使用Cisco IDS UNIX Director的IDS PIX迴避

目錄

簡介

本文檔介紹如何在Cisco IDS UNIX Director（以前稱為Netranger Director）和Sensor的幫助下在PIX上配置迴避。本文檔假設感測器和控制器工作正常，並且感測器的嗅探介面設定為跨越到PIX外部介面。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- Cisco IDS UNIX導向器2.2.3
- Cisco IDS UNIX感應器3.0.5
- 採用6.1.1的Cisco安全PIX**注意：**如果使用6.2.x版本，您可以使用安全殼層協定(SSH)管理，但不能使用Telnet。如需詳細資訊，請參閱Cisco錯誤ID CSCdx55215(僅限註冊客戶)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

本節提供用於設定本檔案中所述功能的資訊。

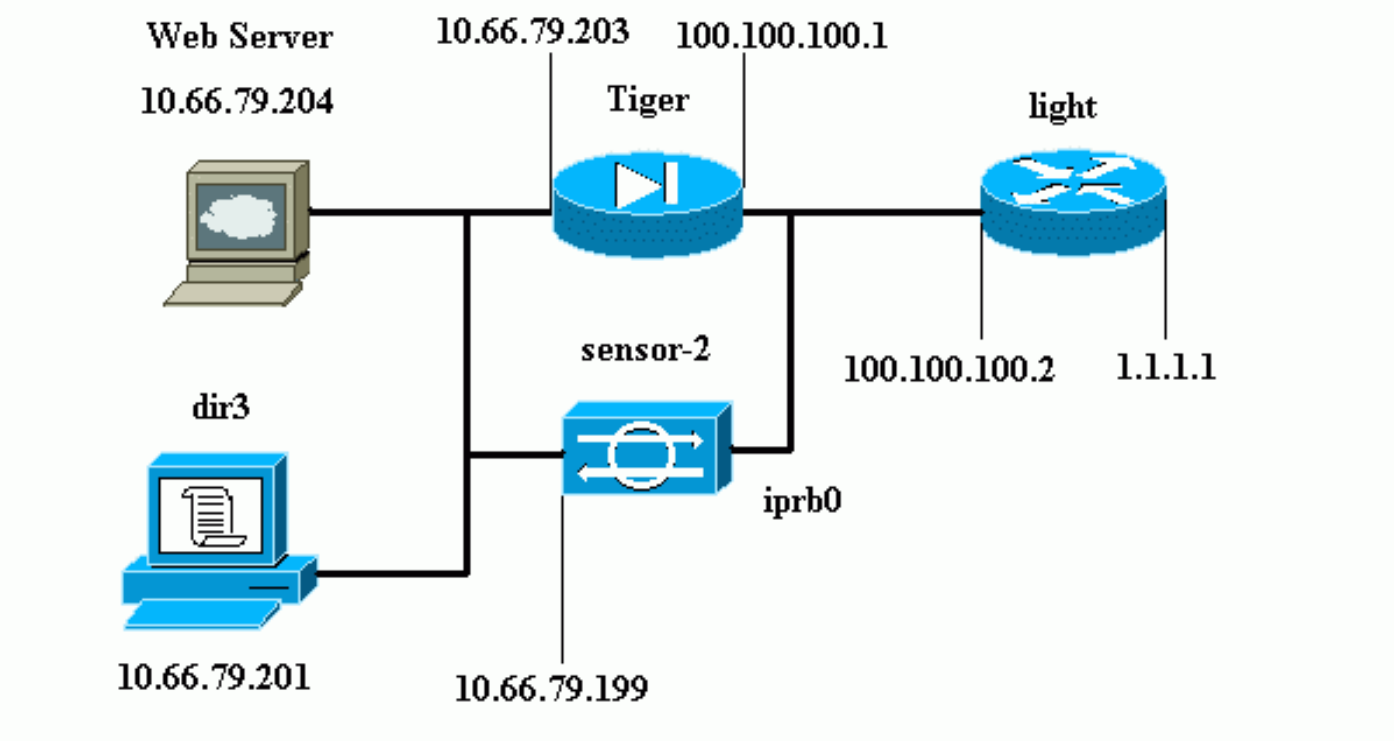
Cisco IDS UNIX Director和Sensor用於管理Cisco Secure PIX，以便迴避。當您考慮此設定時，請記住以下概念：

- 安裝感測器並確保感測器正常工作。
- 確保監聽介面跨越到PIX的外部介面。

注意：要查詢有關本文檔中使用的命令的其他資訊，請參閱命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用此網路設定。



組態

本檔案會使用這些設定。

- 路由器指示燈
- PIX老虎

路由器指示燈

```
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老虎

```
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
```

配置感測器

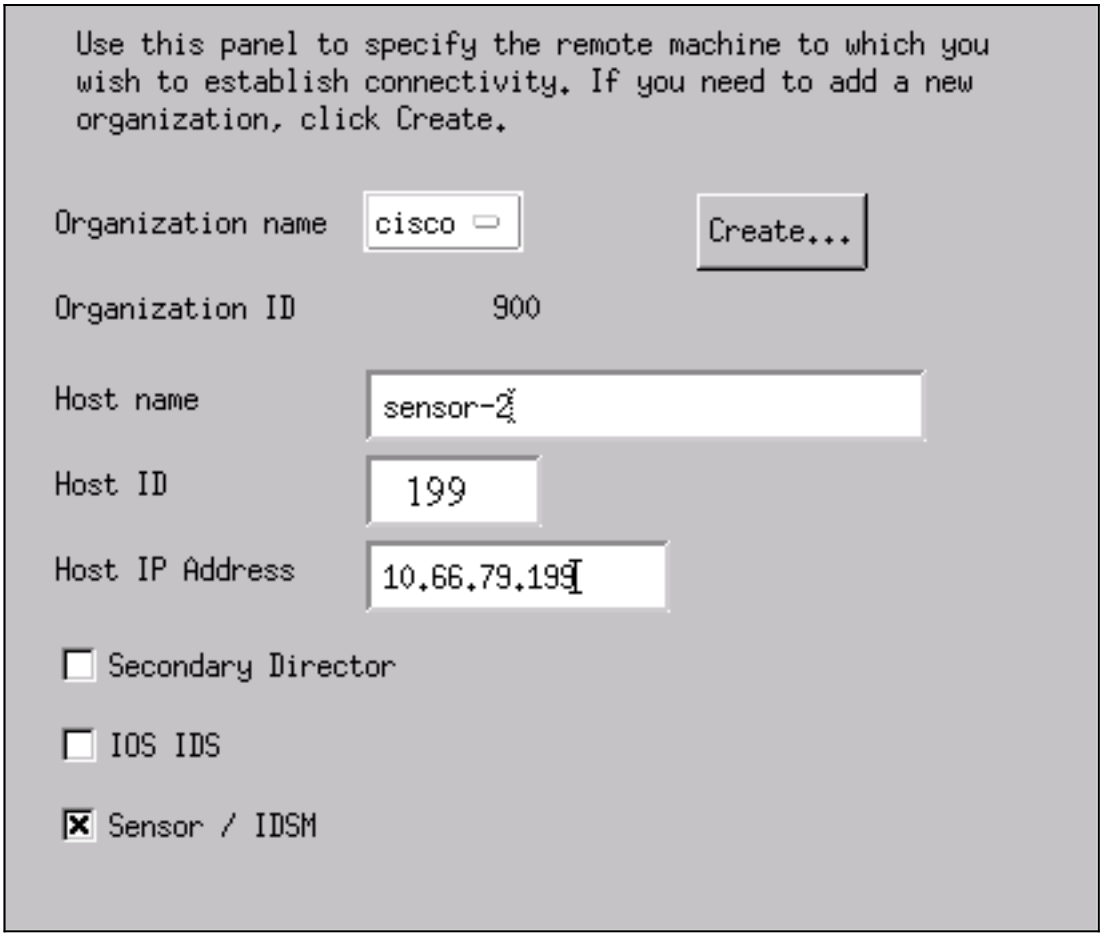
以下步驟描述如何配置感測器。

1. Telnet至**10.66.79.199**，使用使用者名稱**root**和密碼**攻擊**。
2. 輸入**sysconfig-sensor**。
3. 輸入以下資訊：IP 位址:**10.66.79.199**IP網路掩碼：**255.255.255.224**IP主機名：**sensor-2**預設路由：**10.66.79.193**網路存取控制**10.**通訊基礎架構感測器主機ID:**49**感測器組織ID:**900**感測器主機名：**sensor-2**感測器組織名稱：**思科**感測器IP地址：**10.66.79.199**IDS管理器主機ID:**50**IDS管理員組織ID:**900**IDS管理器主機名：**dir3**IDS管理員組織名稱：**思科**IDS管理器IP地址：**10.66.79.201**
4. 儲存組態。然後感測器重新啟動。

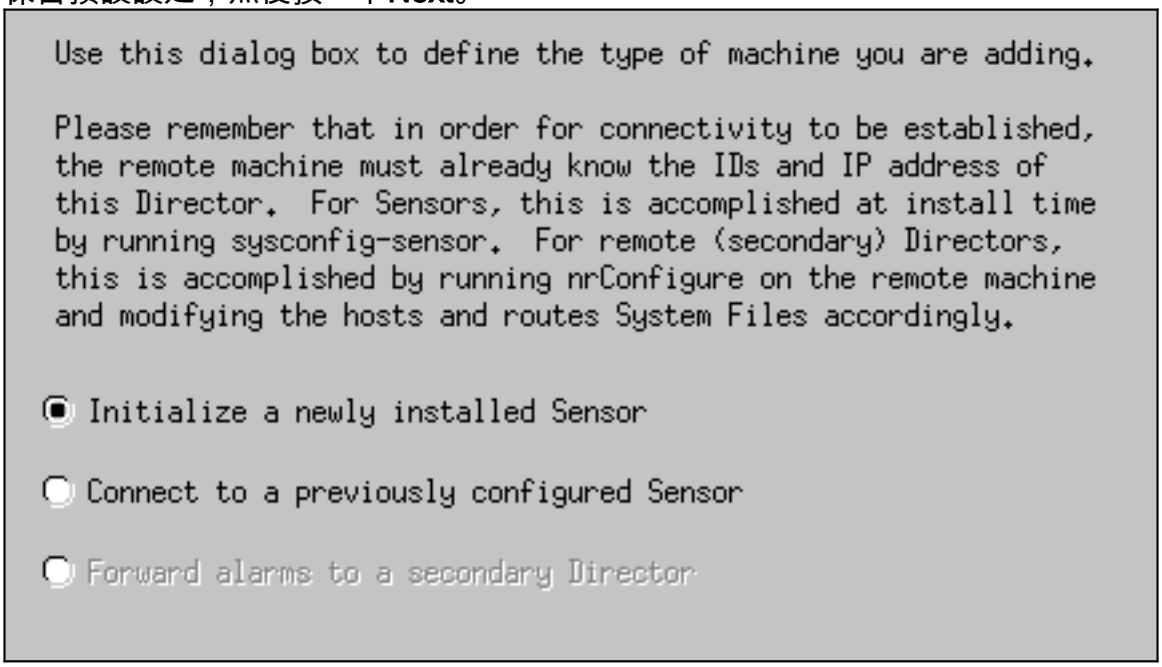
將感測器新增到指揮交換機中

完成這些步驟，將感測器新增到Director。

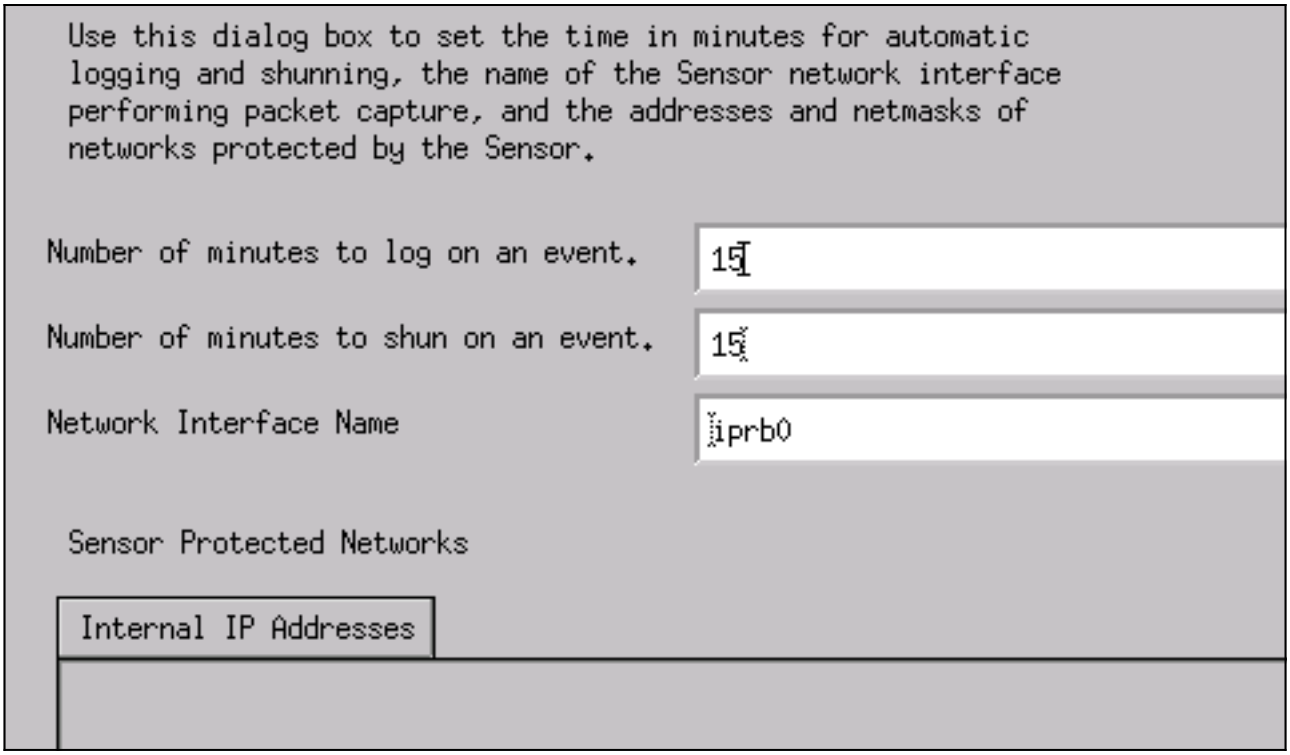
1. Telnet至**10.66.79.201**，使用使用者名稱**netrangr**和密碼**攻擊**。
2. 輸入**ovw&**以啟動HP OpenView。
3. 在主選單中，選擇**Security > Configure**。
4. 在Netranger Configuration Menu中，選擇**File > Add Host**，然後按一下**Next**。
5. 輸入此資訊，然後按一下**下一步**。



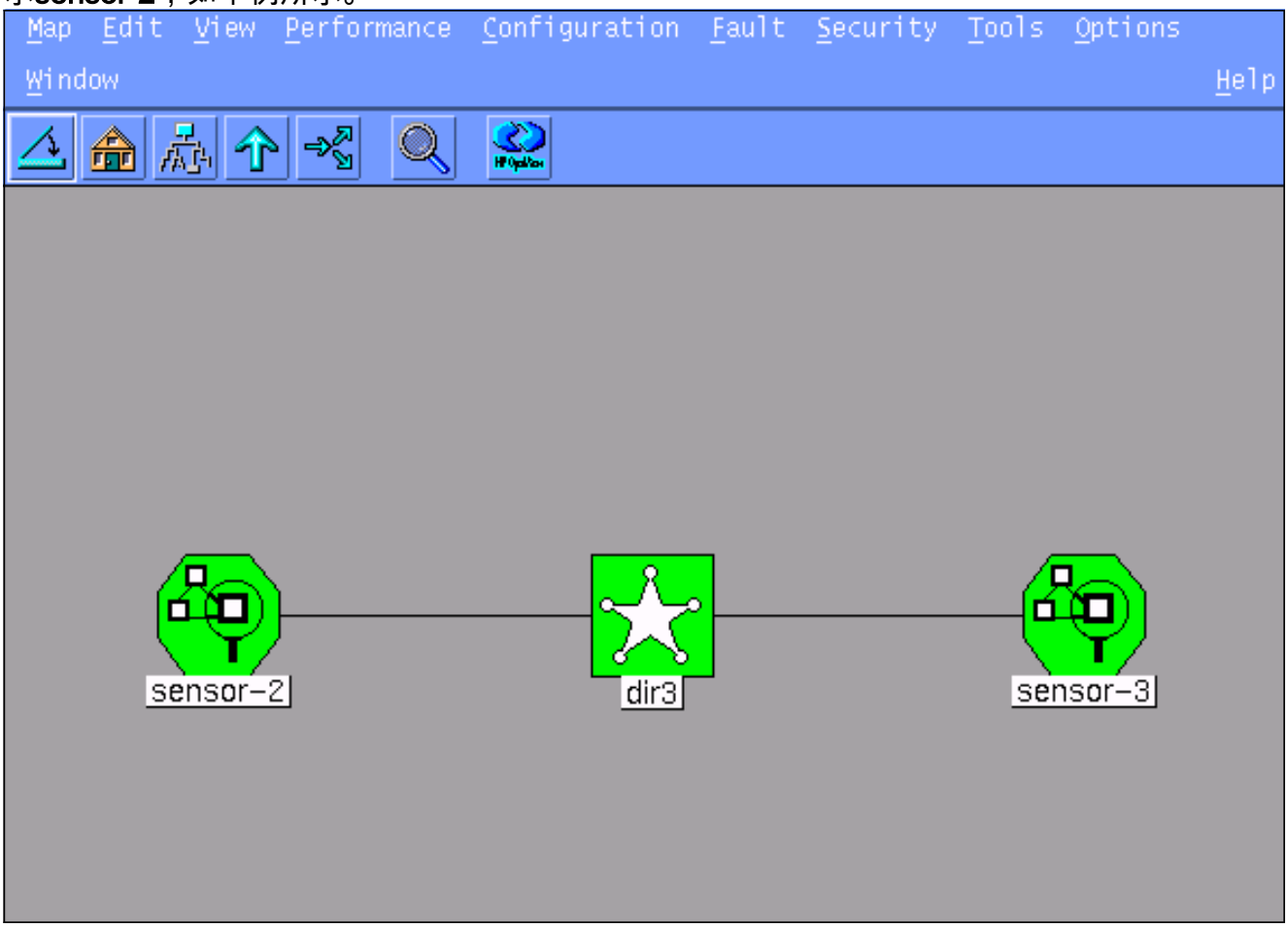
6. 保留預設設定，然後按一下**Next**。



7. 更改日誌和迴避分鐘數，或在值可接受的情況下將其保留為預設值。將Network Interface名稱更改為監聽介面的名稱。在本示例中，它是「iprb0」。 它可以是「spwr0」或其他任何形式，具體取決於感測器型別和連線感測器的方式。



8. 按一下**Next**，直到有選項可按一下**Finish**。感測器現在已成功新增到指揮交換機中。主選單顯示**sensor-2**，如本例所示。

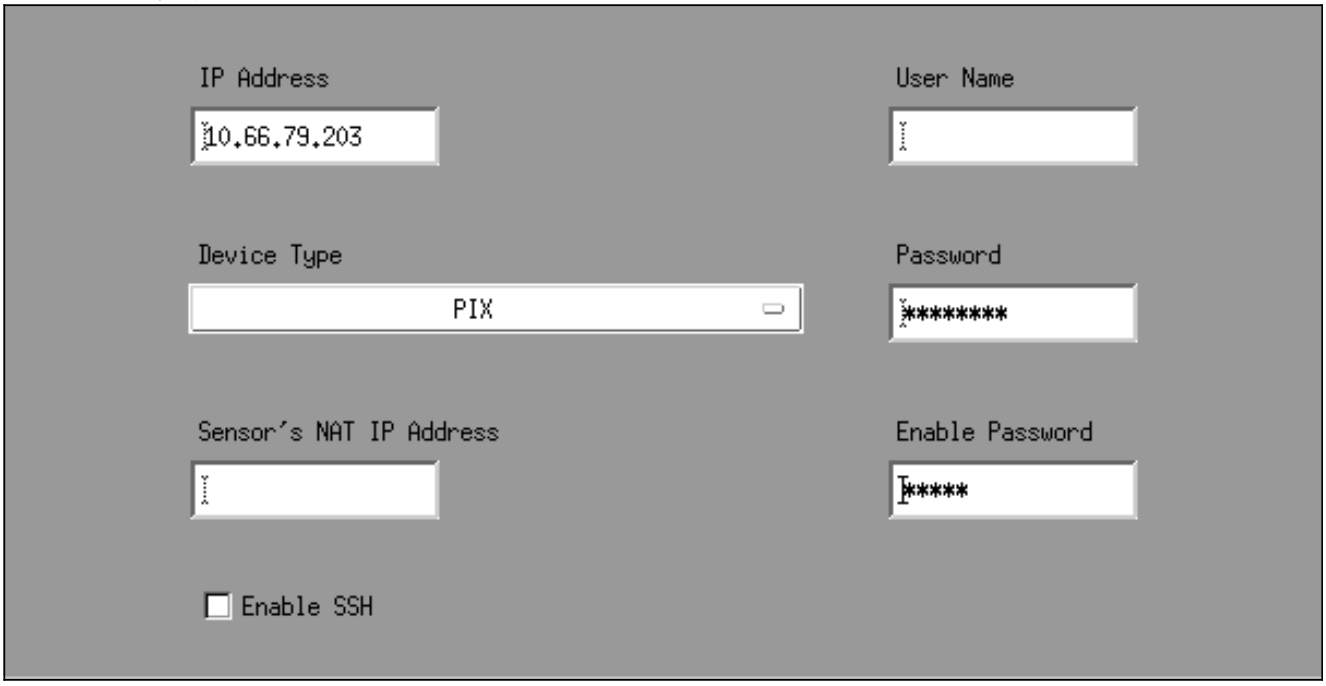


配置PIX的迴避

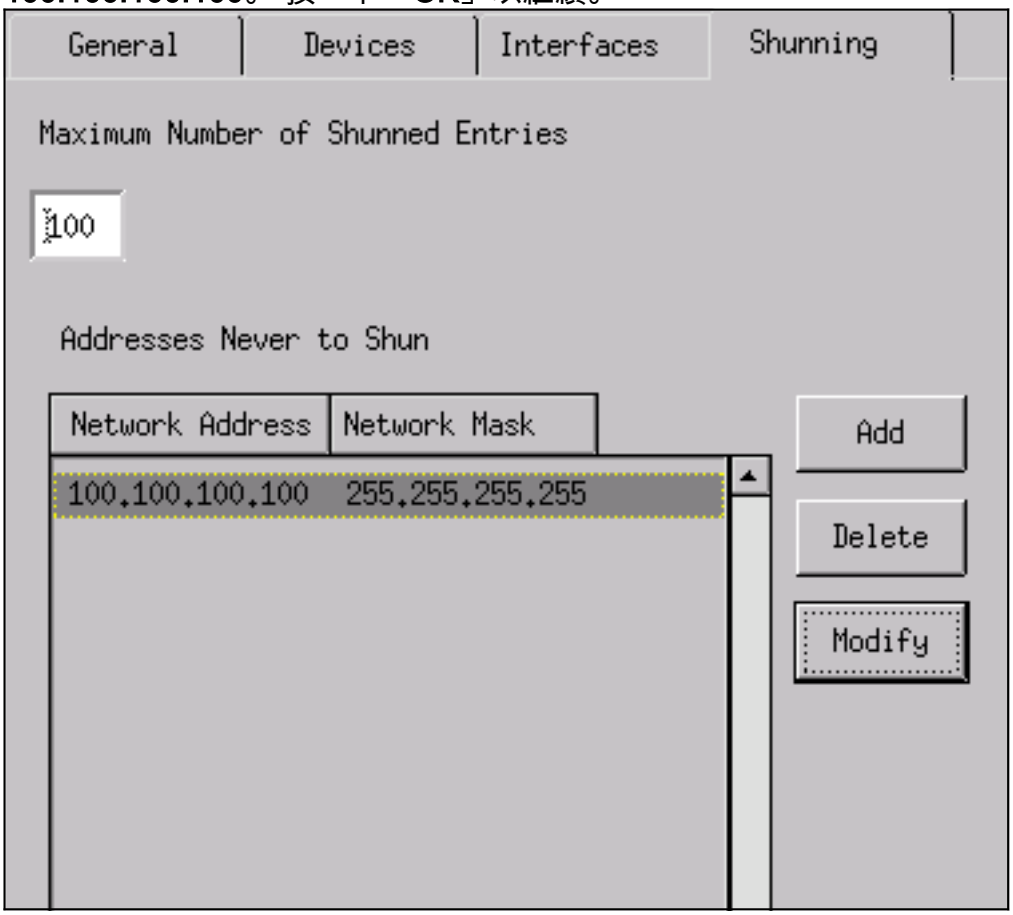
完成以下步驟以配置PIX的迴避。

1. 在主選單中，選擇**Security > Configure**。

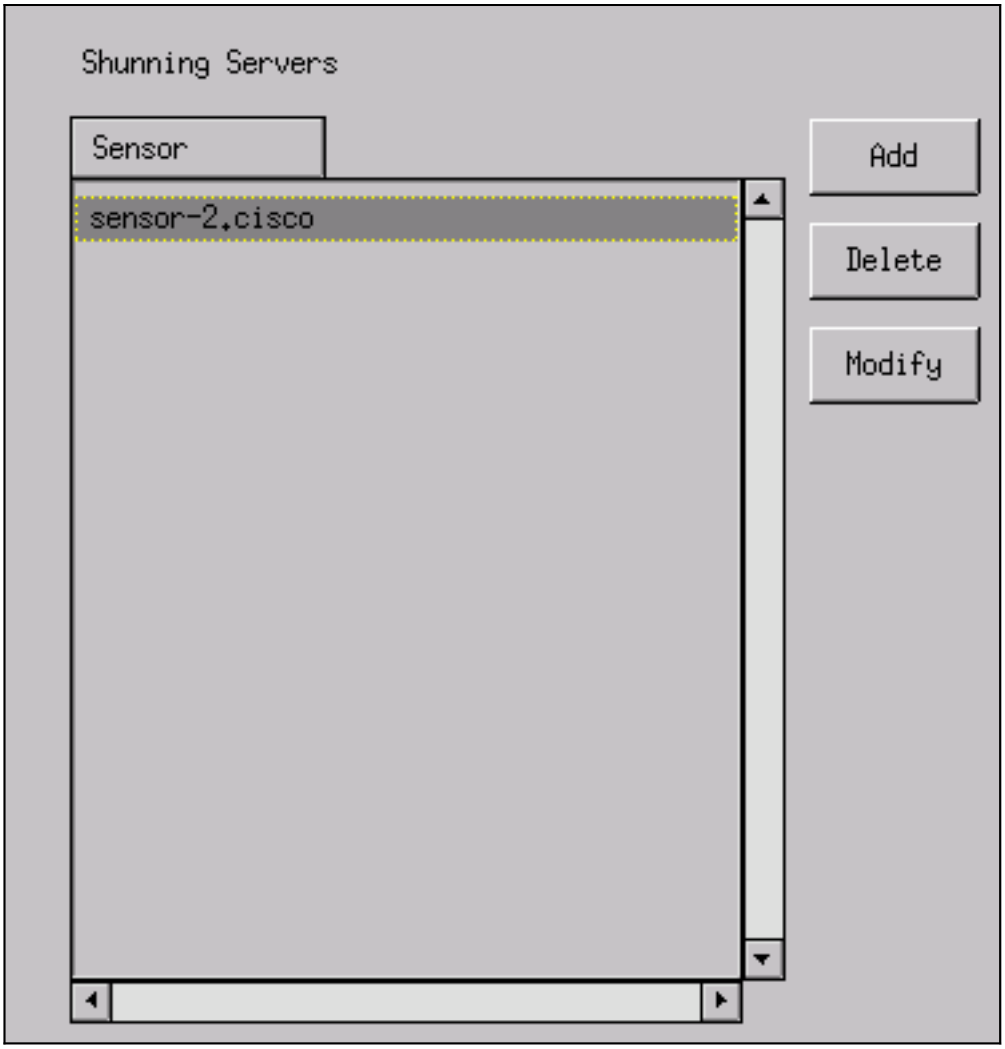
2. 在Netranger Configuration Menu中，選中**sensor-2**並按兩下它。
3. 開啟**Device Management**。
4. 按一下「**Devices**」>「**Add**」，然後輸入以下範例中所示的資訊。按一下「**OK**」以繼續。Telnet和啟用密碼均為「Cisco」。



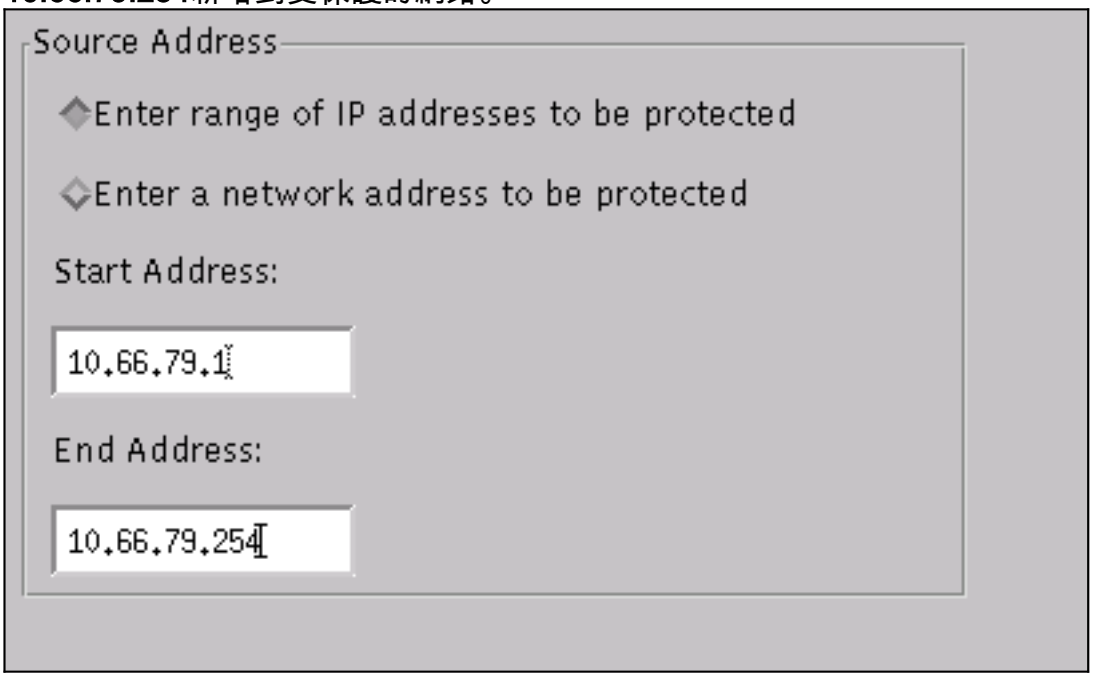
5. 按一下「**Shunning**」>「**Add**」。在「Addresses Never to Shun」下新增主機**100.100.100.100**。 按一下「**OK**」以繼續。



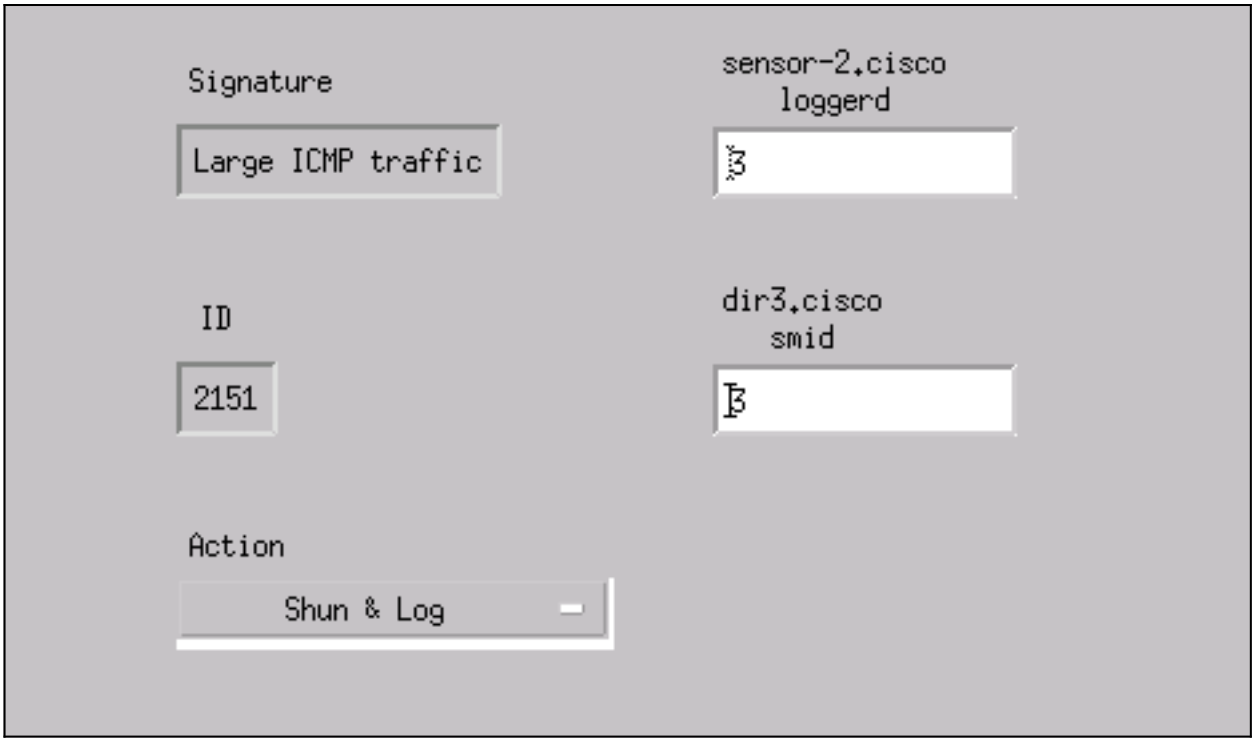
6. 按一下**Shunning > Add**，然後選擇**sensor-2.cisco**作為迴避伺服器。此部分配置已完成。關閉「Device Management（裝置管理）」視窗。



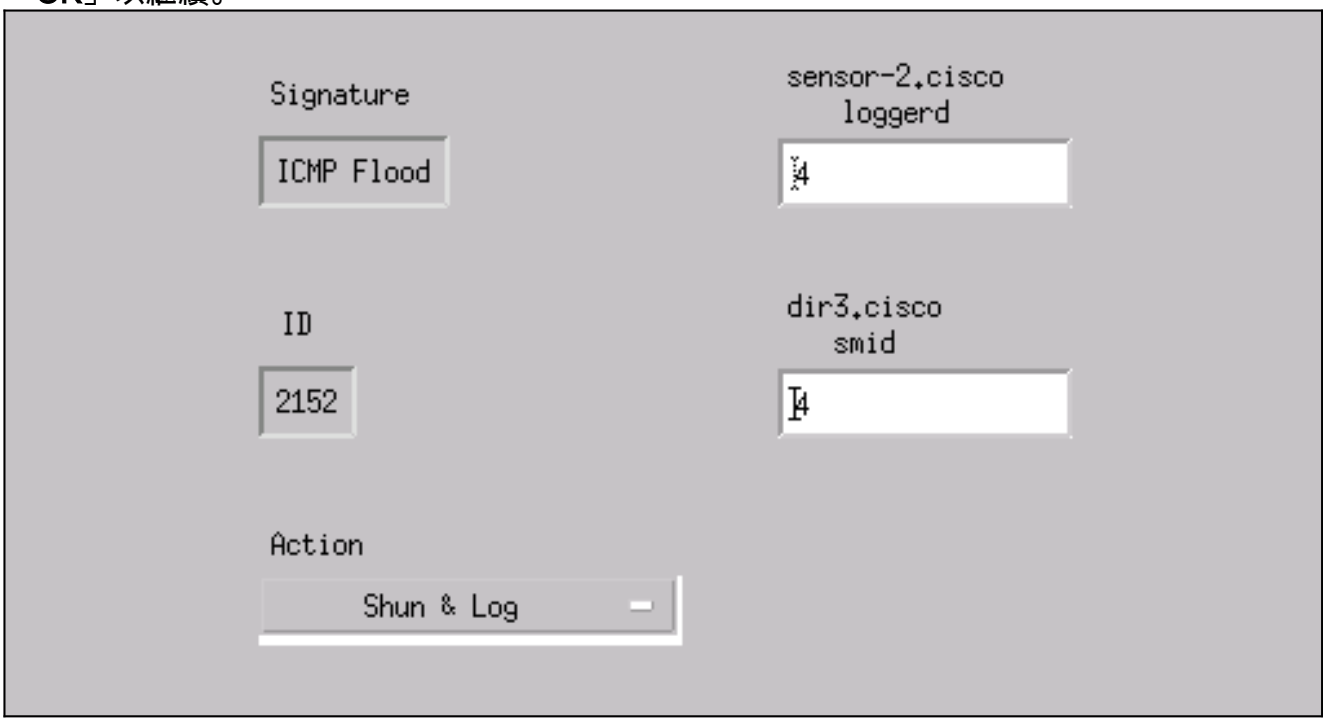
7. 開啟Intrusion Detection視窗，然後按一下**Protected Networks**。將**10.66.79.1**到**10.66.79.254**新增到受保護的網路。



8. 按一下「**Profile**」，然後選擇「**Manual Configuration**」>「**Modify Signatures**」。選擇**Large ICMP Traffic**和**ID:2151**，按一下**Modify**，並將Action從None更改為**Shun and Log**。按一下「**OK**」以繼續。

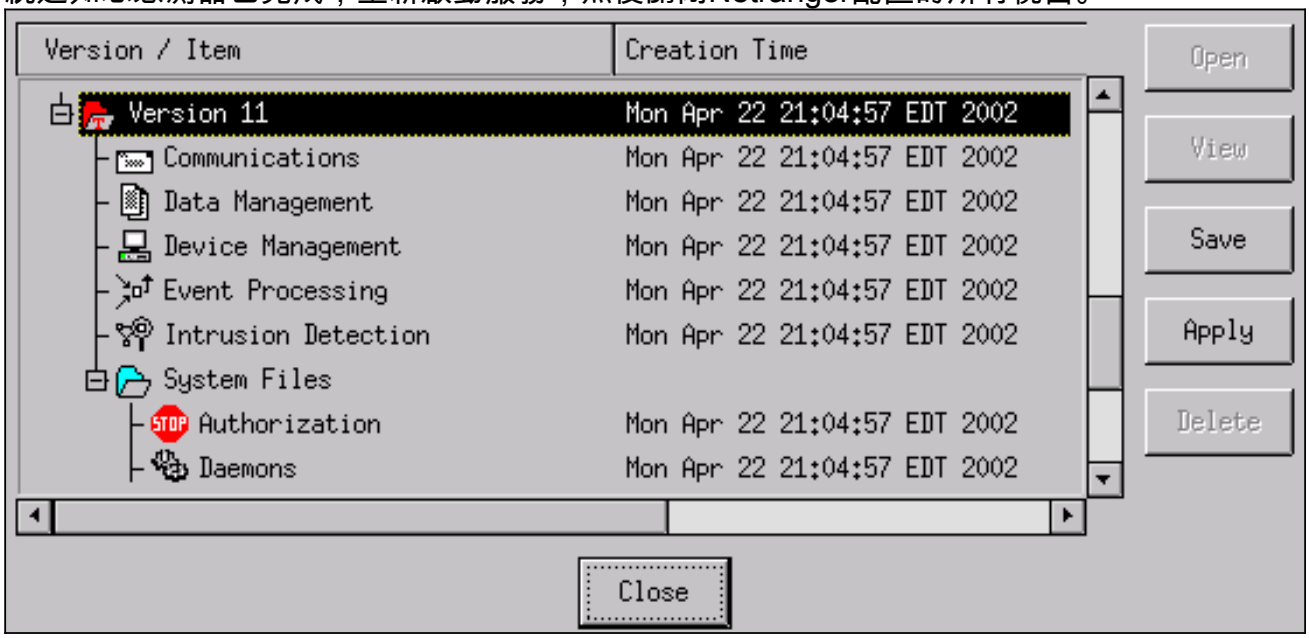


9. 選擇**ICMP Flood**和**ID:2152**，按一下**Modify**，並將Action從**None更改為Shun and Log**。按一下「**OK**」以繼續。



10. 此部分配置已完成。按一下**OK**以關閉Intrusion Detection視窗。
11. 開啟**System Files資料夾**並開啟**Daemons**視窗。確保已啟用以下守護程式：

12. 按一下「OK」以繼續，然後選擇您剛才修改的版本。按一下「Save」>「Apply」。等待系統通知您感測器已完成，重新啟動服務，然後關閉Netranger配置的所有視窗。



驗證

本節提供的資訊可協助您確認組態是否正常運作。

攻擊前

```
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
```

發動攻擊和迴避

```
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分鐘後，回撥至正常狀態，因為回撥時間設定為15分鐘。

```
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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco IDS Director銷售終止
- Cisco IDS感應器軟體版本3.x的壽命終止
- 思科入侵防禦系統產品支援
- Cisco PIX防火牆軟體產品支援
- Cisco Secure PIX防火牆命令參考
- 技術支援與文件 - Cisco Systems