

使用IDS Director配置TCP重置

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[配置感測器](#)

[將感測器新增到指揮交換機中](#)

[為Cisco IOS路由器配置TCP重置](#)

[啟動攻擊和TCP重置](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文描述如何配置入侵檢測系統 (IDS, 以前稱為NetRanger) 導向器和感測器, 以便在嘗試的Telnet中傳送TCP重置, 如果傳送的字串是「testattack」, 則這些重置將包含受管路由器。

必要條件

需求

考慮此配置時, 請記住:

- 執行此配置之前, 請安裝感測器並驗證其是否正常工作。
- 確保監聽介面跨越到受管路由器的外部介面。

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
- 執行軟件版本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](#)。

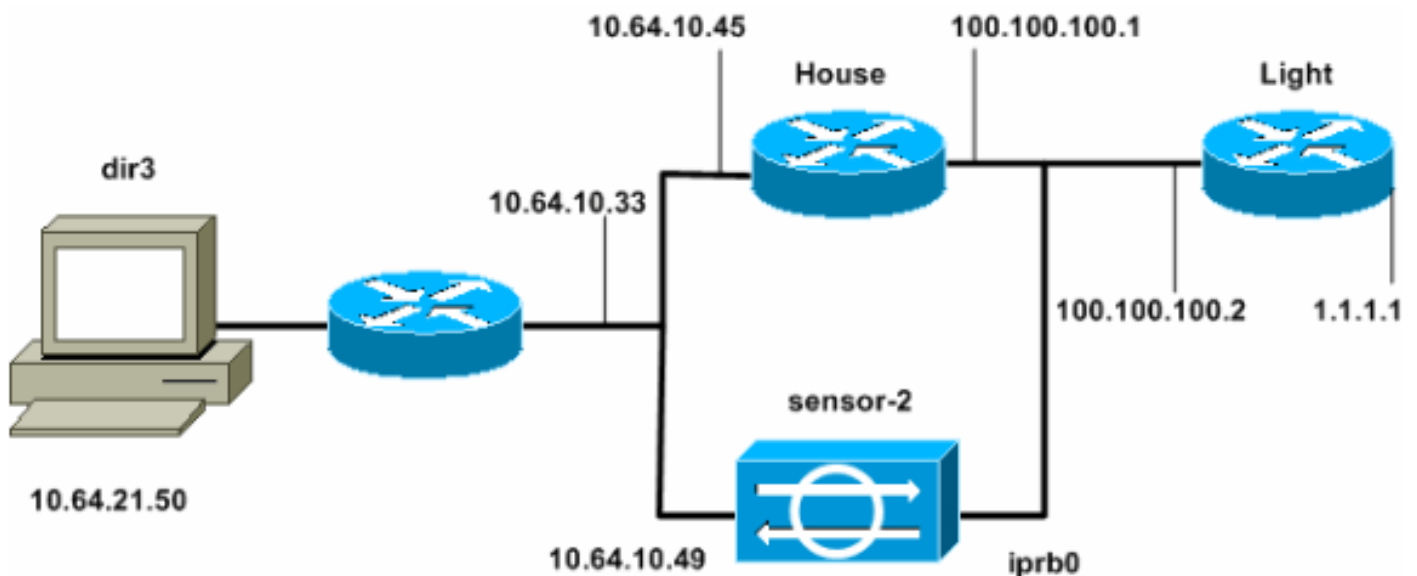
設定

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
!
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
  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#
```

配置感測器

完成以下步驟以配置感測器。

1. 使用使用者名稱root和密碼攻擊Telnet至10.64.10.49 (IDS感測器)。

2. 鍵入sysconfig-sensor。

3. 出現提示時，輸入組態資訊，如以下範例所示：

```
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. 使用使用者名稱netrangr和密碼攻擊Telnet至10.64.21.50(IDS Director)。

2. 鍵入ovw&以啟動HP OpenView。

3. 從主選單，轉到安全>配置。

4. 在配置檔案管理實用程式中，轉至檔案>新增主機，然後按一下下一步。

5. 如本例所示，填寫感測器主機資訊。按「Next」(下一步)。

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. 接受電腦型別的預設設定，然後按一下**下一步**，如下例所示。

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

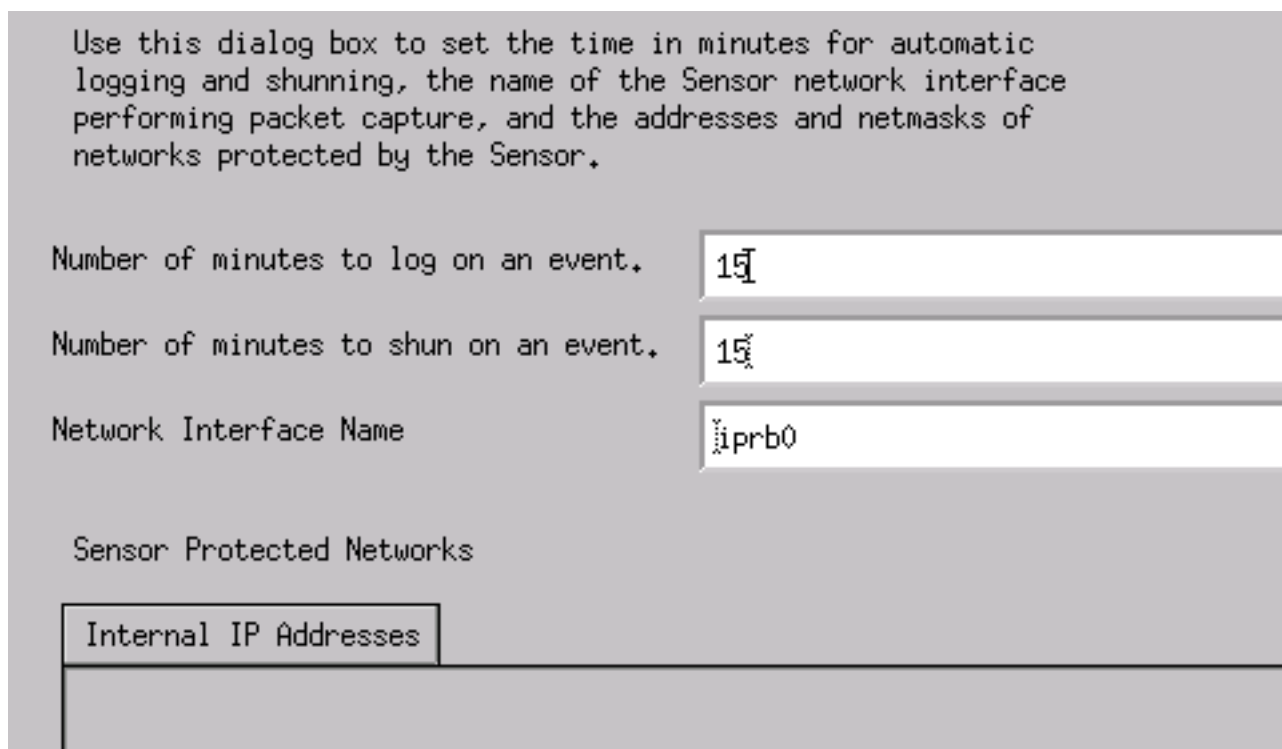
Please remember that in order for connectivity to be established, the remote machine must already know the IDs and IP address of this Director. For Sensors, this is accomplished at install time by running `sysconfig-sensor`. For remote (secondary) Directors, this is accomplished by running `nrConfigure`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

Initialize a newly installed Sensor

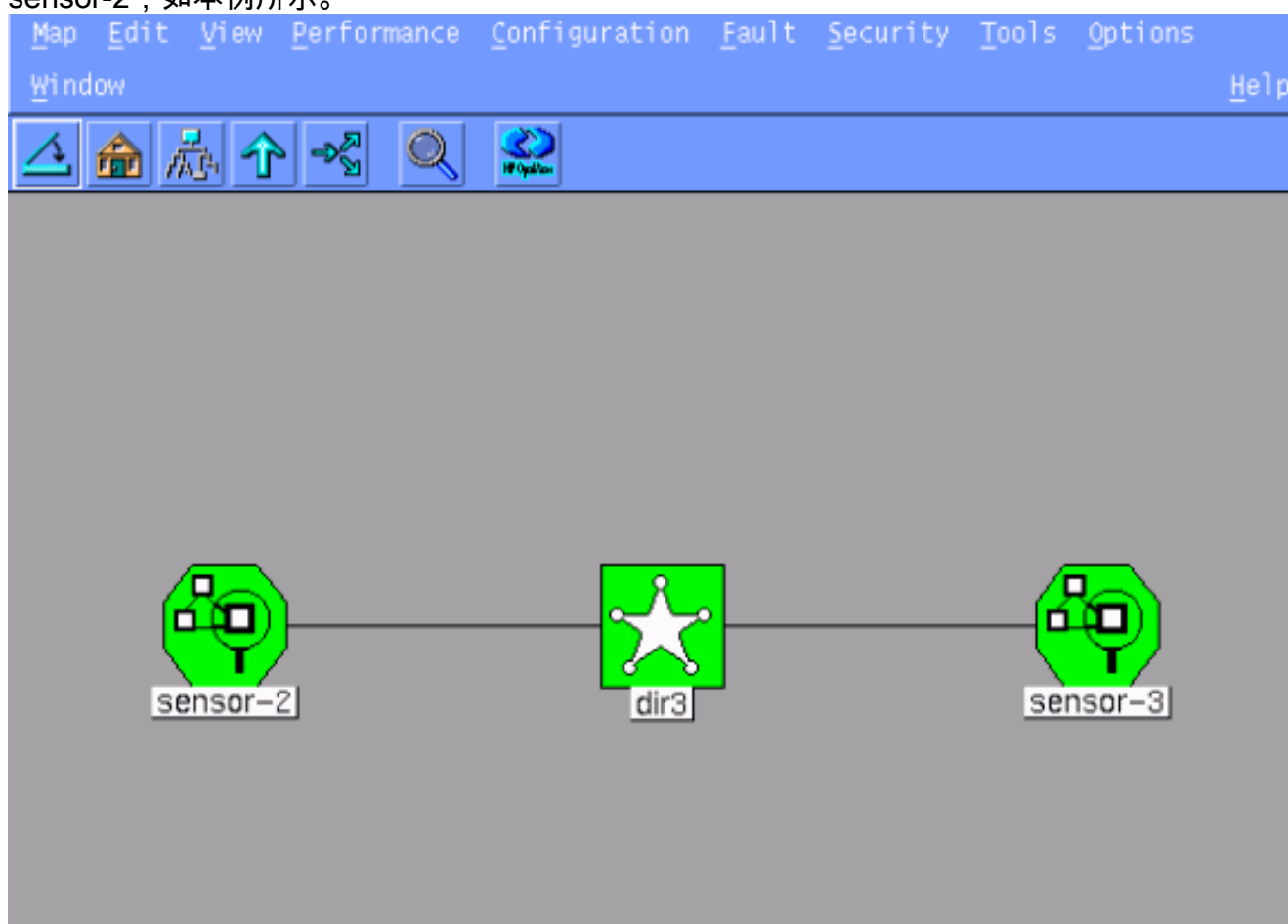
Connect to a previously configured Sensor

Forward alarms to a secondary Director

7. 您可以更改日誌和迴避分鐘數，也可以接受預設值。但是，您必須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。



- 繼續按一下**Next**，然後按一下**Finish**將感測器新增到Director。現在，您應該從主選單中看到sensor-2，如本例所示。



[為Cisco IOS路由器配置TCP重置](#)

完成以下步驟，為Cisco IOS路由器配置TCP重置。

- 在「Main Menu (主選單)」中，轉至**Security > Configure**。

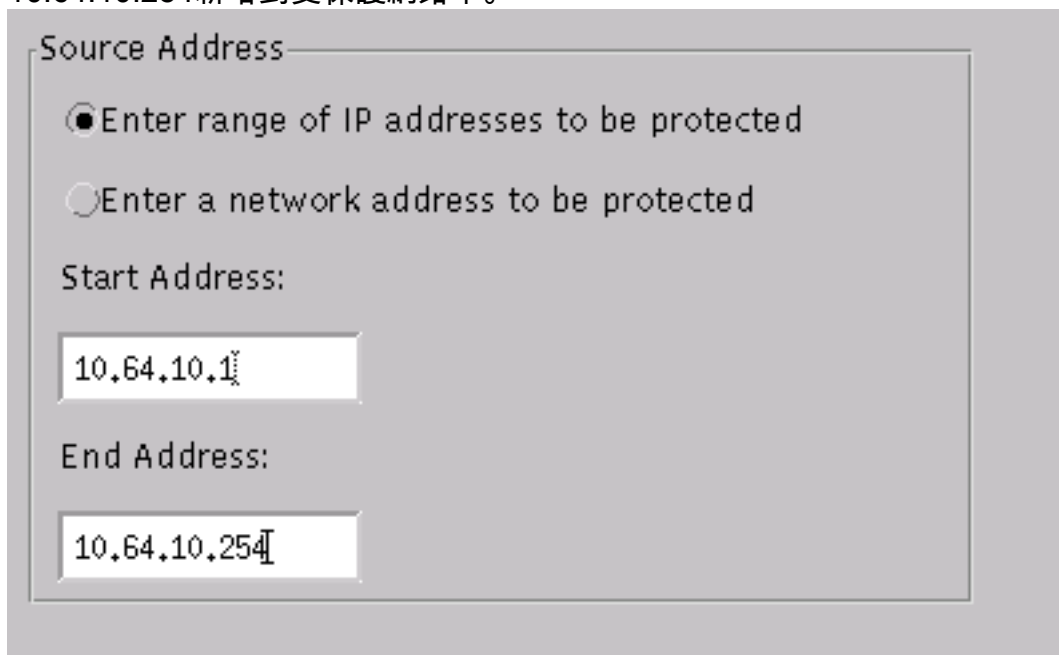
2. 在「Configuration File Management Utility (配置檔案管理實用程式)」中，選中**sensor-2**，然後按兩下它。
3. 開啟裝置管理。
4. 按一下「**Devices > Add**」。輸入裝置資訊，如下例所示。按一下**OK**繼續。Telnet口令和啟用口令均為Cisco。



The screenshot shows a configuration form for adding a device. It has the following fields and values:

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

5. 開啟Intrusion Detection視窗，然後按一下**Protected Networks**。將地址範圍10.64.10.1到10.64.10.254新增到受保護網路中。



The screenshot shows the 'Protected Networks' configuration window. It has the following fields and values:

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

6. 按一下「**Profile**」，然後選擇「**Manual Configuration**」。接下來，按一下**Modify Signatures**。選擇ID為8000的**匹配字串**。按一下**Expand > Add**新增名為**testattack**的新字串。輸入字串資訊 (如本例所示)，然後按一下**OK**繼續。

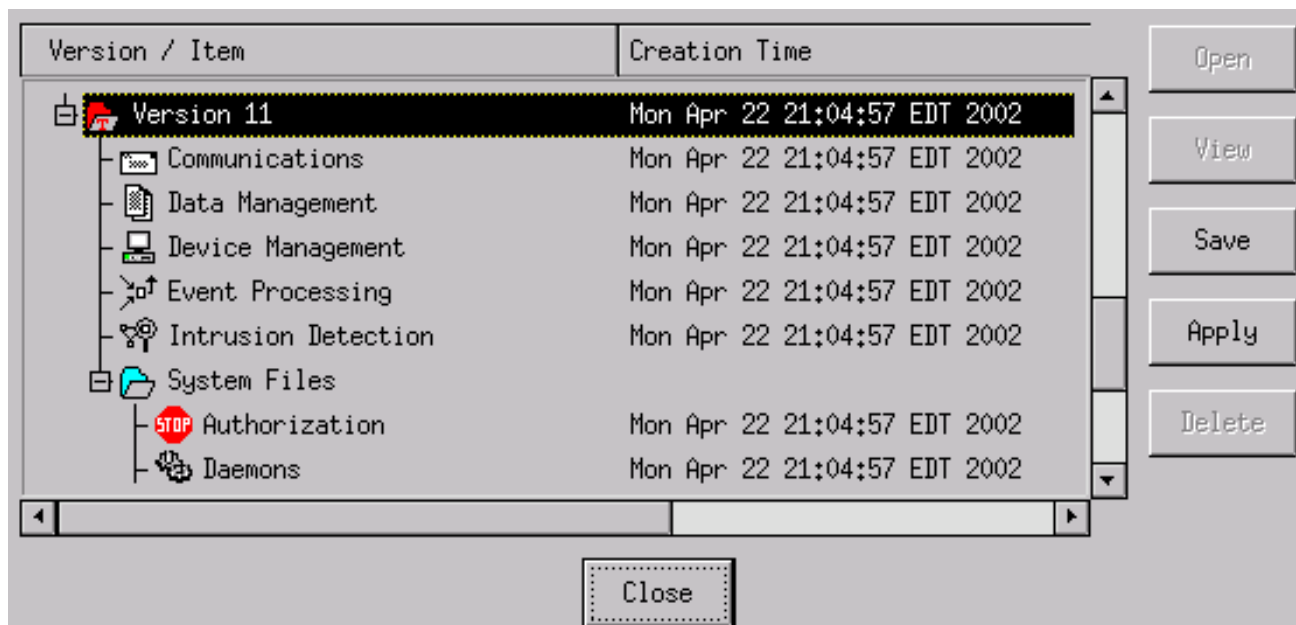
String	Occurrences
testattack	1
ID	Action
51304	TCP Reset
Port	sensor-2.cisco loggerd
23	5
Direction	dir3.cisco smid
To & From	5

7. 您已完成此部分的配置。按一下**OK**關閉Intrusion Detection視窗。
8. 開啟System Files資料夾，然後開啟Daemons視窗。確保啟用以下守護程式：

Daemons

<input checked="" type="checkbox"/> nr.postofficed	<input checked="" type="checkbox"/> nr.configd
<input checked="" type="checkbox"/> nr.loggerd	<input type="checkbox"/> nr.smid
<input checked="" type="checkbox"/> nr.sensord	<input type="checkbox"/> nr.eventd
<input checked="" type="checkbox"/> nr.packetd	<input checked="" type="checkbox"/> nr.sapd
<input checked="" type="checkbox"/> nr.managed	<input checked="" type="checkbox"/> nr.filexfend

9. 按一下**OK**繼續。
10. 選擇剛修改的版本，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。



啟動攻擊和TCP重置

從Router Light (路由器指示燈) Telnet至Router House , 然後鍵入testattack。只要按下Space或Enter鍵 , Telnet會話就會重置。您將連線到Router 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.
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

使用使用者名稱root和密碼攻擊,Telnet至感測器10.64.10.49。鍵入cd /usr/nr/etc。輸入cat packetd.conf。如果為testattack正確設定了TCP重設 , 您應該在Action Codes欄位中看到四(4)。這表示TCP重設 , 如以下範例所示。

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

如果在簽名中意外將操作設定為「無」 , 則在「操作代碼」欄位中將看到零(0)。這表示未執行本示

例中所示的操作。

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

TCP重置從感測器的監聽介面傳送。如果有交換機將感測器介面連線到受管路由器的外部介面，則在交換機中使用**set span** 命令配置時，請使用以下語法：

```
set span
```

```
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
```

[相關資訊](#)

- [社群與培訓](#)
- [思科安全入侵防禦支援頁面](#)