配置使用IME的IPS阻拦

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[网络图](#)
[配置](#)
[开始传感器配置](#)
[添加传感器到IME](#)
[配置Cisco IOS路由器的阻塞](#)
[验证](#)
[启动攻击和阻塞](#)
[故障排除](#)
[提示](#)
[相关信息](#)

简介

本文与使用IPS管理器讨论入侵防御系统(IPS)阻塞的配置Express (IME)。IME和IPS传感器用于管理阻塞的一个Cisco路由器。当您考虑此配置时，请切记这些项目：

- 安装传感器并且适当地确保传感器工作。
- 做探测接口间距到路由器接口的外部。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IPS Manager Express 7.0
- 思科IPS传感器7.0(0.88)E3
- Cisco IOS路由器用Cisco IOS软件版本12.4

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。

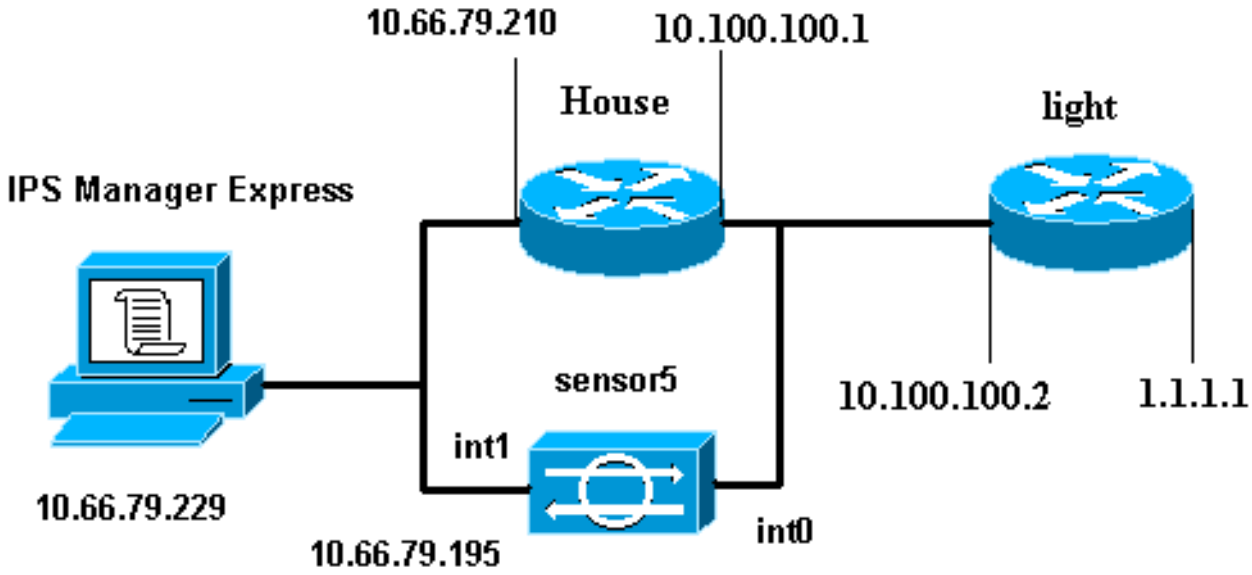
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

网络图

本文档使用此网络设置。



配置

本文档使用以下配置。

- 路由器灯
- 路由器 House

路由器灯

```
Current configuration : 906 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light ! enable password cisco ! username cisco
password 0 cisco ip subnet-zero ! ! ! ip ssh time-out
120 ip ssh authentication-retries 3 ! call rsvp-sync ! !
! fax interface-type modem mta receive maximum-
recipients 0 ! controller E1 2/0 ! ! ! interface
FastEthernet0/0 ip address 10.100.100.2 255.255.255.0
```

```
duplex auto speed auto ! interface FastEthernet0/1 ip address 1.1.1.1 255.255.255.0 duplex auto speed auto ! interface BRI4/0 no ip address shutdown interface BRI4/1 no ip address shutdown ! interface BRI4/2 no ip address shutdown ! interface BRI4/3 no ip address shutdown ! ip classless ip route 0.0.0.0 0.0.0.0 10.100.100.1 ip http server ip pim bidir-enable ! ! dial-peer cor custom ! ! line con 0 line 97 108 line aux 0 line vty 0 4 login ! end
```

路由器 House

```
Current configuration : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! logging queue-limit 100 enable password cisco ! ip subnet-zero ! ! no ip cef no ip domain lookup ! ip audit notify log ip audit po max-events 100 ! ! no voice hpi capture buffer no voice hpi capture destination ! ! ! ! interface FastEthernet0/0 ip address 10.66.79.210 255.255.255.224 duplex auto speed auto ! interface FastEthernet0/1 ip address 10.100.100.1 255.255.255.0 ip access-group IDS_FastEthernet0/1_in_0 in !--- After you configure blocking, !--- IDS Sensor inserts this line. duplex auto speed auto ! interface ATM1/0 no ip address shutdown no atm ilmi-keepalive ! ip classless ip route 0.0.0.0 0.0.0.0 10.66.79.193 ip route 1.1.1.0 255.255.255.0 10.100.100.2 no ip http server no ip http secure-server ! ! ip access-list extended IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any permit ip any any !--- After you configure blocking, !--- IDS Sensor inserts this line. ! call rsvp-sync ! ! mgcp profile default ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 exec-timeout 0 0 password cisco login line vty 5 15 login ! ! end
```

开始传感器配置

完成这些步骤开始传感器的配置。

1. 如果这是您第一次登录传感器，您必须在用户名和密码栏输入cisco。
2. 当系统提示您时，请更改您的密码。**注意：** Cisco123是字典词和没有允许在系统。
3. 键入**设置**并且按照系统提示符设置传感器的基本参数。
4. 输入此信息：`sensor5#setup --- System Configuration Dialog --- !--- At any point you may enter a question mark '?' for help. !--- Use ctrl-c to abort the configuration dialog at any prompt. !--- Default settings are in square brackets '[]'. Current time: Thu Oct 22 21:19:51 2009 Setup Configuration last modified: Enter host name[sensor]: Enter IP interface[10.66.79.195/24,10.66.79.193]: Modify current access list?[no]: Current access list entries: !--- permit the ip address of workstation or network with IME Permit:10.66.79.0/24 Permit: Modify system clock settings?[no]: Modify summer time settings?[no]: Use USA SummerTime Defaults?[yes]: Recurring, Date or Disable?[Recurring]: Start Month[march]: Start Week[second]: Start Day[sunday]: Start Time[02:00:00]: End Month[november]: End Week[first]: End Day[sunday]: End Time[02:00:00]: DST Zone[]: Offset[60]: Modify system timezone?[no]: Timezone[UTC]: UTC Offset[0]: Use NTP?[no]: yes NTP Server IP Address[]: Use NTP Authentication?[no]: yes NTP Key ID[]: 1 NTP Key Value[]: 8675309`
5. 保存配置。它能花费传感器的几分钟能保存配置。`[0] Go to the command prompt without`

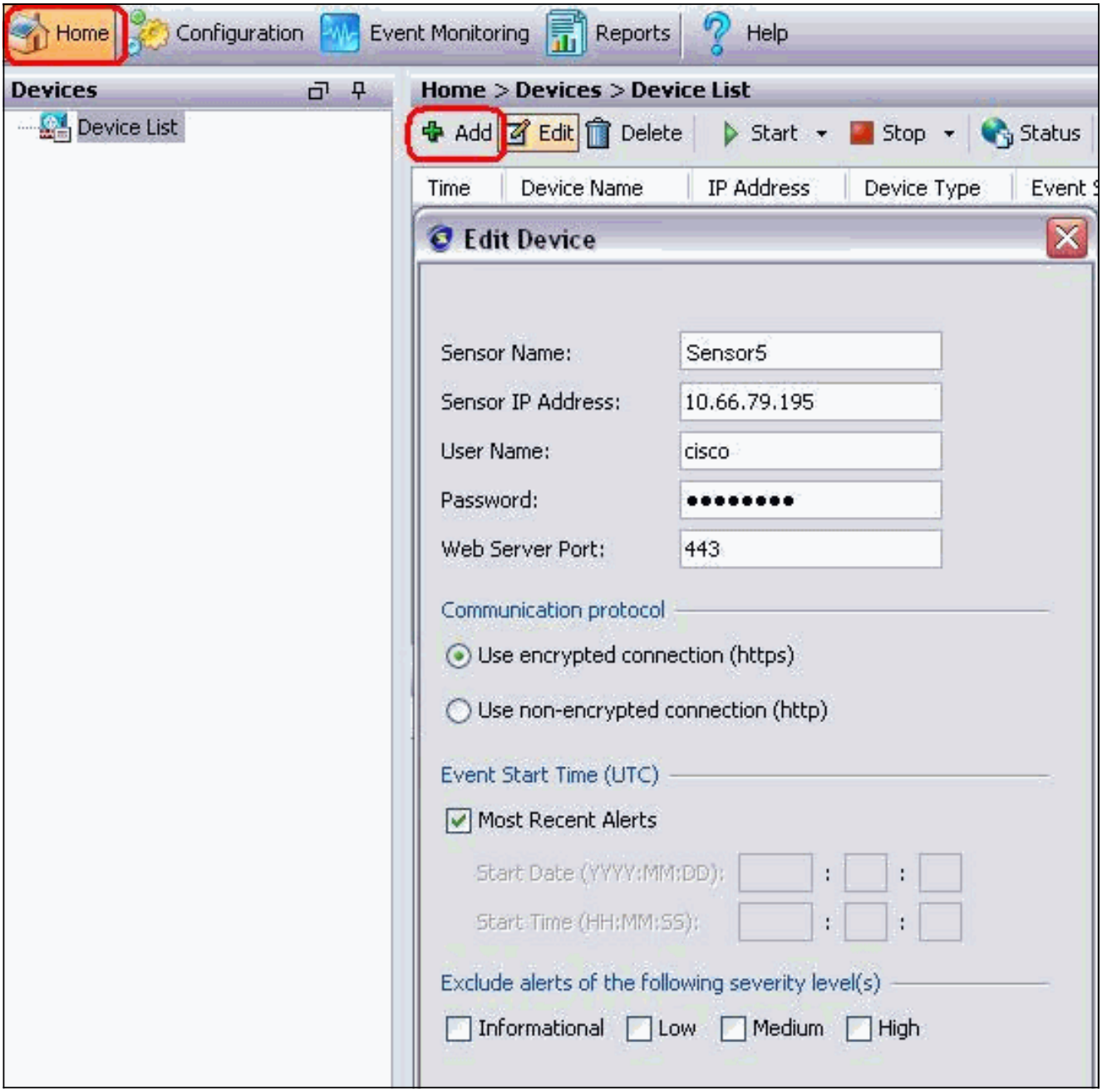
```
saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

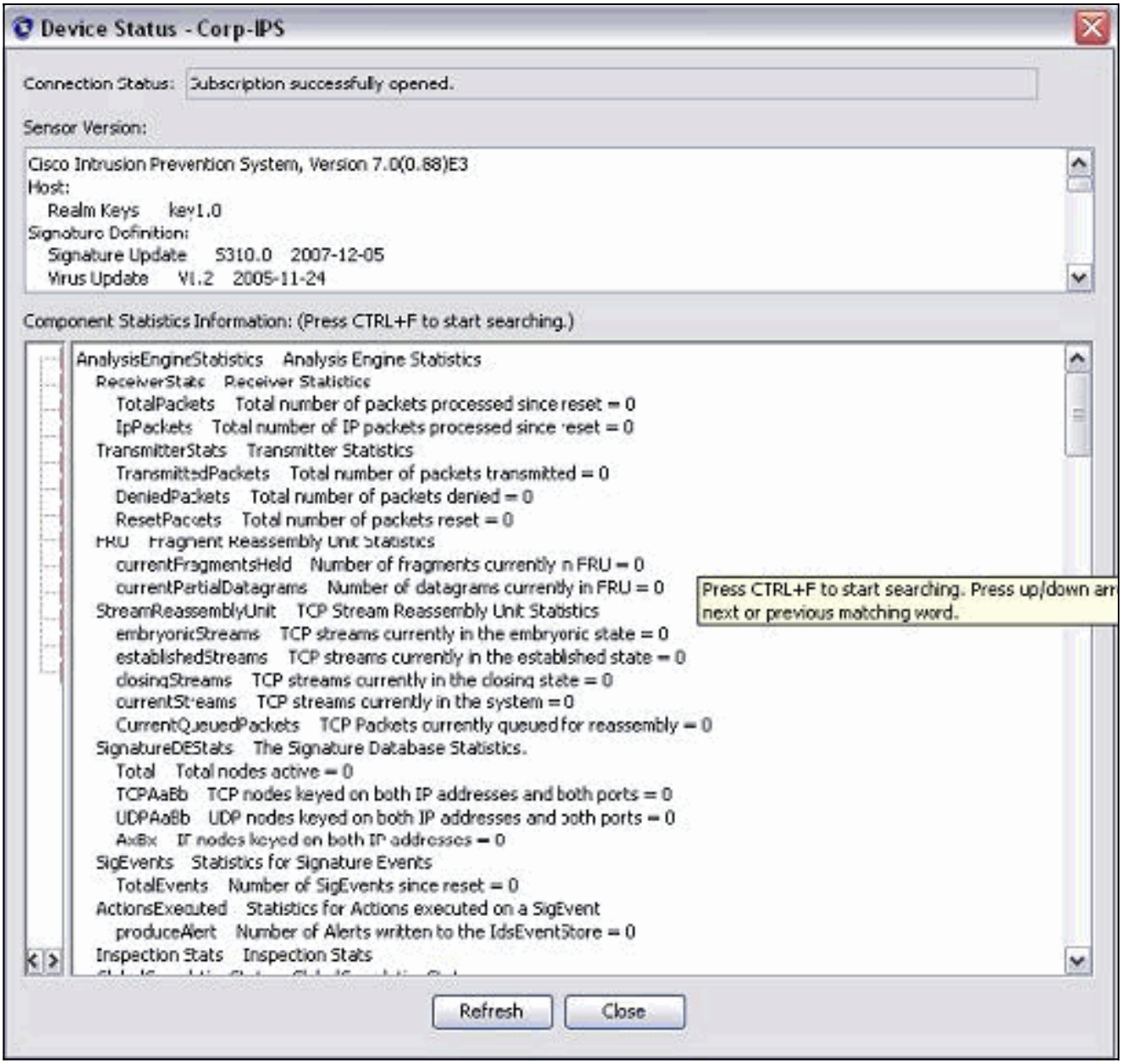
添加传感器到IME

完成这些步骤为了添加传感器到IME。

1. 去Windows PC，安装IPS管理器Express并且打开**IPS管理器Express**。
2. 选择**家庭>Add**。
3. 键入此信息并且点击OK键为了停止配置。



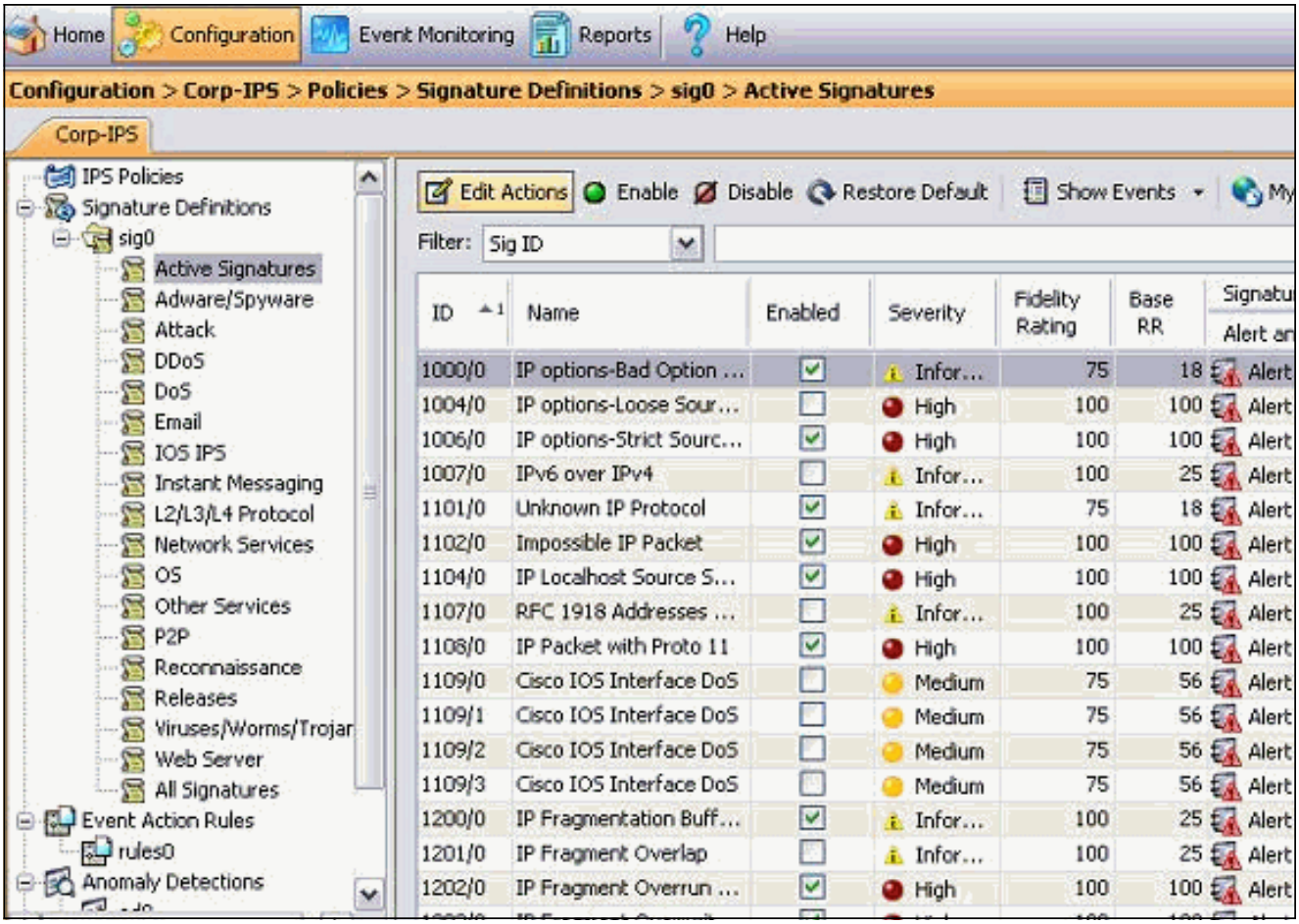
4. 选择**设备>传感器5**为了验证传感器状态然后用鼠标右键单击选择**状态**。确保您能看到*成功打开的订阅*。消息。



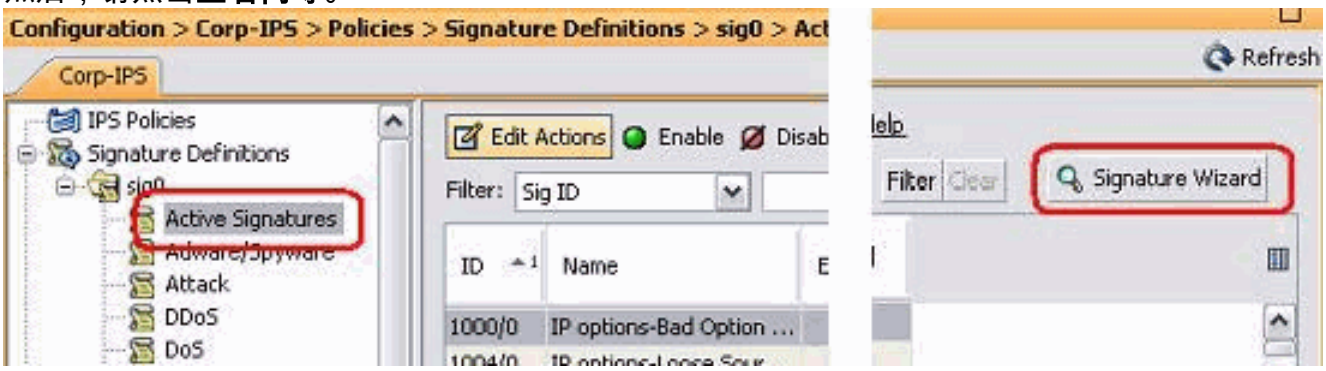
配置Cisco IOS路由器的阻塞

完成这些步骤为了配置Cisco IOS路由的阻塞：。

1. 从IME PC，请打开您的Web浏览器并且去**https://10.66.79.195**。
2. 点击OK键为了接受从传感器下载的HTTPS证书。
3. 在Login窗口中输入用户名cisco和密码123cisco123。此IME管理接口出现：

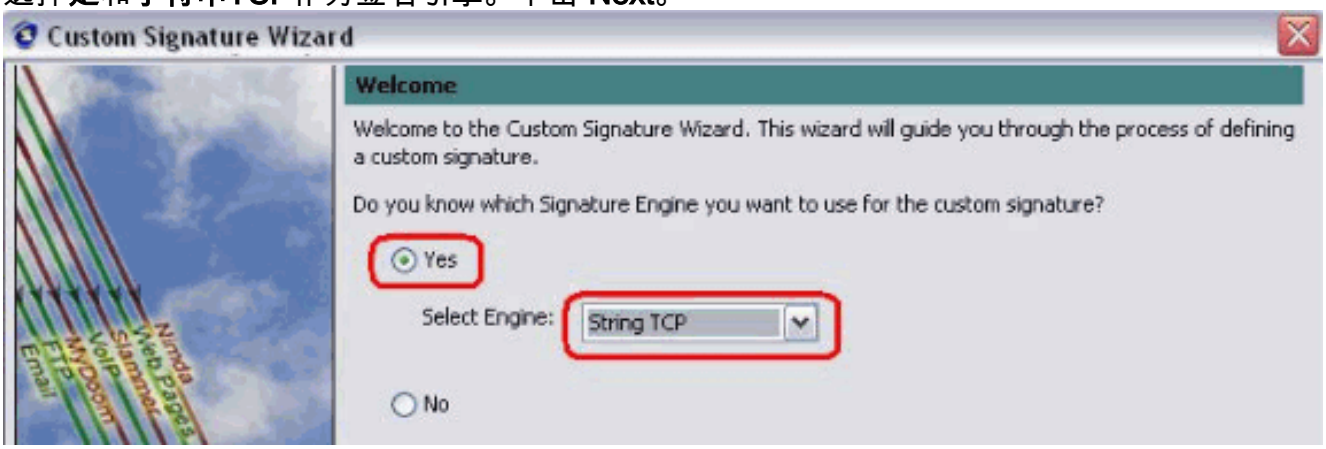


4. 从Configuration选项，请点击**活动签名**。
5. 然后，请点击**签名向导**。

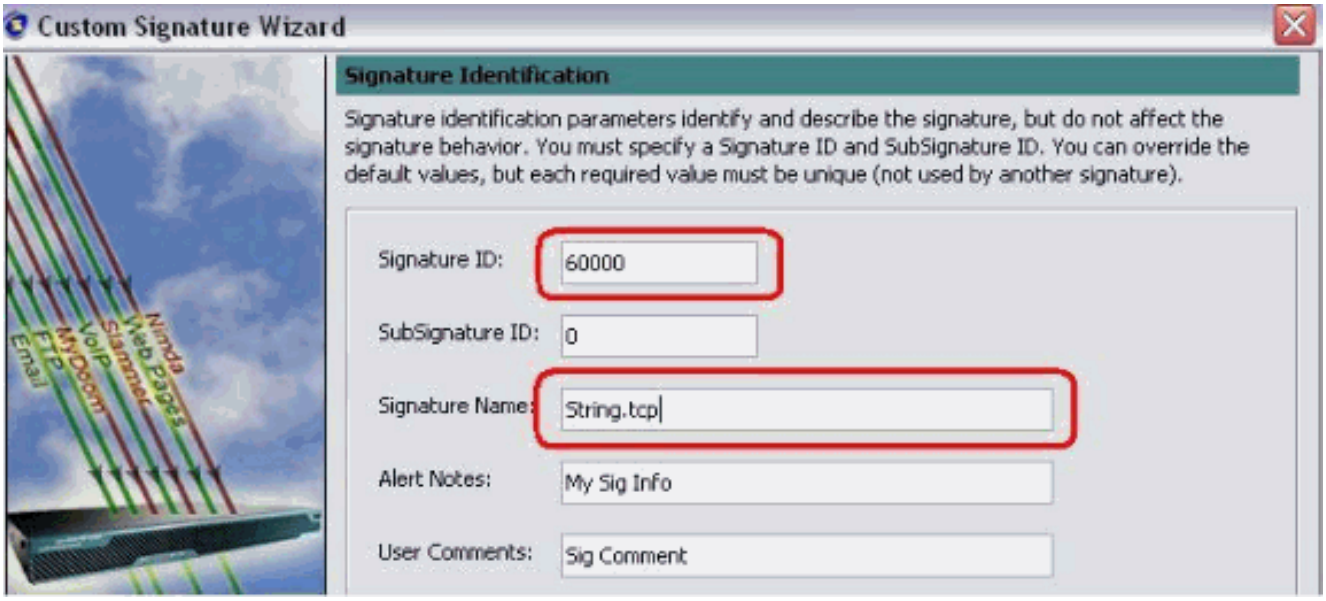


注意： 上一个屏幕画面剪切成两部分由于空间限制。

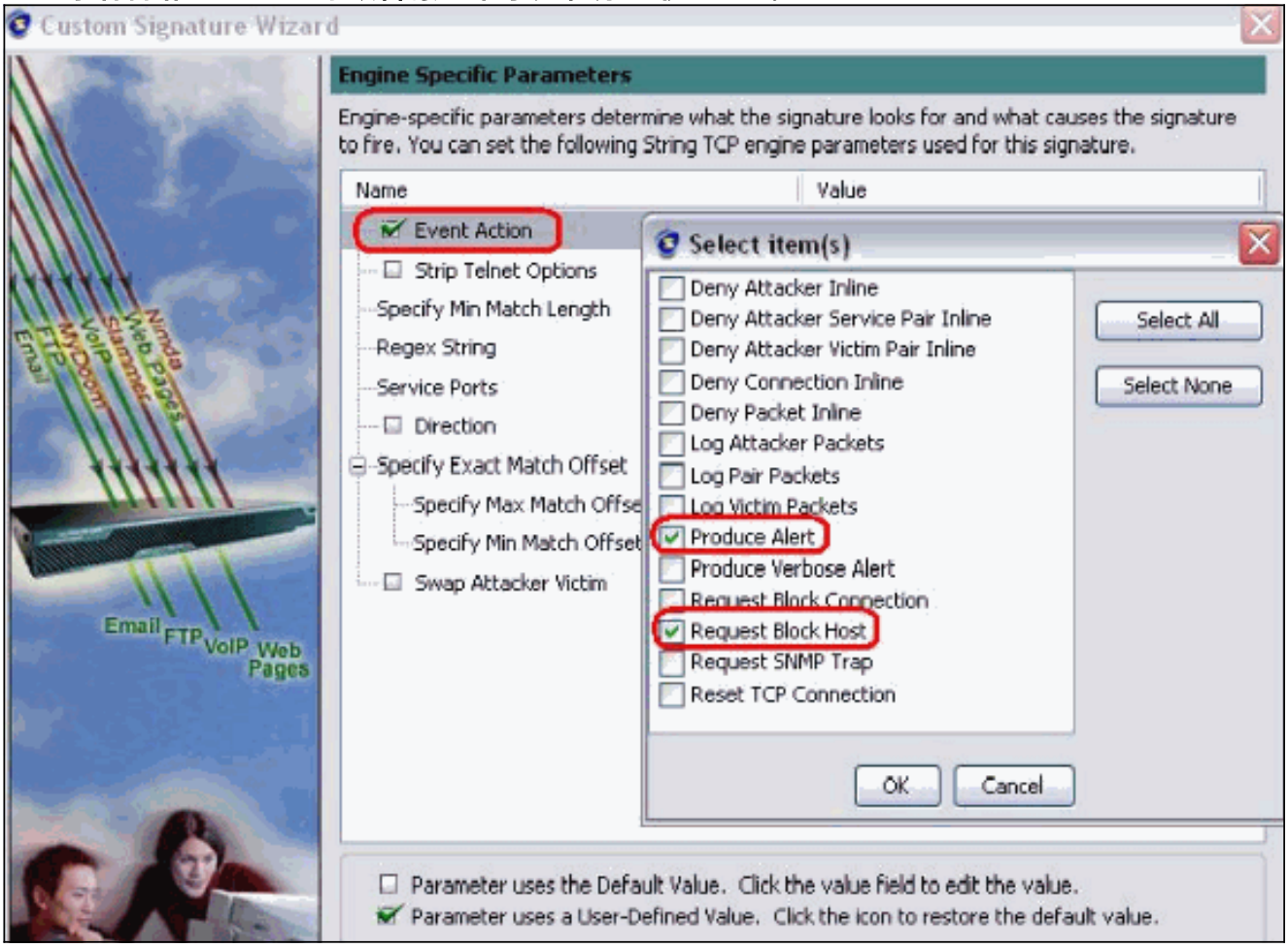
6. 选择**是**和**字符串TCP**作为签名引擎。单击 **Next**。



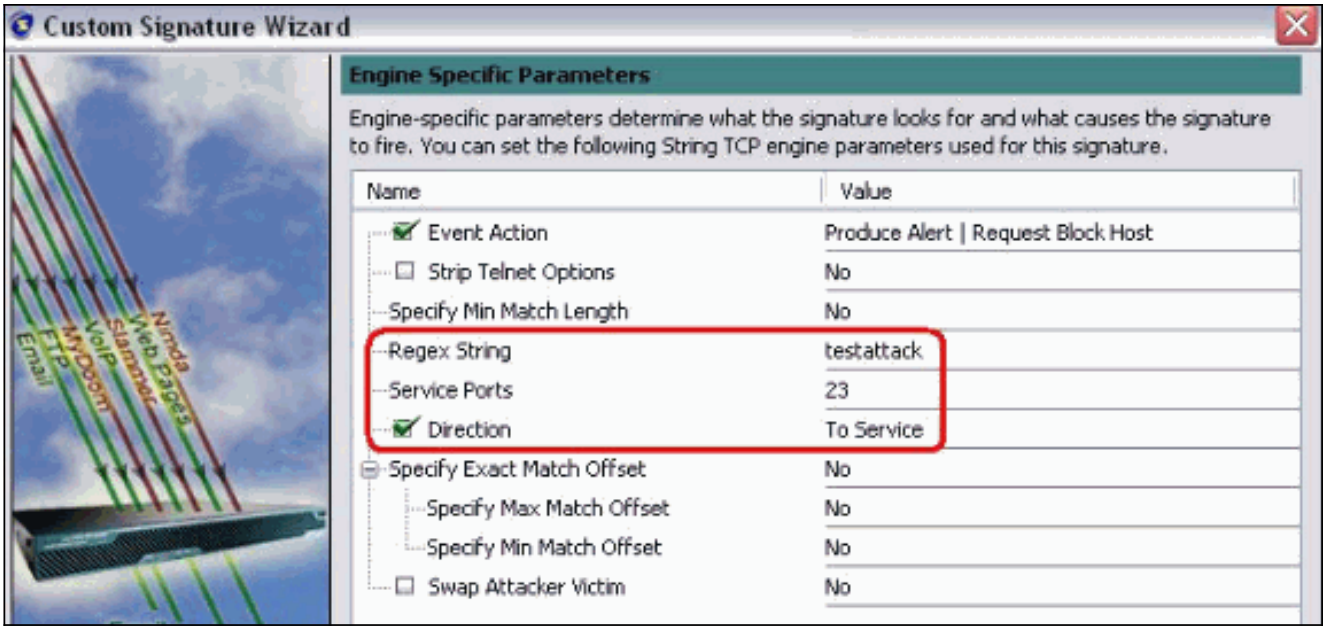
7. 您能留下此信息作为默认或输入您自己的签名ID、签名名称和用户笔记。单击 **Next**。



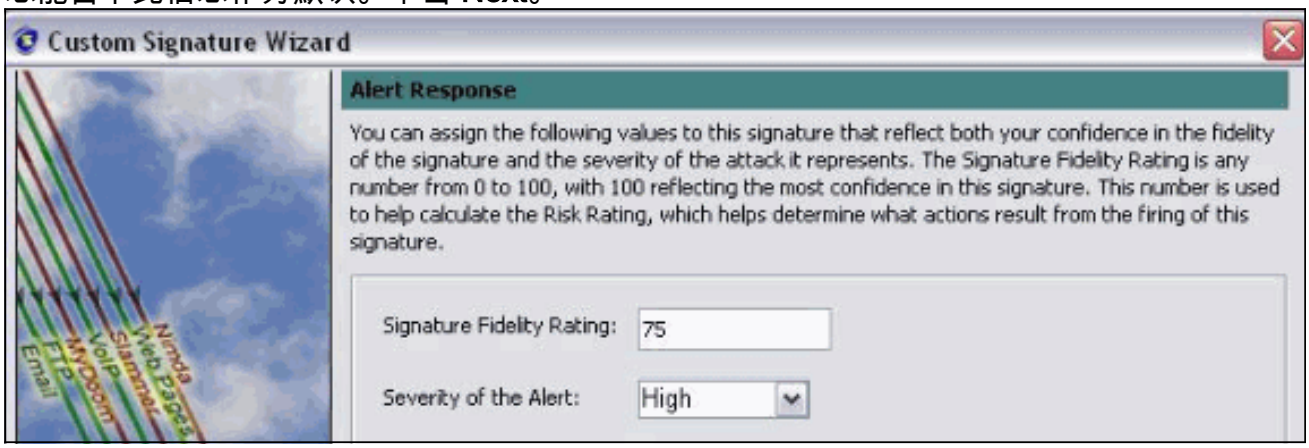
8. 选择**事件操作**并且选择**导致警报**和**请求分程序主机**。单击 **Next** 继续操作。



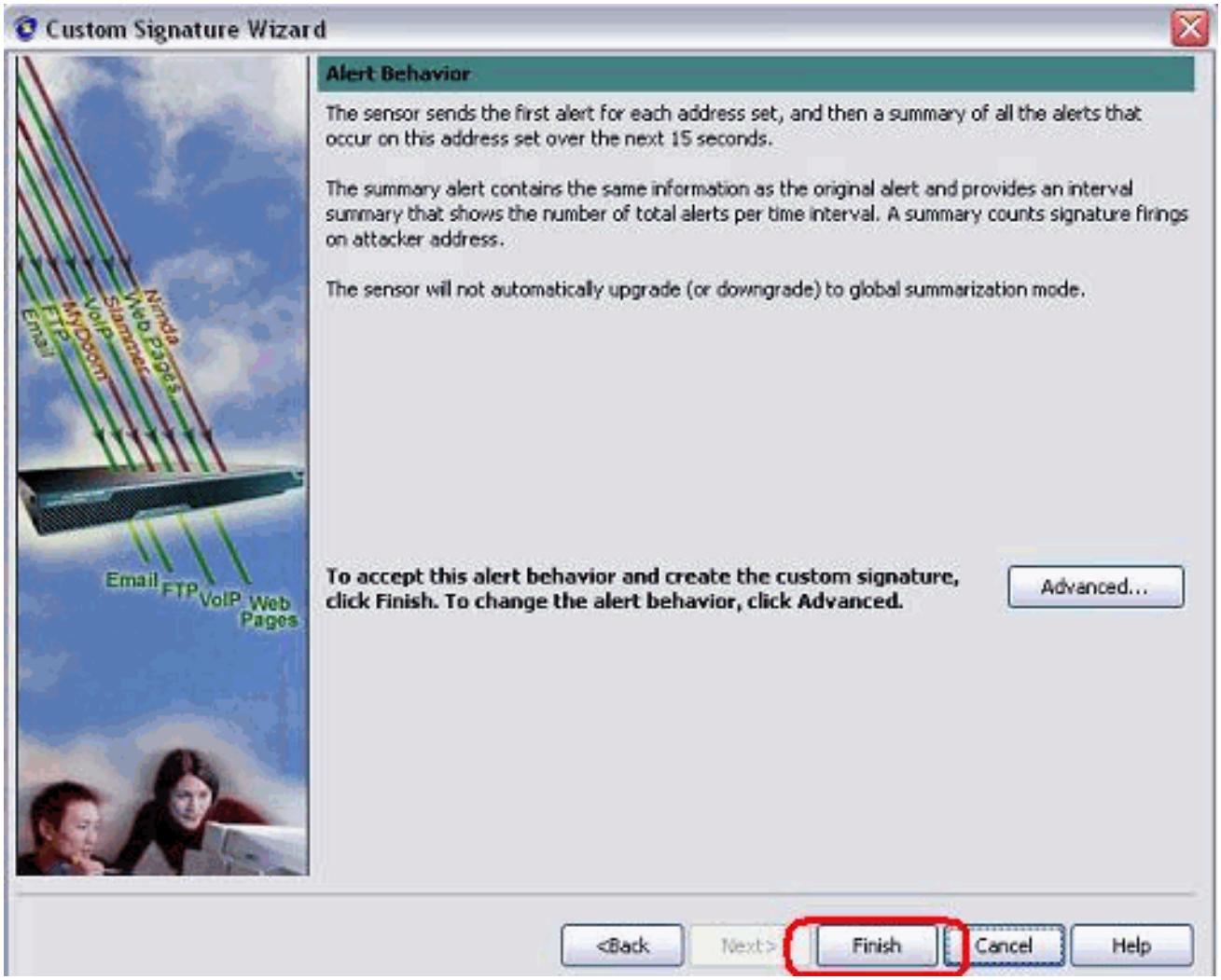
9. 输入常规表示，在本例中是*testattack*，输入**23**服务端口的，选择为方向**服务**，并且**其次**单击为了继续。



10. 您能留下此信息作为默认。单击 **Next**。

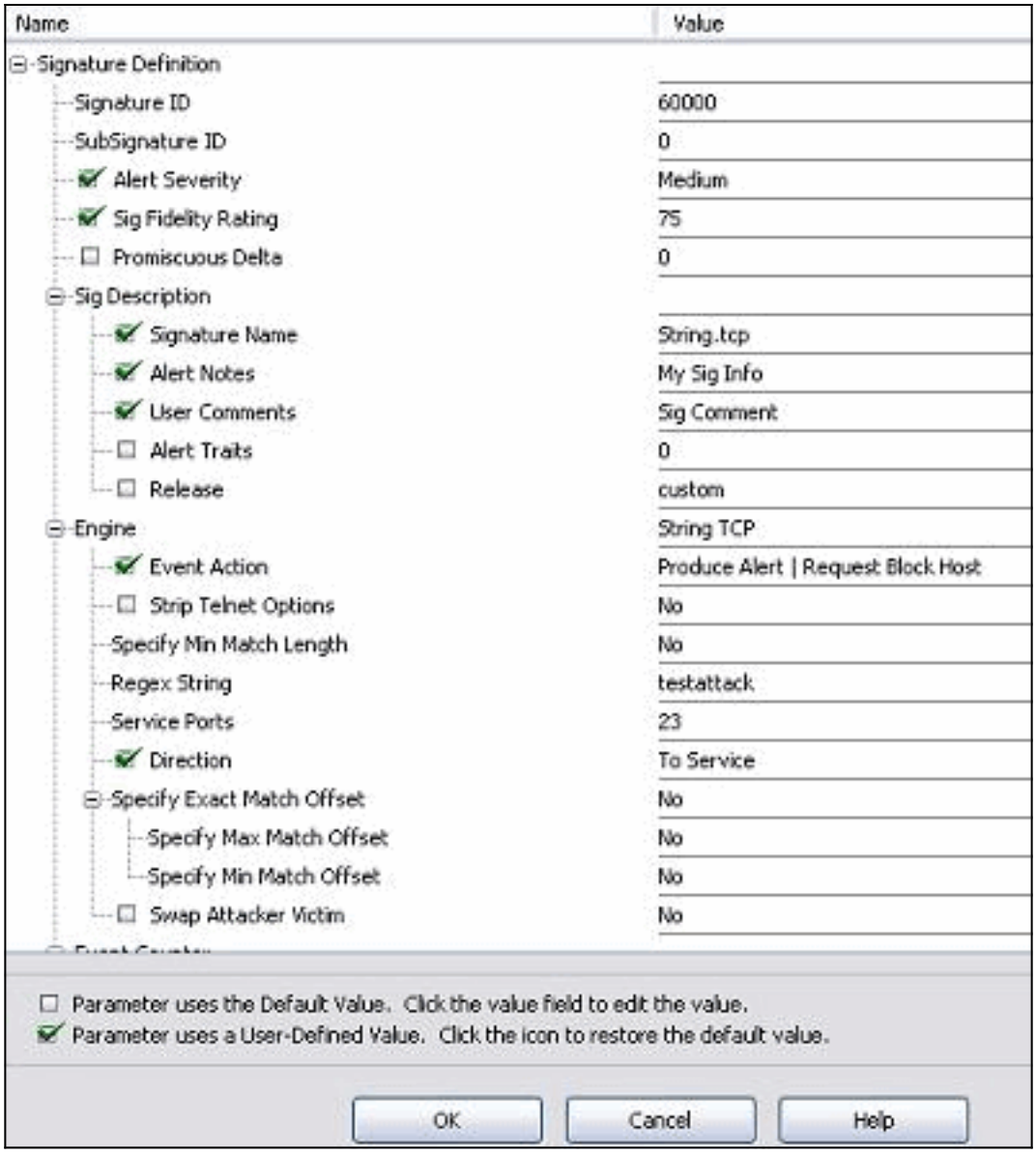


11. 点击**芬通社**为了完成向导。

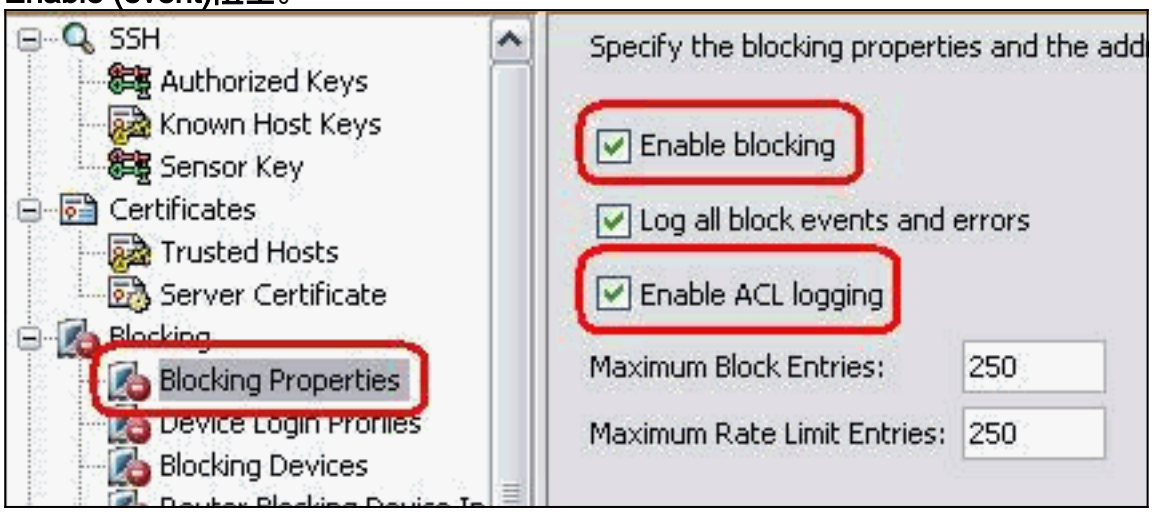


12. 选择**Configuration> sig0 >活动签名**按顺序由**签名ID**或**签名名称**找出新建立的签名。单击**编辑**

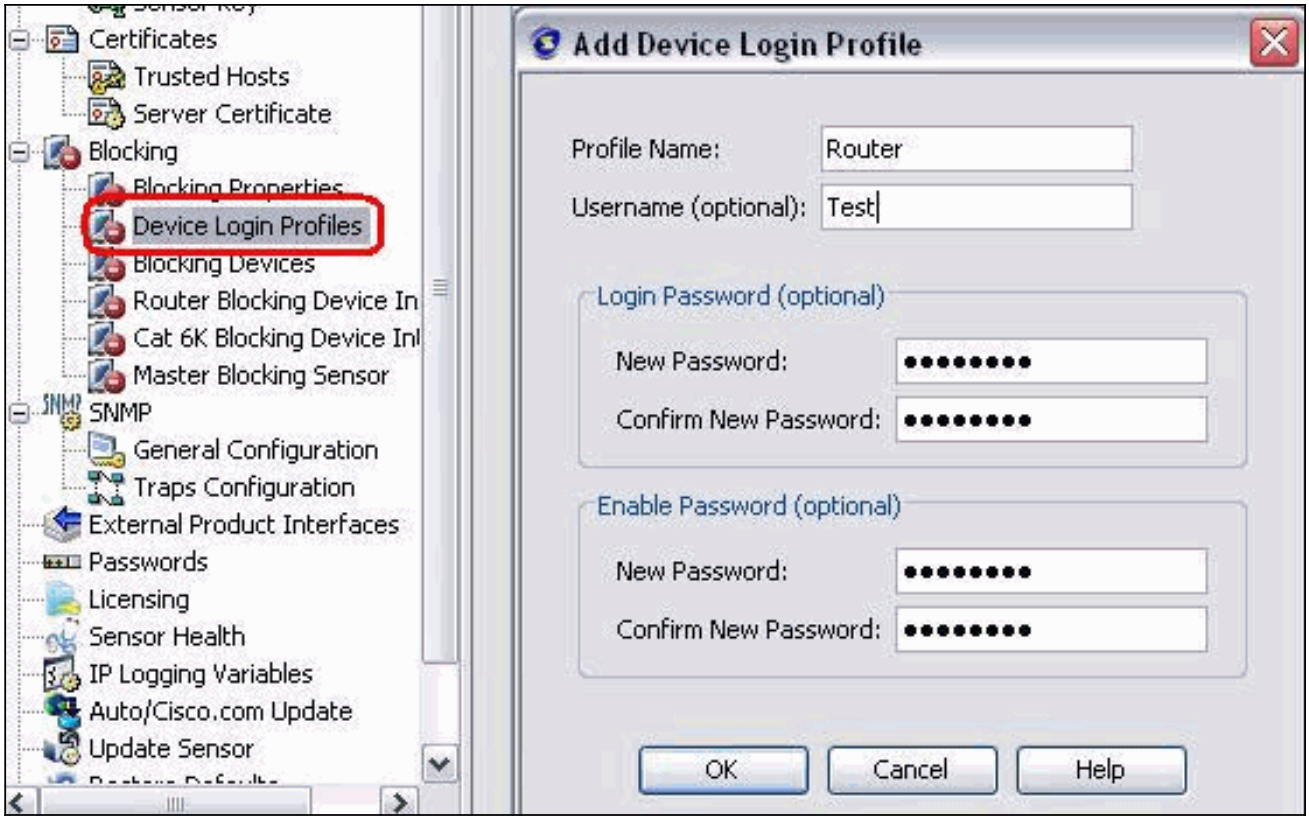
为了查看签名。



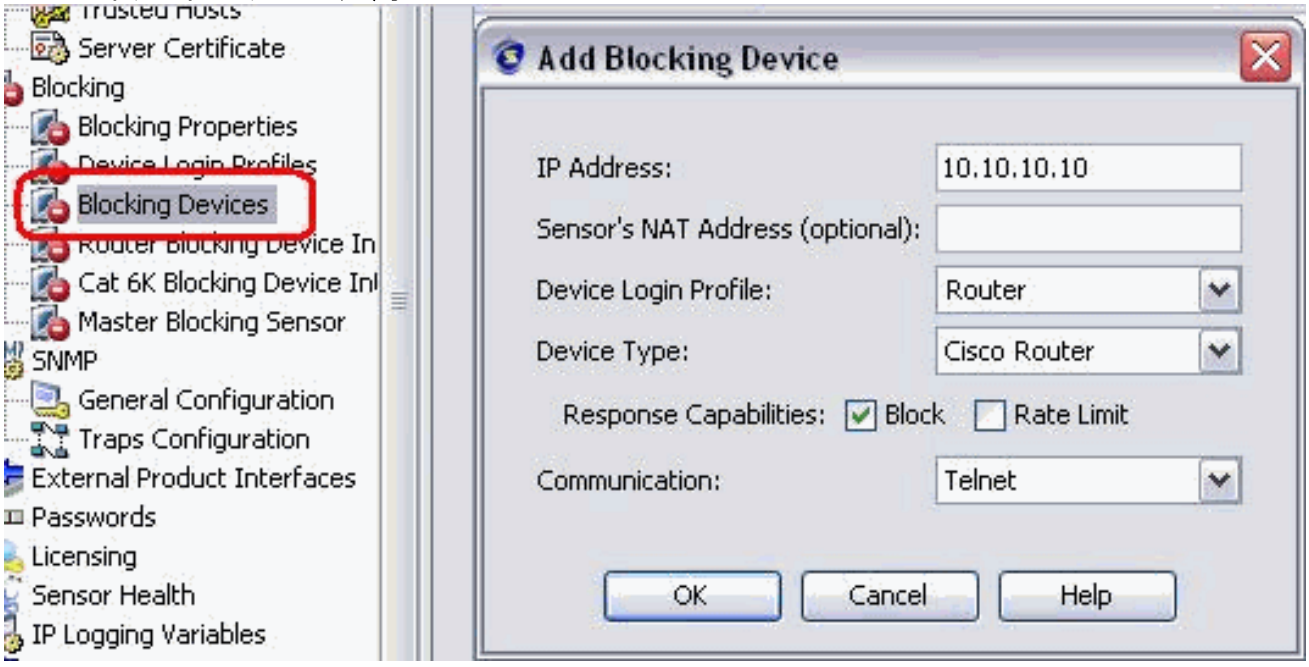
13. 在您确认并且点击**Apply按钮**为了应用签名到传感器后，请点击OK键。
14. 从Configuration选项，在传感器管理下请点击**阻塞**。从左窗格，请选择**阻塞属性**并且检查**Enable (event)阻塞**。



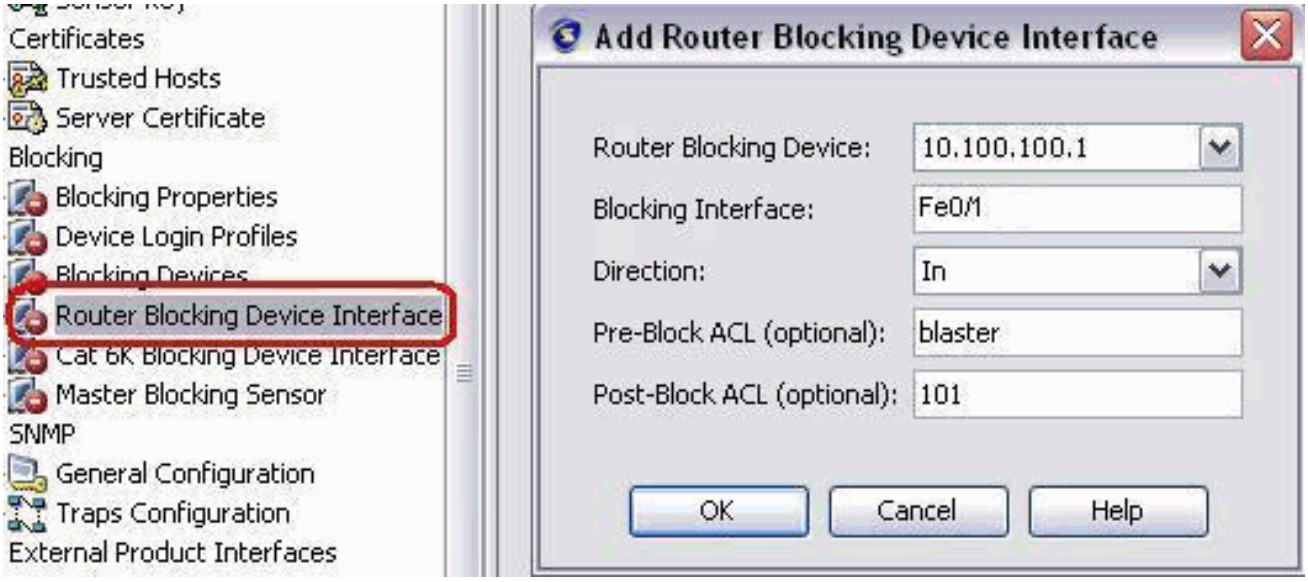
15. 现在从左窗格，请去**设备洛金配置文件**。为了创建新配置文件，请单击**添加**。一旦已创建请点击OK键并且**应用**为了传感器并且继续。



16. 下一步是配置路由器作为阻塞设备。从左窗格，请选择**阻塞设备**，单击**添加**为了添加此信息。然后请点击OK键并且**应用**。



17. 现在从左窗格请配置阻塞设备接口。添加信息，点击OK键并且**应用**。



验证

启动攻击和阻塞

完成这些步骤发起攻击和阻塞：

1. 在您发起攻击前，去IME，选择**事件监控>已丢失攻击视图**并且选择在右边的传感器。
2. 远程登录到路由器House并且验证从服务器的通信用这些命令。`house#show user Line User Host(s) Idle Location * 0 con 0 idle 00:00:00 226 vty 0 idle 00:00:17 10.66.79.195 house#show access-list Extended IP access list IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any permit ip any any (12 matches) house#`
3. 从路由器Light，请远程登录到路由器House并且键入**testattack**。点击**<space>**或**<enter>**为了重置您的远程登录会话。`light#telnet 10.100.100.1 Trying 10.100.100.1 ... Open User Access Verification Password: house>en Password: house#testattack [Connection to 10.100.100.1 lost] !--- Host 10.100.100.2 has been blocked due to the !--- signature "testattack" triggered.`
4. 远程登录到路由器House并且请使用**show access-list命令**如显示此处。`house#show access-list Extended IP access list IDS_FastEthernet0/1_in_0 10 permit ip host 10.66.79.195 any 20 deny ip host 10.100.100.2 any (71 matches) 30 permit ip any any`
5. 从IDS Event Viewer的控制板，一旦攻击启动，红色警报出现。

故障排除

本部分提供的信息可用于对配置进行故障排除。

提示

请使用这些故障排除提示：

- 从传感器请查看输出的**show statistics网络访问**并且确保"是活跃的。从控制台或SSH到传感器，此信息查看：`sensor5#**show statistics network-access** Current Configuration AllowSensorShun = false ShunMaxEntries = 100 NetDevice Type = Cisco IP = 10.66.79.210 NATAddr = 0.0.0.0 Communications = telnet ShunInterface InterfaceName = FastEthernet0/1 InterfaceDirection = in State ShunEnable = true NetDevice IP = 10.66.79.210 AclSupport = uses Named ACLs State = Active ShunnedAddr Host IP = 10.100.100.2 ShunMinutes = 15 MinutesRemaining = 12 sensor5#`
- 确保通信参数显示正确协议使用例如Telnet或SSH与3DES。您能尝试一手工的SSH或从PC的一个SSH/Telnet客户端远程登录为了检查用户名和密码凭证正确。然后从传感器到路由器中尝试Telnet或SSH操作，看您是否能成功登录路由器。

相关信息

- Cisco Secure入侵防御支持页面
- 技术支持和文档 - Cisco Systems