CS-MARS ：添加Cisco IPS传感器作为CS-MARS的报告设备配置示例

目录

简介

本文解释如何准备Cisco Secure入侵防御系统(IPS)设备和所有已配置的虚拟传感器作为报告的设备到Cisco安全监听、分析和答复系统(CS-MARS)。

先决条件

要求

使用在SSL的SDEE对于思科IPS 5.x、6.x和7.x设备，毁损下拉式日志。所以，火星必须得以进入对传感器的HTTPS。为了准备传感器，您必须使在传感器的HTTP服务器， enable (event) TLS允许HTTPS访问，并且确保，火星的IP地址定义作为一台允许主机，能访问传感器和下拉菜单事件的一。如果传感器配置对从有限的主机或子网的允许在网络，您能使用**access-list ip_address/网络屏蔽**命令为了启用此访问。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Secure毁损运行软件版本4.2.x和以后的设备
- 运行软件版本6.0及以后的Cisco 4200系列IPS设备

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。

相关产品

此配置可能也与这些传感器一起使用：

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20

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

在此部分，您如何的提交与信息关于添加并且配置Cisco Secure入侵防御系统(IPS)传感器到Cisco安全监听、分析和答复系统(CS-MARS)设备。

添加并且配置在火星的思科IPS 6.x或7.x设备

当您定义了在火星时的一个思科IPS 6.x或7.x设备，您能发现在设备配置的所有虚拟传感器。当您发现这些虚拟传感器时，这允许火星由虚拟传感器分离报告的事件。它也允许您调整受监视网络列表到每个虚拟传感器，改进希望的报告的准确性。

完成这些步骤为了添加和配置在火星的一个思科IPS 6.x或7.x设备：

1. 选择**Admin >System设置> Security并且监控设备**。然后，请点击**Add**。
2. 从设备类型列表选择**思科IPS 6.x或思科IPS 7.x**。现在请进入传感器的主机名在**Device Name字段的**如显示此处。IPS1是用于此示例的设备名。设备名值一定是相同的与已配置的传感器名称。现在请在**报告的IP**字段输入管理IP地址。报告的IP地址是地址和管理IP地址一样。
3. 在**洛金字段**，请输入用户名关联与使用访问报告的设备的管理帐户。现在，在**密码字段**，请输入密码关联与在**洛金字段**指定的用户名。**用户名**是**cisco，**并且使用的**密码**是在本例中的**cisco123**。并且请输入在传感器的网络服务器运行在**端口字段**侦听的TCP端口号。默认HTTPS端口是443。**注意：** 当配置仅时HTTP是可能的，火星要求HTTPS。
4. 现在请验证**没有**在**箴言报资源使用**列表chosed。当箴言报资源使用选项出现在此页时，不为思科IPS作用。
5. 为了请求从传感器的IP日志，请从**下拉菜单IP**记录表选择**是**。这是可选功能，可以如果必须使用。此设置适用于整个传感器，包括为虚拟传感器警报生成的那些日志。
6. 点击**测验连接**为了验证配置和启用虚拟传感器发现。
7. 单击**发现**为了发现所有定义虚拟传感器。**注意：** 火星对变动是做的没有察觉的对传感器。您做对虚拟传感器设置的变动，您在该传感器配置页必须单击**发现**为了刷新在火星的虚拟传感器详细信息。
8. 在虚拟传感器名称旁边选择复选框并且单击**编辑**为了定义每个虚拟传感器的受监视网络。现在IPS模块页出版如显示此处。
9. 对于攻击路径计算和缓解，请指定传感器监控的网络。选择**定义网络**单选按钮为了手工定义网络。然后请完成这些步骤为了定义网络：在**网络IP**字段输入网络地址。在**掩码字段**输入相应的网络掩码值。单击**添加**为了搬入指定的网络受监视网络字段。如果有需要定义更多网络，请重复上一个步骤。**注意：** 这是可选功能联机，并且可以被跳过，如果没要求。
10. 点击**精选网络**单选按钮按顺序选择附加到设备的网络。然后请完成这些步骤为了选择网络：从**精选**选择网络**网络列表**。单击**添加**为了搬入指定的网络受监视网络字段。如果有需要选

择更多网络，请重复上一个步骤。**注意：** 这是可选功能联机，并且可以被跳过，如果没要求。

11. 重复每个虚拟传感器的**步骤8**至**步骤10**。
12. 单击**提交**为了保存您的更改。设备名出现在安全和监听信息列表下。提交操作记录在数据库表上的变化。但是，它不装载更改到火星设备的工作内存。激活操作负载提交更改到工作内存。
13. 单击**激活**为了使火星开始sessionize从此设备的事件。火星开始sessionize此模块生成的事件和评估那些事件使用定义检查和下降规则。设备发布的任何事件对火星，在激活可以查询用设备的报告的IP地址作为匹配标准前。参考请激活报告和缓解设备。关于激活操作的更多信息。

验证火星拉从思科IPS设备的事件

它是普通创建在网络的良性事件为了验证数据流。完成这些步骤为了验证在思科IPS设备和火星之间的数据流：

1. 在思科IPS设备、enable (event)和警报在签名2000年和2004年。签名监视器ICMP消息(ping)。
2. ping在思科IPS设备侦听的子网的一个设备。事件由火星生成并且拉。
3. 验证事件在火星Web接口出现。您可用思科IPS设备执行查询。
4. 一旦数据流验证，您能禁用在思科IPS设备的2000年和2004个签名。**注意：** 如果测验连接操作不在一个思科IPS设备的配置时在火星Web接口的失效，则通信启用。此任务允许您进一步验证警报正确地生成并且被拉。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科安全检测、分析及响应系统支持页面
- Cisco 入侵防御系统支持页
- 思科安全检测、分析及响应系统-兼容性信息
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems