IDS PIX-switching met Cisco IDS UNIX Director

Inhoud

Inleiding

Dit document beschrijft hoe u het draaien op een PIX kunt configureren met behulp van Cisco IDS UNIX Director (voorheen bekend als Network Director) en Sensor. In dit document wordt ervan uitgegaan dat de sensor en de Director operationeel zijn en dat de snuifinterface van de sensor is ingesteld om te spannen op de PIX-interface buiten.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies.

- Cisco IDS UNIX Director 2.2.3
- Cisco IDS UNIX-sensor 3.0.5
- Cisco Secure PIX met 6.1.1**Opmerking:** Als u de 6.2.x versie gebruikt, kunt u Secure Shell Protocol (SSH)-beheer gebruiken, maar niet telnet. Raadpleeg Cisco bug-ID CSCdx5215

(alleen geregistreerde klanten) voor meer informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

In deze sectie wordt u gepresenteerd met de informatie die wordt gebruikt om de functies te configureren die in dit document worden beschreven.

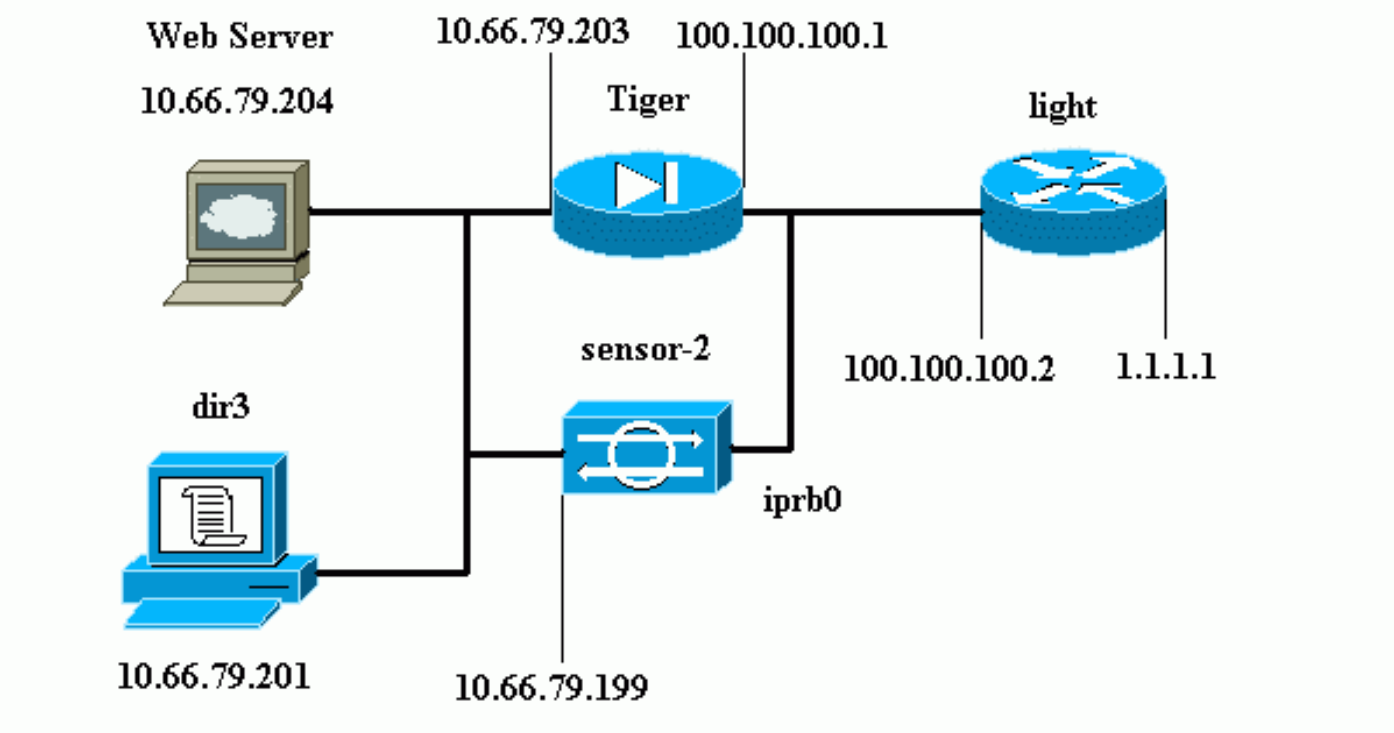
Cisco IDS UNIX Director en Sensor worden gebruikt om Cisco Secure PIX te beheren voor routing. Denk aan deze concepten:

- Installeer de sensor en controleer of de sensor goed werkt.
- Zorg ervoor dat de snuifinterface zich uitstrekt tot de buiteninterface van de PIX.

N.B.: Raadpleeg het Opdrachtplanningsgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten in dit document.

Netwerkdiagram

Dit document maakt gebruik van deze netwerkinstellingen.



Configuraties

Dit document gebruikt deze configuraties.

- Routerlicht
- PIX Tiger

Routerlicht

```
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
```

De sensor configureren

In deze stappen wordt beschreven hoe u de sensor moet configureren.

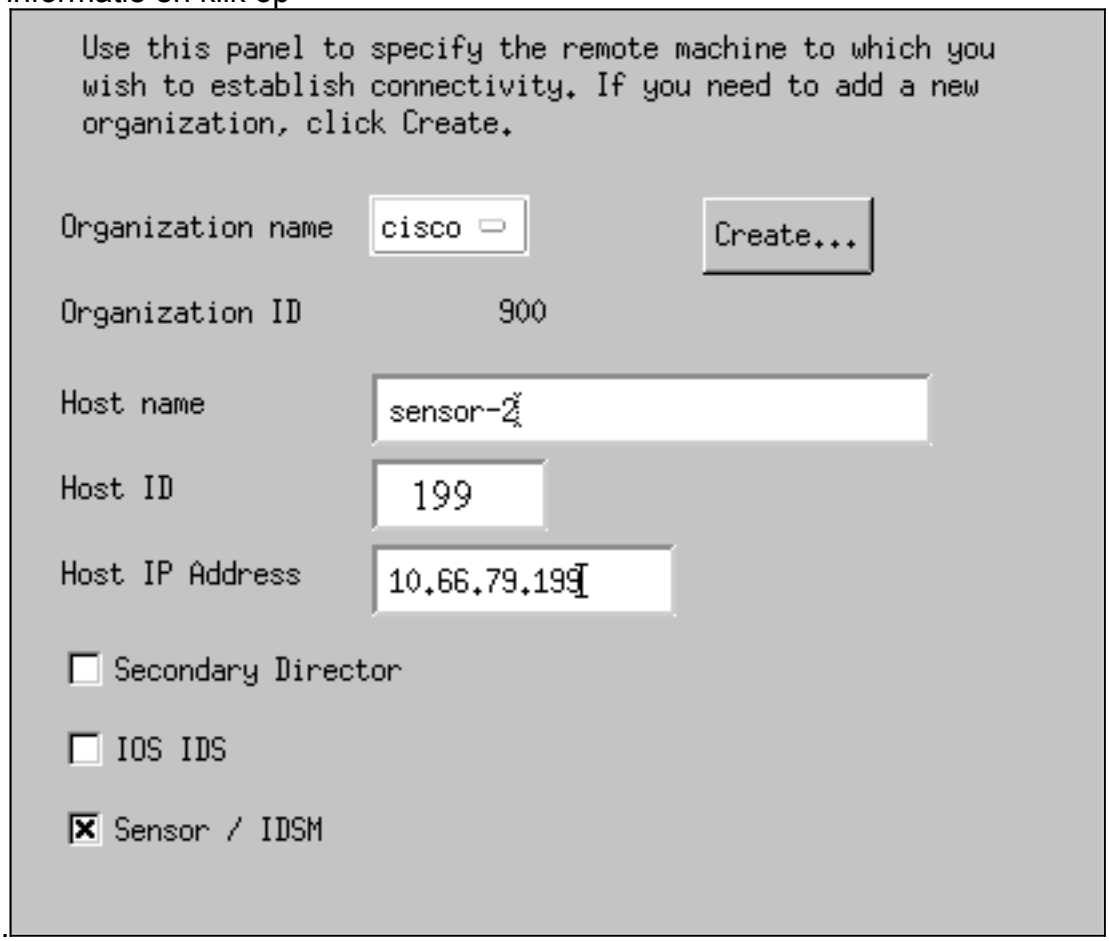
1. Telnet aan **10.66.79.199** met **gebruikersnaam wortel** en **wachtwoordaanval**.
2. Voer **een sysconfiguratie-sensor in**.
3. Voer deze informatie in:IP-adres: **10.66.79.199**IP-netwerkmasker: 255.255.255.224IP-hostnaam: **sensor-2**Standaard route: **10.66.79.193**Netwerktoegangscontrole**10.**Communicatie-infrastructuurSensor host-ID: 49ID van de sensor: 900Sensor hostnaam: **sensor-2**Naam van de sensor: **Cisco**IP-adres sensor: **10.66.79.199**IDS Manager Host ID: 50ID van IDS Manager-organisatie: 900IDS Manager-hostnaam: **dir3**Naam van IDS Manager-organisatie: **Cisco**IDS Manager IP-adres: **10.66.79.201**
4. Bewaar de configuratie. De sensor start opnieuw.

Stop de sensor in de regisseur

Volg deze stappen om de sensor aan de directeur toe te voegen.

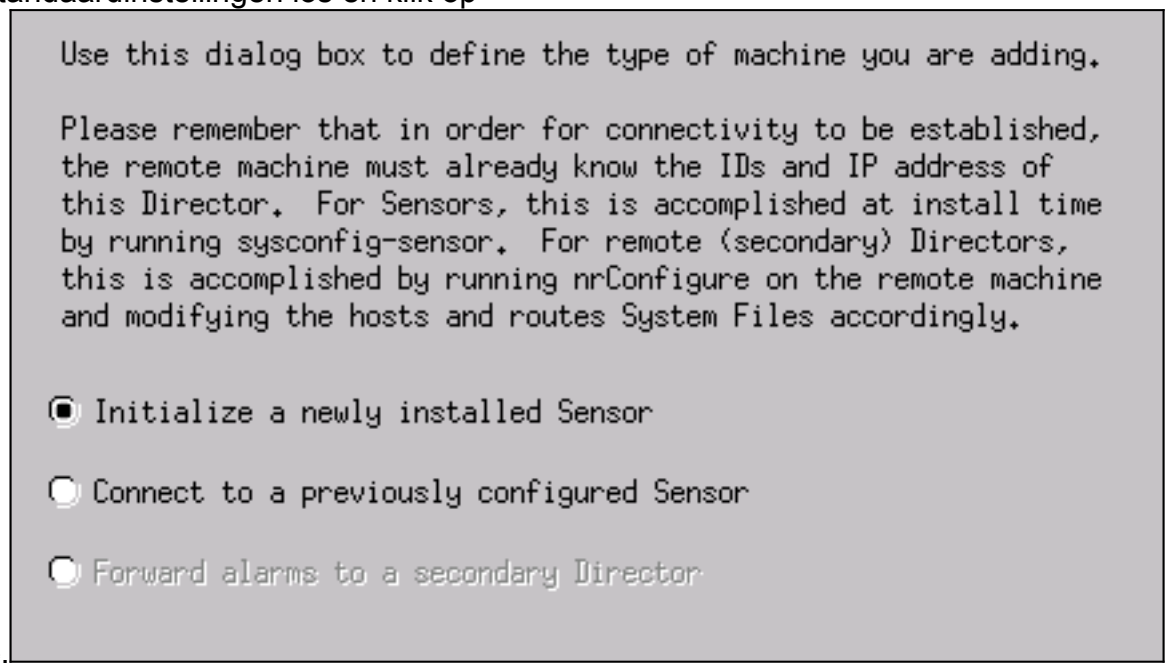
1. Telnet aan **10.66.79.201** met **gebruikersnaamnetwerk** en **wachtwoordaanval**.

2. Voer **ovw&** in om HP OpenView te starten.
3. Selecteer in het hoofdmenu de optie **Beveiliging** > **Configureren**.
4. Selecteer in het menu Network Configuration **File** > **Add Host** en klik op **Next**.
5. Typ deze informatie en klik op



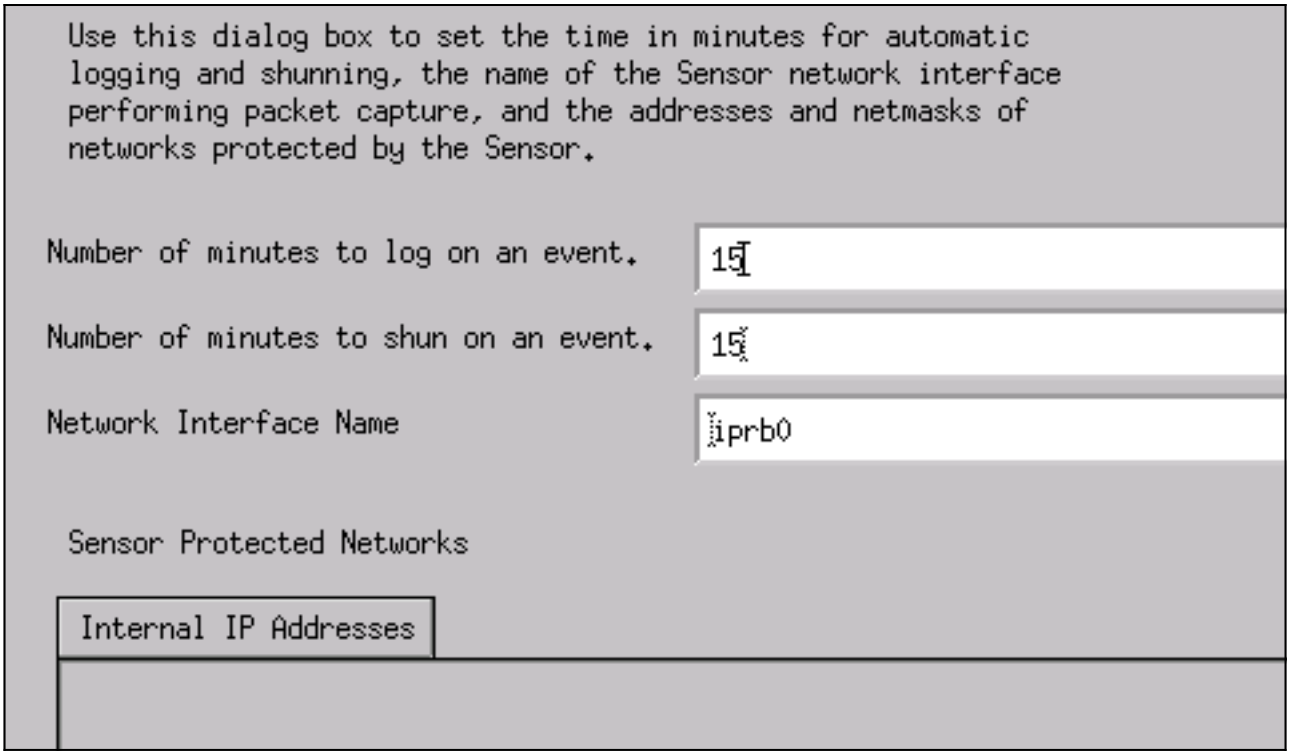
Volgende.

6. Laat de standaardinstellingen los en klik op

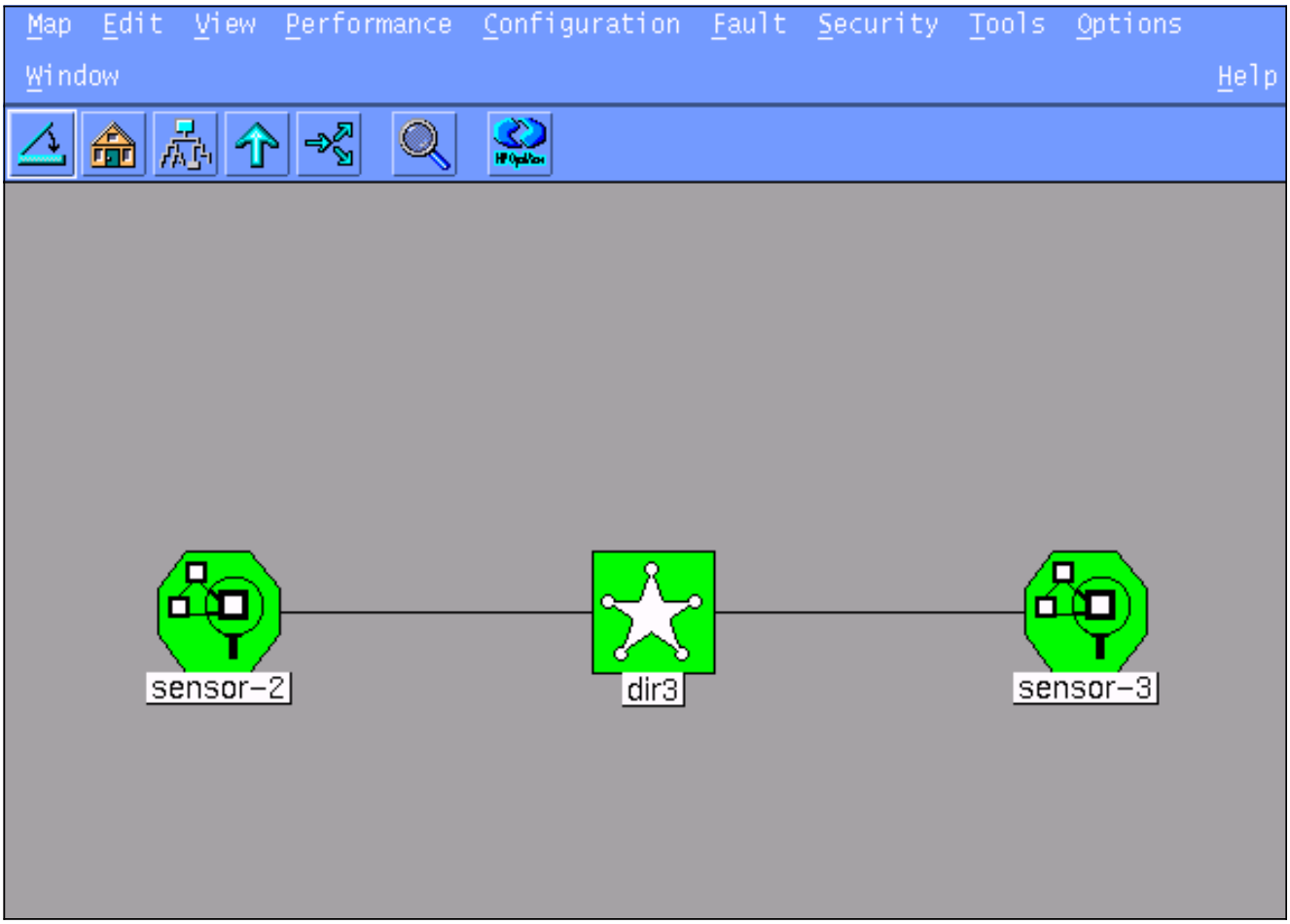


Volgende.

7. Wijzig het logbestand en de minuten in of laat deze standaard als de waarden acceptabel zijn. Wijzig de naam van de interface van het netwerk in de naam van uw snuffelinterface. In dit voorbeeld is het "iprb0". Dit kan zijn "spwr0" of iets anders, gebaseerd op het type sensor en de manier waarop u de sensor
aansluit.



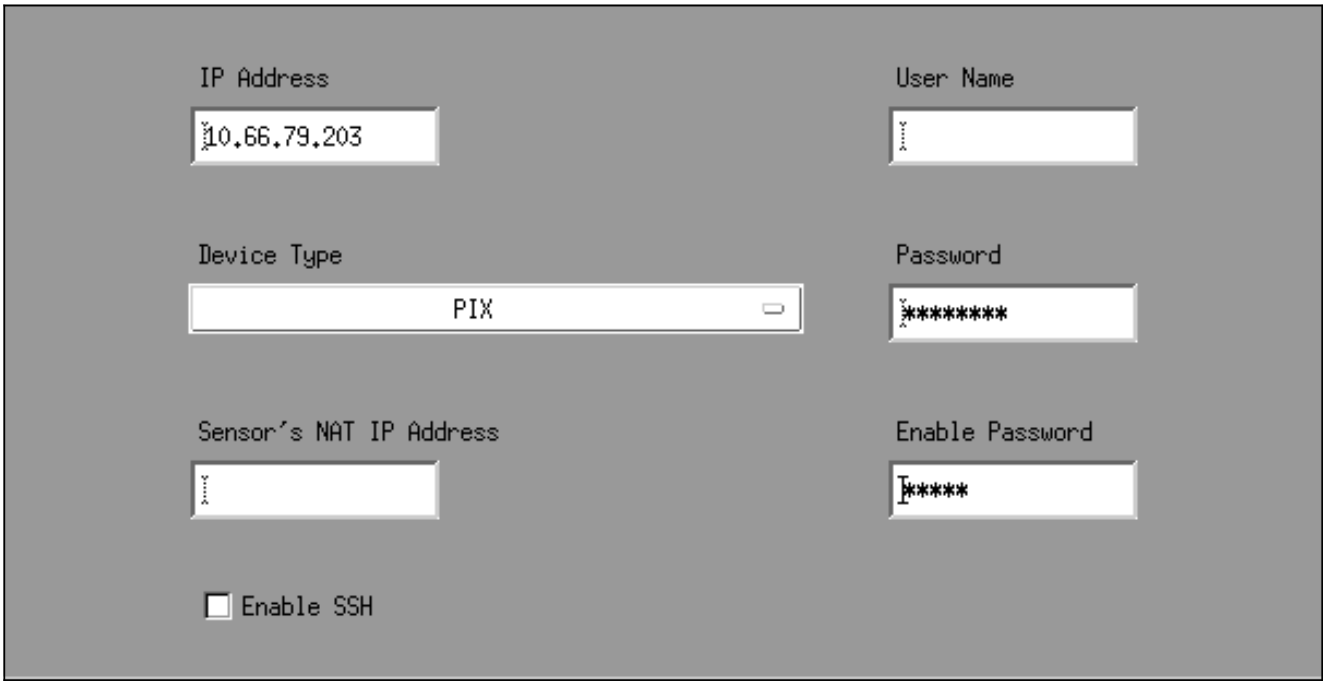
8. Klik op **Volgende** totdat er een optie is om op **Voltooien** te klikken.De sensor wordt nu toegevoegd aan de Director. In het hoofdmenu wordt **sensor-2** weergegeven, zoals in dit voorbeeld.



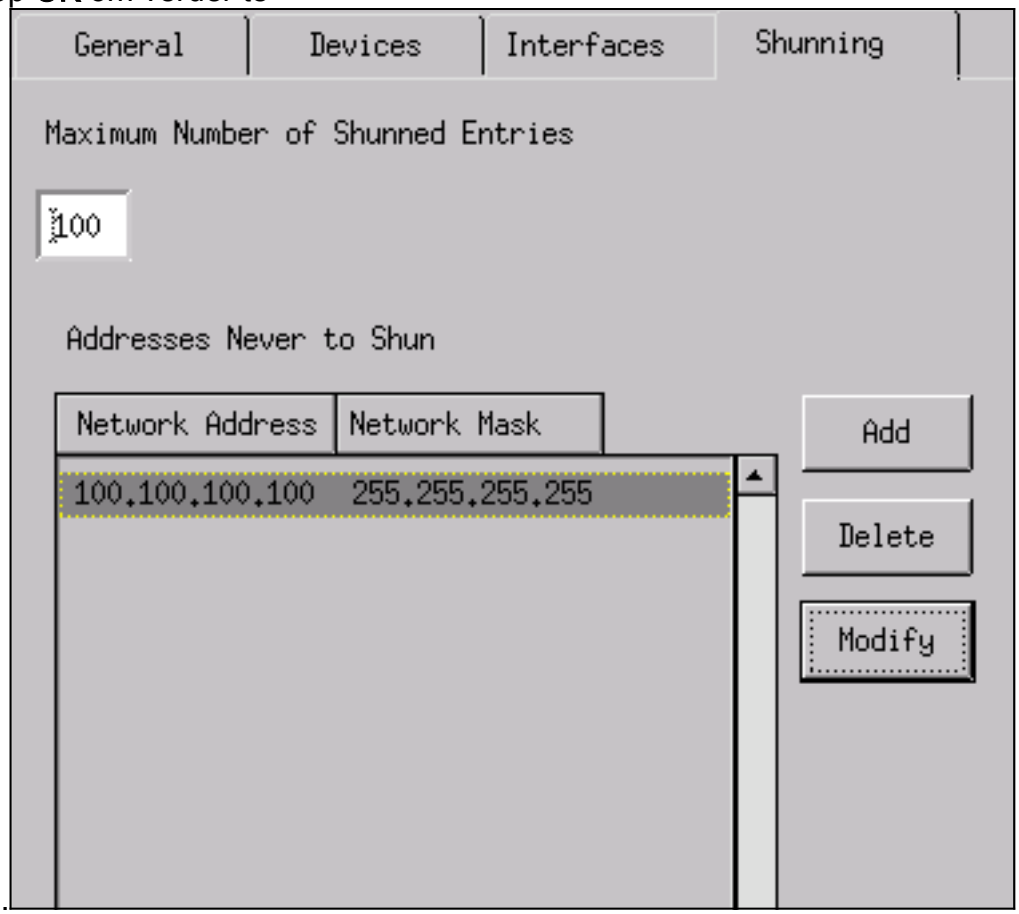
Shunning voor PIX configureren

Voltooi deze stappen om het draaien voor PIX te configureren.

1. Selecteer in het hoofdmenu de optie **Beveiliging > Configureren**.
2. Markeer in het menu Network Configuration **sensor-2** en dubbelklik op deze.
3. **Apparaatbeheer** openen.
4. Klik op **Apparaten > Add** en voer de informatie in zoals in dit voorbeeld. Klik op **OK** om verder te gaan. Het telnet en laat wachtwoord toe zijn beiden "Cisco".

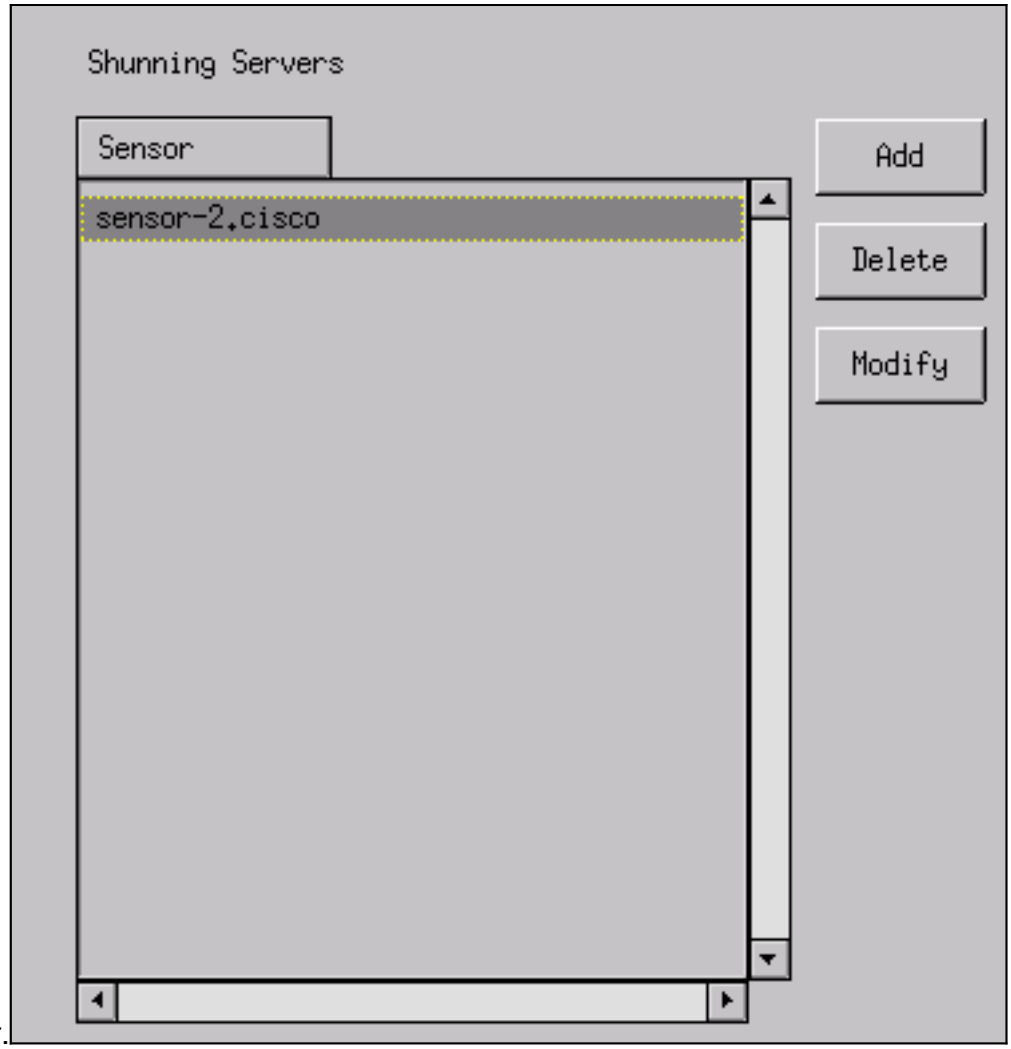


5. Klik op **Shunning > Add**. Voeg host **100.100.100.100** toe onder "Adressaten nooit aan Shun." Klik op **OK** om verder te gaan.

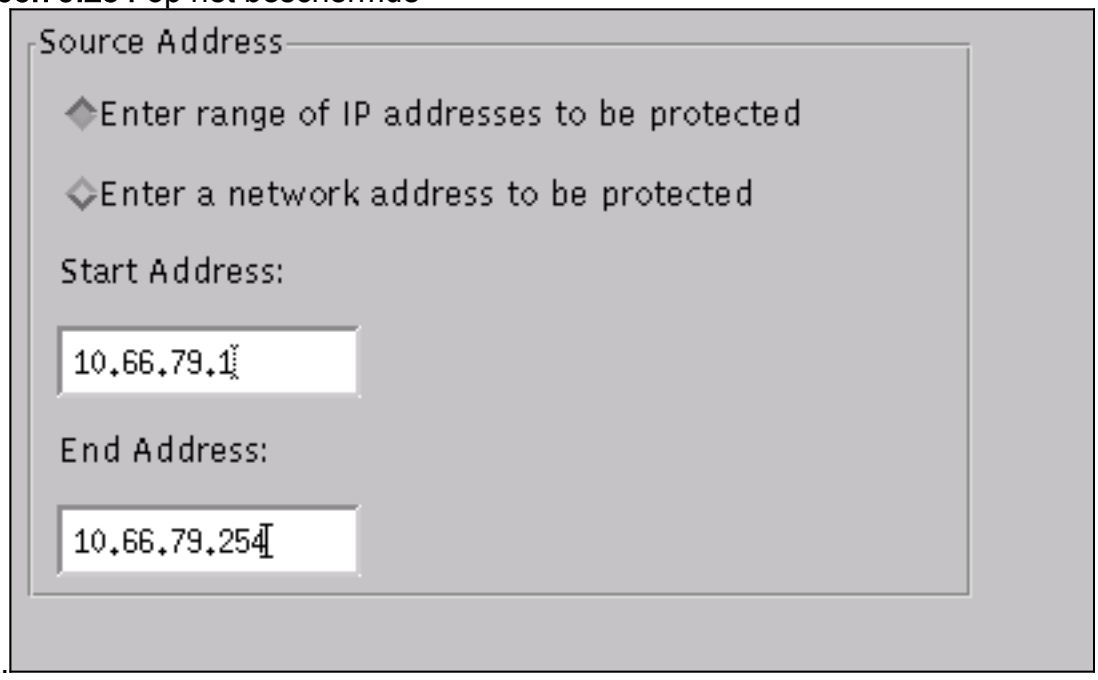


6. Klik op **Shunning > Add** en selecteer **sensor-2.cisco** als de schaduwservers. Dit gedeelte van de configuratie is voltooid. Sluit het venster

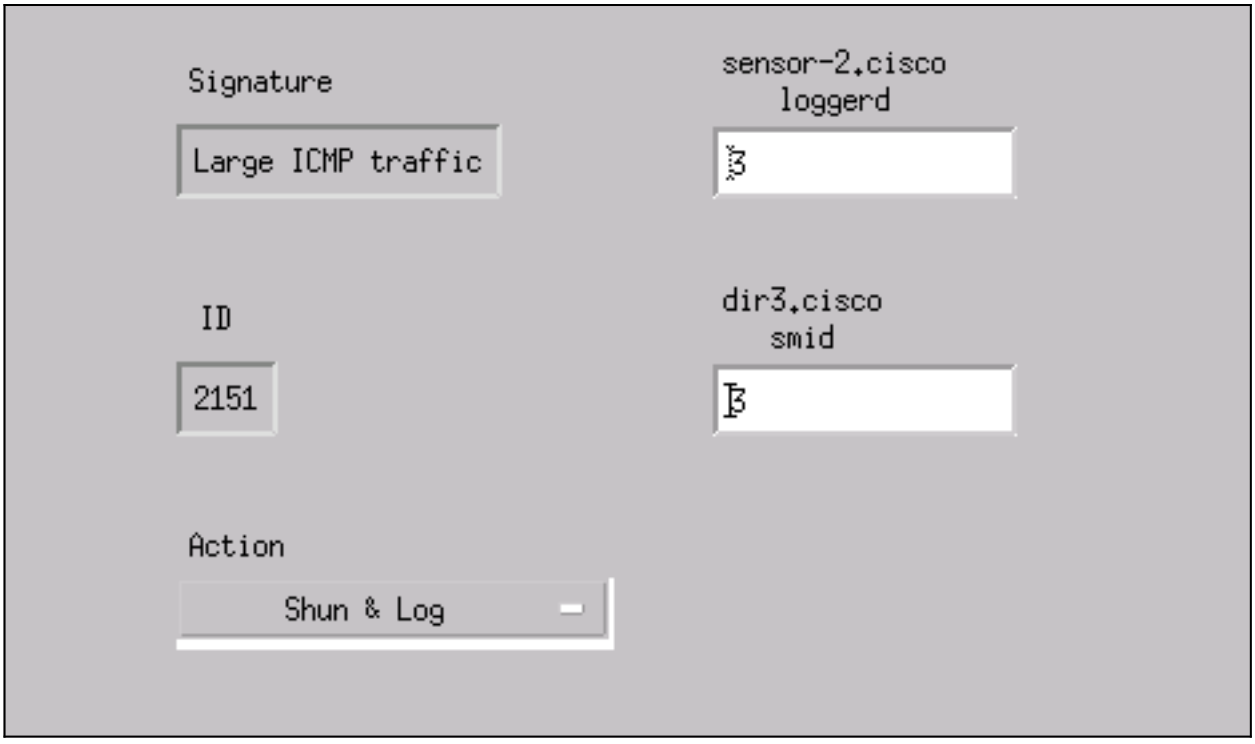
Apparaatbeheer.



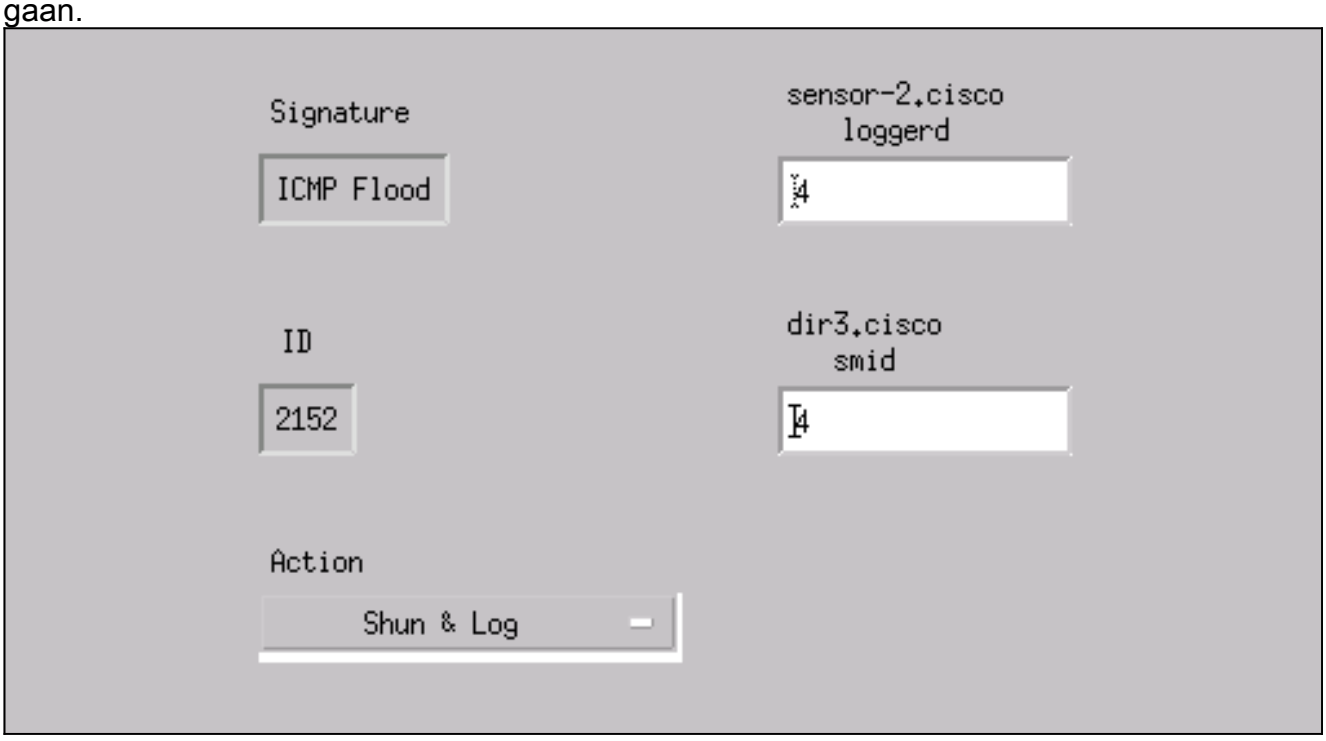
7. Open het venster voor inbraakdetectie en klik op **Beveiligde netwerken**. Voeg **10.66.79.1** toe aan **10.66.79.254** op het beschermde netwerk.



8. Klik op **Profiel** en selecteer **Handmatige configuratie > Handtekeningen wijzigen**. Selecteer **Groot ICMP verkeer** en **ID: 2151**, klik op **Wijzigen**, en wijzig de Actie van Geen in **Shun en Log**. Klik op **OK** om verder te gaan.

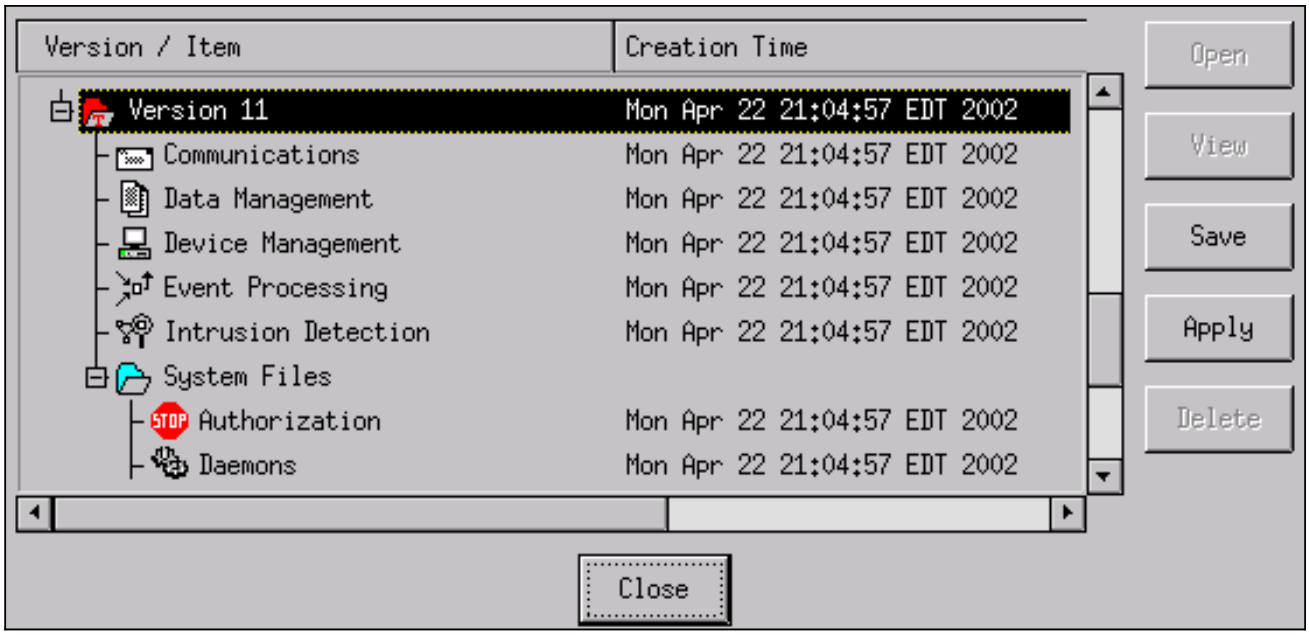


9. Selecteer **ICMP Flood** and **ID: 2152**, klik op **Wijzigen**, en wijzig de Actie van **Geen** in **Shun en Log**. Klik op **OK** om verder te
gaan.



10. Dit gedeelte van de configuratie is voltooid. Klik op **OK** om het venster voor inbraakdetectie te sluiten.
11. Open de map **Systeembestanden** en open het venster **Daemons**. Zorg ervoor dat u deze datums hebt
ingeschakeld:

12. Klik op **OK** om door te gaan en selecteer de zojuist aangepaste versie. Klik op **Opslaan** > **Toepassen**. Wacht totdat het systeem u heeft verteld dat de Sensor klaar is, start de services opnieuw en sluit alle vensters voor de configuratie van Netor.



Verifiëren

Deze sectie verschaft informatie die u helpt om te bevestigen dat de configuratie correct werkt.

Voordat u de aanval start

```
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
```

De aanval en de planning starten

```
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
```

Vijftien minuten later is het weer normaal, want de planning wordt op vijftien minuten gesteld.

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- End-of-sale voor Cisco IDS Director
- End-of-life voor Cisco IDS Sensor softwareversie 3.x
- Productondersteuning voor Cisco-inbraakpreventiesysteem
- Productondersteuning voor Cisco PIX-firewall
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Technische ondersteuning en documentatie – Cisco Systems