Shun IDS PIX con Cisco IDS UNIX Director

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Configurazione
Esempio di rete
Configurazioni
Configurazione del sensore
Aggiungere il sensore al director
Configurazione dello shun per PIX
Verifica
Prima di lanciare l'attacco
Lanciare l'attacco e la fuga
Risoluzione dei problemi
Informazioni correlate

Introduzione

Questo documento descrive come configurare lo shun su un PIX con l'aiuto di Cisco IDS UNIX Director (in precedenza Netranger Director) e Sensor. in questo documento si presume che il sensore e il director siano operativi e che l'interfaccia di sniffing del sensore sia configurata per estendersi all'interfaccia esterna PIX.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

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

- Cisco IDS UNIX Director 2.2.3
- Cisco IDS UNIX Sensor 3.0.5
- Cisco Secure PIX con 6.1.1**Nota:** se si usa la versione 6.2.x, è possibile usare la gestione

SSH (Secure Shell Protocol), ma non Telnet. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCdx55215 (solo utenti registrati).

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 utilizzate per configurare le funzionalità descritte più avanti nel documento.

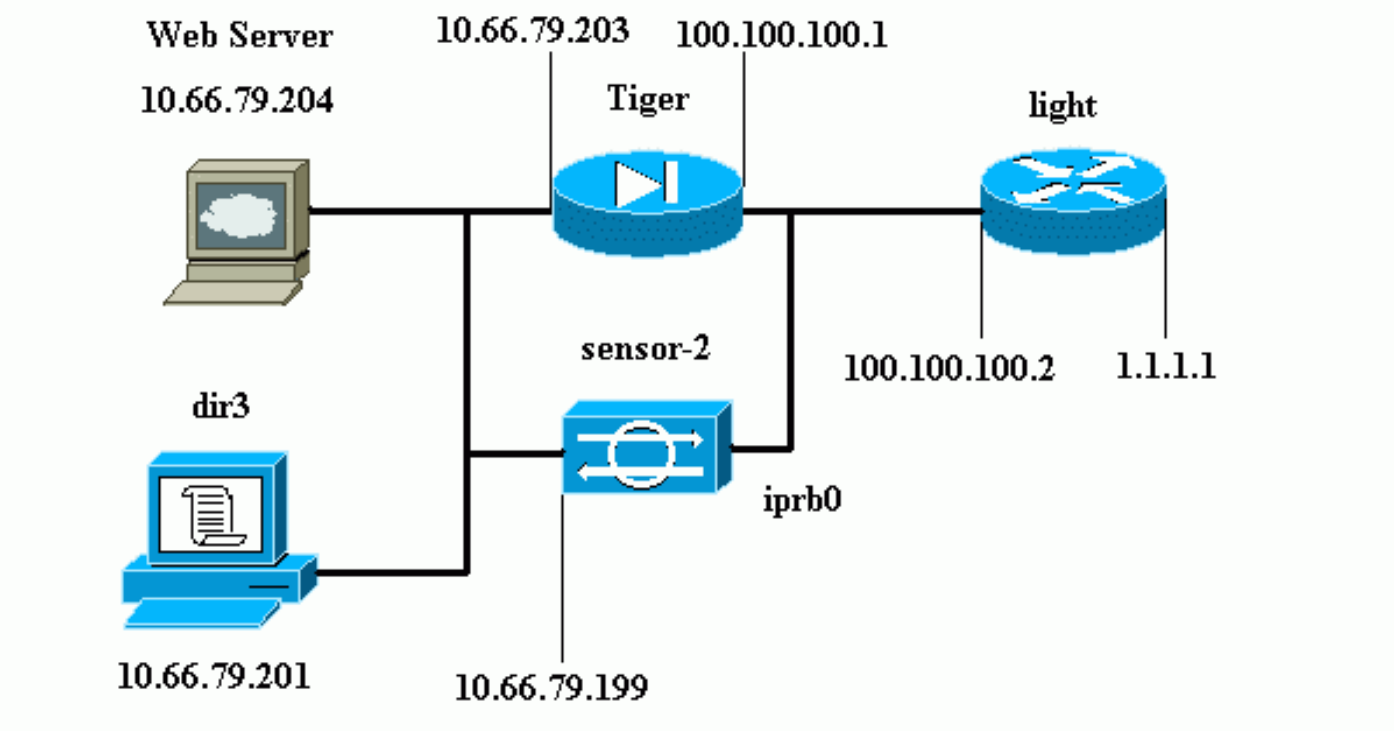
Cisco IDS UNIX Director e Sensor vengono usati per gestire un Cisco Secure PIX per lo shun. Se si considera questa configurazione, tenere presente quanto segue:

- Installare il sensore e accertarsi che funzioni correttamente.
- Assicurarsi che l'interfaccia di sniffing si estenda fino all'interfaccia esterna del PIX.

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

Esempio di rete

Nel documento viene usata questa impostazione di rete.



Configurazioni

Nel documento vengono usate queste configurazioni.

- Luce router
- PIX Tiger

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
```

PIX Tiger

```
PIX Version 6.1(1)
nameif gb-ethernet0 intf2 security10
nameif gb-ethernet1 intf3 security15
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 9jNfZuG3TC5tCVH0 encrypted
hostname Tiger
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Allows ICMP traffic and HTTP to pass through the
PIX !--- to the Web Server. access-list 101 permit icmp
any host 100.100.100.100
access-list 101 permit tcp any host 100.100.100.100 eq
www
pager lines 24
logging on
logging buffered debugging
interface gb-ethernet0 1000auto shutdown
interface gb-ethernet1 1000auto shutdown
interface ethernet0 auto
interface ethernet1 auto
mtu intf2 1500
mtu intf3 1500
mtu outside 1500
mtu inside 1500
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255
ip address outside 100.100.100.1 255.255.255.0
ip address inside 10.66.79.203 255.255.255.224
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
```

```
failover poll 15
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Static NAT for the Web Server. static
(inside,outside) 100.100.100.100 10.66.79.204
  netmask 255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 100.100.100.2 1
route inside 10.66.0.0 255.255.0.0 10.66.79.193 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
  h323 0:05:00 s0
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
!--- Allows Sensor Telnet to the PIX from the inside
interface. telnet 10.66.79.199 255.255.255.255 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:b4c820ba31fbb3996ca8891503ebacbc
: end
```

Configurazione del sensore

In questa procedura viene descritto come configurare il sensore.

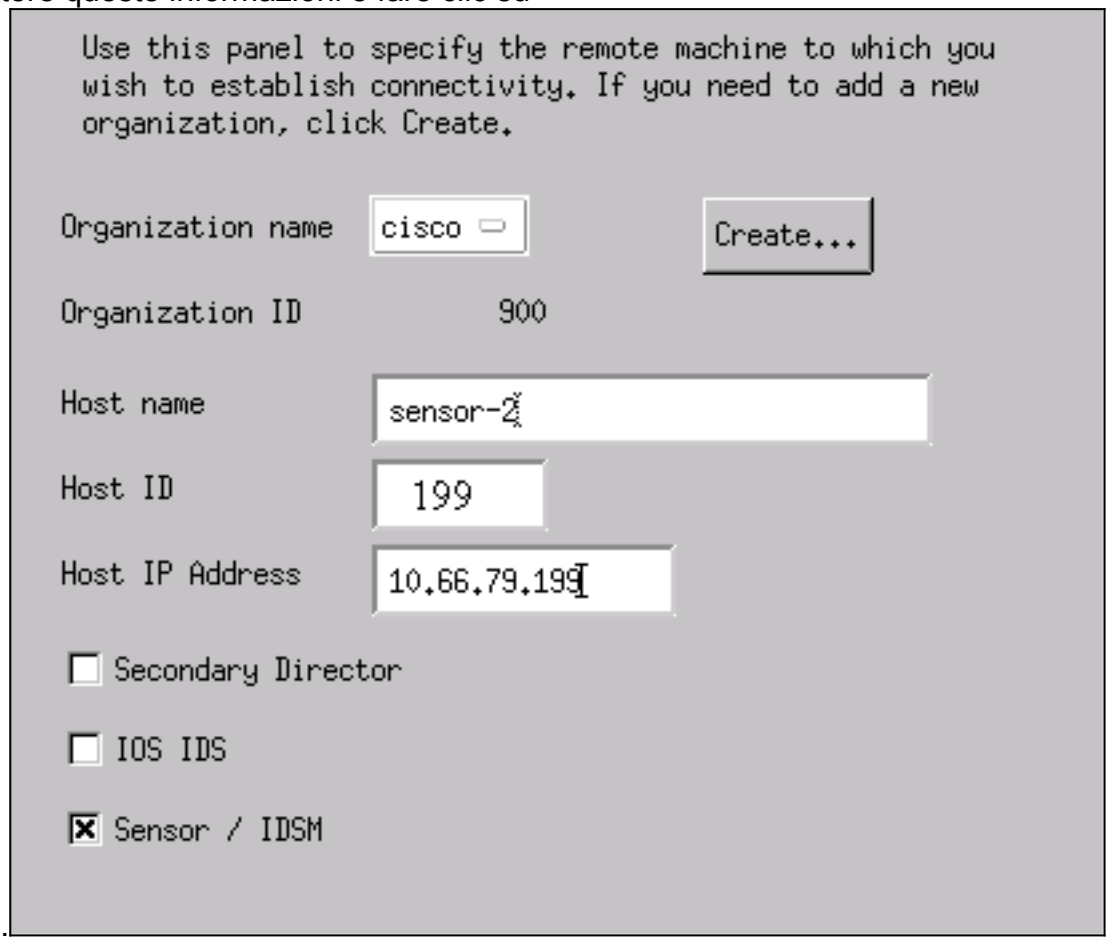
1. Telnet to **10.66.79.199** con **attacco di** nome utente **root** e password.
2. Immettere **sysconfig-sensor**.
3. Immettere le informazioni seguenti:Indirizzo IP: **10.66.79.199**Netmask IP: **255.255.255.224**Nome host IP: **sensor-2**Route predefinita: **10.66.79.193**Controllo degli accessi alla rete**10.**Infrastruttura di comunicazioneID host sensore: **49**ID organizzazione sensore: **900**Nome host sensore: **sensor-2**Nome organizzazione sensore: **cisco**Indirizzo IP sensore: **10.66.79.199**ID host di IDS Manager: **50**ID organizzazione gestore IDS: **900**Nome host di IDS Manager: **dir3**Nome organizzazione gestore IDS: **cisco**Indirizzo IP di IDS Manager: **10.66.79.201**
4. Salvare la configurazione. Il sensore si riavvia.

Aggiungere il sensore al director

Completare questa procedura per aggiungere il sensore al Director.

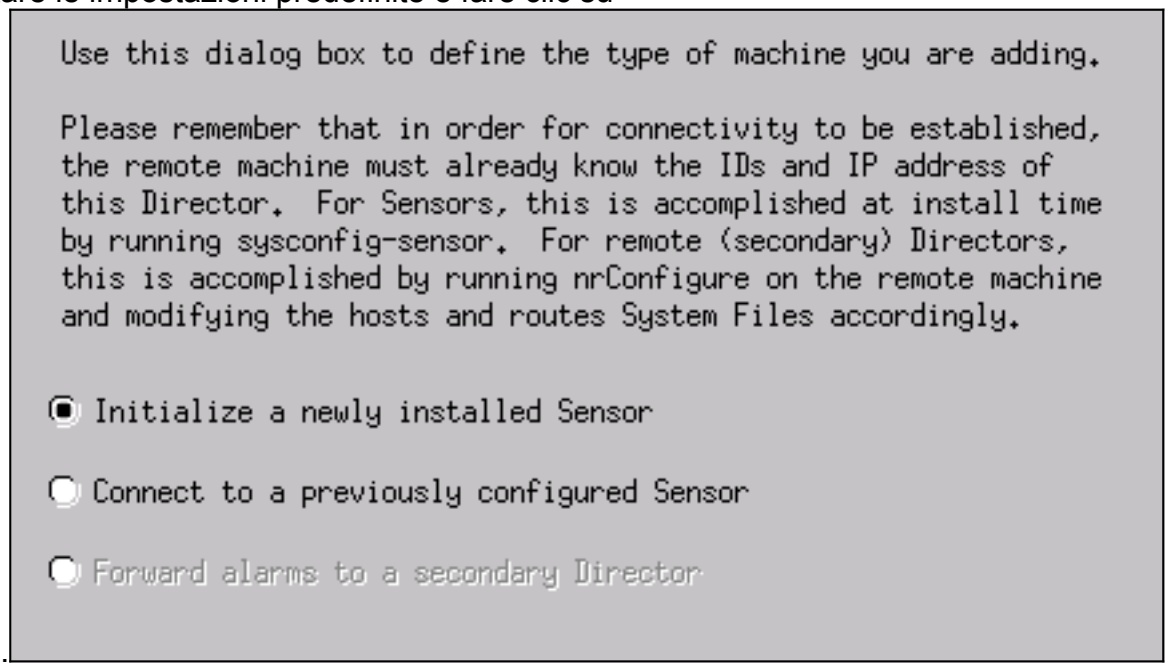
1. Telnet to **10.66.79.201** con nome utente **netranger** e password **attack**.

2. Immettere **ovw&** per avviare HP OpenView.
3. Nel menu principale, selezionare **Security > Configure** (Protezione **> Configura)**.
4. Nel menu Configurazione Netranger, selezionare **File > Aggiungi host**, quindi fare clic su **Avanti**.
5. Immettere queste informazioni e fare clic su



Avanti.

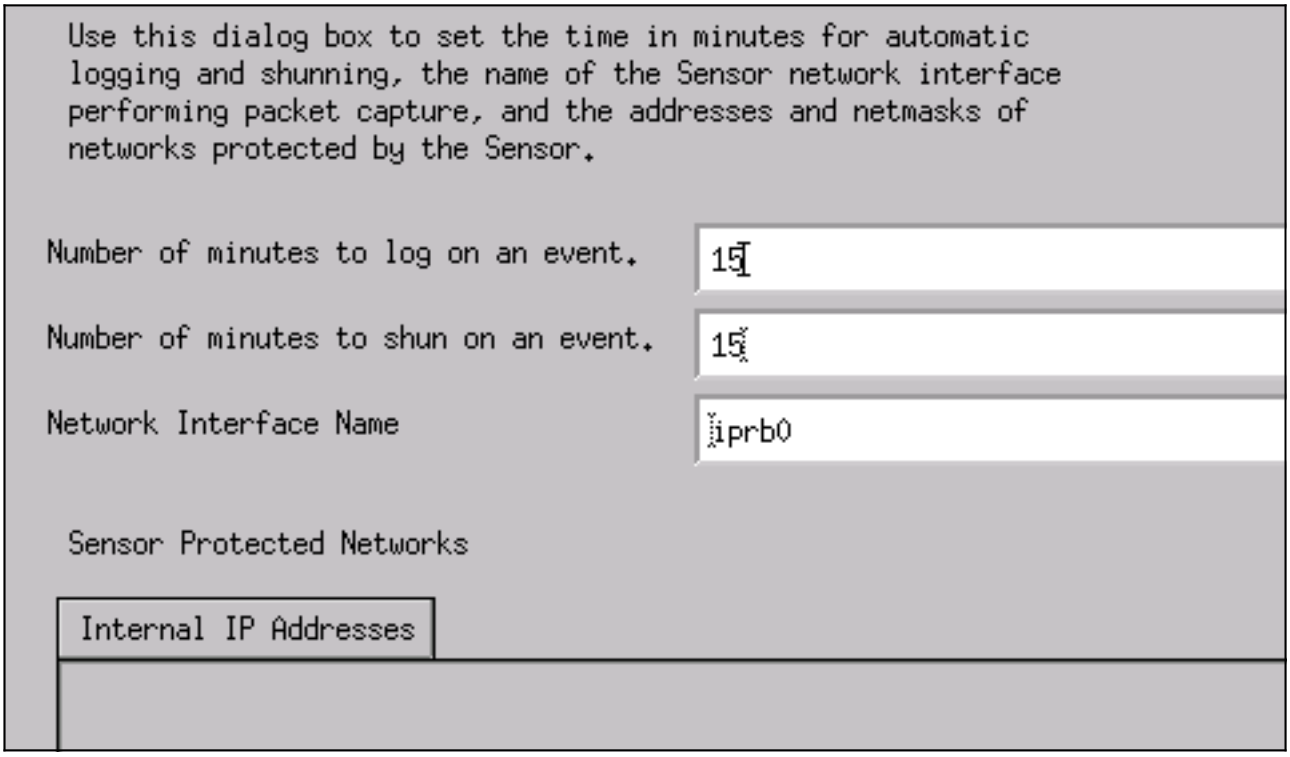
6. Accettare le impostazioni predefinite e fare clic su



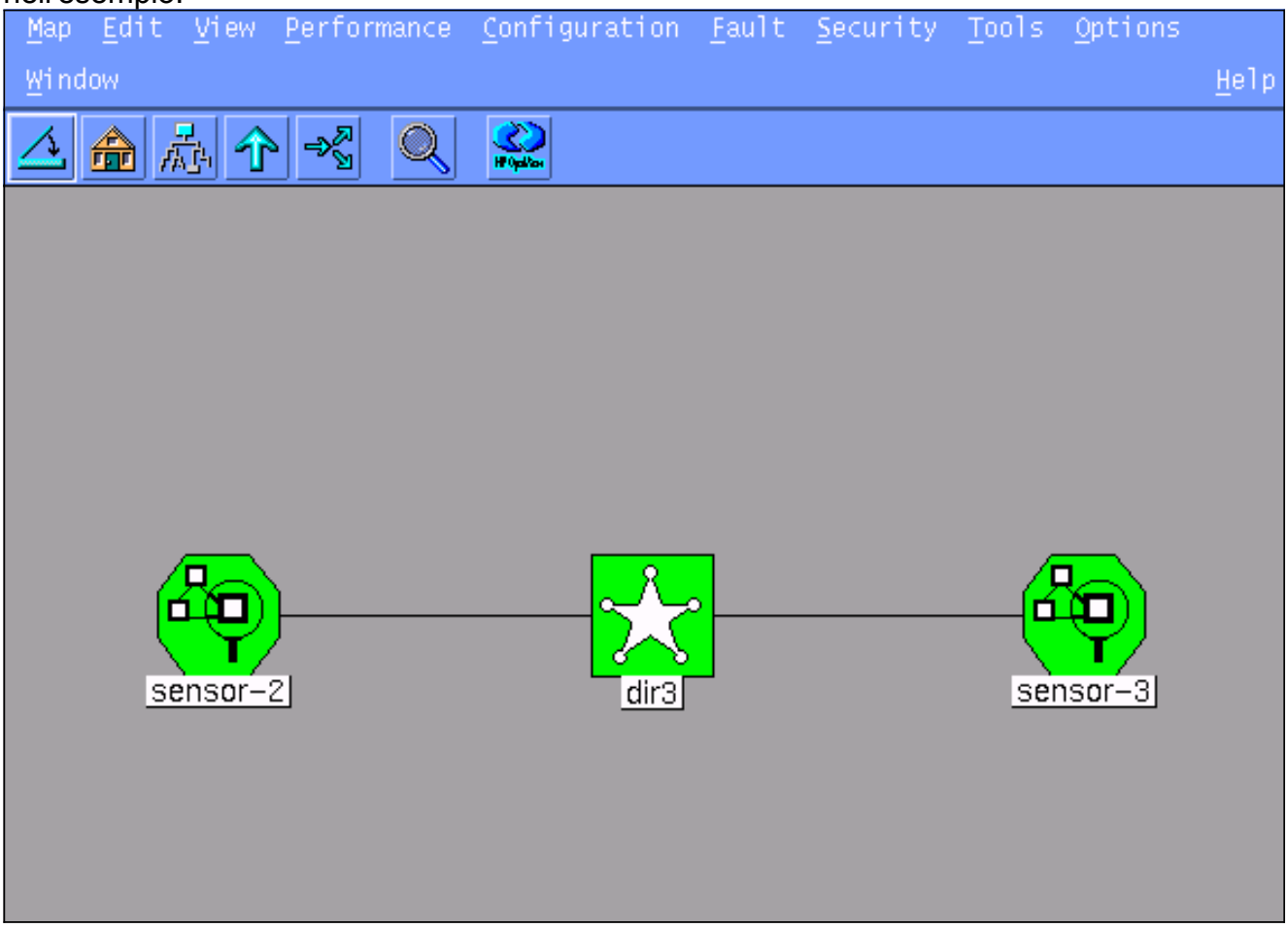
Avanti.

7. Modificare i minuti di log e di shun o lasciarli come predefiniti se i valori sono accettabili. 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 basata sul tipo di sensore e su come si collega il

sensore.



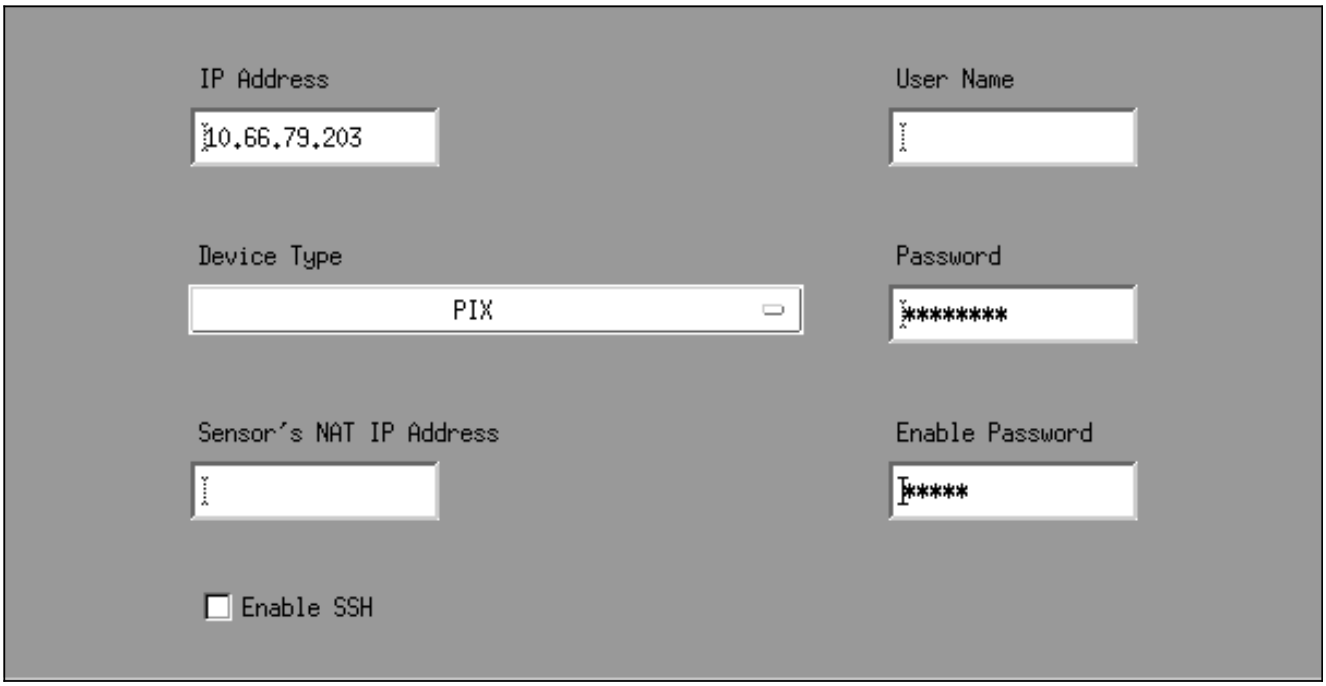
8. Fare clic su **Avanti** finché non viene visualizzata un'opzione che consente di fare clic su **Fine**.Il sensore è stato aggiunto correttamente al Director. Dal menu principale, viene visualizzato **sensor-2**, come mostrato nell'esempio.



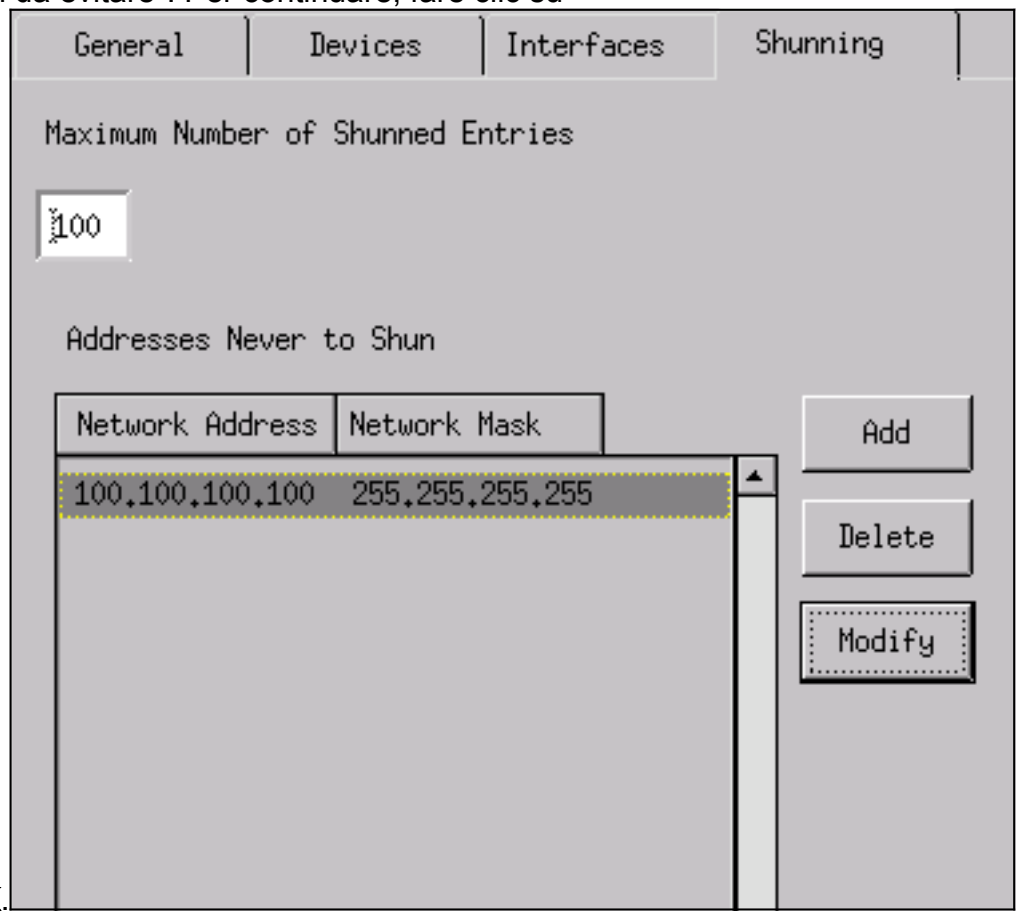
Configurazione dello shun per PIX

Completare questa procedura per configurare lo shun per PIX.

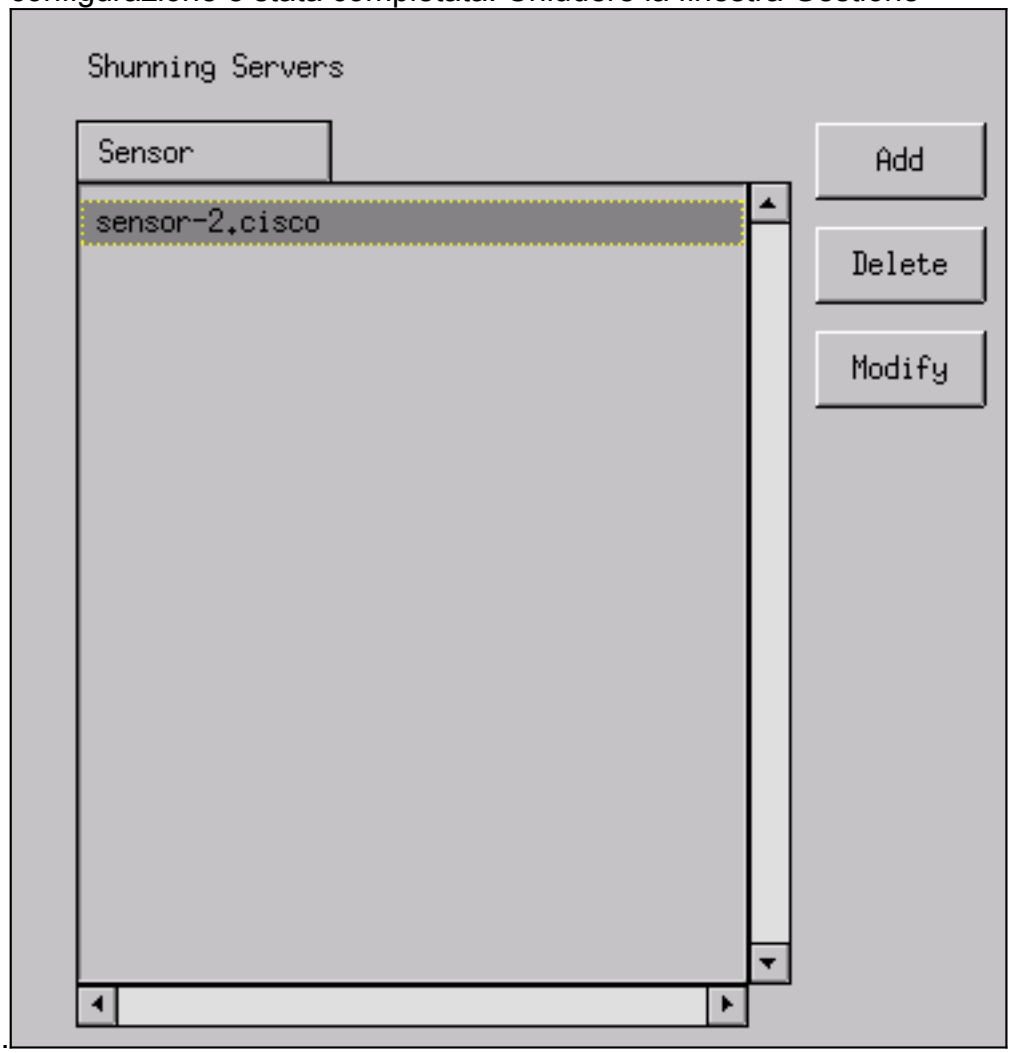
1. Nel menu principale, selezionare **Security > Configure** (Protezione **> Configura)**.
2. Nel menu Configurazione Netranger, evidenziare **sensor-2** e fare doppio clic su di esso.
3. Aprire **Gestione dispositivi**.
4. Fare clic su **Dispositivi > Aggiungi** e immettere le informazioni come mostrato nell'esempio. Per continuare, fare clic su **OK**. La password Telnet e la password di abilitazione sono entrambe
"Cisco".



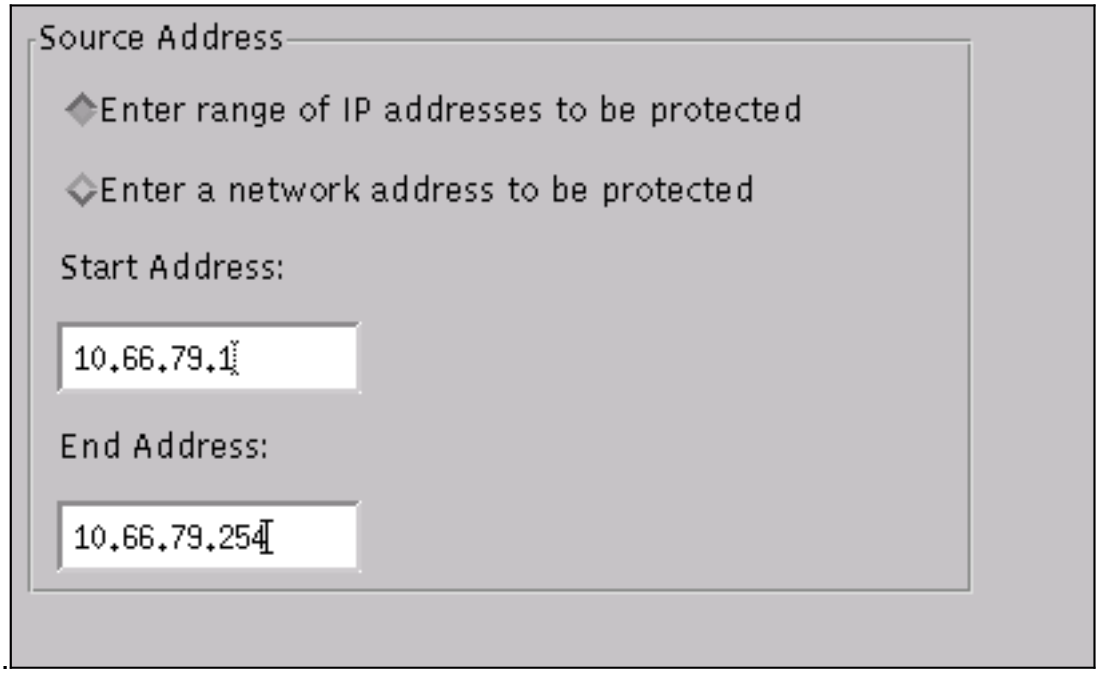
5. Selezionate **Shun > Aggiungi (Add)**. Aggiungere l'host **100.100.100.100** alla voce "Indirizzi mai da evitare". Per continuare, fare clic su
OK.



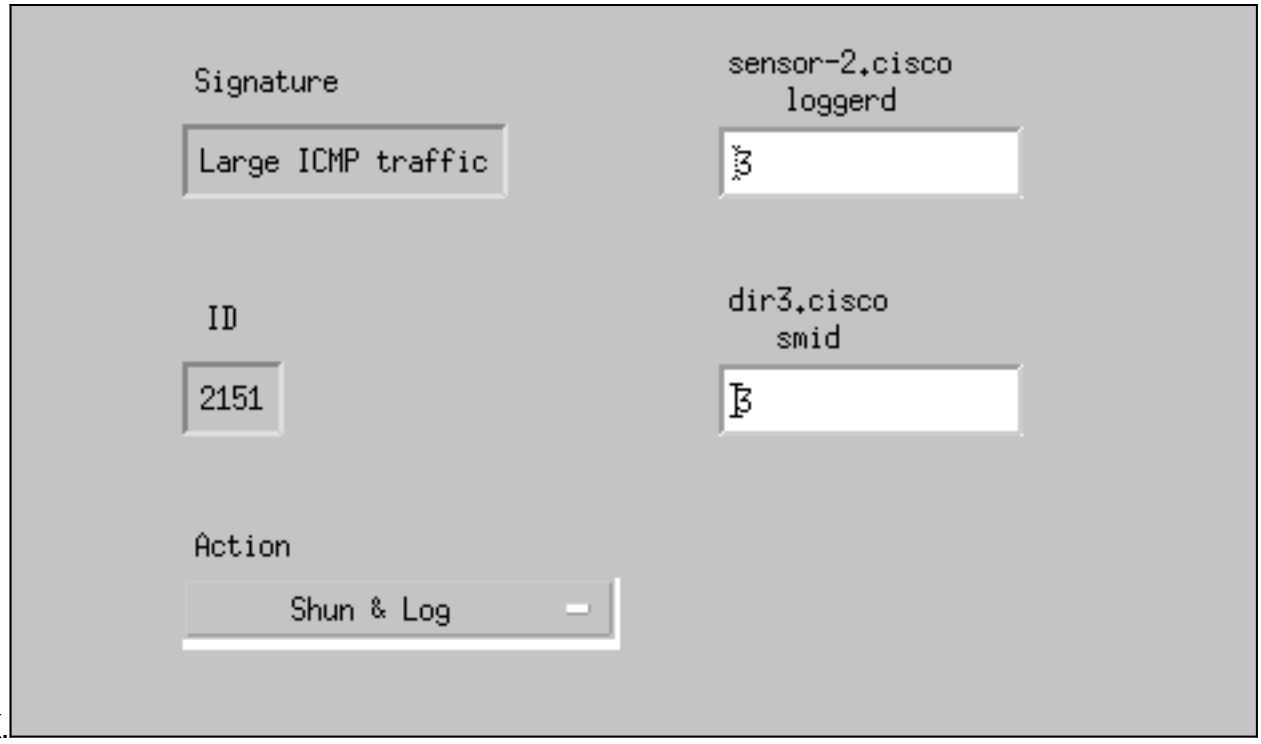
6. Fare clic su **Shun > Aggiungi** e selezionare **sensor-2.cisco** come server di shun. Questa parte della configurazione è stata completata. Chiudere la finestra Gestione periferiche.



7. Aprire la finestra Rilevamento intrusioni e fare clic su **Reti protette**. Aggiungere **10.66.79.1** a **10.66.79.254** nella rete protetta.

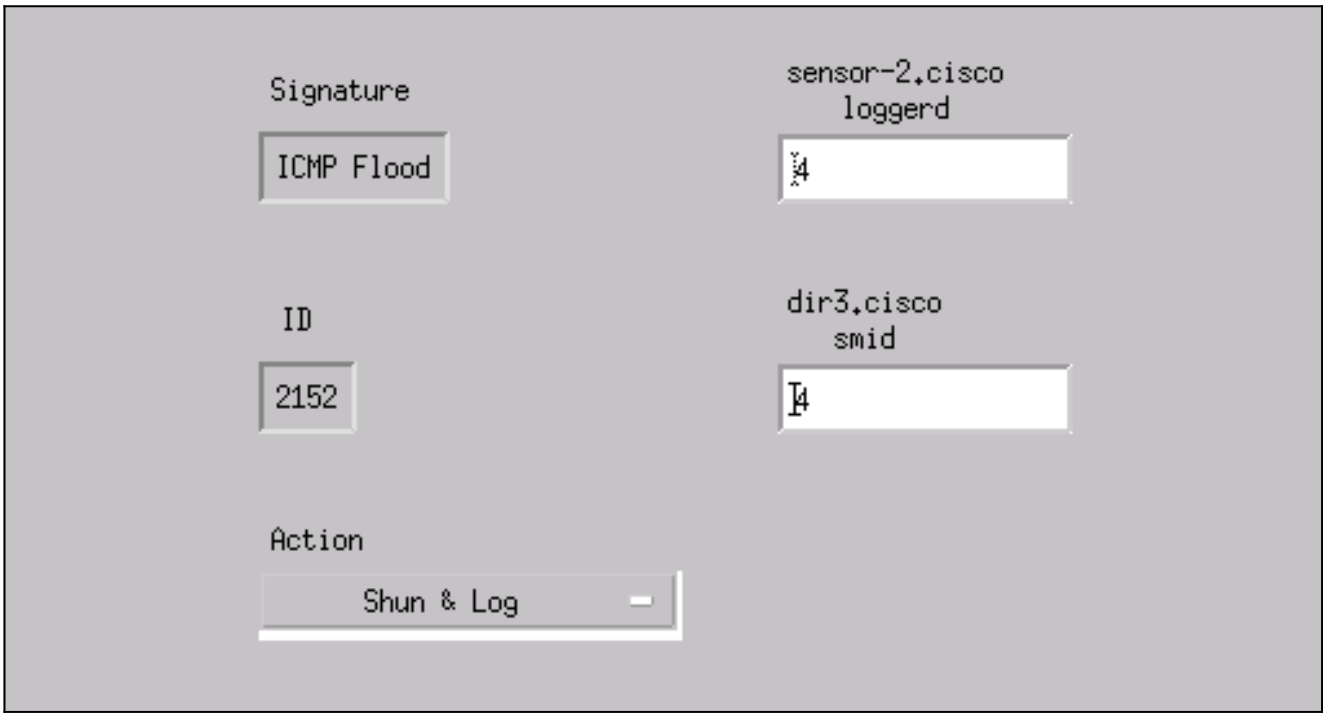


8. Fare clic su **Profilo** e selezionare **Configurazione manuale > Modifica firme**. Selezionare **Large ICMP Traffic** and **ID: 2151**, fare clic su **Modifica**, quindi modificare l'azione da Nessuna a **Shun e Log**. Per continuare, fare clic su



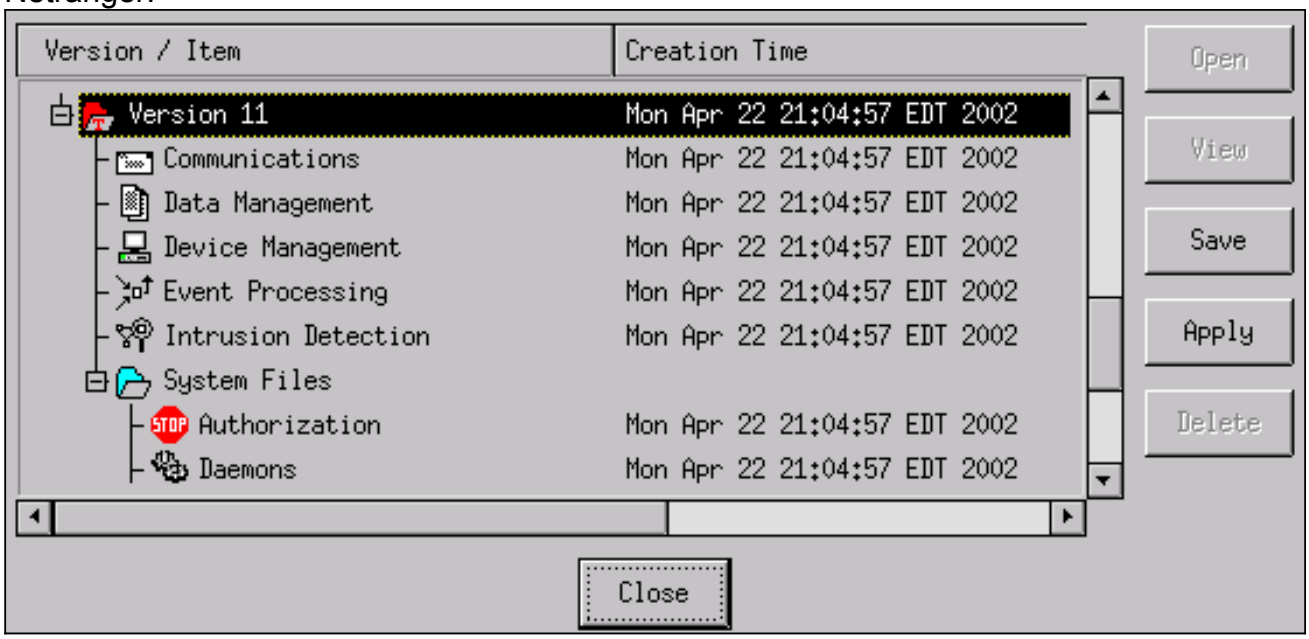
OK.

9. Selezionare **ICMP Flood** and **ID: 2152**, fare clic su **Modifica**, quindi modificare l'azione da **Nessuno** a **Shun e Log**. Per continuare, fare clic su
OK.



10. Questa parte della configurazione è stata completata. Per chiudere la finestra Rilevamento intrusioni, fare clic su **OK**.
11. Aprire la cartella **File di sistema** e aprire la finestra **Daemons**. Assicurarsi di aver abilitato i seguenti
daemon:

12. Fare clic su **OK** per continuare e selezionare la versione appena modificata. Selezionate **Salva (Save) > Applica (Apply)**. Attendere che il sistema comunichi il completamento del sensore, riavviare i servizi e chiudere tutte le finestre per la configurazione di Netranger.



Verifica

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

Prima di lanciare l'attacco

```
Tiger(config)# show telnet
10.66.79.199 255.255.255.255 inside
Tiger(config)# who
        0: 10.66.79.199

Tiger(config)# show xlate
1 in use, 1 most used
```

```
Global 100.100.100.100 Local 10.66.79.204 static

Light#ping 100.100.100.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/195/217 ms

Light#telnet 100.100.100.100 80
Trying 100.100.100.100, 80 ... Open
```

Lanciare l'attacco e la fuga

```
Light#ping
Protocol [ip]:
Target IP address: 100.100.100.100
Repeat count [5]: 100000
Datagram size [100]: 18000
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100000, 18000-byte ICMP Echos to 100.100.100.100, timeout is 2 seconds:
!.....................
Success rate is 4 percent (1/21), round-trip min/avg/max = 281/281/281 ms

Light#telnet 100.100.100.100 80
Trying 100.100.100.100, 80 ...
% Connection timed out; remote host not responding

Tiger(config)# show shun
Shun 100.100.100.2 0.0.0

Tiger(config)# show shun stat
intf2=OFF, cnt=0
intf3=OFF, cnt=0
outside=ON, cnt=2604
inside=OFF, cnt=0
intf4=OFF, cnt=0
intf5=OFF, cnt=0
intf6=OFF, cnt=0
intf7=OFF, cnt=0
intf8=OFF, cnt=0
intf9=OFF, cnt=0
Shun 100.100.100.2 cnt=403, time=(0:01:00).0 0 0
```

Quindici minuti dopo, ritorna alla normalità perché lo shun è impostato su quindici minuti.

```
Tiger(config)# show shun

Tiger(config)# show shun stat
intf2=OFF, cnt=0
intf3=OFF, cnt=0
outside=OFF, cnt=4437
inside=OFF, cnt=0
intf4=OFF, cnt=0
intf5=OFF, cnt=0
intf6=OFF, cnt=0
intf7=OFF, cnt=0
intf8=OFF, cnt=0
```

```
intf9=OFF, cnt=0

Light#ping 100.100.100.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

Light#telnet 100.100.100.100 80
Trying 100.100.100.100, 80 ... Open
```

Risoluzione dei problemi

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

Informazioni correlate

- Fine vendita per Cisco IDS Director
- Fine del ciclo di vita del software sensore Cisco IDS versione 3.x
- Supporto dei prodotti Cisco Intrusion Prevention System
- Supporto dei prodotti software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Documentazione e supporto tecnico – Cisco Systems