Ciscoworks IPS MC在Cisco IOS IPS的配置示例

目录

简介

CiscoWorks Management Center for IPS Sensors (IPS MC)是思科IPS设备的管理控制台。IPS MC版本2.2支持入侵防御系统(IPS)功能的供应在Cisco IOS软件路由器的。本文描述如何使用IPS MC 2.2配置Cisco IOS IPS。

关于如何使用(包括如何使用它配置设备没有根据Cisco IOS软件)的IPS MC的更多信息，参考CiscoWorks Management Center for IPS Sensors文档在此URL ：

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据CiscoWorks Management Center for IPS Sensors (IPS MC)版本2.2。

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。

配置

配置任务基本的了解

IPS MC用于管理Cisco IOS IPS路由器的一组的配置。注意IPS MC不管理从运行IPS的路由器的警报。思科推荐思科安全检测、分析及响应系统(Cisco安全火星) IPS监控的。配置管理包括在本文描述的一系列的任务。这些任务可以分开成三个相位：导入、配置和部署如此镜像所显示。

每个相位有其自己的套责任和功能：

- *导入*—导入路由器到IPS MC。在您能使用IPS MC配置它前，您必须导入路由器到IPS MC。路由器不可能导入，除非初始IPS配置在路由器存在(详细信息给以后在本文)。
- *配置*—配置设备。例如，您能配置Cisco IOS IPS路由器使用其中一个思科推荐的pretuned签名文件。配置更改存储在IPS MC，但是没有发送到路由器在此相位。
- *部署*—提供对实际设备的配置更改。在此相位期间您承诺做的变化在配置任务上给路由器。
- *另外的任务*— IPS MC提供一个autodownload功能自动地下载从Cisco.com的签名更新。

您必须了解此被逐步采用的方法为了有效使用IPS MC。它是与基于设备的管理Guis不同，例如思科路由器和安全设备管理器(SDM)。基于设备的Guis操作直接地在单个路由器，而IPS MC设计研究networkwide的路由器(和其他IPS设备的组例如Cisco IPS 4200系列传感器)。

本文在图表中提供关于其中每一的信息任务帮助您使用IPS MC管理Cisco IOS IPS路由器。

Cisco IOS IPS路由器初始配置

为了成功导入或添加Cisco IOS IPS路由器到IPS MC，您必须执行在Cisco IOS IPS路由器的某些初始配置步骤。此部分描述那些步骤。

您必须通过思科IPS MC启用在一个Cisco IOS IPS路由器的安全壳SSH协议配置、导入和部署的。另外，必须为报告目的事件启用安全设备事件Exchange (SDEE)协议(虽然这些警报没有被发送对IPS MC，因为IPS MC仅使用设置，不报告)。最后，您需要确保在IPS路由器的时钟设置与IPS MC同步。

完成这些步骤为了配置您的IOS IPS路由器：

1. 创建一个本地用户名和密码对于路由器。`Router#config terminal Router(config)#username <username> password <password>`
2. 启用在VTY线路接口的本地登录。`Router#config terminal Router(config)#line vty 0 15 Router(config-line)#login local Router(config-line)#exit` 如果传输输入或transport output命令行界面(CLI)配置在VTY line configuration下，请确保SSH启用。例如：`Router#conf terminal Router(config)#line vty 0 15 Router(config-line)#transport input ssh telnet Router(config-line)#exit`
3. (如果密钥已经不存在)，请生成1024位RSA密钥。SSH在加密算法密钥生成以后自动地启用。`Router#conf terminal Enter configuration commands, one per line. End with CNTL/Z.`

```
Router(config)#crypto key generate rsa The name for the keys will be: Router.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the
modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Router(config)# *Jan 23 00:44:40.952: %SSH-5-ENABLED: SSH 1.99 has been enabled Router
config)#
```

4. 在路由器的Enable (event) SDEE。`Router(config)#ip ips notify sdee`
5. Enable (event) HTTPS。HTTP或HTTPS要求为了IPS MC能与有SDEE的路由器联络收集事件信息。`Router(config)#ip http authentication local Router(config)#ip http secure-server`
6. 请使用外部网络时间协议(NTP)服务器或clock命令为了配置在IPS路由器的时钟设置。`Router(config)#clock set hh:mm:ss day month year`

现在Cisco IOS IPS路由器准备好，并且可以导入到进一步配置和管理的IPS MC。

导入Cisco IOS IPS路由器到IPS MC

一旦完成在路由器的初始配置，您能添加(或导入)它到IPS MC。

1. 启动您的Web浏览器和点对CiscoWorks服务器。CiscoWorks洛金管理器出现。**注意：** Web服务器的默认的端口号是1741;因此，您应该使用URL类似于http:// <server *ip address>:1741/*。
2. 回车用户名和密码为了登陆。CiscoWorks主页出版。
3. 在左侧导航窗格中，请选择**VPN/安全管理解决方案**，然后选择**管理中心**。IPS传感器页的管理中心出现。此页显示这五选项卡：*设备*—在Devices选项，您能执行初始设置和管理所有deviceson系统。*配置*—在Configuration选项，您可执行供应功能。您能配置设备在级的各台设备或在社团级别。一个设备组能包含多个设备。必须保存通过配置任务做的所有变动。配置功能不立即做对设备的变动。您必须使用部署功能为了部署您的更改。*部署*—在部署选项卡，您能部署您的对设备的配置更改。当配置更改应该生效时，请安排功能提供灵活控制。*报告*—在Reports选项，您能生成多种系统操作报告。在Admin选项卡的*Admin* -，您可执行系统管理任务，例如数据库管理、系统配置和许可证管理。
4. 点击**Devices选项**为了添加新设备。传感器页出版。
5. 单击 **Add**。挑选页心出版。您必须通知IPS MC什么类型添加您要执行的功能。此列表描述每个选项：*从设备的导入配置*—请使用此选项添加到IPS在网络当前运行的MC设备。*创建默认配置*—请使用此选项在网络当前不运行的添加设备。*添加多个设备*—请使用此选项添加多个设备。您能创建.csv或包含所有设备信息的.xml文件然后导入它到IPS MC为了一次添加设备。**提示：** 示例.csv格式和.xml格式文件查找在：InstallDirectory \ MDC \等\ ID \和被命名MultipleAddDevices-format.csv和MultipleAddDevices-format.xml，分别。
6. 选择适当添加Type选项，并且**其次**单击。
7. 选择您想要添加Cisco IOS IPS路由器的组，或者请使用默认全局组和**其次**然后单击。回车传感器信息页出版。
8. 在识别页，请输入设备的标识信息。**注意：** 如果用户没有权限级别15访问权限，您必须供应特权密码。在识别页的最后一行，请检查**使用SSH证书检查**复选框。
9. 单击 **Next**。添加传感器摘要出版。
10. 单击 **完成**。设备成功地添加到IPS MC。**注意：** 在导入过程期间，如果遇到错误，请确保您检查这些项目：*事先需要的配置*—这些配置要求为了IPS MC能与Cisco IOS IPS路由器联络。*连接*—确保IPS MC能到达Cisco IOS IPS路由器。*时钟*—检查在IPS MC和Cisco IOS IPS路由器的时代。时间是使用验证https证书的关键组件。时代必须是在12个小时彼此内。(最佳实践是至多一些个小时。)*Cisco IOS IPS证书*—有时存储的Cisco IOS IPS证书不正确。为了删除从Cisco IOS IPS的一证书，您必须从Cisco IOS IPS路由器删除信任点。*更多的配置*—如果**IP HTTP超时策略**用最大请求低数值配置，例如**IP HTTP超时策略空闲生活86400请求1的600**，您必须增加最大请求编号。例如：**IP HTTP超时策略空闲600生活86400请求8400**

配置Cisco IOS IPS路由器使用Pretuned签名文件

在您导入路由器到IPS MC后，您必须选择签名定义文件(自卫队) (包括威胁签名IPS路由器将使用)的文本基于文件和操作采取，当每个签名被触发时(例如，丢弃、TCP重置，报警)。

Cisco系统®建议您使用思科pretuned自卫队文件。目前，有三个这样文件：攻击drop.sdf、128MB.sdf和256MB.sdf。IPS MC能自动地下载从Cisco.com的这些文件。欲知更多信息，请参阅AutodownloadSignature更新。

此步骤使用单个设备为例并且从路由器开始没有IPS配置。您能也使用此步骤在社团级别上的多个设备。

1. 点击**Configuration选项**。配置页出版。
2. 从在页的左边查找的对象选择器，请选择您要配置的Cisco IOS IPS路由器。**注意：** 大多在IPS MC 2.2的配置设置可以配置在社团级别以及在各台设备级别。例如，全局， iosips和sdmlab组是所有可配置对象组。此示例使用sdmlab组单个设备思科。一旦选择您要配置的路由器，路径柱状图查找在配置页显示顶部当前范围配置。例如，此示例的范围*全局> sdmlab > cisco*。*cisco*是当前配置对象(即从对象选择器选择的路由器。
3. 从配置菜单柱状图，请点击**设置**。Settings页出版。在Settings页，您能更改选定对象的配置设置。配置设置特定对Cisco IOS IPS路由器在页的左边查找的TOC部分。这是可用的在TOC部分下任务的列表：*识别*— Cisco IOS IPS路由器基本信息;您能指定一个pretuned自卫队文件此处*签名*— Cisco IOS IPS路由器签名*签名向导*—签名向导添加定制签名*Cisco IOS IPS规则*—配置Cisco IOS使用适用于接口的IPS规则*Cisco IOS IPS过滤器*— Cisco IOS IPS过滤器*Cisco IOS IPS重组*—接口IP虚拟重组配置*Cisco IOS IPS SDEE属性*—配置SDEE设置*Cisco IOS IPS一般属性*—另外的Cisco IOS IPS相关的配置
4. 选择**识别**为了配置pretuned自卫队文件。识别页出版。
5. 从自卫队类型下拉列表，请选择适当的pretuned自卫队，然后单击**应用**为了应用更改。Cisco IOS IPS支持超过1600个签名，是在路由器之外存储器容量接受。SDFs开发作为一个方便方式选择和装载最重要的签名。目前，您能从三SDFs选择。他们大小不同为了使您根据您的路由器DRAM产能选择自卫队文件。可用的选择描述此处：移置—自卫队类型没有设置。ATTACK-DROP —此SDF是为有DRAM 64 MB的路由器。256MB —此SDF是为有DRAM 256 MB的路由器。128MB —此SDF是为有DRAM 128 MB的路由器。**注意：** 128-和256 MB SDFs要求2.001引擎或更加极大。此信息是可用的在**设置>识别UI >版本字段**。**警告：** IPS MC不包括Cisco IOS IPS路由器的管理功能。当您选择您的Cisco IOS IPS路由器的时，自卫队文件小心。保证Cisco IOS IPS路由器有运行的足够的内存选定自卫队文件。**注意：** 当您更改自卫队类型时，您也许收到此消息：*当更改自卫队类型时，您能选择保持或丢弃调整关于设备的签名信息。点击OK键丢弃。点击取消保持。*
6. 点击**取消**为了继续您的签名调整信息。即然您顺利地选择路由器思科的pretuned自卫队，您可执行调整例如的另外的签名添加或编辑，甚至创建您自己的签名，或者您可以跳过调整任务的签名和直接地去创建规则适用于接口。
7. 单击**等待**从配置菜单柱状图。待定页出版。这时，配置任务完成。然而，您必须完成部署任务为了部署您的对目标设备的更改。

修改Pretuned自卫队签名

在您选择路由器的后一个pretuned自卫队文件，您可执行调整任务的另外的签名。您能添加，编辑，删除和修改签名成特别合身您的需要，或者您能当必要时创建您自己的签名。此示例使用IPS MC为了添加另外的签名和修改操作。此镜像显示签名配置接口。

您能使用签名配置为了启用或禁用，选择或者取消选择，添加签名，删除签名，更改签名操作和编辑签名参数。请使用签名向导到左边创建定制的签名。

默认情况下在签名配置用户界面，一些信息显示。选定是指签名是否在自卫队文件包括发送对路由器。如果签名没有选择，不会被添加。只有当签名选择，已启用应用。当签名禁用， IPS引擎不会发送该特定签名的事件。如果签名取消选择，自动地也禁用。

最后两列(支柱Src和参数Src)告诉您签名和其参数何处，分别，来自。签名可能被采取了从pretuned自卫队文件或从您在IOSSxxx.zip文件更新的出厂默认设置(能找到显示，当IOS IPS默认)。这些值适用于参数列。

当您添加签名到Cisco IOS IPS路由器时，必须占内存考虑事项。如果比Cisco IOS IPS路由器能处理添加更多签名， IPS MC不能部署对设备的配置更改。

完成这些步骤为了添加签名5489/x到Cisco IOS IPS路由器：

1. 选择**配置**，然后请使用对象选择器为了选择您要配置IPS签名的Cisco IOS IPS路由器。
2. 选择**Configuration>设置>签名> IOS IPS**。在组页的签名出现。
3. 在发生的签名列表，请由ID选择过滤器，并且键入签名ID 5489。
4. 点击**过滤器**为了搜索签名。搜索结果出现。**注意：** IPS MC不支持在思科SDM的新建的目录联机。
5. 在未选择的签名旁边检查复选框，并且点击**精选**在底下工具栏。
6. 单击**编辑**为了更改签名操作。编辑签名页出版。
7. 检查**选定**复选框，并且选择**报警**、**丢弃**和**重置**从Actions列表。
8. 检查**覆盖**复选框，然后点击OK键。所有签名更改与所需的动作。
9. 去待定任务并且保存所有更改。这完成配置任务。**提示**： 注意密切注意支柱Src列。在修改以后，更改的来源对设备命名了*cisco*，含义所有调整的信息分开保存从默认pretuned自卫队文件。此机制给IPS MC能力保留定制的签名更改。

在前面部分，当您更改自卫队文件类型， IPS MC询问您您是否要继续签名调整信息。这是调整信息的签名是指。

选择定制的签名

如果不要使用默认pretuned自卫队文件，您在部分修改Pretuned自卫队签名能使用指定的步骤为了选择调整您的设备的签名。在识别页，您需要确保类型被移置的自卫队。参考的步骤3配置Cisco IOS IPS路由器使用Pretuned签名文件。

创建规则适用于接口

在调整签名以后，您需要启用在Cisco IOS路由器的IPS。为了启用在路由器的IPS，您必须创建IPS规则和应用它到至少一个接口。

1. 选择**配置**，然后请使用对象选择器为了选择您要配置的Cisco IOS IPS路由器。在路径柱状图验证您的范围在设备级别，不在社团级别。
2. 选择**Configuration>设置> IOS IPS规则**，然后单击**添加**。Details页回车IPS的规则发表。
3. 输入您要应用规则和方向的规则名称和接口的信息。
4. 单击 **Ok**。IOS IPS规则页出版。同样地，您能创建两个方向的规则接口的。
5. 您必须保存配置更改和通过部署过程提供对设备的受影响的设备或组的更改。您可执行其他IPS相关的配置，但是其他任务可选和不需要的。您能在配置用户界面左边找到所有选项。本文不包括可选配置选项。

部署配置

在您做所有配置更改后，您必须使用部署任务为了确认对设备的更改。您做了得到目前为止的所有配置在IPS MC服务器保存本地。

为了部署配置更改，请去部署页，并且完成这些步骤：

1. 点击**部署**选项卡，并且选择**生成**为了生成配置更改。生成页出版。
2. 选择您已配置的，和点击**生成的***Cisco设备*。
3. 点击OK键接受生成的配置，然后点击OK键。Status页出版。
4. 请点击**刷新，**直到生成任务成功地完成。
5. 点击在部署菜单栏和sdmlab组中查找**Approve**为了发现需要批准配置的列表。审批页出版。
6. 选择任务，并且单击**审批**。点击在部署菜单栏查找**Deploy**，并且单击**提交**。SUBMIT页出版。
7. 选择您要提交部署任务的设备。
8. 选择*Cisco设备*，并且单击**部署**。挑选配置页出版。
9. 选择您做到*Cisco设备的*配置，并且**其次**单击。Properties页回车的工作出现。
10. 您能立即部署更改或安排任务以后执行它。在本例中，请选择**立即**选项，**其次**然后单击。一简要工作摘要显示并且准备部署。
11. 单击 **完成**。在部署结束时，对话框显示部署过程的状况。您成功部署Cisco IOS IPS配置到设备。当您配置多个设备时，您在社团级别上能做配置更改然后应用对属于同一组的所有Cisco IOS IPS路由器的更改。**提示**： 此进程是较的，但是奎克交付功能是可用的。当您使用此功能时，您不必须通过**生成>审批>部署**进程。完成这些步骤为了使用功能：在用户界面的上面是小图标行。使用您的在第一个图标的鼠标翱翔，和请查看在此镜像显示的工具套子：为了启用生成和部署任务，去**Admin >System Configuration>配置文件管理**和非选定**Enable (event)手动配置文件更改批准**复选框。使用您的在第一个图标的鼠标翱翔，它显示任务启用。点击此图标。IPS MC自动地生成配置更改并且部署他们到设备。

Autodownload签名更新

IPS MC支持从Cisco.com的autodownload签名更新。它能下载签名更新传感器平台的，以及Cisco IOS IPS平台的。为了配置此功能，请去**Admin >System Configuration>自动下载IPS更新**。

Update页自动下载的IPS出现。

您必须有一个有效Cisco.com帐户为了下载此签名更新。为了检查autodownloaded文件，请去IPS MC安装主目录。默认情况下它是\程序文件\ CSCOpx \ MDC \等\ ID \更新。

此镜像显示下载的文件的镜像在此目录的。

您能看到传感器更新文件。Cisco IOS软件更新文件和pretuned自卫队文件下载。

更新Cisco IOS IPS路由器用新的自卫队文件

对于Cisco IOS IPS路由器配置有pretuned自卫队文件，当自卫队文件的新版本通过autodownload是可用的或复制对更新目录，思科IPS MC认可新版本。在用户界面刷新，可适用的设备的设备图标启用黄色后。

1. 点击**部署**，并且通过生成，审批，并且部署进程。
2. 在成功的部署以后， Cisco IOS IPS路由器使用自卫队文件新版本。

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