

# 在UNIX Director上設定Shunning

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[攻擊發起之前](#)

[發動攻擊和迴避](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

Cisco Intrusion Detection System(IDS)Director和Sensor可用於管理規避的Cisco路由器。在本文檔中，感測器(sensor-2)被配置為檢測對路由器「House」的攻擊，並將此資訊傳遞給導向器「dir3」。配置後，從路由器「Light」發起攻擊 ( ping大於1024位元組，即特徵碼2151，以及網際網路控制消息協定[ICMP]泛洪，即特徵碼2152 )。感測器檢測到攻擊並將此資訊傳送給導向器。訪問控制清單(ACL)會下載到路由器以避免來自攻擊者的流量。在攻擊者主機上顯示，而在受害者上則顯示下載的ACL。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- 安裝感測器並確保其正常工作。
- 確保監聽介面跨越到路由器的外部介面。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IDS導向器2.2.3
- Cisco IDS感應器3.0.5

- 採用12.2.6的Cisco IOS® 路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

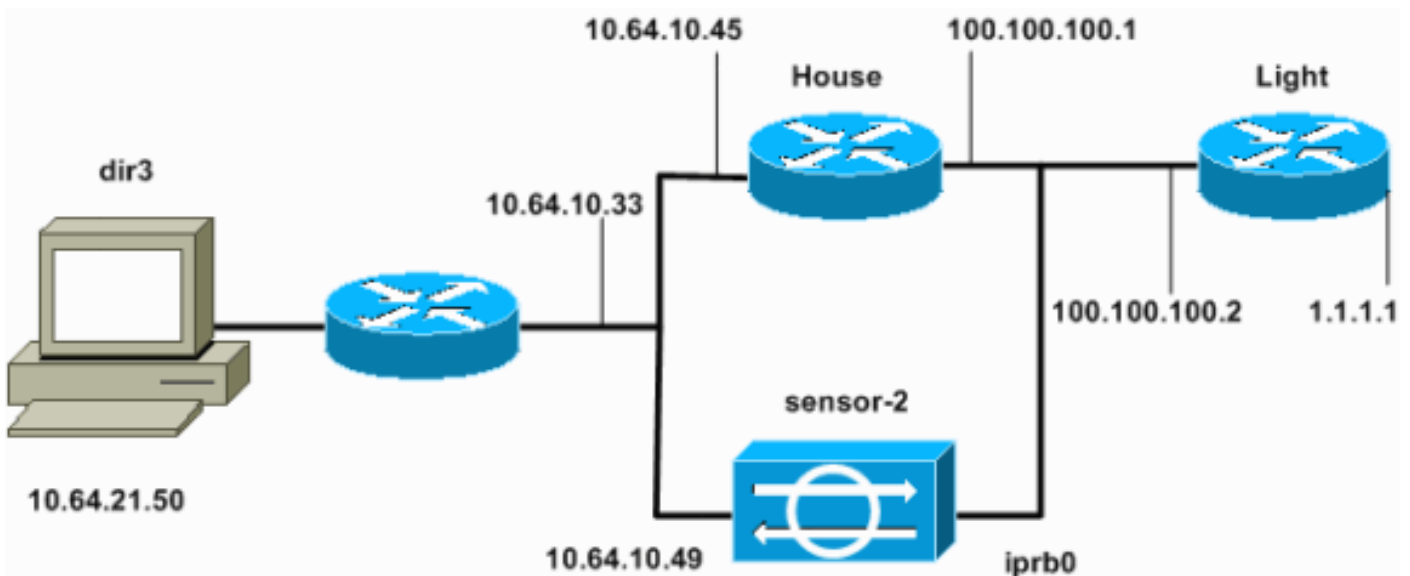
## 設定

本節提供用於設定本文件中所述功能的資訊。

**注意：**要查詢有關本文檔中使用的命令的其他資訊，請使用[命令查詢工具](#)（[僅限註冊客戶](#)）。

## 網路圖表

本檔案會使用下圖中所示的網路設定。



## 組態

本檔案會使用這些設定。

- [路由器指示燈](#)
- [路由器外殼](#)

### 路由器指示燈

```
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
```

## 路由器外壳

```
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#
```

## 配置感測器

完成以下步驟以配置感測器。

1. Telnet至10.64.10.49，使用使用者名稱root和密碼攻擊。
2. 輸入sysconfig-sensor。
3. 出現提示時，輸入配置資訊，如本例所示。

```
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. 出現提示時，儲存配置並允許感測器重新啟動。

## 將感測器新增到指揮交換機中

完成以下步驟，將感測器新增到Director。

1. Telnet至10.64.21.50，使用使用者名稱netrangr和密碼攻擊。
2. 輸入ovw&以啟動HP OpenView。
3. 在主選單中，選擇Security > Configure。
4. 在配置檔案管理實用程式中，選擇檔案>新增主機，然後按一下下一步。
5. 這是一個如何填寫請求資訊的示例。

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

6. 接受機器型別的預設設定，然後按一下**Next**，如下例所示。

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

7. 更改日誌和迴避分鐘數，或在值可接受的情況下將其保留為預設值。將網路介面名稱更改為監聽介面的名稱。在本示例中，它是「`iprb0`」。它可能是「`spwr0`」或其它任何型別，具體取決於感測器型別和連線方式。

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.

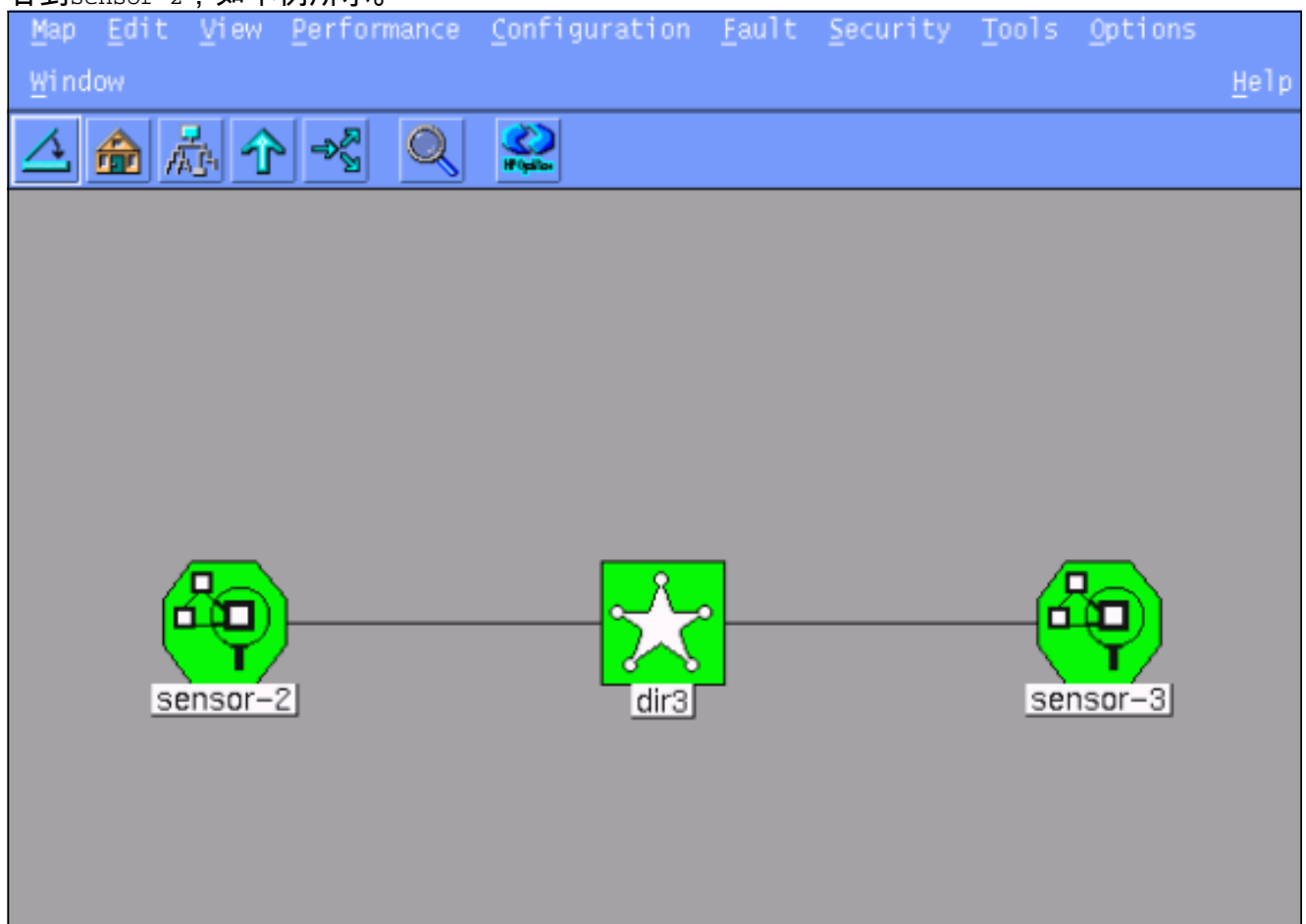
Number of minutes to log on an event.

Number of minutes to shun on an event.

Network Interface Name

Sensor Protected Networks

8. 按一下**Next**，直到有選項可按一下**Finish**。您已成功將感測器新增到Director。從主選單中應該看到sensor-2，如本例所示。

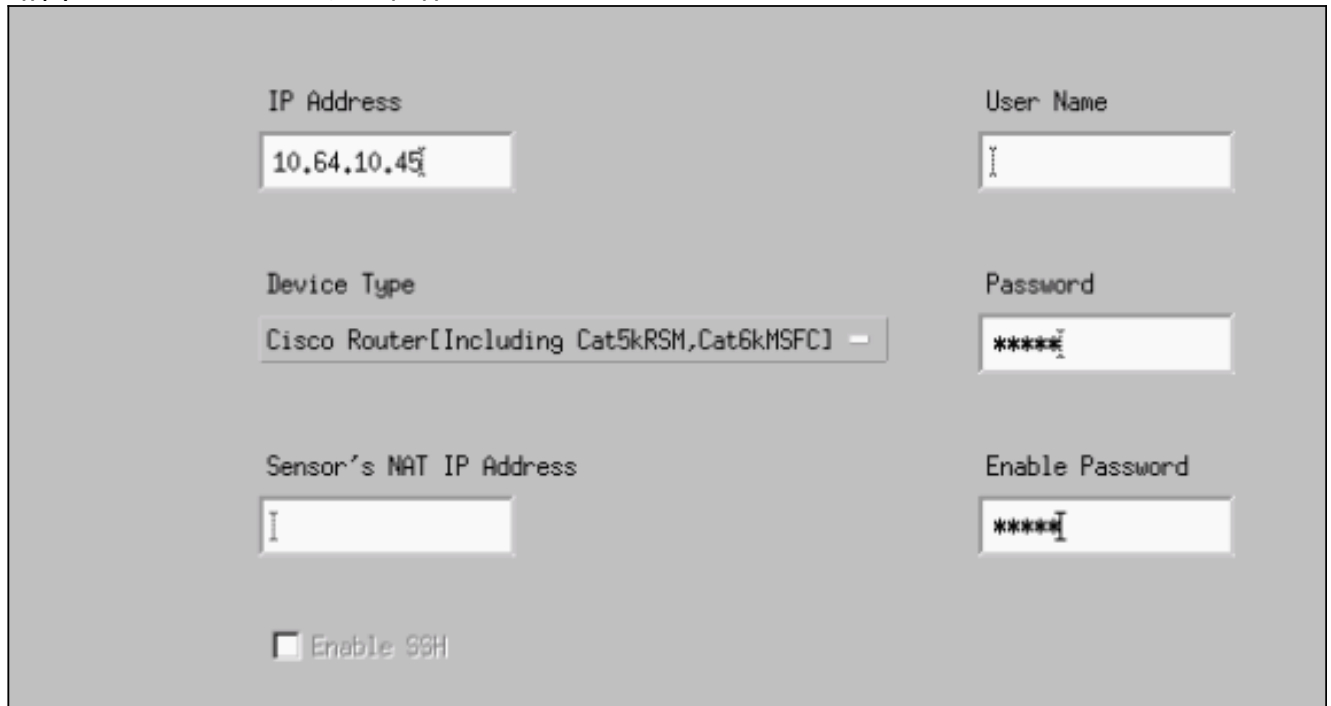


### [配置Cisco IOS路由器的迴避](#)

完成以下步驟以配置Cisco IOS路由器的迴避。

1. 在主選單中，選擇**Security > Configure**。

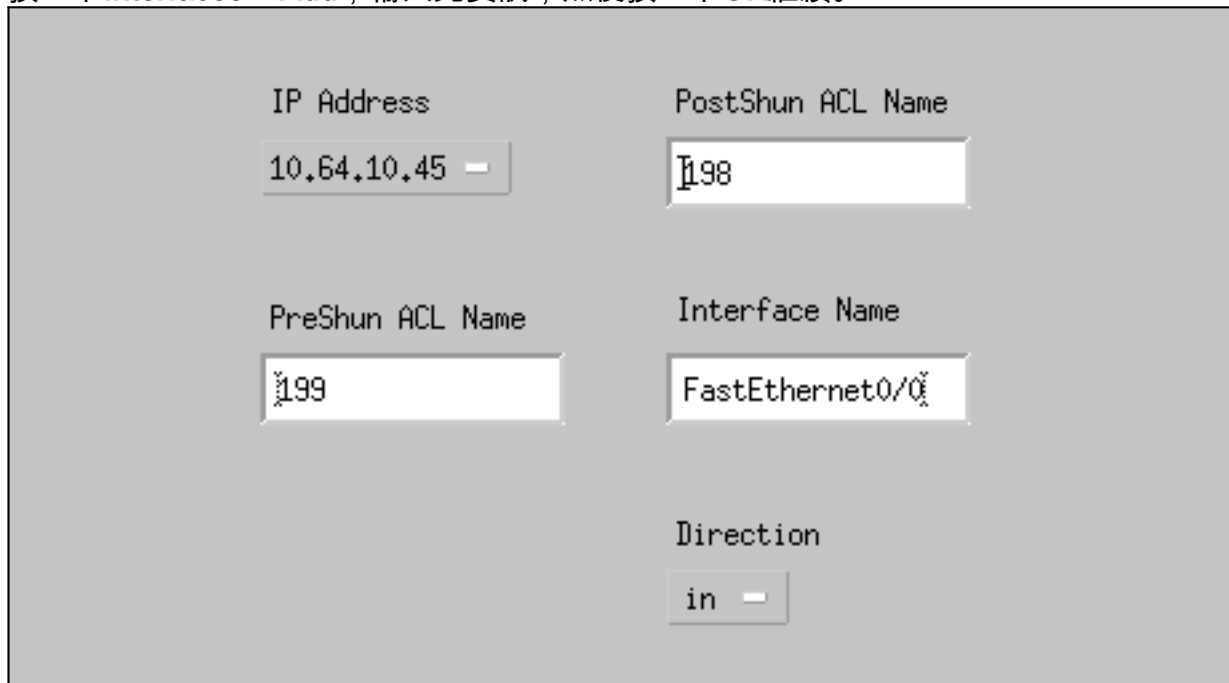
- 在「Configuration File Management Utility ( 配置檔案管理實用程式 )」中，選中**sensor-2**，然後按兩下它。
- 開啟**Device Management**。
- 按一下**Devices > Add**，然後輸入如本範例所示的資訊。按一下**OK**繼續。Telnet和啟用密碼與路由器「House」中的密碼匹配。



The screenshot shows a configuration form for adding a device. The fields are as follows:

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 99H			

- 按一下**Interfaces > Add**，輸入此資訊，然後按一下**OK**繼續。

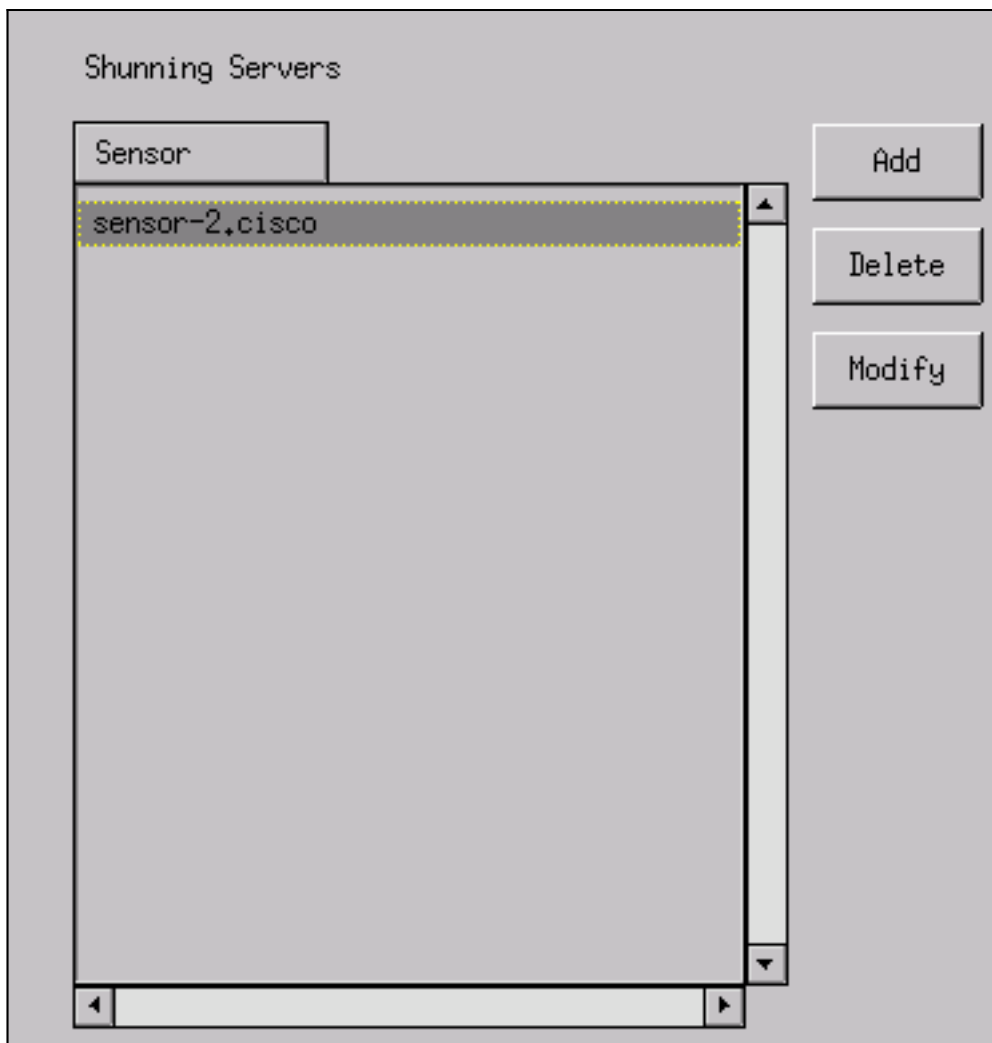


The screenshot shows a configuration form for adding an interface. The fields are as follows:

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

- 按一下**Shunning > Add**，然後選擇**sensor-2.cisco**作為迴避伺服器。完成後，關閉「裝置管理





」視窗。

7. 開啟Intrusion Detection視窗，然後按一下**Protected Networks**。將範圍**10.64.10.1**到**10.64.10.254**新增到受保護網路中，如本例所示。

Source Address

Enter range of IP addresses to be protected

Enter a network address to be protected

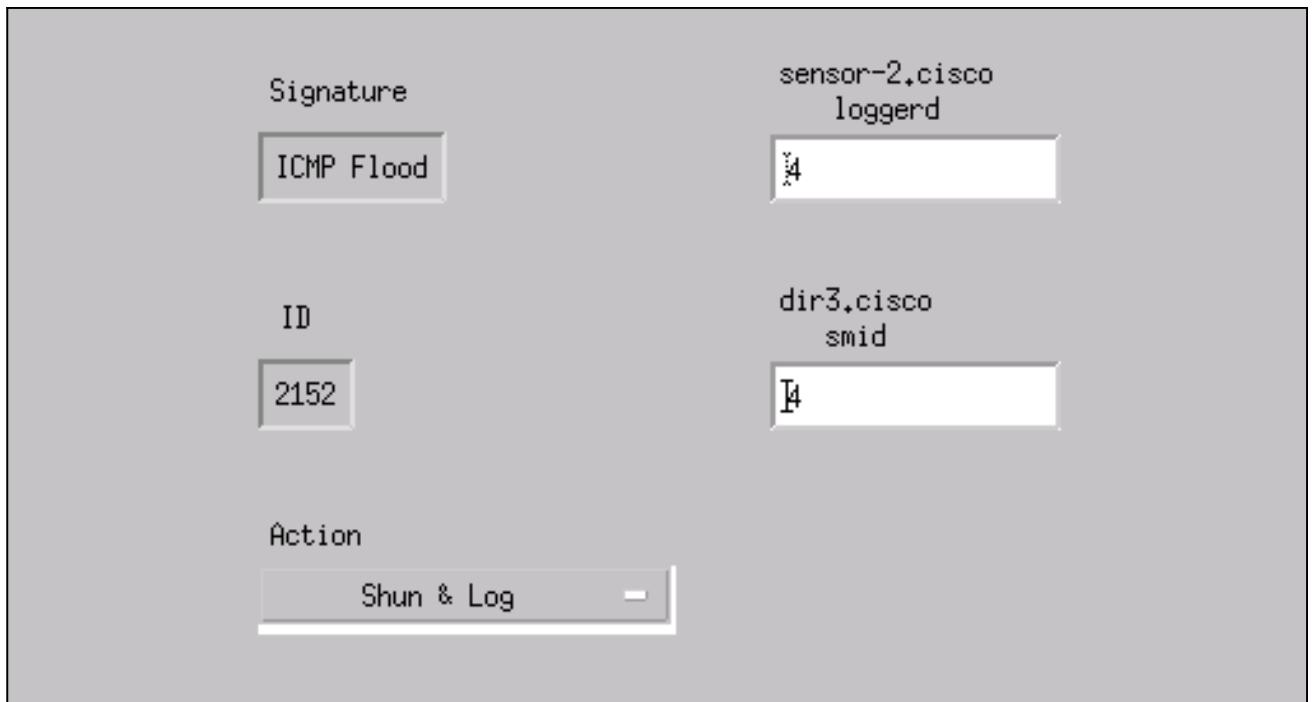
Start Address:

10.64.10.1

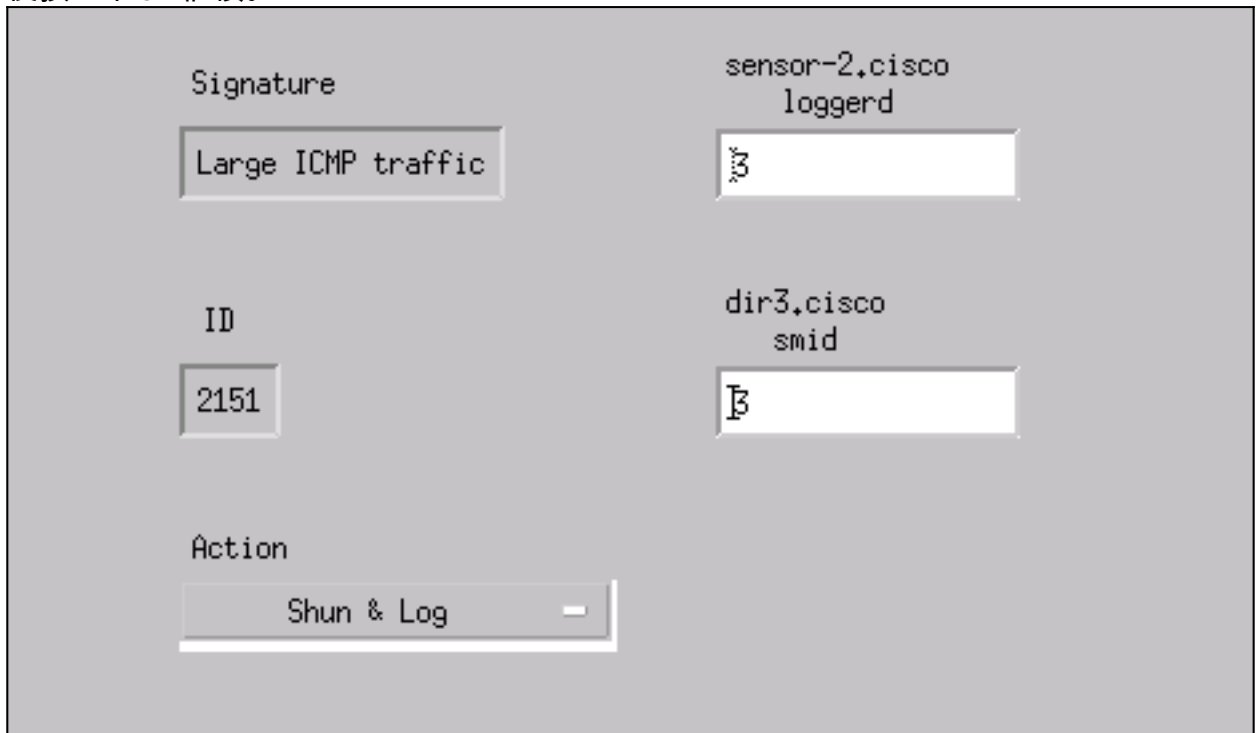
End Address:

10.64.10.254

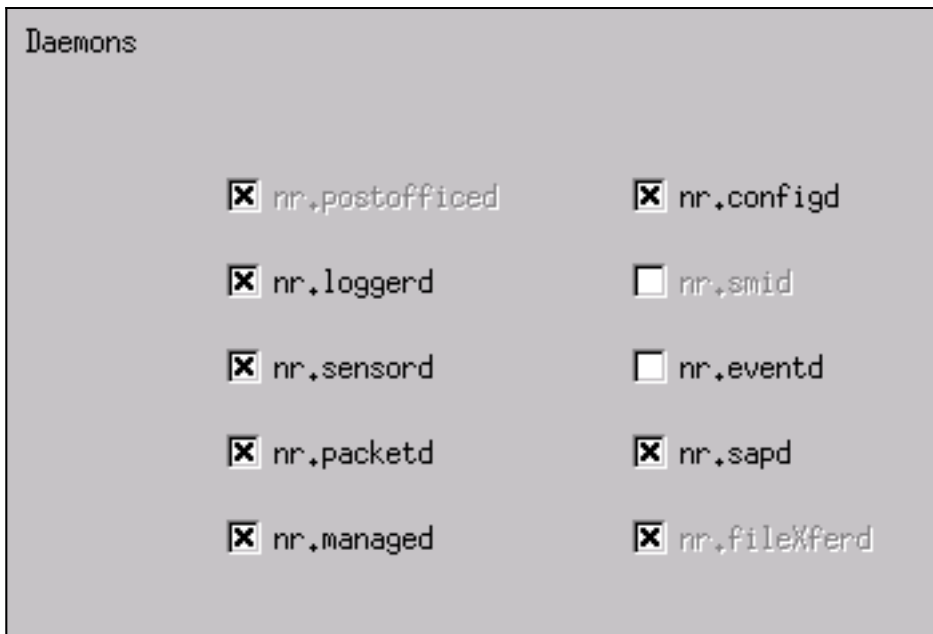
8. 按一下**Profile > Manual Configuration**。
9. 選擇**Modify Signatures > Large ICMP Traffic**(修改ID為2151的簽名)。
10. 按一下**Modify**，將Action從None更改為**Shun & Log**，然後按一下**OK**繼續。



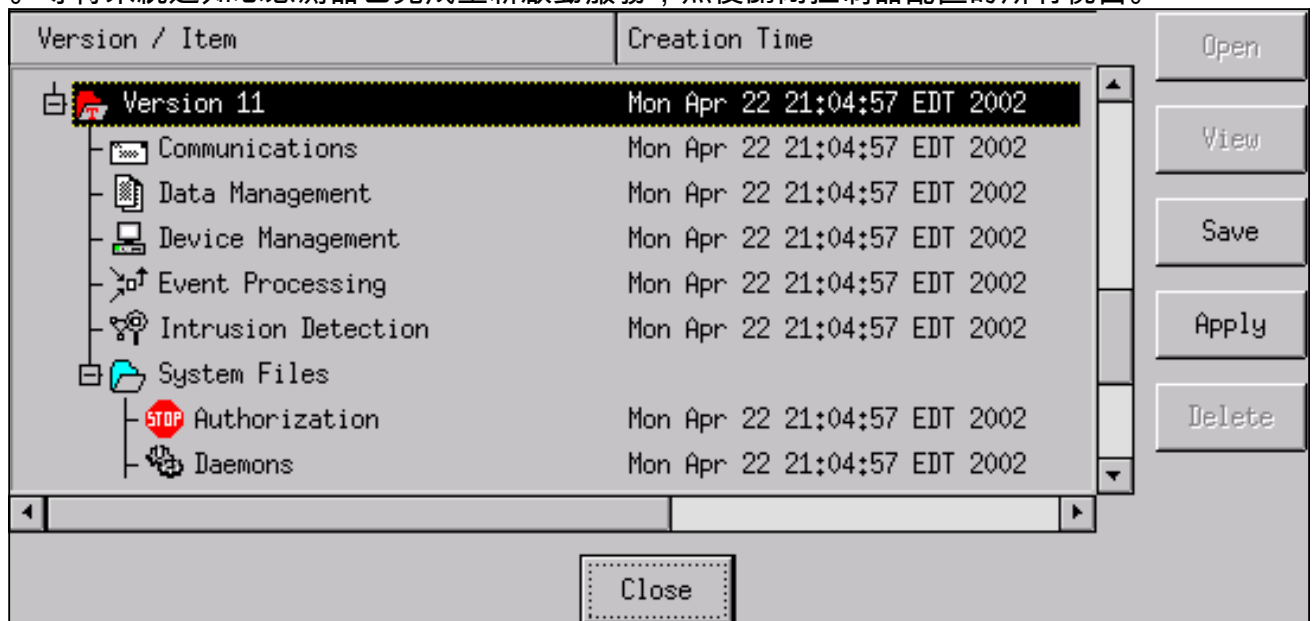
11. 選擇ID為2152的ICMP Flood，然後按一下Modify。將Action從None更改為Shun & Log，然後按一下OK繼續。



12. 按一下OK關閉Intrusion Detection視窗。
13. 開啟[系統檔案]資料夾，然後開啟[守護程式]視窗。請確保已啟用以下守護程式



14. 按一下「OK」以繼續，選擇剛才修改的版本，然後按一下「Save」，然後按一下「Apply」。等待系統通知您感測器已完成重新啟動服務，然後關閉控制器配置的所有視窗。



## 驗證

本節提供的資訊可用於確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- **show access-list** -列出路由器組態中的access-list命令語句。它還列出一個命中計數，它指示在access-list命令搜尋期間元素已匹配的次數。
- **ping** — 用於診斷基本網路連線。

## 攻擊發起之前

發動攻擊之前，請發出以下命令。

```

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#

```

## 發動攻擊和迴避

從路由器「Light」向受害者「House」發起攻擊。當ACL生效時，將會看到無法到達的專案。

```

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.

```

感測器檢測到攻擊後，即會下載ACL，此輸出將顯示在「House」上。

```

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

```

「Light」上仍會顯示無法到達的專案，如本例所示。

```

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)

```

15分鐘後，「房子」恢復正常，因為迴避被設定為15分鐘。

```

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」可以ping「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
```

## [疑難排解](#)

目前尚無適用於此組態的具體疑難排解資訊。

## [相關資訊](#)

- [思科安全入侵防禦支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)