

IDS PIX Shunding mit Cisco IDS UNIX Director

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Konfigurieren des Sensors](#)

[Hinzufügen des Sensors zum Director](#)

[Konfigurieren des Shings für PIX](#)

[Überprüfen](#)

[Bevor Sie den Angriff starten](#)

[Starten und Beenden des Angriffs](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird beschrieben, wie Sie mithilfe von Cisco IDS UNIX Director (ehemals Netranger Director) und Sensor das Herunterfahren auf einem PIX konfigurieren. In diesem Dokument wird davon ausgegangen, dass der Sensor und Director betriebsbereit sind und die Sniffing-Schnittstelle des Sensors so eingerichtet ist, dass sie bis zur externen PIX-Schnittstelle reicht.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf diesen Software- und Hardwareversionen.

- Cisco IDS UNIX Director 2.2.3
- Cisco IDS UNIX Sensor 3.0.5
- Cisco Secure PIX mit 6.1.1 **Hinweis:** Wenn Sie die Version 6.2.x verwenden, können Sie

Secure Shell Protocol (SSH)-Management verwenden, jedoch nicht Telnet. Weitere Informationen finden Sie unter Cisco Bug ID [CSCdx55215](#) (nur [registrierte](#) Kunden).

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 finden Sie die Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

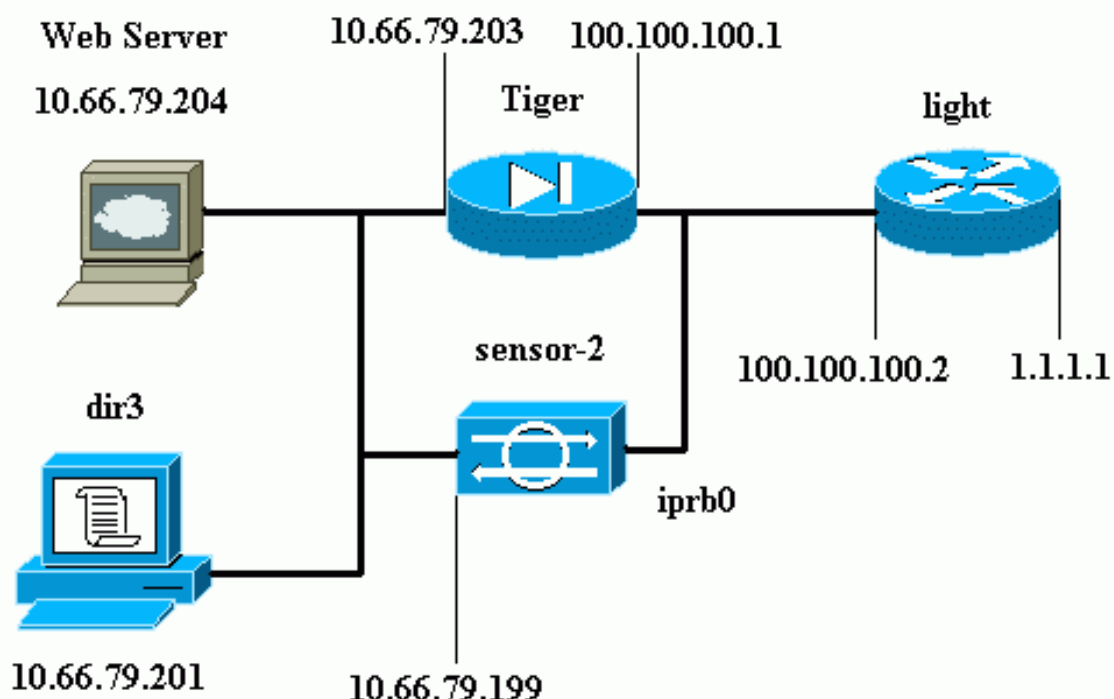
Cisco IDS UNIX Director und Sensor werden zur Verwaltung eines Cisco Secure PIX zum Shunting verwendet. Beachten Sie bei der Betrachtung dieser Konfiguration folgende Konzepte:

- Installieren Sie den Sensor, und stellen Sie sicher, dass der Sensor ordnungsgemäß funktioniert.
- Stellen Sie sicher, dass sich die Sniffing-Schnittstelle auf die externe Schnittstelle des PIX erstreckt.

Hinweis: Weitere Informationen zu den in diesem Dokument verwendeten Befehlen finden Sie im [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- [Routerleuchte](#)
- [PIX Tiger](#)

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
```

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

```

Konfigurieren des Sensors

In diesen Schritten wird beschrieben, wie der Sensor konfiguriert wird.

1. Telnet bis **10.66.79.199** mit Benutzernamen **root-** und **Kennwort-Angriff**.
2. Geben Sie **sysconfig-sensor** ein.
3. Geben Sie folgende Informationen ein: IP-Adresse: **10.66.79.199** IP-Netzmaske: **255 255 255 224** IP-Hostname: **Sensor 2** Standardroute: **10.66.79.193** Netzwerkzugriffskontrolle **10**. Kommunikationsinfrastruktur Sensor-Host-ID: **49** Sensor-Organisations-ID: **900** Sensor-Hostname: **Sensor 2** Name der Sensororganisation: **Cisco** Sensor-IP-Adresse: **10.66.79.199** IDS Manager-Host-ID: **50** IDS Manager-Organisations-ID: **900** IDS Manager-Hostname: **Verzeichnis3** Name der IDS Manager-Organisation: **Cisco** IP-Adresse des IDS Managers: **10.66.79.201**
4. Speichern Sie die Konfiguration. Der Sensor wird dann neu gestartet.

Hinzufügen des Sensors zum Director

Führen Sie diese Schritte aus, um den Sensor dem Director hinzuzufügen.

1. Telnet bis **10.66.79.201** mit Benutzernamen **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 Netranger-Konfigurationsmenü **Datei > Host hinzufügen aus**, und klicken Sie auf **Weiter**.
5. Geben Sie diese Informationen ein, und 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. Lassen Sie die Standardeinstellungen unverändert, und klicken Sie auf

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

Weiter.

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, basierend auf dem Sensortyp und der Art, wie Sie den Sensor verbinden.

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.

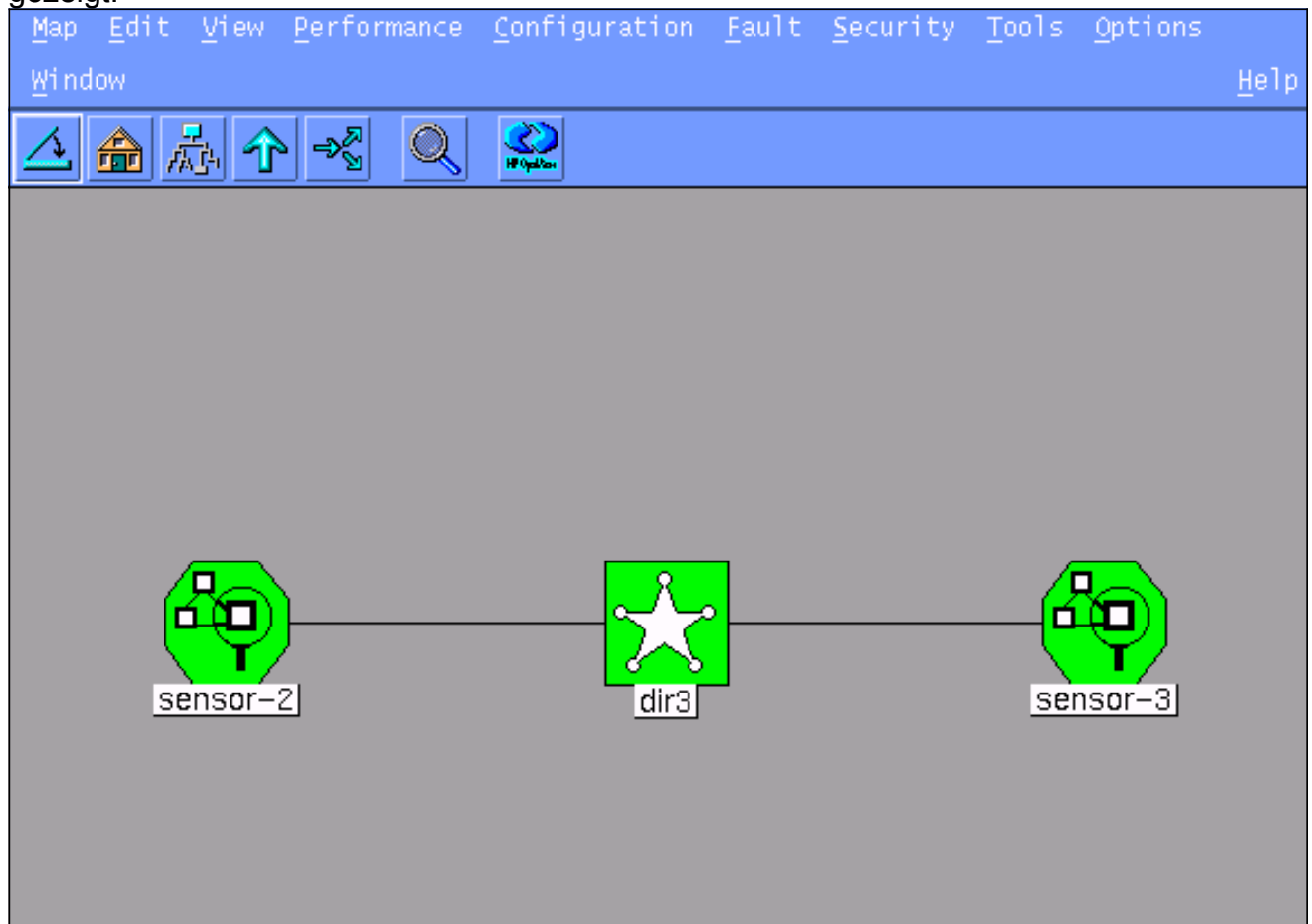
Number of minutes to log on an event.

Number of minutes to shun on an event.

Network Interface Name

Sensor Protected Networks

8. Klicken Sie auf **Weiter**, bis eine Option zum Klicken auf **Fertig stellen** ist. Der Sensor wurde nun erfolgreich zum Director hinzugefügt. Im Hauptmenü wird **sensor-2** angezeigt, wie in diesem Beispiel gezeigt.



Führen Sie diese Schritte aus, um die Fehlerbehebung für PIX zu konfigurieren.

1. Wählen Sie im Hauptmenü **Sicherheit > Konfigurieren aus**.
2. Markieren Sie im Netranger-Konfigurationsmenü den Eintrag **sensor-2**, und doppelklicken Sie darauf.
3. Öffnen Sie **die Geräteverwaltung**.
4. Klicken Sie auf **Geräte > Hinzufügen**, und geben Sie die in diesem Beispiel gezeigten Informationen ein. Klicken Sie auf **OK**, um fortzufahren. Telnet und enable sind beide "Cisco".

The screenshot shows a configuration form with the following fields and values:

IP Address	10.66.79.203	User Name	
Device Type	PIX	Password	*****
Sensor's NAT IP Address		Enable Password	*****
<input type="checkbox"/> Enable SSH			

5. Klicken Sie auf **Herunterfahren > Hinzufügen**. Fügen Sie Host **100.100.100.100** unter "Niemals zu schließende Adressen" hinzu. Klicken Sie auf **OK**, um

The screenshot shows the 'Addresses Never to Shun' configuration window with the following details:

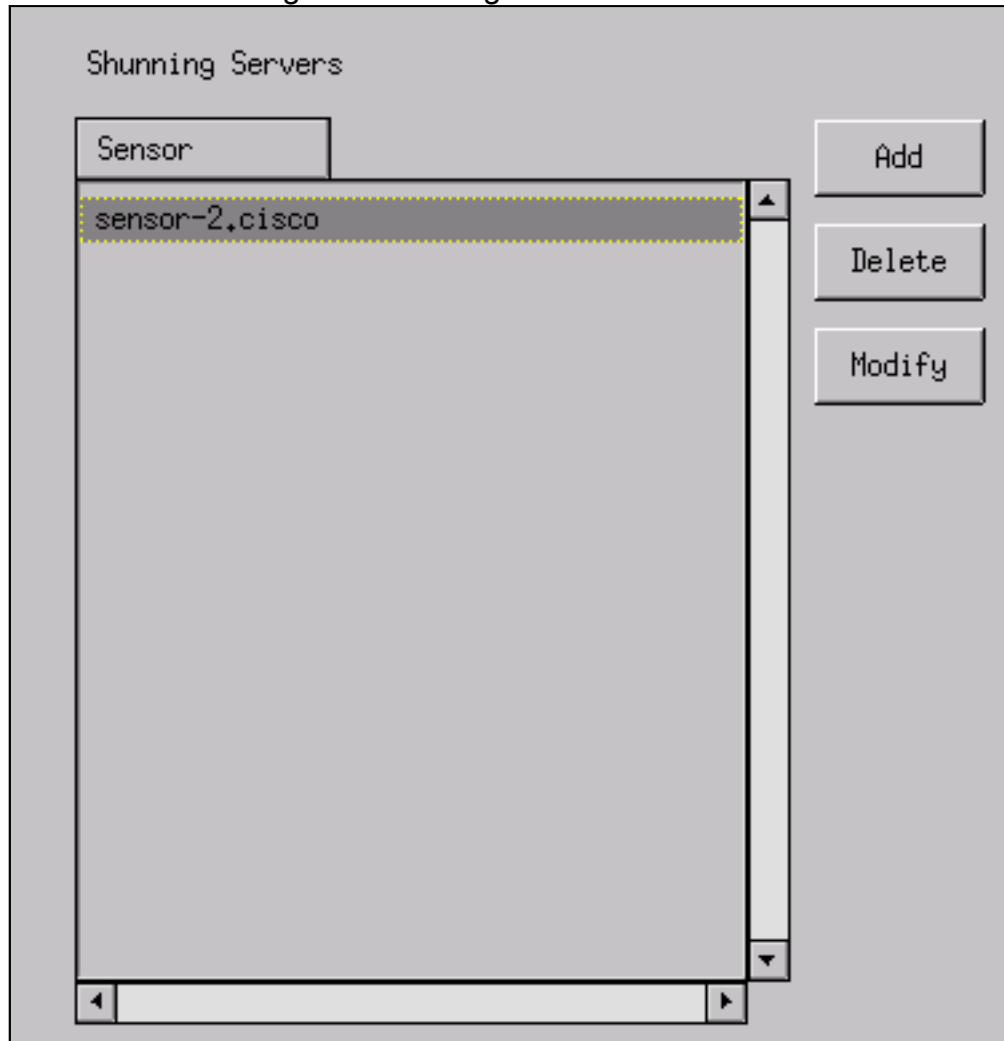
- Maximum Number of Shunned Entries: 100
- Addresses Never to Shun table:

Network Address	Network Mask
100.100.100.100	255.255.255.255

Buttons: Add, Delete, Modify

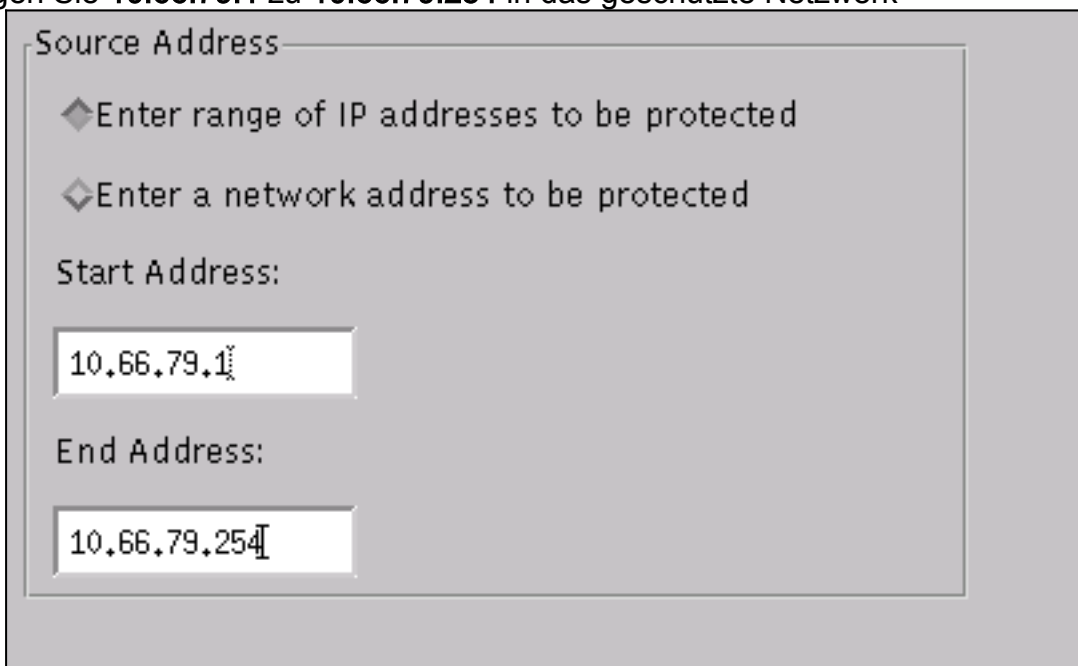
fortzufahren.

6. Klicken Sie auf **Shunning > Add**, und wählen Sie **sensor-2.cisco** als die Server aus, die nicht geladen werden. Dieser Teil der Konfiguration ist abgeschlossen. Schließen Sie das Fenster



Geräteverwaltung.

7. Öffnen Sie das Fenster Angriffserkennung, und klicken Sie auf **Geschützte Netzwerke**. Fügen Sie **10.66.79.1** zu **10.66.79.254** in das geschützte Netzwerk



ein.

8. Klicken Sie auf **Profil** und wählen Sie **Manuelle Konfiguration > Signaturen ändern aus**. Wählen Sie **Large ICMP Traffic and ID: 2151** klicken Sie auf **Ändern**, und ändern Sie die Aktion von **Keine** in **Beenden und Anmelden**. Klicken Sie auf **OK**, um

fortzufahren.

Signature	sensor-2,cisco loggerd
Large ICMP traffic	3
ID	dir3,cisco smid
2151	3
Action	
Shun & Log	

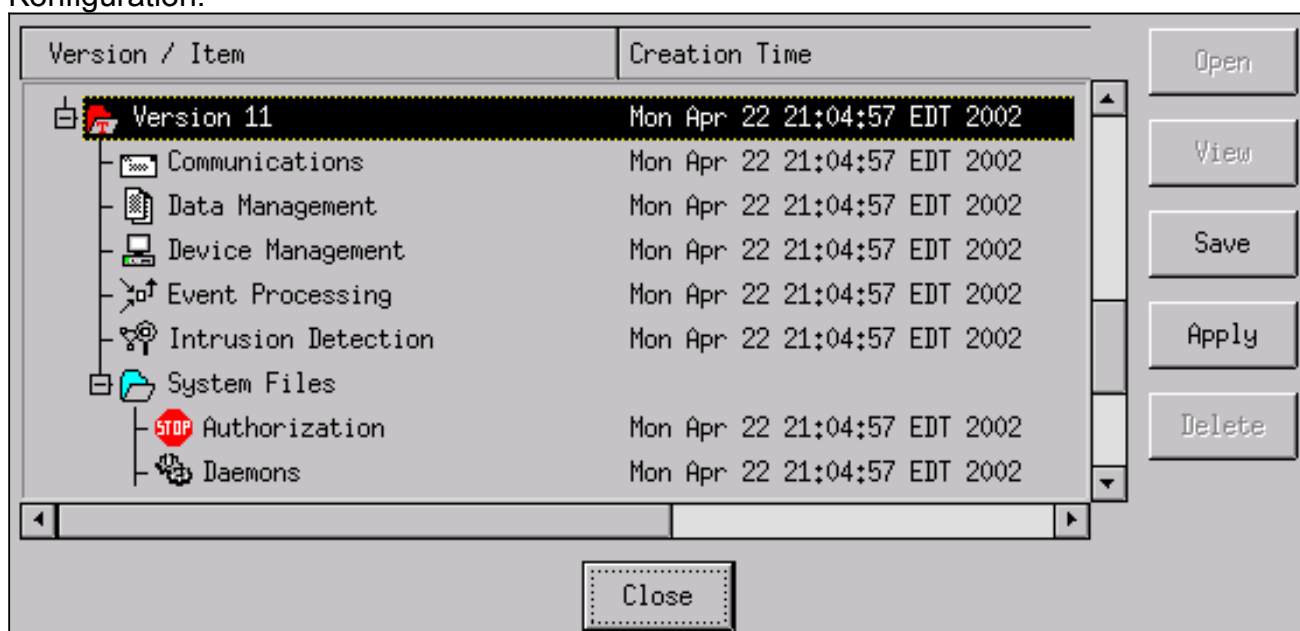
9. Wählen Sie **ICMP Flood** und **ID: 2152** klicken Sie auf **Ändern**, und ändern Sie die Aktion von **Keine** in **Beenden und Protokoll**. Klicken Sie auf **OK**, um fortzufahren.

Signature	sensor-2,cisco loggerd
ICMP Flood	4
ID	dir3,cisco smid
2152	4
Action	
Shun & Log	

10. Dieser Teil der Konfiguration ist abgeschlossen. Klicken Sie auf **OK**, um das Fenster Intrusion Detection (Angriffserkennung) zu schließen.
11. Öffnen Sie den Ordner **Systemdateien**, und öffnen Sie das Fenster **Daemons**. Stellen Sie sicher, dass Sie diese Daemons aktiviert haben:



12. Klicken Sie auf **OK**, um fortzufahren, und wählen Sie die Version aus, die Sie gerade geändert haben. Klicken Sie auf **Speichern > Übernehmen**. Warten Sie, bis das System Ihnen mitteilt, dass der Sensor fertig ist, starten Sie die Dienste neu, und schließen Sie alle Fenster für die Netranger-Konfiguration.



Überprüfen

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

Bevor Sie den Angriff starten

```
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

Starten und Beenden des Angriffs

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

15 Minuten später kehrt er wieder zur Normalität zurück, da das Geräusch auf 15 Minuten eingestellt ist.

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
```

Fehlerbehebung

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

Zugehörige Informationen

- [End-of-Sale für Cisco IDS Director](#)
- [End-of-Life für Cisco IDS Sensor Software Version 3.x](#)
- [Produkt-Support für das Cisco Intrusion Prevention System](#)
- [Produkt-Support für die Cisco PIX Firewall](#)
- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)