

在 UNIX Director 上设置规避

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[在攻击前启动](#)

[发起攻击和规避](#)

[故障排除](#)

[相关信息](#)

简介

Cisco入侵检测系统(IDS)导向器和传感器可以用于管理避开的一个Cisco路由器。在本文中，传感器(sensor-2)配置为了检测在路由器“议院”的攻击和为了传达此信息到导向器一次配置的"dir3."，攻击从路由器“灯启动(大于1024个字节，是签名2151和一互联网控制消息协议[ICMP]充斥ping，是签名2152)”。传感器检测攻击并且传达此对导向器。访问控制表(ACL)下载到路由器避开从攻击者的流量。在攻击者显示，并且在受害者下载的ACL显示。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 安装传感器并且确保它适当地工作。
- 保证探测接口间距对路由器的外部接口。

使用的组件

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
- 有12.2.6的Cisco IOS路由器

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](#)。

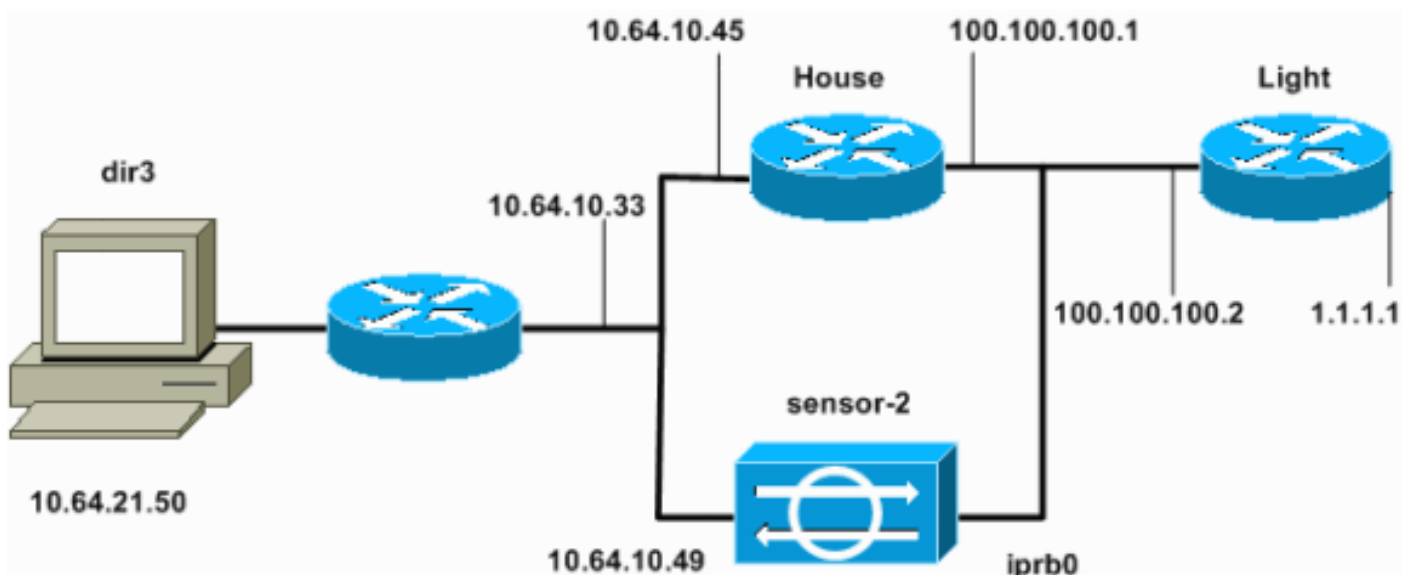
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：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](#)）。

网络图

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 !
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 !--- After you
configure shunning, IDS Sensor puts this line in. ip
access-group IDS_FastEthernet0/0_in_1 in 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 ! ! !--- After you
configure shunning, IDS Sensor puts these lines in. ip
access-list extended IDS_FastEthernet0/0_in deny ip host
100.100.100.2 any permit ip host 10.64.10.49 any permit
ip any any ! 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. 对10.64.10.49的Telnet与用户名根和密码攻击。
2. 回车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. 远程登录到与用户名netrangr和密码攻击的10.64.21.50。
2. 输入ovw&启动HP OpenView。
3. 在主菜单，请选择Security > Configure。

- 在配置文件管理工具中，请选择**File > Add Host**，并且其次单击。
- 这是示例如何填好请求的信息。

Use this panel to specify the remote machine to which you wish to establish connectivity. If you need to add a new organization, click Create.

Organization name

Organization ID

Host name

Host ID

Host IP Address

Secondary Director

IOS IDS

Sensor / IDSM

- 如此示例所显示，接受计算机种类的默认设置，并且其次单击。

Use this dialog box to define the type of machine you are adding.

Please remember that in order for connectivity to be established, the remote machine must already know the IDs and IP address of this Director. For Sensors, this is accomplished at install time by running `sysconfig-sensor`. For remote (secondary) Directors, this is accomplished by running `nrConfigure` on the remote machine and modifying the `hosts` and `routes` System Files accordingly.

Initialize a newly installed Sensor

Connect to a previously configured Sensor

Forward alarms to a secondary Director

- 如果值是可接受，请更改日志并且避开分钟或者留下他们作为默认。更改网络接口名字对您的探测接口名称。在本例中可以是"spwr0"或别的根据传感器类型，并且的它是"iprb0."您如何连接您的传感器。

Use this dialog box to set the time in minutes for automatic logging and shunning, the name of the Sensor network interface performing packet capture, and the addresses and netmasks of networks protected by the Sensor.

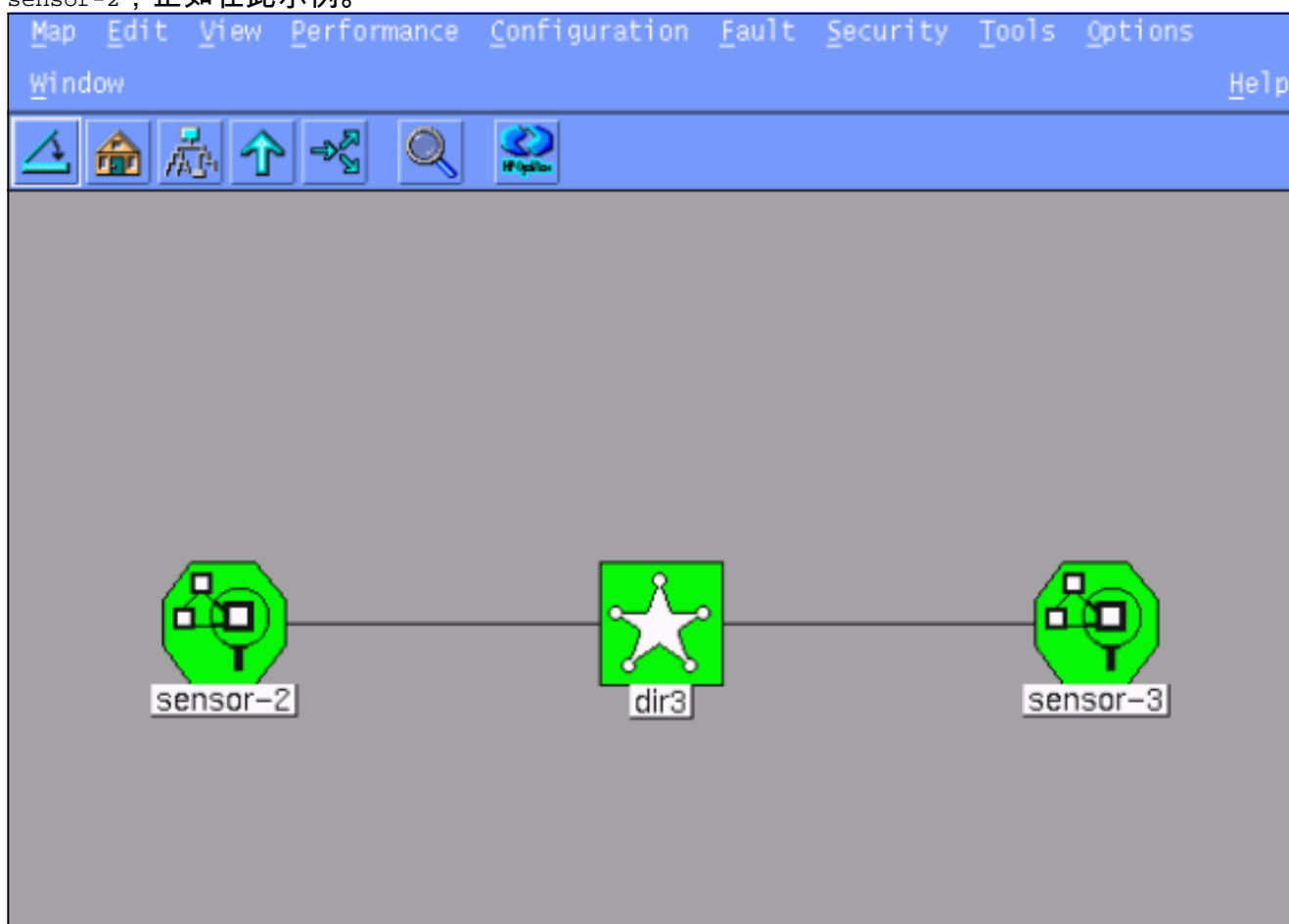
Number of minutes to log on an event.

Number of minutes to shun on an event.

Network Interface Name

Sensor Protected Networks

8. 其次请单击，直到有选项点击芬通社。您成功地添加传感器到导向器。从主菜单，您应该看到 sensor-2，正如在此示例。



[配置Cisco IOS路由器的避开](#)

完成这些步骤配置Cisco IOS路由器的避开。

1. 在主菜单，请选择Security > Configure。

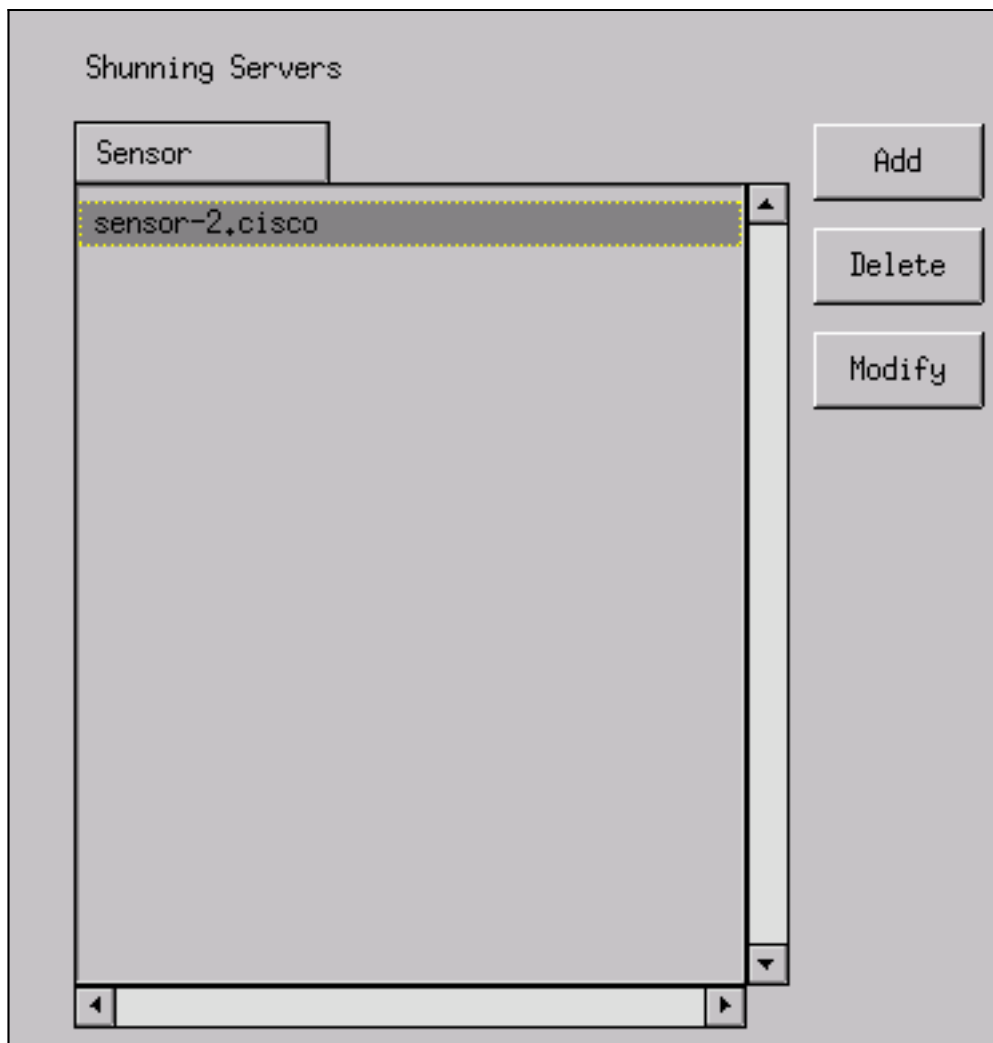
2. 在配置文件管理工具中，点击**sensor-2**并双击它。
3. 打开**设备管理**。
4. 如此示例所显示，点击**Devices > Add**，并且输入信息。单击 **OK** 继续。Telnet和特权密码匹配什么在路由器“议院”。

IP Address	10.64.10.45	User Name	
Device Type	Cisco Router[Including Cat5kRSM,Cat6kMSFC]	Password	*****
Sensor's NAT IP Address		Enable Password	*****
<input type="checkbox"/> Enable SSH			

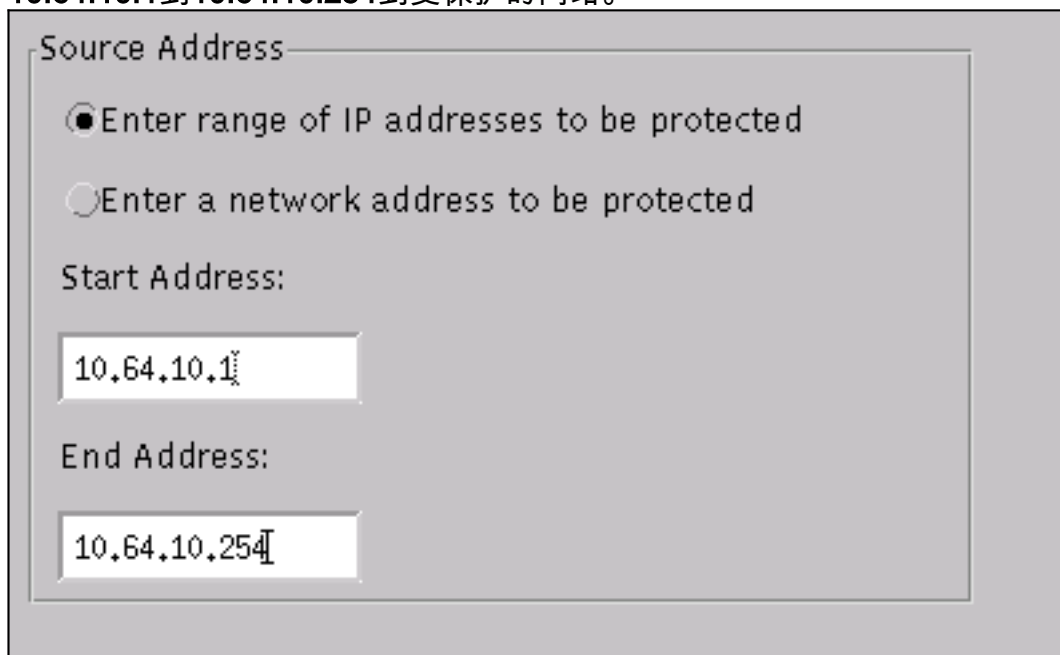
5. 点击**接口>Add**，输入此信息，并且点击**OK**键继续。

IP Address	10.64.10.45	PostShun ACL Name	198
PreShun ACL Name	199	Interface Name	FastEthernet0/0
		Direction	in

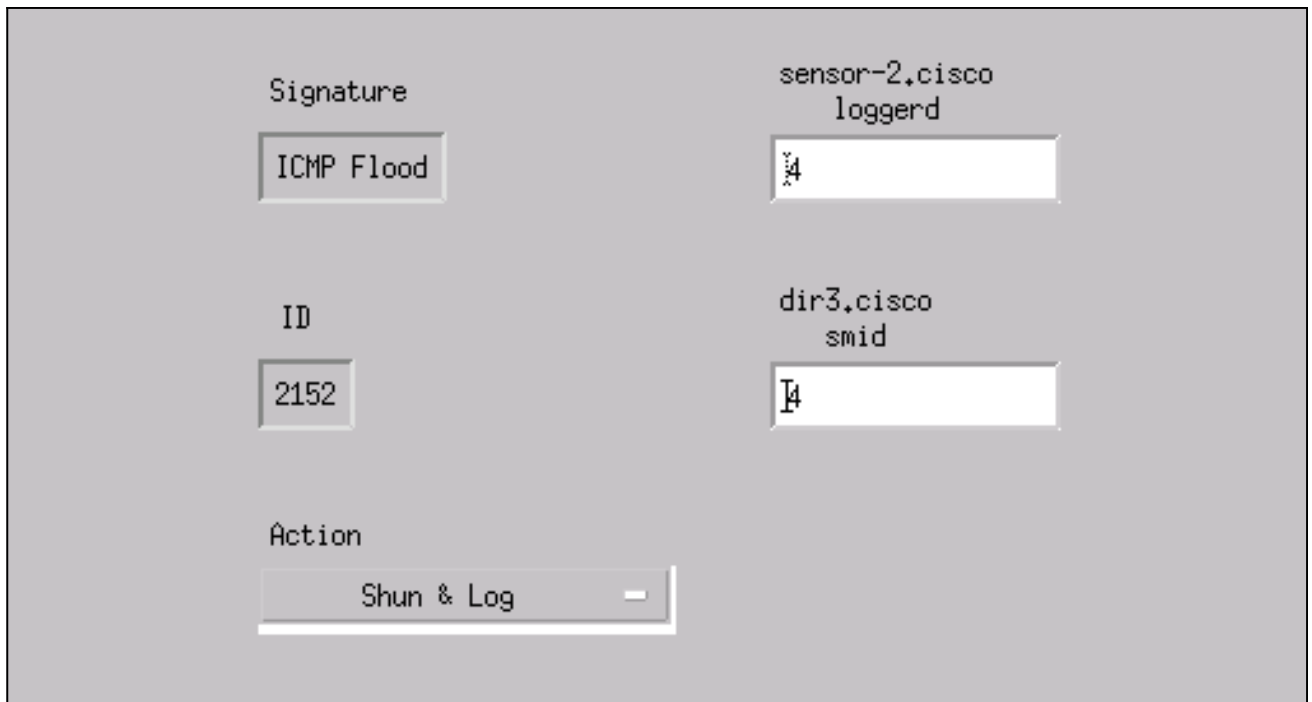
6. 点击**Shunning > Add**并且选择**sensor-2.cisco**作为避开服务器。当你完成的时候，请关上**Device Management**窗口。



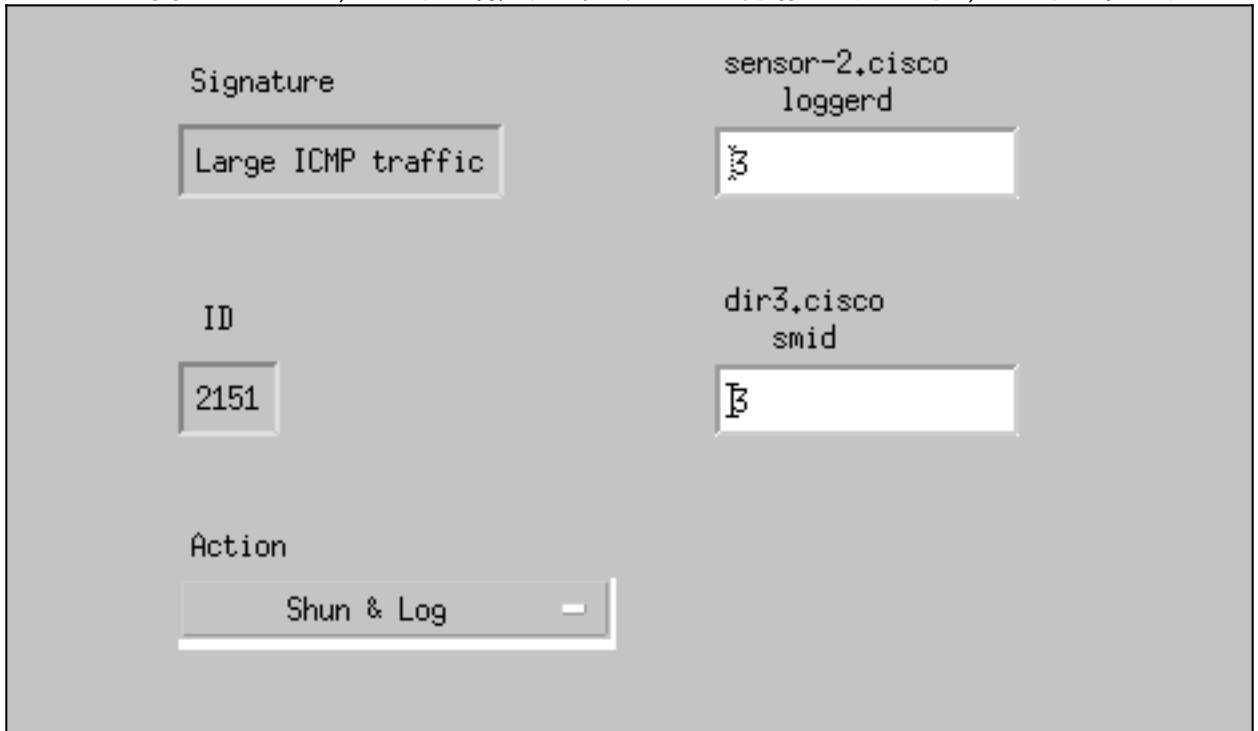
7. 打开Intrusion Detection Window，并且点击**受保护的**网络。如此示例所显示，添加范围**10.64.10.1**到**10.64.10.254**到受保护的**网络**。



8. 点击**配置文件>手动配置**。
9. 选择**修改签名>大ICMP流量**有ID 2151。
10. 点击**修改**，更改从**无的操作避开&记录**，并且点击OK键继续。

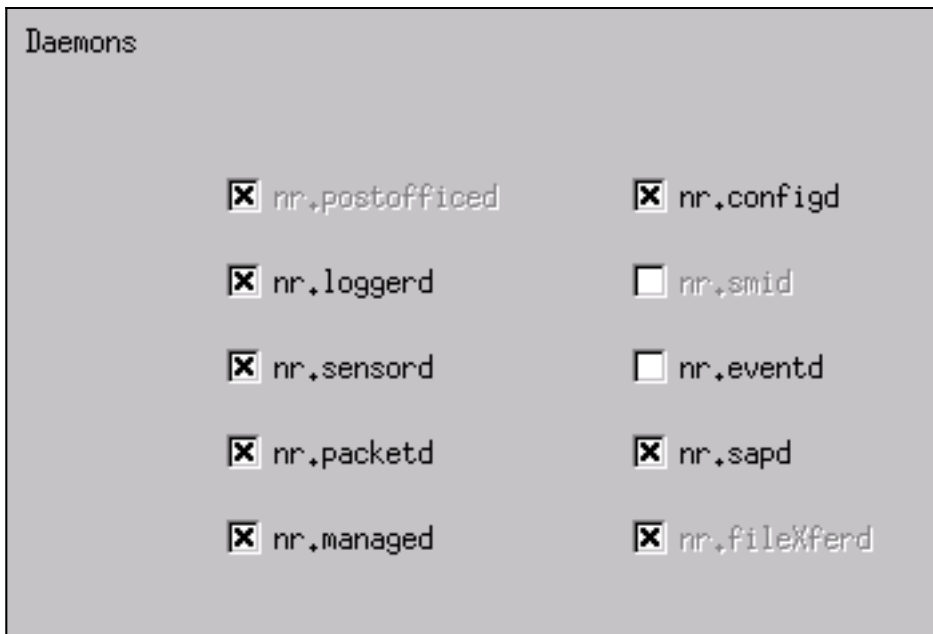


11. 选择ICMP溢出有ID 2152，并且点击**修改**。更改从**无**的**操作避开&记录**，并且点击OK键继续

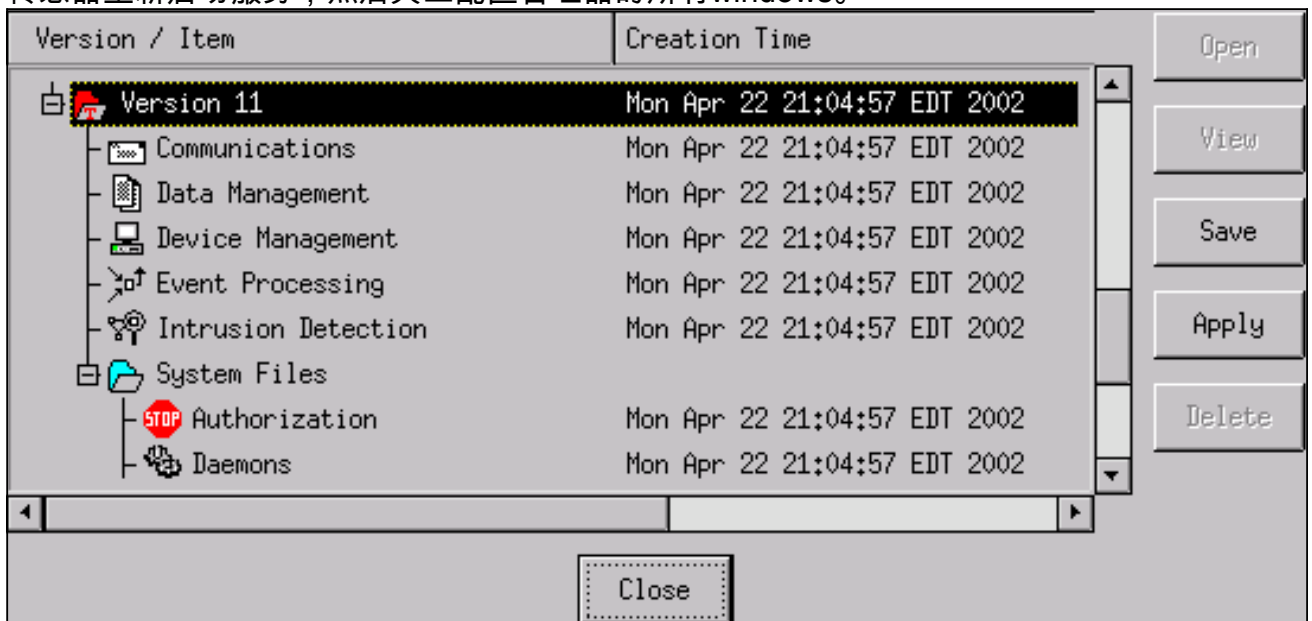


12. 点击OK键关上Intrusion Detection Window。

13. 打开系统文件文件夹，并且打开Daemons窗口。确保您启用这些守护程序



14. 点击OK键继续，选择刚刚被修改的版本，并且点击“Save”然后应用。等待系统告诉您完成的传感器重新启动服务，然后关上配置管理器的所有windows。



验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 `show` 命令，使用此工具可以查看对 `show` 命令输出的分析。

- `show access-list` -在路由器配置里列出`access-list`命令语句。它也列出在一`access-list`命令搜索期间，指示的命中数计数次数元素匹配。
- `ping` -用于诊断基本网络连接。

在攻击前启动

在攻击启动前，请发出这些命令。

```
house#show access-list Extended IP access list IDS_FastEthernet0/0_in_1 permit ip host
10.64.10.49 any permit ip any any (12 matches) house# light#ping 10.64.10.45 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 10.64.10.45, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms light#
```

发起攻击和规避

发起您的来自路由器“灯”的攻击对受害者“议院”。当ACL采取影响时，不可达的被看到。

```
light#ping Protocol [ip]: Target IP address: 10.64.10.45 Repeat count [5]: 1000000 Datagram size
[100]: 18000 Timeout in seconds [2]: Extended commands [n]: Sweep range of sizes [n]: Type
escape sequence to abort. Sending 1000000, 18000-byte ICMP Echos to 10.64.10.45, timeout is 2
seconds: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.U.
```

一旦传感器检测攻击，并且ACL下载和此输出显示在“议院”。

```
house#show access-list Extended IP access list IDS_FastEthernet0/0_in_0 permit ip host
10.64.10.49 any deny ip host 100.100.100.2 any (459 matches) permit ip any any
如此示例所显示，不可达的在“灯仍然被看到”。
```

```
Light#ping 10.64.10.45 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
10.64.10.45, timeout is 2 seconds: U.U.U Success rate is 0 percent (0/5)
因为避开设置为15分钟，十五分钟后，“议院”回到正常。
```

```
House#show access-list Extended IP access list IDS_FastEthernet0/0_in_1 permit ip host
10.64.10.49 any permit ip any any (12 matches) house#
“灯”能ping “议院”。
```

```
Light#ping 10.64.10.45 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
10.64.10.45, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/1/4 ms
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [Cisco Secure入侵防御支持页面](#)
- [技术支持和文档 - Cisco Systems](#)