إعداد التجنب على مدير UNIX

المحتويات

المقدمة

يمكن إستخدام مدير نظام اكتشاف الاقتحام (IDS) والمستشعر من Cisco لإدارة موجه Cisco للتجنب. في هذا المستند، يتم تكوين مستشعر (sensor-2) من أجل اكتشاف الهجمات على الموجه "المنزل" ومن أجل توصيل هذه المعلومات إلى المدير "dir3". وبمجرد تكوينها، يتم تشغيل هجوم (إختبار الاتصال بحجم أكبر من 1024 بايت، وهو التوقيع 2151، وطوفان بروتوكول رسائل التحكم في الإنترنت [ICMP]، وهو التوقيع 2152) من الموجه "Light". يقوم جهاز الاستشعار بالكشف عن الهجوم وإبلاغ ذلك إلى المدير. يتم تنزيل قائمة التحكم في الوصول (ACL) إلى الموجه لتجنب حركة المرور من المهاجم. على الذي يظهر، وعلى الضحية يتم عرض قائمة التحكم في الوصول (ACL) التي تم تنزيلها.

المتطلبات الأساسية

المتطلبات

قبل أن تحاول إجراء هذا التكوين، فتأكد من استيفاء المتطلبات التالية:

- قم بتثبيت "المستشعر" وتأكد من عمله بشكل صحيح.
- ضمنت أن ال ينشق قارن إلى المسحاج تخديد قارن خارجي.

المكونات المستخدمة

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

- مدير Cisco IDS 2.2.3
- مستشعر Cisco IDS 3.0.5

- موجه IOS® من Cisco مع 12.2.6

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.

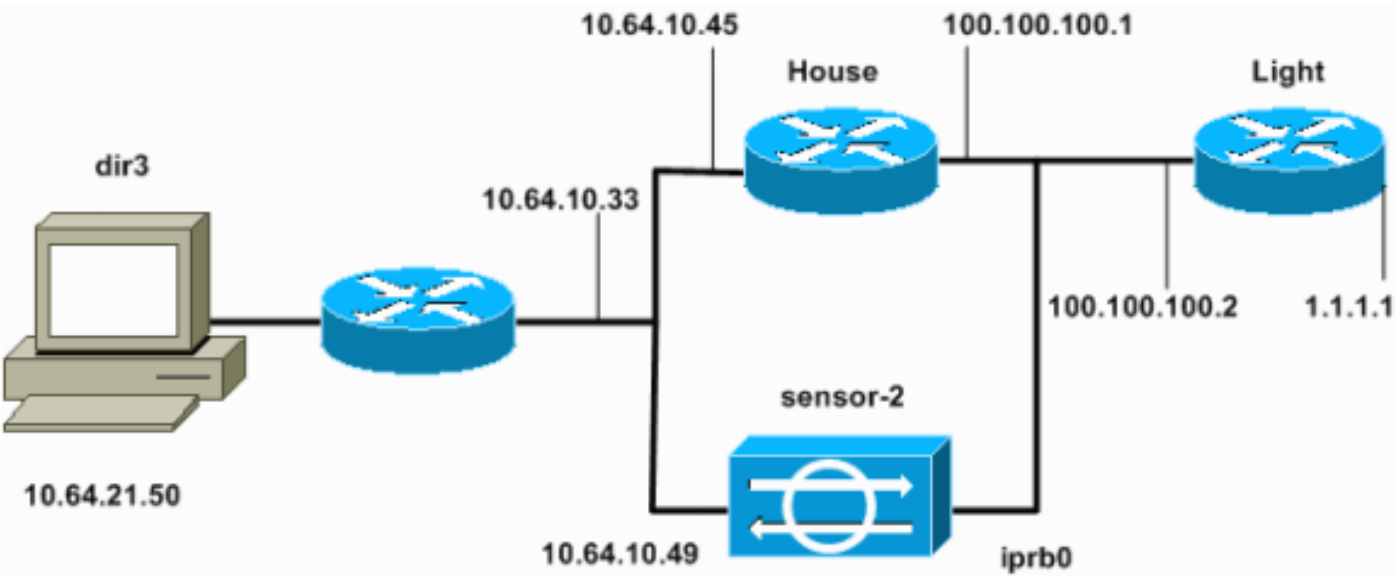
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



التكوينات

يستخدم هذا المستند هذه التكوينات.

- ضوء الموجه
- منزل الموجه

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
!
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
```

منزل الموجه

```
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
```

تكوين جهاز الاستشعار

أكمل الخطوات التالية لتكوين المستشعر.

1. Telnet إلى **10.64.10.49** باسم المستخدم **الجذر** والهجوم **بكلمة المرور**.
2. أدخل **sysconfig-sensor**.
3. أدخل معلومات التكوين، عند طلبها، كما هو موضح في هذا المثال.

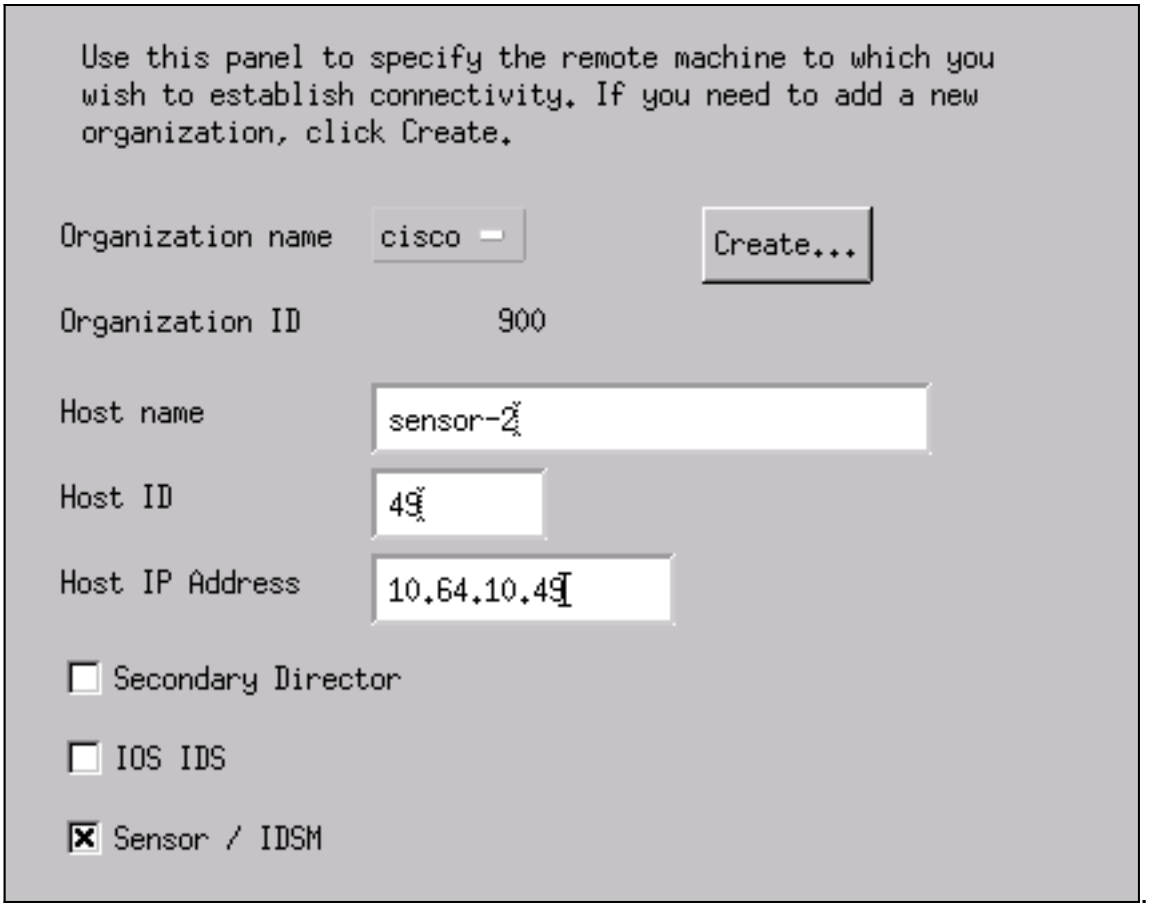
```
IP Address: 10.64.10.49 - 1
IP Netmask: 255.255.255.224 - 2
IP Host Name:  sensor-2 - 3
Default Route     10.64.10.33 - 4
Network Access Control - 5
.64
.10
Communications Infrastructure - 6
Sensor Host ID: 49
Sensor Organization ID:     900
Sensor Host Name: sensor-2
Sensor Organization Name:   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. عند المطالبة، قم بحفظ التكوين والسماح للمستشعر بإعادة التمهيد.

إضافة المستشعر إلى المدير

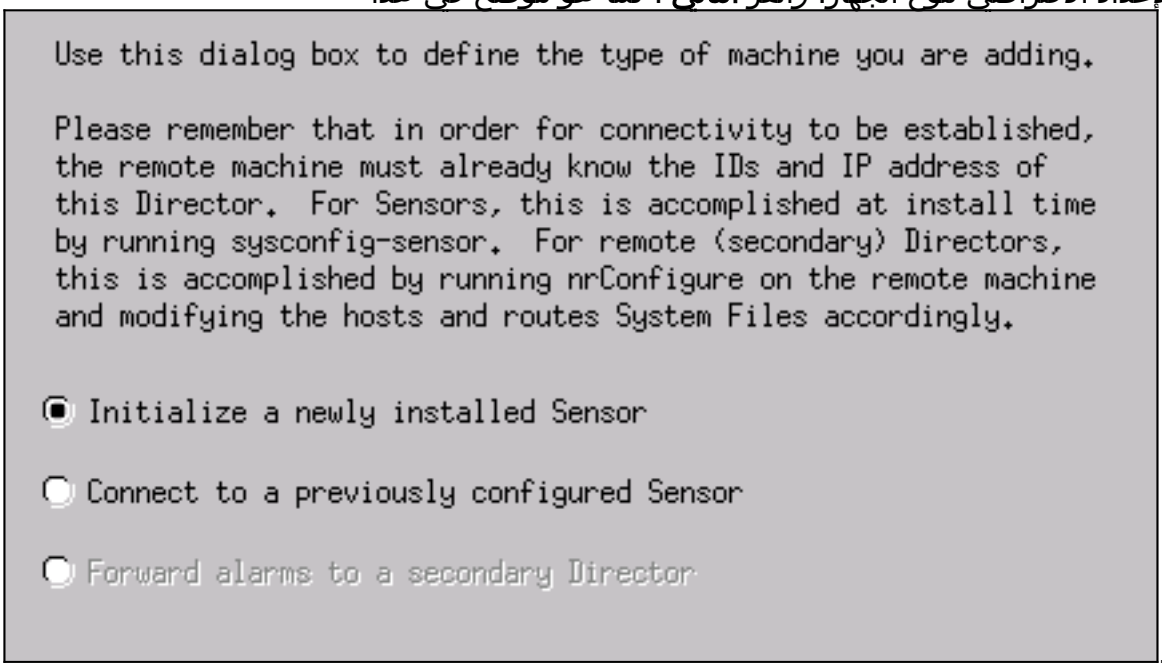
أتمت هذا steps أن يضيف المستشعر إلى المدير.

1. Telnet إلى **10.64.21.50** باسم المستخدم **netrangr** والهجوم **بكلمة المرور**.
2. أدخل **الفيديو** لتشغيل برنامج OpenView من HP.
3. في القائمة الرئيسية، حدد **تأمين > تكوين**.
4. في الأداة المساعدة لإدارة ملف التكوين، حدد **ملف > إضافة مضيف**، ثم انقر **بعد ذلك**.
5. هذا مثال على كيفية ملء المعلومات



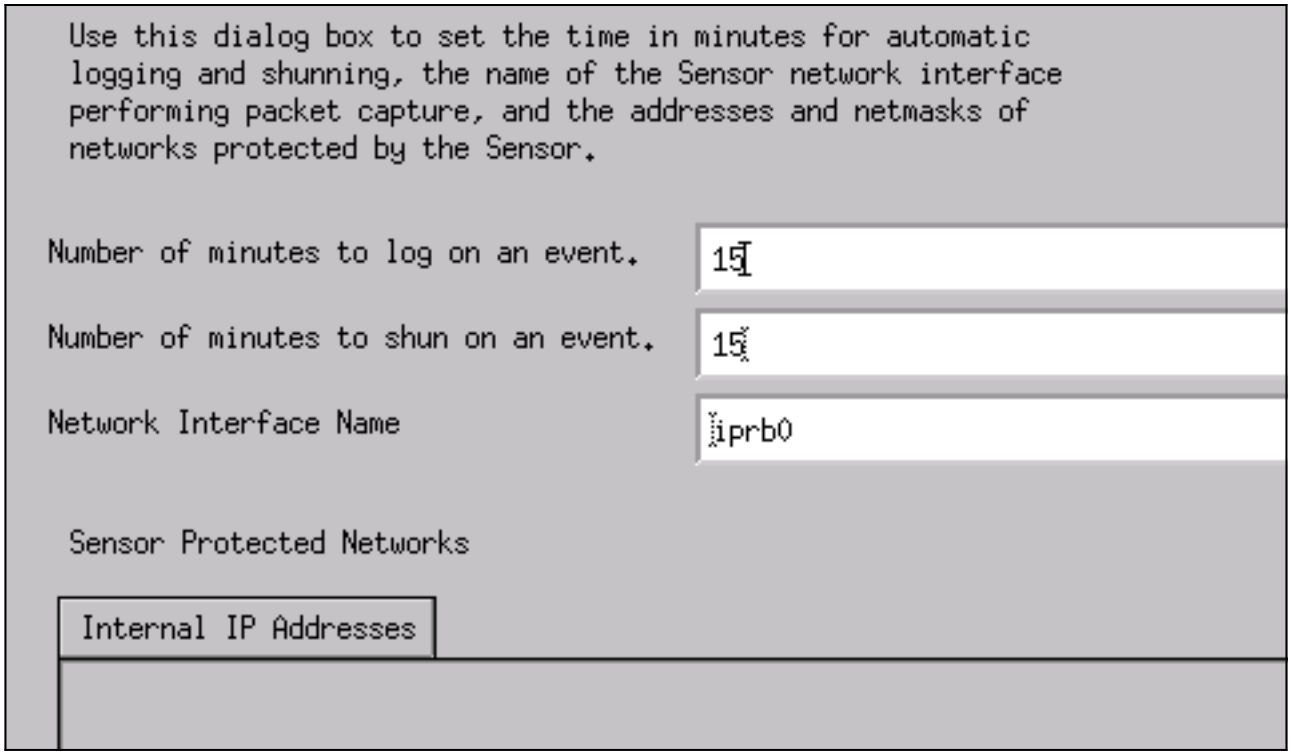
المطلوبة.

6. اقبل الإعداد الافتراضي لنوع الجهاز، وانقر **التالي** ، كما هو موضح في هذا

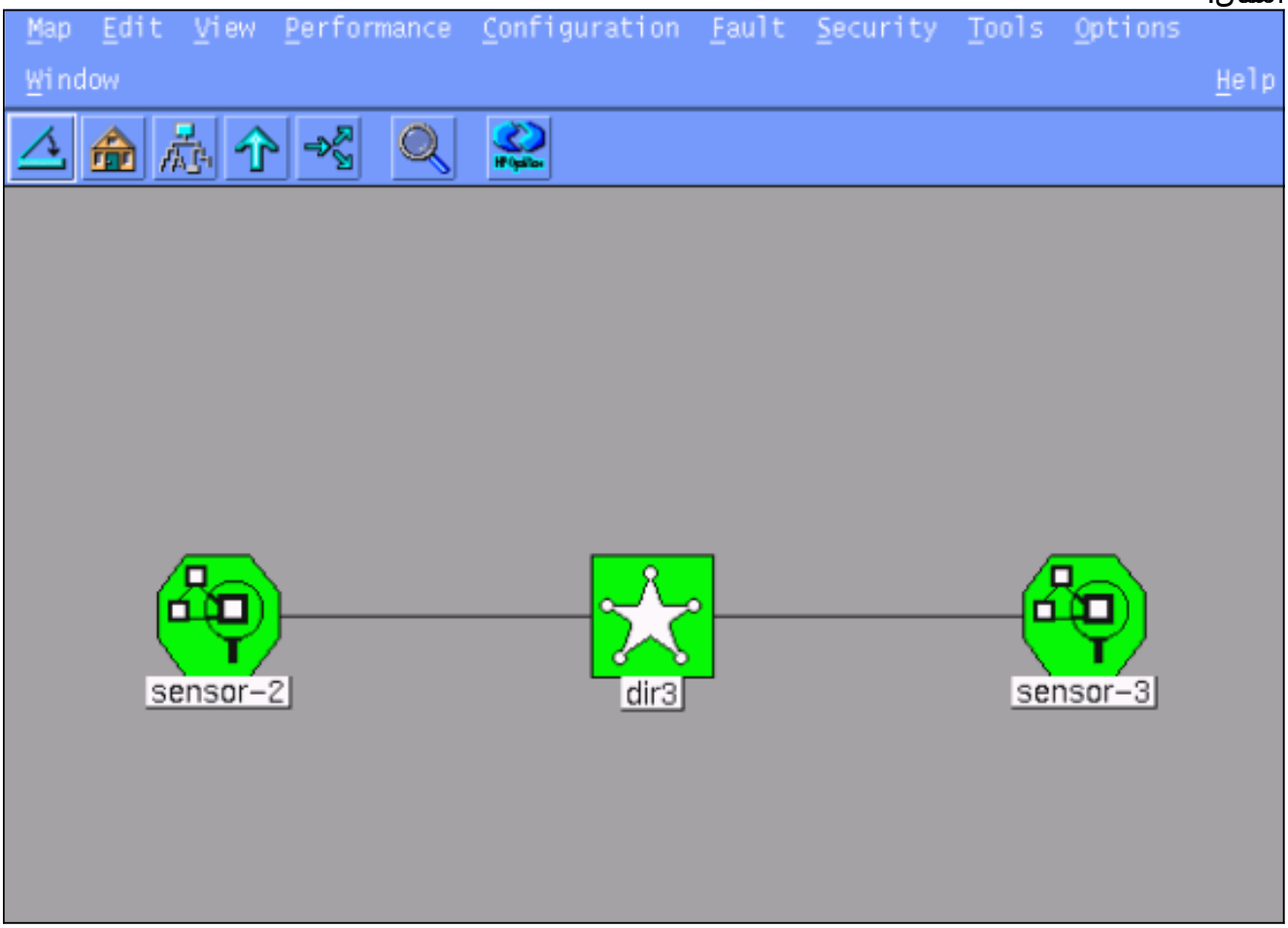


المثال.

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 حسب نوع المستشعر وكيفية توصيل المستشعر الخاص بك.



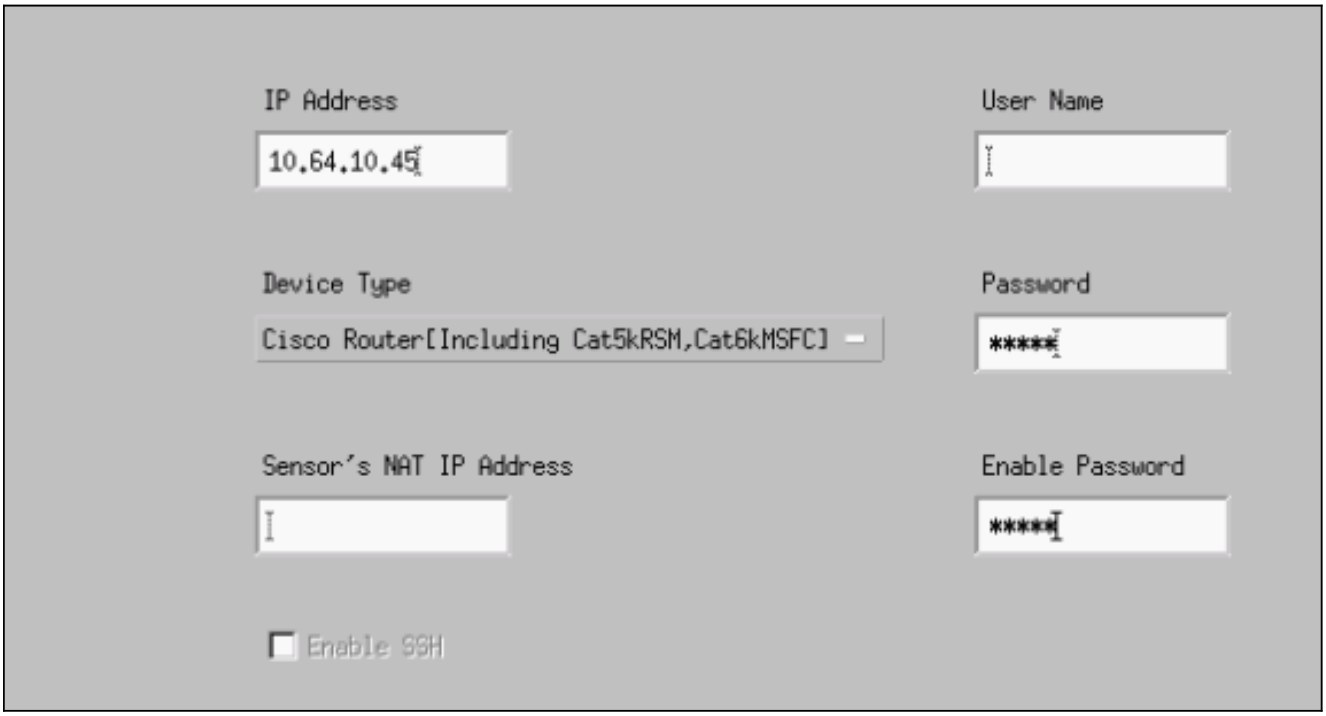
8. طقطقت **بعد ذلك** إلى أن هناك خيار أن يطقطق **إنجاز**.لقد أضفت المستشعر بنجاح إلى Director. من القائمة الرئيسية، يجب أن ترى -2، كما في هذا المثال.



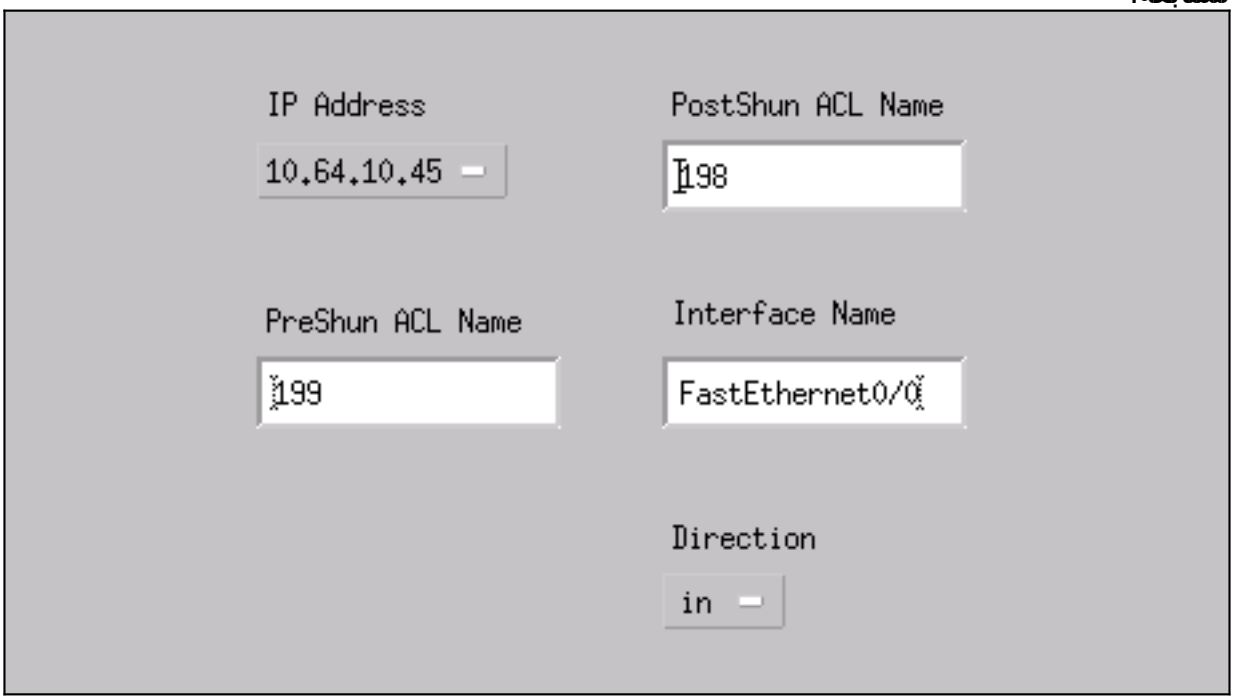
تكوين التجنب لموجه Cisco IOS

أكمل الخطوات التالية لتكوين التجنب لموجه Cisco IOS.

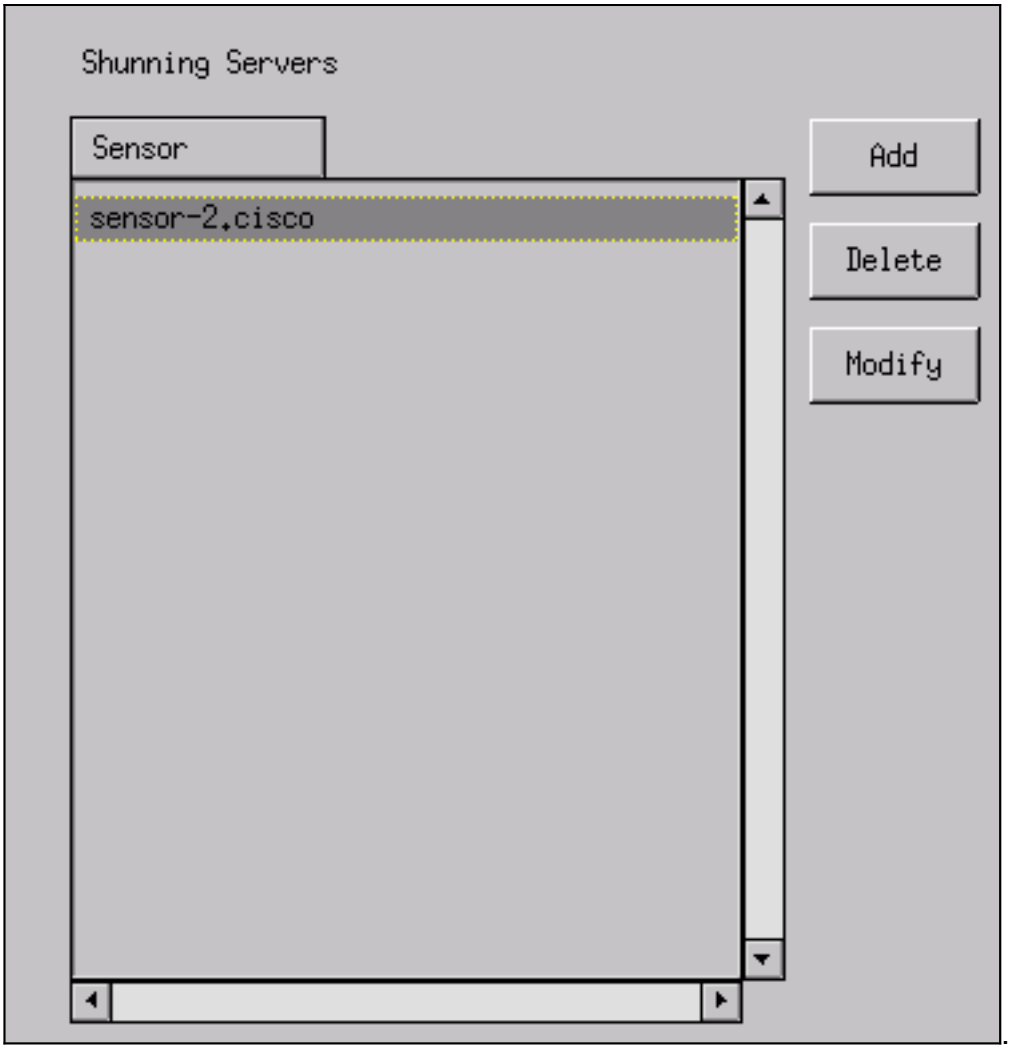
1. في القائمة الرئيسية، حدد **تأمين > تكوين**.
2. في الأداة المساعدة لإدارة ملف التكوين، قم بإبراز **المستشعر-2** وانقر فوقه نقرا مزدوجا.
3. فتح **إدارة الأجهزة**.
4. انقر فوق **أجهزة > إضافة**، وأدخل المعلومات كما هو موضح في هذا المثال. انقر فوق **موافق**" للمتابعة.تطابق كلمات مرور Telnet والتمكين ما هو في الموجه "Home".



5. انقر فوق **الواجهات > إضافة**، وأدخل هذه المعلومات، وانقر فوق **موافق** للمتابعة.

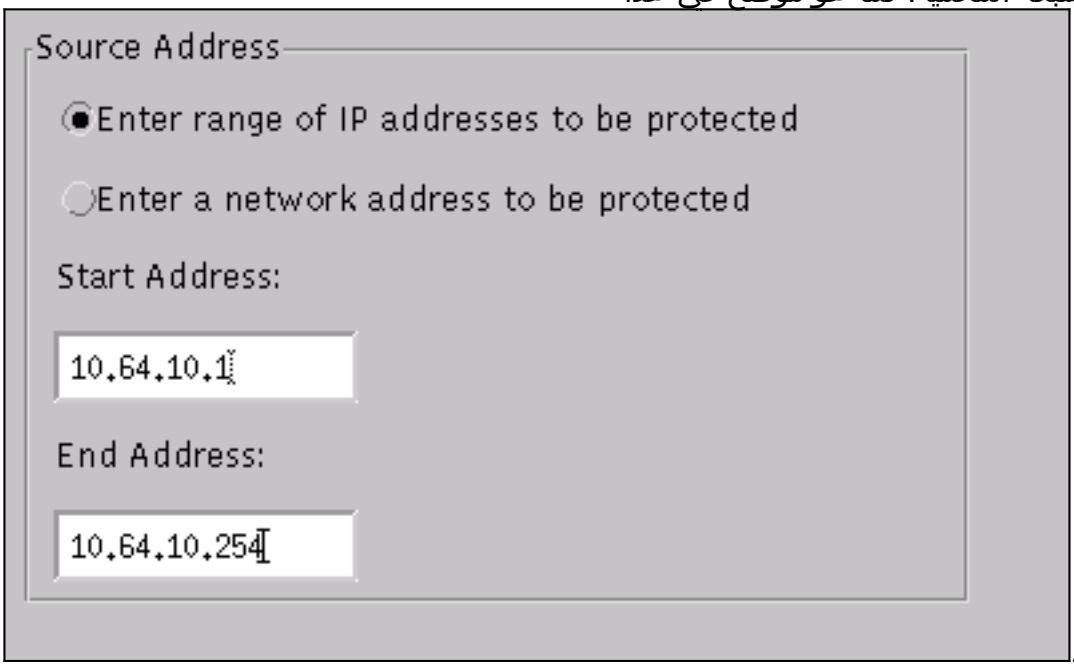


6. انقر فوق **تجنب > إضافة** وحدد **مستشعر-cisco.2** كخادم تجنب. قم بإغلاق إطار إدارة الأجهزة عند



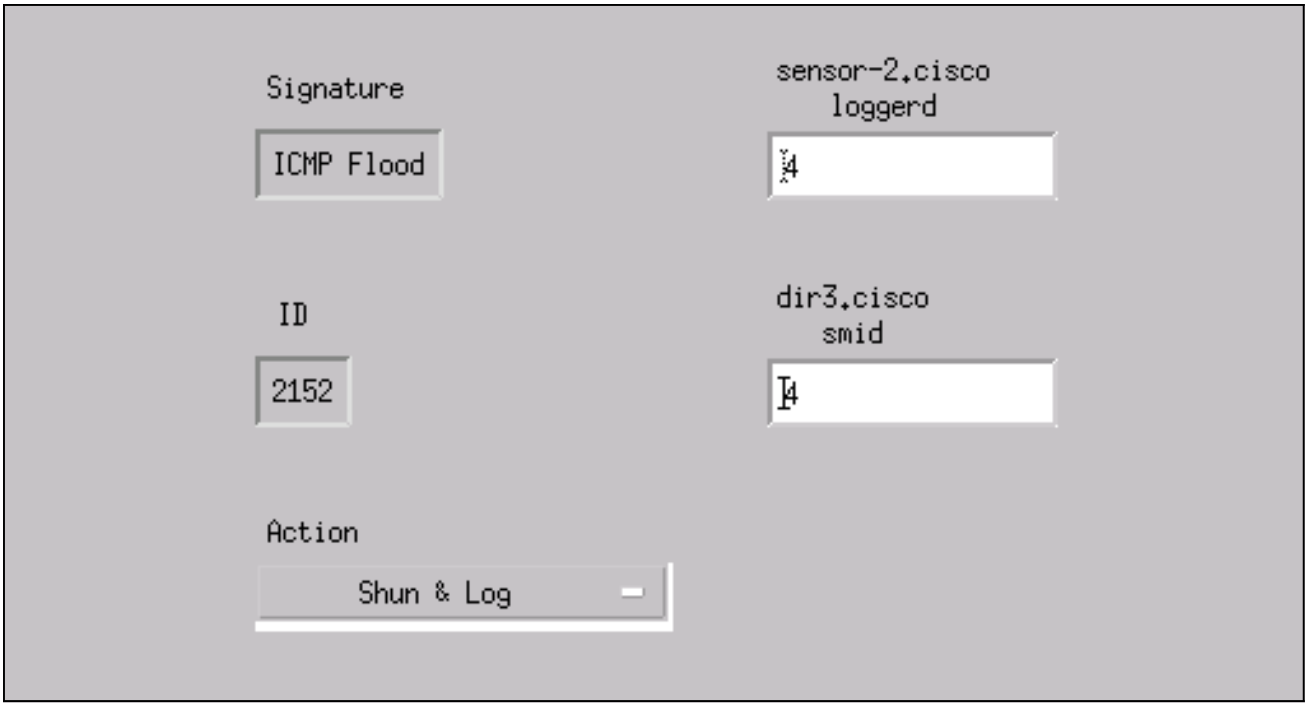
الانتهاء.

7. افتح نافذة اكتشاف الاقتحام، وانقر فوق **الشبكات المحمية**. إضافة النطاق **10.64.10.1** إلى **10.64.10.254** في الشبكة المحمية، كما هو موضح في هذا

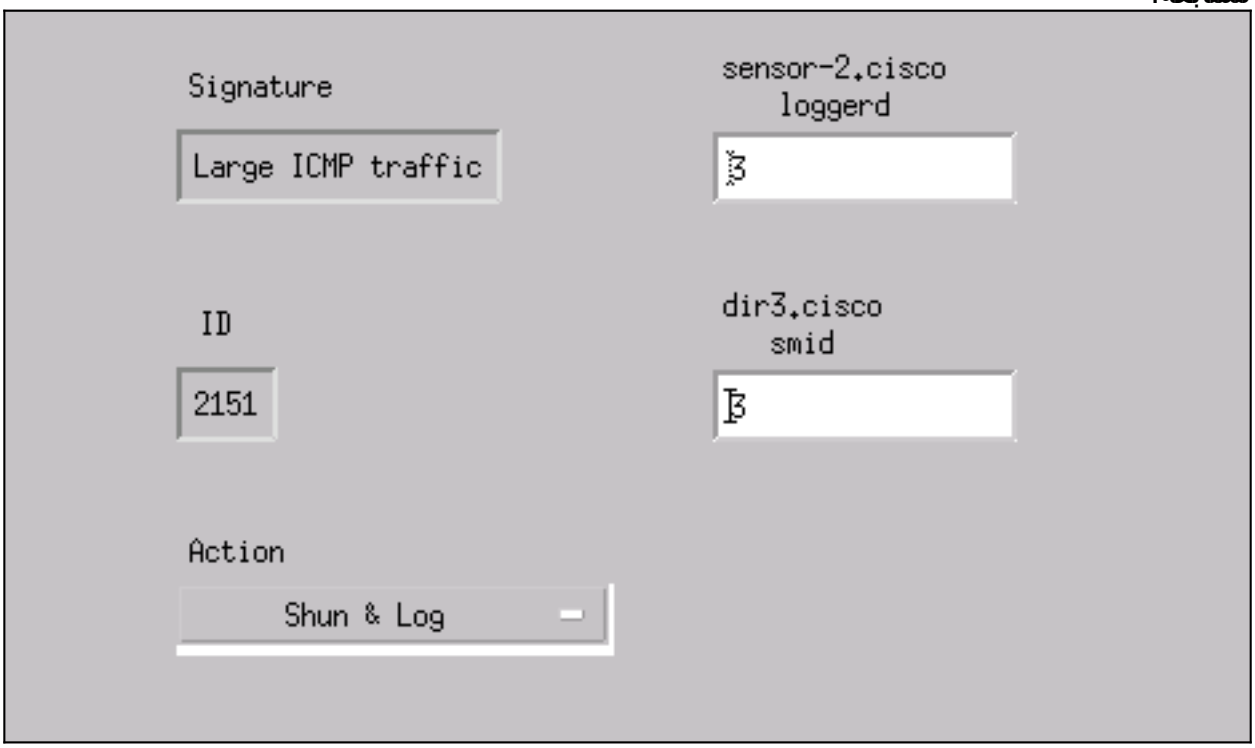


المثال.

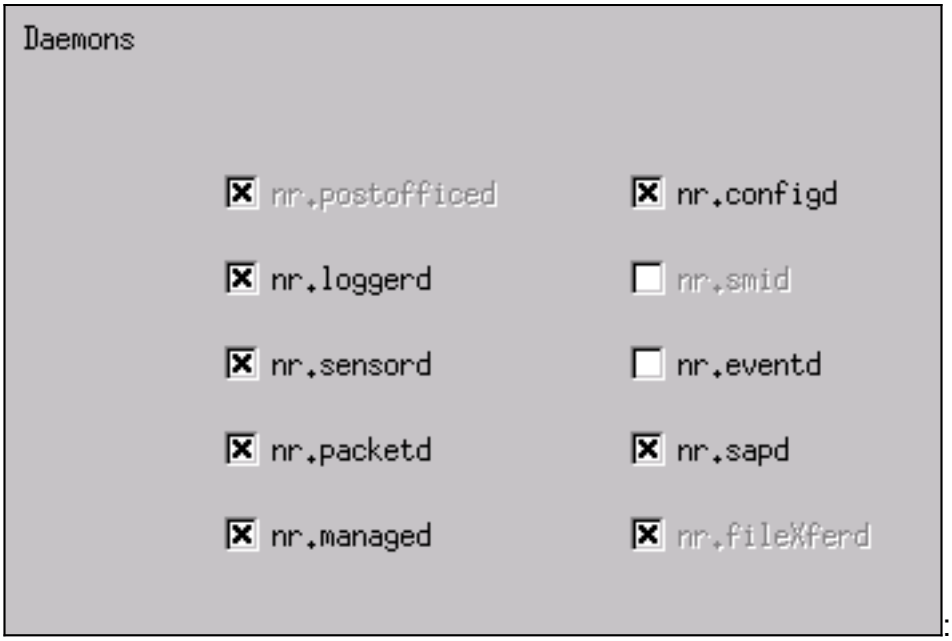
8. انقر على **ملف تخصيص > التكوين اليدوي**.
9. حدد **تعديل التوقيعات > حركة مرور ICMP الكبيرة** بمعرف **2151**.
10. انقر فوق **تعديل**، وقم بتغيير **الإجراء** من لا شيء إلى **تجاهل & تسجيل الدخول**، وانقر فوق **موافق** للمتابعة.



11. أختر **طوفان ICMP** بمعرف **2152**، وانقر فوق **تعديل**. قم بتغيير **الإجراء** من لا شيء إلى **تجاهل & تسجيل الدخول**، وانقر فوق **موافق** للمتابعة.

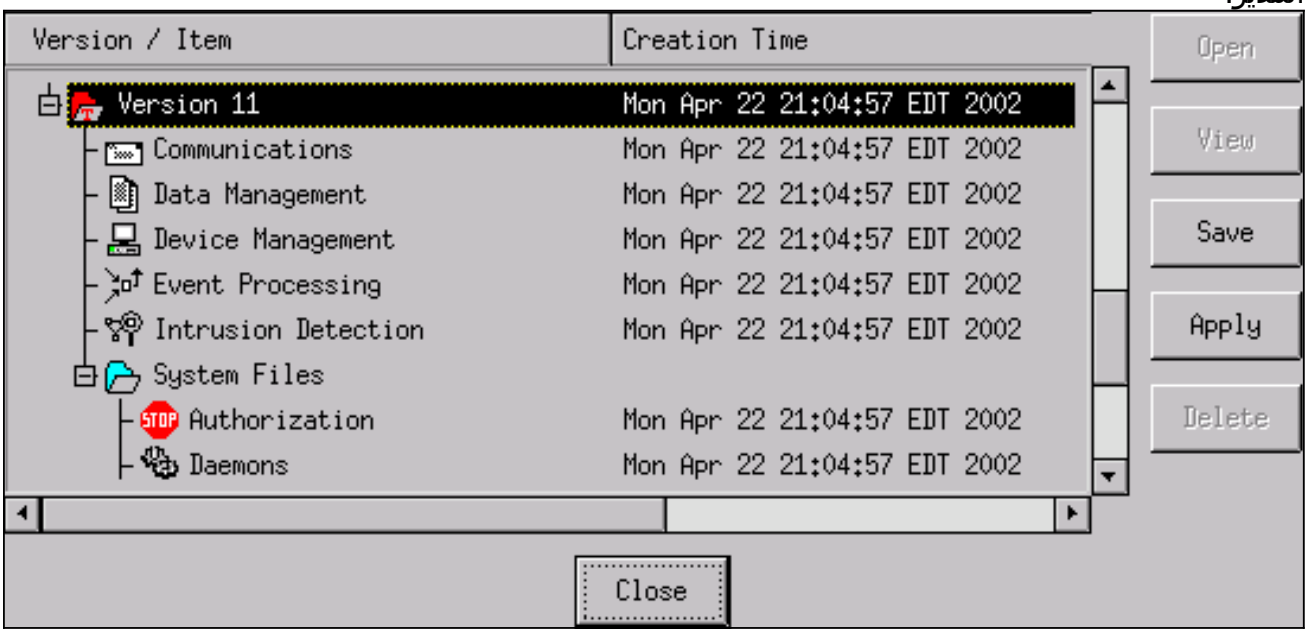


12. انقر فوق **موافق** لإغلاق نافذة اكتشاف الاقتحام.
13. افتح مجلد "ملفات النظام"، وافتح نافذة "ملفات النظام".تأكد من تمكين هذه



الأجهزة:

14. انقر فوق **موافق** للمتابعة، أختر الإصدار الذي تم تعديله للتو، وانقر فوق **حفظ** ثم **تطبيق**.انتظر حتى يخبرك النظام بأن أداة الاستشعار قد انتهت من إعادة تشغيل الخدمات، ثم قم بإغلاق كافة النوافذ الخاصة بتكوين المدير.



التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show access-list** - يسرد عبارات الأوامر **access-list** في تكوين الموجه. كما أنها تسرد عدد مرات مطابقة العنصر أثناء بحث أمر **access-list**.
- **ping** - يستخدم لتشخيص اتصال الشبكة الأساسي.

قبل شن الهجوم

قبل تشغيل هجوم، قم بإصدار هذه الأوامر.

```
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
```

شن الهجوم و التجنب

أطلق هجومك من الموجه "الضوء" إلى "بيت" الضحية. عندما تتأثر قائمة التحكم في الوصول (ACL)، يتم مشاهدة الملفات التي يتعذر الوصول إليها.

```
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.U!!!!!!!!!!!!!!!
```

بمجرد اكتشاف المستشعر للهجوم، ويتم تنزيل قائمة التحكم في الوصول (ACL)، ويتم عرض هذا الإخراج على "House".

```
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
```

لا تزال المناطق التي يتعذر الوصول إليها مرئية على "الضوء"، كما هو موضح في هذا المثال.

```
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
```

بعد 15 دقيقة، يعود "هاوس" إلى طبيعته، لأن التجنب تم ضبطه على 15 دقيقة.

```
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
```

"الضوء" يمكنه إختبار "البيت".

```
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
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- صفحة دعم منع التسلل 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).