# Cisco IDS UNIX مدير مادختساب IDS PIX لهاجت

## المحتويات



## المقدمة

يصف هذا وثيقة كيف أن يشكل تجاهل على PIX بمساعدة من cisco IDS UNIX مدير (المعروف سابقا ب Netranger Director) ومستشعر. يفترض هذا وثيقة أن المستشعر والمدير يكون عمليان وال ينشق قارن من المستشعر setup أن يجسر إلى ال PIX خارجي قارن.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية.

- مدير Cisco IDS UNIX 2.2.3
- مستشعر Cisco IDS UNIX 3.0.5
- Cisco Secure PIX مع 6.1.1**ملاحظة:** إذا كنت تستخدم إصدار x.6.2، فيمكنك إستخدام إدارة بروتوكول طبقة الأمان (SSH)، ولكن ليس برنامج Telnet. راجع معرف تصحيح الأخطاء من Cisco CSCdx55215 (العملاء المسجلون فقط) للحصول على مزيد من المعلومات.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

# التكوين

في هذا القسم، تقدم لك المعلومات المستخدمة لتكوين الميزات الموضحة في هذا المستند.

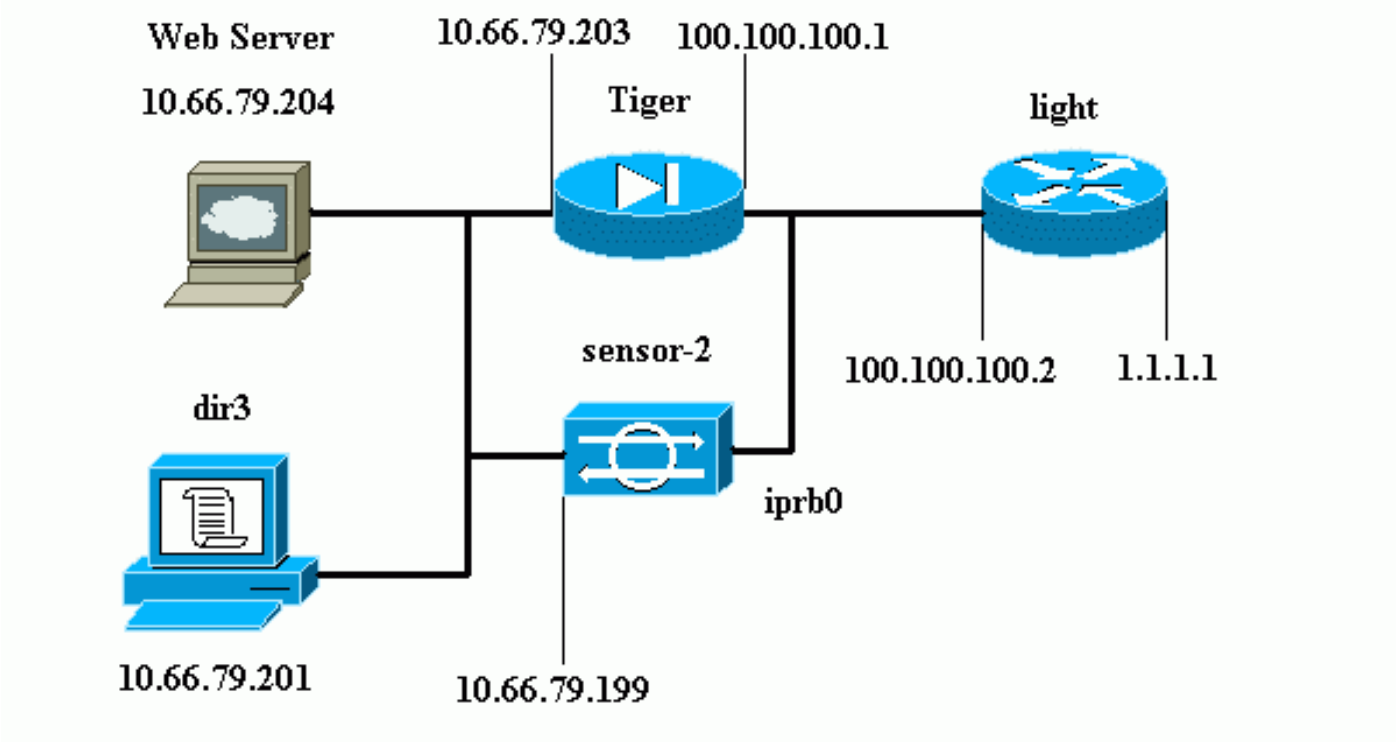
يتم إستخدام مستشعر ومدير Cisco IDS UNIX لإدارة PIX آمن من Cisco للتهرب. عند مراعاة هذا التكوين، تذكر المفاهيم التالية:

- قم بتثبيت "أداة الاستشعار" وتأكد من عمل أداة الاستشعار بشكل صحيح.
- ضمنت أن ال ينشق قارن إلى القارن خارجي من ال PIX.

**ملاحظة:** للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، ارجع إلى أداة بحث الأوامر (للعملاء المسجلين فقط).

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي.




## التكوينات

يستخدم هذا المستند هذه التكوينات.

- ضوء الموجه
- نمر PIX

**ضوء الموجه**

```
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
```

## نمر PIX

```
(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 :
```

## تكوين جهاز الاستشعار

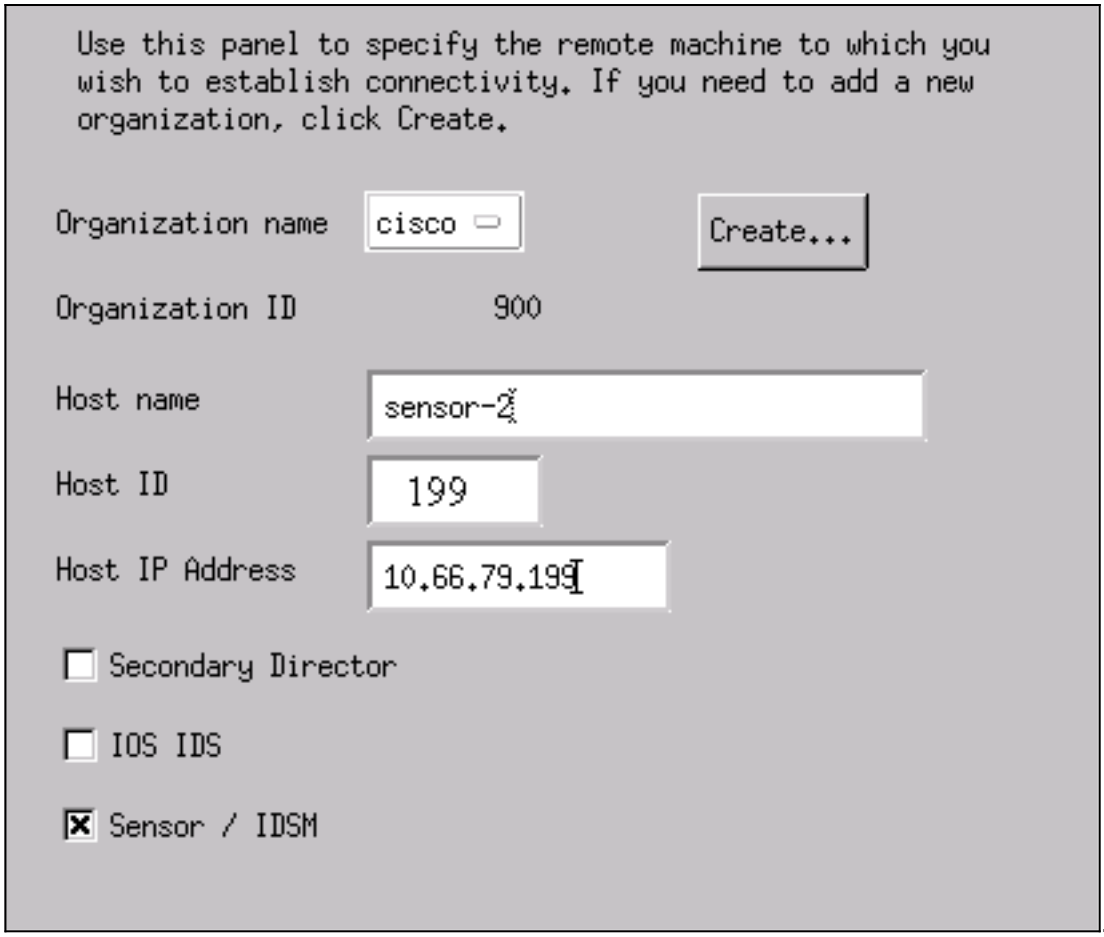
تصف هذه الخطوات كيفية تكوين المستشعر.

1. Telnet إلى **10.66.79.199** باسم المستخدم **الجذر** والهجوم **بكلمة المرور**.
2. أدخل **sysconfig-sensor**.
3. أدخل هذه المعلومات:عنوان IP: **10.66.79.199**قناع شبكة IP: **255.255.255.224**اسم مضيف IP: **المستشعر-2**المسار الافتراضي: **10.66.79.193**التحكم في الوصول إلى الشبكة**10.**البنية الأساسية للإتصالاتمعرف مضيف المستشعر: **49**معرف مؤسسة المستشعر: **900**اسم مضيف المستشعر: **المستشعر-2**اسم مؤسسة المستشعر: **Cisco**عنوان IP للمستشعر: **10.66.79.199**معرف مضيف مدير **50** :IDSمعرف مؤسسة مدير **900** :IDSاسم مضيف مدير **dir3** :IDSاسم مؤسسة مدير **Cisco** :IDSعنوان IP لمدير IDS: **10.66.79.201**
4. قم بحفظ التكوين. ثم يقوم المستشعر بإعادة التشغيل.

## إضافة المستشعر إلى المدير

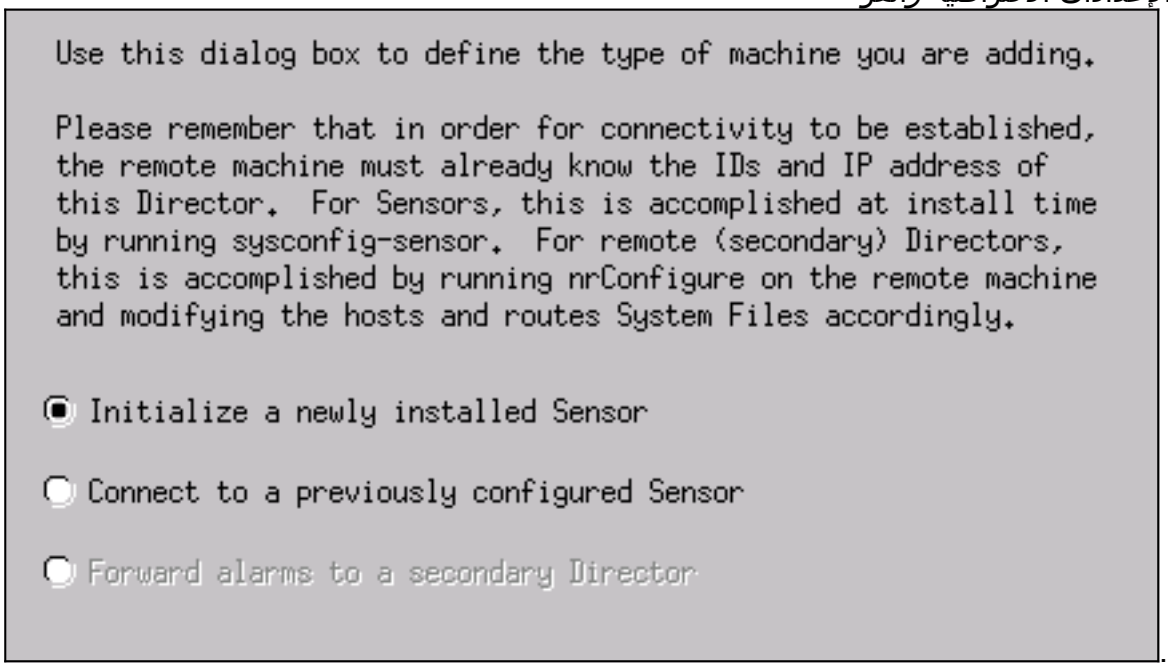
أتمت هذا steps in order to أضفت المستشعر داخل المدير.

1. Telnet إلى **10.66.79.201** باسم المستخدم **netrangr** والهجوم **بكلمة المرور**.
2. أدخل **البيانات&** لبدء تشغيل برنامج OpenView من HP.
3. في القائمة الرئيسية، حدد **تأمين > تكوين**.
4. في قائمة تكوين الشبكة، حدد **ملف > إضافة مضيف**، ثم انقر فوق **التالي**.
5. دخلت هذا معلومة، وطقطقة **بعد**



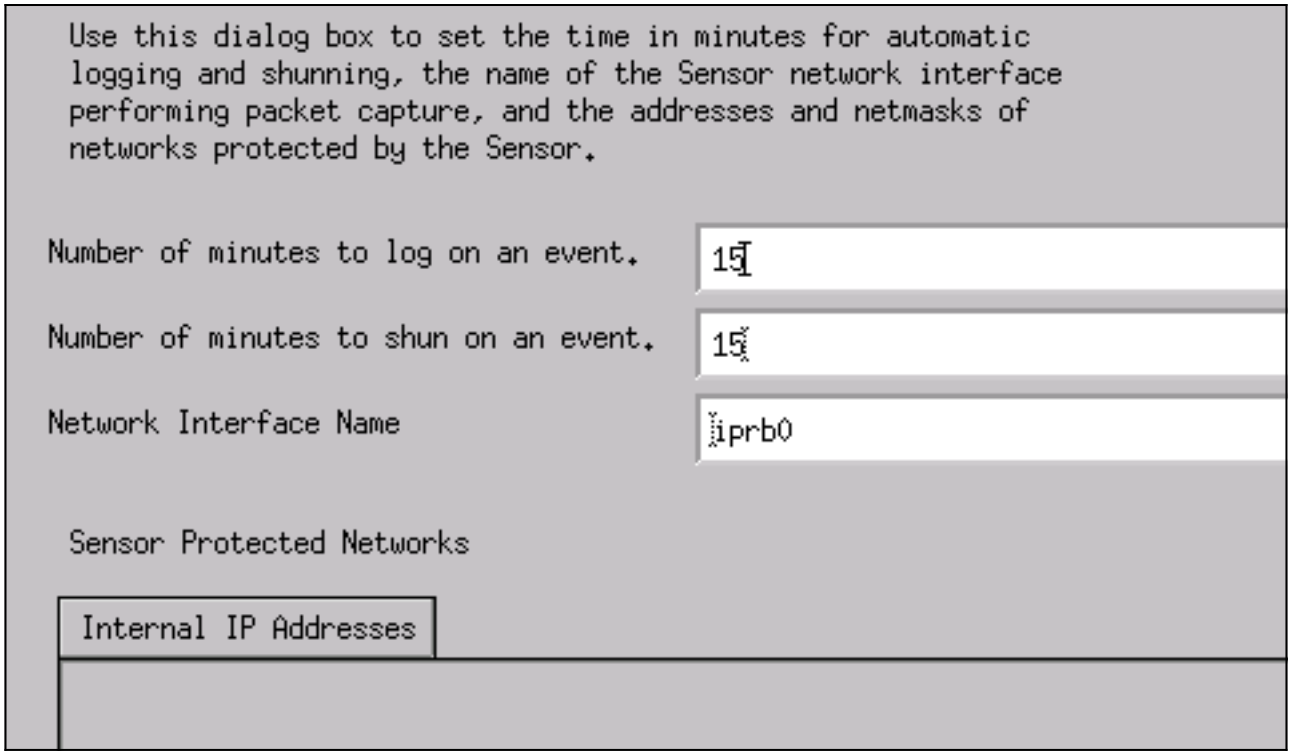

**ذلك**.

6. أترك الإعدادات الافتراضية وانقر

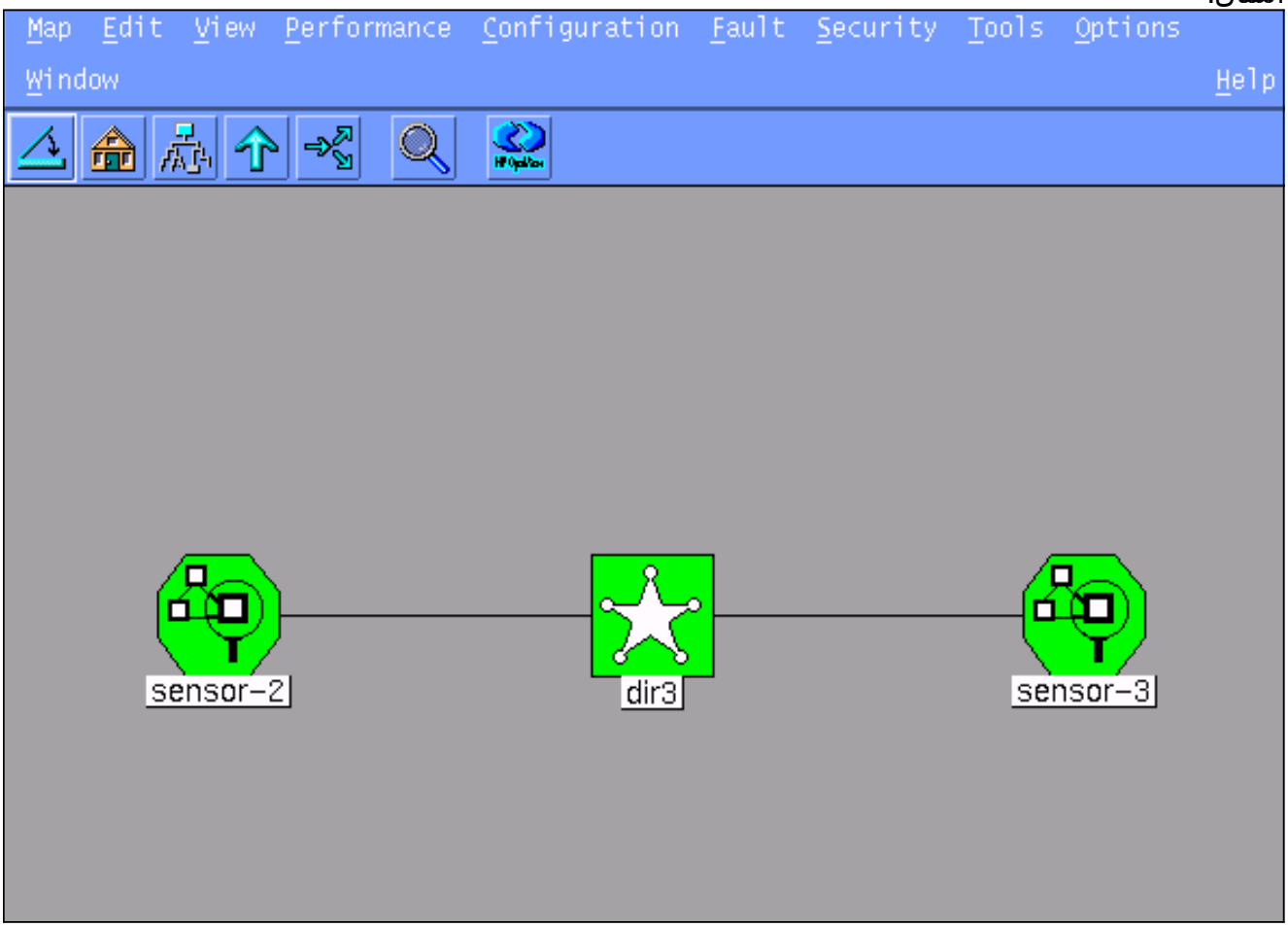



**التالي**.

7. قم بتغيير السجل وإبطال الدقائق أو تركها كقيمة افتراضية إذا كانت القيم مقبولة. غيرت الشبكة قارن إسم إلى الاسم من ك sniffing قارن. في هذا المثال، ستكون "iprb0". يمكن أن يكون "spwr0" أو أي شيء آخر بناء على نوع المستشعر وكيفية توصيلك بالمستشعر.



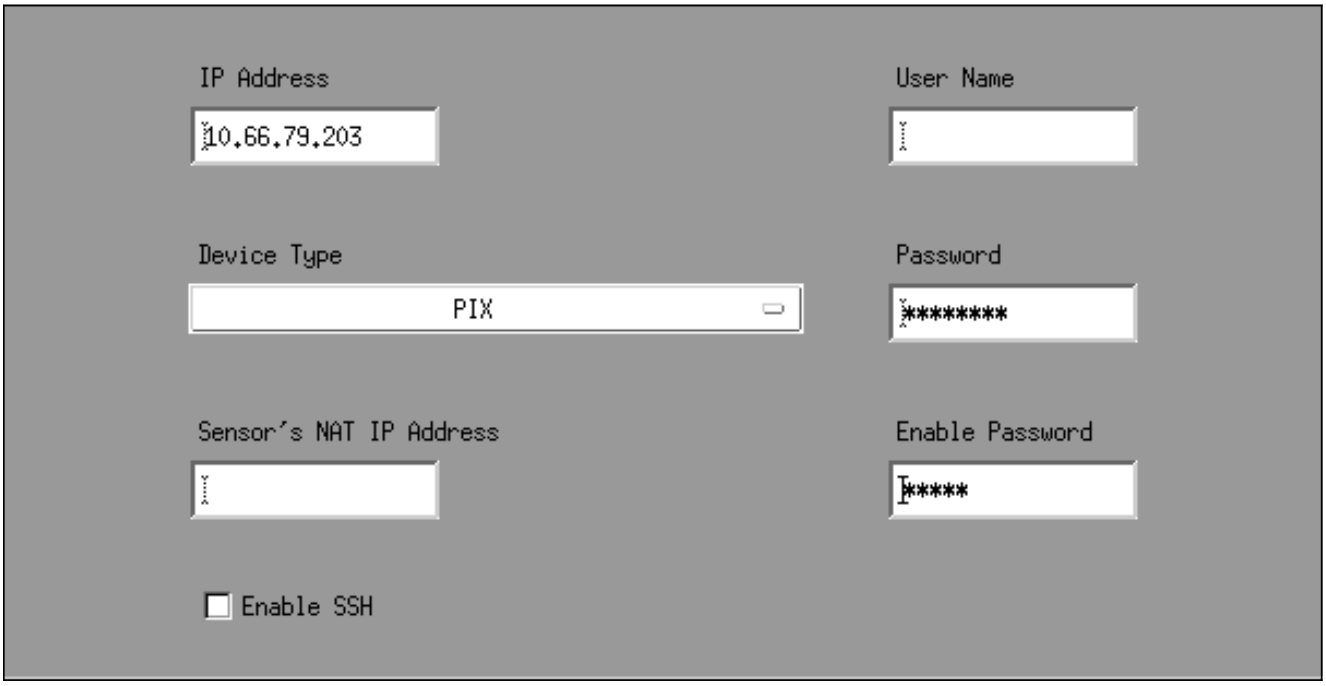

8. طقطقت **بعد ذلك** إلى أن هناك خيار أن يطقطق **إنجاز**.تمت الآن إضافة المستشعر بنجاح إلى المدير. من القائمة الرئيسية، يتم عرض **أداة الاستشعار - 2**، كما هو موضح في هذا المثال.



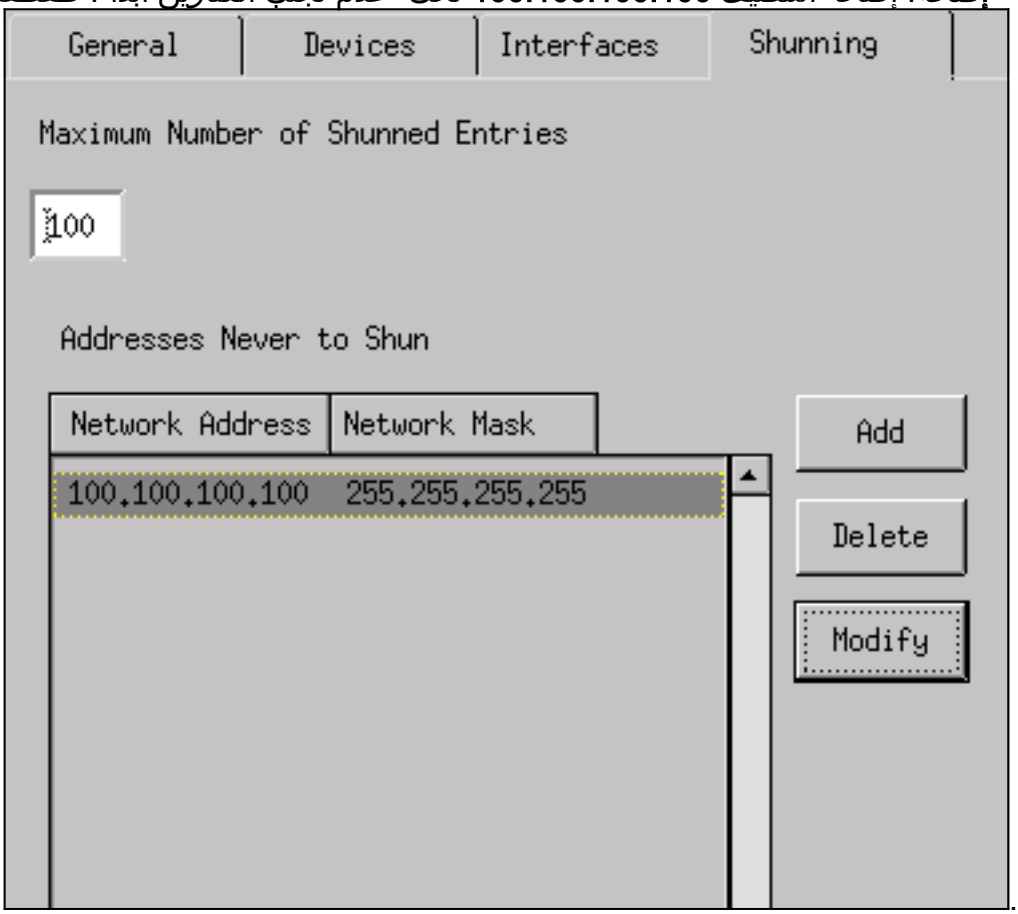

## تكوين التجنب ل PIX

أتمت هذا steps in order to شكلت تجنب ل PIX.

1. في القائمة الرئيسية، حدد **تأمين > تكوين**.
2. في قائمة تكوين الشبكة، قم بإبراز **المستشعر-2** وانقر فوقه نقرا مزدوجا.
3. فتح **إدارة الأجهزة**.
4. انقر فوق **الأجهزة > إضافة** وأدخل المعلومات كما هو موضح في هذا المثال. طقطقة ok in order to تابعت. ال telnet و enable كلمة على حد سواء "cisco".

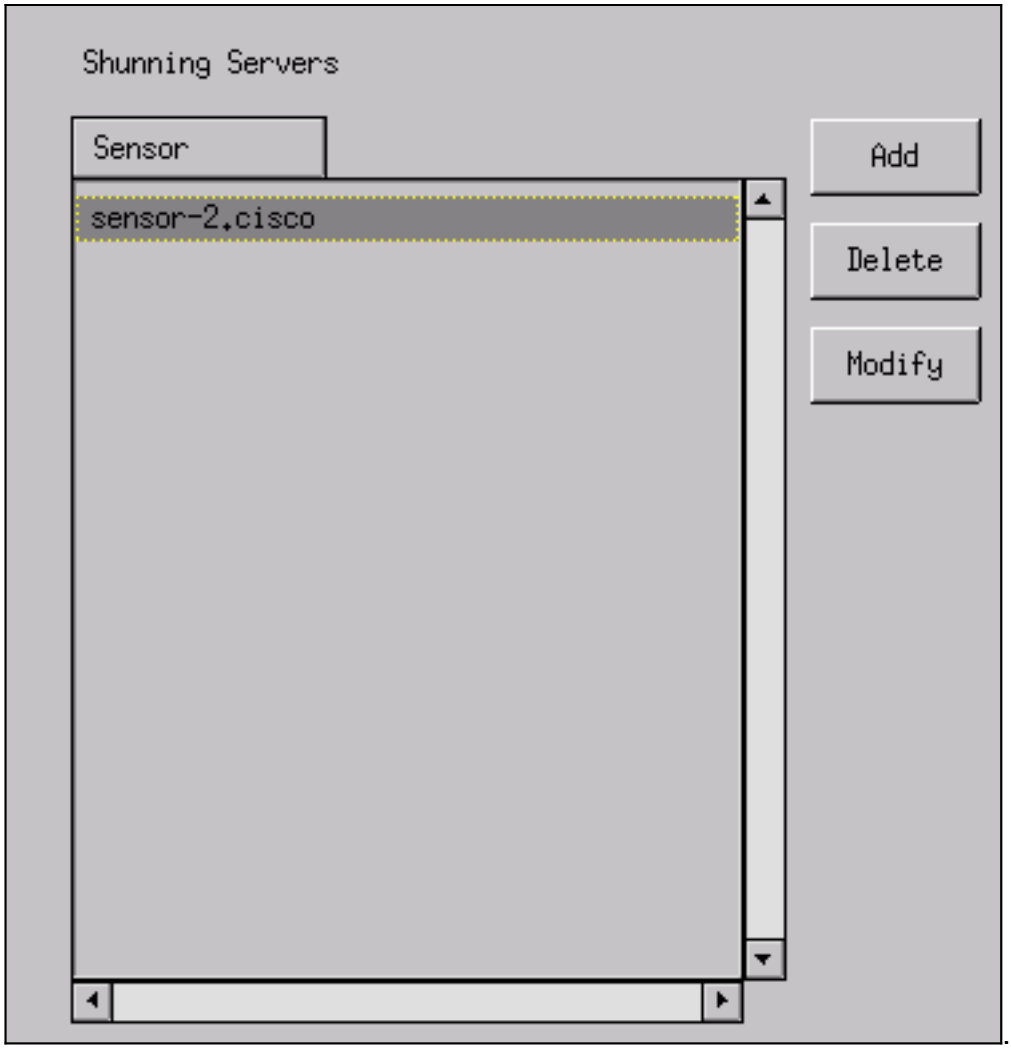



5. انقر فوق **تجنب > إضافة**. إضافة المضيف **100.100.100.100** تحت "عدم تجنب العناوين أبدا". طقطقة ok in



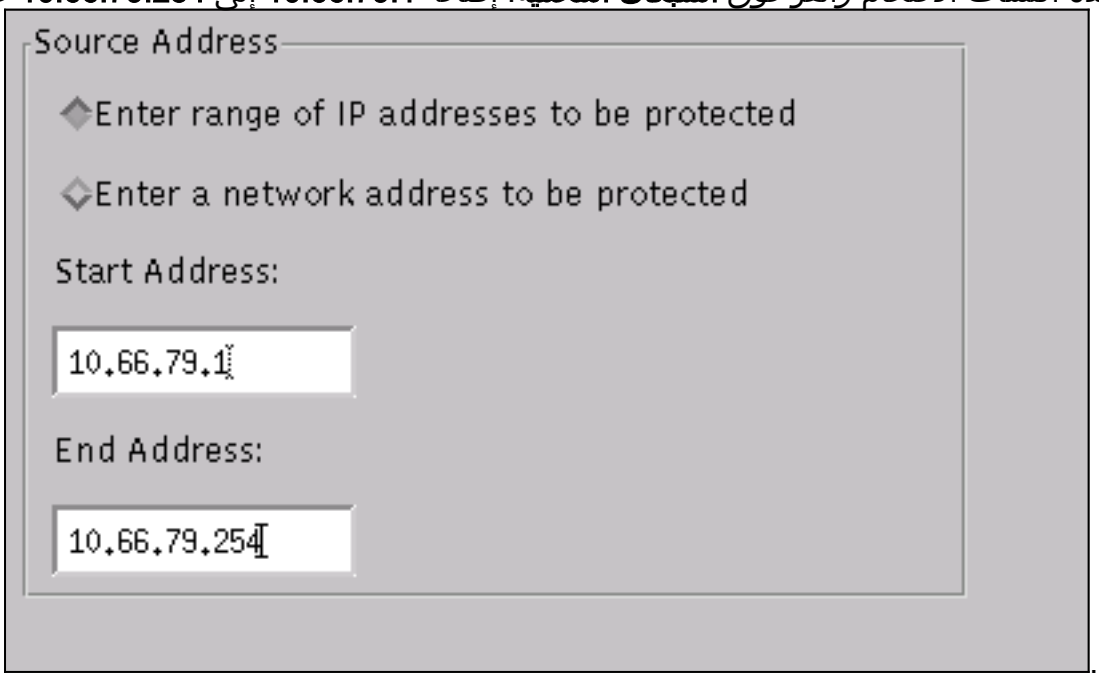

order to تابعت.

6. انقر فوق **تجنب > إضافة** وحدد **مستشعر-cisco.2** كخوادم تجنب. اكتمل هذا الجزء من التكوين. إغلاق إطار



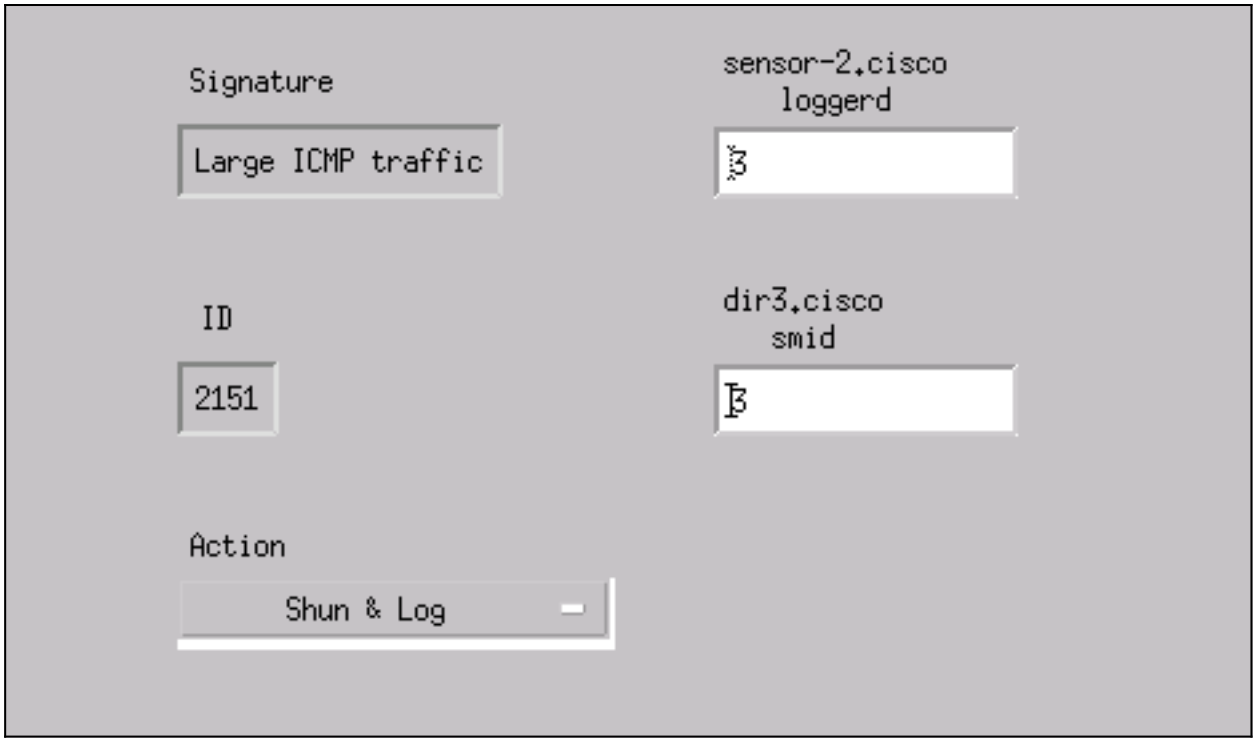

إدارة الأجهزة.

7. افتح نافذة اكتشاف الاقتحام وانقر فوق **الشبكات المحمية**. إضافة **10.66.79.1** إلى **10.66.79.254** في الشبكة

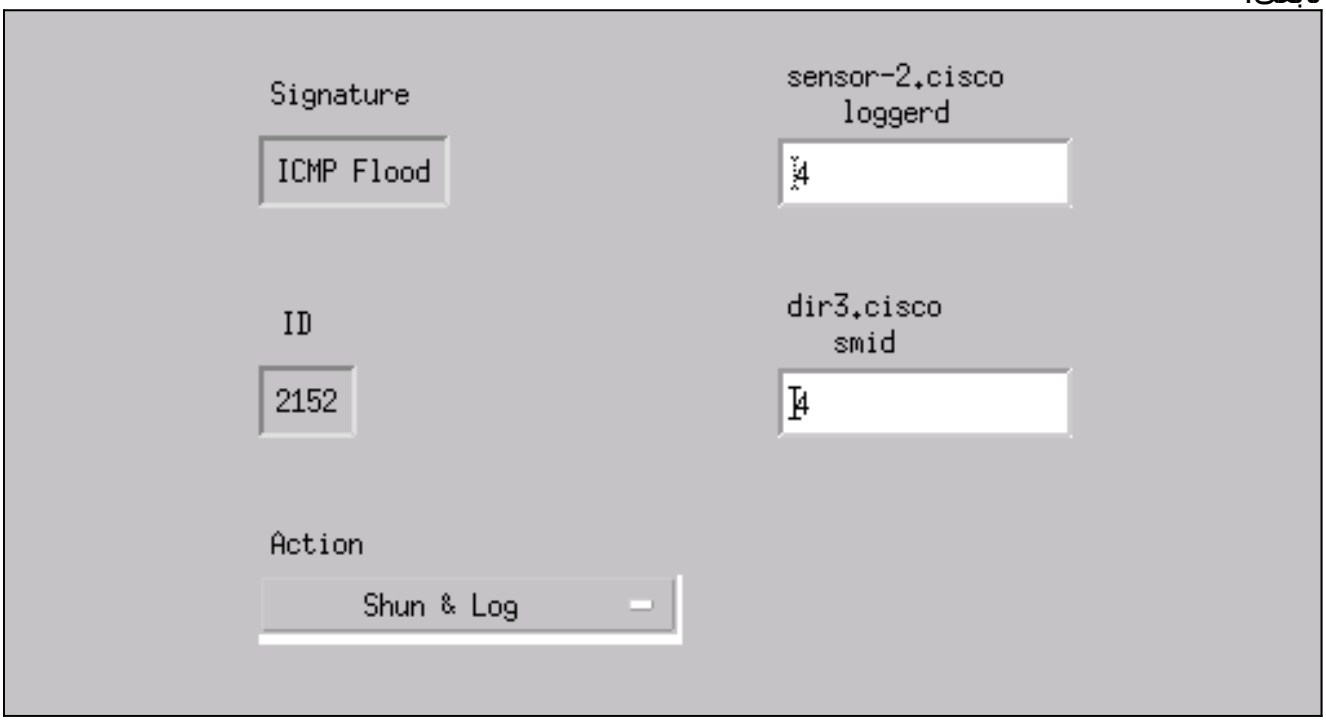



المحمية.

8. انقر **ملف تخصيص** وحدد **تشكيل يدوي** > **تعديل التوقيعات**. حدد **حركة مرور ICMP الكبيرة** و**المعرف: 2151**، انقر فوق **تعديل**، وقم بتغيير الإجراء من لا شيء إلى **تفريغ وتسجيل**. طقطقة ok in order to تابعت.

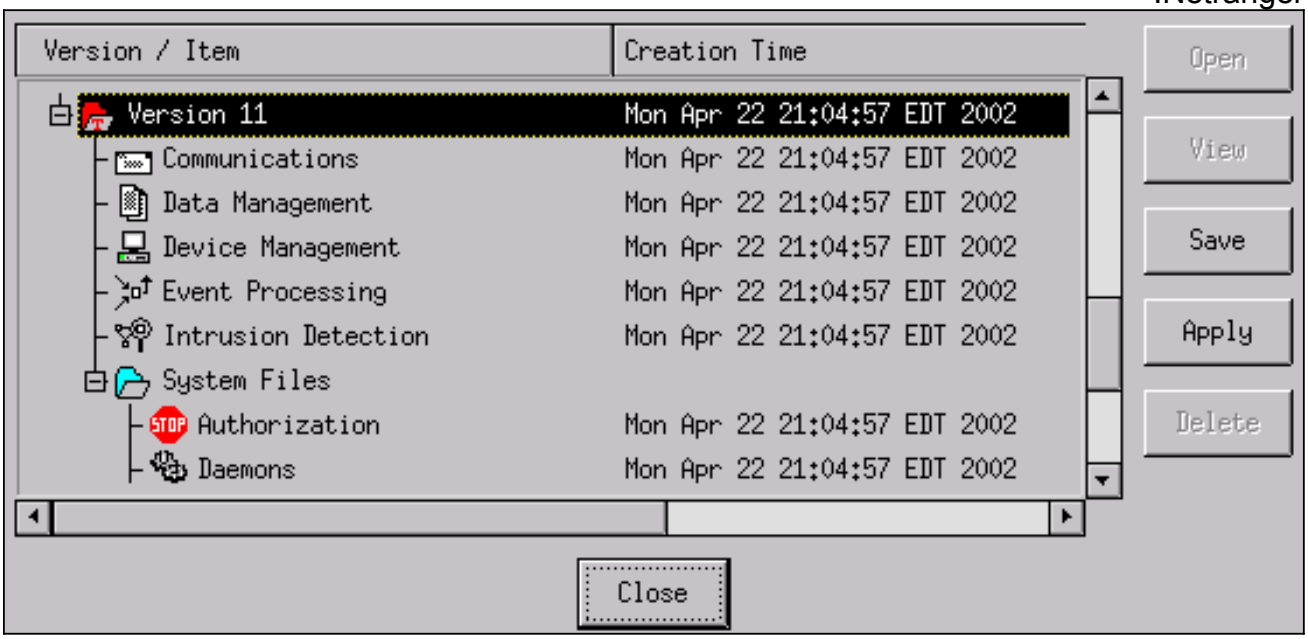



9. حدد طوفان ICMP و**المعرف: 2152**، انقر فوق **تعديل**، وقم بتغيير الإجراء من **none** إلى **التجاهل والسجل**. طقطقة in order to **ok**
تابعت.




10. هذا الجزء من التكوين مكتمل. طقطقة in order to **ok** أغلقت نافذة كشف التسلل.
11. افتح مجلد **ملفات النظام** وافتح نافذة **برنامج التشغيل**. تأكد من تمكين هذه
الأجهزة:


12. انقر فوق **موافق** للمتابعة، وحدد الإصدار الذي قمت بتعديله للتو. انقر فوق **حفظ** > **تطبيق**. انتظر حتى يخبرك النظام عن انتهاء أداة الاستشعار، ثم أعد تشغيل "الخدمات"، وأغلق كافة النوافذ لتكوين Netranger.




## التحقق من الصحة

يوفر هذا القسم معلومات تساعدك على تأكيد عمل التكوين بشكل صحيح.

### قبل أن تشن الهجوم

```
Tiger(config)# show telnet
inside 255.255.255.255 10.66.79.199
Tiger(config)# who
10.66.79.199 :0

Tiger(config)# show xlate
in use, 1 most used 1
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
```

## شن الهجوم و التجنب

```
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
```

بعد 15 دقيقة، ترجع إلى الحالة الطبيعية لأن التجنب مضبوط على 15 دقيقة.

```
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
```

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## معلومات ذات صلة

- نهاية البيع لمدير معرفات Cisco
- نهاية العمر الافتراضي لبرنامج مستشعر نظام اكتشاف الاقتحام Cisco IDS، الإصدار x.3
- دعم منتجات نظام منع التسلل من Cisco
- دعم منتج برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).