تكوين إعادة تعيين TCP باستخدام مدير IDS

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين مدير ومستشعر نظام اكتشاف الاقتحام (IDS، المعروف سابقا باسم NetRanger) لإرسال رسائل إعادة توجيه TCP على برنامج Telnet تم محاولة إرساله إلى نطاق من العناوين التي تتضمن الموجه المدار إذا كانت السلسلة المرسلة هي "testattack".

المتطلبات الأساسية

المتطلبات

عند النظر في هذا التكوين، يرجى تذكر ما يلي:

- قم بتثبيت Sensor وتحقق من أنه يعمل بشكل صحيح قبل تنفيذ هذا التكوين.
- ضمنت أن ال ينشق قارن إلى المسحاج تخديد مدار 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
- برنامج تشغيل موجه IOS® من Cisco، الإصدار 12.2.6

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

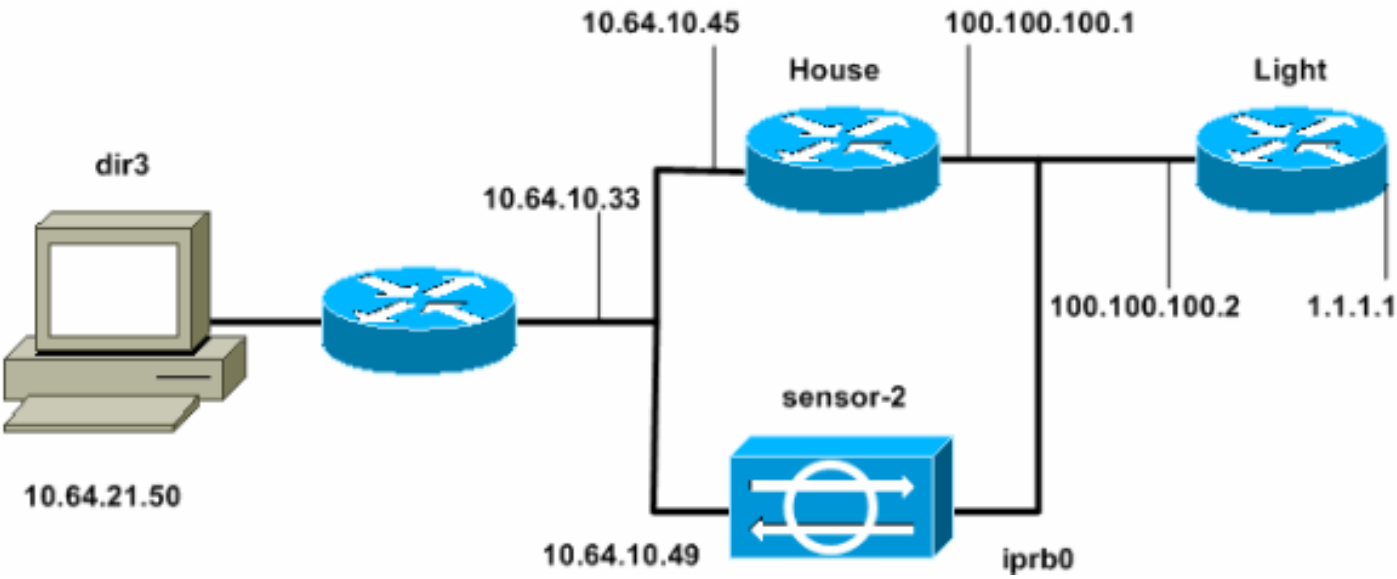
التكوين

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
!
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
```

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
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
!
!
!
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 (مستشعر IDS) مع **جذر** اسم المستخدم والهجوم **على** كلمة المرور.
2. اكتب **sysconfig-sensor**.
3. أدخل معلومات التكوين، عند طلبها، كما هو موضح في هذا المثال:

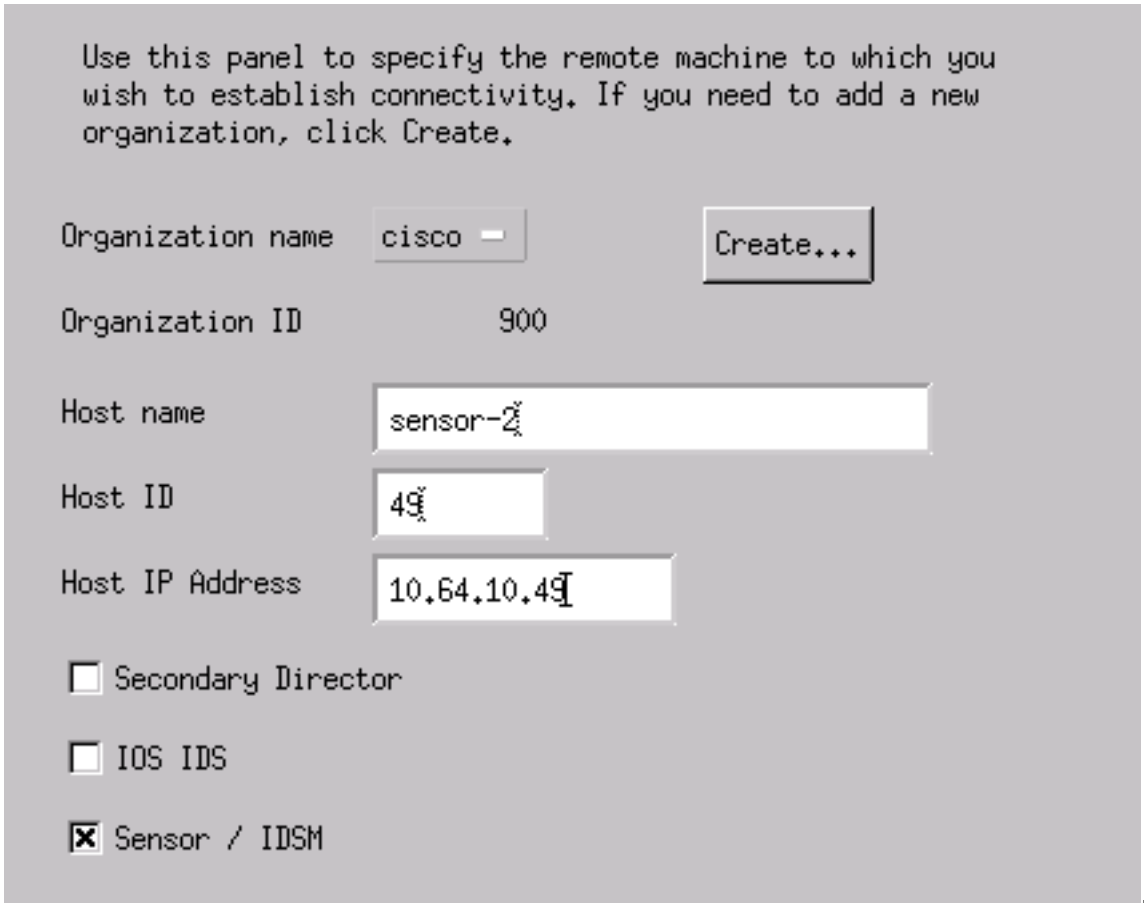
```
IP Address:  10.64.10.49 - 1
IP Netmask:  255.255.255.224 - 2
IP Host Name:  sensor-2 - 3
Default Route:  10.64.10.33 - 4
Network Access Control - 5
.64
.10
Communications Infrastructure - 6
Sensor Host ID:  49
Sensor Organization ID:  900
Sensor Host Name:  sensor-2
Sensor Organization Name:  cisco
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 (مدير IDS) مع اسم المستخدم **netrangr** والهجوم **بكلمة المرور**.
2. اكتب **&vw** لتشغيل برنامج OpenView من HP.
3. من القائمة الرئيسية، انتقل إلى **التأمين > التكوين**.
4. في الأداة المساعدة لإدارة ملفات التكوين، انتقل إلى **ملف > إضافة مضيف** وانقر **بعد ذلك**.
5. أكمل معلومات مضيف المستشعر، كما هو موضح في هذا المثال. انقر فوق **Next**

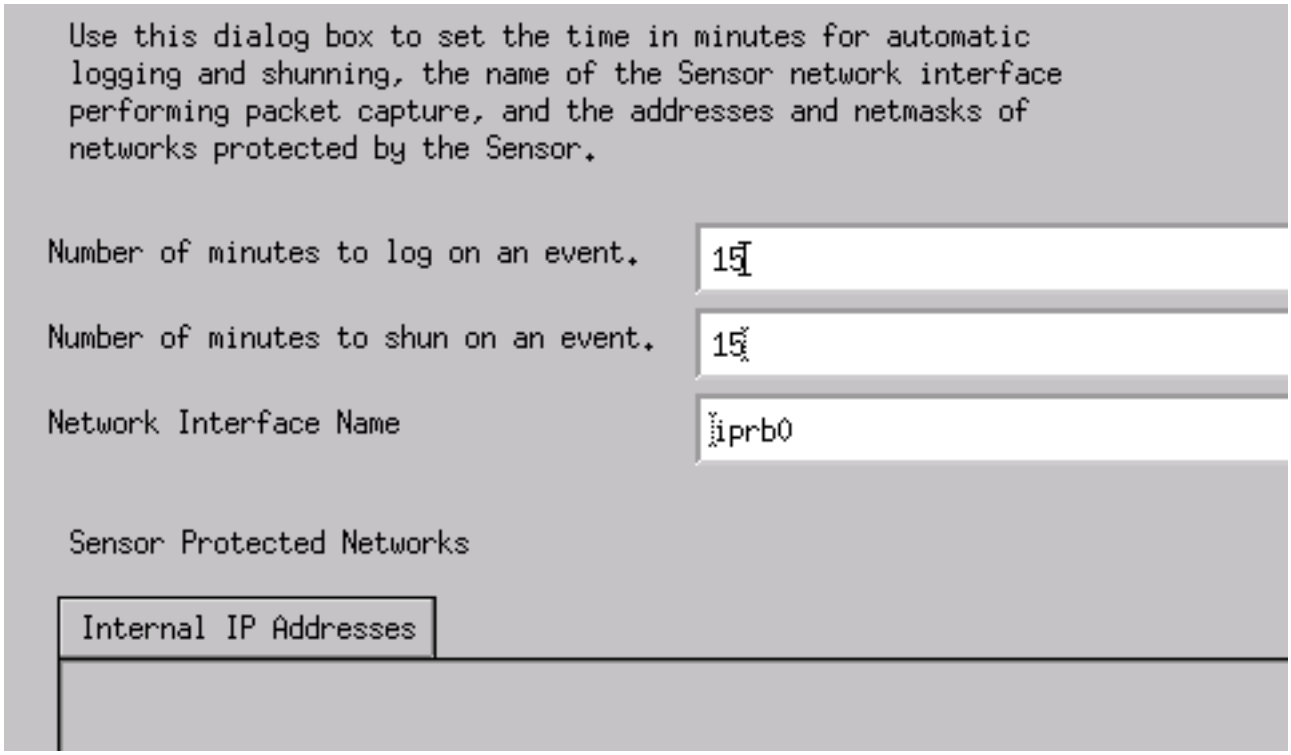


(التالي).

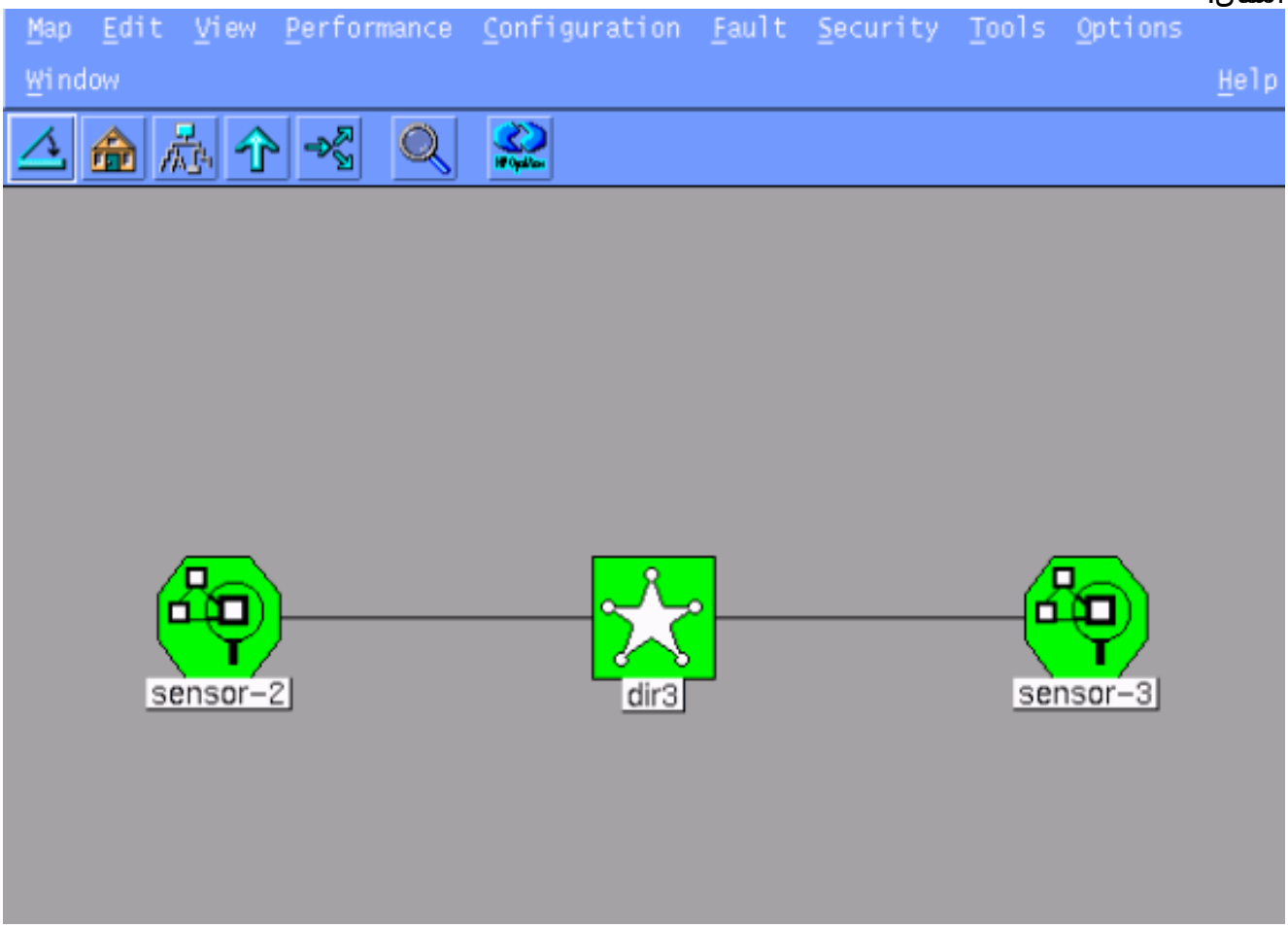
6. اقبل الإعدادات الافتراضية لنوع الجهاز، وانقر **التالي**، كما هو موضح في هذا

المثال.

7. يمكنك إما تغيير السجل وإبطال الدقائق أو قبول القيم الافتراضية. مهما، أنت ينبغي 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. استمر في النقر فوق **التالي** ثم انقر فوق **إنهاء** لإضافة المستشعر إلى المدير. من القائمة الرئيسية، يجب أن ترى الآن المستشعر-2، كما في هذا المثال.

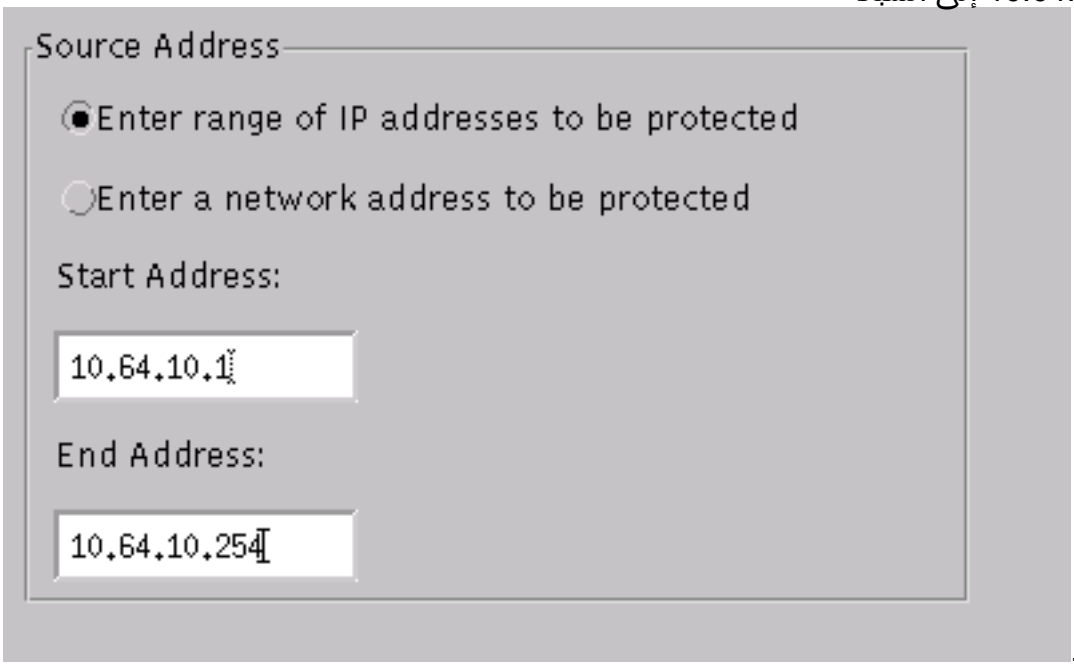


تكوين إعادة تعيين TCP لموجه Cisco IOS

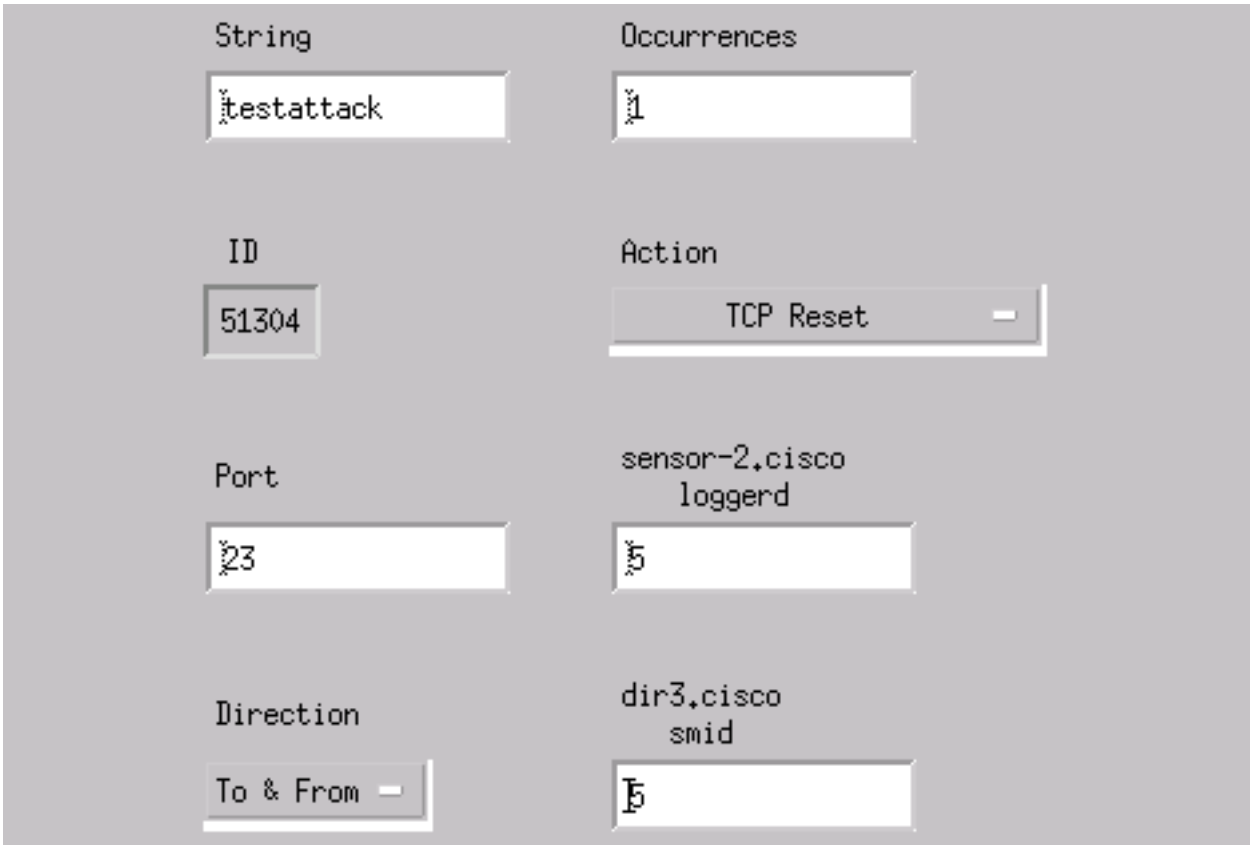
أكمل هذه الخطوات لتكوين إعادة تعيين TCP لموجه Cisco IOS.

1. في القائمة الرئيسية، انتقل إلى **التأمين > التكوين**.
2. في الأداة المساعدة لإدارة ملف التكوين، قم بإبراز **المستشعر-2** وانقر نقرا مزدوجا عليه.
3. فتح إدارة الأجهزة.
4. انقر فوق **أجهزة > إضافة**. أدخل معلومات الجهاز، كما هو موضح في المثال التالي. انقر فوق **موافق**" للمتابعة. كل من Telnet و enable كلمة cisco.

5. افتح نافذة اكتشاف الاقتحام وانقر فوق **الشبكات المحمية**. إضافة نطاق العناوين من 10.64.10.1 إلى 10.64.10.254 إلى الشبكة

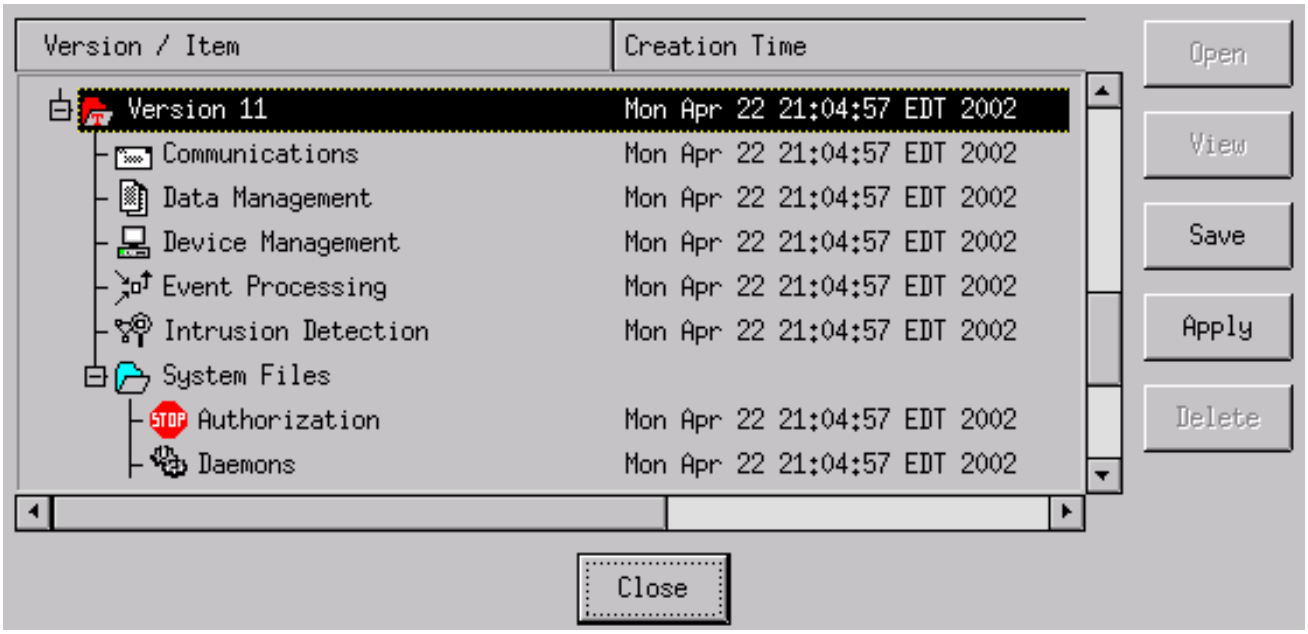


المحمية.
6. انقر على **توصيف** وحدد **تشكيل يدوي**. بعد ذلك، انقر فوق **تعديل التواقيع**. أختر **سلاسل مطابقة** بمعرف 8000. انقر فوق **توسيع > إضافة** لإضافة سلسلة جديدة تسمى **هجوم التجربة**. أدخل معلومات السلسلة، كما هو موضح في هذا المثال، وانقر فوق **موافق**للمتابعة.



7. لقد انتهيت من هذا الجزء من التكوين. انقر فوق **موافق** لإغلاق نافذة اكتشاف الاقتحام.
8. افتح مجلد "ملفات النظام"، ثم نافذة "ملفات النظام". تأكد من تمكين هذه الخواتم:

9. انقر فوق **موافق**" للمتابعة.
10. أختر الإصدار الذي قمت بتعديله للتو، انقر 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.



تشغيل الهجوم وإعادة تعيين TCP

برنامج Telnet من ضوء الموجه إلى منزل الموجه ونوع **هجوم** التجربة. بمجرد النقر فوق Space أو Enter key، يتم إعادة تعيين جلسة عمل برنامج Telnet. سيتم الاتصال بمنزل الموجه.

```
light#telnet 10.64.10.45
Trying 10.64.10.45 ... Open

User Access Verification
:Password
house>en
:Password
house#testattack
[Connection to 10.64.10.45 closed by foreign host]
.Telnet session has been reset because the !--- signature testattack was triggered ---!
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

Telnet إلى 10.64.10.49، المستشعر، باستخدام **جذر** اسم المستخدم والهجوم **على كلمة المرور**. اكتب **cd /usr/nr/etc**. اكتب **cat packet d.conf**. إذا قمت بتعيين إعادة تعيين TCP بشكل صحيح لهجوم الاختبار، فيجب أن ترى أربعة (4) في حقل رموز الإجراءات. يشير ذلك إلى إعادة تعيين TCP كما هو موضح في هذا المثال.

```
netrangr@sensor-2:/usr/nr/etc
"cat packetd.conf | grep "testattack<
"RecordOfStringName 51304 23 3 1 "testattack
"SigOfStringMatch 51304 4 5 5 # "testattack
```

إذا قمت بضبط الإجراء عن طريق الخطأ على "لا شيء" في التوقيع، سترى صفرا (0) في حقل رموز الإجراءات. يشير

ذلك إلى عدم وجود إجراء كما هو موضح في هذا المثال.

```
netrangr@sensor-2:/usr/nr/etc
"cat packetd.conf | grep "testattack<
"RecordOfStringName 51304 23 3 1 "testattack
"SigOfStringMatch 51304 0 5 5 # "testattack
```

يتم إرسال عمليات إعادة توجيه TCP من واجهة التقاط "المستشعر". إن هناك مفتاح يربط المستشعر قارن إلى القارن خارجي من المسحاج تخديد مدار، عندما أنت تشكل يستعمل **المجموعة فسحة بين دعامتين** أمر في المفتاح، استعملت هذا إعراب:

```
set span
```

```
banana (enable) set span 2/12 3/6 both inpkts enable
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12
.Incoming Packets enabled. Learning enabled. Multicast enabled
(banana (enable
(banana (enable
banana (enable) show span

Destination     : Port 3/6
Connect to sniffing interface of the Sensor. Admin Source : Port 2/12 ---!
Connect to FastEthernet0/0 of Router House. Oper Source : Port 2/12 ---!
Direction       : transmit/receive
Incoming Packets: enabled
Learning        : enabled
Multicast       : enabled
```

معلومات ذات صلة

- الإعلامات الميدانية
- صفحة دعم منع التسلل الآمن من Cisco

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).