使用5.x格式签名配置IPS

目录

简介

本文档介绍如何在Cisco IOS® IPS中配置5.x格式签名，并分为两个部分：

- I. Getting Started Configuration Steps — 此部分提供使用Cisco IOS命令行界面(CLI)以开始使用IOS IPS 5.x格式签名所需的步骤。本节介绍以下步骤：步骤1.下载IOS IPS文件。步骤2.在闪存上创建IOS IPS配置目录。步骤3.配置IOS IPS加密密钥。步骤4.启用IOS IPS。步骤5.将IOS IPS签名包加载到路由器。详细描述了每个步骤和特定命令，以及其他命令和参考。每个命令下方显示一个配置示例。
- 第二节。高级配置选项 — 本部分提供有关签名优化高级选项的说明和示例。它包含以下选项：停用或停用签名启用或禁用签名更改签名操作

先决条件

要求

在完成本文档中的步骤之前，请确保您具有正确的组件（如“已使用的组件”中所述）。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科集成多业务路由器（87x、18xx、28xx或38xx）
- 128MB或更高DRAM和至少2MB空闲闪存
- 与路由器的控制台或telnet连接
- 思科IOS版本12.4(15)T3或更高版本
- 有效的CCO(Cisco.com)登录用户名和密码
- 许可的签名更新服务的当前思科IPS服务合同

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。

第I部分：入门配置步骤

步骤1.下载IOS IPS文件

第一步是从Cisco.com下载IOS IPS签名软件包文件和公共加密密钥。

将所需的签名文件从Cisco.com下载到您的PC:

- 地点：http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup(仅限注册客户)
- 要下载的文件：IOS-Sxxx-CLI.pkg(仅注册客户) — 这是最新的签名包。realm-cisco.pub.key.txt(仅注册客户) — 这是IOS IPS使用的公共加密密钥。

步骤2.在闪存上创建IOS IPS配置目录

第二步是在路由器闪存上创建一个目录，在其中存储所需的签名文件和配置。或者，您可以使用连接到路由器USB端口的思科USB闪存驱动器存储签名文件和配置。如果USB闪存驱动器用作IOS IPS配置目录位置，则它必须保持与路由器USB端口的连接。IOS IPS还支持任何IOS文件系统作为其配置位置，并具有适当的写访问权限。

要创建目录，请在路由器提示符下输入以下命令：**mkdir *<目录名>***

例如：

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

其他命令和参考

要验证闪存的内容，请在路由器提示符下输入以下命令：**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)
```

要重命名目录名称，请使用以下命令：**重命名*<当前*名称> *<新名*称>**

例如：

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

步骤3.配置IOS IPS加密密钥

第三步是配置IOS IPS使用的加密密钥。此密钥位于步骤1中下载的realm-cisco.pub.key.txt文件中。

加密密钥用于验证主签名文件(sigdef-default.xml)的数字签名，其内容由思科私钥签名，以保证其在每个版本中的真实性和完整性。

1. 打开文本文件，并复制文件的内容。
2. 使用**configure terminal**命令进入路由器配置模式。
3. 在<hostname>(config)#提示符内容。
4. 退出路由器配置模式。
5. 在路由器提示符下输入**show run**命令，以确认已配置加密密钥。您应在配置中看到以下输出：

```
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. 使用以下命令保存配置：**copy running-configure startup-configure**

其他命令和参考

如果密钥配置不正确，您必须先删除加密密钥，然后重新配置：

1. 要删除密钥，请按下列顺序输入以下命令：

```
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**命令验证密钥是否已从配置中删除。
3. 完成步骤3中的步骤以重新配置密钥。

步骤4.启用IOS IPS

第四步是配置IOS IPS。要配置IOS IPS，请完成以下步骤：

1. 使用**ip ips name <*rule name*> < *optional ACL*>命令以创建规则名称。**（这将用于接口以启用IPS。）例如：

```
router#configure terminal
router(config)#ip ips name iosips
```

您可以指定可选的扩展或标准访问控制列表(ACL)，以便过滤将由此规则名称扫描的流量。ACL允许的所有流量都受IPS的检查。ACL拒绝的流量不由IPS检查。

```
router(config)#ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
```

2. 请使**用ip ips config location flash:<*directory name*>**命令配置IPS签名存储位置。(这是在步*骤*2中创建的ips目录。)例如：

```
router(config)#ip ips config location flash:ips
```

3. 使用**ip ips notify sdee**命令以启用IPS SDEE事件通知。例如：

```
router(config)#ip ips notify sdee
```

要使用SDEE，必须启用HTTP服务器(使用**ip http server命**令)。 如果HTTP服务器未启用，则路由器无法响应SDEE客户端，因为它看不到请求。SDEE通知默认为禁用状态，必须明确启用。IOS IPS还支持使用系统日志来发送事件通知。SDEE和系统日志可以独立使用或同时启用，以发送IOS IPS事件通知。系统日志通知默认启用。如果启用日志记录控制台，您将看到IPS系统日志消息。要启用系统日志，请使用以下命令：

```
router(config)#ip ips notify log
```

4. 将IOS IPS配置为使用预定义的签名类别之一。具有Cisco 5.x格式签名的IOS IPS与签名类别（与Cisco IPS设备一样）一起运行。 所有签名都分为多个类别，并且类别是分层的。这有助于对签名进行分类，以便于分组和调整。**警告**：所有签名类别包含签名版本中的所有签名。由于IOS IPS无法同时编译和使用签名版本中包含的所有签名，*因此不要取消所有类别*;否则，路由器将耗尽内存。**注：配**置IOS IPS时，必须先停用所有类别中的所*有*签名，然后取消停用所选签名类别。**注意**：在路由器上配置签名类别的顺序也很重要。IOS IPS按配置中列出的顺序处理类别命令。某些签名属于多个类别。如果配置了多个类别，并且签名属于多个类别，则IOS IPS将使用最后配置类别中签名的属性（例如，停用、未停用、操作等）。在本例中，“all”类别中的所有签名都将停用，然后IOS IPS基*本类别将*不停用。

```
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接口上启用IPS规则，并指定规则的应用方向：**interface <*interface name*>ip ips <*规则名称*> [*in |输出*]**例如：

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

in参数表示IPS只检查进入接口的流量。out参数表示IPS只检查从接口传出的流量。要使IPS能够检查接口的传入和传出流量，请在同一接口上分别输入*传入*和*传出*的IPS规则名称：

```
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#
```

步骤5.将IOS IPS签名包加载到路由器

最后一步是将步骤1中下载的签名包加载到路由器。

注意：将签名软件包加载到路由器的最常见方法是使用FTP或TFTP。此过程使用FTP。有关加载IOS IPS签名*包的替代方法*，请参阅本过程中的"其他命令和参考"部分。如果使用telnet会话，请使用terminal monitor命令查看控制台输出。

要将签名包加载到路由器，请完成以下步骤：

1. 使用以下命令将下载的签名包从FTP服务器复制到路由器：**copy ftp://<*ftp_user:password@Server_IP_address*>/<signature_*package*> idconf注意**：请记住在copy命令*结*尾使用idconf参数。**注意**：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]
```

签名编译在签名包加载到路由器后立即开始。您可以看到路由器上启用了6级或更高级日志的日志。

```
*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**命令验证签名包是否已正确编译。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#
```

其他命令和参考

如果您在签名编译时收到类似于以下错误消息的错误消息，则公共加密密钥无效：

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

有关详细信息，请参阅步骤3。

如果您无法访问FTP或TFTP服务器，可以使用USB闪存驱动器将签名包加载到路由器。首先，将签名包复制到USB驱动器，将USB驱动器连接到路由器上的一个USB端口，然后使用带*idconf*参数的**copy**命令将签名包复制到路由器。

例如：

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

已配置的IOS IPS存储目录中有六个文件。这些文件使用以下名称格式：<*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#
```

这些文件以压缩格式存储，不能直接编辑或查看。每个文件的内容描述如下：

- *router-sigdef-default.xml包含所*有出厂默认签名定义。
- *router-sigdef-delta.xml包含*已从默认值更改的签名定义。
- *router-sigdef-typedef.xml包含所*有签名参数定义。
- *router-sigdef-category.xml包*含签名类别信息，如category ios_ips basic和advanced。
- *router-seap-delta.xml包*含对默认SEAP参数的更改。
- *router-seap-typedef.xml包含*所有SEAP参数定义。

第二节。高级配置选项

本节提供有关用于签名调整的高级IOS IPS选项的说明和示例。

停用或停用签名

要停用或取消停用签名，意味着选择或取消选择IOS IPS用于扫描流量的签名。

- **停用**签名意味着IOS IPS不会将该签名编译到内存中进行扫描。
- **取消停**用签名会指示IOS IPS将签名编译到内存中并使用签名扫描流量。

您可以使用IOS命令行界面(CLI)停用或停用属于签名类别的单个签名或一组签名。当您停用或取消停用一组签名时，该类别中的所有签名都将停用或未停用。

注意：由于内存不足或参数无效或签名已过时，某些未停用的签名（未停用为单个签名或未停用类别）可能无法编译。

此示例显示如何停用单个签名。例如，子网ID为10的签名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)#
```

此示例显示如何取消停用属于IOS IPS基本类别的所有签名：

```
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)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
```

注意：当IOS IPS基本和IOS IPS高级以外的类别中的签名未作为类别停用时，某些签名或引擎的编译可能会失败，因为这些类别中的某些签名不受IOS IPS支持（请参阅以下示例）。 IOS IPS使用所有其他成功编译（未停用）的签名扫描流量。

```
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
```

启用或禁用签名

启用或禁用签名是当数据包或数据包流与签名匹配时，强制或忽略与IOS IPS签名相关的操作。

注意：启用和禁用不会选择和取消选择IOS IPS使用的签名。

- 启用**签**名意味着当由匹配的数据包（或数据包流）触发时，签名会采取与其关联的适当操作。但是，只有未停用且成功编译的签名在启用时才会采取操作。换句话说，如果签名已停用，即使它已启用，也不会编译（因为它已停用），也不会执行与其关联的操作。
- 禁用**签**名意味着当由匹配的数据包（或数据包流）触发时，签名不会采取与其关联的适当操作。换句话说，当签名被禁用时，即使签名未停用并已成功编译，它也不会执行与其关联的操作。

您可以使用IOS命令行界面(CLI)来根据签名类别启用或禁用单个签名或一组签名。此示例显示如何禁用子网ID为10的签名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)#
```

此示例显示如何启用属于IOS IPS Basic类别的所有签名。

```
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)#
```

更改签名操作

您可以使用IOS命令行界面(CLI)，以便根据签名类别更改一个签名或一组签名的签名操作。此示例显示如何将签名操作更改为警报、丢弃和重置子网ID为10的签名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)#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)#
```

此示例显示如何更改属于签名IOS IPS基本类别的所有签名的事件操作。

```
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)#
```

相关信息

- Cisco IOS入侵防御系统(IPS)产品和服务页
- Cisco IOS IPS — 版本5签名软件下载
- IPS 5.x签名格式支持和可用性增强
- 思科安全设备管理器软件下载
- 如何使用CCP配置IOS IPS
- 思科入侵检测系统事件查看器3DES加密软件下载
- 技术支持和文档 - Cisco Systems