带有5.x格式签名的入侵防御系统配置示例

目录

简介

本文描述如何配置5.x在Cisco IOS IPS的格式签名和被组织为两个部分：

- 部分i.开始的配置步骤—此部分提供必要步骤使用Cisco IOS命令行界面(CLI)为了开始与IOS IPS 5.x格式签名。此部分描述这些步骤：步骤1.下载IOS IPS文件。步骤2.创建在闪存的一个IOS IPS配置目录。步骤3.配置IOS IPS加密密钥。步骤4. Enable (event) IOS IPS。步骤5.装载IOS IPS签名包到路由器。每个步骤和特定命令详细描述，以及其它命令和参考。配置示例在每命令之下显示。
- 部分II.高级配置选项—此部分在高级选项提供说明和示例为签名调整。它包含这些选项：退休或撤销收回签名启用或禁用签名更改签名操作

先决条件

要求

保证您有适当的组件(正如使用的组件所描述)，在您完成在本文前的步骤。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科集成业务路由器(87x、18xx、28xx或者38xx)
- 128MB或至少更多的DRAM和2MB空闲闪存
- 控制台或Telnet连接对路由器
- Cisco IOS版本12.4(15)T3或以上
- 一个有效CCO (Cisco.com)登录用户用户名和密码
- 准许的签名更新服务的一个当前思科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。

部分i.开始的配置步骤

步骤1.下载IOS IPS文件

第一步将下载IOS IPS签名包文件和公共加密密钥从Cisco.com。

下载从Cisco.com的需要的签名文件到您的PC:

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

步骤2.创建在闪存的IOS IPS配置目录

第二步将创建在您存储需要的签名文件和配置的您的路由器闪存的一个目录。或者，您能使用思科USB闪存驱动器连接对路由器的USB端口存储签名文件和配置。如果使用作为IOS IPS配置目录位置， USB闪存驱动器一定依然是已连接对路由器的USB端口。IOS IPS也支持所有IOS文件系统作为其有适当的写访问的配置位置。

为了创建目录，请输入此at命令路由器提示：**mkdir <directory** *name***>**

例如：

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

其它命令和参考

为了验证闪存的内容，请输入此at命令路由器提示：**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)
```

为了重命名目录名称，请使用此命令：**重命名<current** *name***> <new** *name***>**

例如：

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

步骤3.配置IOS IPS加密密钥

第三步将配置IOS IPS使用的加密密钥。此密钥在Step1下载的realm-cisco.pub.key.txt文件查找。

加密密钥用于验证内容由思科专用密钥签字保证其真实性和完整性在每版本的重要的签名文件的(sigdef-default.xml)数字签名。

1. 打开文本文件，并且复制文件的内容。
2. 请使用**configure terminal命令**为了输入Configure模式的路由器。
3. 粘贴文本文件内容在<hostname> () #提示符。
4. 退出路由器配置模式。
5. 输入**show run命令**在路由器提示为了确认加密密钥配置。您在配置里应该看到此输出：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. 请使用此命令为了保存配置：**复制运行配置启动配置**

其它命令和参考

如果密钥不正确地配置，您必须首先去除加密密钥然后重新配置它：

1. 为了去除密钥，请输入命令如下列出的这些in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. 请使用**show run命令**为了验证密钥从配置删除。
3. 完成在步骤3的步骤为了重新配置密钥。

步骤4. Enable (event) IOS IPS

第四步将配置IOS IPS。完成此步骤为了配置IOS IPS ：

1. 请使用**ip ips名称<rule** *name*> <*可选ACL* >命令为了创建规则名称。(这在接口将用于启用IPS。)例如：router#**configure terminal** router(config)#**ip ips name iosips** 您能指定可选延长或标准的访问控制表(ACL)为了过滤将由此规则名称扫描的流量。由ACL允许的所有流量是受检查支配由IPS。由ACL拒绝的流量没有由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设置位置flash: <directory** *name*>命令为了配置IPS签名存储位置。(这是在步骤创建的*ips*目录2.)例如：router(config)#**ip ips config location flash:ips**
3. 请使用**ip ips通知sdee**命令为了启用IPS SDEE事件通知。例如：router(config)#**ip ips notify sdee** 为了使用SDEE，必须启用HTTP服务器(用**ip http server命令**)。如果HTTP服务器没有启用，路由器不能回应对SDEE客户端，因为看不到请求。默认情况下SDEE通知禁用并且必须明确地启用。IOS IPS也支持使用Syslog为了发送事件通知。可以独立地使用SDEE和

Syslog或同时启用为了发送IOS IPS事件通知。默认情况下系统日志通知启用。如果logging console启用，您将看到IPS系统消息。为了启用Syslog，请使用此命令：`router(config)#ip ips notify log`

4. 配置IOS IPS使用其中一个预定义的签名类别。与思科5.x格式签名的IOS IPS运行与签名类别(正如思科IPS设备)。所有签名分组到类别，并且类别分层的。这帮助分类容易分组和调整的签名。**警告：** *所有*签名类别包含在签名版本的所有签名。因为IOS IPS不能编译，并且使用包含的所有签名在签名一次请发布，不*撤销收回所有类别*;否则，路由器将用尽内存。**注意：** 当您配置IOS IPS时，您必须首先退休在*所有*类别的所有签名，撤销收回然后选择签名类别。**注意：** 签名类别在路由器配置的命令也是重要。IOS IPS处理命令在配置里列出的类别in命令。一些签名属于多个类别。如果多个类别配置，并且签名属于对超过他们中的一个，(例如，退休， unretired，操作等等)在最后已配置的类别IOS IPS使用签名的属性。在本例中，在"所有"类别的所有签名退休， *IOS IPS基本*类别然后unretired。`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. 请使用这些命令为了启用在所需的接口的IPS规则，并且指定规则将应用的方向：**建立接口 <interface name>ip ips <rule** *name***> [***在/***]**例如：`router(config)#interface GigabitEthernet 0/1 router(config-if)#ip ips iosips in router(config-if)#exit router(config)#exit router#` *在*参数含义进入接口的仅流量由IPS检查。*缩小*参数含义流量只出去接口由IPS检查。为了使IPS里里外外检查两接口的流量，*里里外外请分*开进入同一个接口的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.装载IOS IPS签名包到路由器

最后一步是装载对签名包在Step1下载的路由器。

注意： 装载签名包的普通方法对路由器是使用FTP或TFTP。此步骤使用FTP。请参考*其它命令和References部分*在此步骤替代方法的能装载IOS IPS签名包。如果使用一远程登录会话，请使用**terminal monitor命令**为了查看控制台输出。

为了装载签名包到路由器，请完成这些步骤：

1. 请使用此命令为了复制从FTP服务器的下载的签名包到路由器：**复制ftp:// <ftp_user** *：password@Server_IP_address* **>/<signature_package> idconf注意：** 请切记使用*idconf*参数在**copy命令结束时。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]` 在签名包装载到路由器之后，签名编译开始。您能看到注册有日志级别的6或上述已启用路由器。

```
*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. 请使用**count命令显示ip ips的签名**为了验证签名包适当地被编译。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#`

其它命令和参考

如果在签名编译时收到错误消息类似于此错误消息，公共加密密钥无效：

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

参考的步骤3欲知更多信息。

如果不访问FTP或TFTP server，您能使用USB闪存驱动器为了装载签名包到路由器。首先，请复制在USB驱动上的签名包，连接USB驱动到其中一个在路由器的USB端口，以*idconf*参数然后使用**copy命令**为了复制签名包到路由器。

例如：

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

有在已配置的IOS IPS存储设备目录的六个文件。这些文件使用此命名格式：<router NAME >-sigdef-xxx.xml或<路由器名字>-*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#
```

这些文件在被压缩格式存储并且不直接地编辑可能或看得见。每个文件的内容下述：

- *路由器sigdef default.xml包含*所有出厂默认设置签名定义。
- *路由器sigdef delta.xml包含*从默认更改的签名定义。
- *路由器sigdef typedef.xml包含*所有签名参数定义。
- *路由器sigdef category.xml包含*签名类别信息，例如先进类别的ios_ips基本和。
- *路由器SEAPdelta.xml包含*做的变动对默认SEAP参数。
- *路由器SEAPtypedef.xml包含*所有SEAP参数定义。

部分II.高级配置选项

此部分在先进的IOS IPS选项提供说明和示例为签名调整。

退休或撤销收回签名

退休或撤销收回签名平均值选择或取消选定由IOS IPS使用为了扫描流量的签名。

- **退休**签名含义IOS IPS不会编译该签名到扫描的内存。
- **Unretiring**签名指示IOS IPS编译签名到内存和使用签名扫描流量。

您能使用IOS命令行界面(CLI)为了退休或撤销收回各自的签名或属于签名类别签名的一组。当您退休或撤销收回每签名的组时，在该类别的所有签名退休或unretired。

注意： 一些unretired签名(unretired作为单个签名或在一个unretired类别内)可能不编译由于内存不足或无效参数或者，如果签名是已废弃的。

此示例显示如何退休各自的签名。例如，签名6130有subsig ID 10 ：

```
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)#
```

此示例显示如何对撤销收回属于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： 当在类别的签名除基本IOS的IPS和提前的IOS IPS之外unretired作为类别时，一些签名或引擎的编译可能发生故障，因为IOS IPS不支持在那些类别的某些签名(请参见下面的示例)。顺利地编译(unretired)签名IOS IPS用于所有其他扫描流量。

```
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
```

Enable (event)或禁用签名

当数据包或数据包流匹配签名时，要启用或禁用签名是强制执行或忽视操作关联与签名由IOS IPS。

注意： Enable (event)和禁用不选择并且取消选定IOS IPS将使用的签名。

- 要**启用**签名意味着，当触发由匹配数据包(或数据包流)，签名采取适当行为关联与它。然而，当他们启用，只unretired和顺利地编译签名将采取行动。换句话说，如果签名退休，即使启用，它不会被编译(因为退休)，并且不会采取行动关联与它。
- 要**禁用**签名意味着，当触发由匹配数据包(或数据包流)，签名不采取适当行为关联与它。换句话说，当签名禁用，即使unretired和顺利地被编译，它不会采取行动关联与它。

您能使用IOS命令行界面(CLI)为了启用或禁用各自的签名或根据签名类别的签名的一组。此示例显示如何禁用签名6130有subsig ID 10。

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

崔凡吉莱签名操作

您能使用IOS命令行界面(CLI)为了更改一个签名或根据签名类别的签名的一组的签名操作。此示例显示如何更改签名操作为签名6130警告，丢弃和重置有subsig ID 10。

```
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& Services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
- Cisco Secure设备管理器软件下载
- 如何使用CCP配置IOS IPS
- Cisco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