Configurazione del reset TCP con IDS Director

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazioni](#)
[Configurazione del sensore](#)
[Aggiungere il sensore al director](#)
[Configurazione del reset TCP per il router Cisco IOS](#)
[Avvia attacco e reimpostazione TCP](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare un director e un sensore Intrusion Detection System (IDS, in precedenza NetRanger) in modo che invii le reimpostazioni TCP su un tentativo Telnet a un intervallo di indirizzi che include il router gestito se la stringa inviata è "testattack".

Prerequisiti

Requisiti

Quando si prende in considerazione questa configurazione, ricordarsi di:

- Prima di eseguire la configurazione, installare il sensore e verificarne il corretto funzionamento.
- Accertarsi che l'interfaccia di sniffing si estenda sull'interfaccia esterna del router gestito.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IDS Director 2.2.3
- Cisco IDS Sensor 3.0.5
- Router Cisco IOS® con software release 12.2.6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

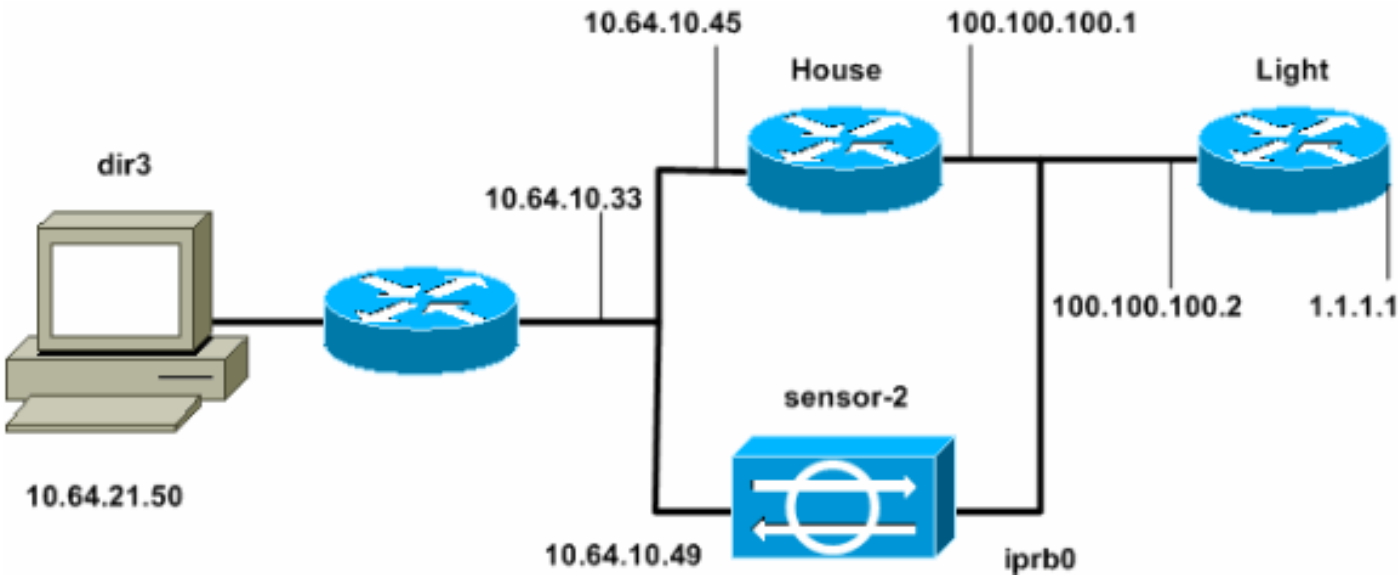
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate queste configurazioni.

- Luce router
- Router House

Luce router

```
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
```

Router 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#
```

Configurazione del sensore

Completare la procedura seguente per configurare il sensore.

1. Telnet su 10.64.10.49 (il sensore IDS) con il nome utente **root** e la password **attack**.
2. Digitare **sysconfig-sensor**.
3. Quando richiesto, immettere le informazioni di configurazione, come illustrato nell'esempio seguente:

```
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
```

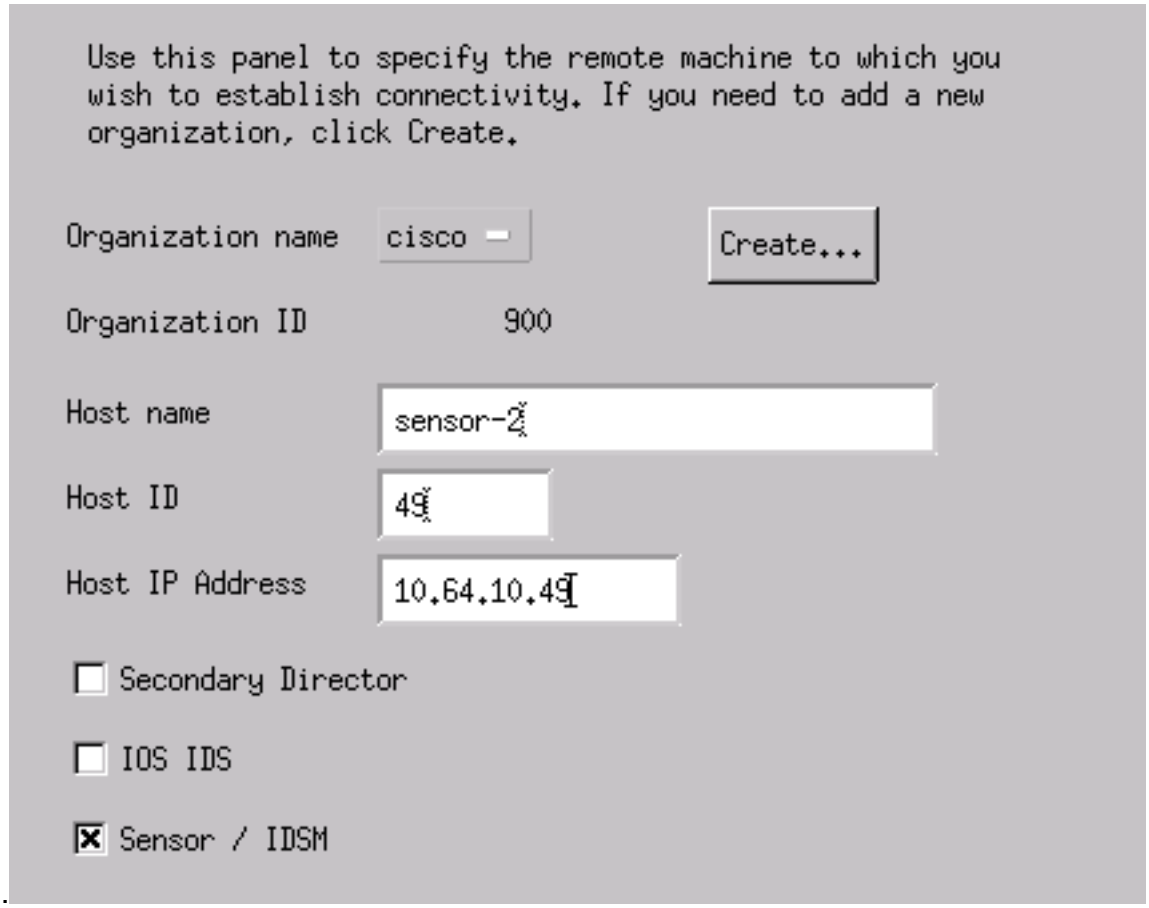
4. Quando richiesto, salvare la configurazione e consentire il riavvio del sensore.

Aggiungere il sensore al director

Completare questi passaggi per aggiungere il sensore al Director.

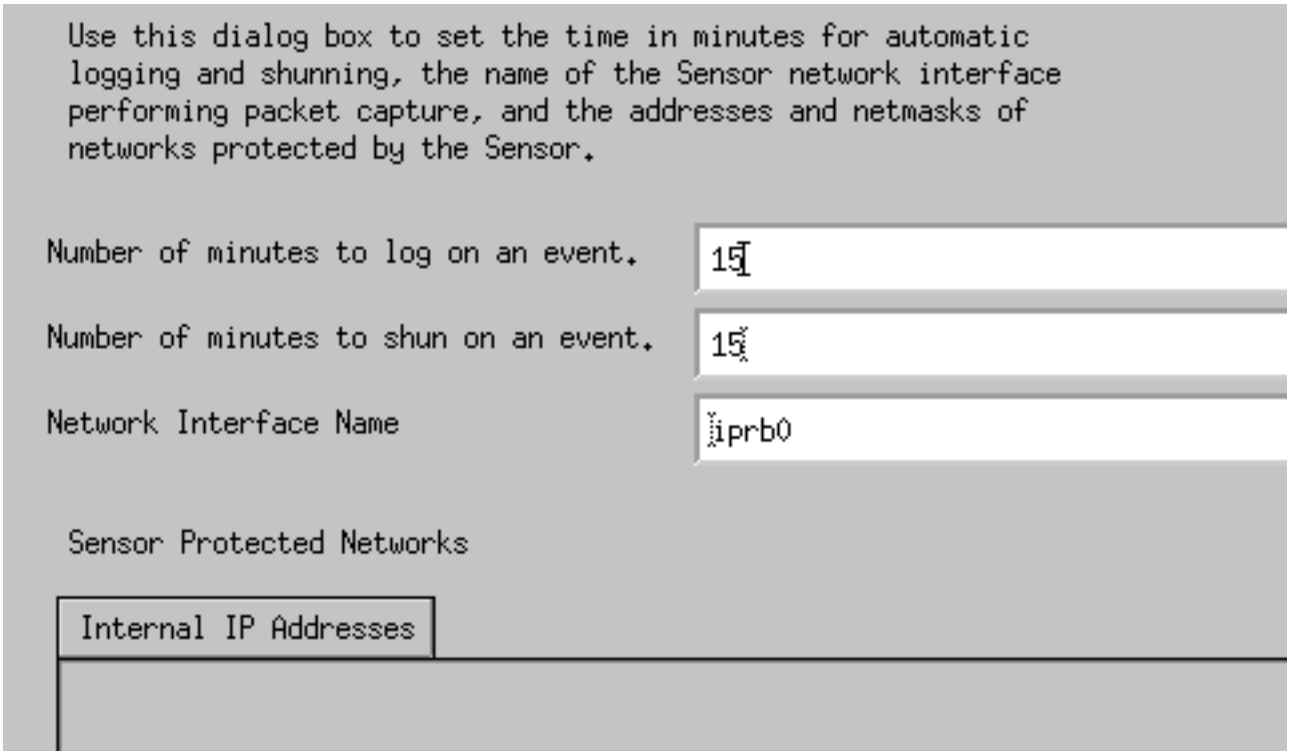
1. Telnet su 10.64.21.50 (il director IDS) con il nome utente **netranger** e la password di **attacco**.
2. Digitare **ovw&** per avviare HP OpenView.
3. Dal menu principale, selezionare **Protezione > Configura**.
4. In Configuration File Management Utility, selezionare **file > Aggiungi host**, quindi fare clic su **Avanti**.

5. Completare le informazioni sull'host del sensore, come mostrato nell'esempio. Fare clic su **Next** (Avanti).

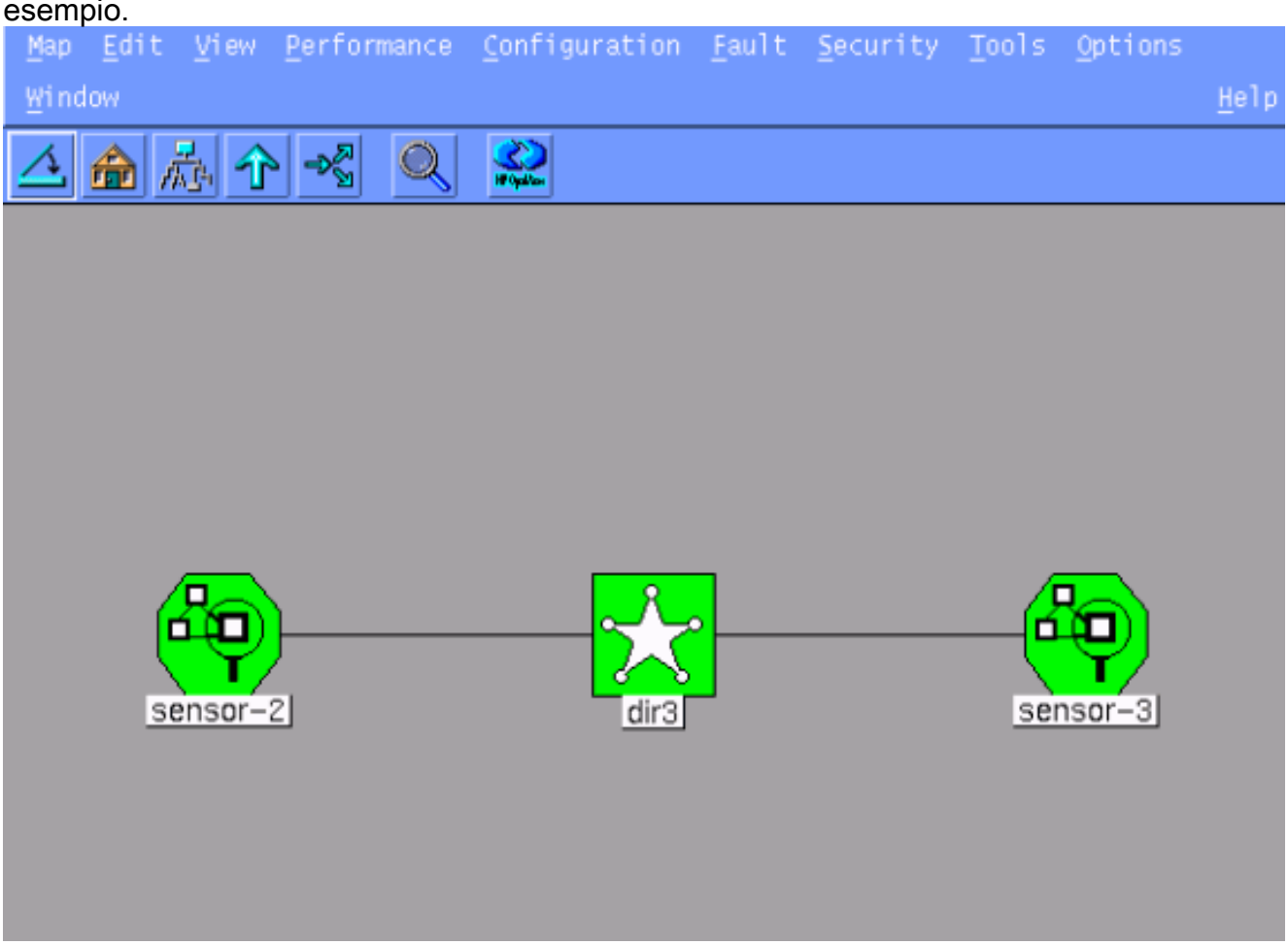


6. Accettare le impostazioni predefinite per il tipo di computer e fare clic su **Avanti**, come mostrato nell'esempio.

7. Èpossibile modificare il registro e ridurre i minuti oppure accettare i valori predefiniti. Tuttavia, è necessario modificare il nome dell'interfaccia di rete nel nome dell'interfaccia di sniffing. Nell'esempio, questo valore è "iprb0". Può essere "spwr0" o qualsiasi altra cosa, a seconda del tipo di sensore e della modalità di connessione.



8. Continuare a fare clic su **Next** (Avanti), quindi su **Finish** (Fine) per aggiungere il sensore in Director. Dal menu principale dovrebbe essere visualizzato sensor-2, come in questo esempio.

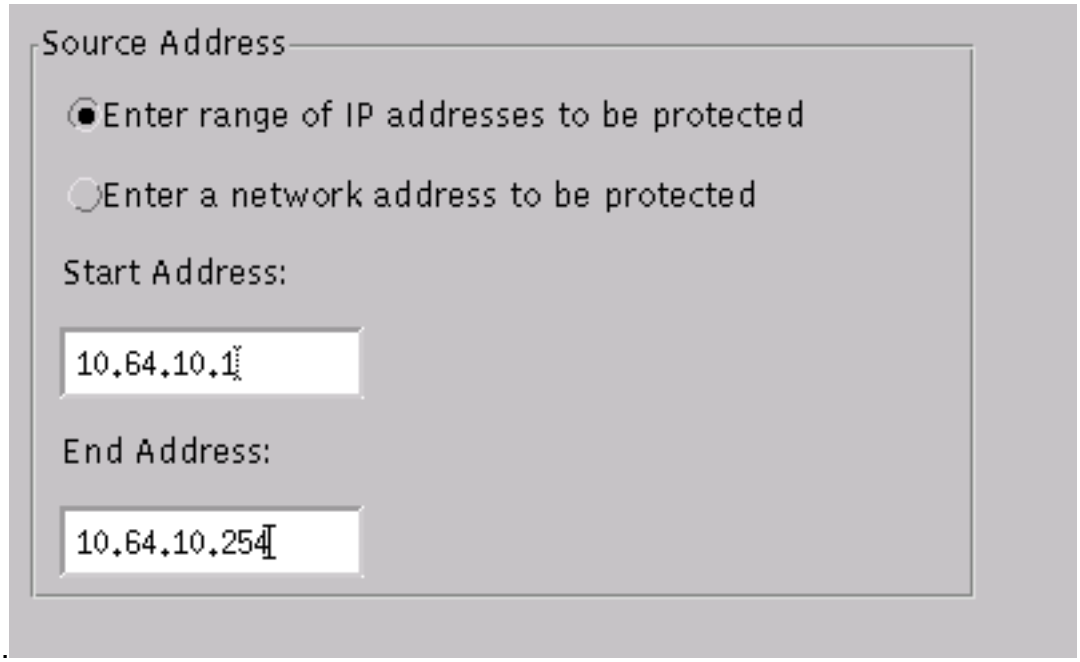


Configurazione del reset TCP per il router Cisco IOS

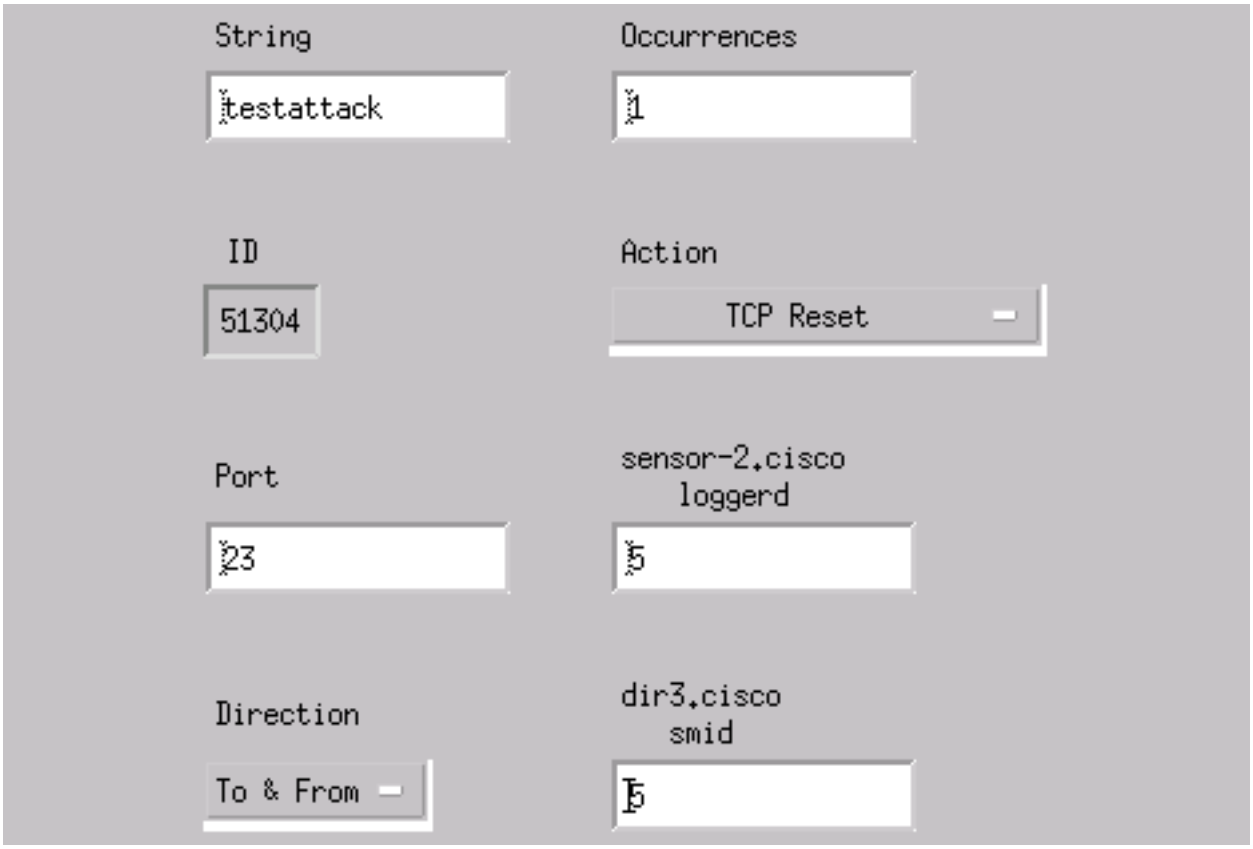
Completare la procedura seguente per configurare il reset TCP per il router Cisco IOS.

1. Nel Menu principale, andare a **Protezione > Configura**.
2. In Configuration File Management Utility, evidenziare **sensor-2** e fare doppio clic su di esso.
3. Aprire Gestione dispositivi.
4. Fare clic su **Dispositivi > Aggiungi**. Immettere le informazioni sulla periferica, come illustrato nell'esempio seguente. Fare clic su **OK** per continuare. Le password Telnet e enable sono entrambe di
   Cisco.

5. Aprire la finestra Rilevamento intrusioni e fare clic su **Reti protette**. Aggiungere l'intervallo di indirizzi da 10.64.10.1 a 10.64.10.254 nella rete
   protetta.

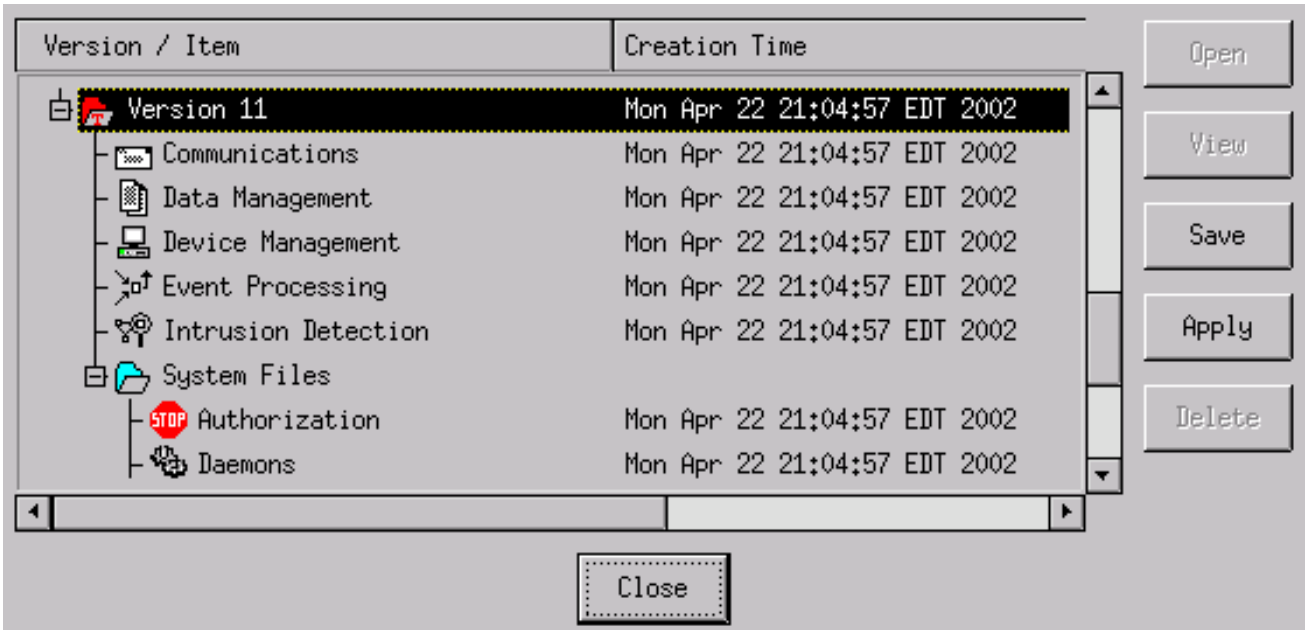


6. Fare clic su **Profilo** e selezionare **Configurazione manuale**. Fare quindi clic su **Modifica firme**. Scegliere **Stringhe corrispondenti** con ID 8000. Selezionate **Espandi (Expand) > Aggiungi (Add)** per aggiungere una nuova stringa denominata **testattack**. Immettere le informazioni sulla stringa, come illustrato nell'esempio, e fare clic su **OK** per
   continuare.



7. Questa parte della configurazione è stata completata. Fare clic su **OK** per chiudere la finestra Rilevamento intrusioni.
8. Aprire la cartella System Files, quindi la finestra Daemons. Assicurarsi che i seguenti daemon siano
   abilitati:

9. Fare clic su **OK** per continuare.
10. Scegliere la versione appena modificata, fare clic su **Salva**, quindi su **Applica**. Attendere che il sistema comunichi all'utente che il sensore ha completato il riavvio dei servizi, quindi chiudere tutte le finestre per la configurazione del
    director.



Avvia attacco e reimpostazione TCP

Telnet da Router Light a Router House e tipo **testattack**. Non appena si preme il tasto Space o Enter, la sessione Telnet viene ripristinata. Il cliente si connetterà a 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.
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Telnet su 10.64.10.49, il sensore, usando il nome utente **root** e la password **attack**. Digitare **cd /usr/nr/etc**. Digitare **cat packetd.conf**. Se si imposta correttamente il reset TCP per l'attacco di test, dovrebbe essere visualizzato un quattro (4) nel campo Codici di azione. Indica la reimpostazione del protocollo TCP, come mostrato nell'esempio.

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

Se si imposta accidentalmente l'azione su "nessuno" nella firma, nel campo Codici azione verrà visualizzato uno zero (0). Ciò indica che non è stata eseguita alcuna azione come illustrato nell'esempio.

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

I reset TCP vengono inviati dall'interfaccia di sniffing del sensore. Se è presente uno switch che collega l'interfaccia del sensore all'interfaccia esterna del router gestito, quando si configura lo switch con il comando **set span**, usare questa sintassi:

```
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
```

Informazioni correlate

- Notifiche sul campo
- Pagina di supporto per Cisco Secure Intrusion Prevention