配置TCP重置使用IDS控制器

Contents

Introduction

本文描述如何配置入侵检测系统(IDS，以前NetRanger)导向器和传感器发送包括被管理的路由器在尝试的Telnet的TCP重置到地址范围，如果被发送的字符串是“testattack”。

Prerequisites

Requirements

就此配置而论，当，请切记对：

- 安装传感器并且验证适当地运作，在您执行此配置前。
- 保证探测接口间距到被管理的路由器的外部接口。

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco IDS Director 2.2.3
- Cisco IDS传感器3.0.5
- 运行软件版本12.2.6的Cisco IOS路由器

The information in this document was created from the devices in a specific lab environment.All of

the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

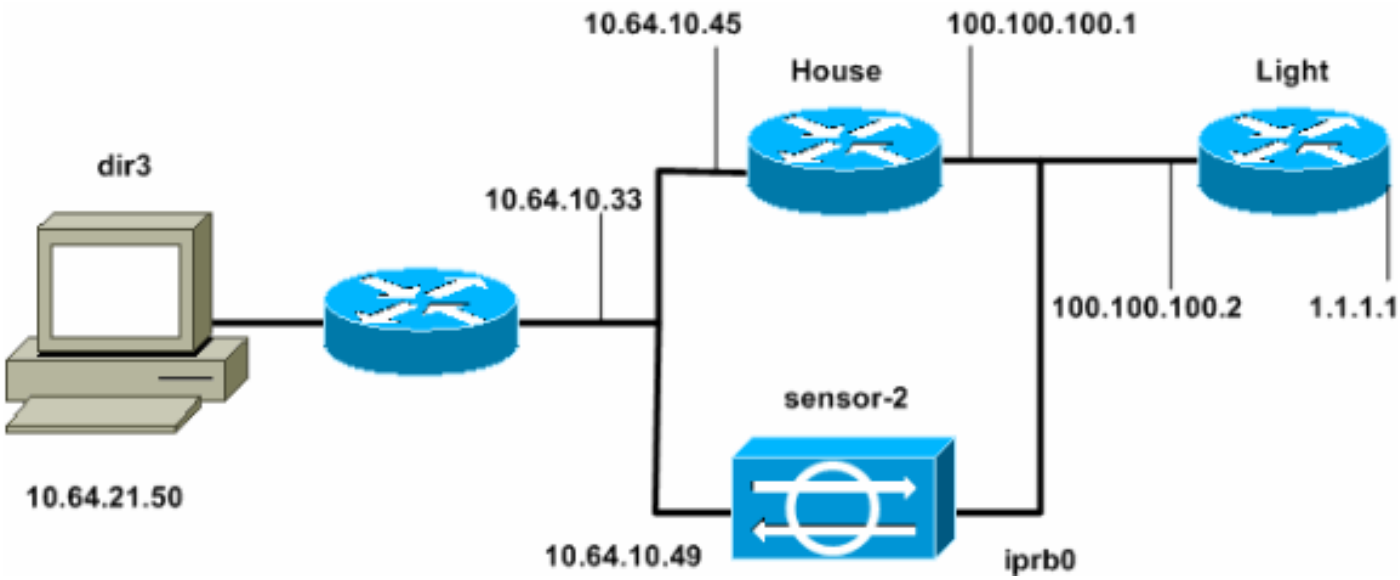
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

Network Diagram

本文档使用此图所示的网络设置。



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 12.2
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 100.100.100.2 255.255.255.0
 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 0.0.0.0 100.100.100.1
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 : 2187 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
enable password cisco
!
!
!
ip subnet-zero
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
!
!
!
interface FastEthernet0/0
 ip address 100.100.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.64.10.45 255.255.255.224
 duplex auto
 speed auto
!
!
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
ip route 1.1.1.0 255.255.255.0 100.100.100.2
ip http server
ip pim bidir-enable
!
!
!
snmp-server manager
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
line aux 0
```

```
line vty 0 4
 password cisco
 login
!
!
end

house#
```

配置传感器

完成这些步骤配置传感器。

1. 远程登录到10.64.10.49 (IDS传感器)与用户名根和**密码攻击**。
2. 键入**sysconfig-sensor**。
3. 如此示例所显示，当提示，请输入配置信息， ：

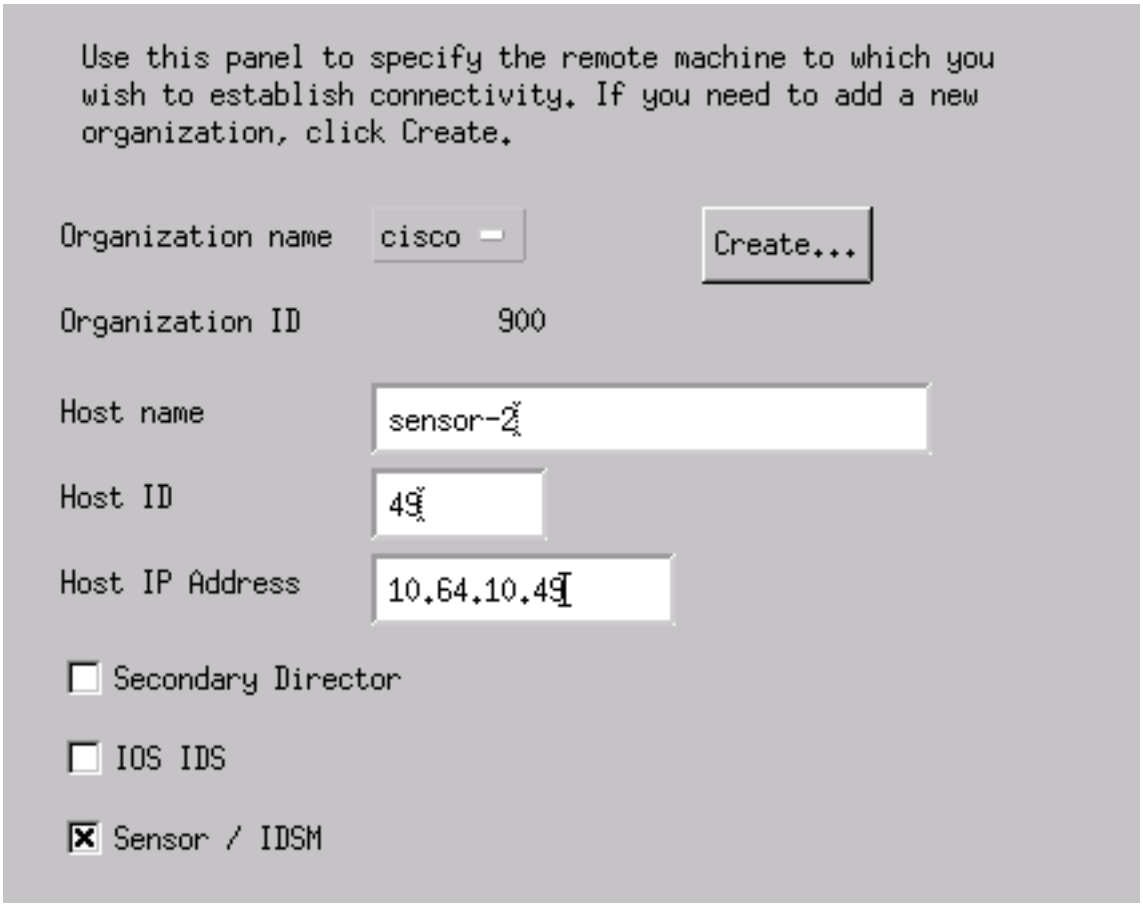
```
1 - IP Address:  10.64.10.49
2 - IP Netmask:  255.255.255.224
3 - IP Host Name:  sensor-2
4 - Default Route:  10.64.10.33
5 - Network Access Control
          64.
          10.
6 - Communications Infrastructure
Sensor Host ID:  49
Sensor Organization ID:  900
Sensor Host Name:  sensor-2
Sensor Organization Name:  cisco
Sensor IP Address:  10.64.10.49
IDS Manager Host ID:  50
IDS Manager Organization ID:  900
IDS Manager Host Name:  dir3
IDS Manager Organization Name:  cisco
IDS Manager IP Address:  10.64.21.50
```

4. 当提示，请保存配置并且允许传感器重新启动。

添加传感器到导向器

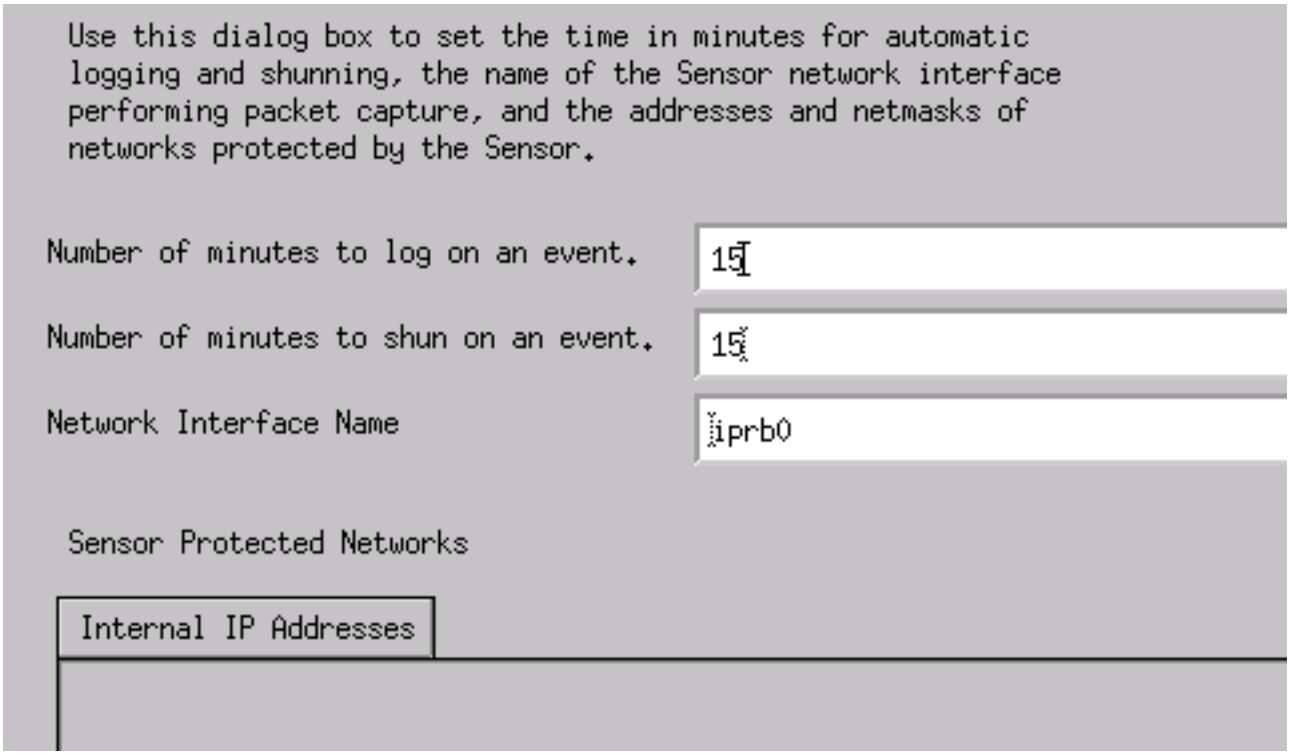
完成这些步骤添加传感器到导向器。

1. 远程登录到10.64.21.50 (IDS控制器)与用户名**netrangr**和**密码攻击**。
2. 键入**ovw&**启动HP OpenView。
3. 从主菜单，请去**Security > Configure**。
4. 在配置文件管理工具中，请去**File > Add Host**并且**其次**点击。
5. 如此示例所显示，完成传感器主机信息。单击 **Next**。

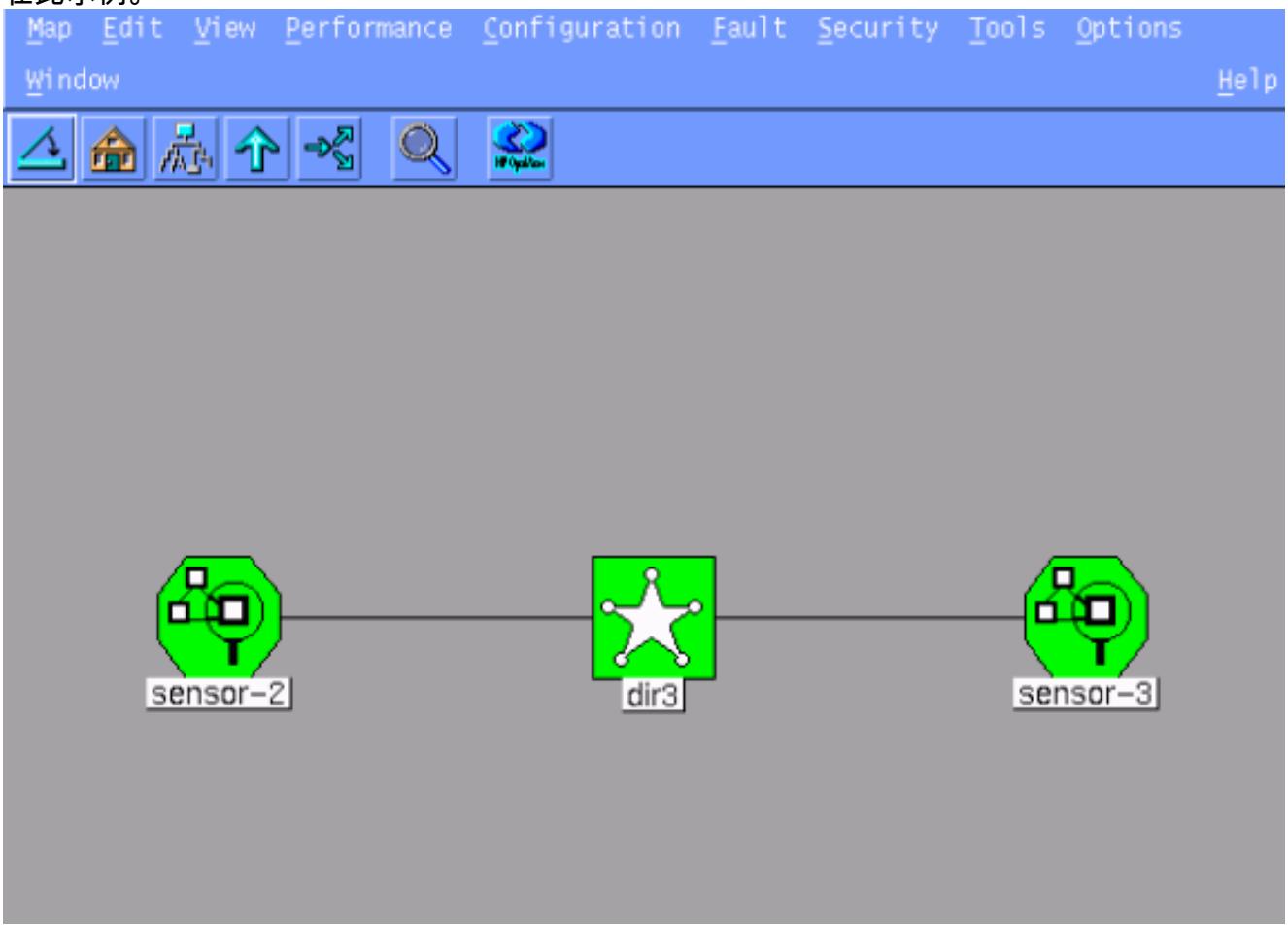


6. 如此示例所显示，接受机器的种类的默认设置，并且**其次**点击。

7. 您可以更改日志，并且避开分钟或您可能接收默认值。然而，您必须更改网络接口名称到您的探测接口的名字。在本例中，它是"iprb0"。它可以是"spwr0"或别的根据传感器类型，并且您如何连接您的传感器。



8. 继续**其次**点击然后点击**完成**添加传感器到导向器。从主菜单，您应该当前看到sensor-2，正如在此示例。



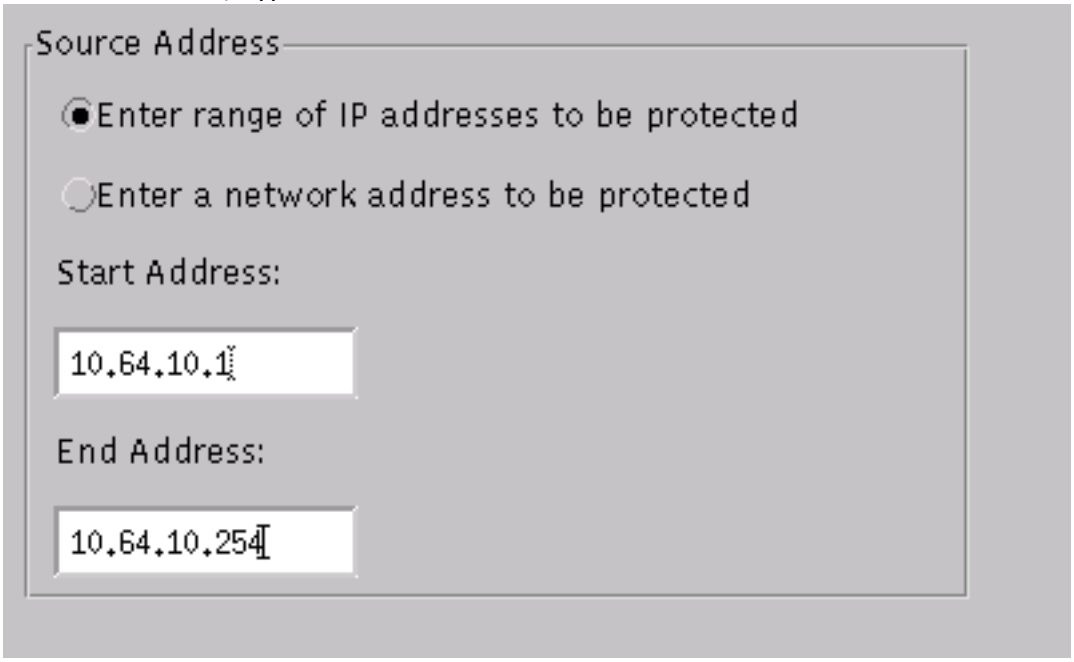
配置Cisco IOS路由器的TCP重置

完成这些步骤配置Cisco IOS路由器的TCP重置。

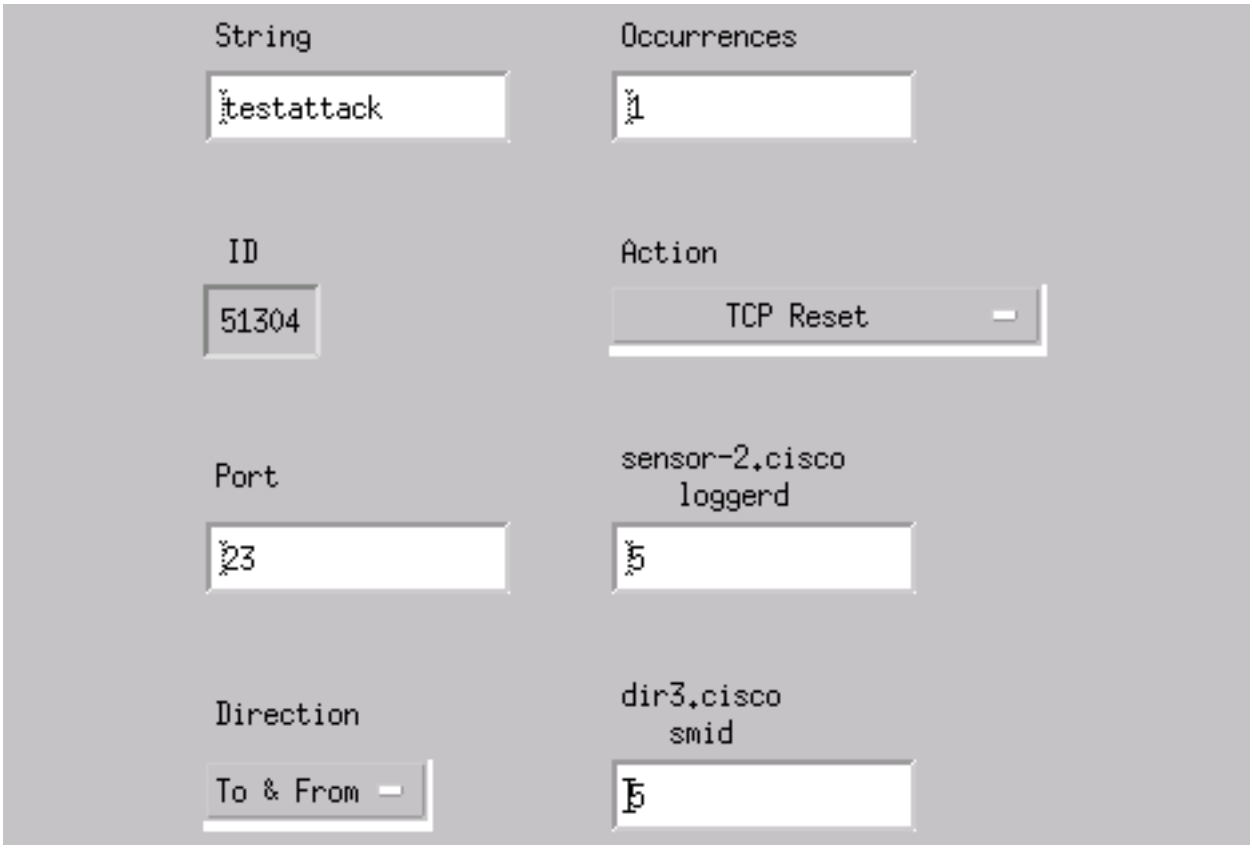
1. 在主菜单，请去**Security > Configure**。

2. 在配置文件管理工具中，高亮度显示**sensor-2**和双击它。
3. 打开设备管理。
4. 点击**Devices > Add**。如以下示例所显示，输入设备信息。点击OK键继续。Telnet和特权密码是Cisco。

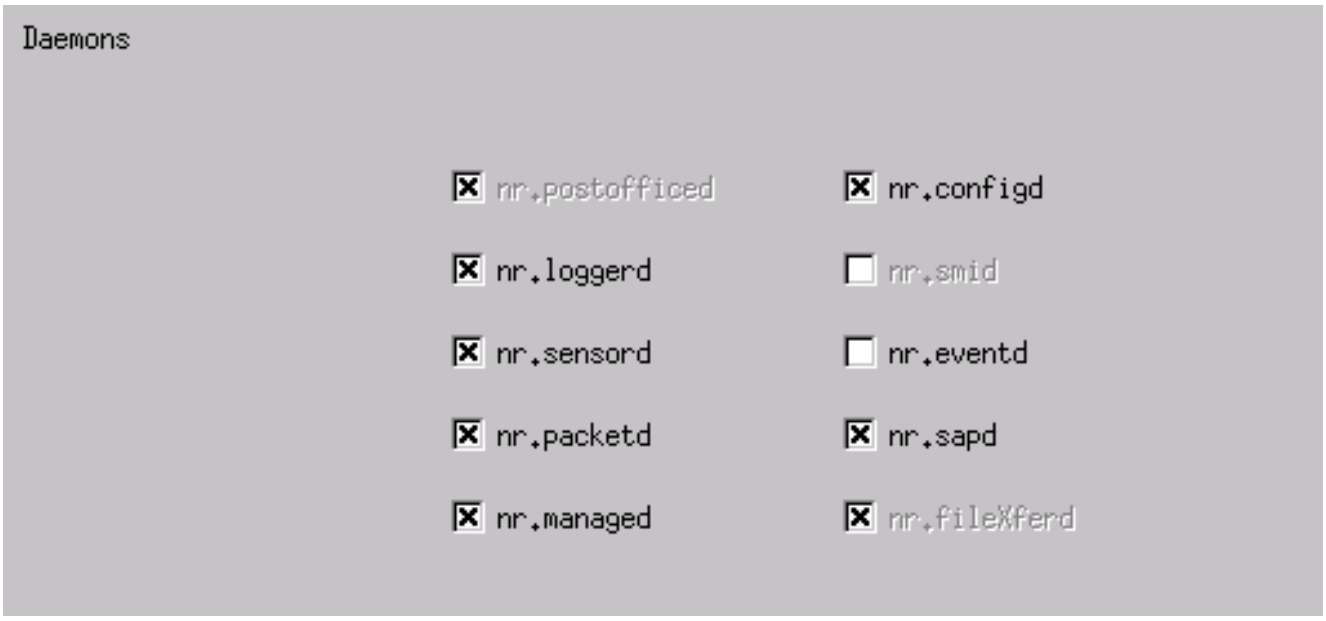
5. 打开Intrusion Detection Window并且点击**受保护的网络**。从10.64.10.1添加地址范围到10.64.10.254到受保护的网络。



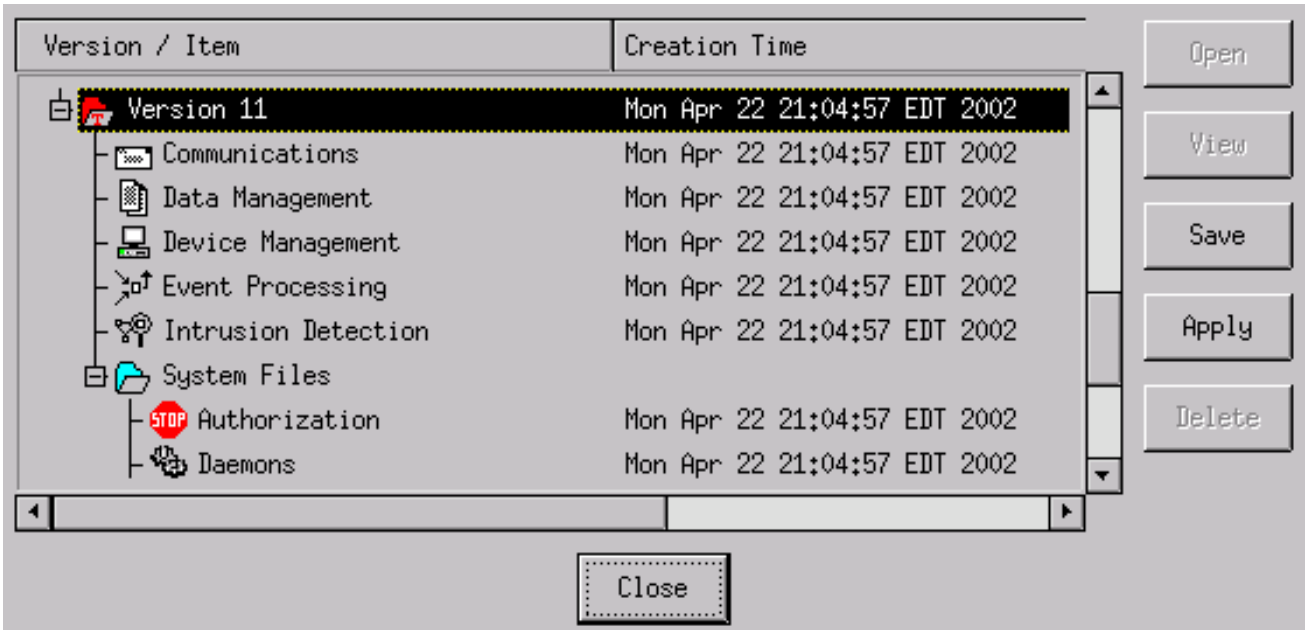
6. 点击**配置文件**并且选择**手动配置**。其次，请点击**修改签名**。选择**被匹配的字符串**有ID 8000。点击**Expand > Add**添加称为**testattack的**一个新的字符串。如此示例所显示，输入字符串信息，并且点击OK键继续。



7. 您完成了配置的这部分。点击OK键关上Intrusion Detection Window。
8. 打开系统文件文件夹，然后Daemons窗口。保证您安排这些守护程序被启用
   ：



9. 点击OK键继续。
10. 选择您修改的版本，点击**"Save"**然后**适用**。等待系统告诉您传感器完成重新启动服务，然后关上配置管理器的所有窗口。



启动攻击和TCP重置

从路由器Light远程登录到路由器House并且键入**testattack**。当您击了空间或enter键，您的远程登录会话重置。您将连接到路由器House。

```
light#telnet 10.64.10.45
Trying 10.64.10.45 ... Open

User Access Verification
Password:
house>en
Password:
house#testattack
[Connection to 10.64.10.45 closed by foreign host]
 !--- Telnet session has been reset because the !--- signature testattack was triggered.
```

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

使用用户名根和**密码攻击，**远程登录到10.64.10.49，传感器。键入**cd /usr/nr/etc**。键入**cat packetd.conf。如果**正确地设置testattack的TCP重置，您应该看到四(4)在Action Codes字段。如此示例所显示，这指示TCP重置。

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 4 5 5 # "testattack"
```

如果偶然地设置动作对“无”在签名，您将看到一零(0)在Action Codes字段。这不如在此示例中看到

指示动作。

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
RecordOfStringName 51304 23 3 1 "testattack"
SigOfStringMatch 51304 0 5 5 # "testattack"
```

TCP重置从传感器的探测接口被发送。如果有连接传感器接口的交换机到被管理的路由器的外部接口，使用**set span命令**在交换机时，当您配置，请使用此语法：

```
set span <src_mod/src_port><dest_mod/dest_port> both inpkts enable
```

```
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
Learning        : enabled
Multicast       : enabled
```

Related Information

- Field Notices
- Cisco Secure入侵防御支持页面