# Shunning instellen op een UNIX-directeur

## Inhoud



## Inleiding

Cisco Inbraakdetectiesysteem (IDS) Director en Sensor kunnen worden gebruikt om een Cisco-router voor routing te beheren. In dit document is een sensor (sensor-2) ingesteld om aanvallen op de router "House" te detecteren en deze informatie door te geven aan de directeur "dir3". Zodra deze geconfigureerd is een aanval gestart (ping van meer dan 1024 bytes, wat kenmerkend is voor 2151, en een Internet Control Message Protocol [ICMP], dat kenmerkend is voor 2152) van router "Light". De sensor detecteert de aanval en deelt dit aan de directeur mee. Een toegangscontrolelijst (ACL) wordt gedownload naar de router om verkeer vanaf de aanvaller te verwijderen. Op de aanslagpleger `gastheer onbereikbaar` wordt getoond, en op het slachtoffer wordt gedownload ACL getoond.

## Voorwaarden

### Vereisten

Zorg er voordat u deze configuratie probeert voor dat u aan deze vereisten voldoet:

- Installeer de sensor en controleer of deze goed werkt.
- Zorg ervoor dat de snuffelinterface zich uitstrekt tot aan de externe interface van de router.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IDS Director 2.2.3
- Cisco IDS-sensor 3.0.5
- Cisco IOS-router met 12.2.6

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.

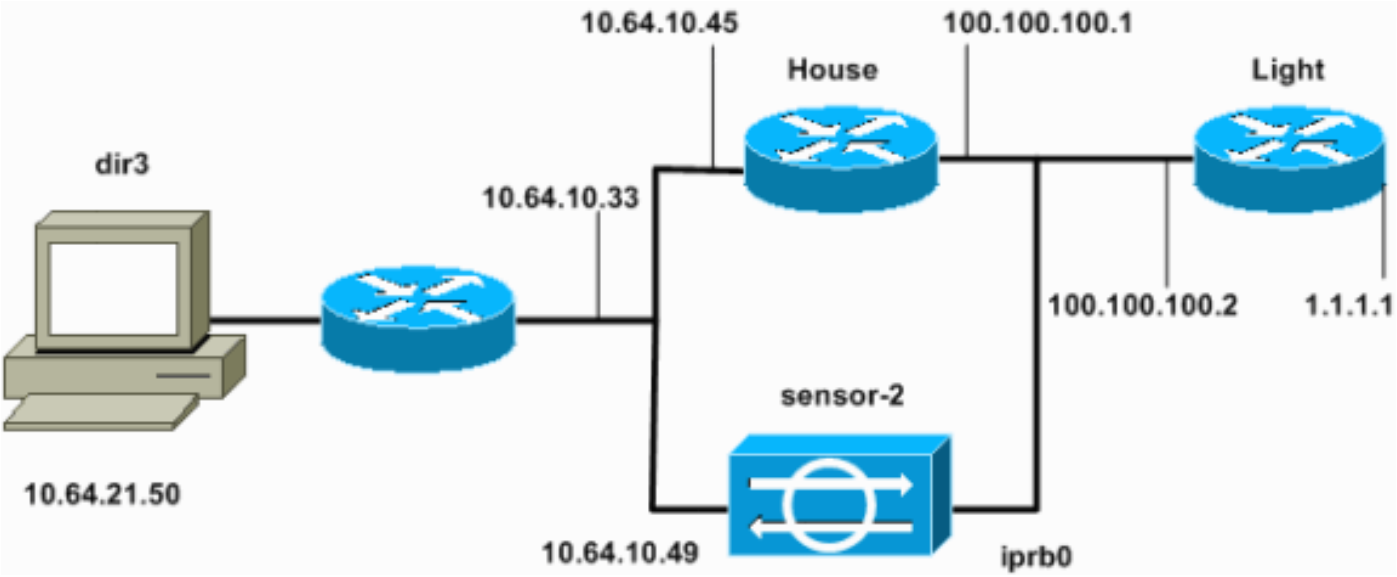
# Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**N.B.:** Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

## Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.




## Configuraties

Dit document gebruikt deze configuraties.

- Routerlicht
- Routerhuis

| 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
!
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
```

## Routerhuis

```
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#
```

## De sensor configureren

Volg deze stappen om de sensor te configureren.

1. Telnet aan **10.64.10.49** met **gebruikersnaam wortel** en **wachtwoordaanval**.
2. Voer **een sysconfiguratie-sensor in**.
3. Voer de configuratieinformatie in, zoals in dit voorbeeld, wanneer gevraagd.

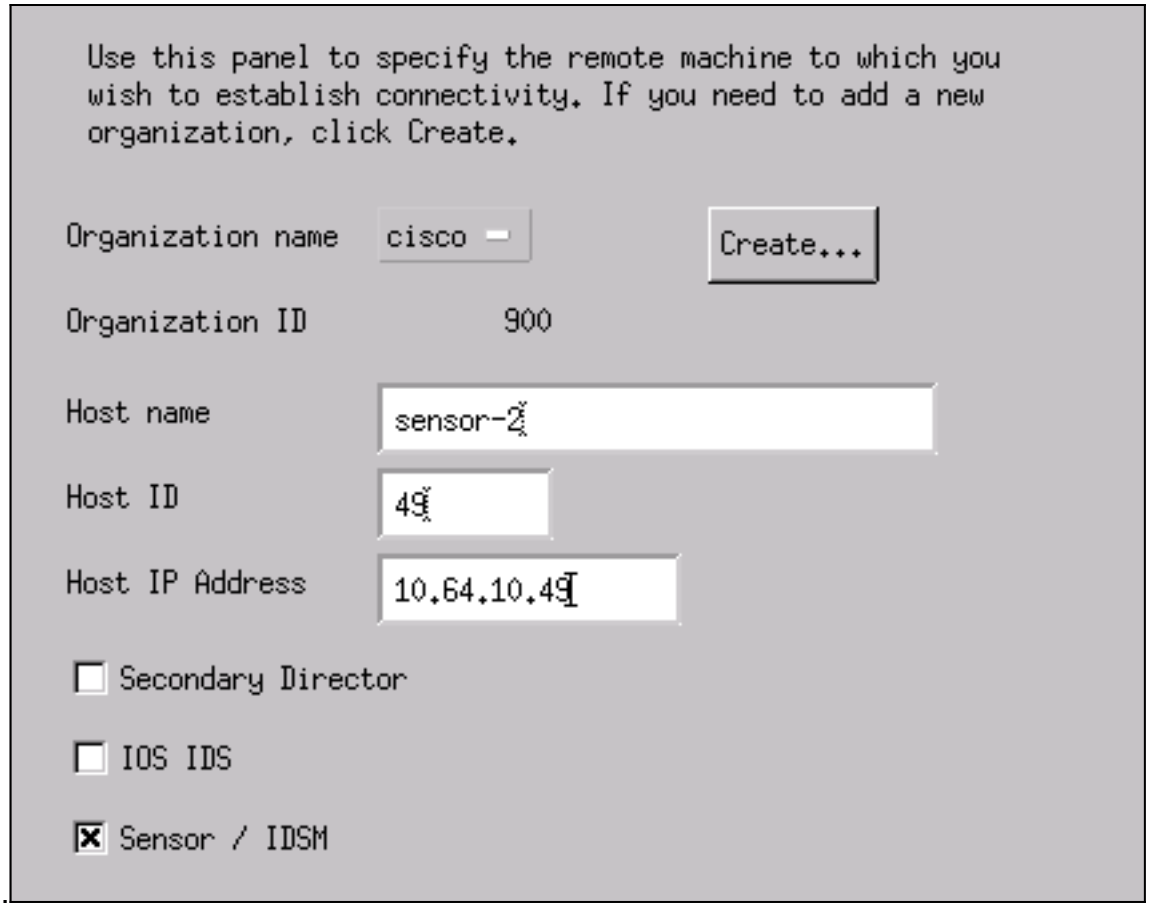
```
1 - IP Address: 10.64.10.49
2 - IP Netmask: 255.255.255.224
3 - IP Host Name:  sensor-2
4 - Default Route     10.64.10.33
5 - Network Access Control
          64.
          10.
6 - Communications Infrastructure
Sensor Host ID: 49
Sensor Organization ID:     900
Sensor Host Name: sensor-2
Sensor Organization 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. Bewaar de configuratie wanneer dit wordt gevraagd en laat de sensor opnieuw opstarten.

## Voeg de sensor toe aan de directeur

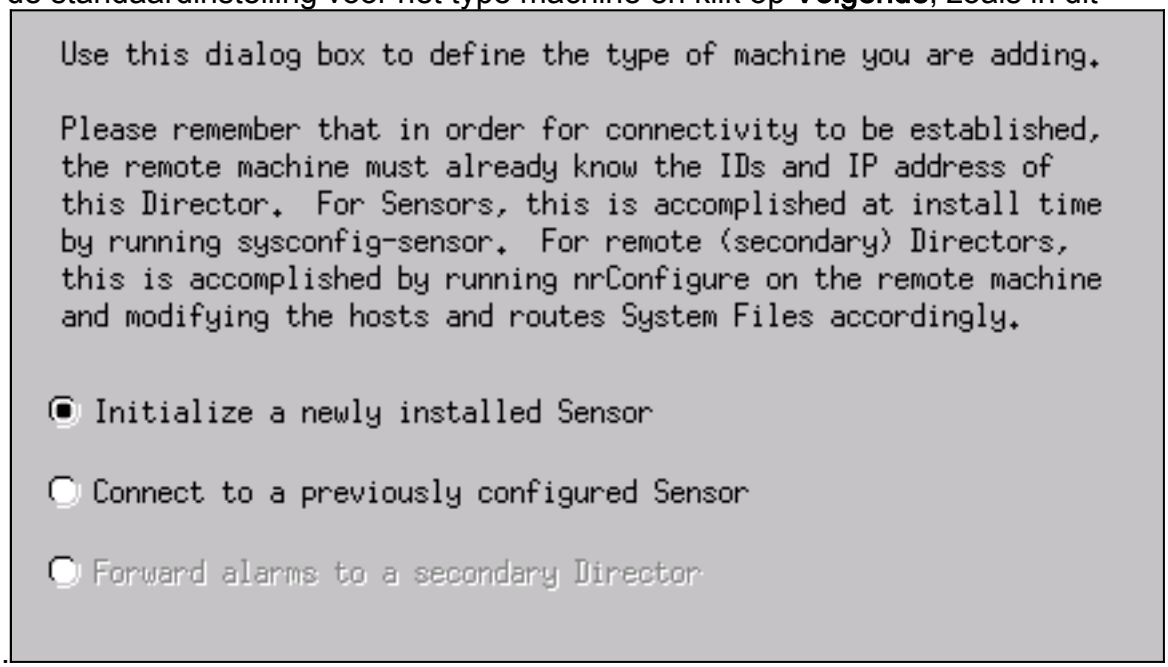
Volg deze stappen om de sensor aan de directeur toe te voegen.

1. Telnet aan **10.64.21.50** met **gebruikersnaamnetwerk** en **wachtwoordaanval**.
2. Voer **ovw&** om HP OpenView in te starten.
3. Selecteer in het hoofdmenu de optie **Beveiliging > Configureren**.
4. Selecteer in het hulpprogramma Configuration File Management **File > Add Host**, en klik op **Next**.
5. Dit is een voorbeeld van hoe de gevraagde informatie moet worden



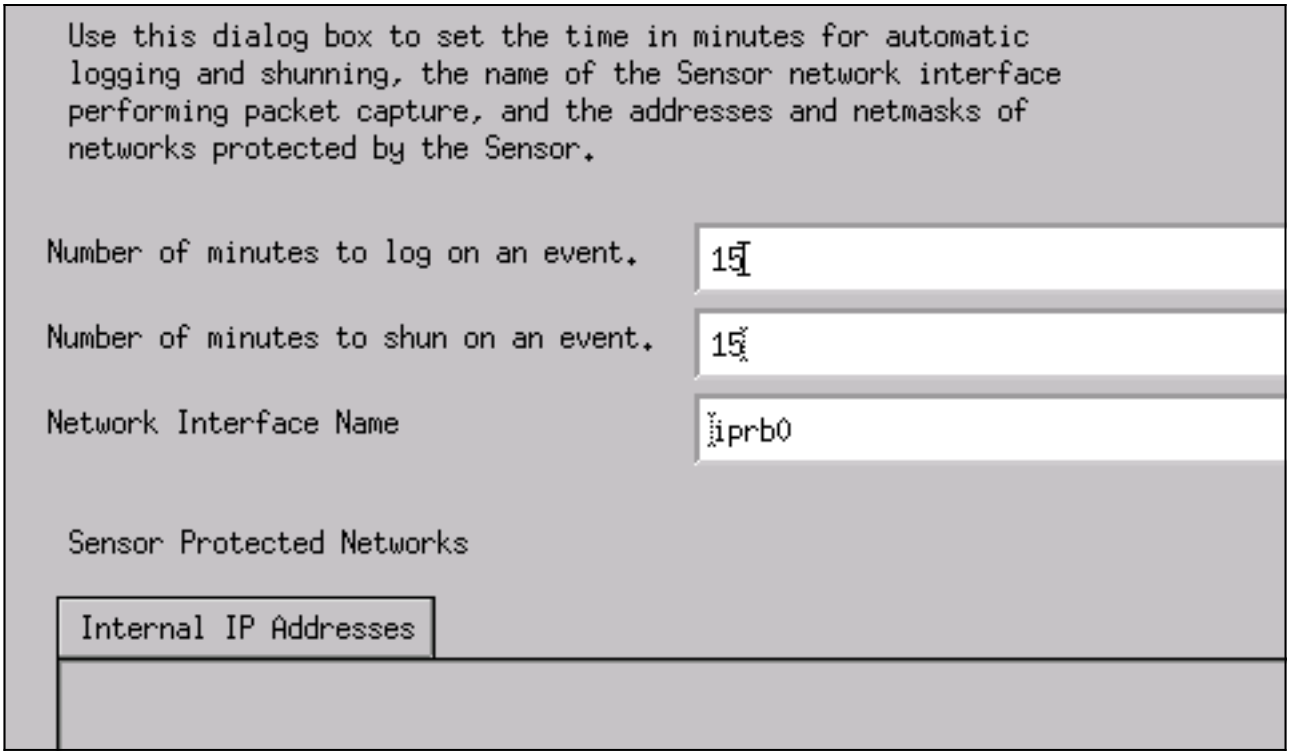

ingevuld.

6. Aanvaard de standaardinstelling voor het type machine en klik op **Volgende**, zoals in dit

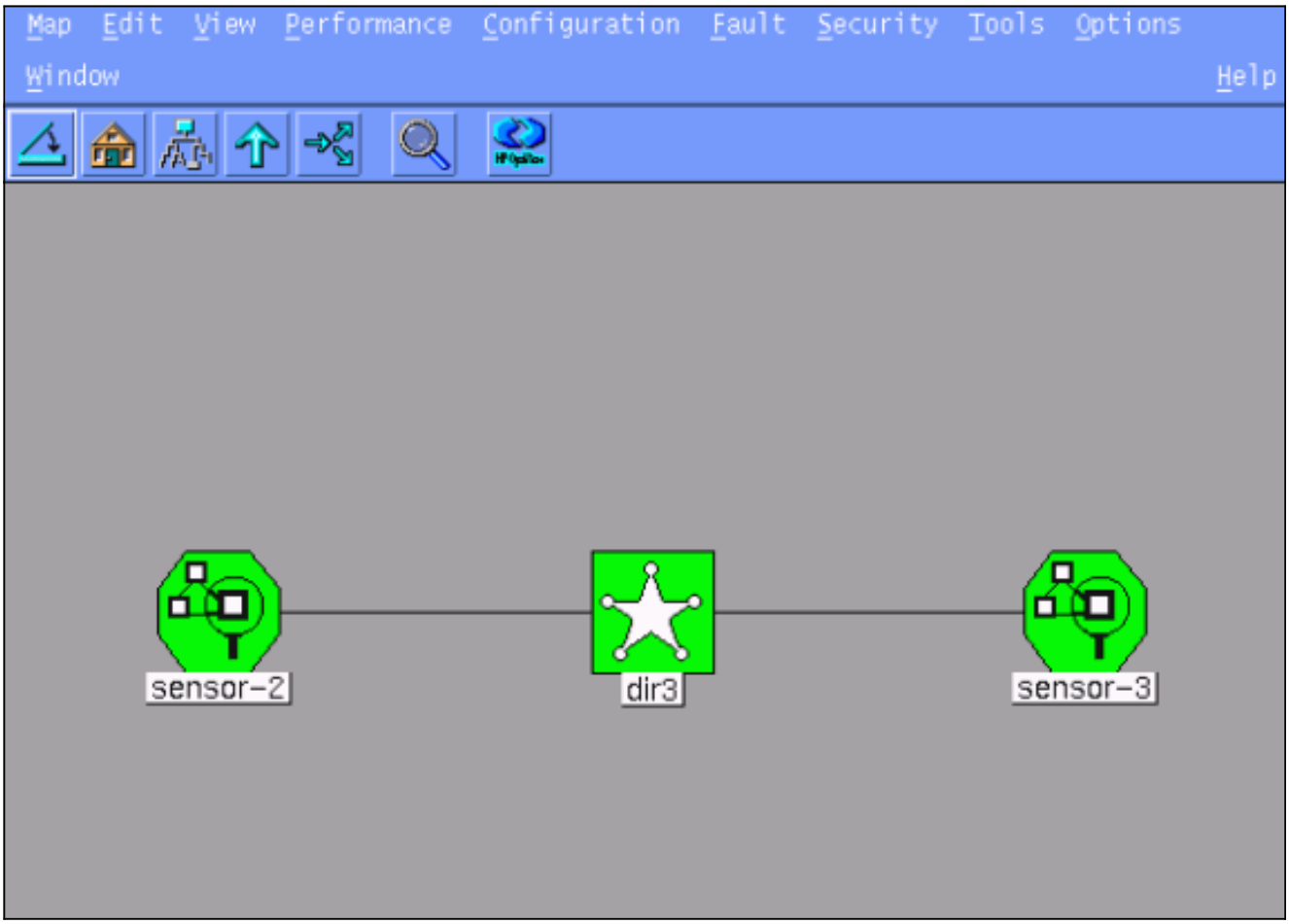



voorbeeld.

7. Wijzig het logbestand en de minuten uit, of laat deze standaard als de waarden acceptabel zijn. Wijzig de naam van de netwerkinterface in de naam van uw snuffelinterface.In dit voorbeeld is het "iprb0". Afhankelijk van het type sensor en de manier waarop u de sensor aansluit, kan deze "SPW0" of iets anders
zijn.



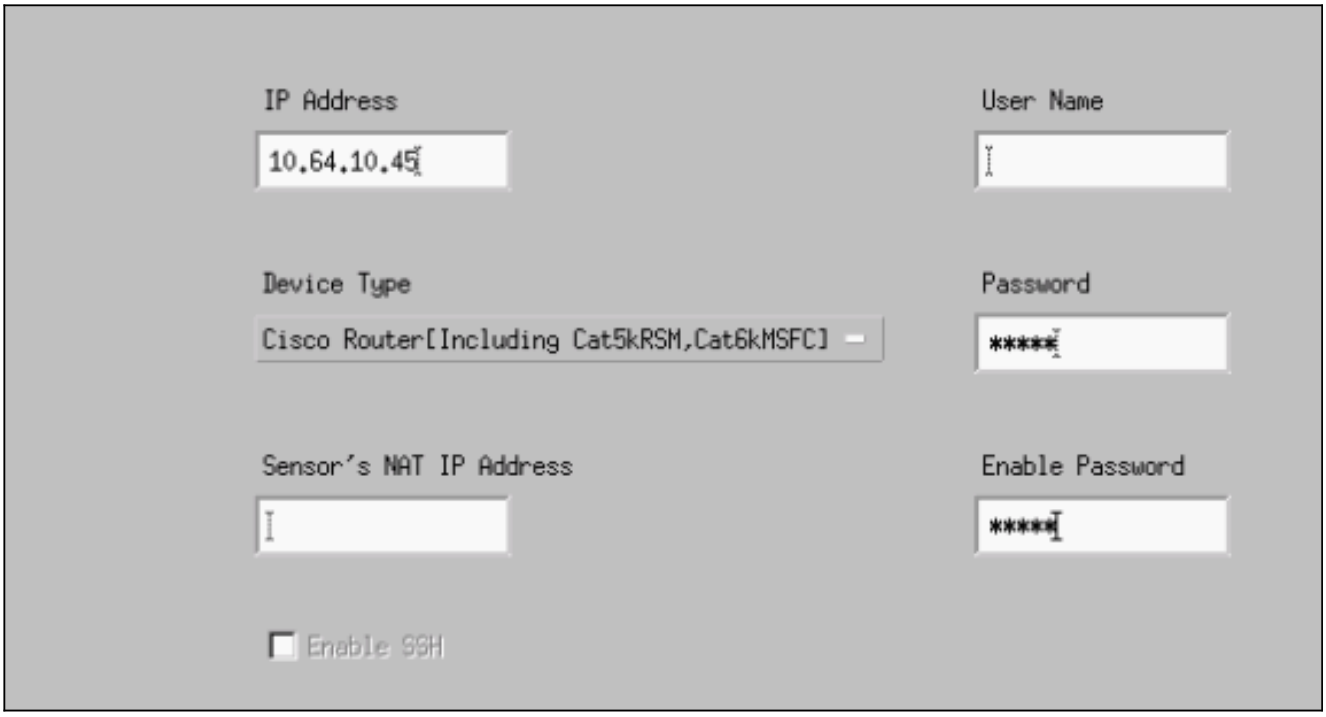

8. Klik op **Volgende** totdat er een optie is om op **Voltooien** te klikken.U hebt de sensor toegevoegd aan Director. In het hoofdmenu moet u `sensor-2` zien, zoals in dit voorbeeld.



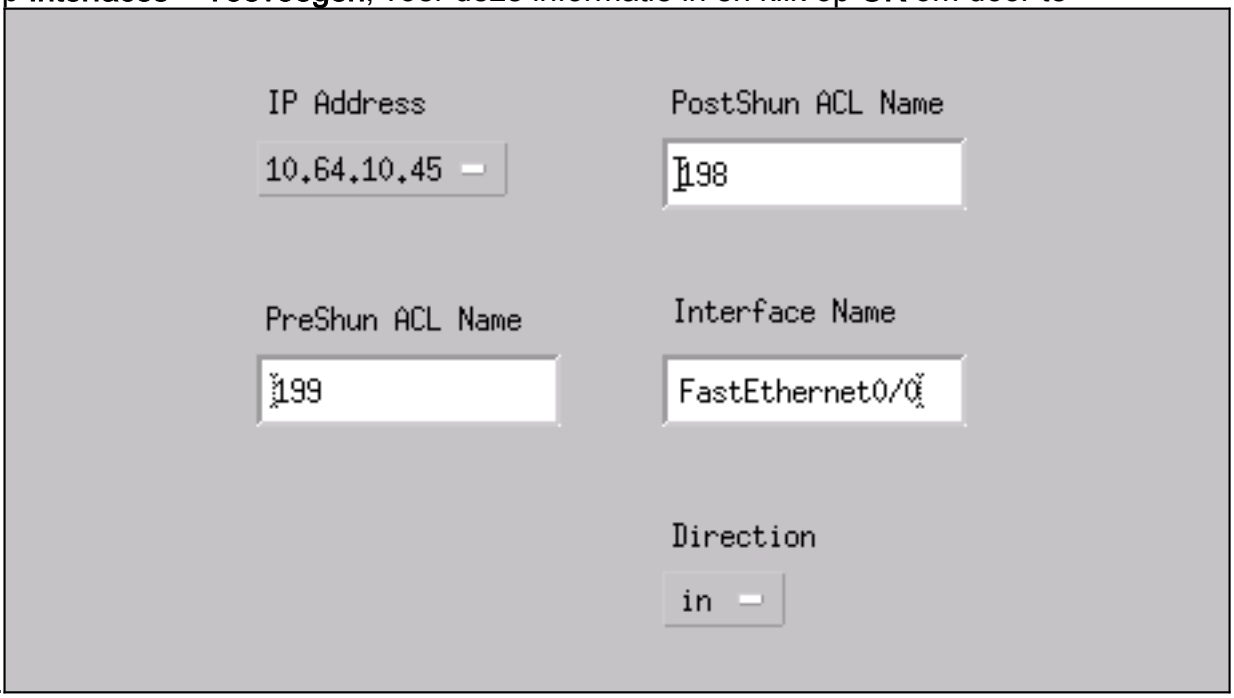

## Shunning configureren voor Cisco IOS-router

Voltooi deze stappen om het shunning voor de Cisco IOS router te configureren.

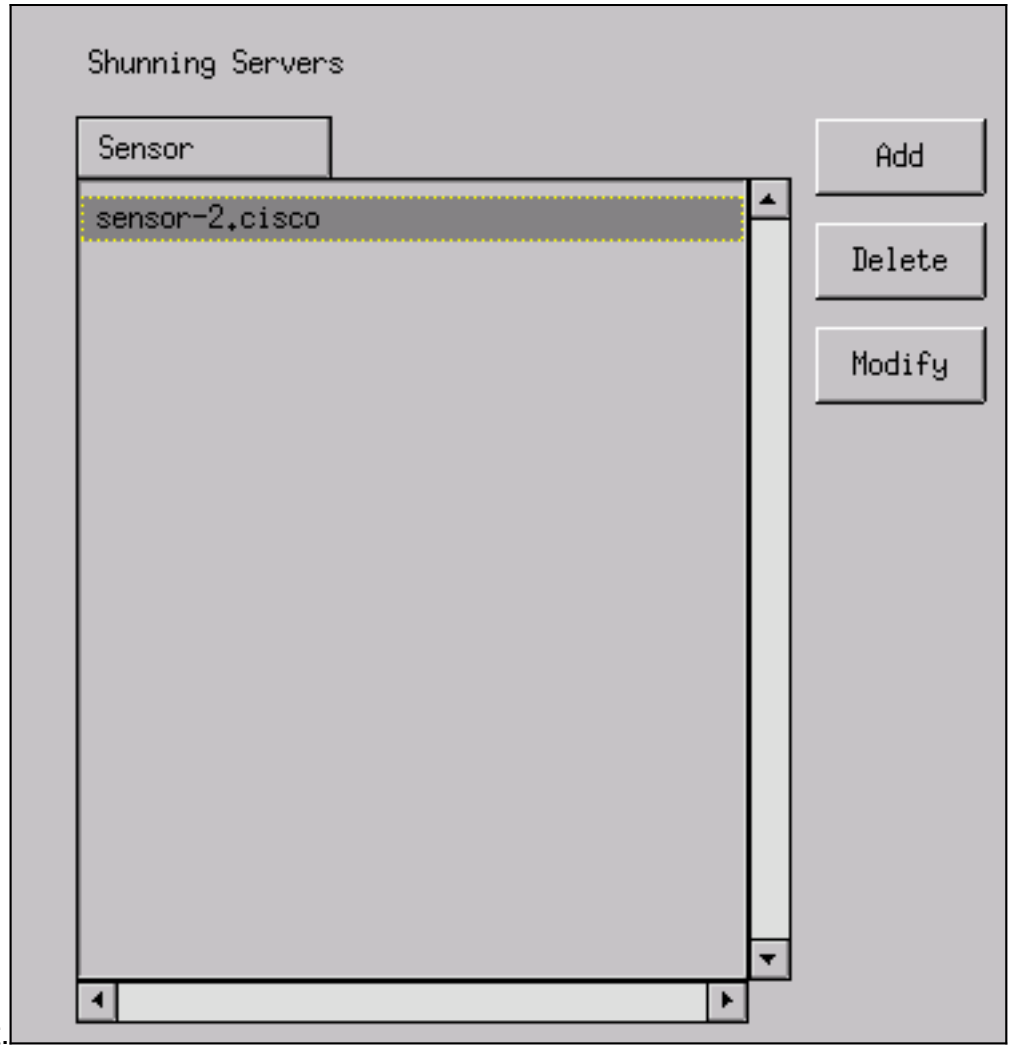
1. Selecteer in het hoofdmenu de optie **Beveiliging > Configureren**.
2. Markeer **sensor-2** in het **hulpprogramma** Configuration File Management en dubbelklik op deze optie.
3. **Apparaatbeheer** openen.
4. Klik op **Apparaten > Toevoegen** en voer de informatie in zoals in dit voorbeeld. Klik op **OK** om verder te gaan.Het telnet en laat wachtwoorden toe om te passen wat in de router "Huis" is.




5. Klik op **Interfaces > Toevoegen**, voer deze informatie in en klik op **OK** om door te gaan.

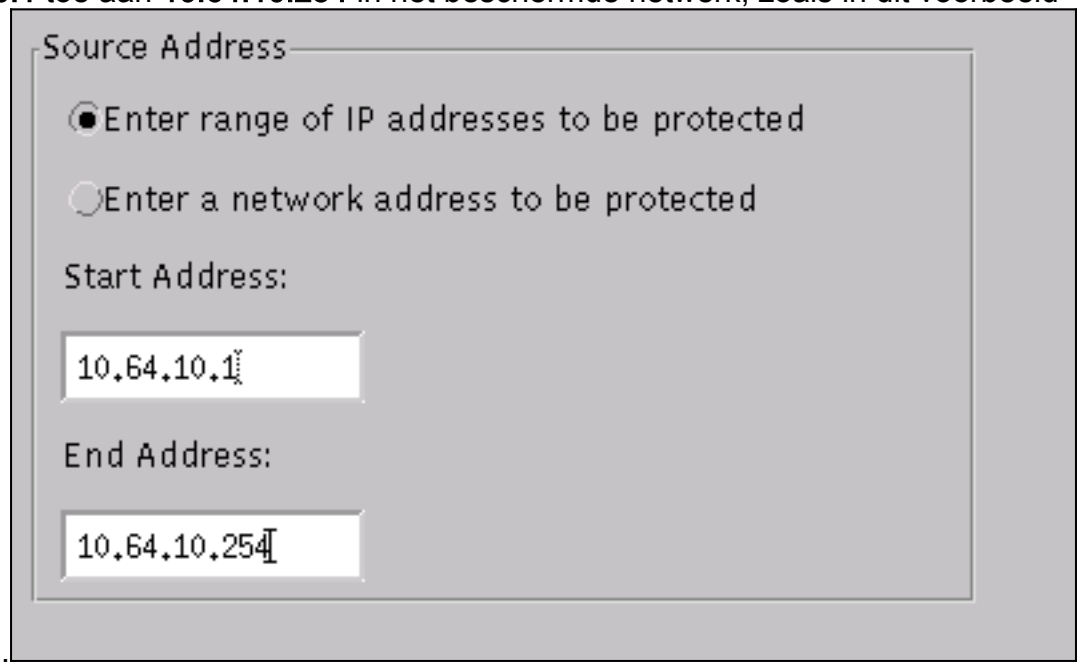



6. Klik op **Shunning > Add** en selecteer **sensor-2.cisco** als de schaduwserver. Sluit het venster Apparaatbeheer wanneer u klaar



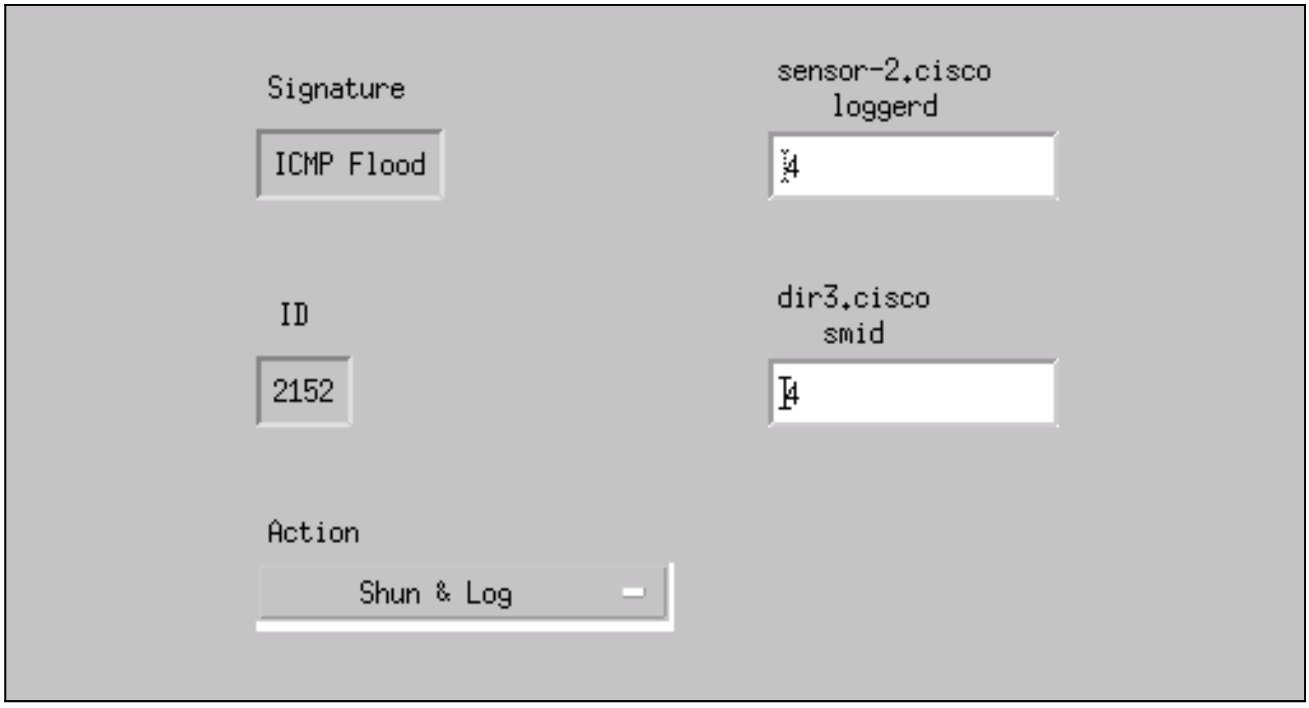

bent.

7. Open het venster voor inbraakdetectie en klik op **Beveiligde netwerken**. Voeg het bereik **10.64.10.1** toe aan **10.64.10.254** in het beschermde netwerk, zoals in dit voorbeeld

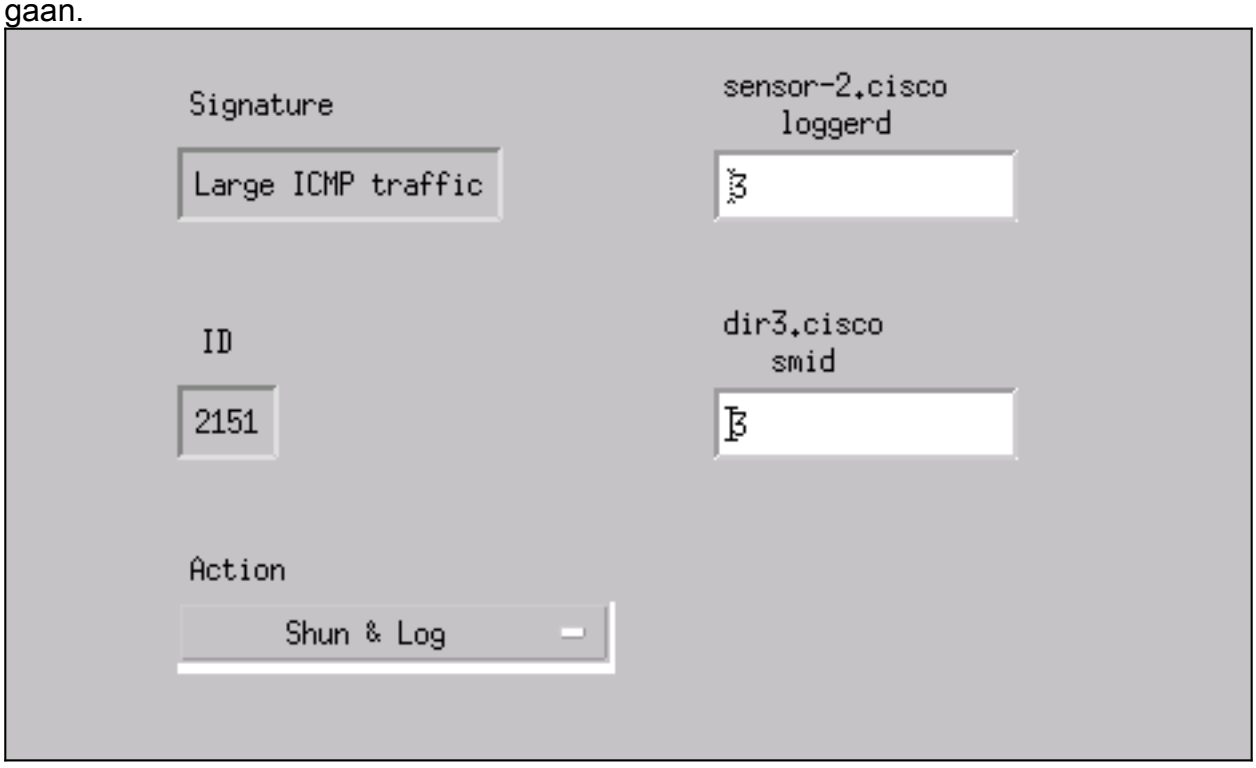



getoond.

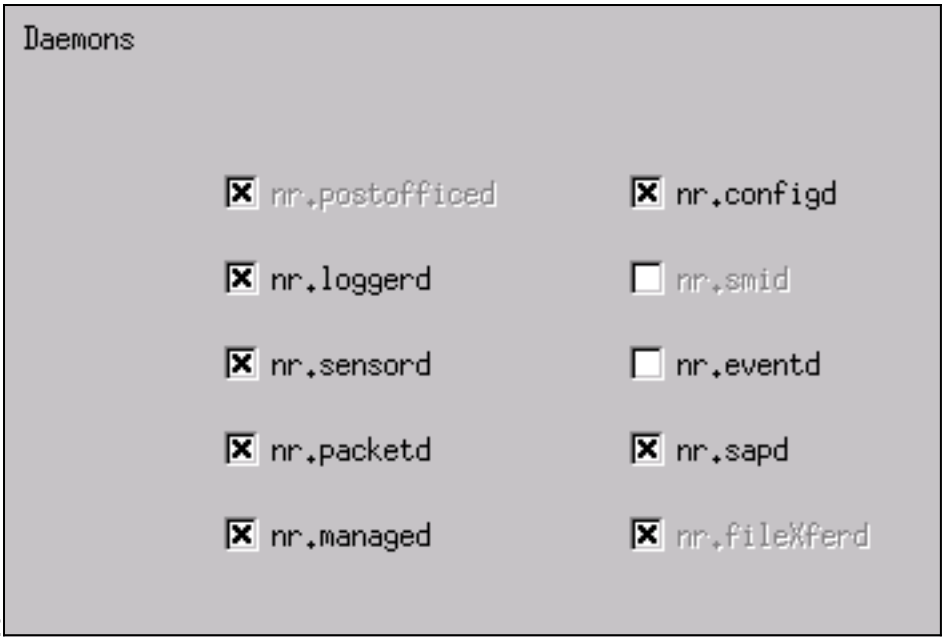
8. Klik op **Profiel > Handmatige configuratie**.
9. Selecteer **Handtekeningen wijzigen > Groot ICMP-verkeer** met een ID van **2151**.
10. Klik op **Wijzigen**, wijzig de **Actie** van Geen in **Shun & Log** en klik op **OK** om verder te gaan.




11. Kies **ICMP Flood** met een ID van **2152** en klik **Wijzigen**. Verander de **Actie** van Geen in **Shun & Log** en klik op **OK** om door te gaan.

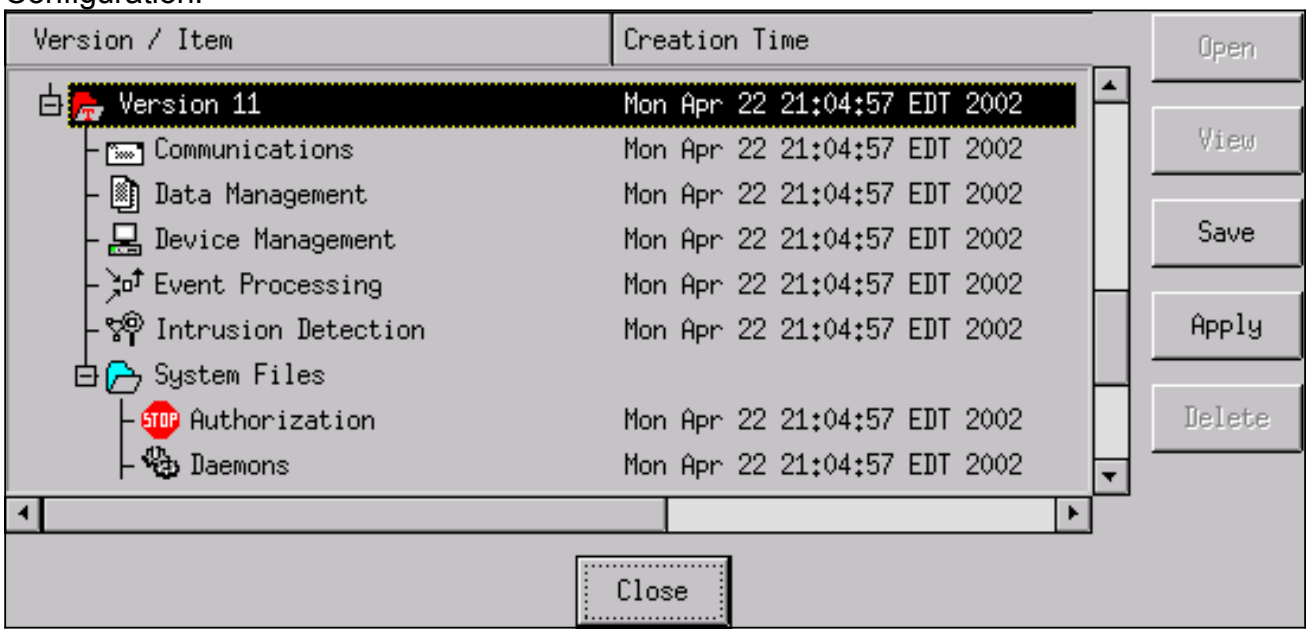



12. Klik op **OK** om het venster voor inbraakdetectie te sluiten.
13. Open de map Systeembestanden en open het Datumvenster.Zorg ervoor dat u deze datums hebt




ingeschakeld:

14. Klik op **OK** om door te gaan, kies de zojuist aangepaste versie en klik op **Opslaan** en **Toepassen**.Wacht totdat het systeem u heeft verteld dat de Sensor klaar is met het herstarten van de services en sluit vervolgens alle vensters voor de Director Configuration.




## Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **Toon toegang-lijst** - Toont de **toegang-lijst** bevelverklaringen in de routerconfiguratie. Het maakt ook een lijst van een hit die het aantal keer aangeeft dat een element is gematcht tijdens een opdracht **op een toegangslijst**.
- **ping** - gebruikt om de basisnetwerkconnectiviteit te diagnosticeren.

## Voordat er een aanval wordt gestart

Voordat een aanval wordt gestart, geeft u deze opdrachten uit.

```
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#
```

## De aanval en de planning starten

Start uw aanval van de router "Licht" naar het slachtoffer "Huis". Wanneer ACL wordt beïnvloed, worden de onbereikbare gebieden gezien.

```
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.U.
```

Zodra de Sensor de aanval heeft gedetecteerd, wordt ACL gedownload, en deze uitvoer wordt weergegeven op "House".

```
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
```

Onbereikbaar zijn nog steeds te zien op "Licht", zoals in dit voorbeeld wordt getoond.

```
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)
```

Vijftien minuten later is 'Huis' weer normaal, want het is ingesteld op 15 minuten.

```
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#
```

'Licht' kan 'Huis' pingelen.

```
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
```

## Problemen oplossen

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

## Gerelateerde informatie

- Cisco-pagina voor beveiligde inbraakpreventie
- Technische ondersteuning en documentatie – Cisco Systems