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)设备和所有被配置的虚拟传感器作为报告的设备到Cisco安全监控、分析和回应系统(CS-MARS)。

先决条件

要求

使用在SSL的SDEE对于Cisco IPS 5.x、6.x和7.x设备， MARS拉日志。所以， MARS必须得以进入对传感器的HTTPS。为了准备传感器，您必须enable (event)在传感器的HTTP服务器， enable (event) TLS允许HTTPS访问，并且确信， MARS的IP地址被定义作为一台允许的主机，能访问传感器和拉事件的一。如果传感器被配置了对从有限的主机的在网络的允许或子网，您能使用**访问列表ip_address/网络屏蔽**命令为了enable (event)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运行软件版本4.2.x和以后的MARS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

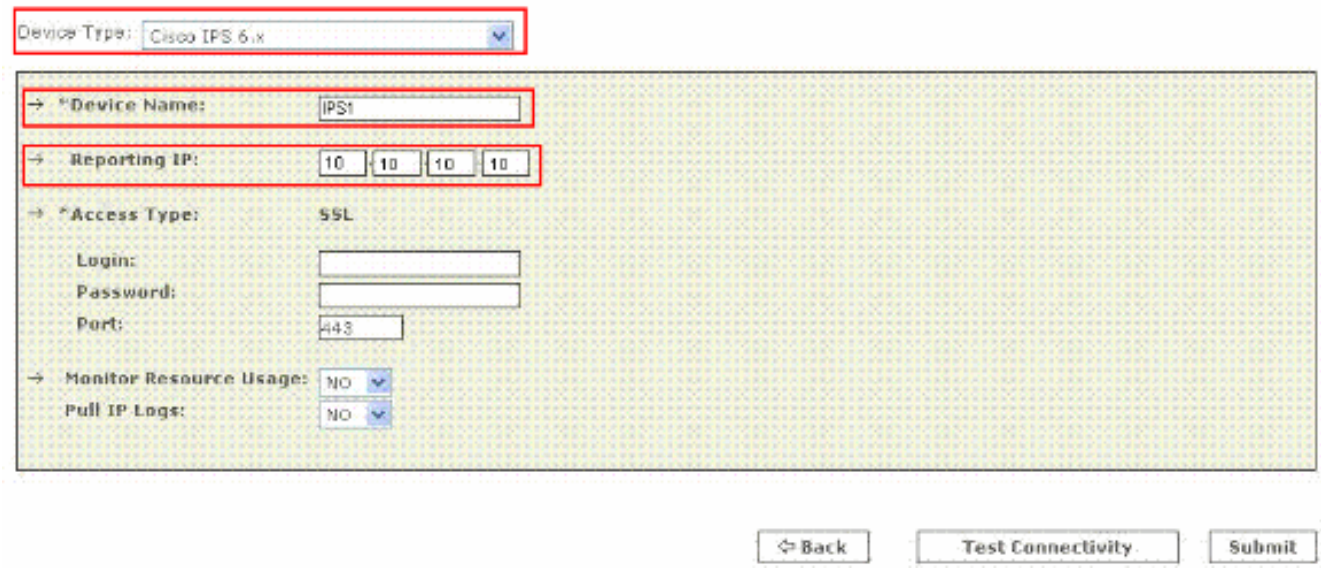
在此部分，向您介绍关于如何的信息添加和配置Cisco Secure入侵防御系统(IPS)传感器到Cisco安全监控、分析和回应系统(CS-MARS)设备。

添加并且配置在MARS的Cisco IPS 6.x或7.x设备

当您定义了在MARS时的Cisco 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MARS由虚拟传感器分离报告的事件。它也允许您调整被监控的网络列表到每个虚拟传感器，改进期望报告的准确性。

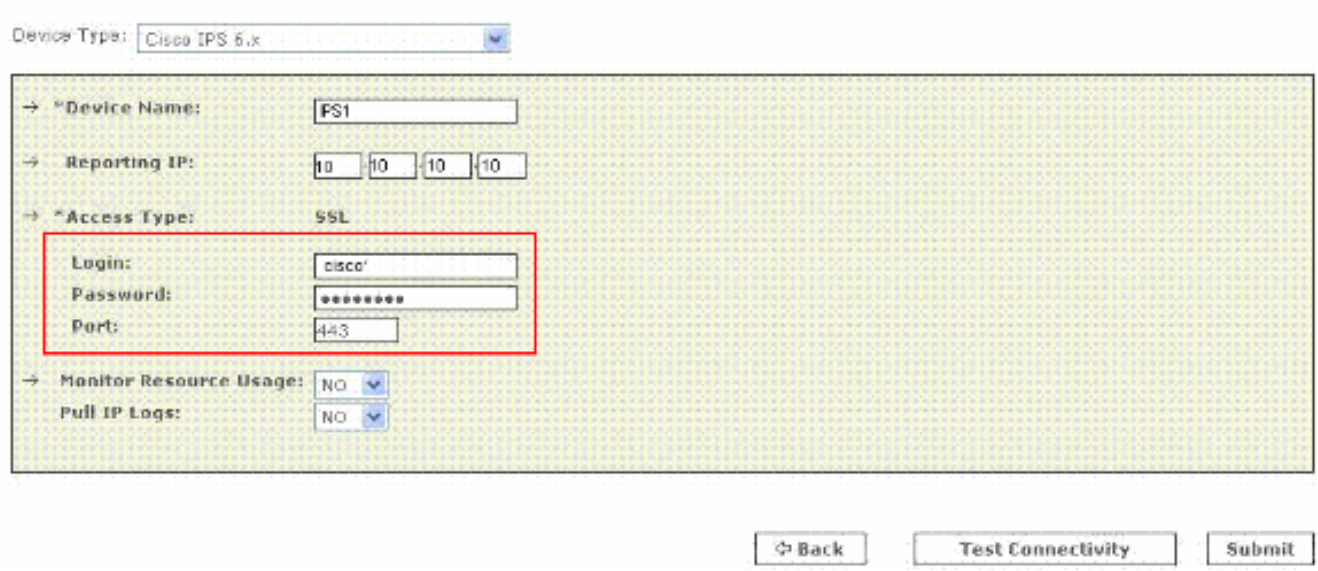
完成这些步骤为了添加和配置在MARS的Cisco IPS 6.x或7.x设备：

1. 选择**Admin >System设置> Security和监控程序设备**。然后，请点击**Add**。
2. 从设备类型列表选择**Cisco IPS 6.x或Cisco IPS 7.x**。现在请进入主机名-在**Device Name字段的**传感器如显示这里。IPS1是用于此示例的设备名。设备名值一定是相同的与被配置的传感器名字。



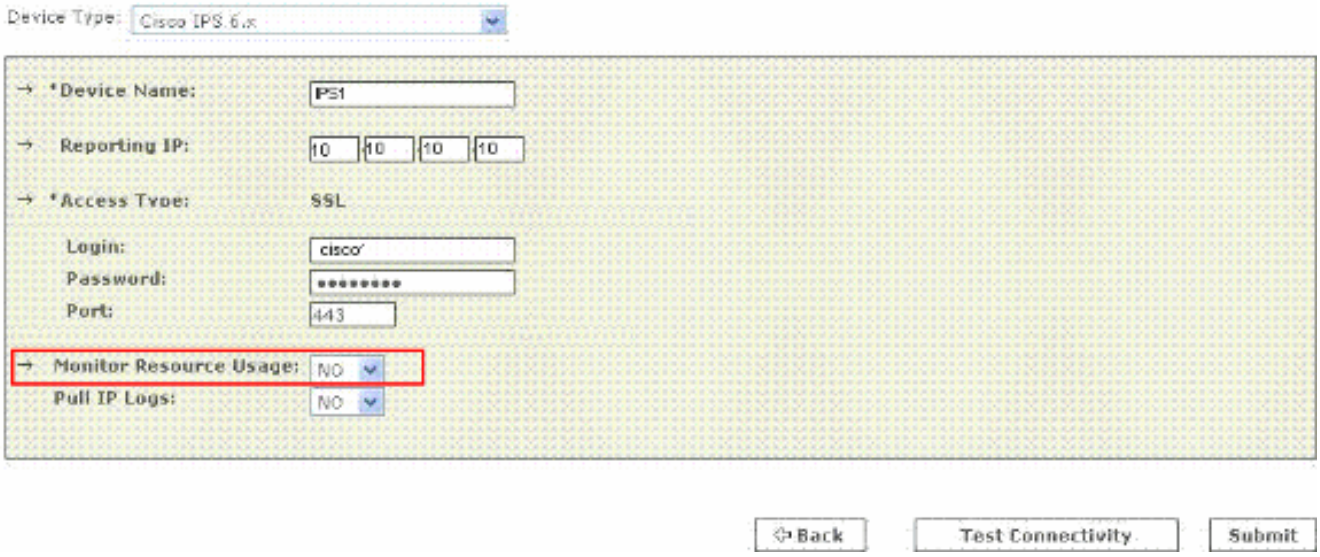
现在请输入管理IP地址在**报告的IP**字段。报告的IP地址是地址和管理IP地址一样。

3. 在**洛金字段**，请输入与使用访问报告的设备的管理帐户产生关联的用户名。现在，在**密码字段**，请输入与用户名产生关联的密码指定在**洛金字段**。**用户名**是**cisco**，并且使用的**密码**是在本例中的**cisco123**。并且请输入运行在传感器的网络服务器在**Port字段**监听的TCP端口编号。默认HTTPS端口是443。

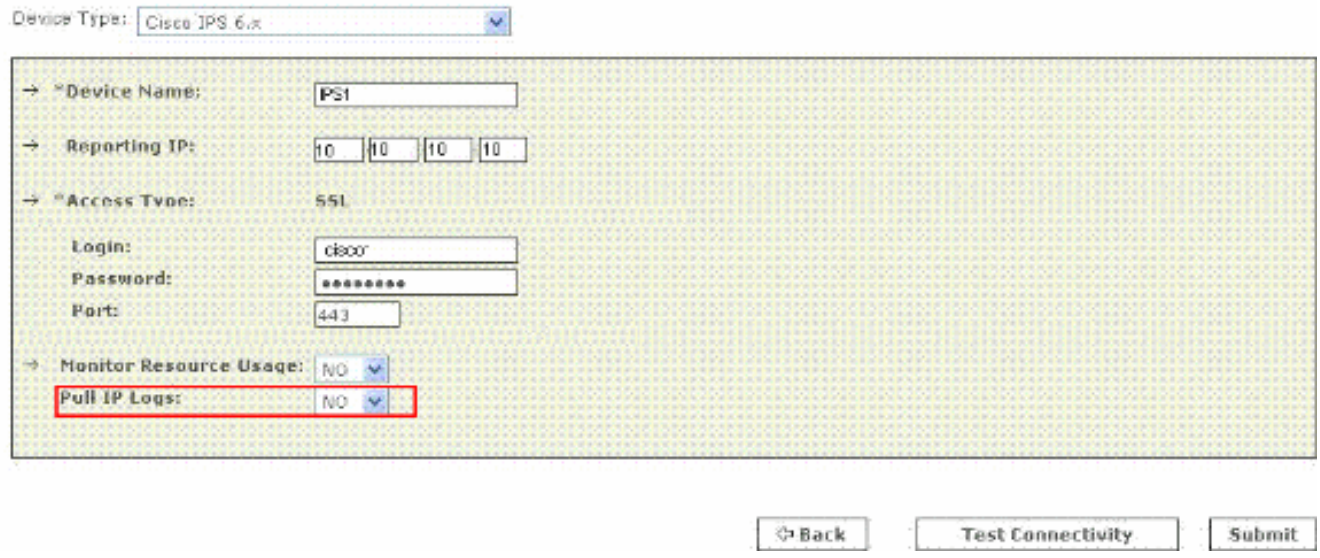


注意： 当配置仅时HTTP是可能的， MARS要求HTTPS。

4. 现在请验证**没有**在**监控程序资源使用**列表chosed。当监控程序资源使用选项出现在此页时，不为Cisco IPS作用。

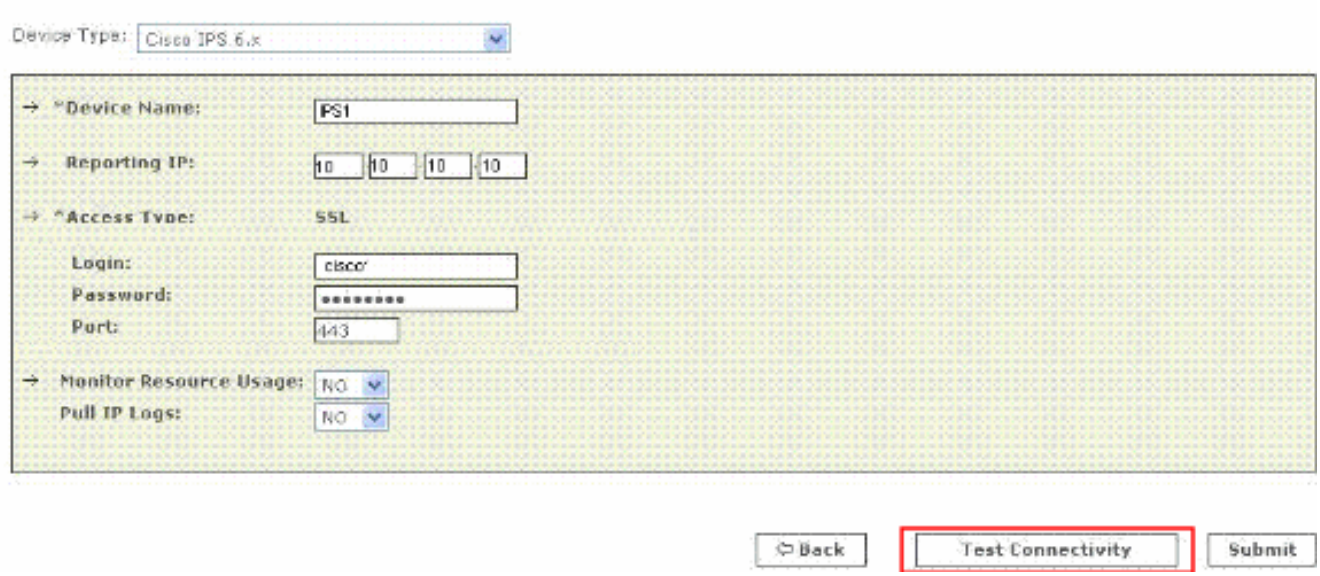


5. 为了拉从传感器的IP日志，从**下拉式IP**记录表**是请**选择。这是可选功能，可以如果必须使用。

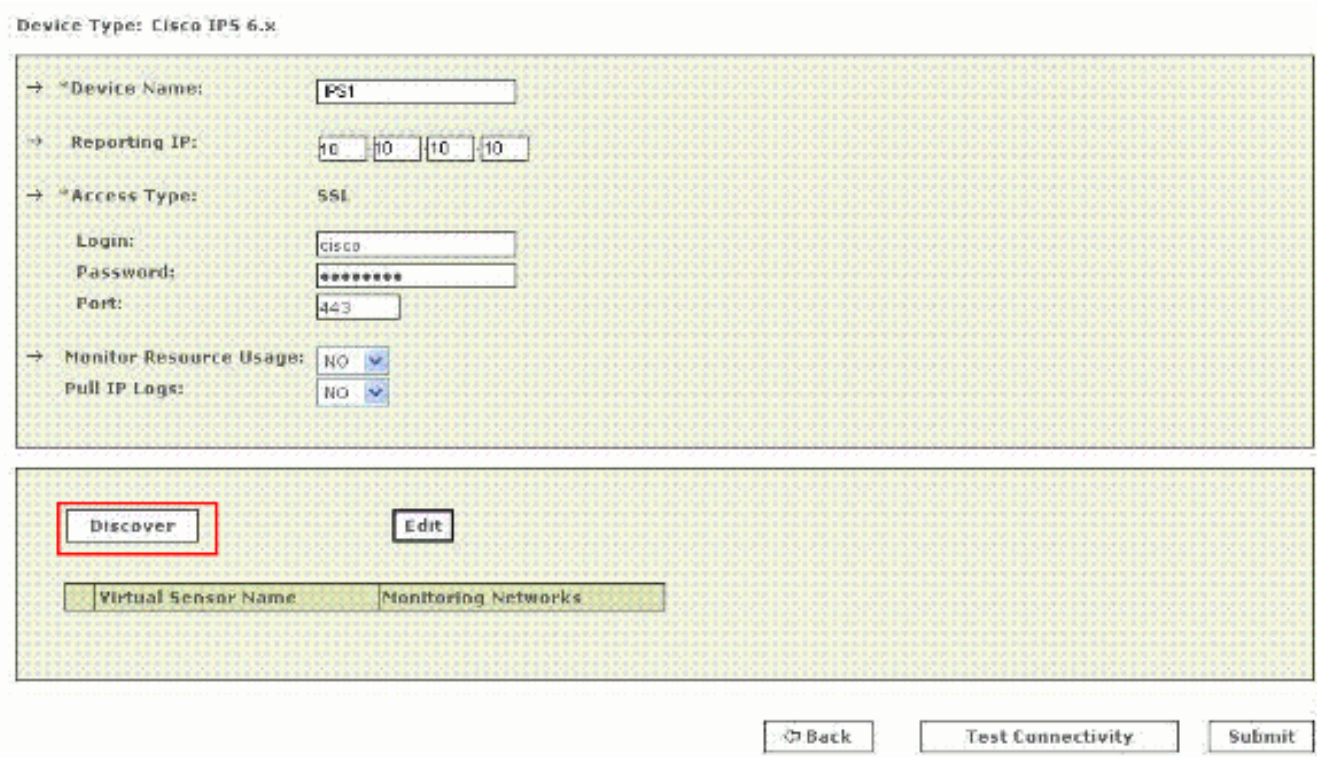


此设置适用于整个传感器，包括为虚拟传感器戒备生成的那些日志。

6. 点击**测试连接**为了验证配置和enable (event)在虚拟传感器的发现上。

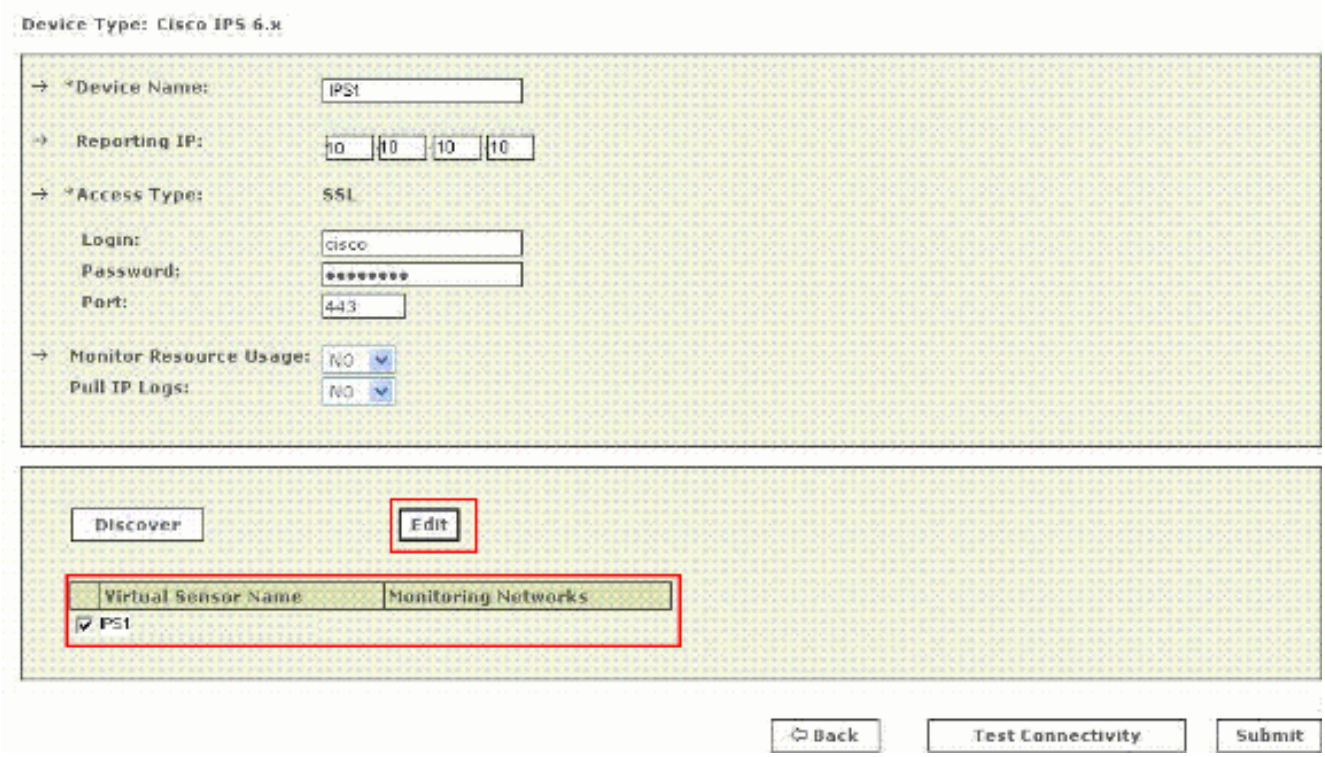


7. 点击**发现**为了发现所有被定义的虚拟传感器。

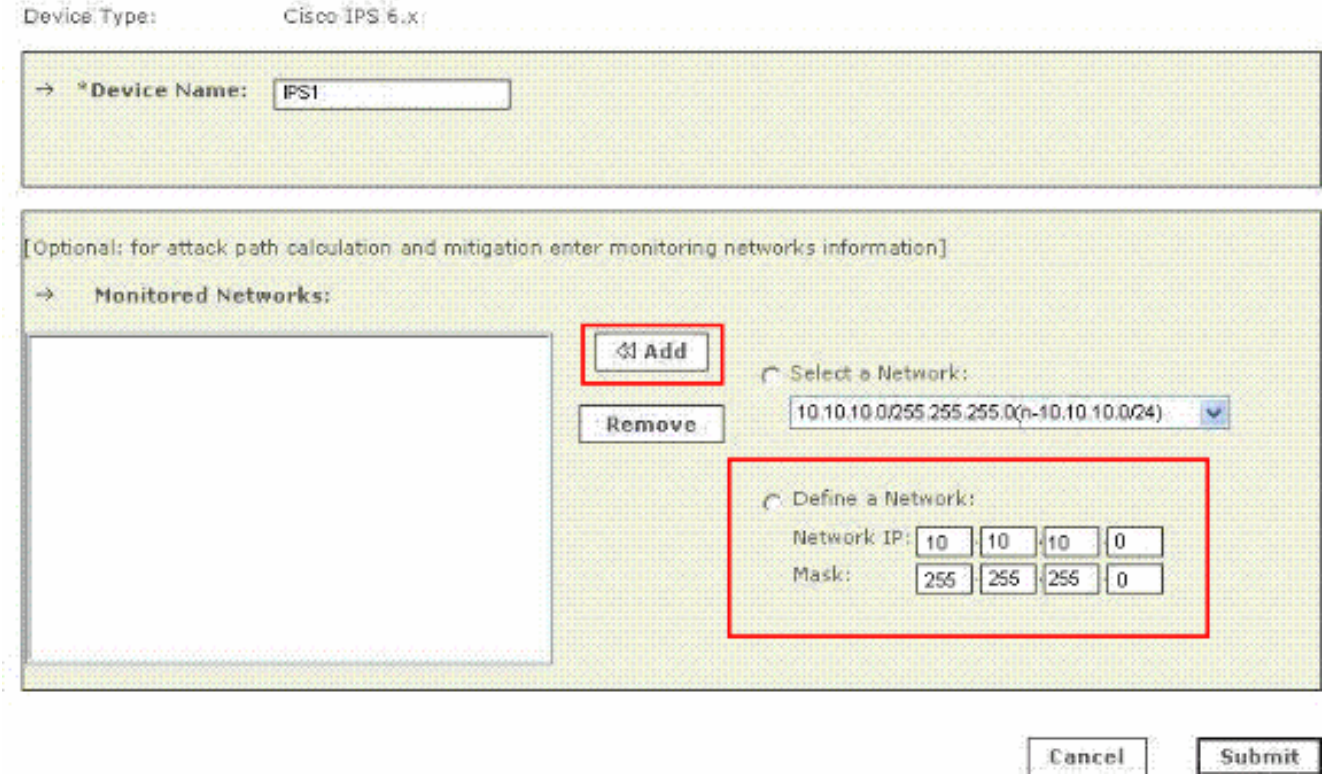


注意： MARS对变动是做的没有察觉的对传感器。您做对虚拟传感器设置的变动，您在该传感器配置页必须点击**发现**为了刷新在MARS的虚拟传感器详细资料。

8. 在虚拟传感器名字旁边选择复选框并且点击**编辑**为了定义每个虚拟传感器的被监控的网络。现在IPS模块页出版如显示这里。

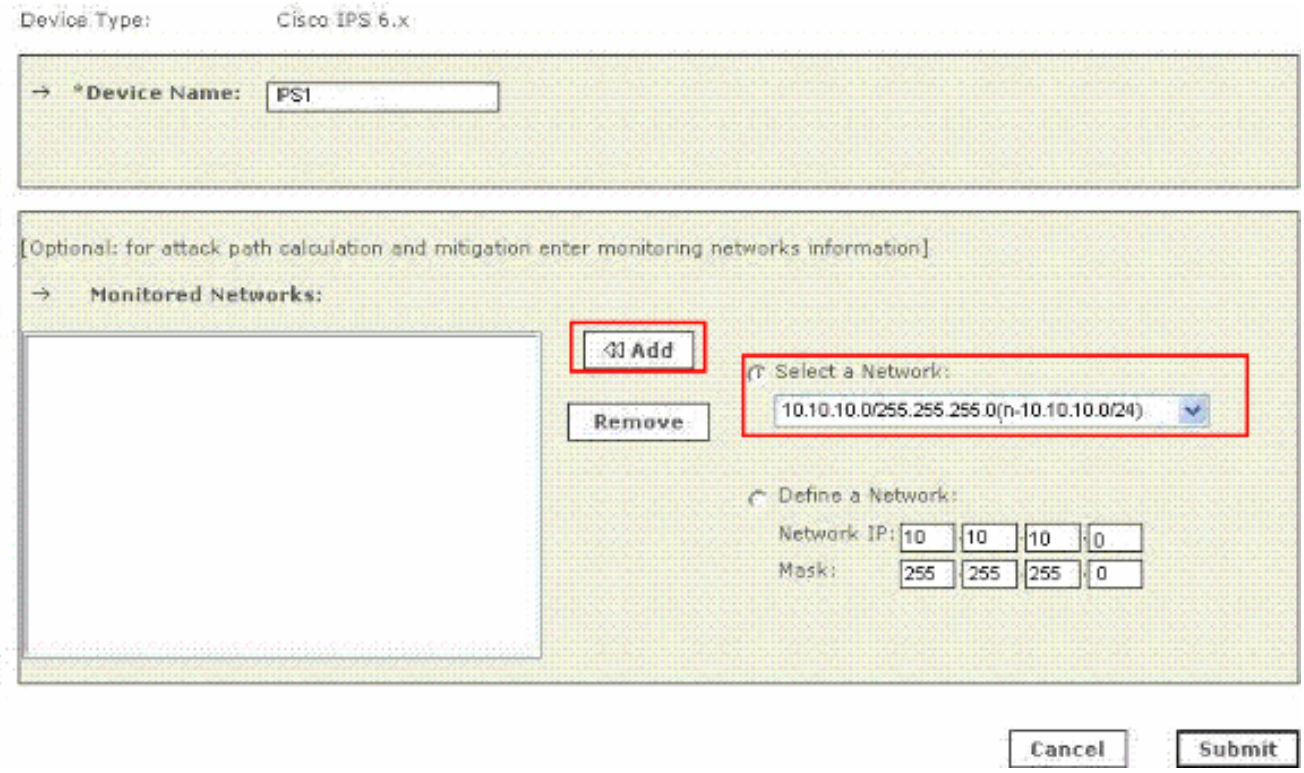


9. 对于攻击路径计算和缓解，请指定传感器被监控的网络。选择**定义网络**单选按钮为了手工定义网络。然后请完成这些步骤为了定义网络：输入网络地址在**网络IP**字段。输入相应的网络掩码值在**掩码**字段。点击**添加**为了搬入指定的网络被监控的网络字段。如果有需要定义更多网络，请重复早先步骤。



注意： 这是可用的可选功能，并且可以被跳过，如果没要求。

10. 点击**精选**单选按钮按顺序选择网络连接设备的**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。点击**添加**为了搬入指定的网络被监控的网络字段。如果有需要选择更多网络，请重复早先步骤。



注意： 这是可用的可选功能，并且可以被跳过，如果没要求。

11. 重复每个虚拟传感器的第**8步**至第**10步**。
12. 点击**提交**为了保存您的更改。设备名出现在安全和监控信息列表下。提交操作记录在数据库表上的变化。但是，它不装载更改到MARS工具的工作内存。激活操作负荷提交了更改到工作内存。
13. 点击**激活**为了enable (event) MARS开始sessionize从此设备的事件。MARS开始sessionize此模块生成的事件和评估那些事件使用被定义的检查和下降规则。设备发布的任何事件对MARS，在启动可以查询用设备的报告的IP地址作为匹配标准前。请参见激活报告和缓解设备。关于激活动作的更多信息。

验证MARS拉从Cisco 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Cisco IPS设备和MARS之间的数据流：

1. 在Cisco IPS设备、enable (event)和戒备在签名2000年和2004年。签名监控程序ICMP消息(ping)。
2. 连接在Cisco IPS设备监听的子网的一个设备。事件是由MARS生成的并且拉。
3. 验证事件出现于MARS Web接口。您可用Cisco IPS设备执行查询。
4. 一旦数据流被验证，您能禁用在Cisco IPS设备的2000年和2004个签名。**注意：** 如果测试连接操作不在Cisco IPS设备的配置时失效MARS Web接口，则通信是启用的。此任务允许您进一步验证戒备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