Einrichten von Shuning auf einem UNIX Director

Inhalt

Einführung

Cisco Intrusion Detection System (IDS) Director und Sensor können zur Verwaltung eines Cisco Routers verwendet werden. In diesem Dokument wird ein Sensor (sensor-2) konfiguriert, um Angriffe auf den Router "House" zu erkennen und diese Informationen an den Director "dir3" zu übermitteln. Nach der Konfiguration wird ein Angriff gestartet (Ping von mehr als 1024 Byte, Signatur 2151, und eine ICMP-Flood (Internet Control Message Protocol) (Signatur 2152) vom Router "Light". Der Sensor erkennt den Angriff und leitet ihn an den Director weiter. Eine Zugriffskontrollliste (ACL) wird auf den Router heruntergeladen, um den Datenverkehr vom Angreifer zu meiden. Auf dem `Host` des Angreifers wird `unerreichbar` angezeigt, und im Opfer wird die heruntergeladene ACL angezeigt.

Voraussetzungen

Anforderungen

Bevor Sie diese Konfiguration versuchen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Installieren Sie den Sensor, und stellen Sie sicher, dass er ordnungsgemäß funktioniert.
- Stellen Sie sicher, dass sich die Sniffing-Schnittstelle auf die externe Schnittstelle des 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® Router mit 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.

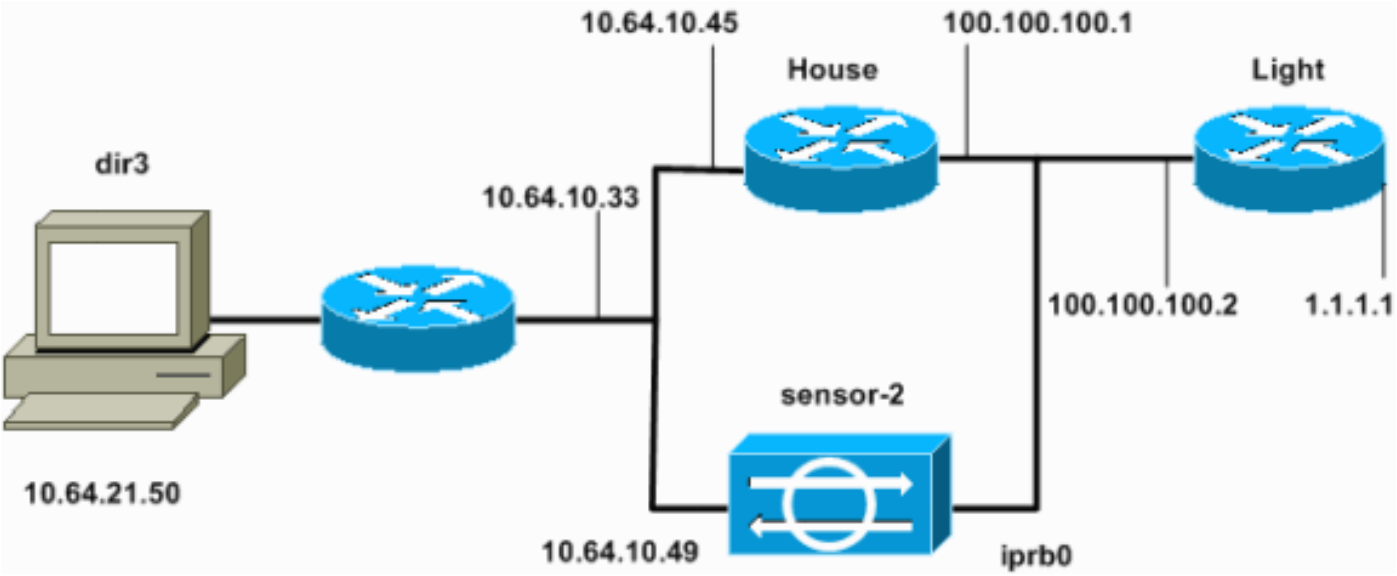
Konfigurieren

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
!
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
!--- 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#
```

Konfigurieren des Sensors

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

1. Telnet bis **10.64.10.49** mit dem Benutzernamen **root** und Passwort **Angriff**.
2. Geben Sie **sysconfig-sensor ein**.
3. Geben Sie bei Aufforderung die Konfigurationsinformationen ein, wie in diesem Beispiel gezeigt.

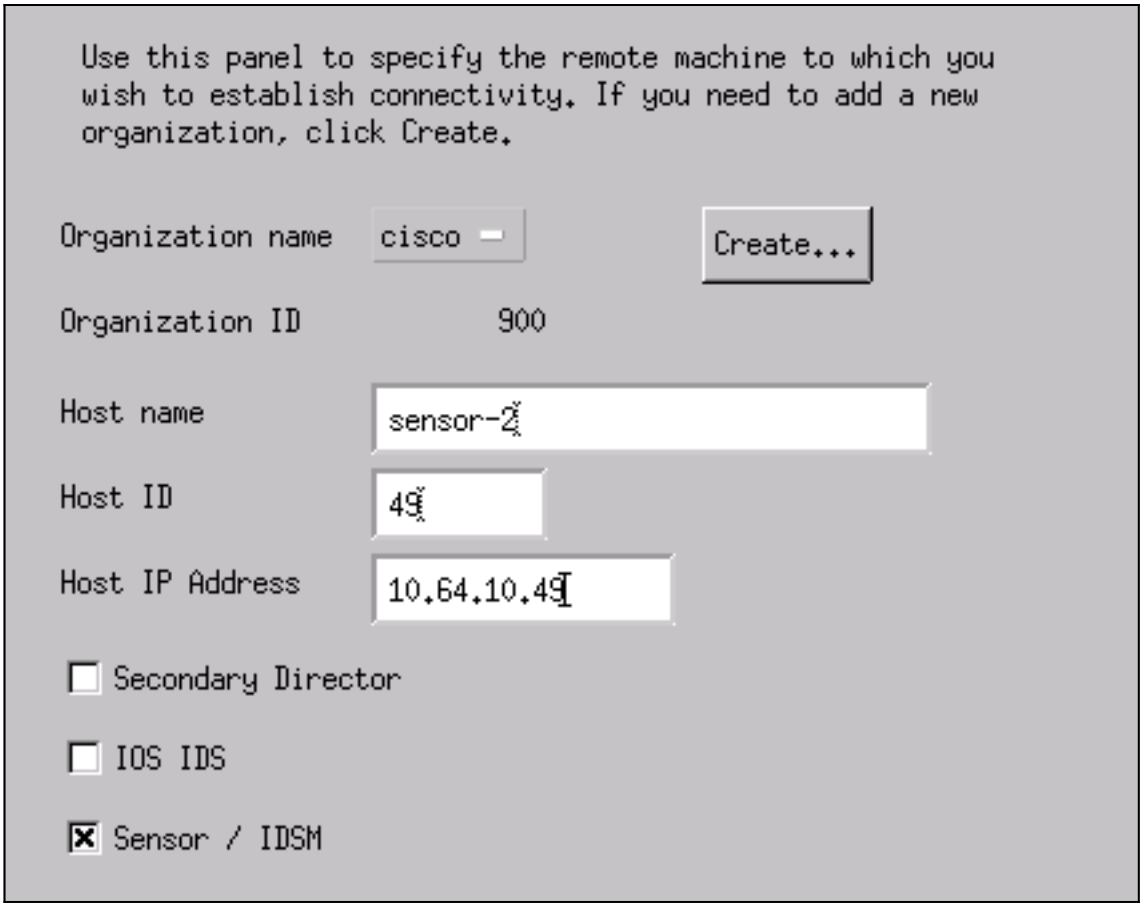
```
1 - IP Address: 10.64.10.49
2 - IP Netmask: 255.255.255.224
3 - IP Host Name:  sensor-2
4 - Default Route     10.64.10.33
5 - Network Access Control
          64.
          10.
6 - Communications Infrastructure
Sensor Host ID: 49
Sensor Organization ID:     900
Sensor Host Name: sensor-2
Sensor Organization 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.

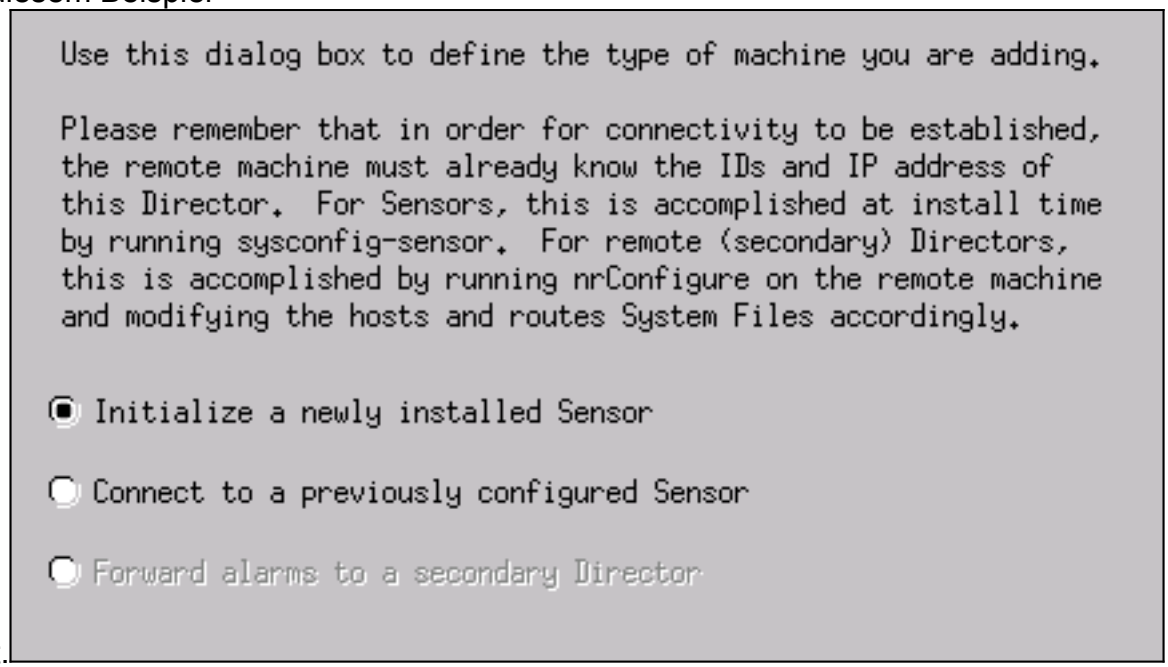
Hinzufügen des Sensors zum Director

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

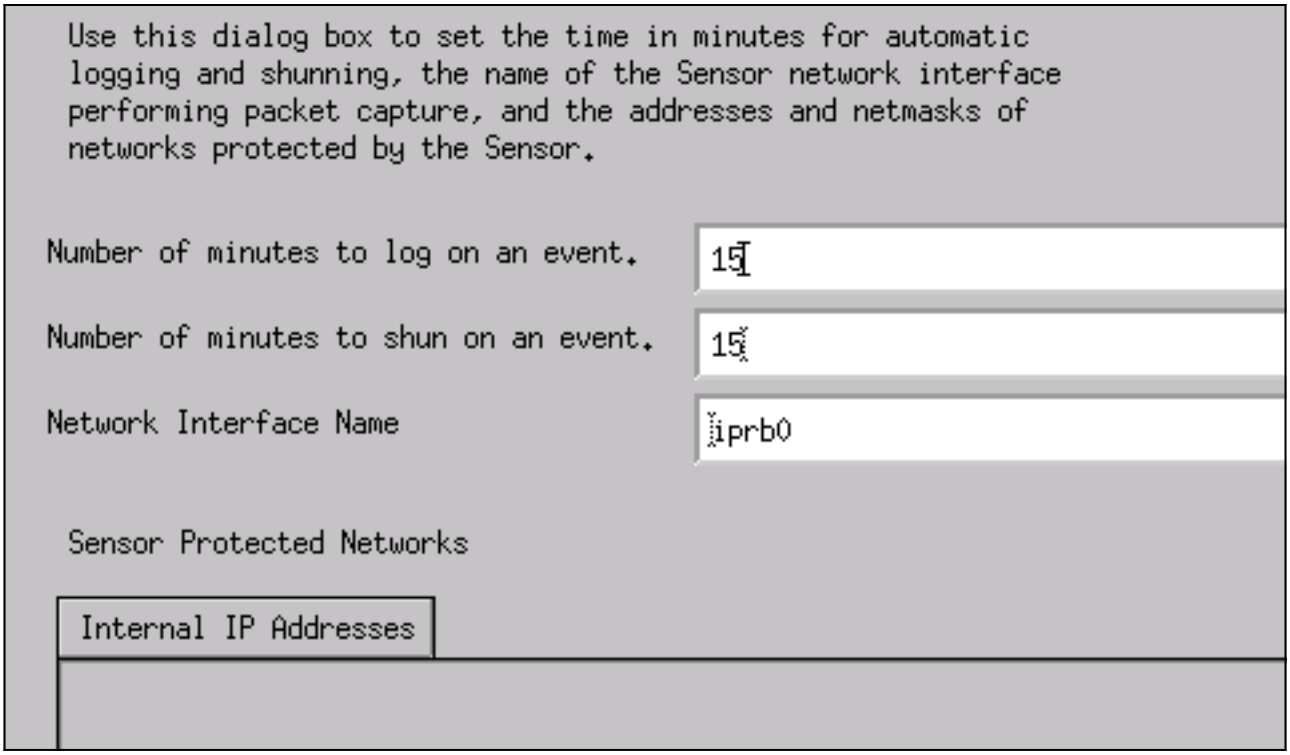
1. Telnet bis **10.64.21.50** mit Benutzername **netrangr** und Kennwort-**Angriff**.
2. Geben Sie **ovw&** ein, um HP OpenView zu starten.
3. Wählen Sie im Hauptmenü **Sicherheit > Konfigurieren aus**.
4. Wählen Sie im Konfigurationsdateiverwaltungsprogramm **Datei > Host hinzufügen aus**, und klicken Sie auf **Weiter**.
5. Dies ist ein Beispiel für das Ausfüllen der angeforderten Informationen.



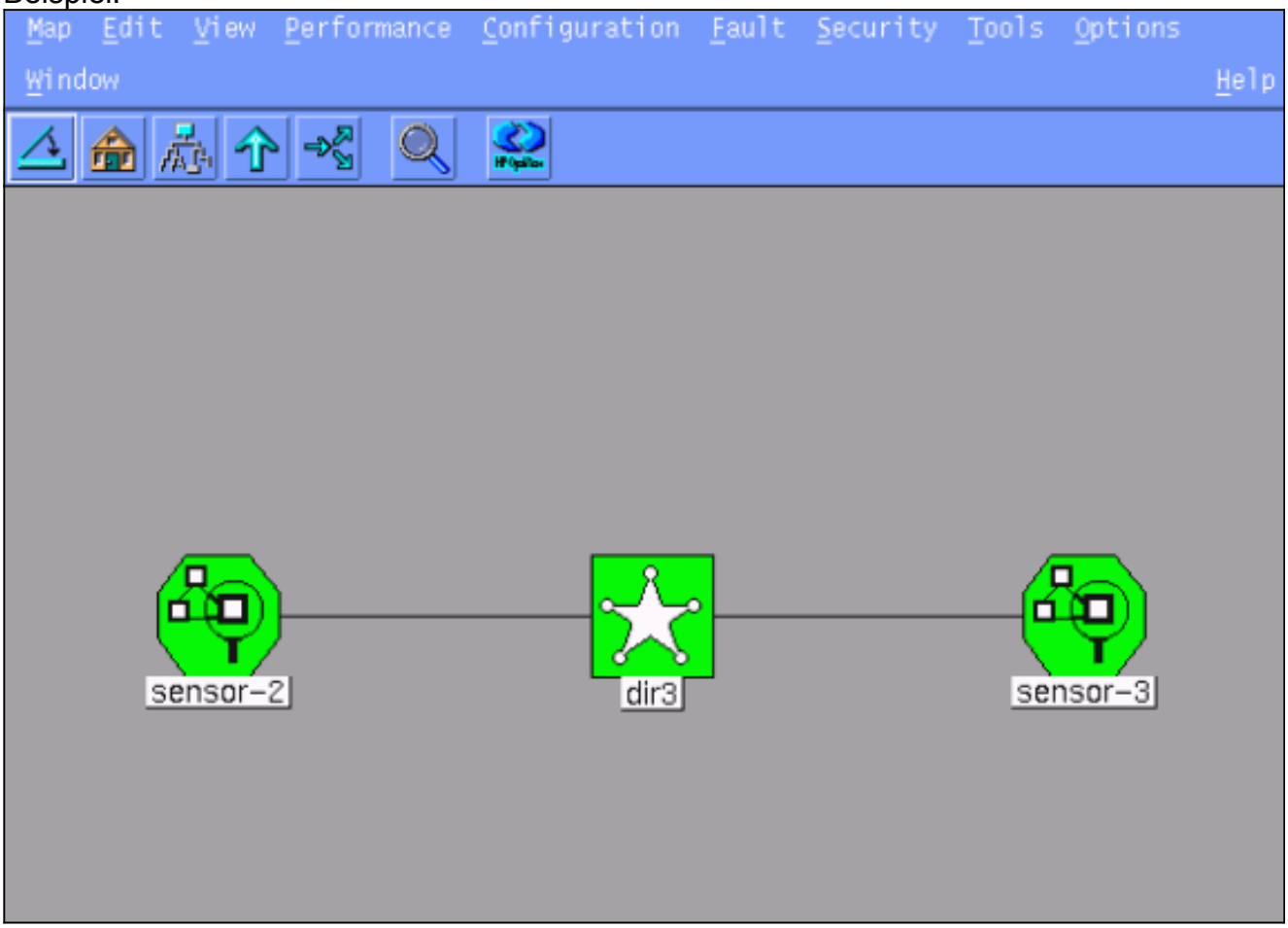
6. Akzeptieren Sie die Standardeinstellung für den Computertyp, und klicken Sie auf **Weiter**, wie in diesem Beispiel gezeigt.



7. Ändern Sie die Protokoll- und Shun-Minuten, oder belassen Sie sie als Standard, wenn die Werte zulässig sind. Ändern Sie den Namen der Netzwerkschnittstelle in den Namen der Sniffing-Schnittstelle.In diesem Beispiel ist es "iprb0". Es kann "spwr0" oder alles andere sein, abhängig vom Sensortyp und wie Sie Ihren Sensor anschließen.



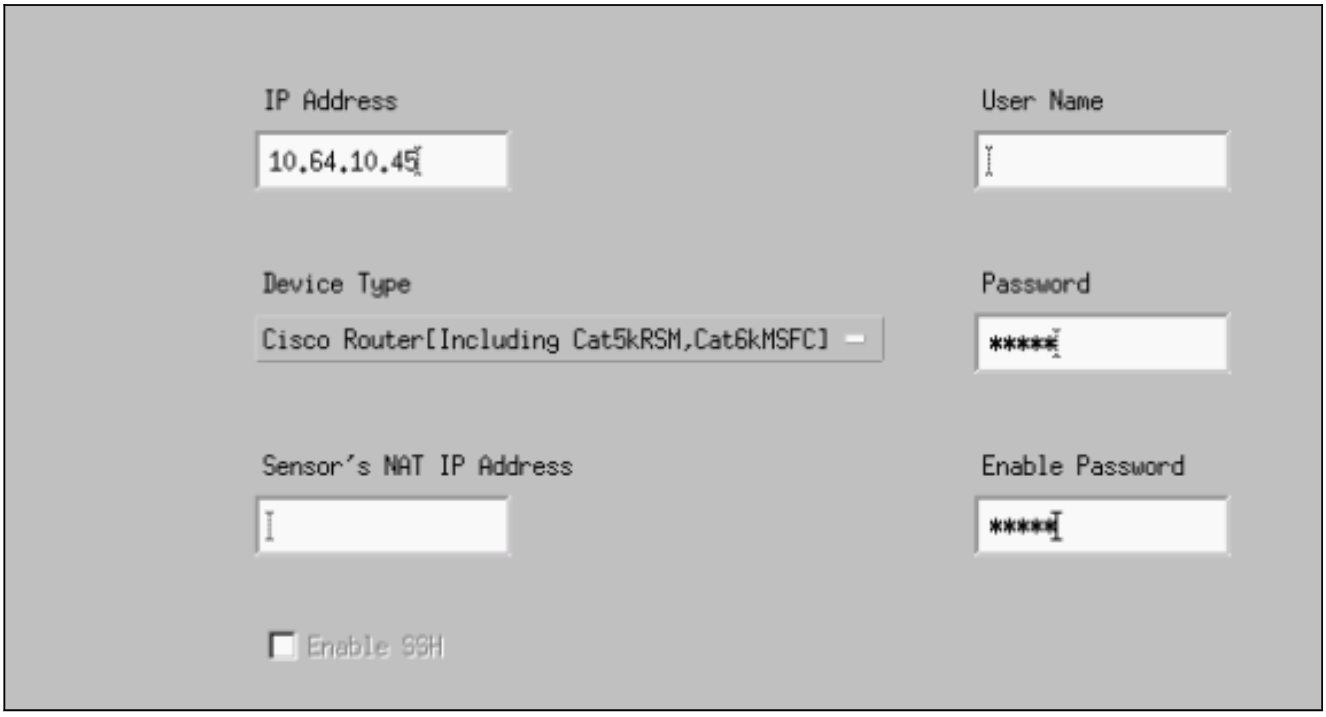
8. Klicken Sie auf **Weiter**, bis eine Option zum Klicken auf **Fertig stellen** ist.Sie haben den Sensor erfolgreich zum Director hinzugefügt. Im Hauptmenü sollte `sensor-2` angezeigt werden, wie in diesem
Beispiel.



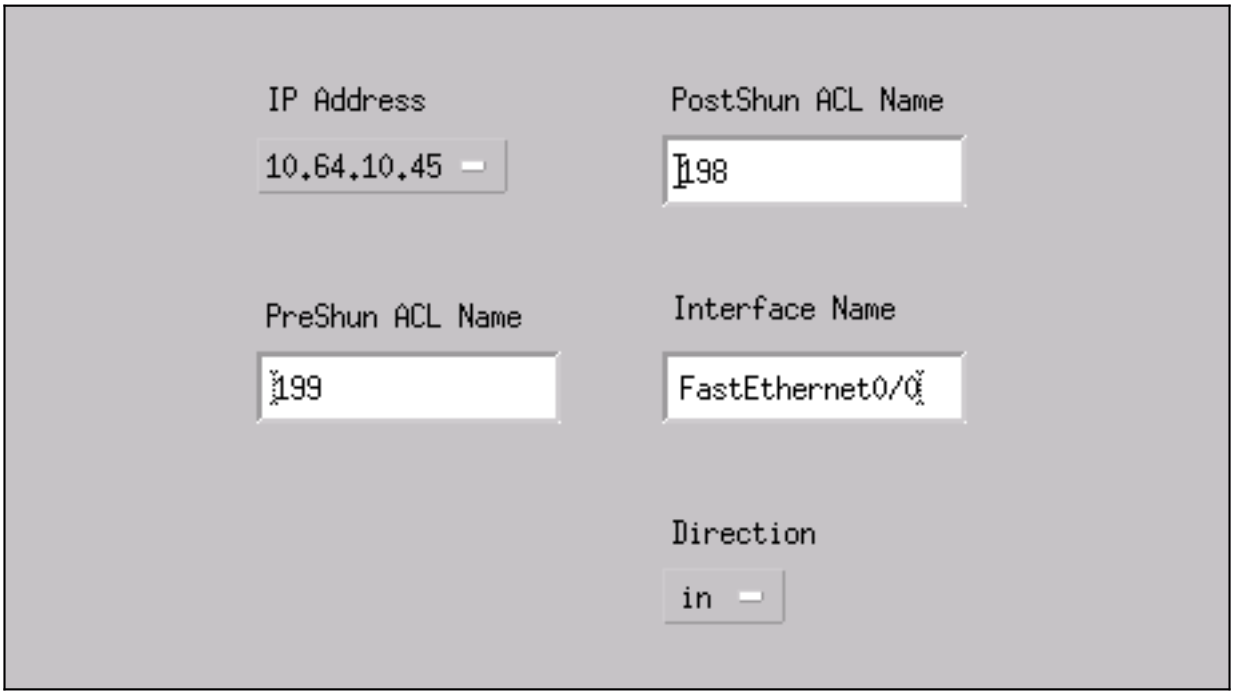
Konfigurieren Sie das Abschalten für den Cisco IOS-Router.

Gehen Sie wie folgt vor, um das Herunterfahren des Cisco IOS-Routers zu konfigurieren.

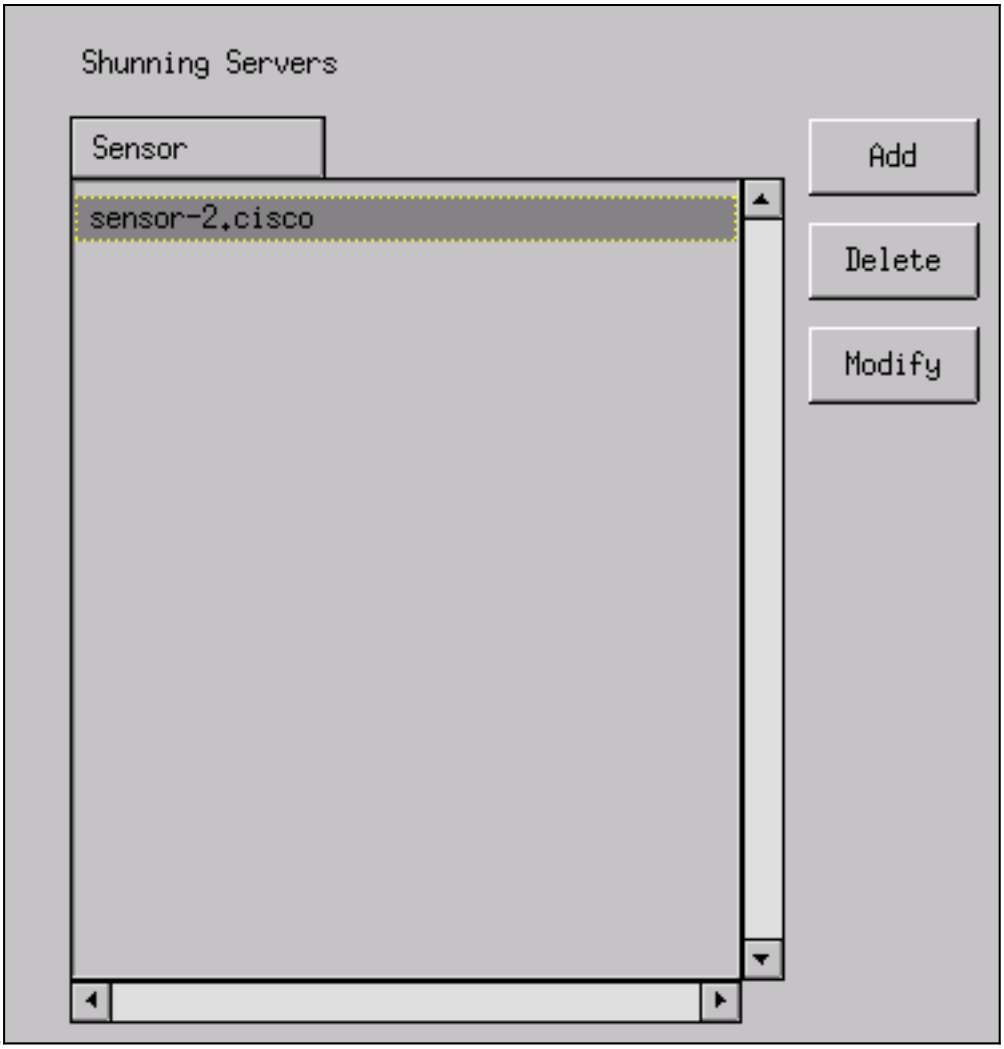
1. Wählen Sie im Hauptmenü **Sicherheit > Konfigurieren aus**.
2. Markieren Sie im Konfigurationsdateiverwaltungsprogramm **sensor-2** und doppelklicken Sie darauf.
3. Öffnen Sie **die Geräteverwaltung**.
4. Klicken Sie auf **Geräte > Hinzufügen**, und geben Sie die Informationen wie in diesem Beispiel dargestellt ein. Klicken Sie auf **OK**, um fortzufahren.Das Telnet und das Aktivieren von Passwörtern stimmen mit dem überein, was im Router "Haus" angezeigt wird.



5. Klicken Sie auf **Schnittstellen > Hinzufügen**, geben Sie diese Informationen ein, und klicken Sie auf **OK**, um fortzufahren.

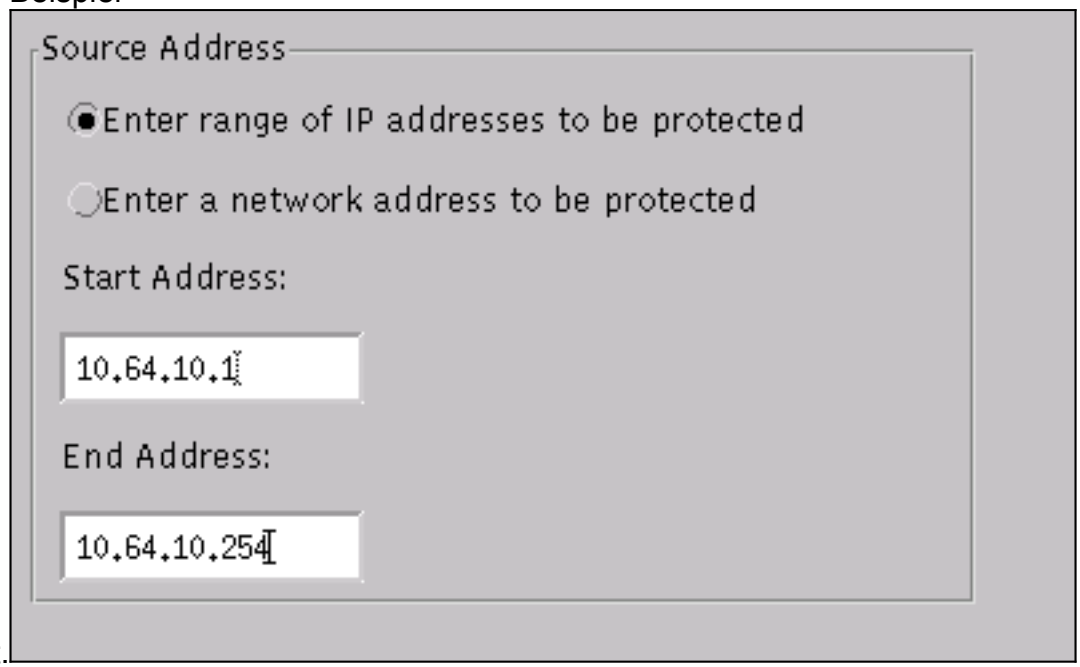


6. Klicken Sie auf **Shunning > Add**, und wählen Sie **sensor-2.cisco** als Shunning-Server aus. Schließen Sie das Fenster Geräteverwaltung, wenn Sie fertig



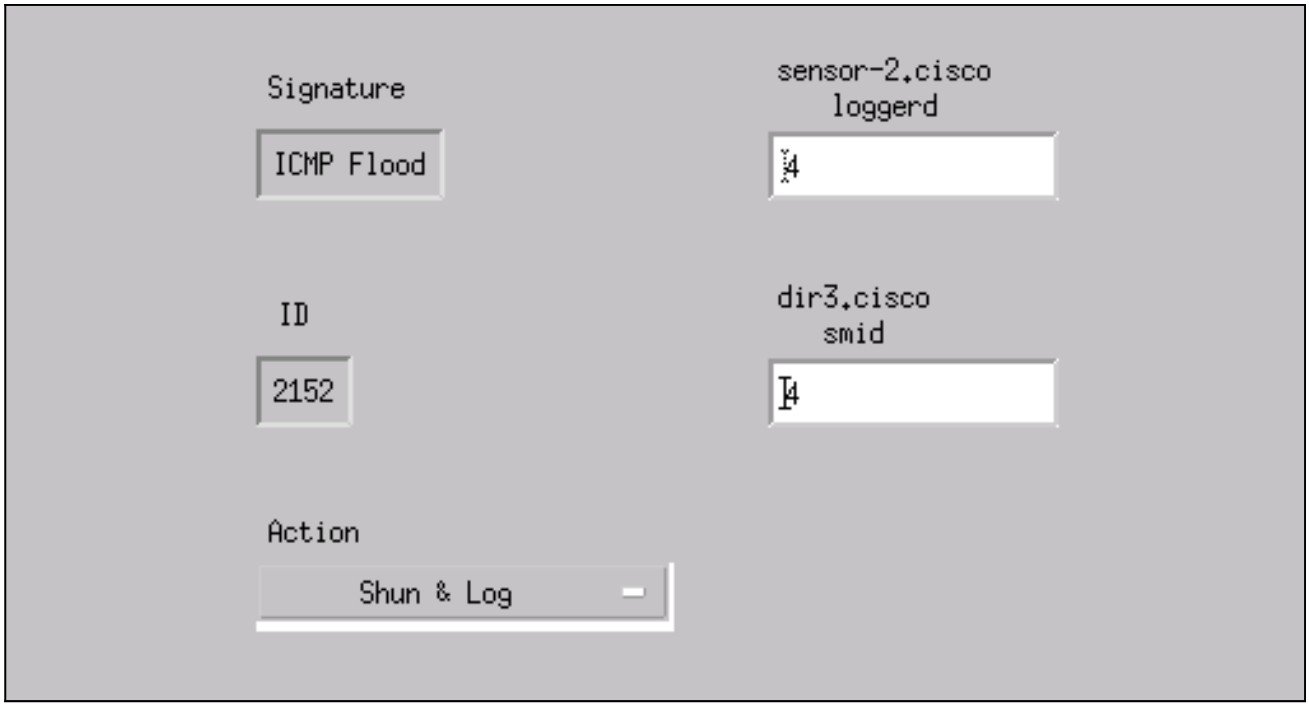
sind.

7. Öffnen Sie das Fenster Angriffserkennung, und klicken Sie auf **Geschützte Netzwerke**. Fügen Sie den Bereich **10.64.10.1** bis **10.64.10.254** in das geschützte Netzwerk ein, wie in diesem Beispiel

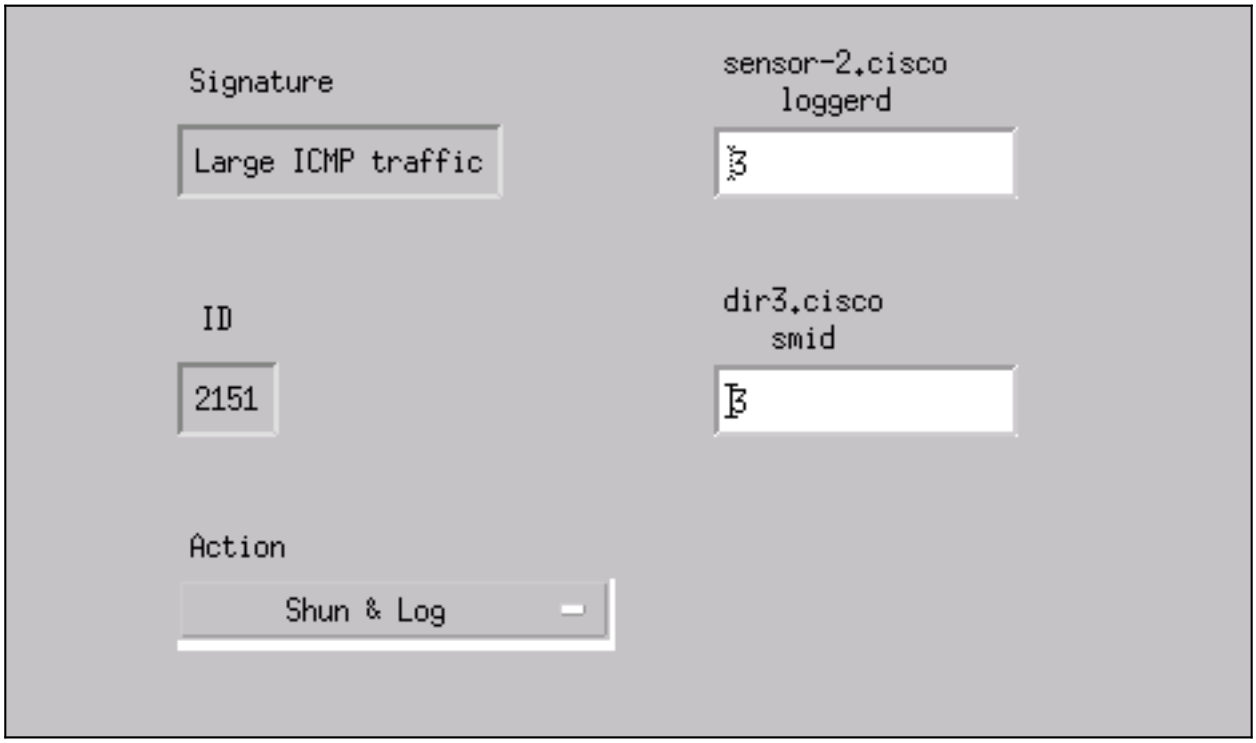


gezeigt.

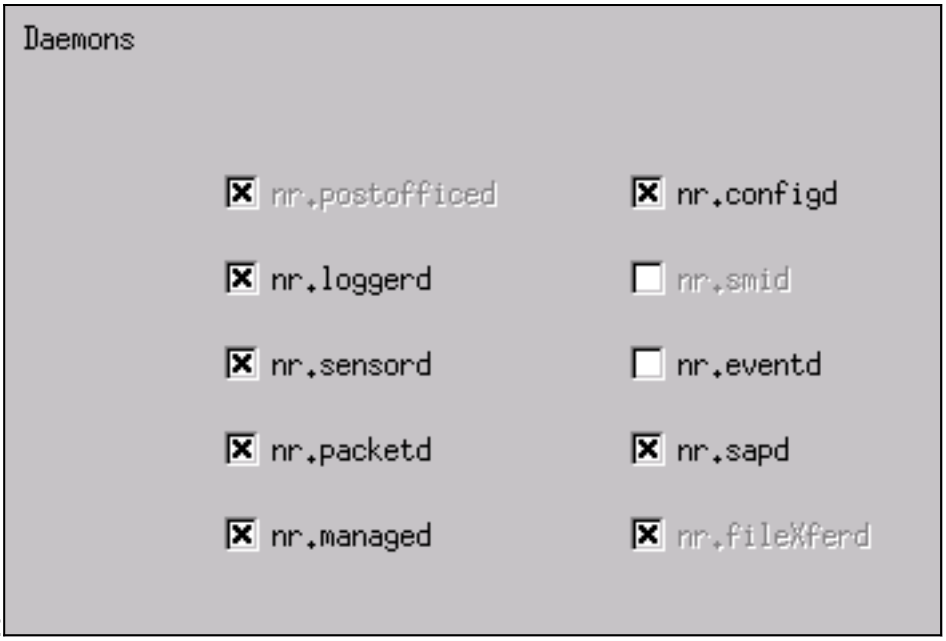
8. Klicken Sie auf **Profil > Manuelle Konfiguration**.
9. Wählen Sie **Signaturen ändern > Groß angelegter ICMP-Datenverkehr** mit der ID **2151 aus**.
10. Klicken Sie auf **Ändern**, ändern Sie die **Aktion** von "Keine" in "**Shun & Log**", und klicken Sie auf **OK**, um
    fortzufahren.



11. Wählen Sie **ICMP Flood** mit der ID **2152 aus**, und klicken Sie auf **Ändern**. Ändern Sie die **Aktion** von "Keine" in "**Shun & Log**", und klicken Sie auf **OK**, um fortzufahren.

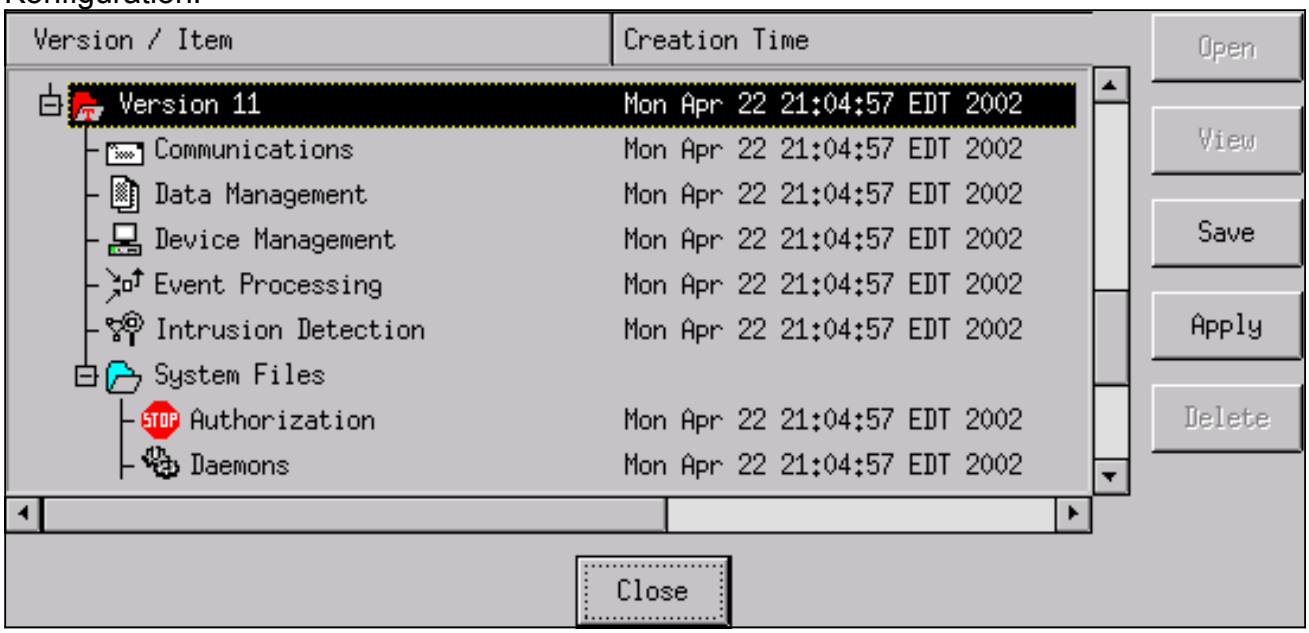


12. Klicken Sie auf **OK**, um das Fenster Intrusion Detection (Angriffserkennung) zu schließen.
13. Öffnen Sie den Ordner Systemdateien, und öffnen Sie das Fenster Daemons.Stellen Sie sicher, dass Sie diese Daemons aktiviert



haben:

14. Klicken Sie auf **OK**, um fortzufahren, wählen Sie die gerade geänderte Version aus, und 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.



Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show access-list** - Listet die **Zugriffslisten**-Befehlsanweisungen in der Router-Konfiguration auf. Außerdem wird eine Trefferzählung aufgelistet, die angibt, wie oft ein Element bei einer Befehlssuche **in der Zugriffsliste** zugeordnet wurde.
- **Ping** - Dient zum Diagnostizieren grundlegender Netzwerkverbindungen.

Bevor ein Angriff gestartet wird

Führen Sie diese Befehle aus, bevor ein Angriff gestartet wird.

```
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#
```

Starten und Beenden des Angriffs

Starten Sie den Angriff vom Router "Light" zum Opfer "House". Wenn die Zugriffskontrollliste die Zugriffsrechte übernimmt, werden die nicht erreichbaren Werte angezeigt.

```
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.
```

Sobald der Sensor den Angriff erkannt hat und die ACL heruntergeladen wird, wird diese Ausgabe im "Haus" angezeigt.

```
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
```

Die Unerreichbaren sind noch unter "Light" zu sehen, wie in diesem Beispiel gezeigt.

```
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)
```

15 Minuten später kehrt das "Haus" wieder zum Normalzustand zurück, da das "Shunning" auf 15 Minuten eingestellt war.

```
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" kann "Haus" pingen.

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Support-Seite für Cisco Secure Intrusion Prevention
- Technischer Support und Dokumentation - Cisco Systems