

# Konfigurieren von TCP-Zurücksetzen mithilfe von IDS Director

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren des Sensors](#)

[Hinzufügen des Sensors zum Director](#)

[Konfigurieren des TCP-Zurücksetzens für den Cisco IOS-Router](#)

[Attack und TCP Reset starten](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## [Einführung](#)

In diesem Dokument wird beschrieben, wie Sie einen IDS (früher NetRanger) Director und Sensor konfigurieren, um TCP-Resets auf einem versuchten Telnet an eine Reihe von Adressen zu senden, darunter den verwalteten Router, wenn die gesendete Zeichenfolge "testattack" lautet.

## [Voraussetzungen](#)

### [Anforderungen](#)

Beachten Sie bei der Konfiguration Folgendes:

- Installieren Sie den Sensor, und überprüfen Sie, ob er ordnungsgemäß funktioniert, bevor Sie diese Konfiguration durchführen.
- Stellen Sie sicher, dass sich die Sniffing-Schnittstelle auf die externe Schnittstelle des verwalteten Routers erstreckt.

### [Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- Cisco IDS Director 2.2.3
- Cisco IDS Sensor 3.0.5
- Cisco IOS<sup>®</sup> Router mit Softwareversion 12.2.6

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

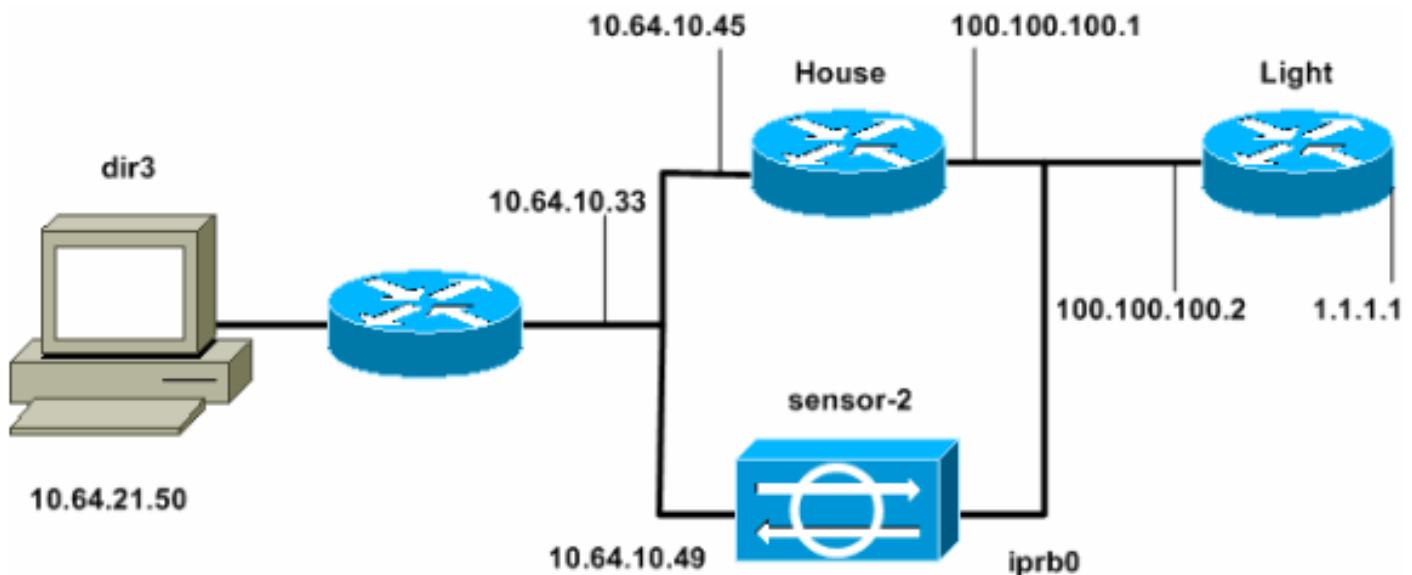
## Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

## Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



## Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- [Routerleuchte](#)
- [Router-Haus](#)

## Routerleuchte

```
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
```

## Router-Haus

```
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#
```

## Konfigurieren des Sensors

Führen Sie diese Schritte aus, um den Sensor zu konfigurieren.

1. Telnet bis 10.64.10.49 (der IDS-Sensor) mit dem Benutzernamen **root** und dem Kennwort-**Angriff**.
2. Geben Sie **sysconfig-sensor** ein.
3. Geben Sie bei Aufforderung die Konfigurationsinformationen ein, wie in diesem Beispiel gezeigt:

```
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. Speichern Sie die Konfiguration, wenn Sie dazu aufgefordert werden, und lassen Sie den Sensor neu starten.

## Hinzufügen des Sensors zum Director

Gehen Sie wie folgt vor, um den Sensor dem Director hinzuzufügen.

1. Telnet bis 10.64.21.50 (der IDS Director) mit dem Benutzernamen **netrangr** und dem Kennwort-**Angriff**.
2. Geben Sie **ovw&** ein, um HP OpenView zu starten.
3. Gehen Sie im Hauptmenü zu **Sicherheit > Konfigurieren**.
4. Gehen Sie im Konfigurationsdateiverwaltungsprogramm zu **Datei > Host hinzufügen**, und klicken Sie auf **Weiter**.
5. Füllen Sie die Sensor-Hostinformationen aus, wie in diesem Beispiel gezeigt. Klicken Sie auf

Use this panel to specify the remote machine to which you wish to establish connectivity. If you need to add a new organization, click Create.

Organization name

Organization ID

Host name

Host ID

Host IP Address

Secondary Director

IOS IDS

Sensor / IDSM

**Weiter.**

6. Akzeptieren Sie die Standardeinstellungen für den Computertyp, und klicken Sie auf **Weiter**, wie in diesem Beispiel

Use this dialog box to define the type of machine you are adding.

Please remember that in order for connectivity to be established, the remote machine must already know the IDs and IP address of this Director. For Sensors, this is accomplished at install time by running sysconfig-sensor. For remote (secondary) Directors, this is accomplished by running nrConfigure on the remote machine and modifying the hosts and routes System Files accordingly.

Initialize a newly installed Sensor

Connect to a previously configured Sensor

Forward alarms to a secondary Director

gezeigt.

7. Sie können entweder das Protokoll ändern und die Minuten schließen oder die Standardwerte akzeptieren. Sie müssen jedoch den Namen der Netzwerkschnittstelle in den

Namen der Sniffing-Schnittstelle ändern. In diesem Beispiel ist es "iprb0". Es kann "spwr0" oder alles andere sein, abhängig vom Sensortyp und wie Sie Ihren Sensor anschließen.

Use this dialog box to set the time in minutes for automatic logging and shunning, the name of the Sensor network interface performing packet capture, and the addresses and netmasks of networks protected by the Sensor.

Number of minutes to log on an event.

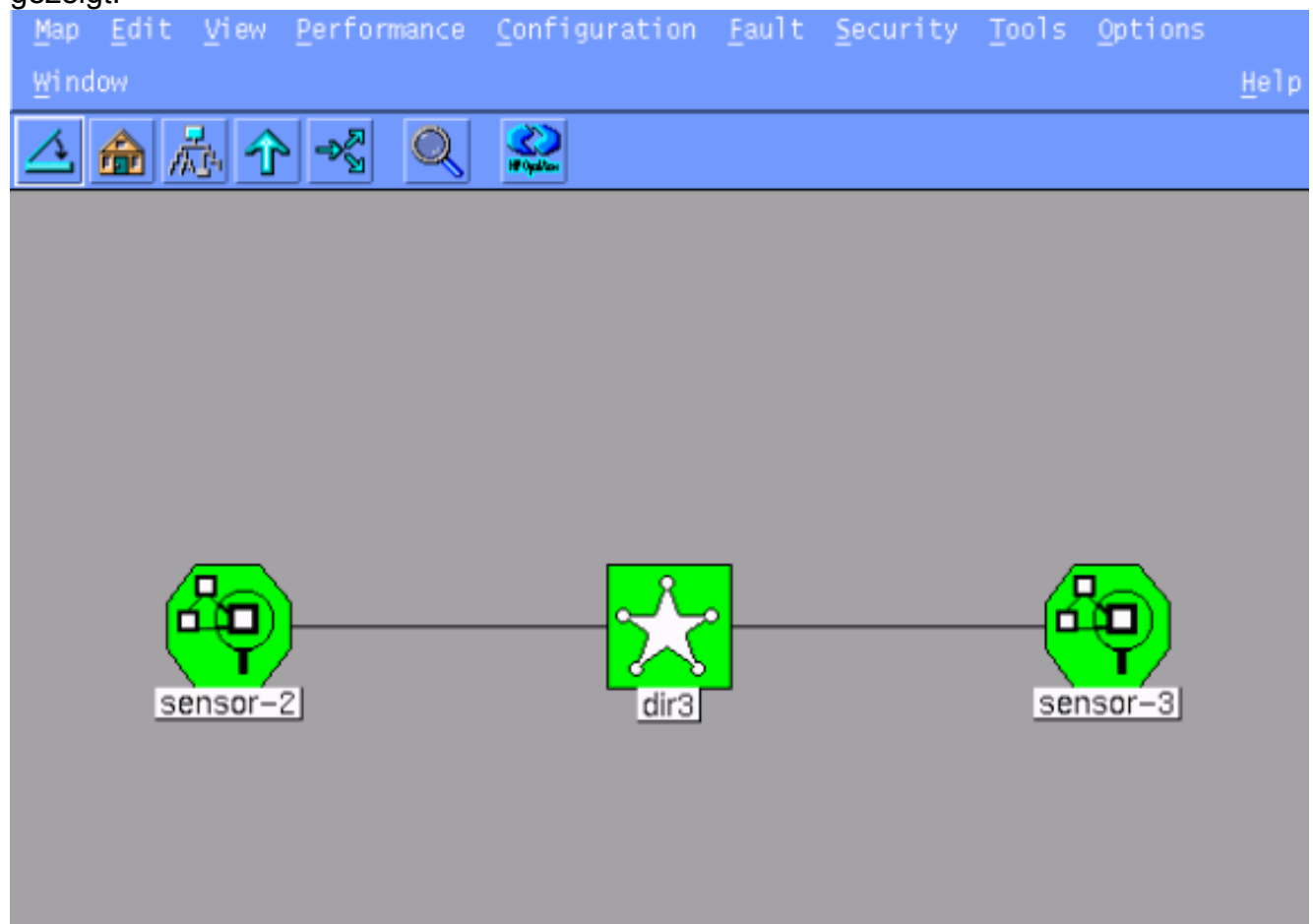
Number of minutes to shun on an event.

Network Interface Name

Sensor Protected Networks

Internal IP Addresses


8. Klicken Sie weiter auf **Weiter** und klicken Sie dann auf **Beenden**, um den Sensor dem Director hinzuzufügen. Im Hauptmenü sollte jetzt Sensor-2 angezeigt werden, wie in diesem Beispiel gezeigt.



## Konfigurieren des TCP-Zurücksetzens für den Cisco IOS-Router

Gehen Sie wie folgt vor, um das Zurücksetzen von TCP für den Cisco IOS-Router zu konfigurieren.

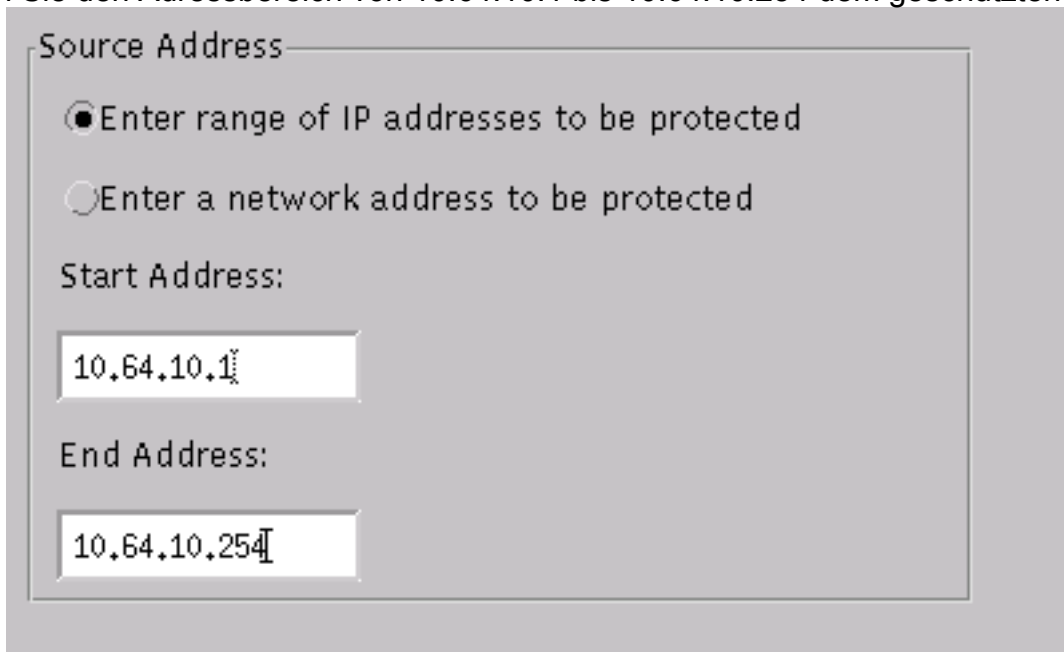
1. Gehen Sie im Hauptmenü zu **Sicherheit > Konfigurieren**.
2. Markieren Sie im Konfigurationsdateiverwaltungsprogramm **sensor-2** und doppelklicken Sie darauf.
3. Öffnen Sie die Geräteverwaltung.
4. Klicken Sie auf **Geräte > Hinzufügen**. Geben Sie die Geräteinformationen ein, wie im folgenden Beispiel gezeigt. Klicken Sie auf **OK**, um fortzufahren. Sowohl das Telnet- als auch das Aktivierungskennwort sind Cisco.



The screenshot shows a configuration window with the following fields:

- IP Address:** 10.64.10.45
- User Name:** [empty]
- Device Type:** Cisco Router[Including Cat5kRSM,Cat6kMSFC] -
- Password:** \*\*\*\*
- Sensor's NAT IP Address:** [empty]
- Enable Password:** \*\*\*\*
- Enable SSH**

5. Öffnen Sie das Fenster Angriffserkennung, und klicken Sie auf **Geschützte Netzwerke**. Fügen Sie den Adressbereich von 10.64.10.1 bis 10.64.10.254 dem geschützten Netzwerk



The screenshot shows a configuration window for protected networks with the following options and fields:

- Source Address:**
  - Enter range of IP addresses to be protected
  - Enter a network address to be protected
- Start Address:** 10.64.10.1
- End Address:** 10.64.10.254

hinzu.

6. Klicken Sie auf **Profil** und wählen Sie **Manuelle Konfiguration**. Klicken Sie anschließend auf



**Signaturen ändern.** Wählen Sie **Zugeordnete Zeichenfolgen** mit der ID 8000 aus. Klicken Sie auf **Erweitern > Hinzufügen**, um eine neue Zeichenfolge mit dem Namen **testattack** hinzuzufügen. Geben Sie die Zeichenfolgeninformationen ein, wie in diesem Beispiel gezeigt, und klicken Sie auf **OK**, um fortzufahren.

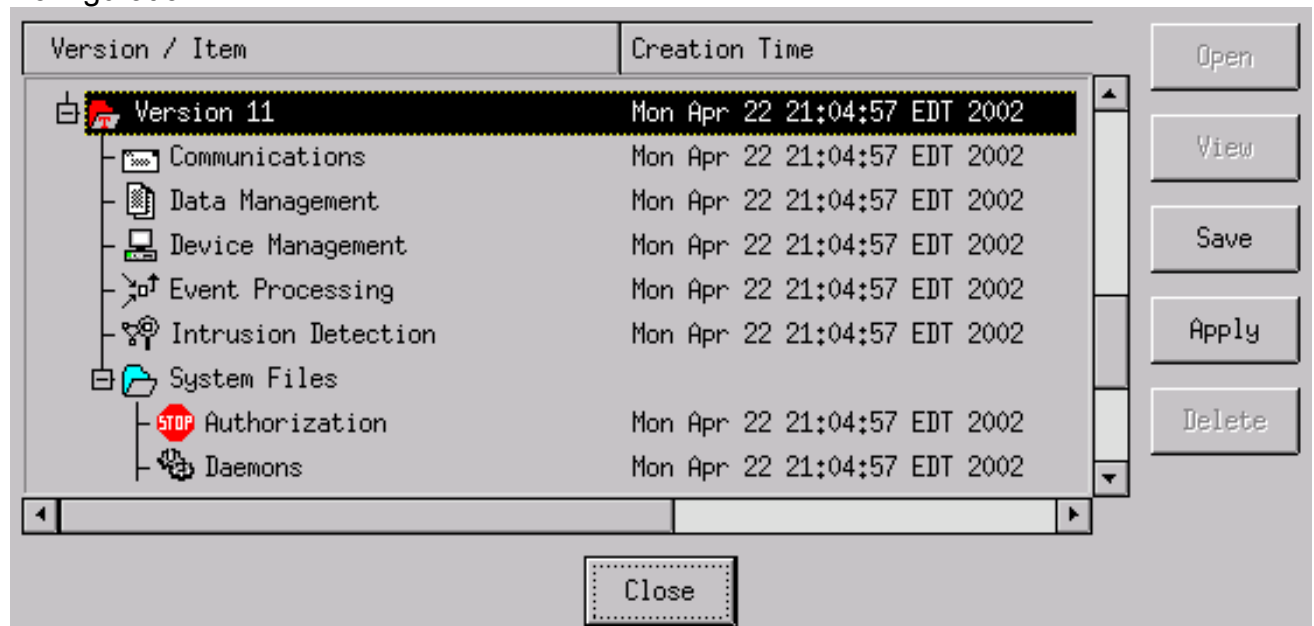
String	Occurrences
<input type="text" value="testattack"/>	<input type="text" value="1"/>
ID	Action
<input type="text" value="51304"/>	<input type="text" value="TCP Reset"/>
Port	sensor-2.cisco loggerd
<input type="text" value="23"/>	<input type="text" value="5"/>
Direction	dir3.cisco smid
<input type="text" value="To &amp; From"/>	<input type="text" value="5"/>

7. Sie haben diesen Teil der Konfiguration abgeschlossen. Klicken Sie auf **OK**, um das Fenster Intrusion Detection (Angriffserkennung) zu schließen.
8. Öffnen Sie den Ordner Systemdateien und anschließend das Fenster Daemons. Stellen Sie sicher, dass diese Daemons aktiviert sind:

Daemons	
<input checked="" type="checkbox"/> nr.postofficed	<input checked="" type="checkbox"/> nr.configd
<input checked="" type="checkbox"/> nr.loggerd	<input type="checkbox"/> nr.smid
<input checked="" type="checkbox"/> nr.sensord	<input type="checkbox"/> nr.eventd
<input checked="" type="checkbox"/> nr.packetd	<input checked="" type="checkbox"/> nr.sapd
<input checked="" type="checkbox"/> nr.managed	<input checked="" type="checkbox"/> nr.fileXferd

9. Klicken Sie auf **OK**, um fortzufahren.
10. Wählen Sie die Version aus, die Sie gerade geändert haben, klicken Sie auf **Speichern** und dann auf **Übernehmen**. Warten Sie, bis das System Ihnen mitteilt, dass der Sensor die

Dienste neu gestartet hat, und schließen Sie dann alle Fenster für die Director-Konfiguration.



## Attack und TCP Reset starten

Telnet von Router Light zu Router House und geben **testattack** ein. Sobald Sie die Leertaste oder die Eingabetaste drücken, wird die Telnet-Sitzung zurückgesetzt. Sie stellen eine Verbindung zu Router House her.

```
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.
```

## Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Telnet zu 10.64.10.49, dem Sensor, unter Verwendung des **root**-Benutzernamens und des Kennwortangriffs. Geben Sie **cd /usr/nr/etc** ein. Geben Sie **cat packetd.conf** ein. Wenn Sie das TCP-Zurücksetzen für die Testversion korrekt eingestellt haben, sollten Sie im Feld Aktionscodes vier (4) sehen. Dies zeigt das Zurücksetzen von TCP an, wie in diesem Beispiel gezeigt.

```
netrangr@sensor-2:/usr/nr/etc
>cat packetd.conf | grep "testattack"
```

```
RecordOfStringName 51304 23 3 1 "testattack"  
SigOfStringMatch 51304 4 5 5 # "testattack"
```

Wenn Sie die Aktion versehentlich auf "none" in der Signatur festlegen, wird im Feld Aktionscodes eine Null (0) angezeigt. Dies weist auf keine Aktion hin, wie im Beispiel gezeigt.

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

Die TCP-Resets werden von der Sniffing-Schnittstelle des Sensors gesendet. Wenn ein Switch vorhanden ist, der die Sensor-Schnittstelle mit der externen Schnittstelle des verwalteten Routers verbindet, verwenden Sie bei der Konfiguration mit dem Befehl **set span** im Switch die folgende Syntax:

```
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
```

## [Zugehörige Informationen](#)

- [Problemhinweise](#)
- [Support-Seite für Cisco Secure Intrusion Prevention](#)