Impostazione dello shun su un director UNIX

Sommario

Introduzione

Il director e il sensore Cisco Intrusion Detection System (IDS) possono essere utilizzati per gestire un router Cisco per lo shun. In questo documento, viene configurato un sensore (sensore-2) per rilevare gli attacchi al router "House" e per comunicare queste informazioni al director "dir3". Dopo la configurazione, viene avviato un attacco (ping di dimensioni superiori a 1024 byte, ovvero la firma 2151, e un'inondazione ICMP (Internet Control Message Protocol), ovvero la firma 2152, dal router "Light". Il sensore rileva l'attacco e lo comunica al direttore. Per bloccare il traffico proveniente dall'autore dell'attacco, viene scaricato sul router un ACL (Access Control List). Sull'`host` non `raggiungibile` viene mostrato, mentre sull'utente vittima viene mostrato l'ACL scaricato.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Installare il sensore e accertarsi che funzioni correttamente.
- Verificare che l'interfaccia di sniffing si estenda sull'interfaccia esterna del router.

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 versione 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.

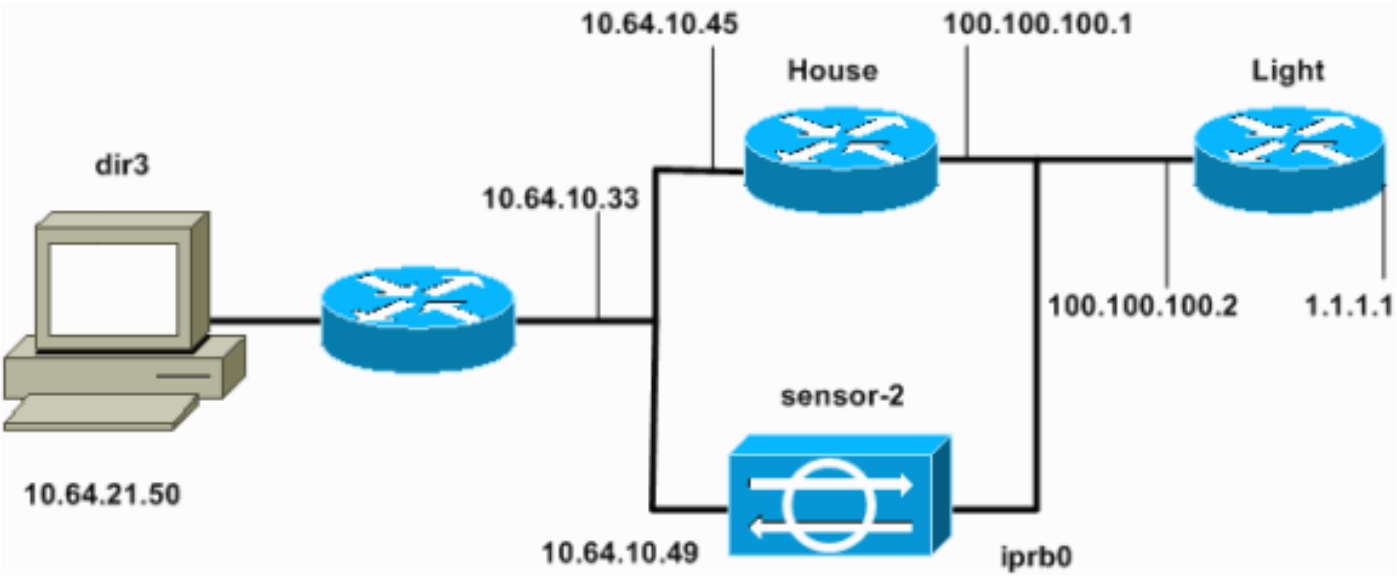
Configurazione

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

Per la stesura di questo documento è stata utilizzata la configurazione di rete illustrata in questo diagramma.



Configurazioni

In questo documento vengono usate le seguenti configurazioni.

- Luce router
- Router House

Luce router

```
<#root>

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
```

Router House

<#root>

```
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#
```

Configurazione del sensore

Completare la procedura seguente per configurare il sensore.

1. Telnet to 10.64.10.49 con attacco di nome utente root e password.
2. Immettere sysconfig-sensor.
3. Quando richiesto, immettere le informazioni di configurazione, come mostrato nell'esempio.

```
<#root>

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:
```

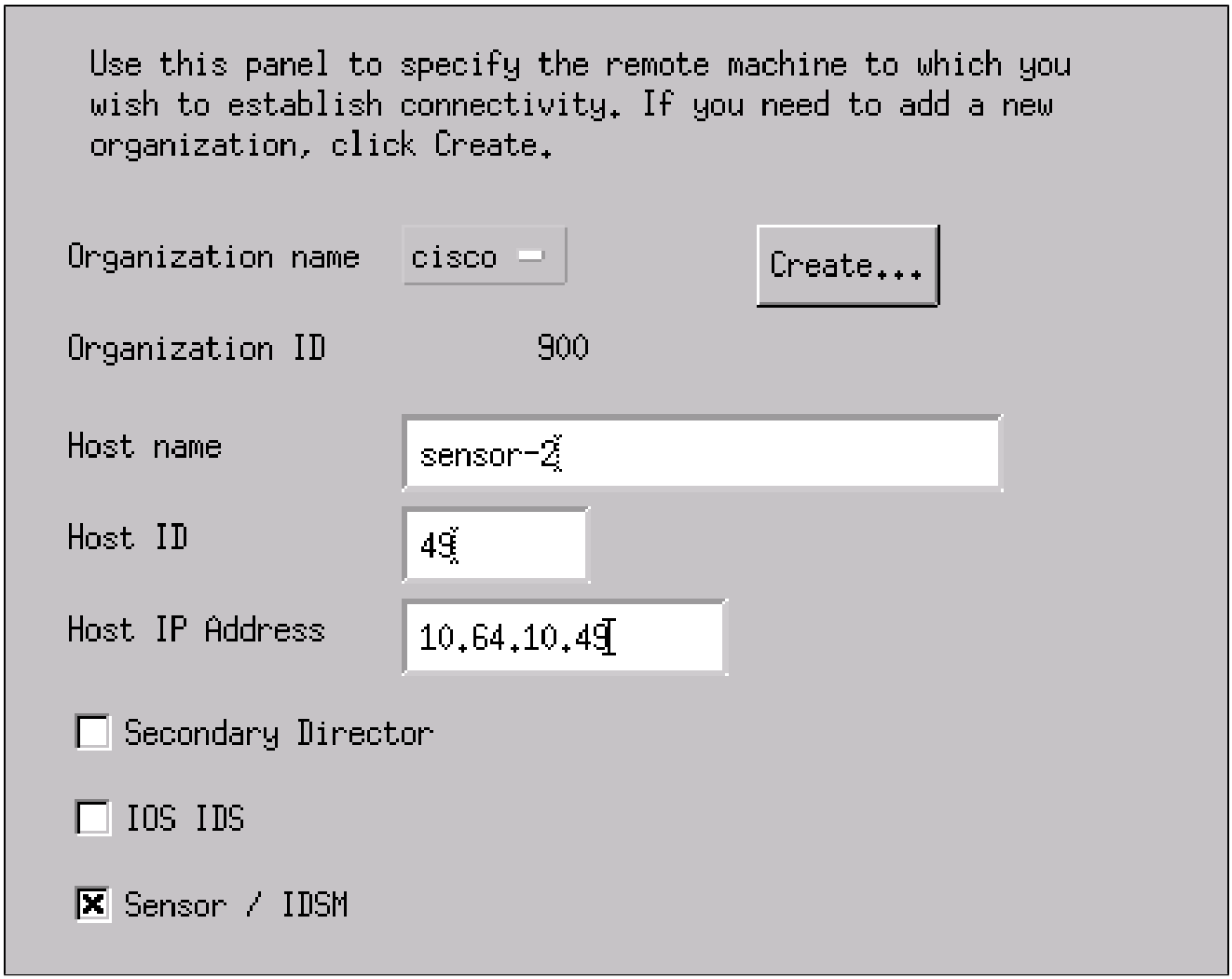
```
50
IDS Manager Organization ID:
900
IDS Manager Host Name:
dir3
IDS Manager Organization Name:
cisco
IDS Manager IP Address:
10.64.21.50
```

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

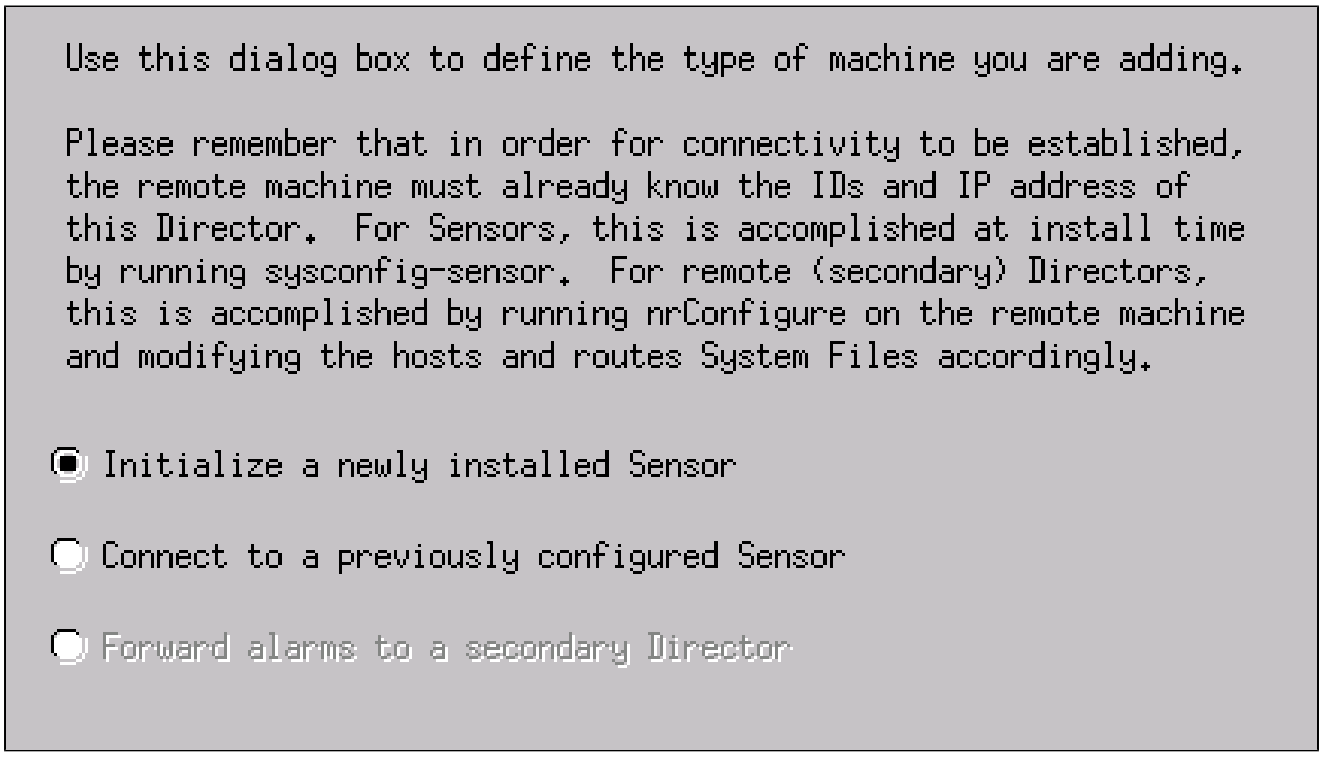
Aggiungere il sensore al director

Completare la procedura seguente per aggiungere il sensore al Director.

1. Telnet to 10.64.21.50 con nome utente netranger e attacco tramite password.
2. Immettere ovw& per avviare HP OpenView.
3. Nel menu principale, selezionare Protezione > Configura.
4. In Configuration File Management Utility, selezionare File > Aggiungi host, quindi fare clic su Avanti.
5. Questo è un esempio di come compilare le informazioni richieste.

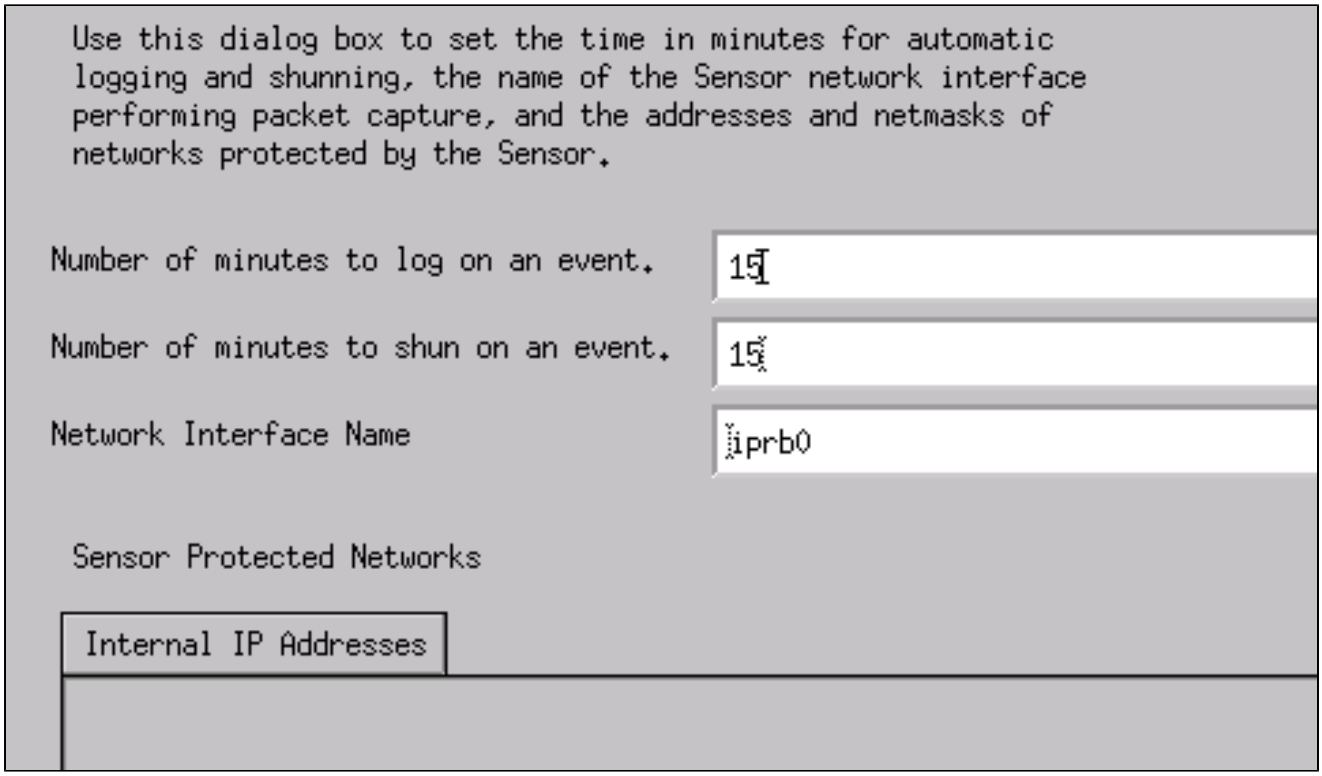


6. Accettate l'impostazione di default per il tipo di macchina e fate clic su Avanti (Next), come mostrato nell'esempio.



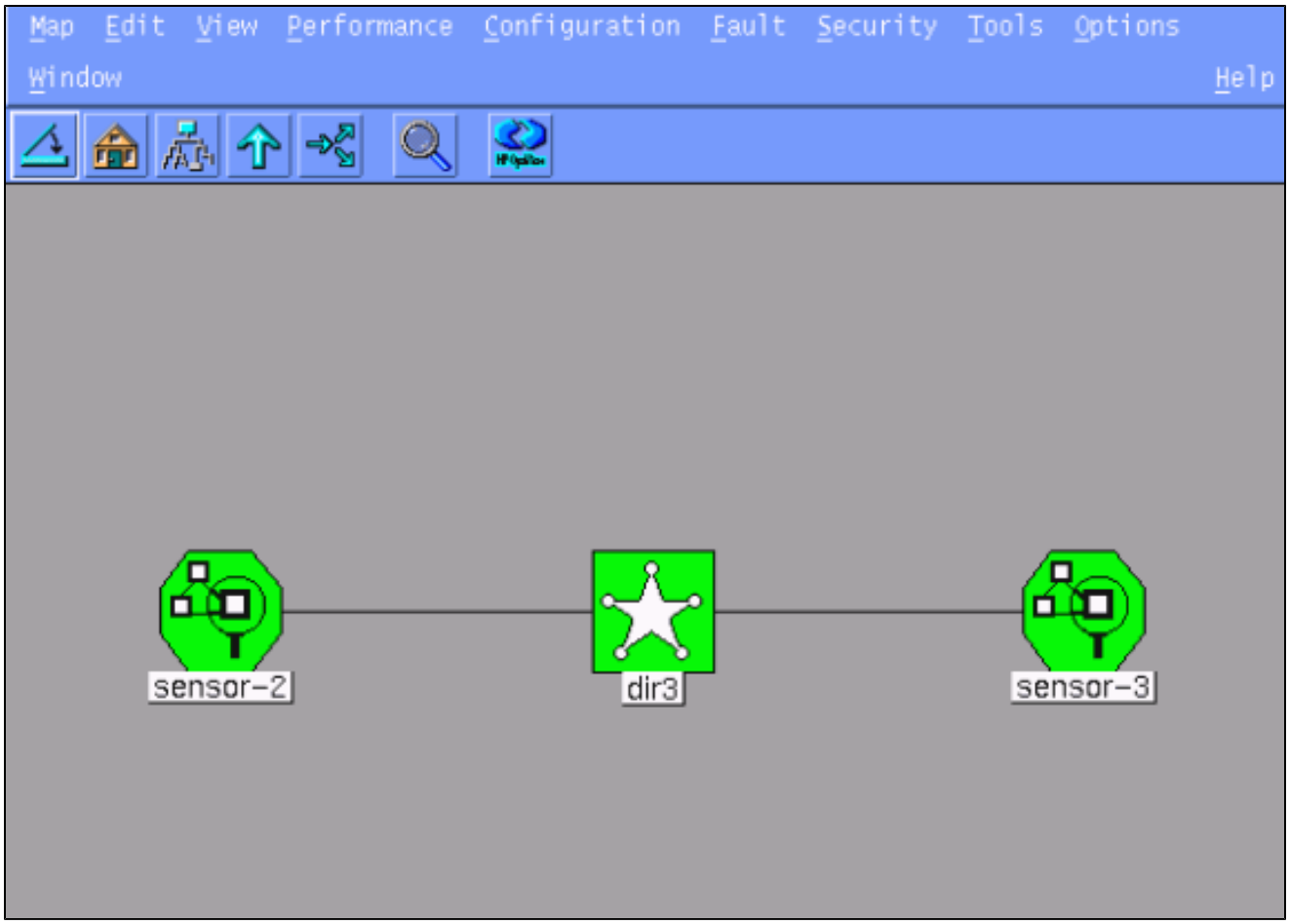
7. Modificare i minuti di log e di shun o lasciarli come predefiniti se i valori sono accettabili. Sostituire il nome dell'interfaccia di rete con il nome dell'interfaccia di sniffing.

   Nell'esempio, questo valore è "iprb0". Può essere "spwr0" o qualsiasi altra cosa, a seconda del tipo di sensore e della modalità di collegamento del sensore.



8. Fare clic su Avanti fino a quando non viene visualizzata un'opzione che consente di fare clic su Fine.

   Il sensore è stato aggiunto a Director. Dal Menu principale dovrebbe essere visualizzato `sensor-2`, come in questo esempio.



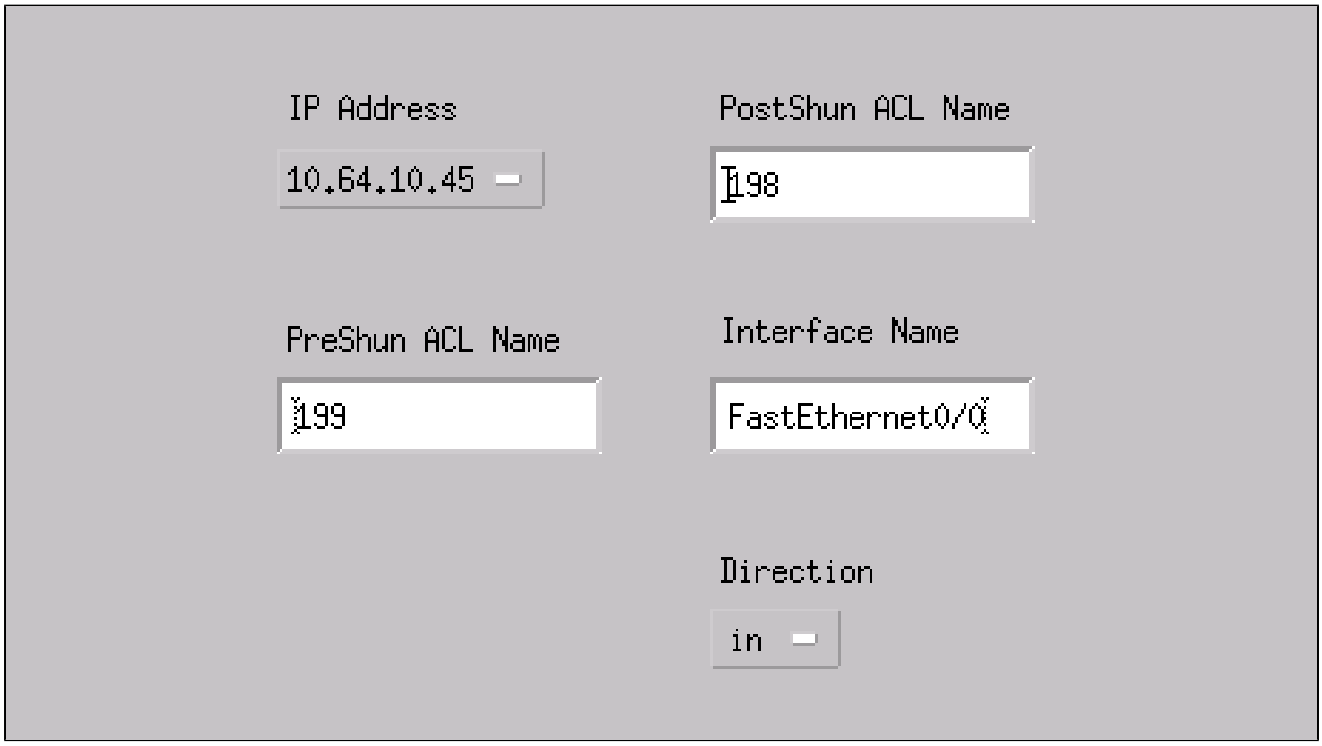
Configurazione dello shun per il router Cisco IOS

Completare la procedura seguente per configurare lo shun per il router Cisco IOS.

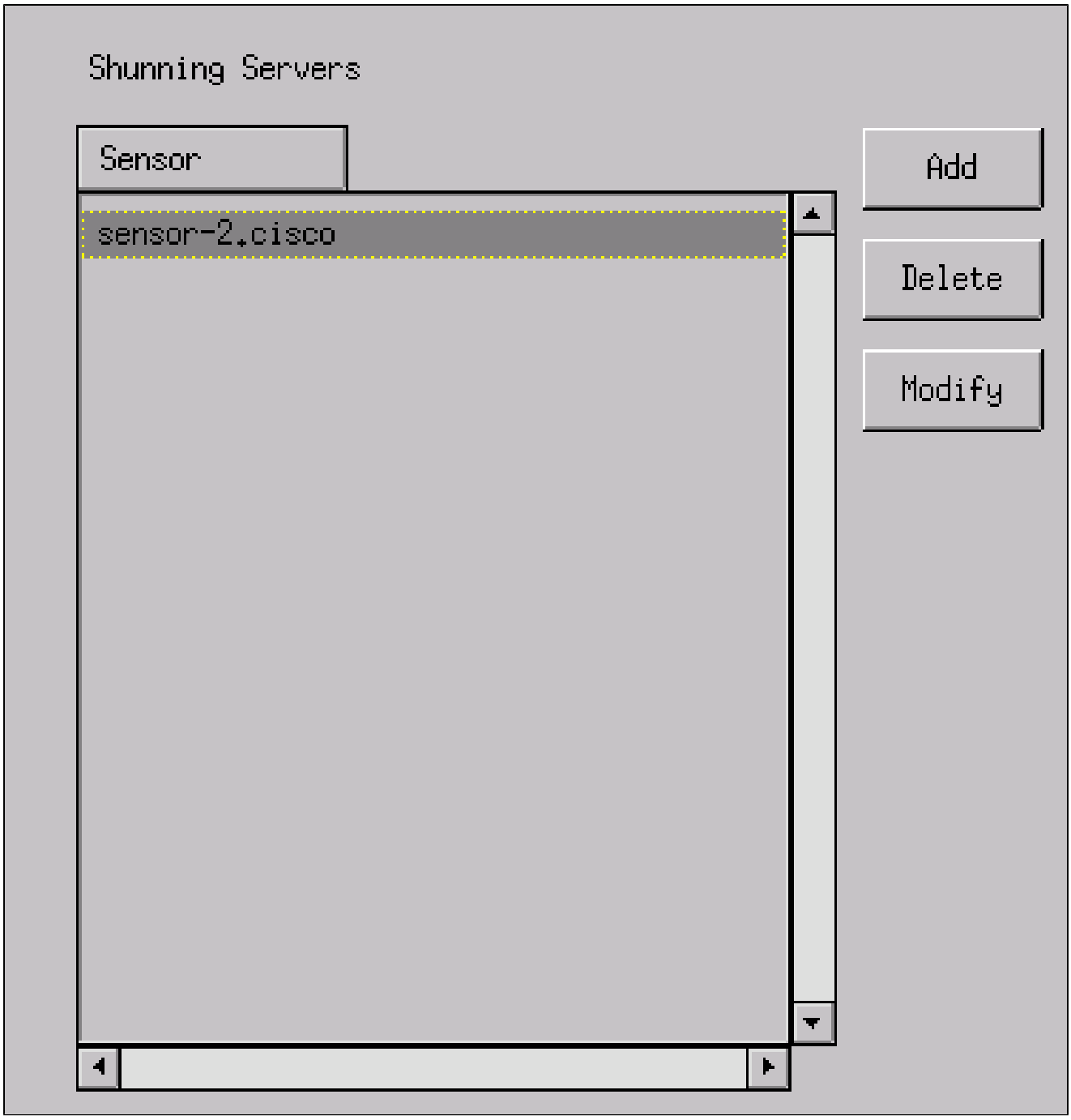
1. Nel menu principale, selezionare Protezione > Configura.
2. In Configuration File Management Utility, evidenziare sensor-2 e fare doppio clic su di esso.
3. Aprire Gestione dispositivi.
4. Fare clic su Dispositivi > Aggiungi e immettere le informazioni come illustrato nell'esempio. Fare clic su OK per continuare.

   Le password Telnet e enable corrispondono a quelle del router "House".

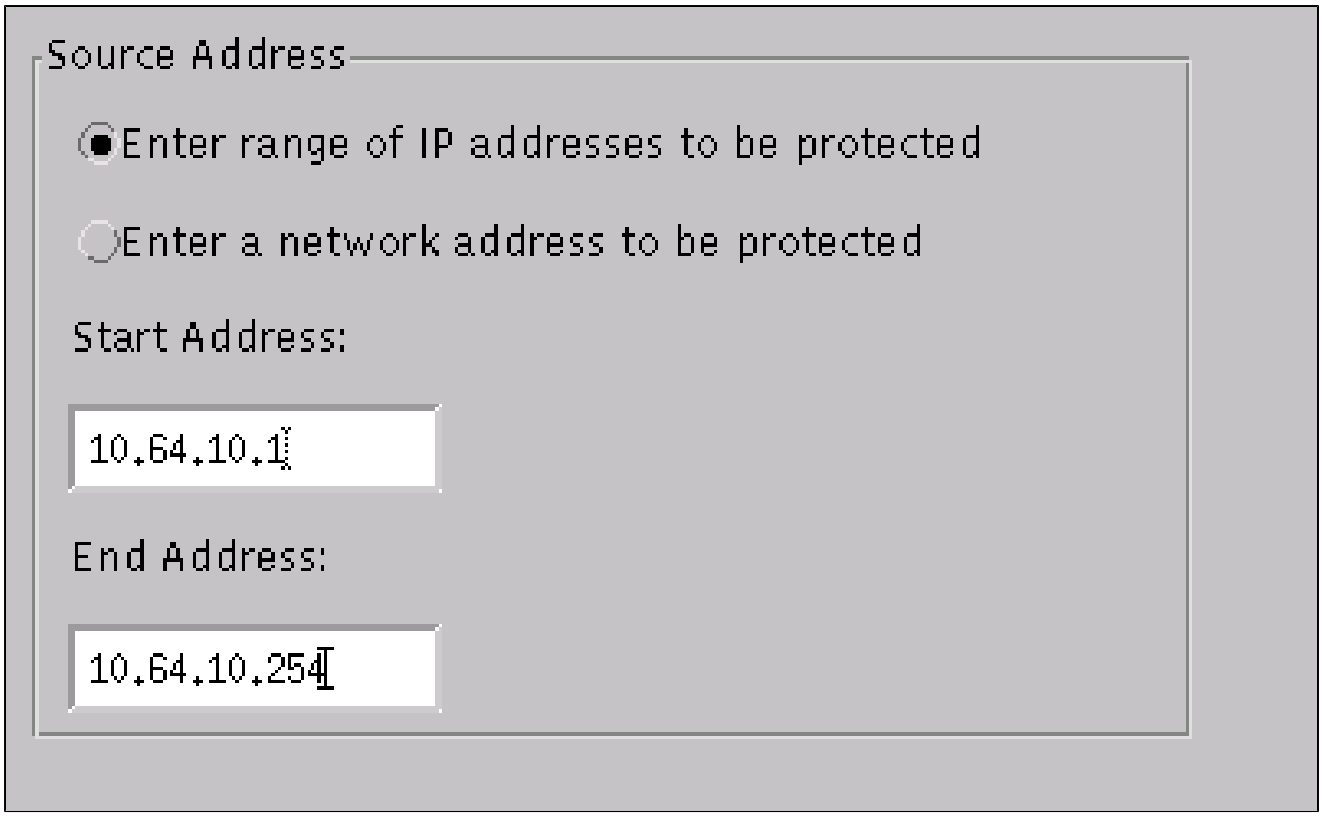
5. Fare clic su Interfacce > Aggiungi, immettere queste informazioni e fare clic su OK per continuare.



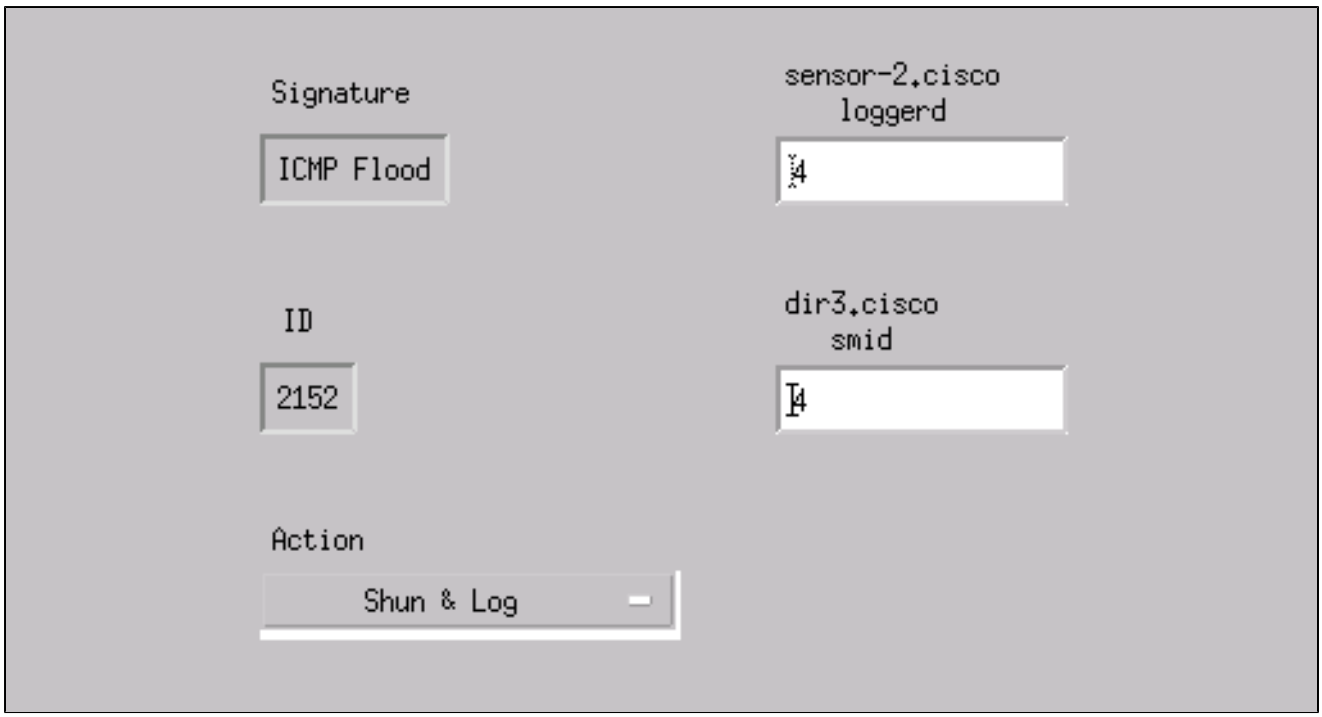
6. Fate clic su Shun > Aggiungi (Add) e selezionate sensor-2.cisco come server di shun. Al termine, chiudere la finestra Gestione periferiche.



7. Aprire la finestra Rilevamento intrusioni e fare clic su Reti protette. Aggiungere l'intervallo da 10.64.10.1 a 10.64.10.254 nella rete protetta, come mostrato nell'esempio.

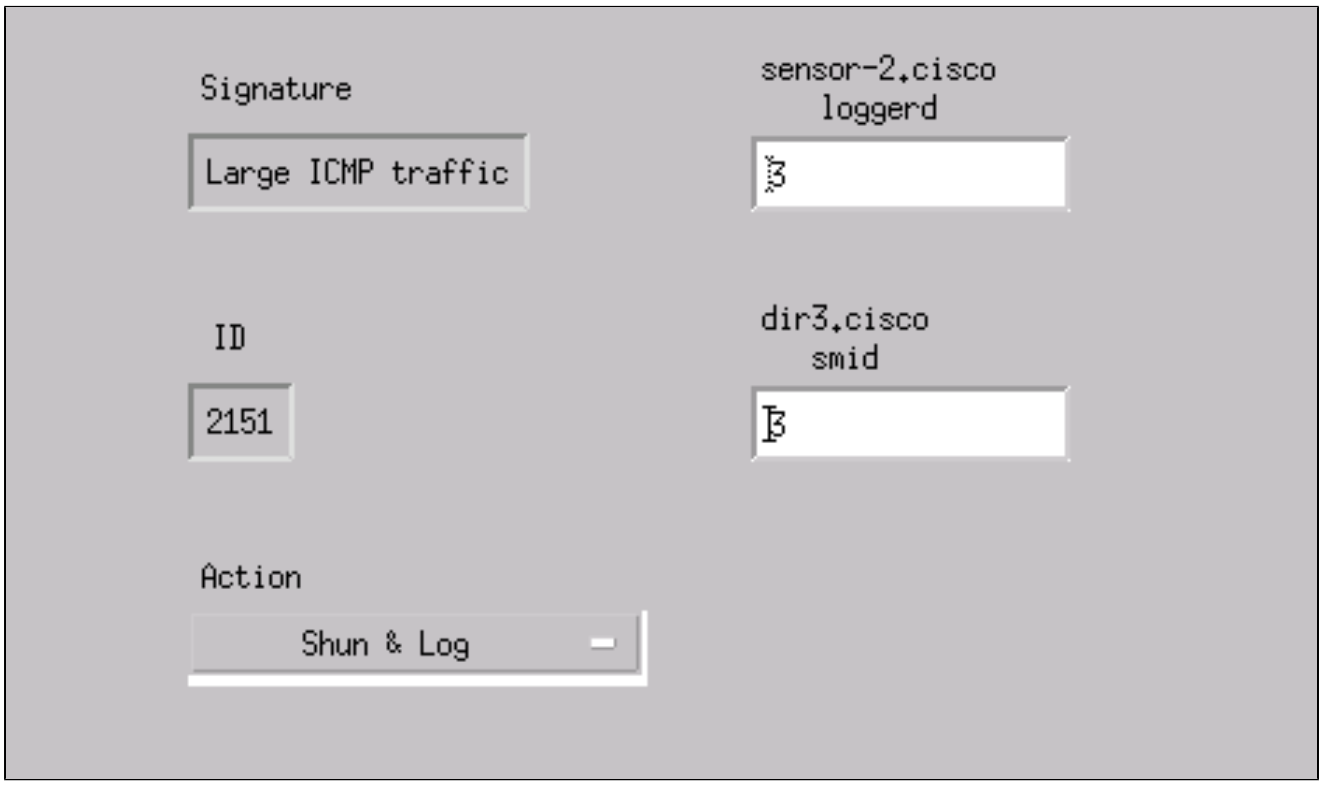


8. Selezionate Profilo (Profile) > Configurazione manuale (Manual Configuration).
9. Selezionare Modifica firme > Traffico ICMP di grandi dimensioni con ID 2151.
10. Fare clic su Modifica, modificare l'azione da Nessuna a Shun & Log e fare clic su OK per continuare.



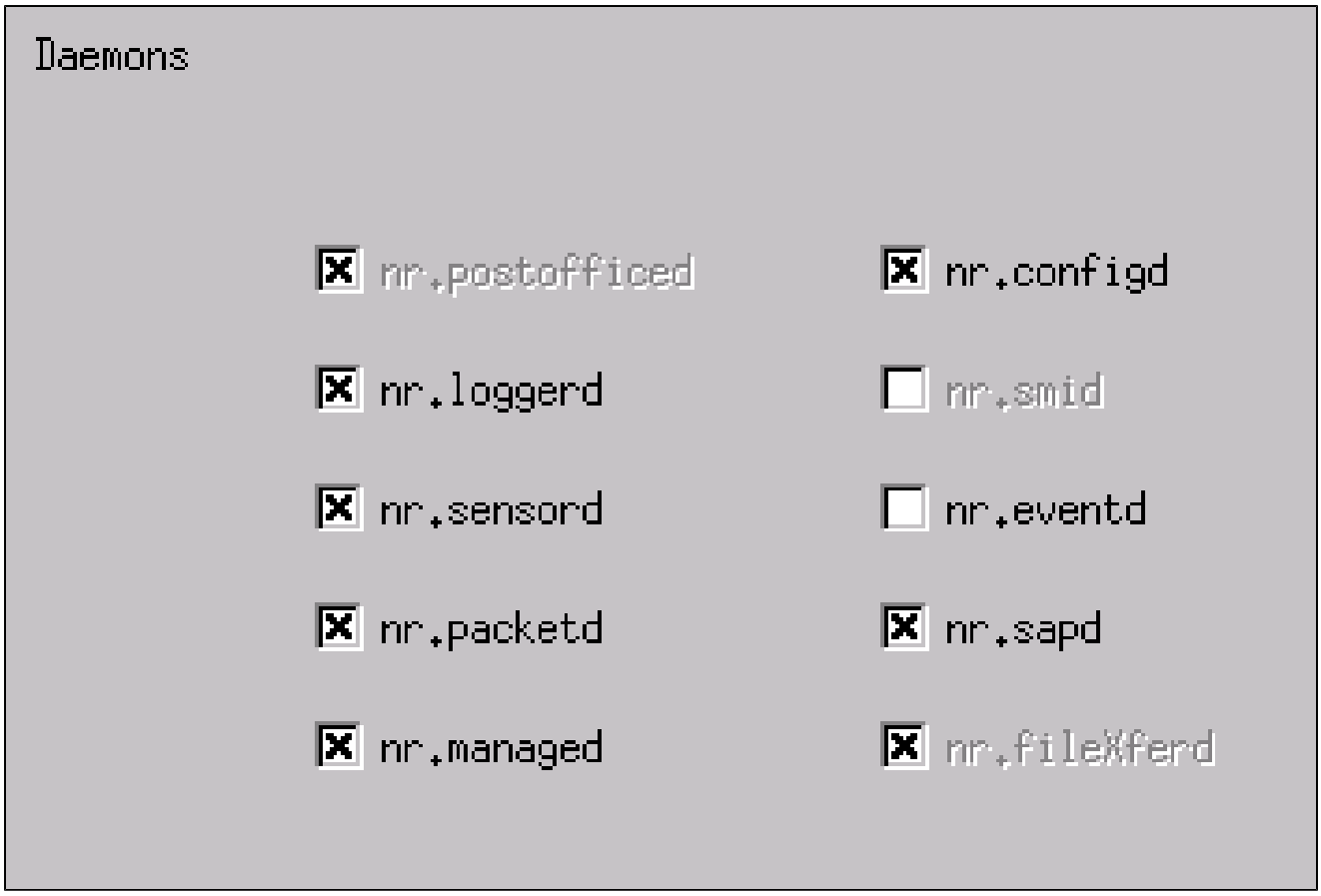
11. Selezionare ICMP Flood con ID 2152, quindi fare clic su Modify (Modifica). Modificare l'opzione Action (Azione) da None (Nessuno) in Shun & Log (Ritira e registra), quindi fare

clic su OK per continuare.



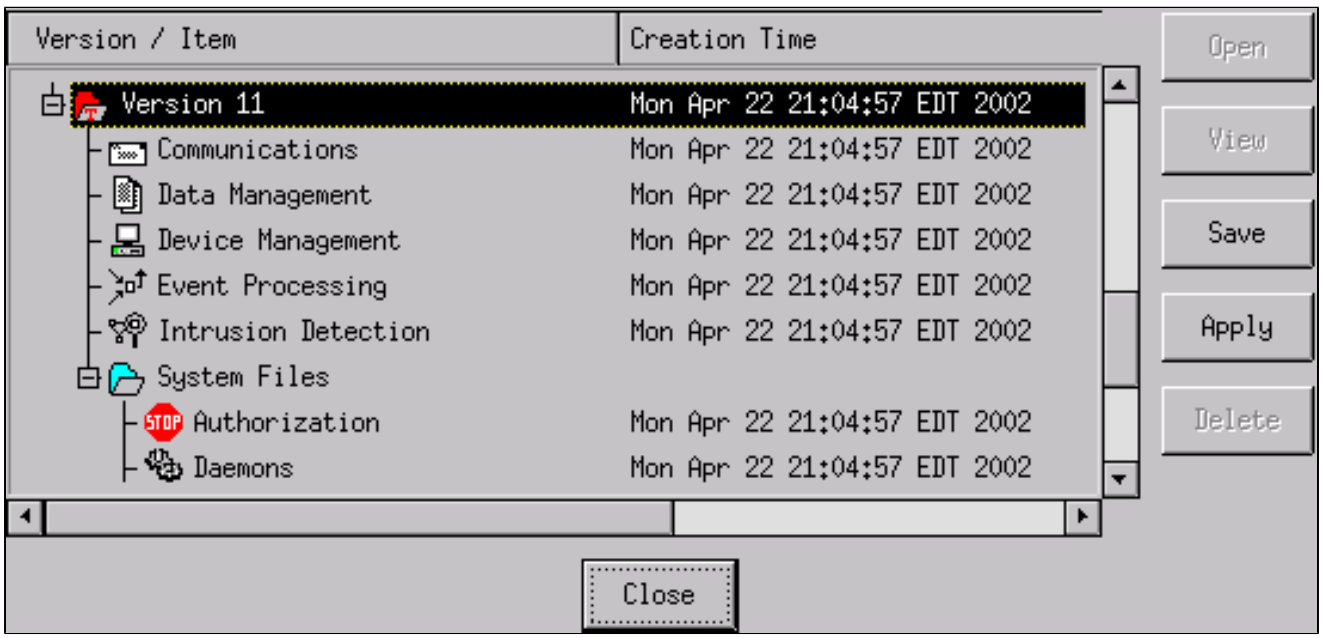
12. Fare clic su OK per chiudere la finestra Rilevamento intrusioni.
13. Aprire la cartella System Files e aprire la finestra Daemons.

    Assicurarsi di aver attivato i seguenti daemon:



14. Fare clic su OK per continuare, scegliere la versione appena modificata e fare clic su Salva, quindi su Applica.

    Attendere che il sistema comunichi all'utente che il sensore ha terminato il riavvio dei servizi, quindi chiudere tutte le finestre per la configurazione del director.



Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione

funzioni correttamente.

Alcuni comandi show sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando show.

- show access-list: elenca le istruzioni di comando access-list nella configurazione del router. Viene inoltre visualizzato un numero di passaggi che indica il numero di volte in cui un elemento è stato trovato durante una ricerca con il comando access-list.
- ping - Utilizzato per diagnosticare la connettività di rete di base.

Prima dell'avvio di un attacco

Prima di lanciare un attacco, eseguire questi comandi.

<#root>

```
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#
```

Lanciare l'attacco e la fuga

Lanciate il vostro attacco dal router "Light" alla vittima "House". Quando l'ACL ha effetto, vengono rilevati gli elementi non raggiungibili.

<#root>

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.

Una volta che il sensore ha rilevato l'attacco, e l'ACL viene scaricato, e questo output viene visualizzato su "House".

<#root>

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

Gli elementi irraggiungibili sono ancora visibili in "Light", come mostrato in questo esempio.

<#root>

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)
```

Quindici minuti dopo, "House" torna alla normalità, perché shunning è stato impostato a 15 minuti.

```
<#root>

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" può eseguire il ping di "House".

```
<#root>

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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Pagina di supporto per Cisco Secure Intrusion Prevention
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).