IDS PIX Shunning Using Cisco IDS UNIX Director

Document ID: 25702

Cisco has announced the end−of−sales for the Cisco Secure IDS Director and the end−of−sales and end−of−life for Cisco IDS 3.x Sensor Software.

Contents

Introduction

This document describes how to configure shunning on a PIX with the help of Cisco IDS UNIX Director (formerly known as Netranger Director) and Sensor. This document assumes that the Sensor and Director are operational and the sniffing interface of the Sensor is set up to span to the PIX outside interface.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions.

- Cisco IDS UNIX Director 2.2.3
- Cisco IDS UNIX Sensor 3.0.5
- Cisco Secure PIX with 6.1.1

Note: If you use the 6.2.x version, you can use Secure Shell Protocol (SSH) management, but not Telnet. Refer to Cisco bug ID CSCdx55215 (registered customers only) for further information.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information used to configure the features described in this document.

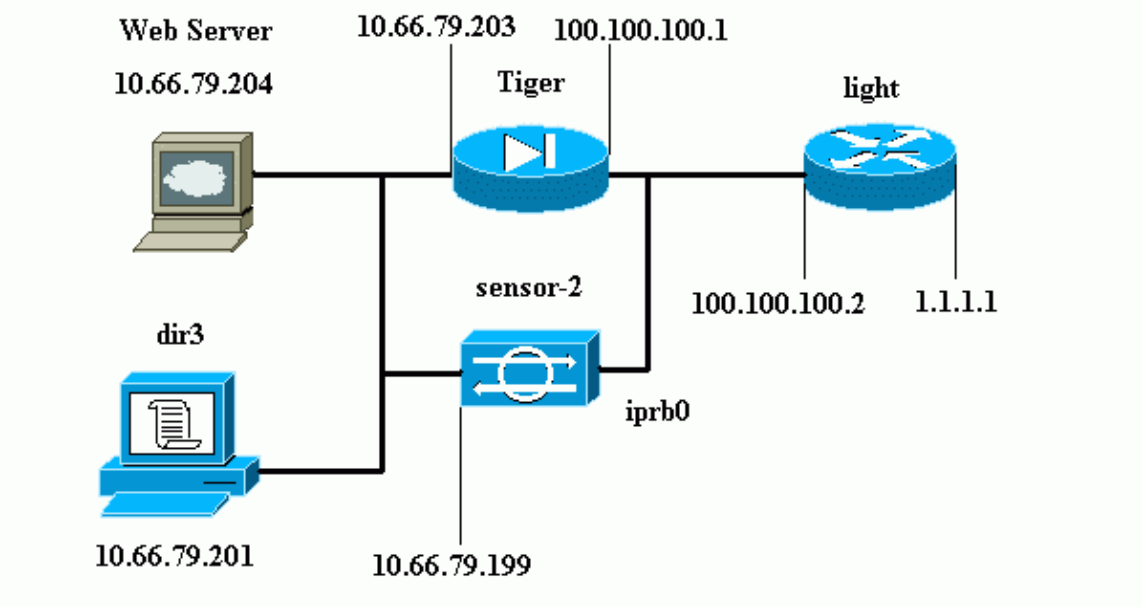
Cisco IDS UNIX Director and Sensor are used in order to manage a Cisco Secure PIX for shunning. When you consider this configuration, remember these concepts:

- Install the Sensor and make sure the Sensor works properly.
- Ensure that the sniffing interface spans to the outside interface of the PIX.

Note: In order to find additional information on the commands used in this document, refer to the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup.



Configurations

This document uses these configurations.

- Router Light
- PIX Tiger

Router Light

```
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
```

Configure the Sensor

These steps describe how to configure the Sensor.

1. Telnet to **10.66.79.199** with username **root** and password **attack**.
2. Enter **sysconfig-sensor**.
3. Enter this information:

    a. IP Address: **10.66.79.199**
    b. IP Netmask: **255.255.255.224**
    c. IP Host Name: **sensor-2**
    d. Default Route: **10.66.79.193**
    e. Network Access Control

    10.
    f. Communications Infrastructure

    Sensor Host ID: **49**

    Sensor Organization ID: **900**

    Sensor Host Name: **sensor-2**

    Sensor Organization Name: **cisco**

    Sensor IP Address: **10.66.79.199**

    IDS Manager Host ID: **50**

    IDS Manager Organization ID: **900**

IDS Manager Host Name: **dir3**

IDS Manager Organization Name: **cisco**

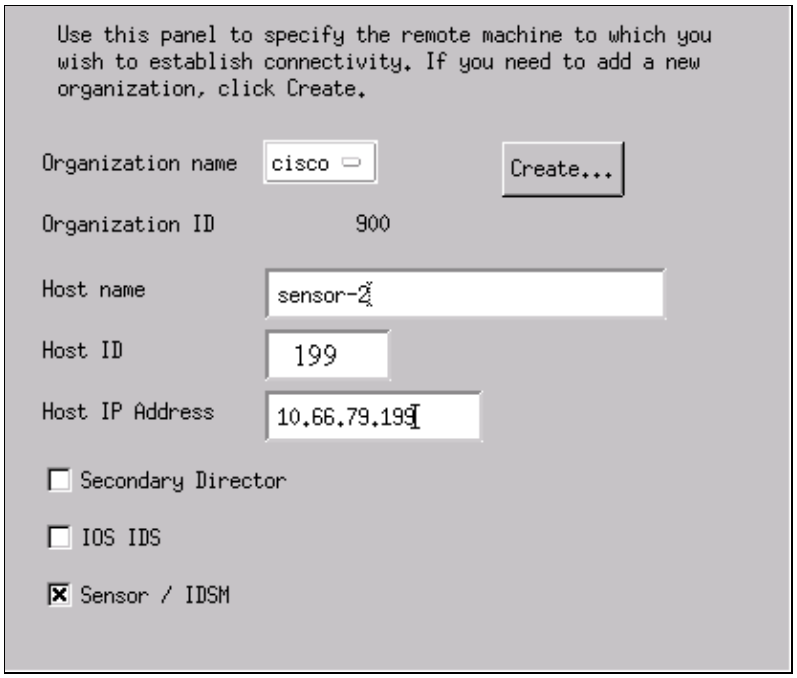
IDS Manager IP Address: **10.66.79.201**

4. Save the configuration. The Sensor then reboots.

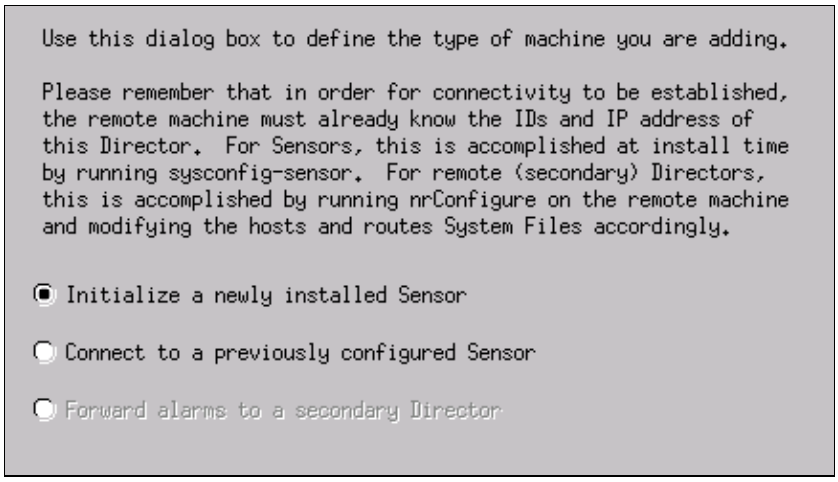
Add the Sensor Into the Director

Complete these steps in order to add the Sensor into the Director.

1. Telnet to **10.66.79.201** with username **netrangr** and password **attack**.
2. Enter **ovw&** in order to launch HP OpenView.
3. In the Main Menu, select **Security** > **Configure**.
4. In the Netranger Configuration Menu, select **File** > **Add Host**, and click **Next**.
5. Enter this information, and click **Next**.

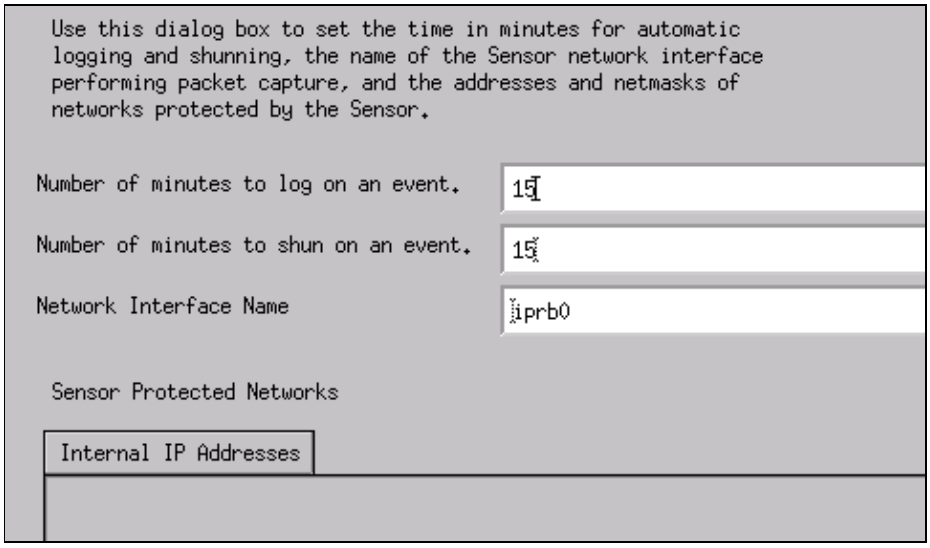


6. Leave the default settings and click **Next**.



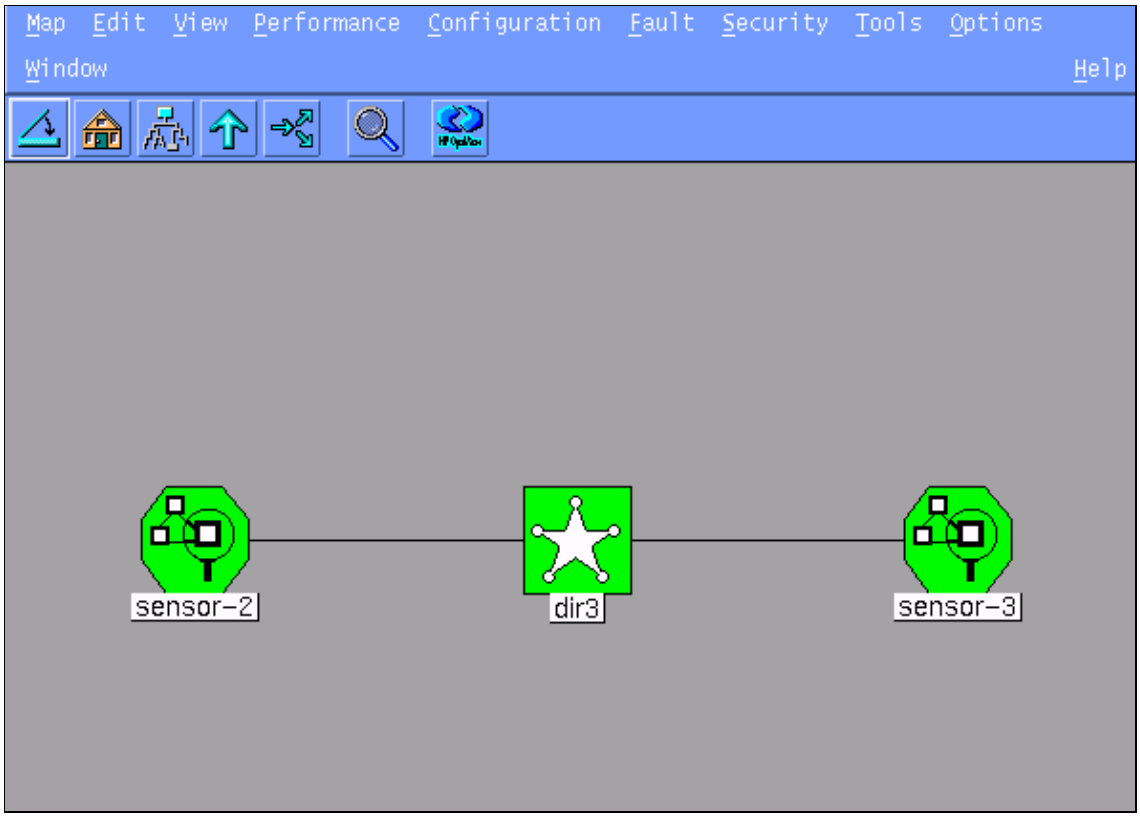
7. Change the log and shun minutes or leave them as the default if the values are acceptable. Change the Network Interface name to the name of your sniffing interface. In this example, it is "iprb0". It can be

"spwr0" or anything else based on the Sensor type and how you connect the Sensor.



8. Click **Next** until there is an option to click **Finish**.

   The Sensor is now successfully added into the Director. From the main menu, **sensor−2** is displayed, as shown in this example.

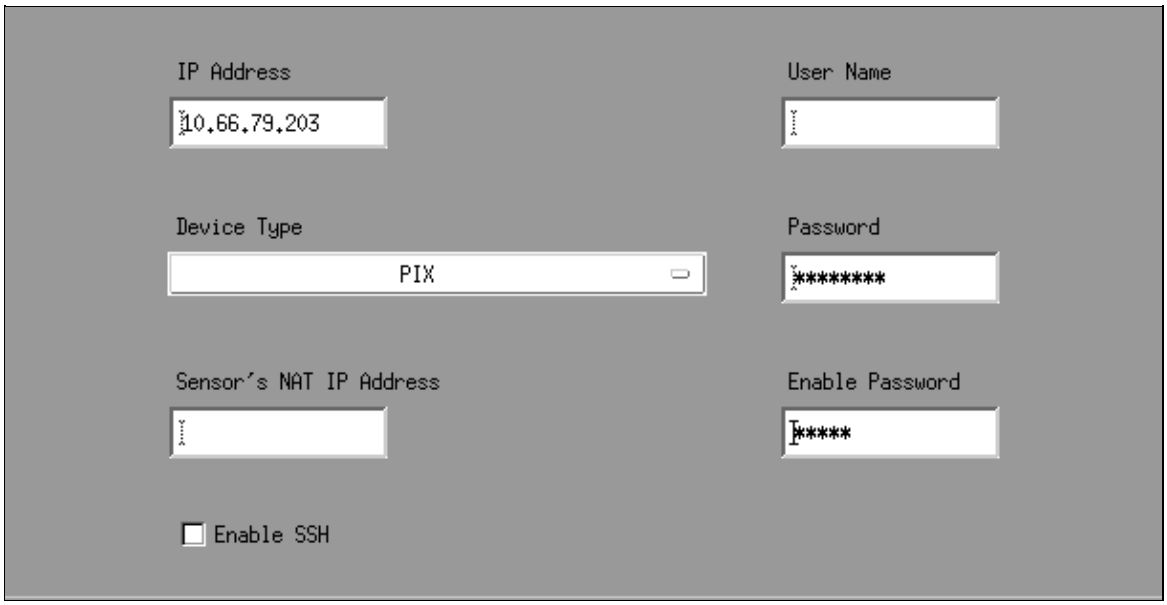


Configure Shunning for PIX

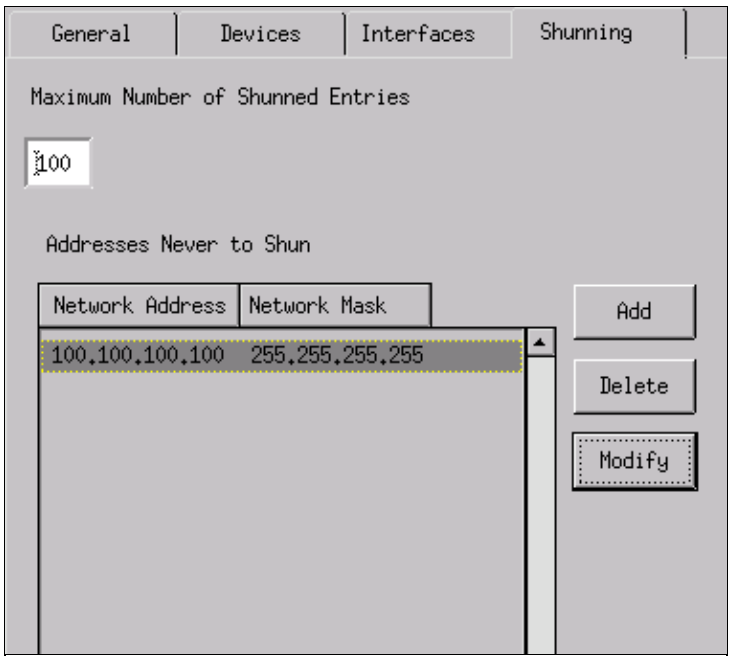
Complete these steps in order to configure shunning for PIX.

1. In the Main Menu, select **Security** > **Configure**.
2. In the Netranger Configuration Menu, highlight **sensor−2** and double click it.
3. Open **Device Management**.

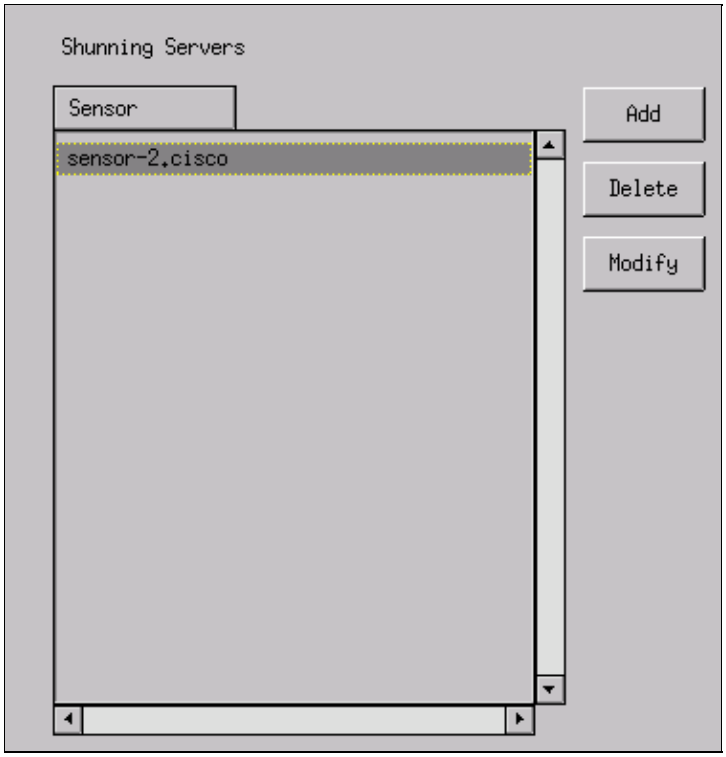
4. Click **Devices** > **Add** and enter the information as shown in this example. Click **OK** in order to continue. The Telnet and enable password are both "Cisco".



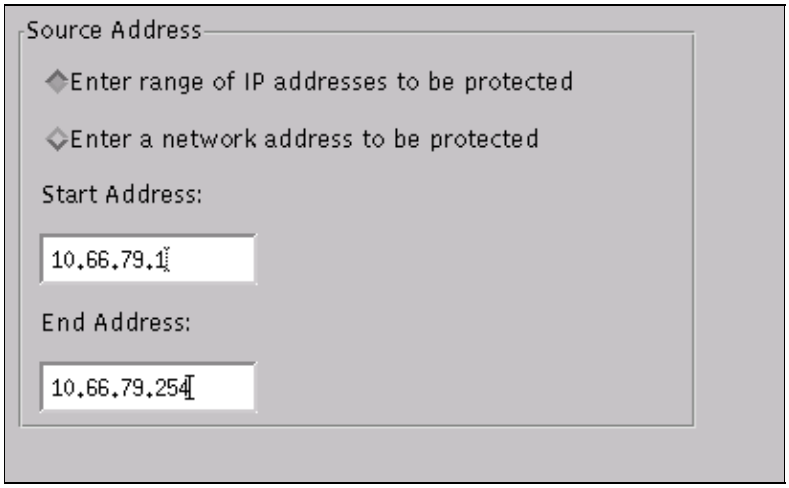
5. Click **Shunning** > **Add**. Add host **100.100.100.100** under "Addresses Never to Shun." Click **OK** in order to continue.



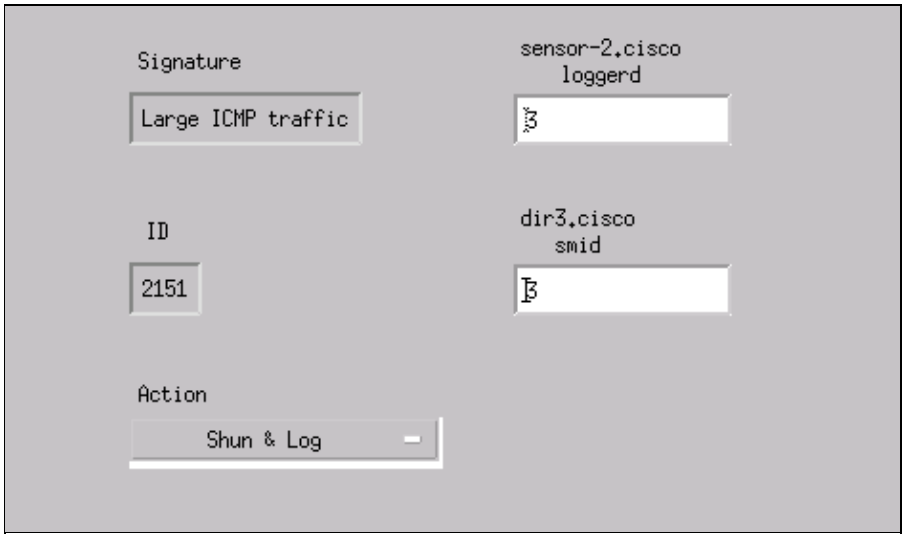
6. Click **Shunning** > **Add** and select **sensor−2.cisco** as the shunning servers. This part of the configuration is completed. Close the Device Management window.



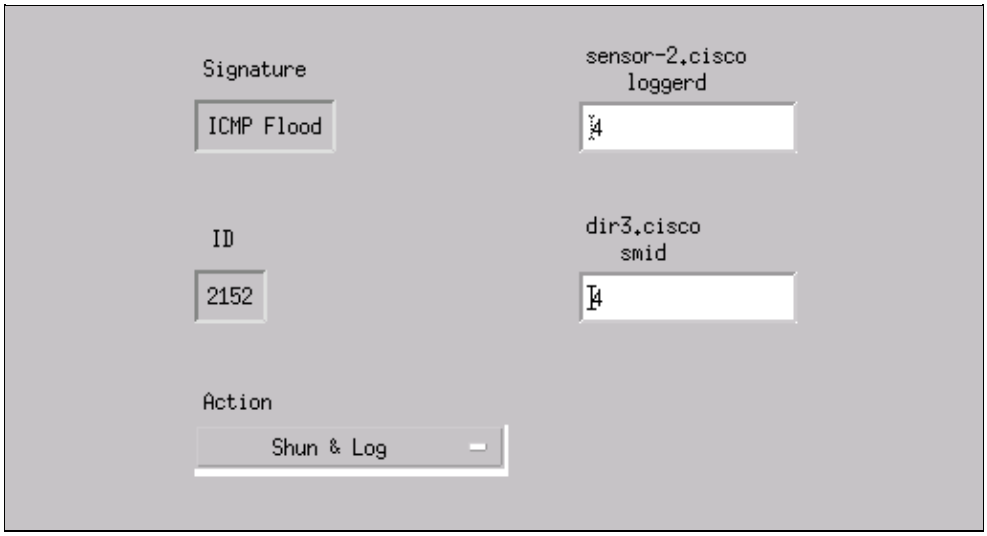
7. Open the Intrusion Detection window and click **Protected Networks**. Add **10.66.79.1** to **10.66.79.254** into the protected network.



8. Click **Profile** and select **Manual Configuration** > **Modify Signatures**. Select **Large ICMP Traffic** and **ID: 2151**, click **Modify**, and change the Action from None to **Shun and Log**. Click **OK** in order to continue.

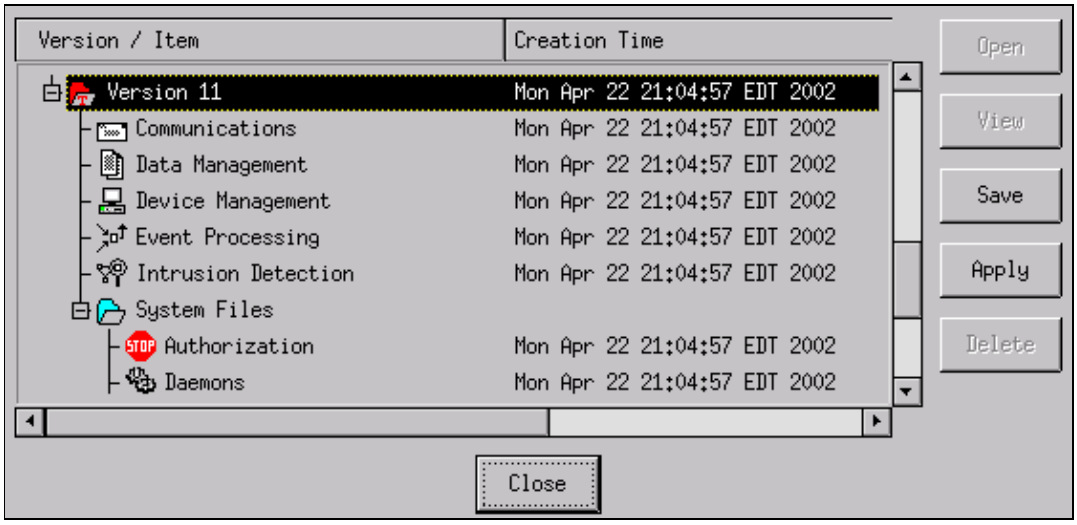


9. Select **ICMP Flood** and **ID: 2152**, click **Modify**, and change the Action from **None** to **Shun and Log**. Click **OK** in order to continue.



10. This part of configuration is complete. Click **OK** in order to close the Intrusion Detection window.
11. Open the **System Files** folder and open the **Daemons** window. Ensure you have enabled these daemons:

12. Click **OK** in order to continue, and select the version you just modified. Click **Save** > **Apply**. Wait for the system to tell you the Sensor is finished, restart Services, and close all the windows for the Netranger configuration.



Verify

This section provides information that helps you to confirm your configuration works properly.

Before You Launch the Attack

```
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
```

Launch the Attack and Shunning

```
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
```

Fifteen minutes later, it goes back to normal because the shunning is set to fifteen minutes.

```
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
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **End−of−Sale for the Cisco IDS Director**
- **End−of−Life for Cisco IDS Sensor Software Version 3.x**
- **Cisco Intrusion Prevention System Product Support**
- **Cisco PIX Firewall Software Product Support**
- **Cisco Secure PIX Firewall Command References**
- **Technical Support & Documentation − Cisco Systems**