# TCP opnieuw instellen met IDS Director

## Inhoud



## Inleiding

Dit document beschrijft hoe u een Inbraakdetectiesysteem (IDS, voorheen NetRanger), directeur en Sensor moet configureren om TCP-resets op een geprobeerd telnet naar een reeks adressen te verzenden die de beheerde router omvatten als de verzonden string "testatack" is.

## Voorwaarden

### Vereisten

Denk er bij het overwegen van deze configuratie aan:

- Installeer de sensor en controleer of de software correct werkt voordat u deze configuratie uitvoert.
- Zorg ervoor dat de snuffelinterface zich uitstrekt tot de externe interface van de beheerde 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 mobiele softwarerelease 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.

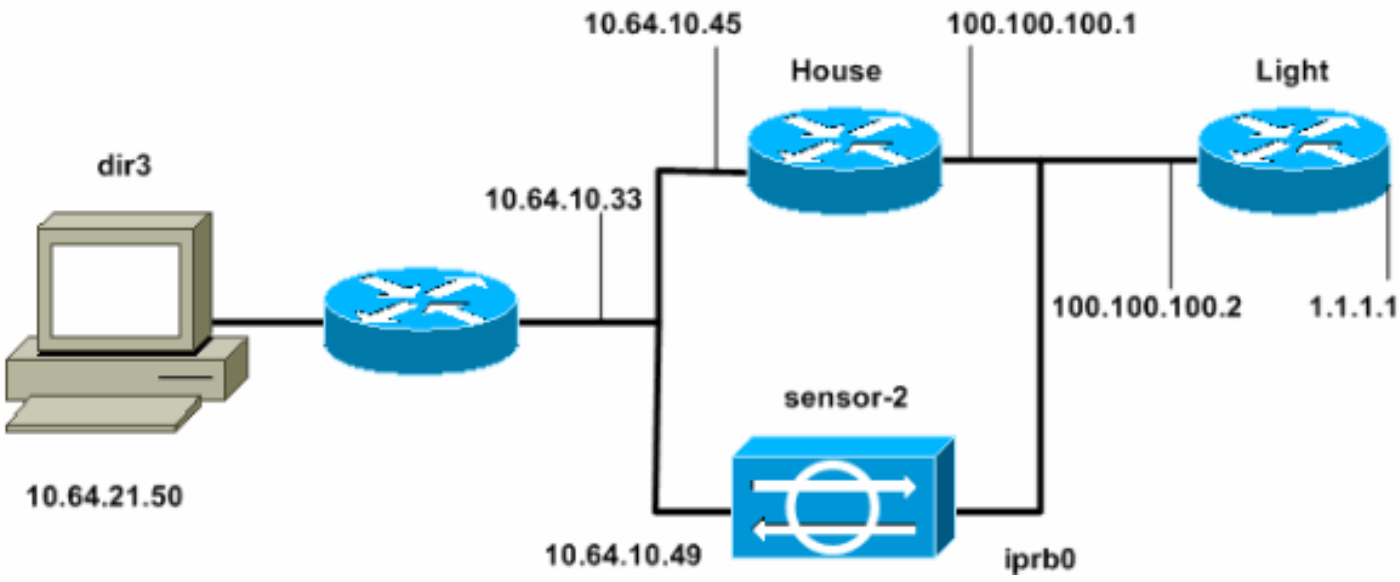
## Configureren

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
!
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
```

## 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
 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#
```

## De sensor configureren

Volg deze stappen om de sensor te configureren.

1. Telnet aan 10.64.10.49 (de IDS Sensor) met de gebruikersnaam **wortel** en de **wachtwoordaanval**.
2. Type **sysconfiguratie-sensor**.
3. Voer desgevraagd de configuratieinformatie in, zoals in dit voorbeeld wordt getoond:

```
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.

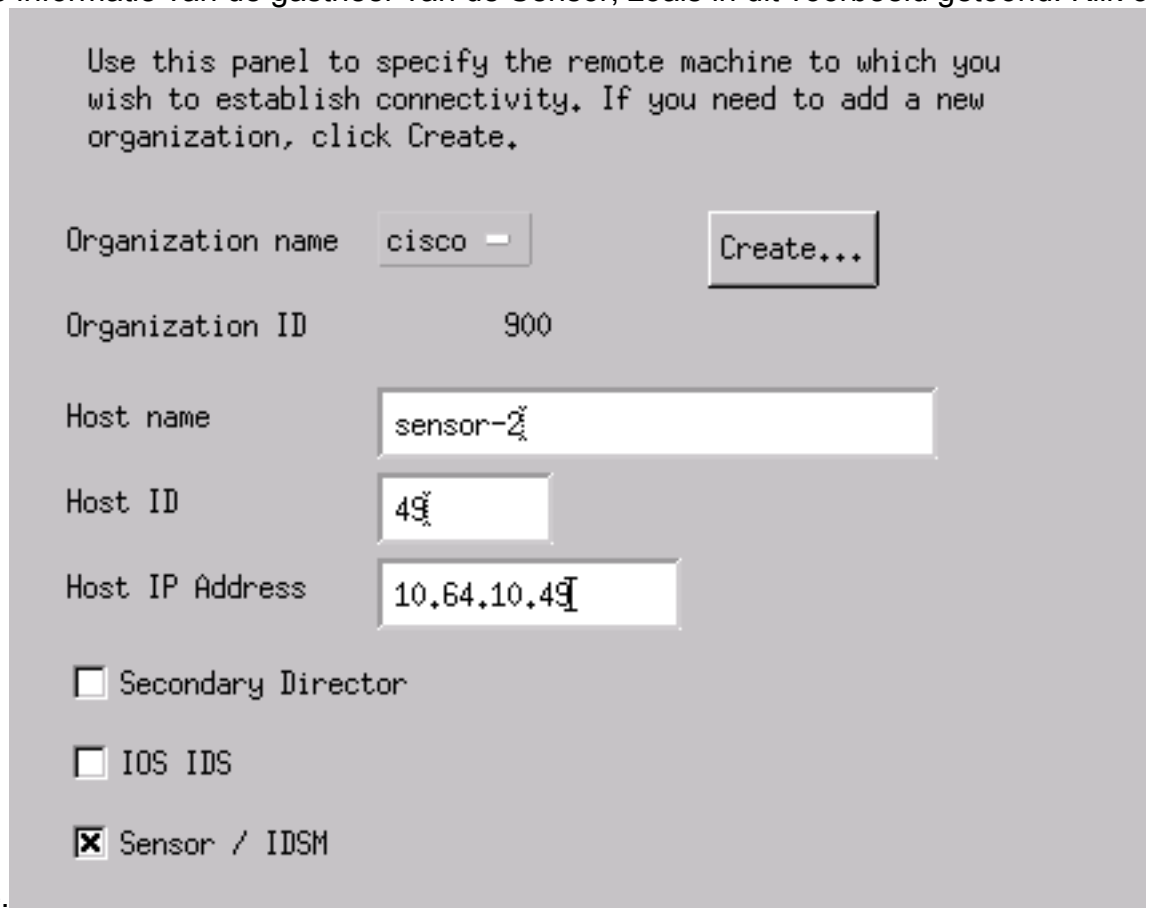
## Voeg de sensor toe aan de directeur

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

1. Telnet aan 10.64.21.50 (de IDS Director) met het gebruikersnaamnetwerk en de **wachtwoordaanval**.
2. Type **ovw&** om HP OpenView te starten.
3. Ga vanuit het hoofdmenu naar **Beveiliging > Configureren**.
4. Ga in het hulpprogramma Configuration File Management naar **bestand > Add Host** en klik

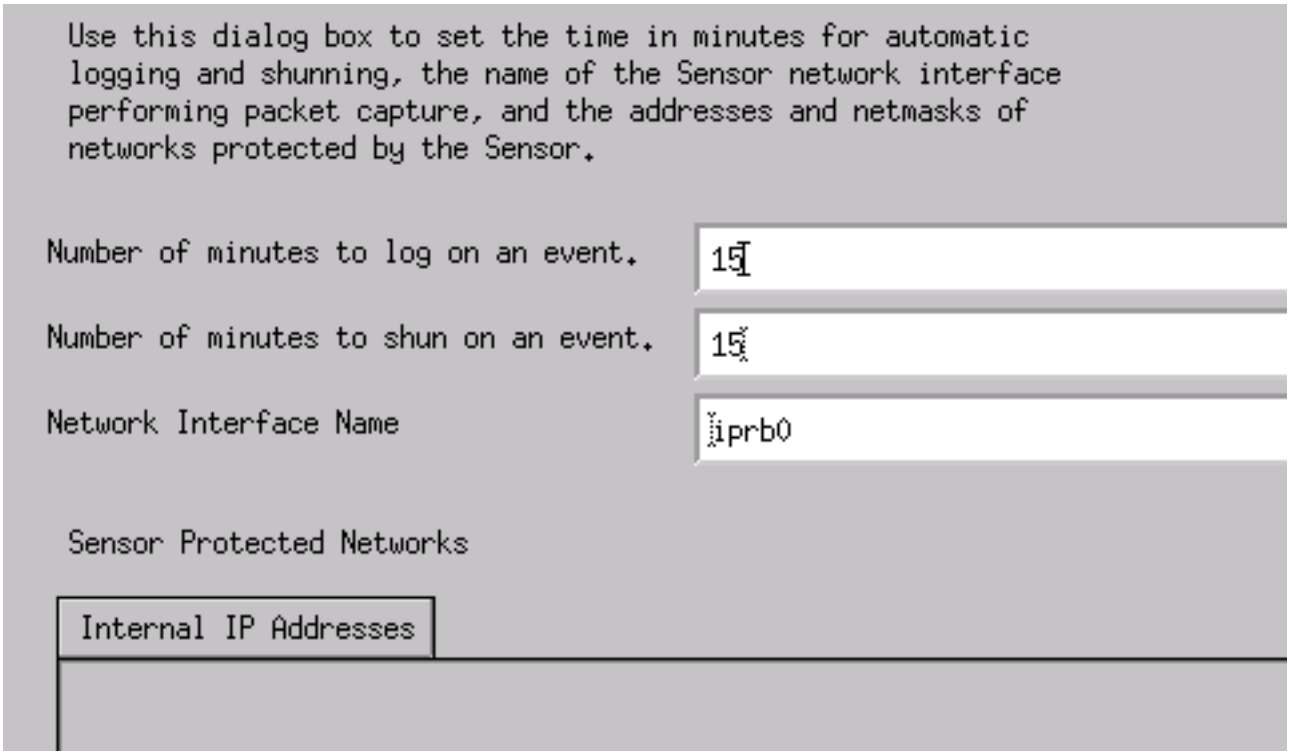
op **Next**.

5. Voltooi de informatie van de gastheer van de Sensor, zoals in dit voorbeeld getoond. Klik op **Volgende**.

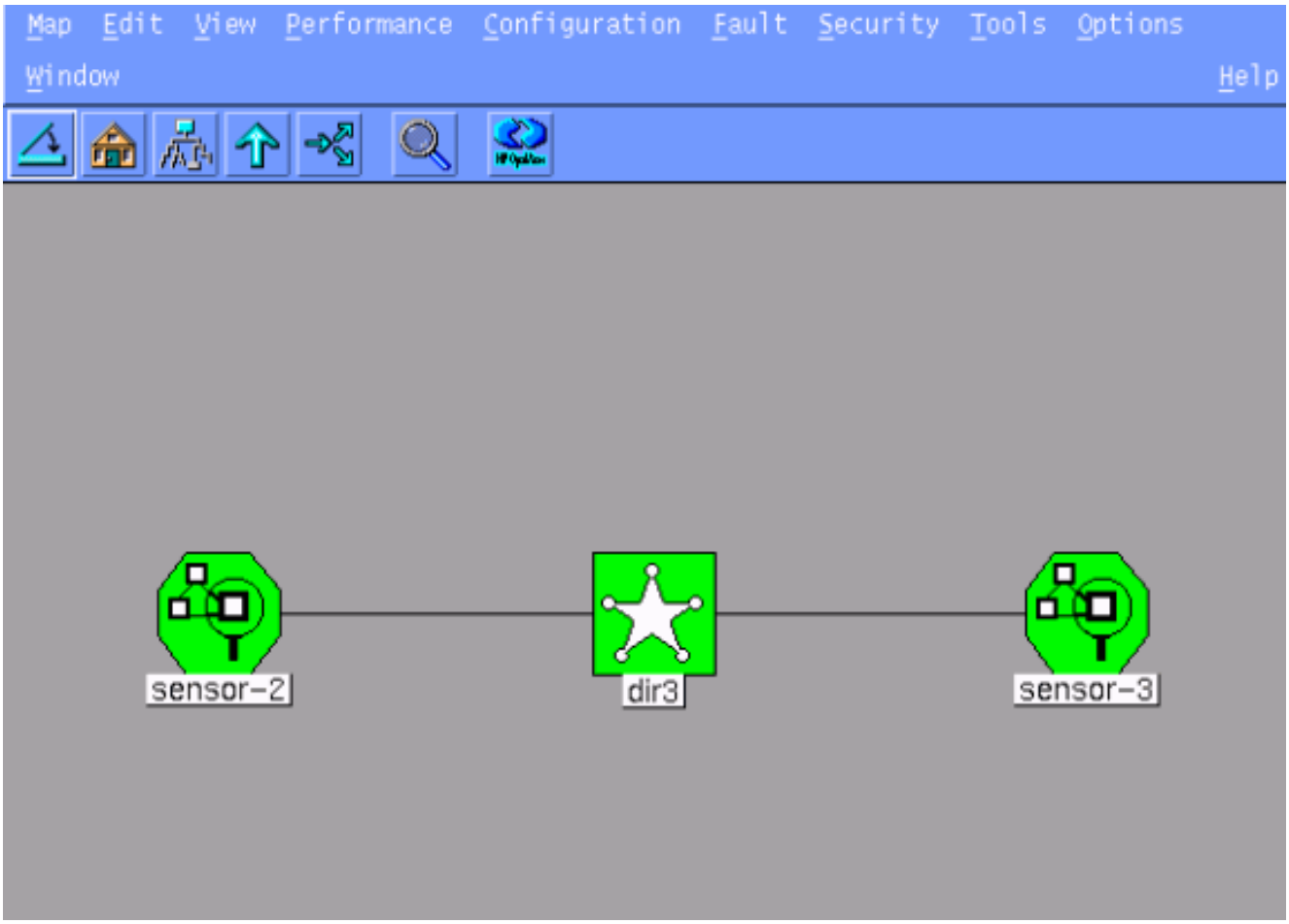



6. Accepteer de standaardinstellingen voor het type machine en klik op **Volgende**, zoals in dit voorbeeld.


7. U kunt het logbestand wijzigen en minuten uitzetten, of u kunt de standaardwaarden accepteren. U moet de naam van de interface van het netwerk echter wijzigen in de naam van de gebruikersinterface. In dit voorbeeld is het "iprb0". Afhankelijk van het type sensor en de manier waarop u de sensor aansluit, kan deze "spwr0" of iets anders zijn.




8. Klik op **Volgende** en klik vervolgens op **Voltooien** om de sensor aan de directeur toe te voegen. Vanaf het hoofdmenu moet je nu sensor-2 zien, zoals in dit voorbeeld.

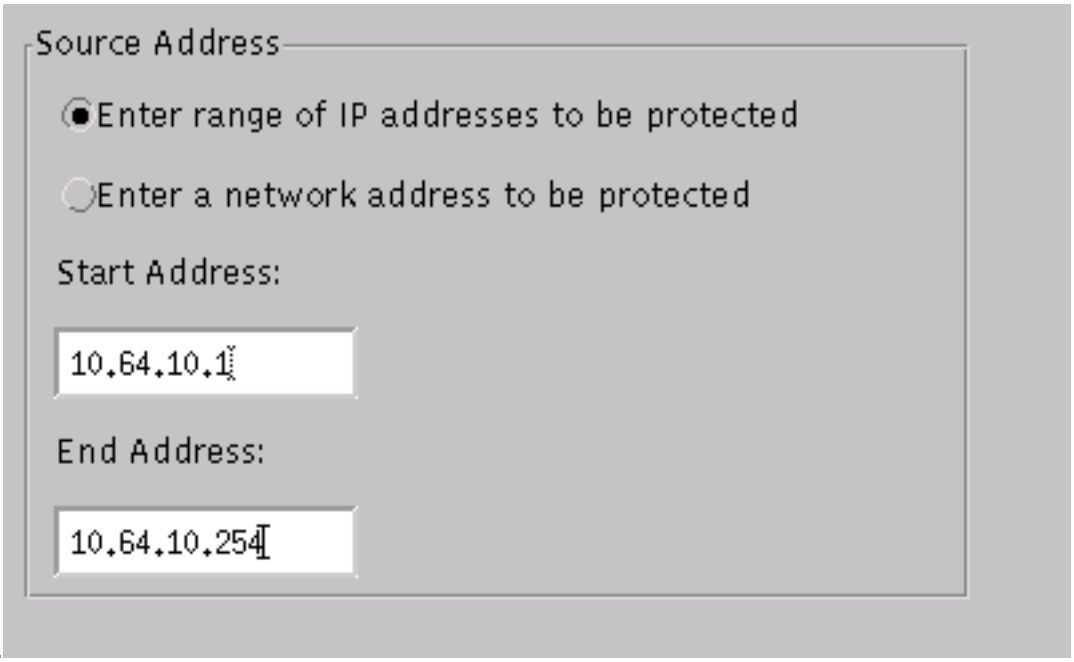



## TCP opnieuw instellen op Cisco IOS-router

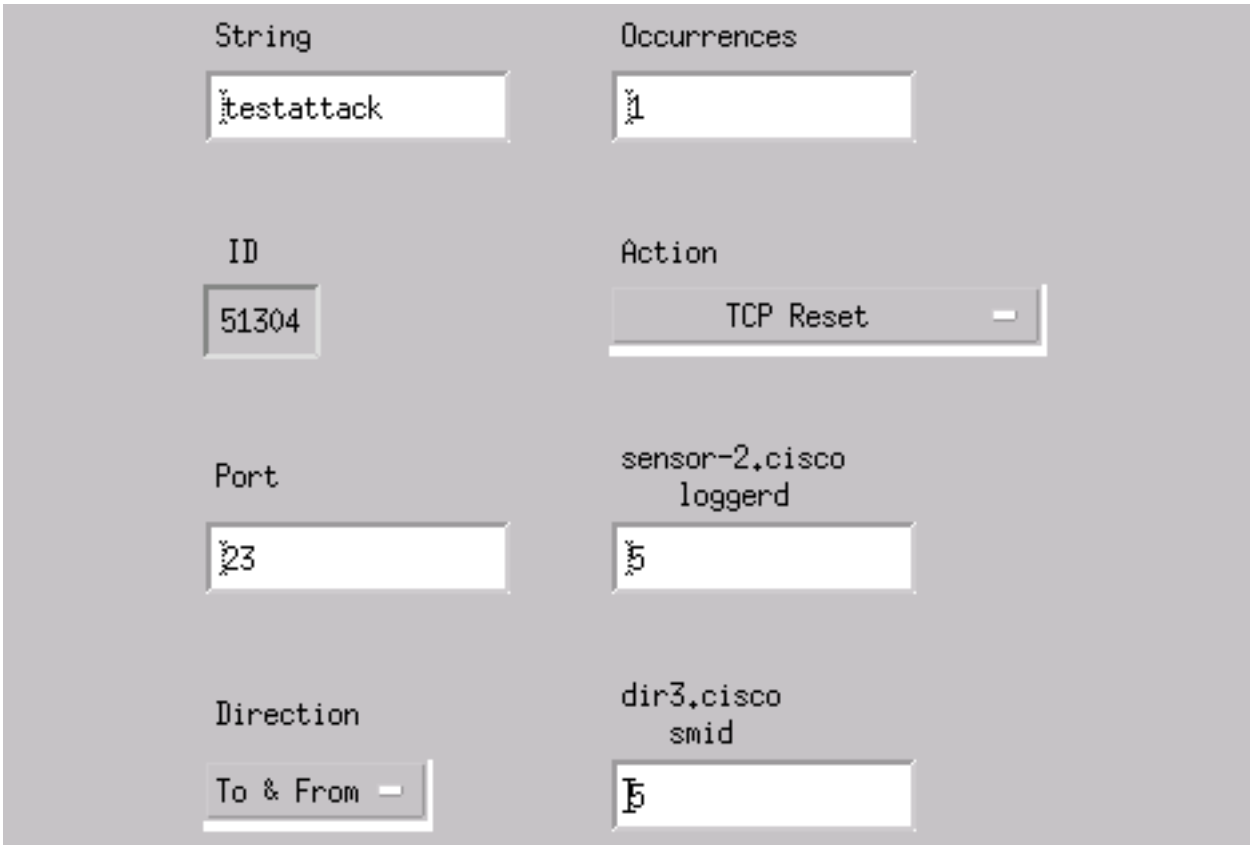
Voltooi deze stappen om TCP te configureren dat opnieuw ingesteld wordt voor de Cisco IOS router.

1. Ga in het hoofdmenu naar **Beveiliging > Configureren**.
2. Markeer **sensor-2** in het **hulpprogramma** Configuration File Management en dubbelklik op **die** optie.
3. Apparaatbeheer openen
4. Klik op **Apparaten > Toevoegen**. Voer de apparaatinformatie in, zoals in het volgende voorbeeld. Klik op **OK** om verder te gaan. Zowel het telnet als het toelaten van wachtwoorden zijn
   Cisco.

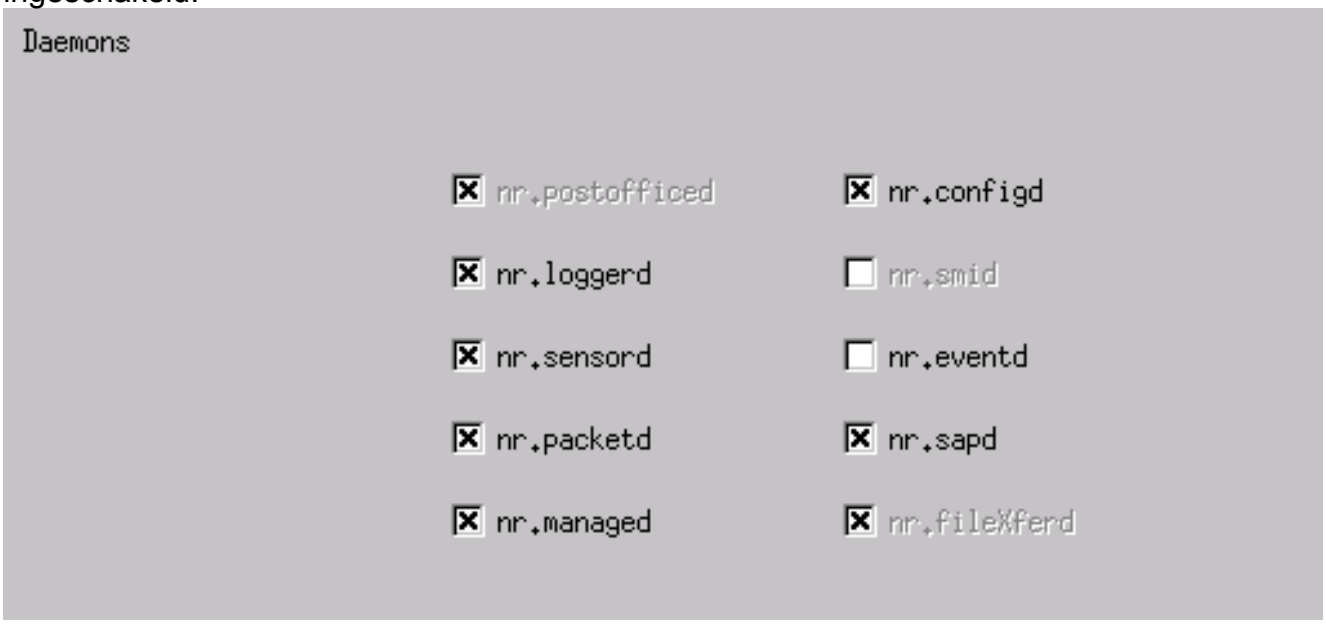

5. Open het venster voor inbraakdetectie en klik op **Beveiligde netwerken**. Voeg het bereik van adressen toe van 10.64.10.1 tot 10.64.10.254 in het beschermde



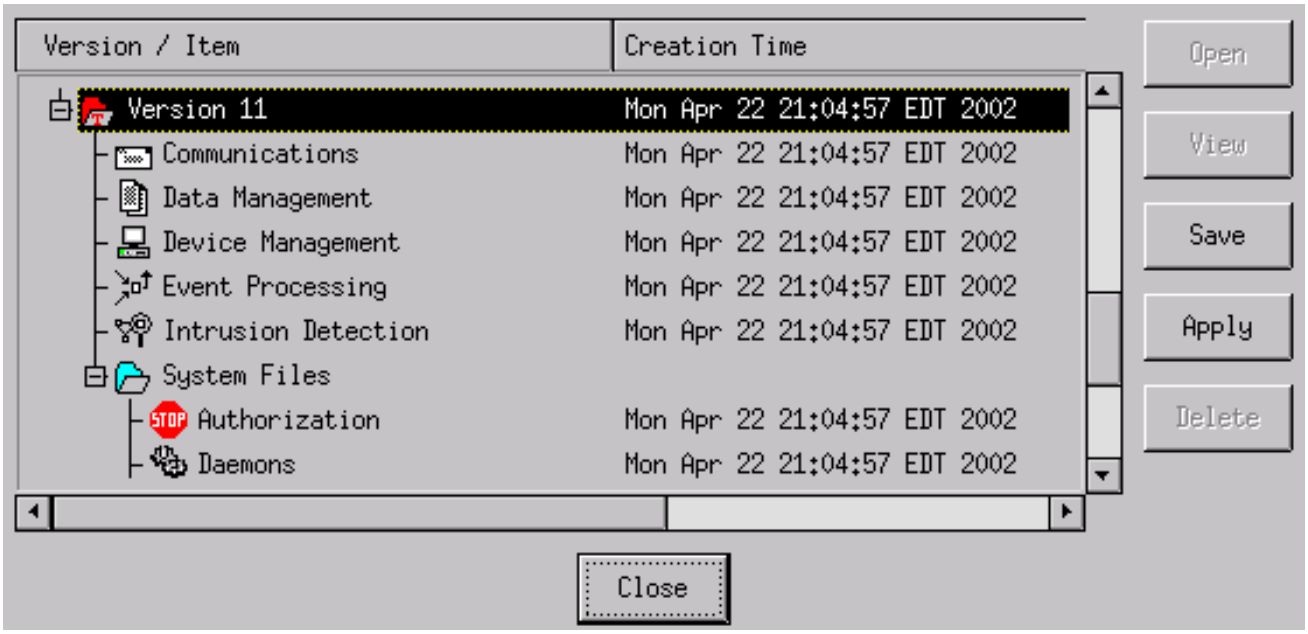

   netwerk.
6. Klik op **Profiel** en selecteer **Handmatige configuratie**. Klik vervolgens op **Handtekeningen wijzigen**. Kies **Matched Strings** met een ID van 8000. Klik op **Uitvouwen > Toevoegen** om een nieuwe string toe te voegen die **testattack** heet. Voer de string informatie in zoals in dit voorbeeld, en klik op **OK** om door te
   gaan.




7. Dit deel van de configuratie is klaar. Klik op **OK** om het venster voor inbraakdetectie te sluiten.
8. Open de map Systeembestanden en vervolgens het Datumvenster. Zorg ervoor dat deze datums zijn
   ingeschakeld:




9. Klik op **OK** om verder te gaan.
10. Kies de versie die u zojuist hebt aangepast, klik op **Opslaan** en **Toepassen**. Wacht tot het systeem u vertelt dat de sensor de services heeft herstart en sluit vervolgens alle vensters voor de Director
    Configuration.




## Start de aanval en TCP-reset

Telnet van routerlicht tot routerhuis en type **testattack**. Zodra u op de toets Ruimte of Voer in, herstelt uw Telnet-sessie. U sluit zich aan bij het routerhuis.

```
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.
```

# Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

# Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Telnet aan 10.64.10.49, de Sensor, die de gebruikersnaam **wortel** en de **wachtwoordaanval** gebruikt. Type **cd /usr/nr/enz**. Type **cat packetd.conf**. Als u TCP correct instelt voor testatack, moet u een vier (4) zien in het veld Action Codes. Dit geeft TCP opnieuw in zoals in dit voorbeeld wordt getoond.

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

Als u de actie per ongeluk op "geen" in de signatuur instelt, ziet u een nul (0) in het veld Action Codes. Dit geeft geen actie aan zoals in dit voorbeeld.

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

De TCP resets worden verzonden vanuit de snuifinterface van de Sensor. Als er een switch is die de Sensor-interface met de externe interface van de beheerde router verbindt, wanneer u de opdracht Sensor in de switch gebruikt, gebruikt u deze syntaxis:

```
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
```

# Gerelateerde informatie

- Veldmeldingen
- Cisco-pagina voor beveiligde inbraakpreventie