
Signature Micro-Engine: multi-string: Total Signatures 8
multi-string enabled signatures: 8
multi-string retired signatures: 8
|
outpt snipped
|
Signature Micro-Engine: service-msrpc: Total Signatures 25
service-msrpc enabled signatures: 25
service-msrpc retired signatures: 18
```

```
     service-msrpc compiled signatures: 1
     service-msrpc inactive signatures - invalid params: 6
     Total Signatures: 2136
     Total Enabled Signatures: 807
     Total Retired Signatures: 1779
     Total Compiled Signatures:
           351  total compiled signatures for the IOS IPS Basic category
     Total Signatures with invalid parameters: 6
     Total Obsoleted Signatures: 11
     router#
```

其他命令和參考

如果在簽名編譯時收到與以下錯誤消息類似的錯誤消息，則公共加密金鑰無效：

```
%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)
```

如需詳細資訊，請參閱步驟3。

如果您無法存取FTP或TFTP伺服器，可以使用USB快閃磁碟機將特徵碼封包載入路由器。首先，將特徵碼包複製到USB驅動器，將USB驅動器連線到路由器上的某個USB埠，然後使用帶有*idconf* 引數的**copy**命令將特徵碼包複製到路由器。

例如：

```
router#copy usbflash1:IOS-S310-CLI.pkg idconf
```

配置的IOS IPS儲存目錄中有六個檔案。這些檔案使用以下名稱格式：<*router-name*>-sigdef-xxx.xml或<*router-name*>-seap-xxx.xml。

```
router#dir ips
Directory of flash:/ips/
7 -rw- 203419 Feb 14 2008 16:45:24 -08:00 router-sigdef-default.xml
8 -rw- 271 Feb 14 2008 16:43:36 -08:00 router-sigdef-delta.xml
9 -rw- 6159 Feb 14 2008 16:44:24 -08:00 router-sigdef-typedef.xml
10 -rw- 22873 Feb 14 2008 16:44:26 -08:00 router-sigdef-category.xml
11 -rw- 257 Feb 14 2008 16:43:36 -08:00 router-seap-delta.xml
12 -rw- 491 Feb 14 2008 16:43:36 -08:00 router-seap-typedef.xml
64016384 bytes total (12693504 bytes free)
router#
```

這些檔案以壓縮格式儲存，不能直接編輯或檢視。每個檔案的內容說明如下：

- *router-sigdef-default.xml包含所有*出廠預設簽名定義。
- *router-sigdef-delta.xml包含*已從預設值更改的簽名定義。
- *router-sigdef-typedef.xml包含*所有簽名引數定義。
- *router-sigdef-category.xml包含*特徵碼類別資訊，例如category ios_ips basic和advanced。
- *router-seap-delta.xml包含對*預設SEAP引數所做的更改。
- *router-seap-typedef.xml包含*所有SEAP引數定義。

第二節 。高級配置選項

本節提供有關用於特徵碼調整的高級IOS IPS選項的說明。

停用或取消停用簽名

註銷或取消註銷簽名是指選擇或取消選擇IOS IPS用於掃描流量的簽名。

- **取消**簽名意味著IOS IPS不會*將該*簽名編譯到記憶體中以供掃描。
- **取消**停用特徵碼會指示IOS IPS將特徵碼編譯到記憶體中並使用特徵碼掃描流量。

您可以使用IOS命令列介面(CLI)停用或取消停用屬於簽名類別的單個簽名或一組簽名。停用或取消停用一組簽名時，該類別中的所有簽名都會被停用或取消停用。

註：某些未停用簽名（作為單個簽名或未停用類別中的未停用簽名）可能由於記憶體不足或引數無效或簽名已過時而無法編譯。

此示例說明如何停用單個簽名。例如，子ID為10的簽名6130:

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status
router(config-sigdef-sig-status)#retired true
router(config-sigdef-sig-status)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

以下示例展示如何取消屬於IOS IPS基本類別的所有特徵碼：

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
```

注意：當類別中除IOS IPS Basic和IOS IPS Advanced之外的簽名作為類別取消停用時，某些簽名或引擎的編譯可能會失敗，因為IOS IPS不支援這些類別中的某些簽名（請參閱下面的示例）。IOS IPS使用其他所有成功編譯（未停用）的簽名來掃描流量。

```
Router(config)#ip ips signature-category
router(config-ips-category)#category os
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
*Feb 14 18:10:46 PST: Applying Category configuration to signatures ...
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDS_STARTED: 08:10:49 PST Feb 18 2008
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures -
                      1 of 13 engines
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_READY: multi-string - build time 136 ms -
                      packets for this engine will be scanned
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures -
                      2 of 13 engines
*Feb 14 18:10:50 PST: %IPS-4-META_ENGINE_UNSUPPORTED: service-http 5903:1 -
```

```
                    this signature is a component of the unsupported META engine
*Feb 14 18:24:42 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5754:0 -
                    compilation of regular expression failed
*Feb 14 18:24:49 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5729:1 -
                    compilation of regular expression failed
```

啟用或禁用簽名

啟用或禁用特徵碼是在資料包或資料包流與特徵碼匹配時，實施或忽略IOS IPS與特徵碼關聯的操作。

注意：啟用和禁用不會選擇和取消選擇IOS IPS要使用的簽名。

- Enable簽名表示當匹配的資料包（或資料包流）觸發時，簽名將執行與其關聯的相應操作。但是，只有未停用且已成功編譯的簽名在啟用時才會執行操作。換句話說，如果簽名被停用，即使它被啟用，它也不會被編譯（因為它已停用），並且它不會執行與其關聯的操作。
- Disable簽名意味著當匹配的資料包（或資料包流）觸發時，簽名不會執行與其關聯的相應操作。換句話說，當簽名被禁用時，即使簽名未停用且編譯成功，它也不會執行與其關聯的操作。

您可以使用IOS命令列介面(CLI)啟用或禁用單個簽名或基於簽名類別的一組簽名。此示例說明如何禁用子級ID為10的簽名6130。

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status
router(config-sigdef-sig-status)#enabled false
router(config-sigdef-sig-status)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

此示例說明如何啟用屬於IOS IPS Basic類別的所有簽名。

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#enabled true
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

更改簽名操作

您可以使用IOS命令列介面(CLI)更改基於簽名類別的一個簽名或一組簽名的簽名操作。此示例說明如何為子級ID為10的簽名6130將簽名操作更改為警報、丟棄和重置。

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#engine
router(config-sigdef-sig-engine)#event-action produce-alert
```

```
router(config-sigdef-sig-engine)#event-action deny-packet-inline
router(config-sigdef-sig-engine)#event-action reset-tcp-connection
router(config-sigdef-sig-engine)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

此示例說明如何更改屬於簽名IOS IPS基本類別的所有簽名的事件操作。

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#event-action produce-alert
router(config-ips-category-action)#event-action deny-packet-inline
router(config-ips-category-action)#event-action reset-tcp-connection
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

相關資訊

- Cisco IOS入侵防禦系統(IPS)產品與服務頁面
- Cisco IOS IPS — 版本5簽章軟體下載
- IPS 5.x特徵碼格式支援和可用性增強功能
- 思科安全裝置管理員軟體下載
- 如何使用CCP配置IOS IPS
- Cisco Intrusion Detection System Event Viewer 3DES加密軟體下載
- 技術支援與文件 - Cisco Systems