配置IPS TCP复位使用IME

目录

简介

使用IPS管理器Express (IME)，本文讨论入侵防御系统(IPS) TCP重置的配置。IME和IPS传感器用于管理TCP重置的一个Cisco路由器。当您查看此配置时，请记住这些项目：

- 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。

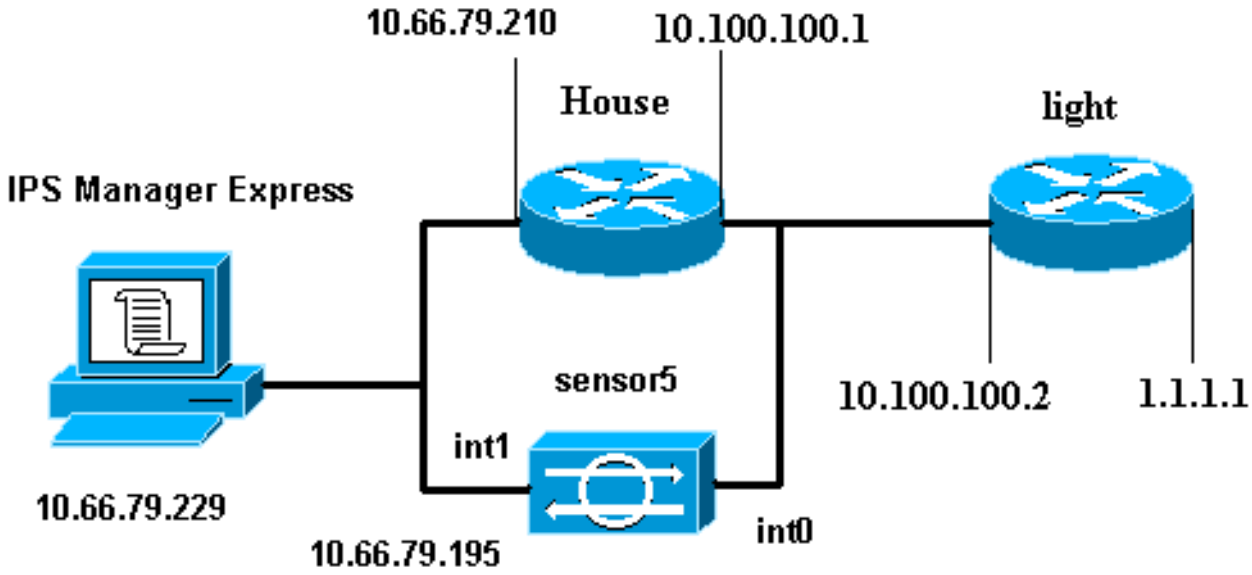
规则

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

本文档使用此图所示的网络设置。



配置

本文档使用此处所示的配置。

- 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 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 ! ! ! ! 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。

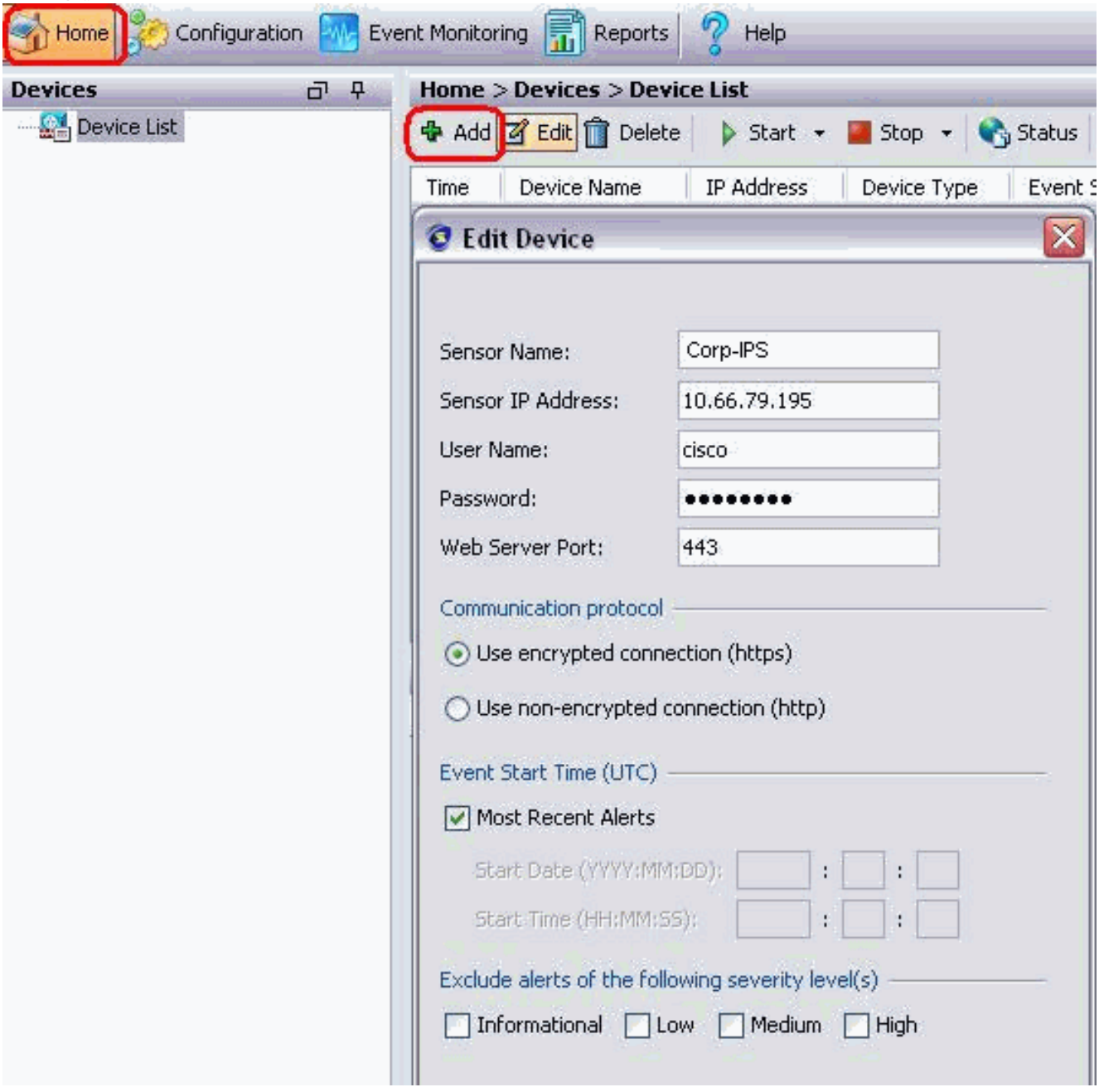
1. 如果这是您的第一次登录传感器，您必须进入**cisco**作为用户名和**cisco**作为密码。
2. 当系统提示您时，请更改您的密码。**注意：** Cisco123是字典词和没有允许在系统。
3. 键入**设置**并且完成系统提示符为了设置传感器的基本参数。
4. 输入此信息：sensor5#**setup** --- System Configuration Dialog --- *!--- At any point you may enter a question mark '?' for help. !--- Use **ctrl-c** to abort the configuration dialog at any prompt. !--- Default settings are in square brackets '[]'.* Current Configuration: networkParams ipAddress **10.66.79.195** netmask **255.255.255.224** defaultGateway **10.66.79.193** hostname **Corp-IPS** telnetOption **enabled** *!--- Permit the IP address of workstation or network with IME* **accessList ipAddress 10.66.79.0 netmask 255.255.255.0** exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit
5. 保存配置。它能花费几分钟为了传感器能保存配置。[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**

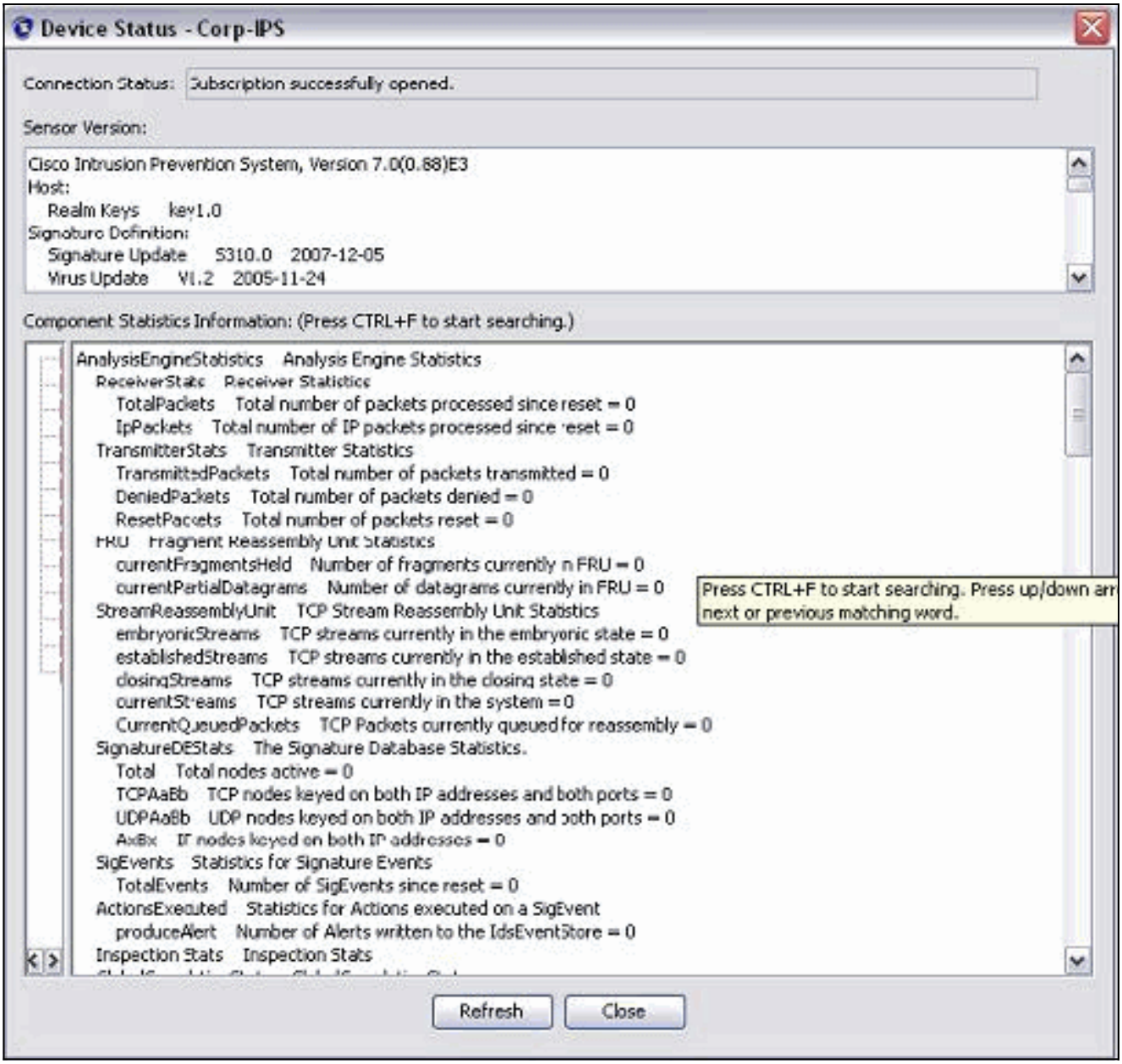
添加传感器到IME

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**。



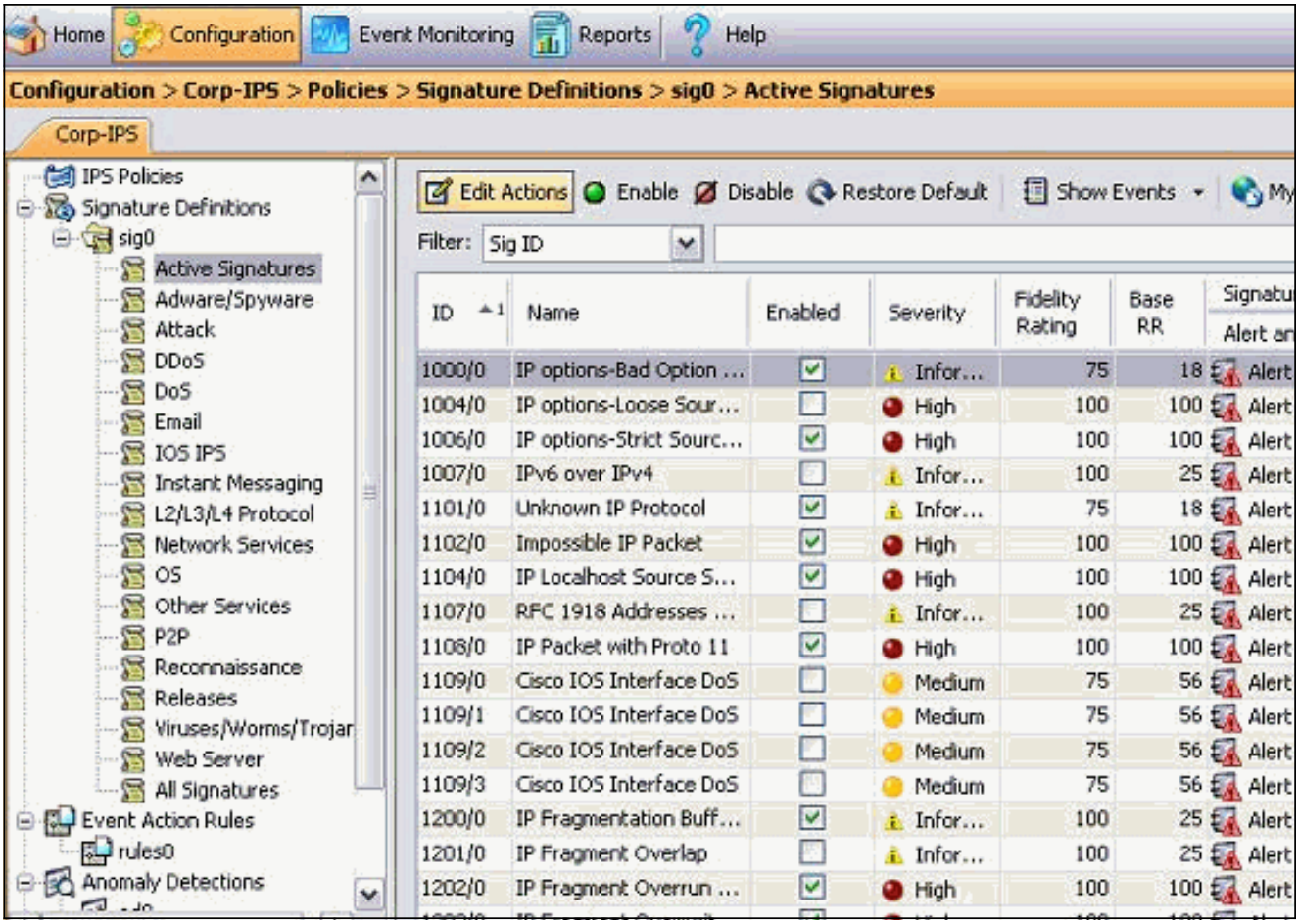
3. 键入此信息并且点击OK键为了停止配置。
4. 选择**设备>公司IPS**为了验证传感器状态然后用鼠标右键单击为了选择**设备状态**。确保您能看到



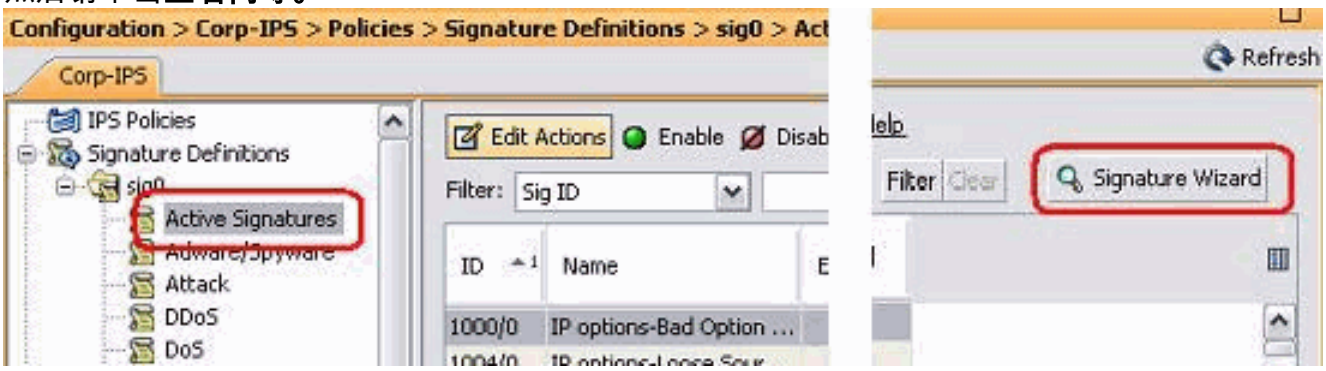
配置Cisco IOS路由器的TCP重置

完成这些步骤为了配置Cisco IOS路由器的TCP重置：

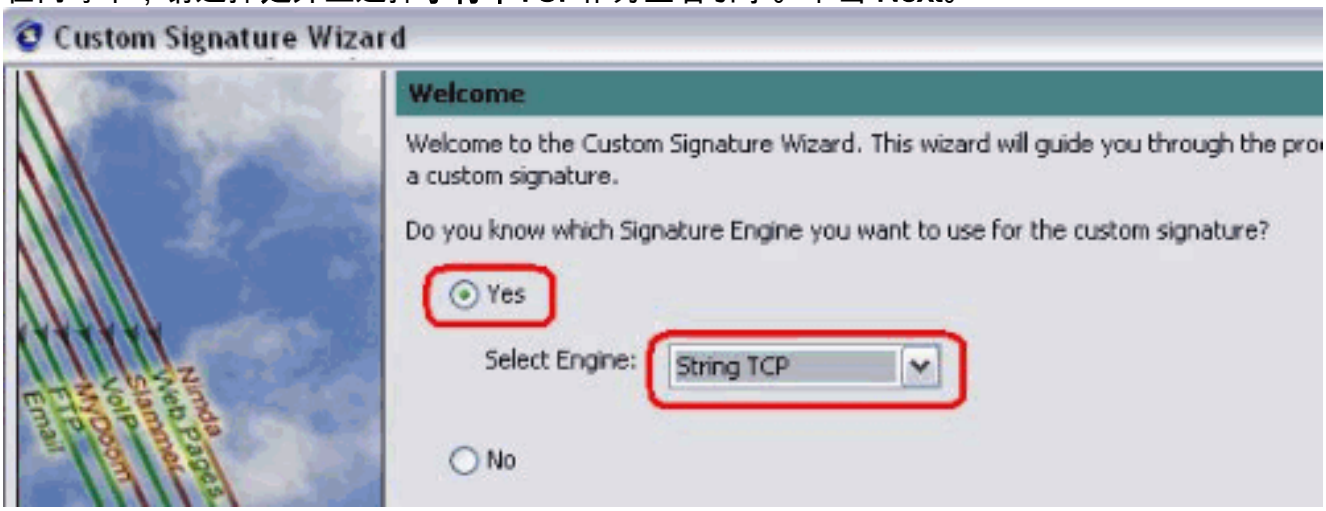
1. 从IME PC，请打开您的Web浏览器并且去**https://10.66.79.195**。
2. 点击OK键为了接受从传感器下载的HTTPS证书。
3. 在登录窗口，请输入用户名的密码的**cisco**和**123cisco123**。此IME管理接口出现：



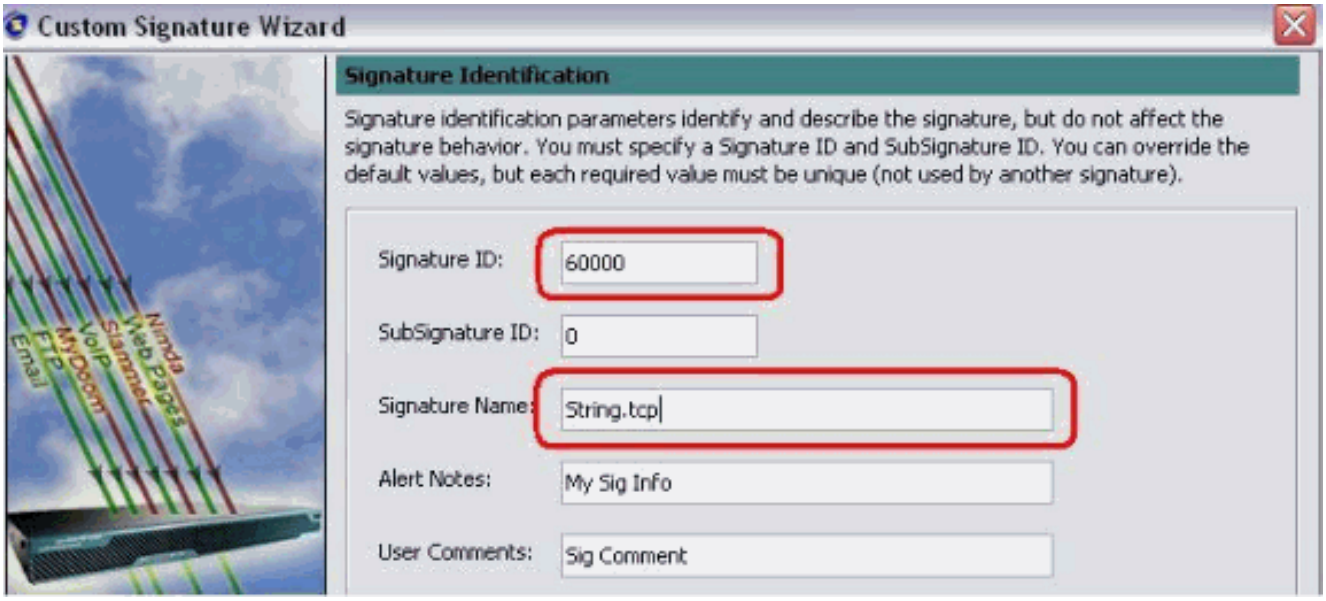
4. 从Configuration选项，请点击**活动签名**。
5. 然后请单击**签名向导。**



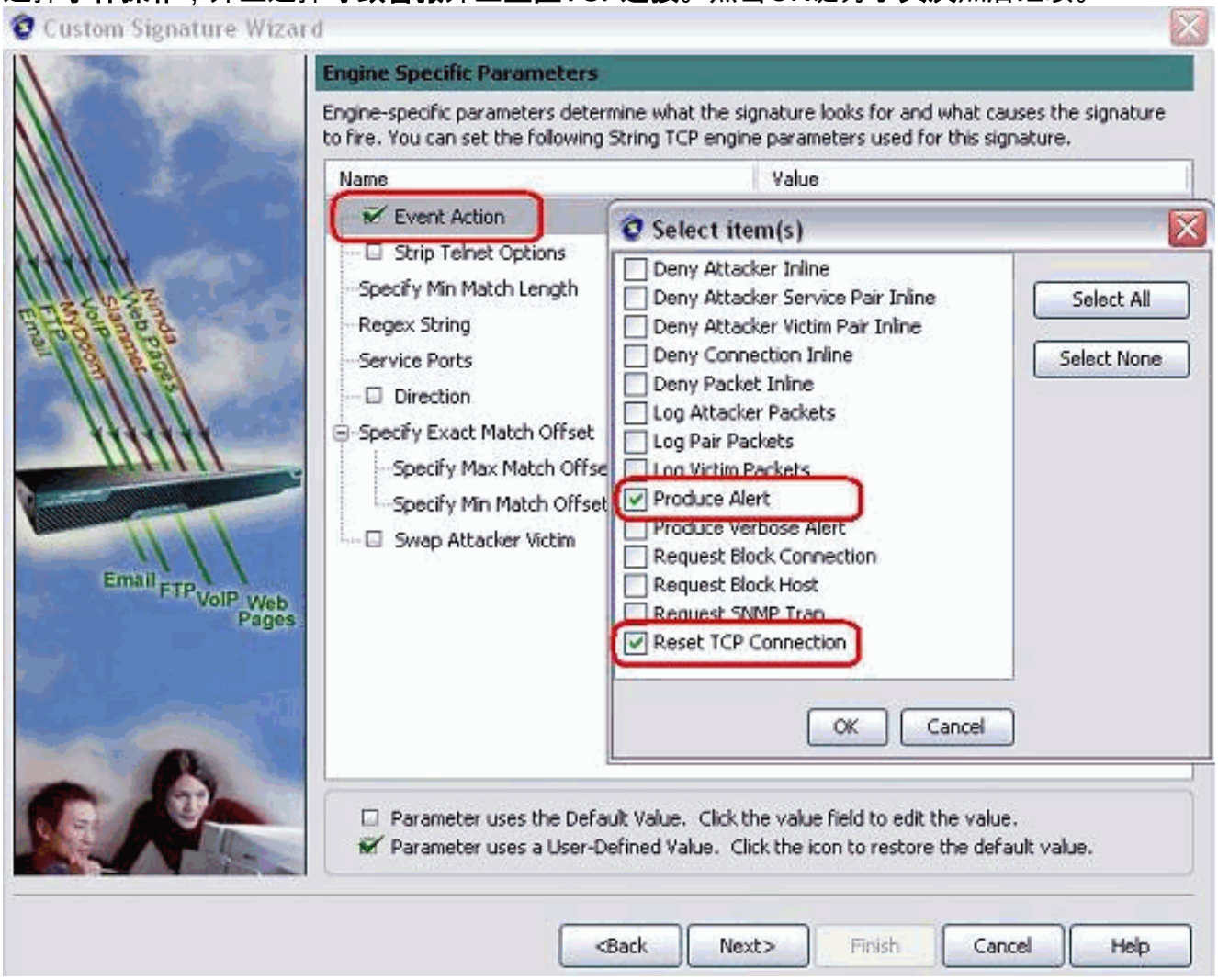
6. 在向导中，请选择**是**并且选择**字符串TCP**作为签名引擎。单击 **Next**。



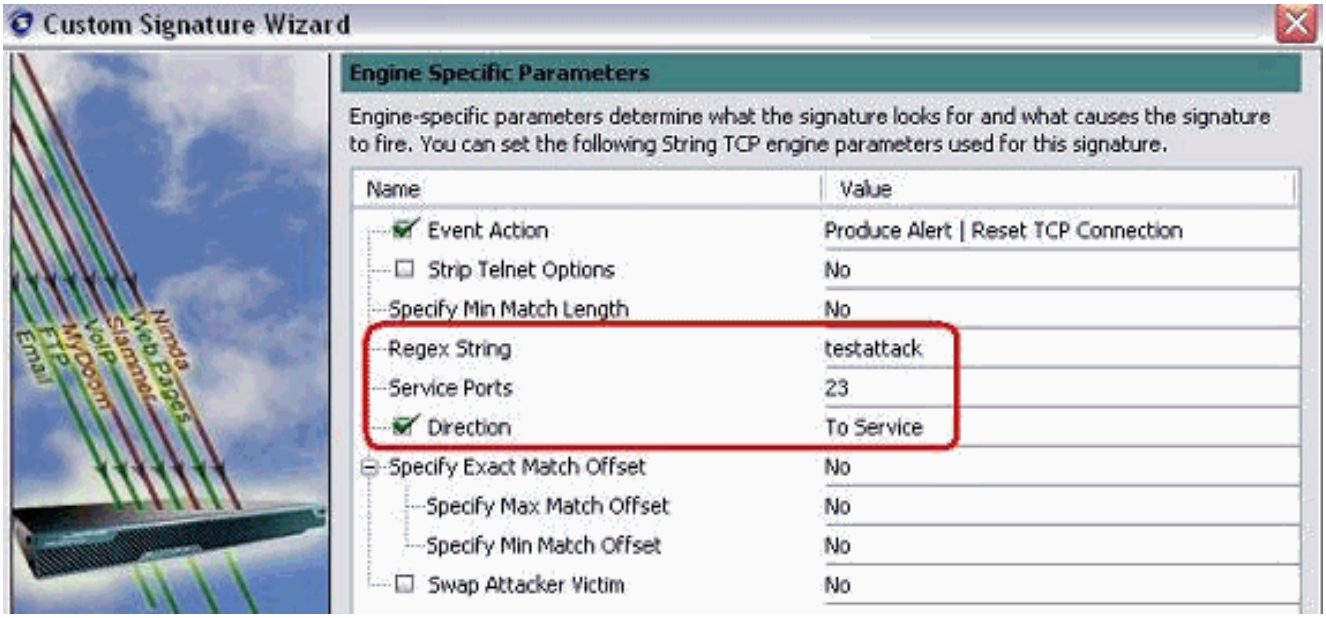
7. 您能留下此信息作为efdault或输入您自己的签名ID、签名名称和用户笔记。单击 **Next**。



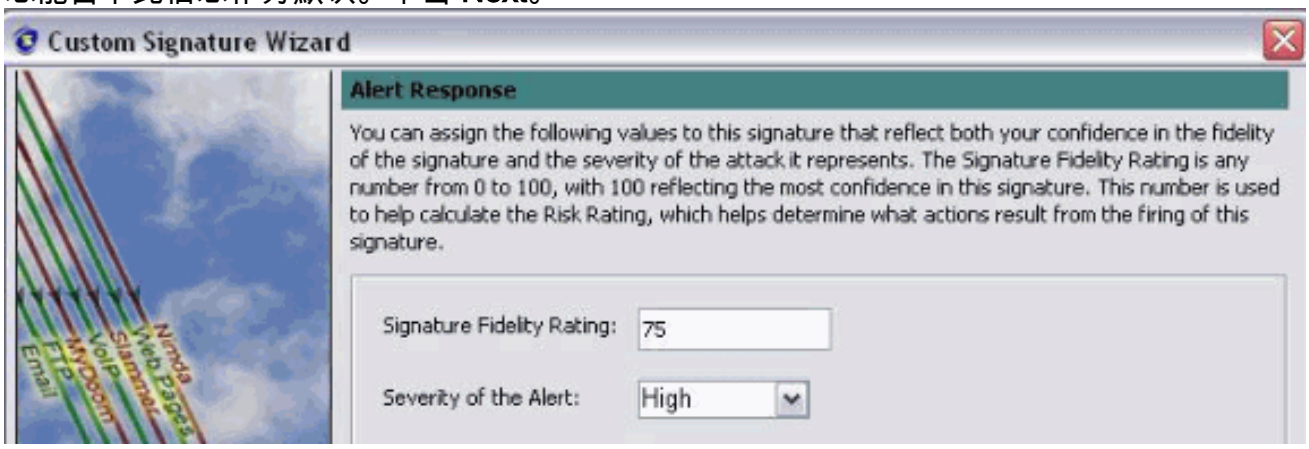
8. 选择**事件操作**，并且选择**导致警报**并且**重置TCP连接**。点击OK键为了**其次**然后继续。



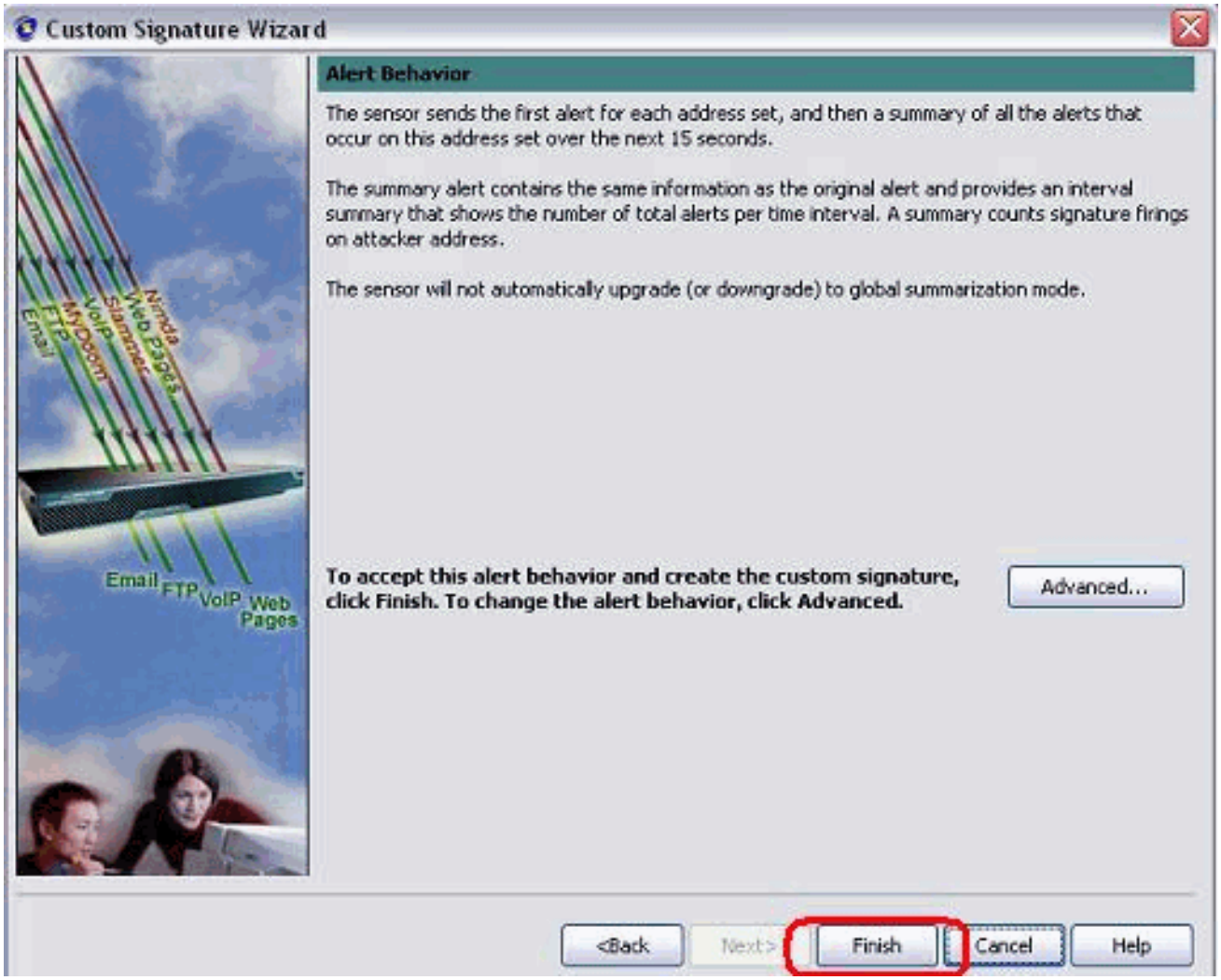
9. 输入常规表示，并且`testattack`用于此示例。服务端口的输入**23**，选择为方向**服务**，并且**其次**单击为了继续。



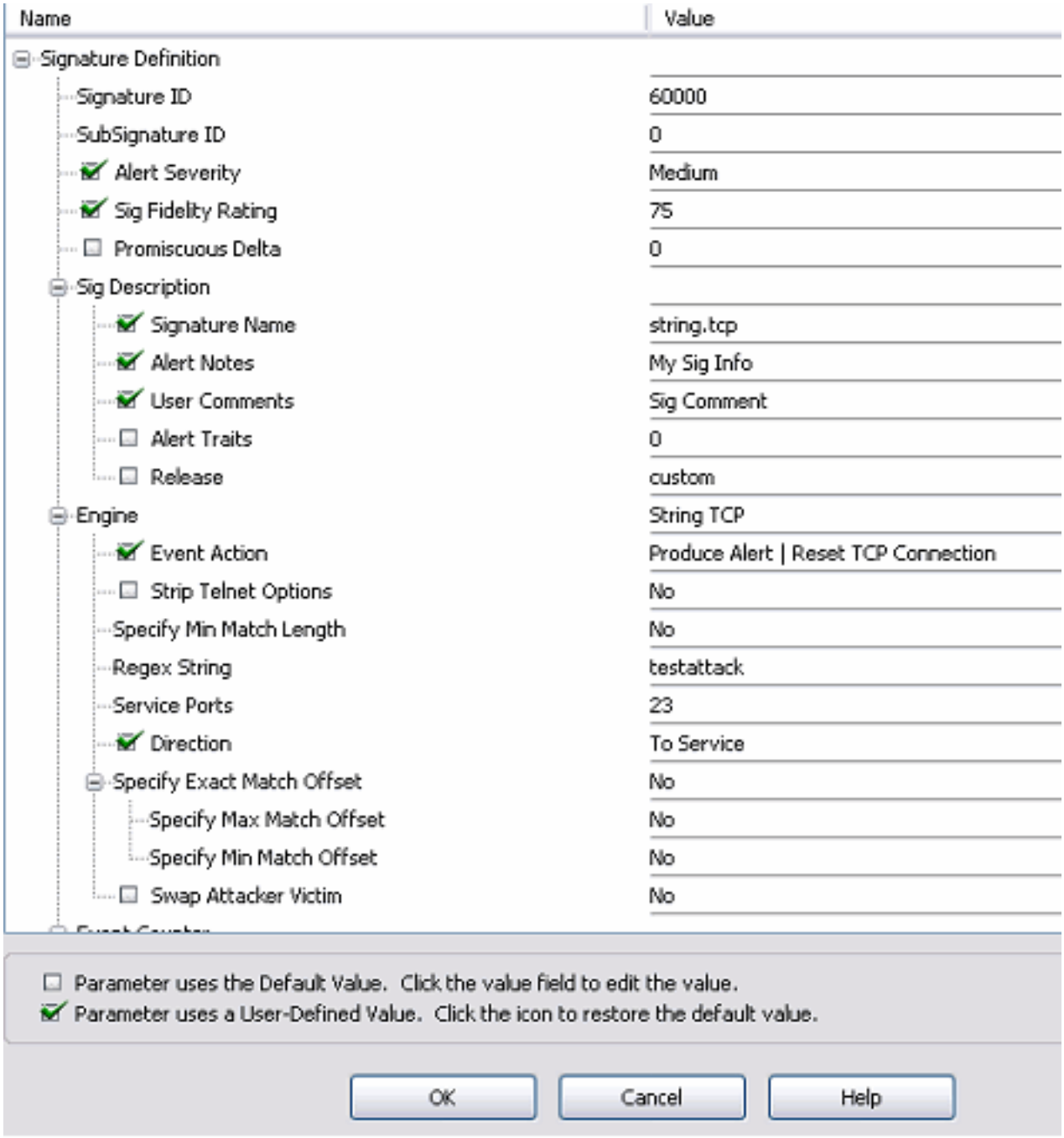
10. 您能留下此信息作为默认。单击 **Next**。



11. 点击**芬通社**为了完成向导。



12. 选择**Configuration> sig0 >活动签名**为了由**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。



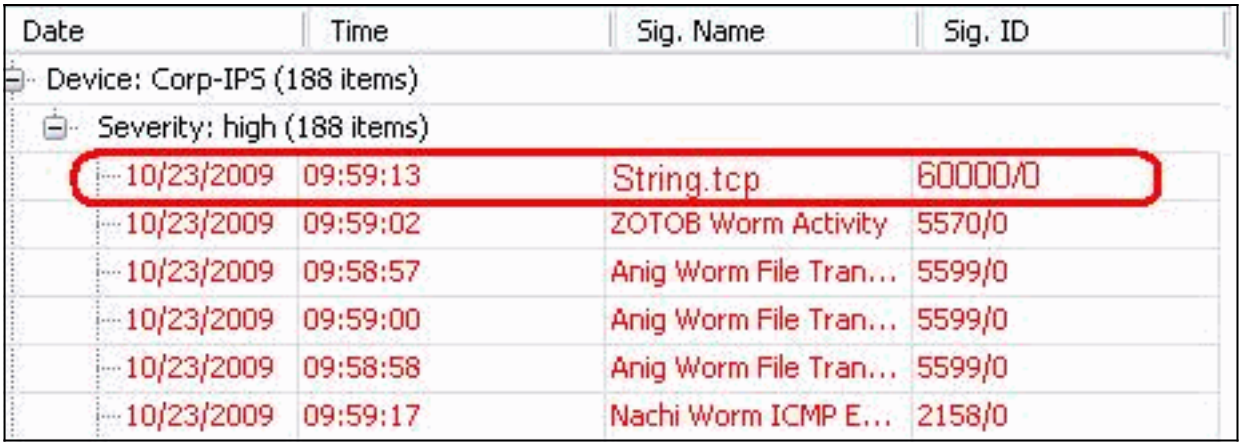
13. 在您确认并且点击**Apply按钮**为了应用签名到传感器后，请点击OK键。

验证

启动攻击和TCP重置

完成这些步骤为了启动攻击和TCP重置：

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. 从路由器Light，请远程登录到路由器House并且输入**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 closed by foreign host] !--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.`
3. 从IPS事件查看器的控制板，一旦攻击启动，红色警报出现。



Date	Time	Sig. Name	Sig. ID
Device: Corp-IPS (188 items)			
Severity: high (188 items)			
10/23/2009	09:59:13	String.tcp	60000/0
10/23/2009	09:59:02	ZOTOB Worm Activity	5570/0
10/23/2009	09:58:57	Anig Worm File Tran...	5599/0
10/23/2009	09:59:00	Anig Worm File Tran...	5599/0
10/23/2009	09:58:58	Anig Worm File Tran...	5599/0
10/23/2009	09:59:17	Nachi Worm ICMP E...	2158/0

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：

- 避开解决命令和控制端口重编程序路由器访问控制列表(ACL)。TCP重置从传感器的**探测接口**被发送。当您在交换机的**set span**，以如显示启用的两流入数据包使用**set span <src_mod/src_port><dest_mod/dest_port>命令**此处。`banana (enable)`**`set span 2/12 3/6 both inpkts enable Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12 Incoming Packets enabled. Learning enabled. Multicast enabled.`** `banana (enable) banana (enable) banana (enable)`**`show span`** `Destination :` **`Port 3/6`** `!--- connect to sniffing interface of the sensor Admin Source :` **`Port 2/12`** `!--- connect to FastEthernet0/0 of Router House Oper Source :` **`Port 2/12`** `Direction :` **`transmit/receive`** `Incoming Packets:` **`enabled`** `Multicast : enabled`
- 如果TCP重置工作，请检查报警是否为操作类型TCP重置被触发。如果报警出现，请检查签名类型设置为TCP重置。登陆使用服务帐户su根源和发出此命令。此命令假设感觉的接口设置为eth0。`[root@sensor1 root]#`**`tcpdump -i eth0 -n`** **注意：** 一百tcp重置获得发送对受害者/目标一百然后获得发送对攻击者/客户端。以下是输出示例：

```
03:06:00.598777 64.104.209.205.1409 >
 10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
 10.66.79.38.telnet: R 108:108(0) ack 72 win 0

03:06:00.599360 10.66.79.38.telnet >
 64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
 64.104.209.205.1409: R 73:73(0) ack 46 win 0
```

相关信息

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