

# 在 CSPM 中配置 Cisco Secure IDS 传感器

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[定义CSPM主机驻留的网络](#)

[添加CSPM主机](#)

[添加传感器设备](#)

[配置传感器](#)

[相关信息](#)

## 简介

本文解释使用的步骤配置Cisco Secure Policy Manager Cisco安全入侵监测系统(IDS)传感器。本文假设，您安装在您的计算机的CSPM版本2.3.1。版本“我”允许IDS设备(设备传感器、Cisco IOS路由器或者IDS前端)的管理在思科Catalyst<sup>®</sup> 6000交换机。本文也假设，IDS postoffice参数正确地定义。这些包括HOSTID、ORGID、主机名和ORGNAME。请注意:为了CSPM主机能通信与传感器，ORGID和ORGNAME必须匹配什么在传感器定义。

## 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CSPM 2.3.1和以后。

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。

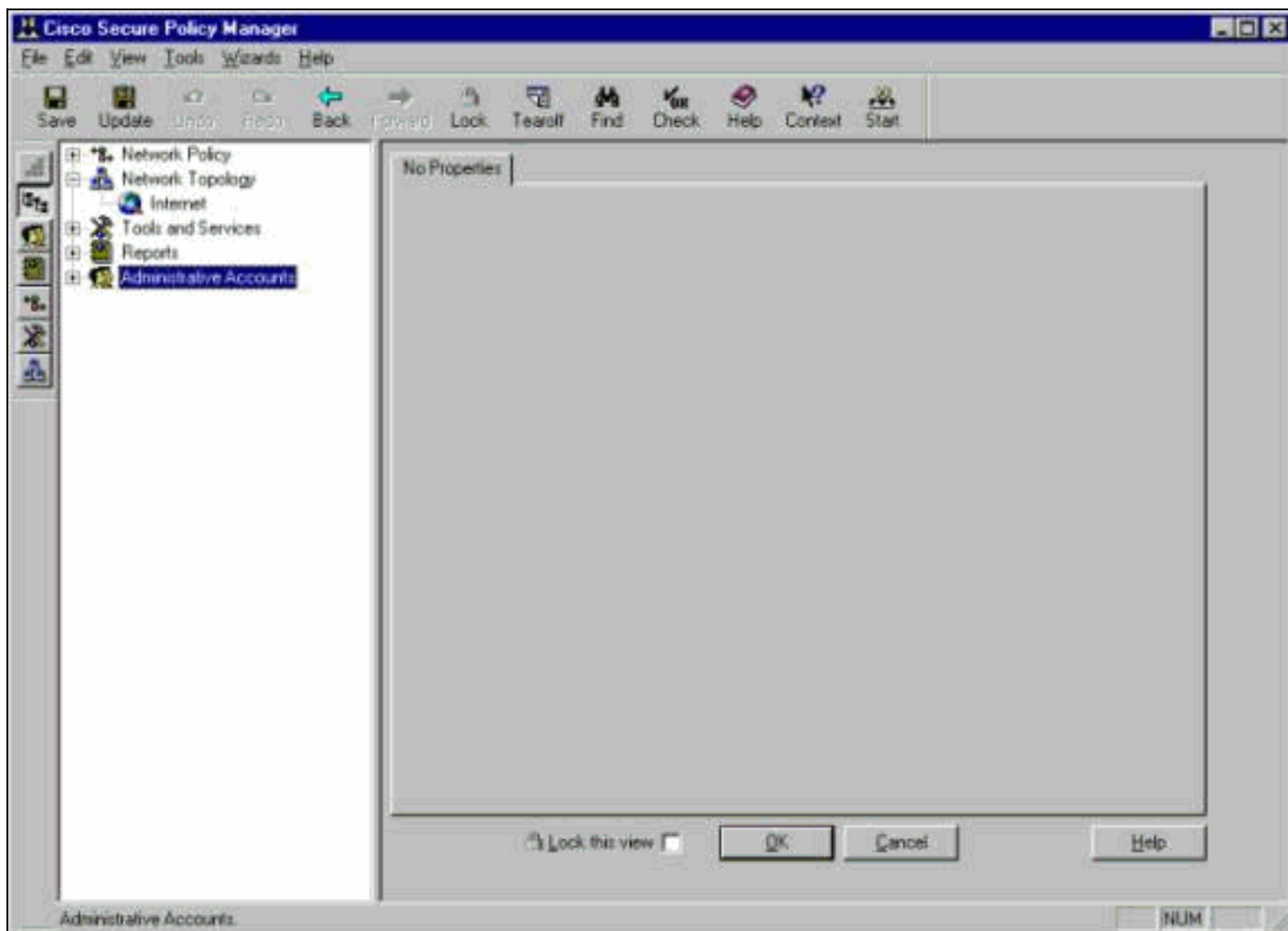
### 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 配置

这些部分说明用于的进程配置在CSPM的IDS传感器。

启动CSPM和登录。允许您定义您的网络的一个空白的模板出现(初始运行)。



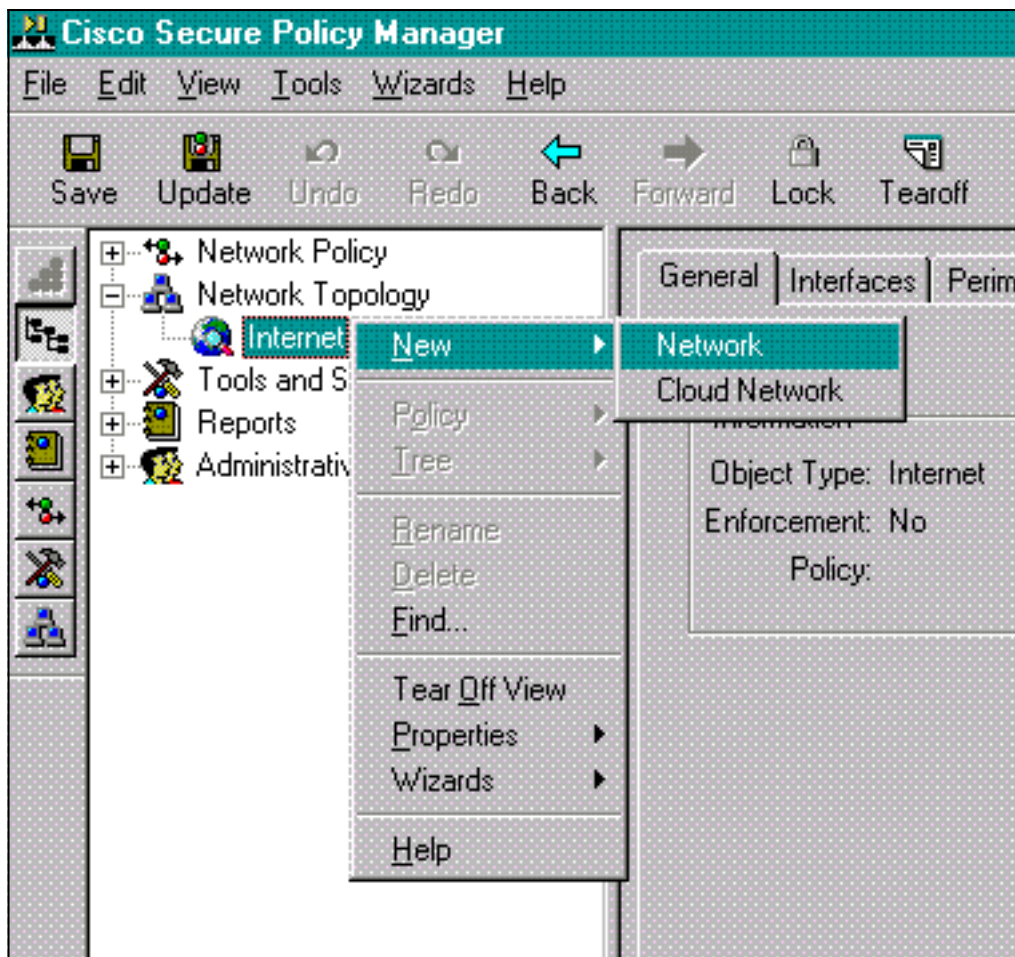
这三个定义在IDS的CSPM拓扑里要求。

1. 定义传感器控制接口位于的网络和CSPM主机驻留的网络。如果他们在相同子网，则仅一网络需要定义。定义此网络第一。
2. 定义在其网络的CSPM主机。没有CSPM主机定义，传感器不可能管理。
3. 定义在其网络的传感器。

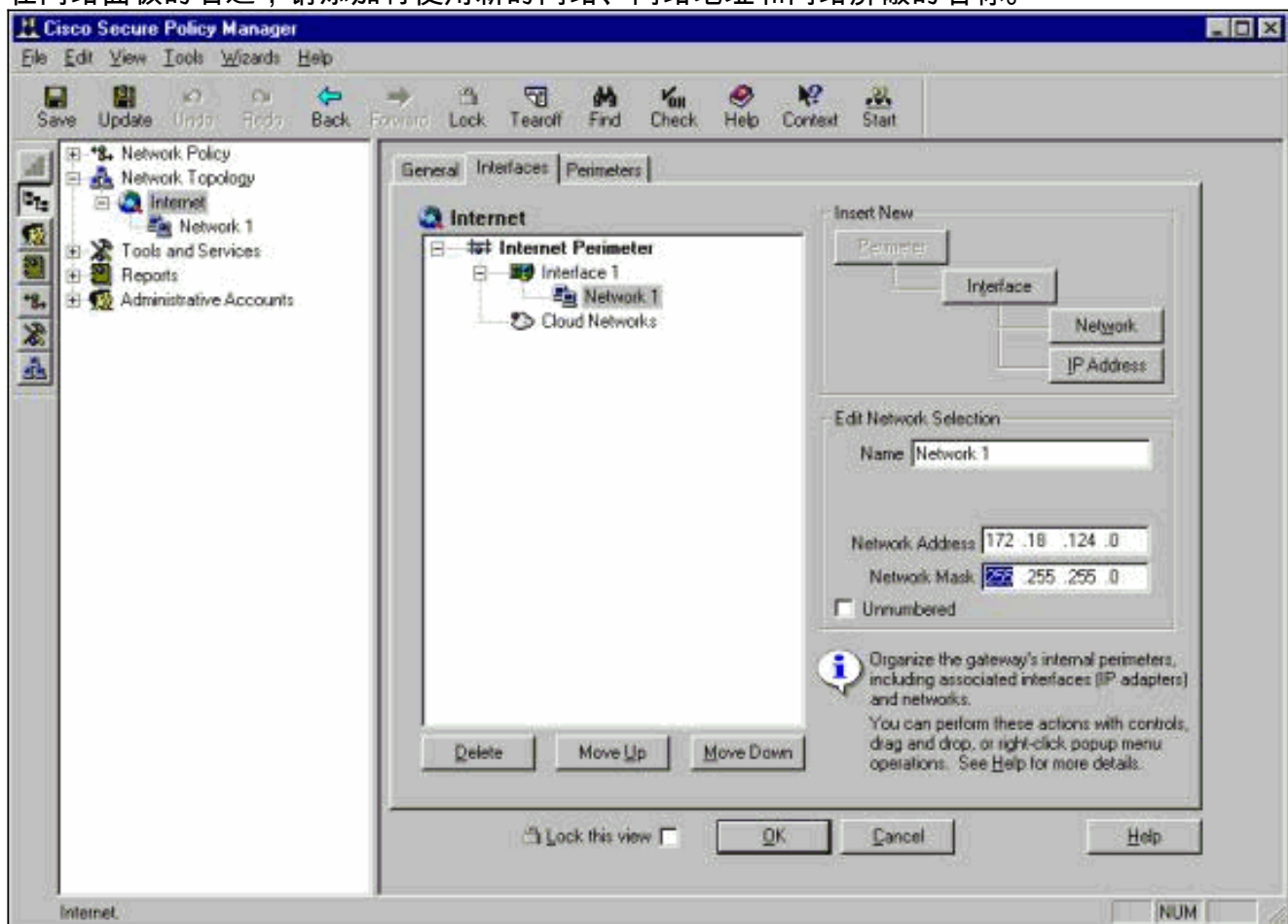
## 定义CSPM主机驻留的网络

完成这些步骤：

1. 用鼠标右键单击在Internet图标在拓扑里并且选择New > Network创建新的网络。



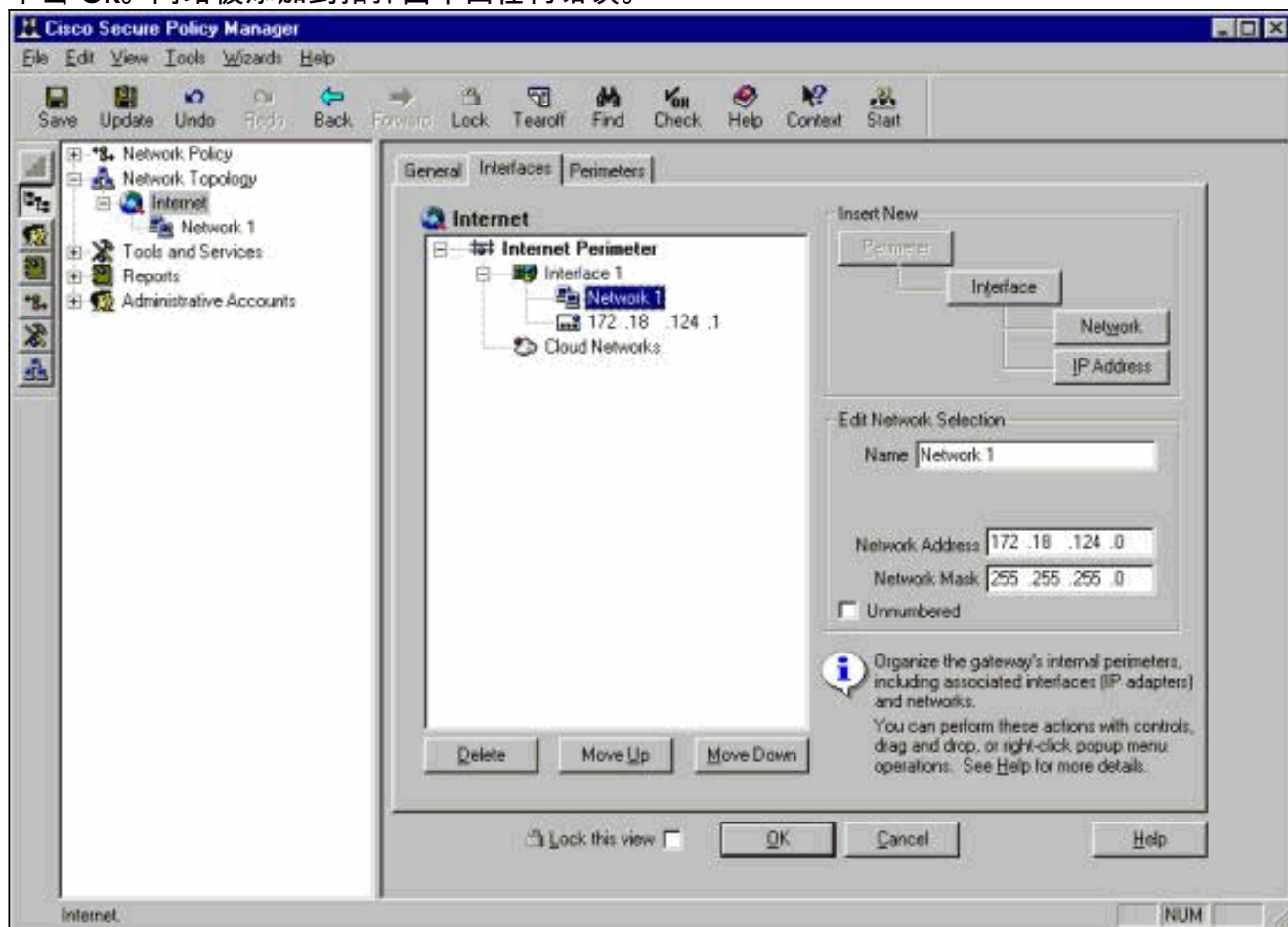
2. 在网络面板的右边，请添加将使用新的网络、网络地址和网络屏蔽的名称。



3. 点击IP Address按钮，并且输入使用到达互联网的您的网络的IP地址。通常它是网络的默认网关。**注意：**当您管理传感器时，网关地址不一定必须正确，因为传感器没有发送此默认网关

信息。在传感器应该已经定义它。

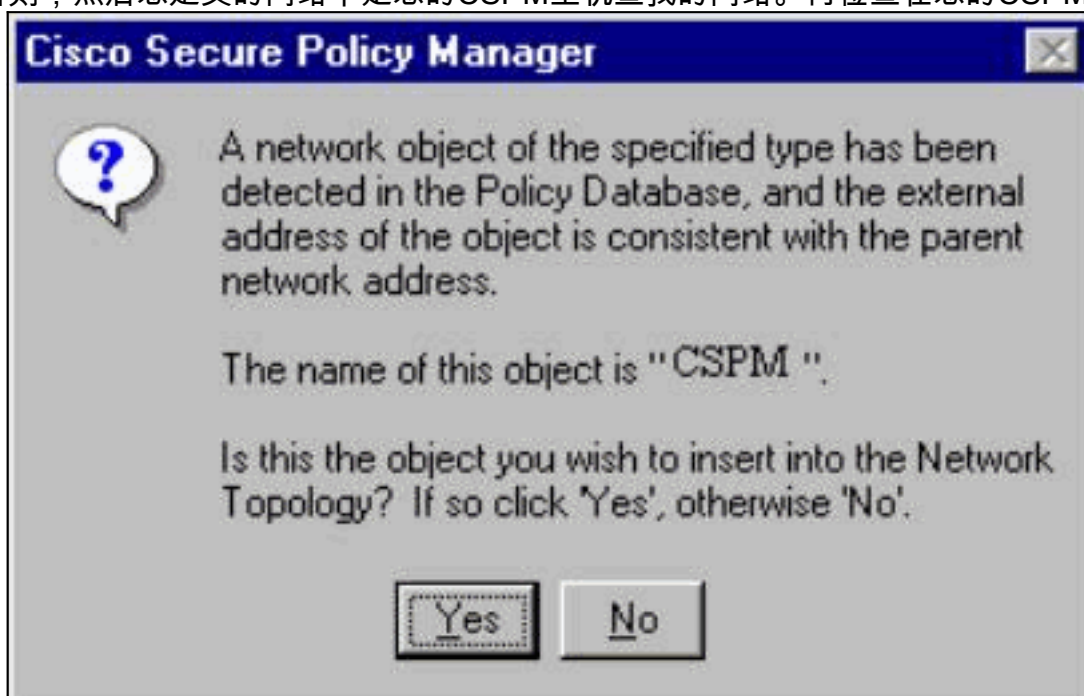
4. 单击 **Ok**。网络被添加到拓扑图不出任何错误。



## 添加CSPM主机

请使用此步骤添加CSPM主机。

1. 在网络拓扑里，请用鼠标右键单击在您添加的网络并且选择**New > Host**。CSPM启动屏幕类似于此。否则，然后您定义的网络不是您的CSPM主机查找的网络。再检查在您的CSPM主机的



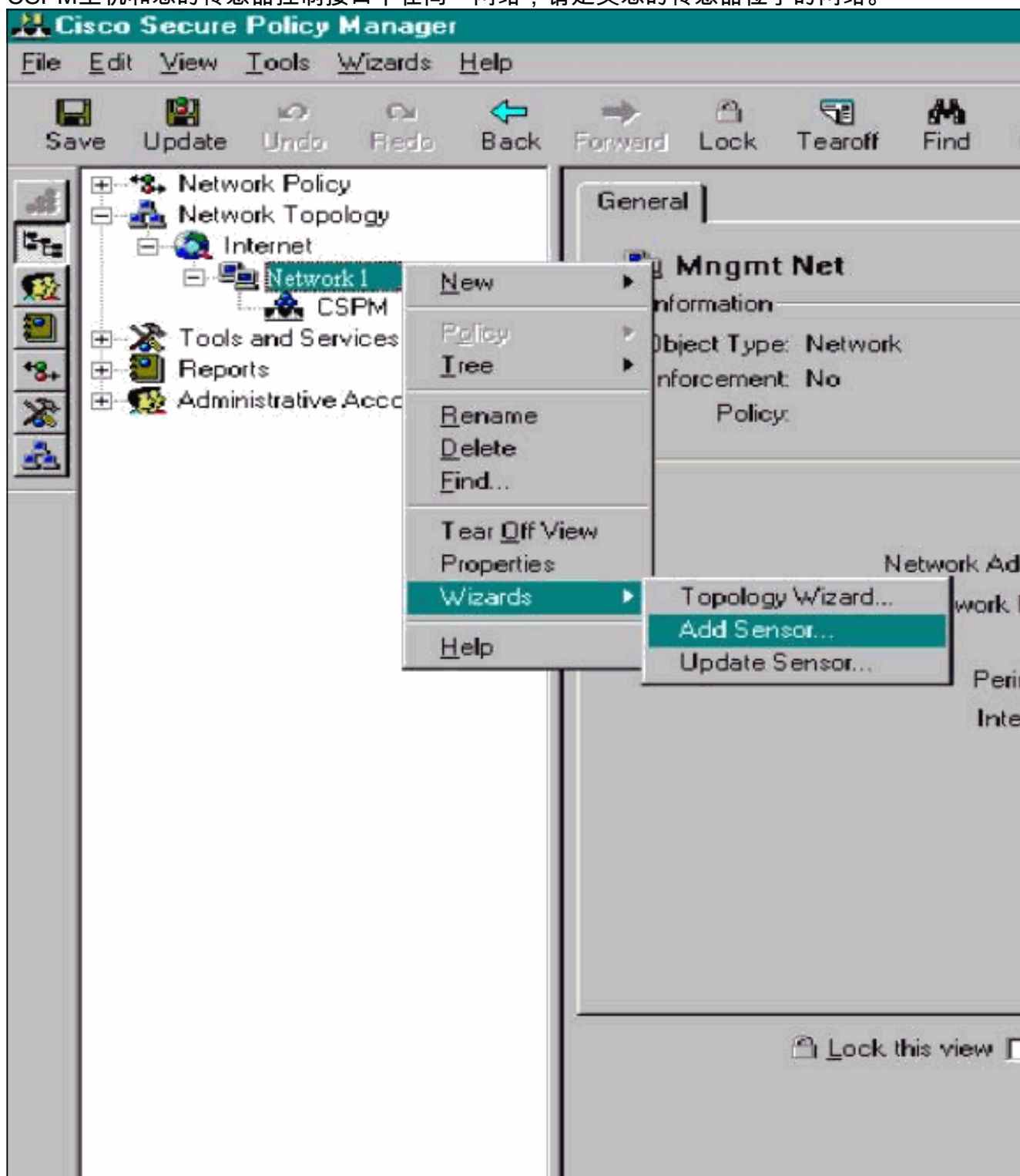
IP地址。

2. 点击是安装CSPM主机到拓扑。
3. 验证关于General屏幕的信息CSPM主机的是好的。
4. 点击OK键在CSPM主机的General屏幕的。

## 添加传感器设备

请使用此步骤添加传感器设备。

1. 用鼠标右键单击在您的传感器位于的网络并且选择Wizards > Add Sensor。注意：如果CSPM主机和您的传感器控制接口不在同一网络，请定义您的传感器位于的网络。



2. 输入传感器的正确postoffice参数。



**Add Sensor Wizard**

**Sensor Identification**

Welcome to the Add Sensor Wizard. To add a Sensor to the topology fill in the following information and press Next.

Sensor Identification

Sensor Name  Host ID  Org. ID

Organization Name

IP Address

Postoffice Heartbeat Interval

Policy Enforcement


Associated Network Service

Port

Comments

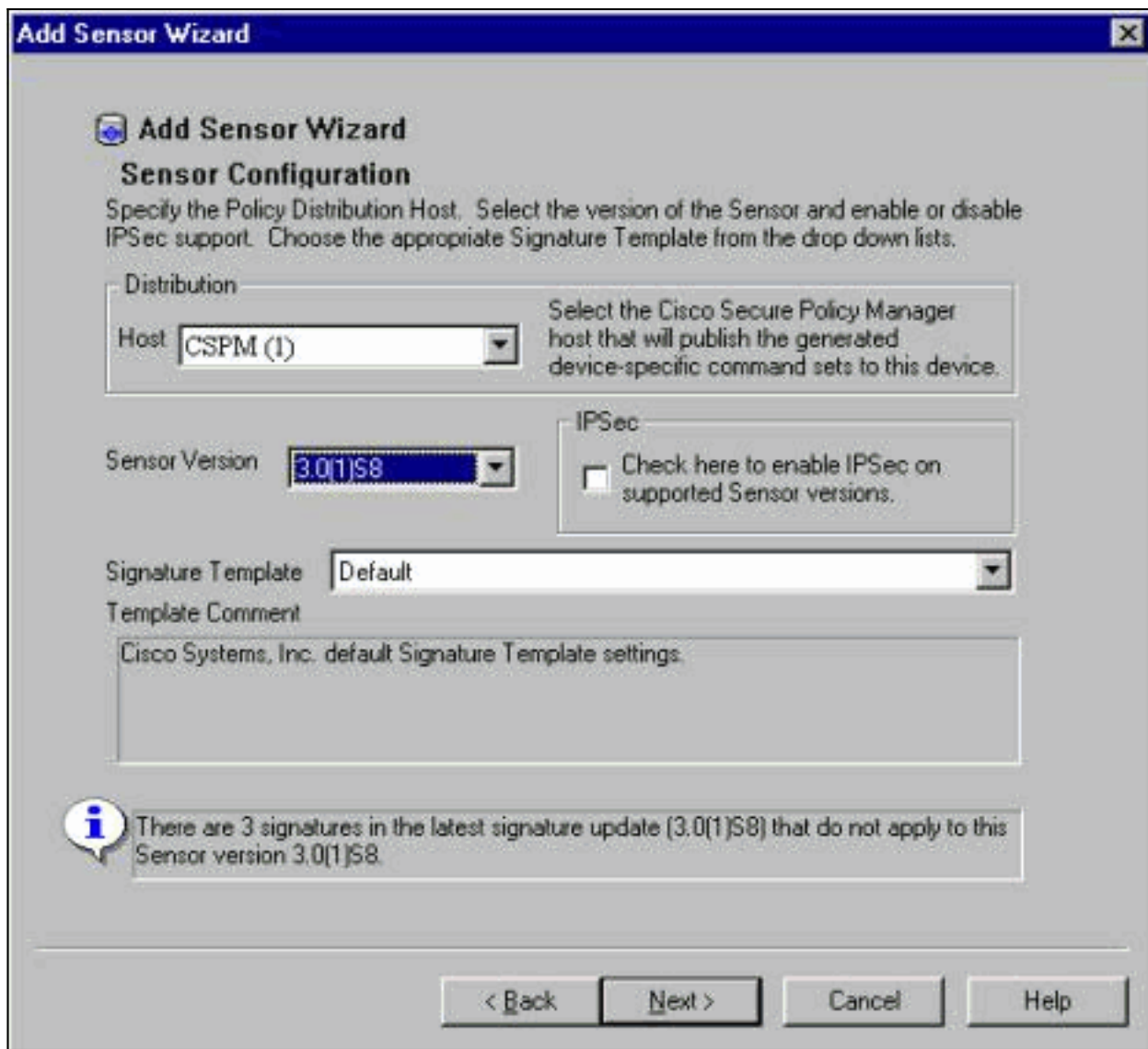
Check here to verify the Sensor's address.

Check here to capture the Sensor's configuration.

 Enter the IP Address and the Host ID will populate automatically. Or you may enter it manually.

< Back   Next >   Cancel   Help

3. 点击此处**检查验证传感器的地址框**。**注意**：如果这第一次是您设置此传感器，您不要捕获传感器的配置。如果通过UNIX向导或另一台CSPM主机在别处以前配置此传感器和做了对传感器签名的配置更改，则您要捕获传感器的配置。
4. 单击在**旁边**定义了传感器的签名版本。您在传感器能也发出**nrvers**命令检查此。



注意

：如果CSPM没有正确传感器版本您在您的传感器运作，请更新在您的CSPM主机的签名。请参阅[软件下载\(仅限注册用户\)](#)关于更新。

5. 单击“Next”按钮继续。
6. 点击**芬通社**完成传感器的安装到拓扑。
7. 从主要CSPM菜单，请选择**File > Save and Update**编译在拓扑里输入的信息到CSPM。请注意：此步骤是必要启动邮政协议CSPM主机。
8. 验证一切工作在登录您的传感器旁边作为netrangr用户。

9. 执行**nrconns**命令。>**nrconns** Connection Status for gacy.rtp cspm.rtp Connection 1:

```
172.18.124.106 45000 1 [Established] sto:0004 with Version 1 netrangr@gacy:/usr/nr > 注意
```

：如果传感器和CSPM主机不通信，输出类似于此出现：netrangr@gacy:/usr/nr

```
>nrconns Connection Status for gacy.rtp insane.rtp Connection 1: 172.18.124.194 45000 1
```

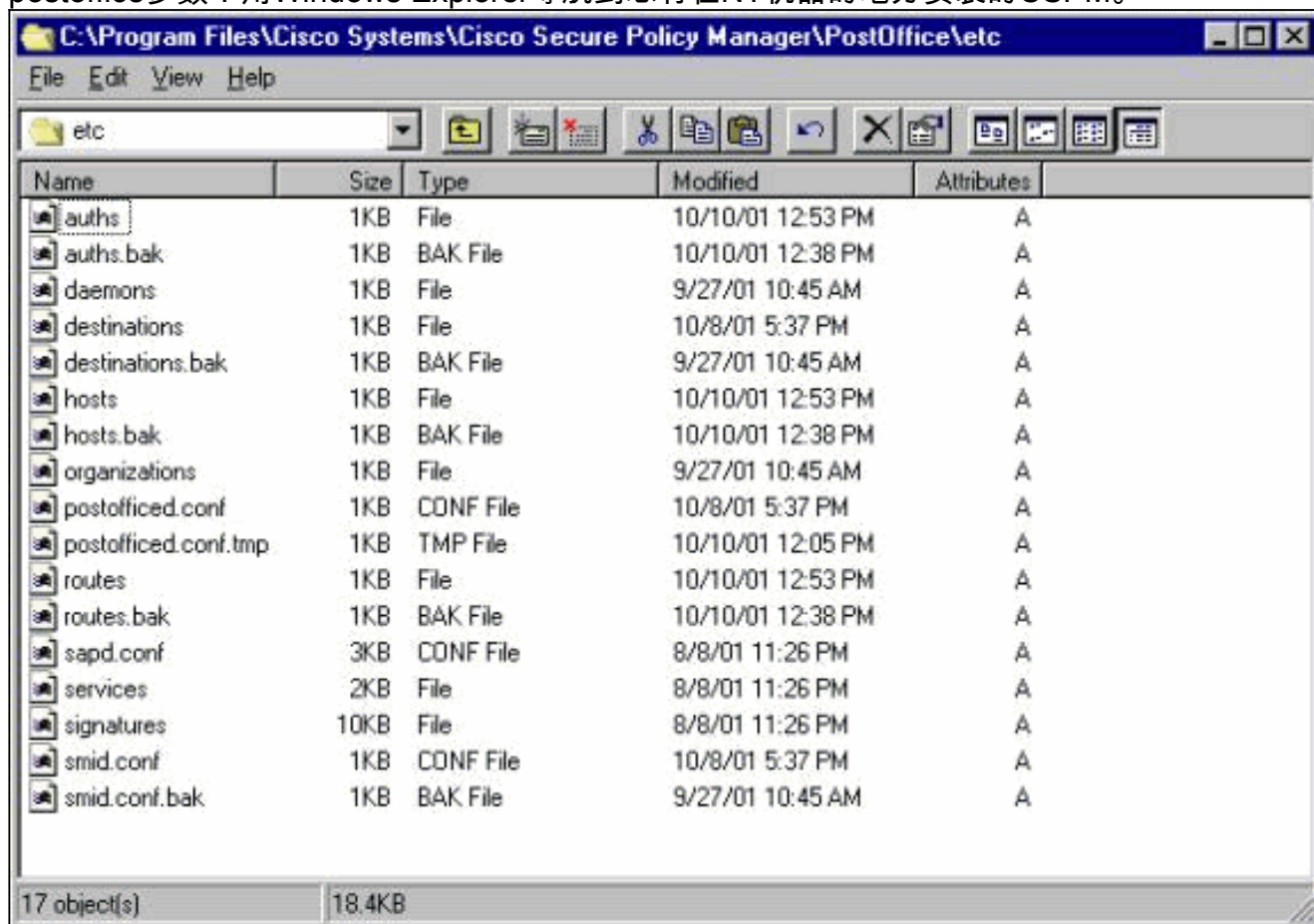
```
[SynSent] sto:5000 syn NOT rcvd! netrangr@gacy:/usr/nr
```

如果这是实际情形，请获得嗅探器跟踪发现两边是否发送UDP 45000数据包。UDP 45000是什么IDS设备使用彼此连通。测试此在传感器，**su**根源和(根据什么传感器您有)执行**监听- d iprb1端口45000** (IDS 4210传感器)和**监听- d iprb0端口45000** (其他型号传感器)。请使用<control-c>发生监听会话。如果没有传感器和CSPM之间的通信此输出出现：netrangr@gacy:/usr/nr

```
>su - Password: Sun Microsystems Inc. SunOS 5.8 Generic February 2000 # snoop -d spwr0 port 45000 Using device /dev/spwr (promiscuous mode) 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 ->
```

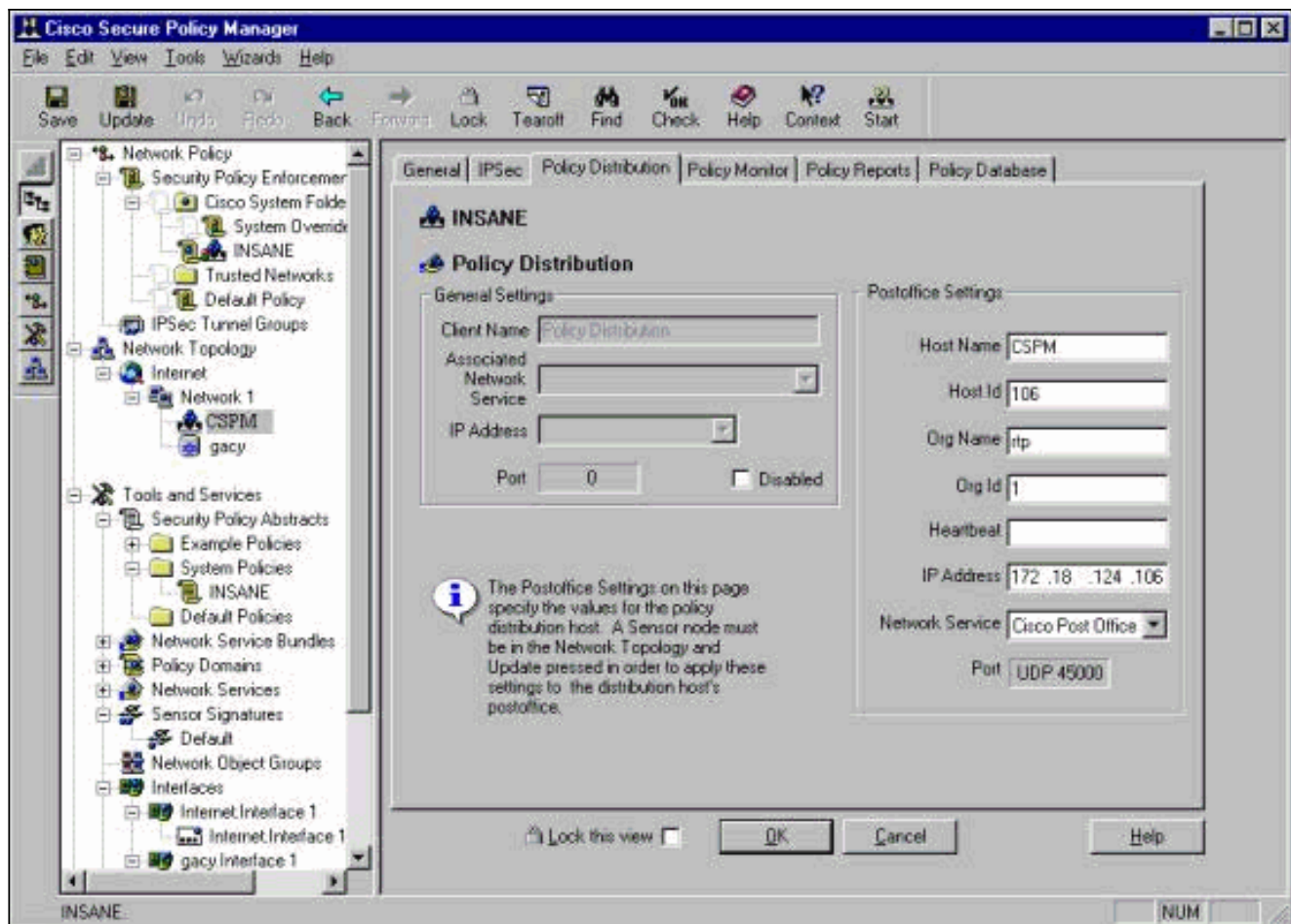
在上述输出中，传感器发送UDP 45000数据包

，但是不接收其中任一。一正确配置生成输出类似于此：`# snoop -d spwr0 port 45000 Using device /dev/iprb (promiscuous mode) 172.18.124.106 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56 172.18.124.142 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56`在上述输出中，UDP 45000流量在两个方向进。如果UDP 45000在两个方向信息包流，并且nrconns输出在传感器的仍然说没有已建立连接，在传感器的postoffice参数和CSPM主机不配比。主机指南检查在CSPM的postoffice参数：用Windows Explorer导航到您有在NT机器的地方安装的CSPM。



编辑主机，路由，并且组织文件与写入或Wordpad (请勿使用Notepad，因为格式化将是损坏的)。保证这些文件为您的安装看起来正确。如果其中任一个值不正确，使用这些步骤，请编辑他们并且重新启动您的NT计算机：在网络拓扑里点击**CSPM图标**。点击Policy Distribution选项输入您的postoffice参数。**保存并且更新您的更改**。重新启动NT计算机。





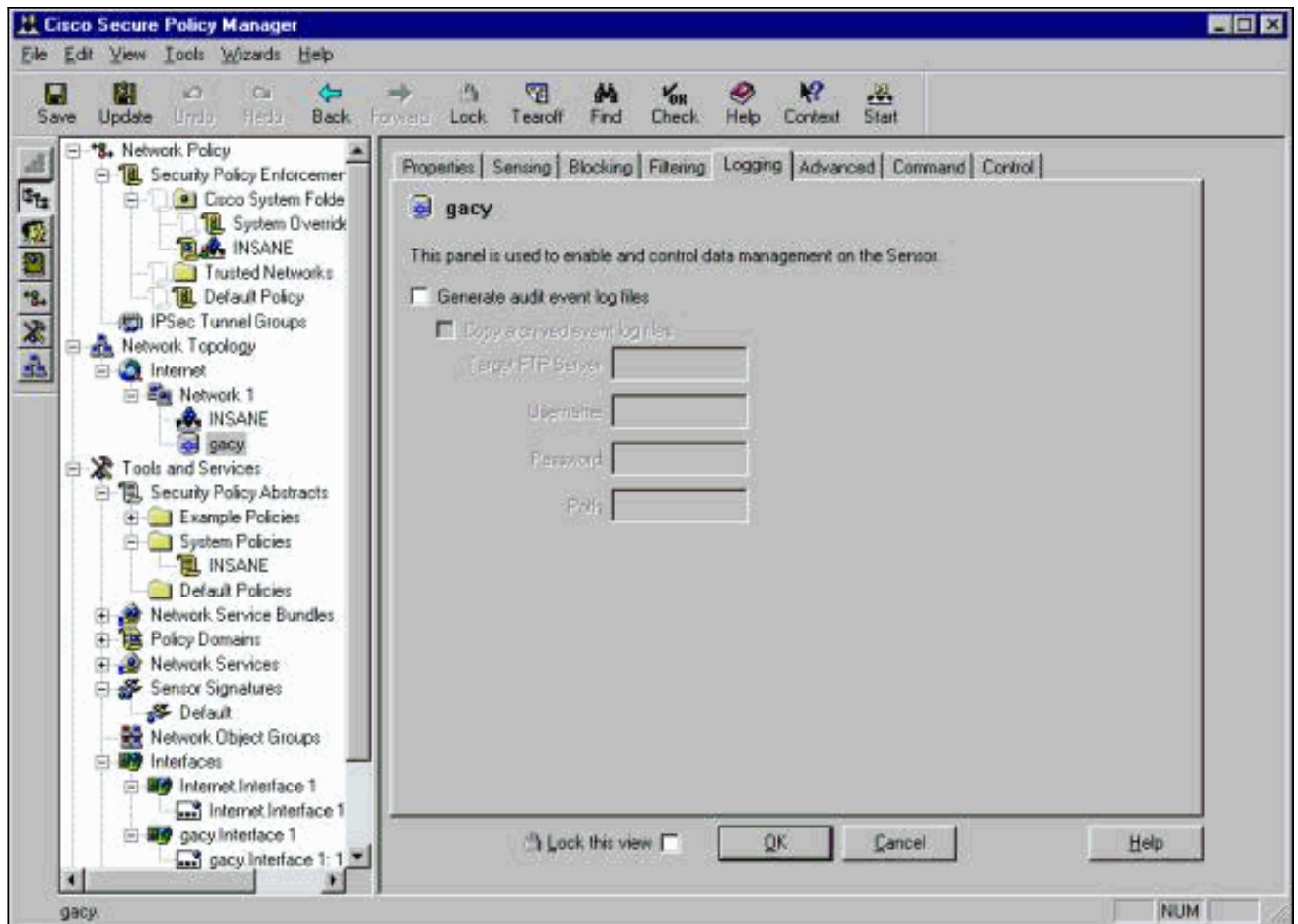
## 配置传感器

在配置在CSPM后保存，请配置传感器。为了执行此，第一组传感器写入看到对其自己的日志的报警。然后请设置传感器“探测”在正确接口。

## 写入报警对日志

使用此步骤写入报警到日志。

1. 点击生成审计事件日志文件方框告诉传感器发送报警到其本地日志。在您增加配置对它后，它也发送报警到默认情况下CSPM方框。

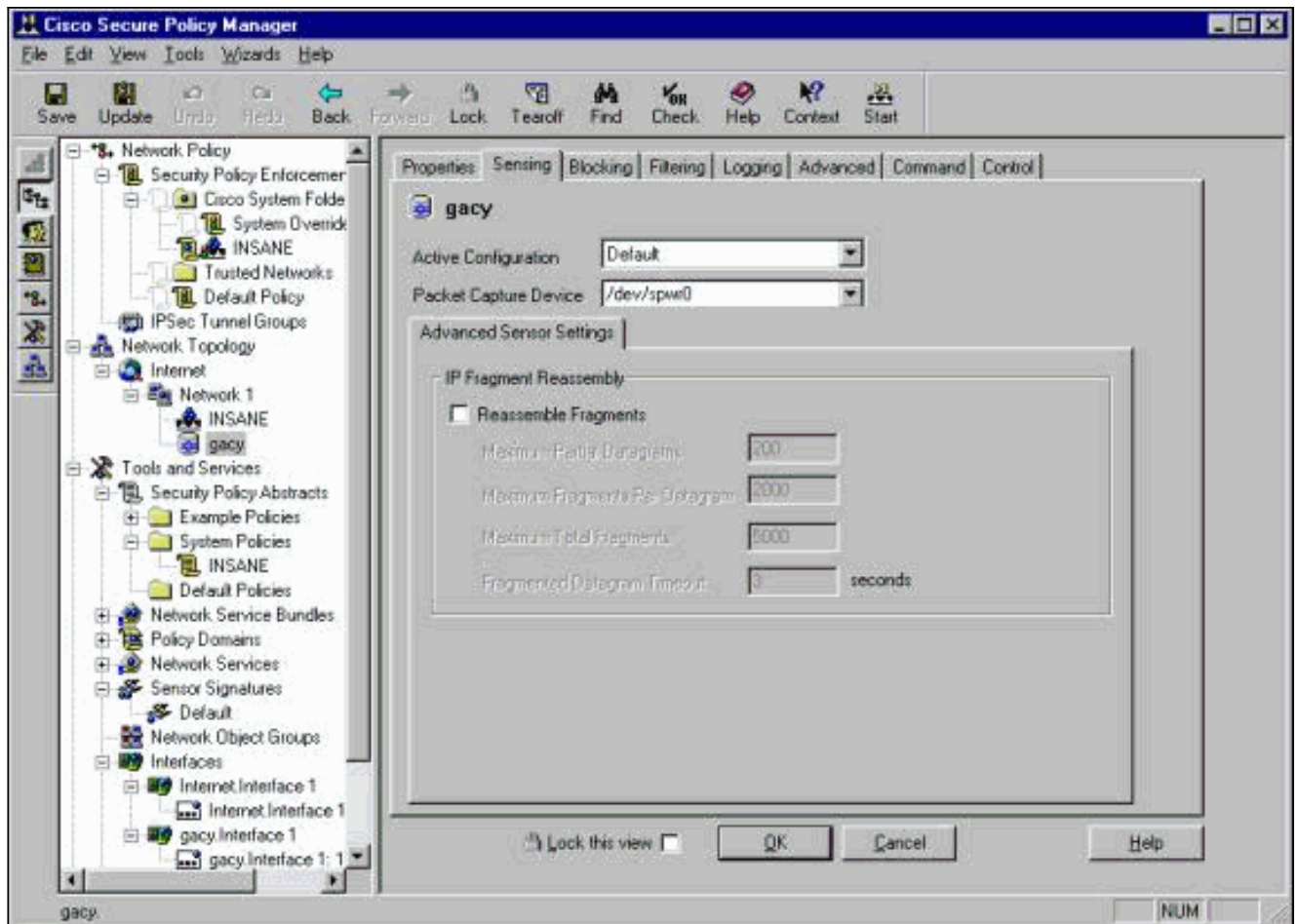


2. 单击 OK 继续。

## 设置传感器“探测”

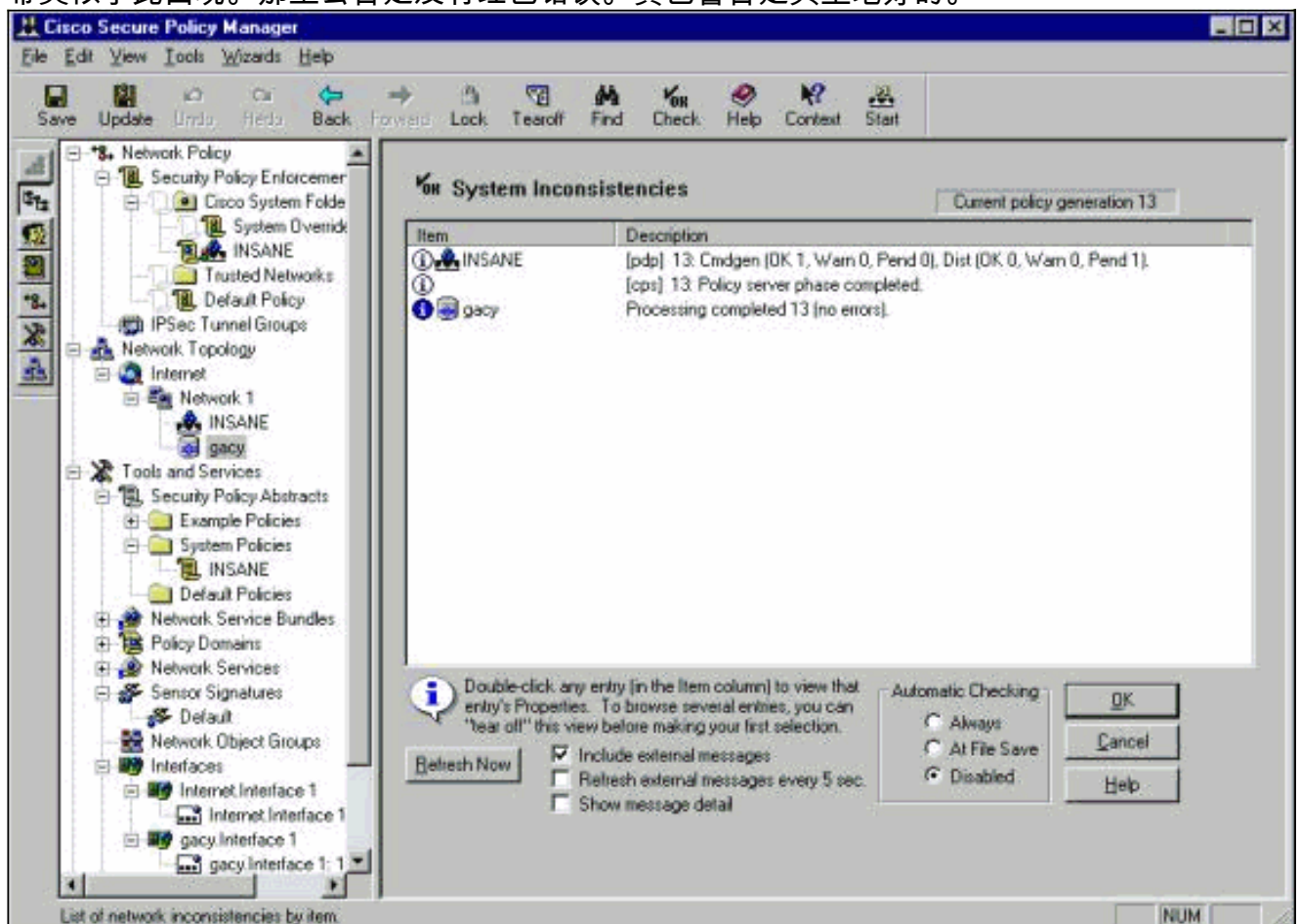
使用此步骤设置传感器“探测”。

1. 在您的CSPM拓扑方面选择传感器并且点击Sensing选项。
2. 定义信息包获取设备：iprb0 - IDS 4210传感器的spwr0 -其他传感器型号的



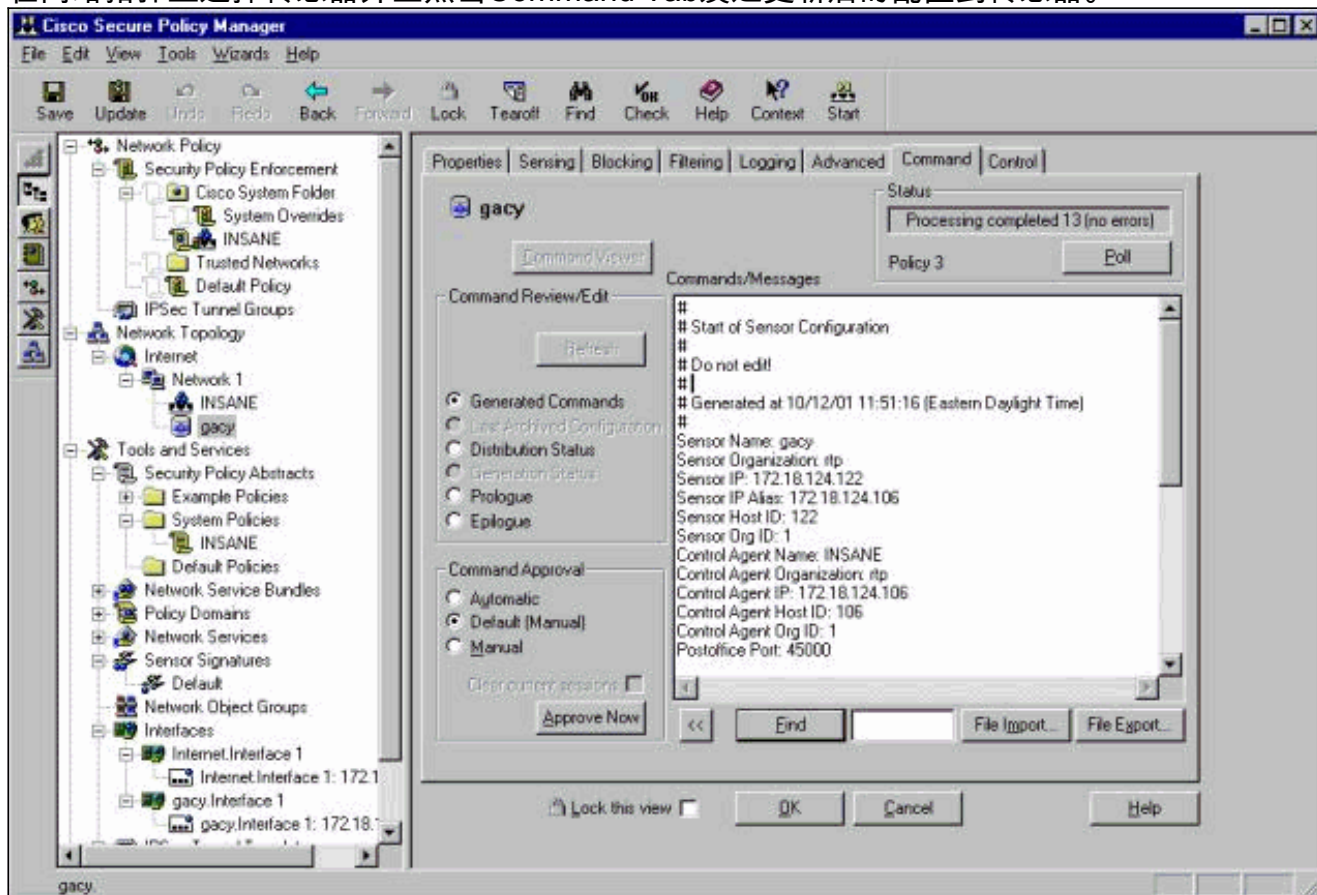
3. 单击 OK 继续。

4. 点击在CSPM菜单柱状图的Update图标更新与信息的CSPM。注意：如果一切进展顺利，屏幕类似于此出现。那里公告是没有红色错误。黄色警告是典型地好的。

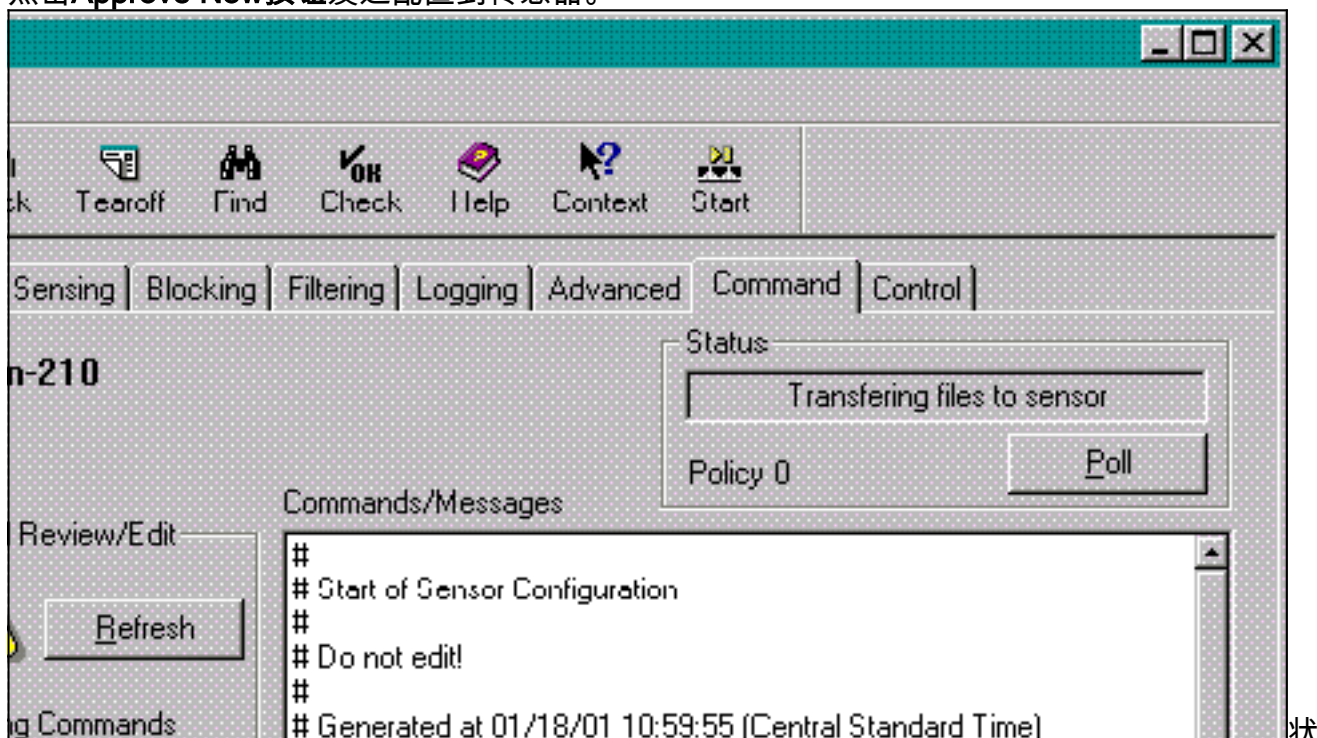




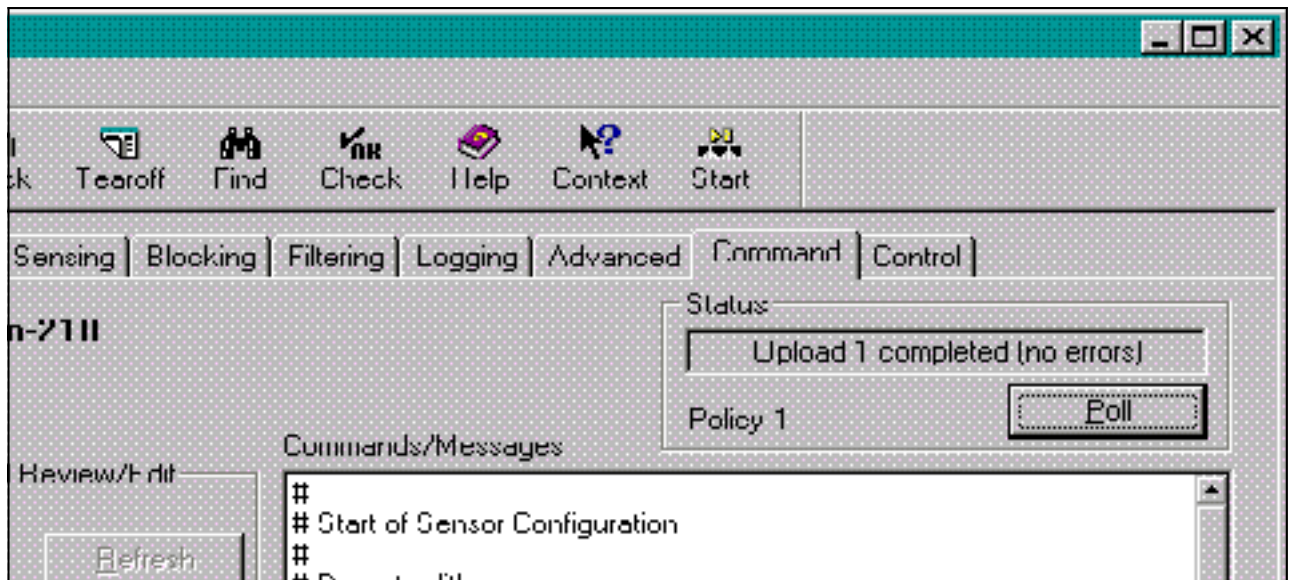
5. 在网络拓扑里选择传感器并且点击Command Tab发送更新后的配置到传感器。



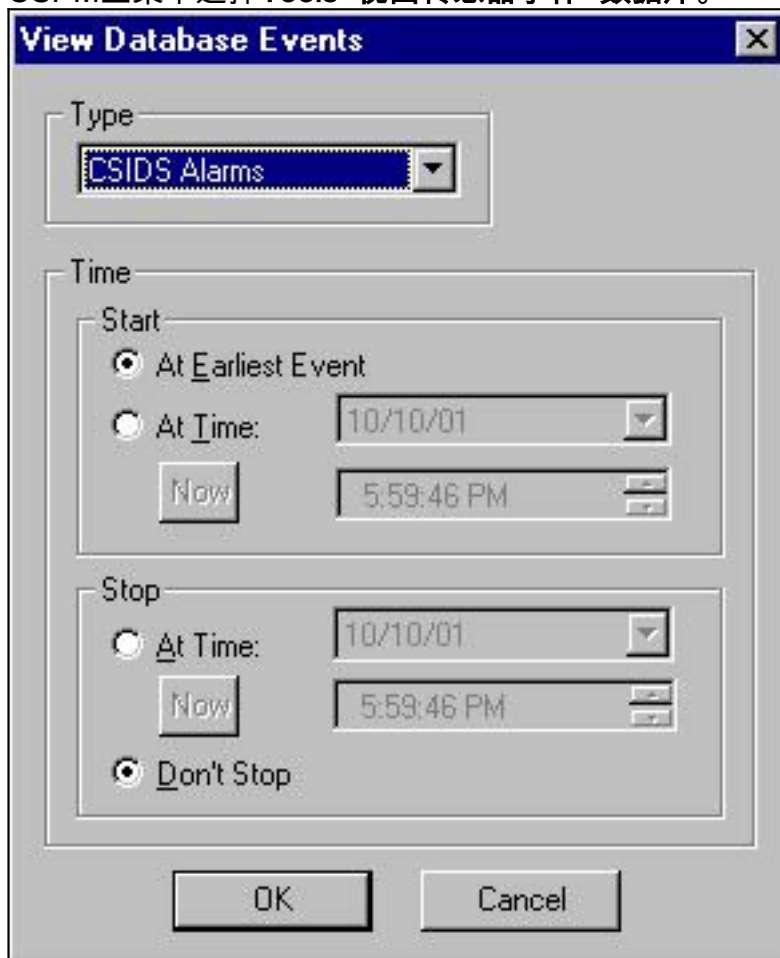
6. 点击Approve Now按钮发送配置到传感器。



状态窗格显示“加载<#>完成的”消息。这指示一有效和完整传输过程。传感器当前更新并且应该正常当前运行。如果传感器正常不运行，去上一步传感器并且检查输出nrconns命令确保，CSPM主机和传感器之间的连接被建立。



在这完成后，您能寻找传感器发送到在事件查看器的CSPM主机的报警。要查看事件查看器，从CSPM主菜单选择Tools>视图传感器事件>数据库。



点击OK键显示事件数据库窗口。您的屏幕根据您可能获得的报警将变化。



The screenshot shows a window titled "Event Viewer - Database Events - CSIDS Alarms". It contains a table with the following columns: Count, Name, Source Address, Dest Address, Details, Source Loc, Dest Loc, SubSig ID, Severity, and Org Name. The table lists various network events such as ICMP echo request, ICMP flood, ICMP smurf attack, etc.

Count	Name	Source Address	Dest Address	Details	Source Loc	Dest Loc	SubSig ID	Severity	Org Name
1134	ICMP echo request	*							
48	ICMP flood	+							
6	ICMP smurf attack	+							
6	ICMP unreachable	10.32.10.10	172.18.124.154	<none>	OUT	OUT	0	Low	rtp
40	IP fragments overlap	+							
38	Net sweep-echo	+							
4	PostOffice Initial Notification	<none>	<none>	postofficed initial notification msg	OUT	OUT	0	Low	rtp
24	Route Down!	<none>	<none>	+					
29	Route Up	<none>	<none>	+					
7	UDP Packet	+							

## 相关信息

- [技术支持和文档 - Cisco Systems](#)