تكوين إعادة تعيين IDS TCP باستخدام VMS IDS MC

المحتويات

المقدمة

يقدم المستند نموذجا لتكوين نظام اكتشاف الاقتحام (IDS) من Cisco من خلال حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN)، وحدة تحكم إدارة معرفات الأجهزة (IDS MC). في هذه الحالة، يتم تكوين إعادة تعيين TCP من مستشعر IDS إلى موجه Cisco.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يتم تركيب جهاز الاستشعار وتهيئته لاستشعار حركة المرور الضرورية.
- يتم تمديد واجهة sniffing إلى الموجه خارج الواجهة.

المكونات المستخدمة

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

- VMS 2.2 مع IDS MC ومراقبة الأمان 1.2.3
- مستشعر Cisco IDS 4.1.3S(63)
- موجه Cisco الذي يشغل برنامج Cisco IOS® الإصدار 12.3.5

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

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

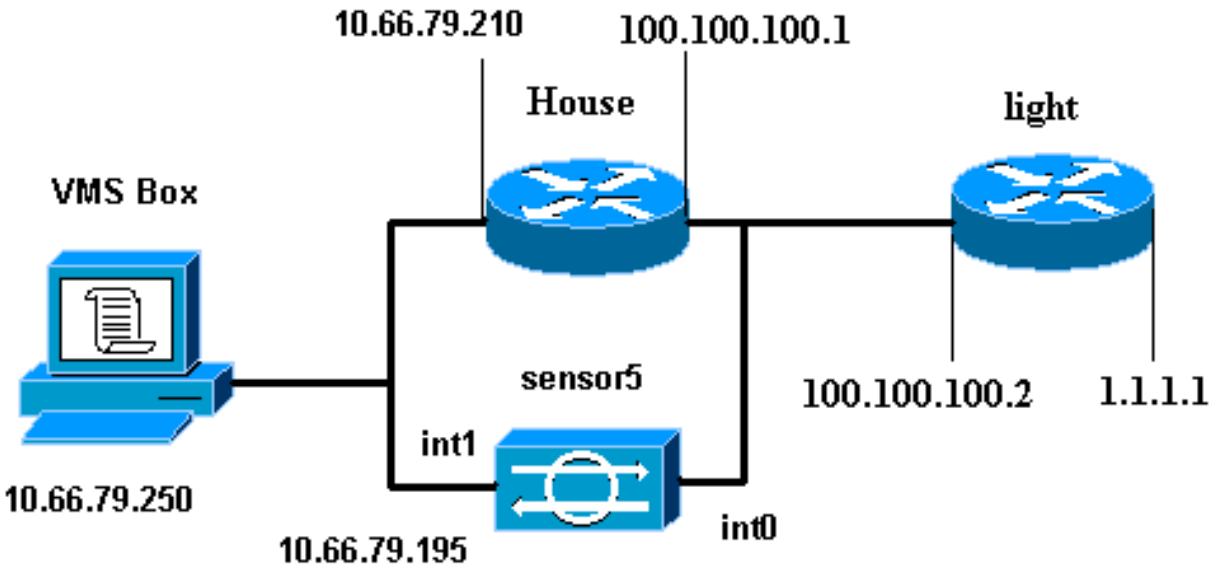
التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند هذه التكوينات.

- ضوء الموجه
- منزل الموجه

ضوء الموجه

```
Current configuration : 906 bytes
!
version 12.3
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

```
...Building configuration

Current configuration : 797 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname House
!
logging queue-limit 100
enable password cisco
!
ip subnet-zero
no ip domain lookup
!
!
interface Ethernet0
ip address 10.66.79.210 255.255.255.224
 hold-queue 100 out
!
interface Ethernet1
ip address 100.100.100.1 255.255.255.0
 ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.193
ip route 1.1.1.0 255.255.255.0 100.100.100.2
ip http server
no ip http secure-server
!
!
!
line con 0
 stopbits 1
line vty 0 4
password cisco
 login
!
scheduler max-task-time 5000
end
```

تكوين المستشعر الأولي

ملاحظة: إذا كنت قد قمت بالفعل بتنفيذ الإعداد الأولي للمستشعر، فقم بالمتابعة إلى قسم إستيراد المستشعر إلى IDS MC.

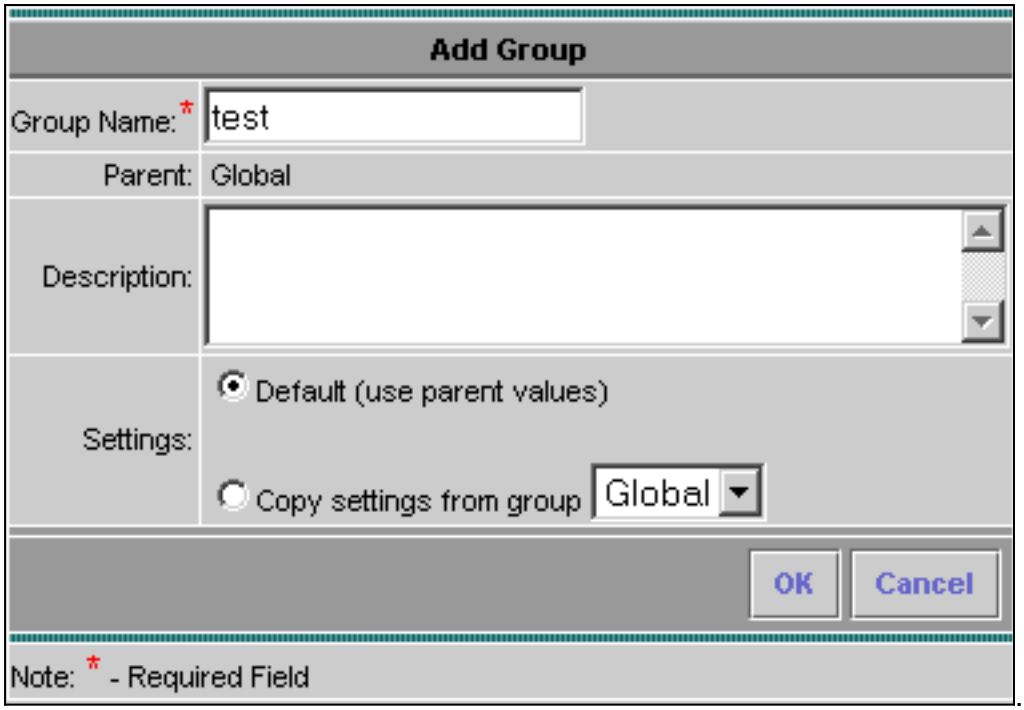
1. وحدة تحكم في المستشعر.أنت حضضت ل username وكلمة. إذا كانت هذه هي المرة الأولى التي تقوم فيها بتوفير التحكم في المستشعر، فيجب عليك تسجيل الدخول باستخدام اسم المستخدم **Cisco** وكلمة المرور **Cisco**.
2. أنت حضضت أن يغير الكلمة وأن يعيد الكلمة جديد أن يؤكد.
3. اكتب **setup** وأدخل المعلومات المناسبة في كل مطالبة لإعداد المعلمات الأساسية للمستشعر الخاص بك، كما هو موضح في هذا المثال:

```
sensor5#setup

                --- System Configuration Dialog ---

.At any point you may enter a question mark '?' for help
.User ctrl-c to abort configuration dialog at any prompt
.'[]' Default settings are in square brackets

                                :Current Configuration

                                        networkParams
                                    ipAddress 10.66.79.195
                                    netmask 255.255.255.224
                                defaultGateway 10.66.79.193
                                        hostname sensor5
                                    telnetOption enabled
                    accessList ipAddress 10.66.79.0 netmask 255.255.255.0
                                                    exit
                                                timeParams
                                            summerTimeParams
                                        active-selection none
                                                    exit
                                                    exit
                                            service webServer
                                                    general
                                                ports 443
                                                    exit
                                                    exit

Save the config:   (It might take a few minutes for the sensor 5
                        (saving the configuration
                .Go to the command prompt without saving this config [0]
                .Return back to the setup without saving this config [1]
                            .Save this configuration and exit setup [2]

                                    Enter your selection[2]: 2
```

إستيراد أداة الاستشعار إلى وحدة التحكم IDS MC

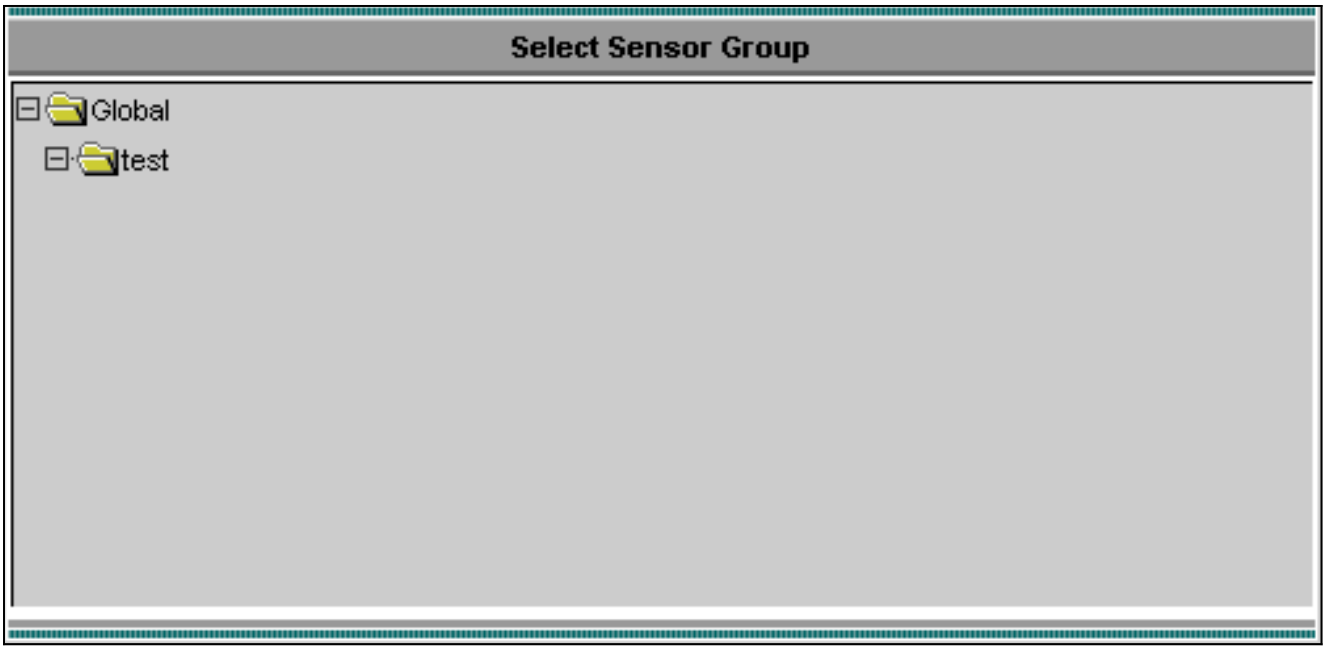
أتمت هذا steps in order to استوردت المستشعر داخل ال IDS mc.

1. الاستعراض للوصول إلى جهاز الاستشعار الخاص بك. في هذه الحالة، إما **http://10.66.79.250:1741** أو **https://10.66.79.250:1742**.
2. قم بتسجيل الدخول باستخدام اسم المستخدم وكلمة المرور الملائمين.في هذا مثال، ال username **admin** وكلمة **cisco**.
3. أخترت **VPN/أمن إدارة حل>إدارة مركز** وطقطقة **IDS جهاز إستشعار**.
4. انقر فوق علامة التبويب الأجهزة واختر **مجموعة المستشعر**.
5. ركزت **شامل** وطقطقة **يخلق مجموعة فرعية**.
6. أدخل اسم المجموعة وتأكد من إختيار **الافتراضي**، ثم انقر فوق **موافق** لإضافة المجموعة الفرعية إلى وحدة التحكم في الوصول للمعرف

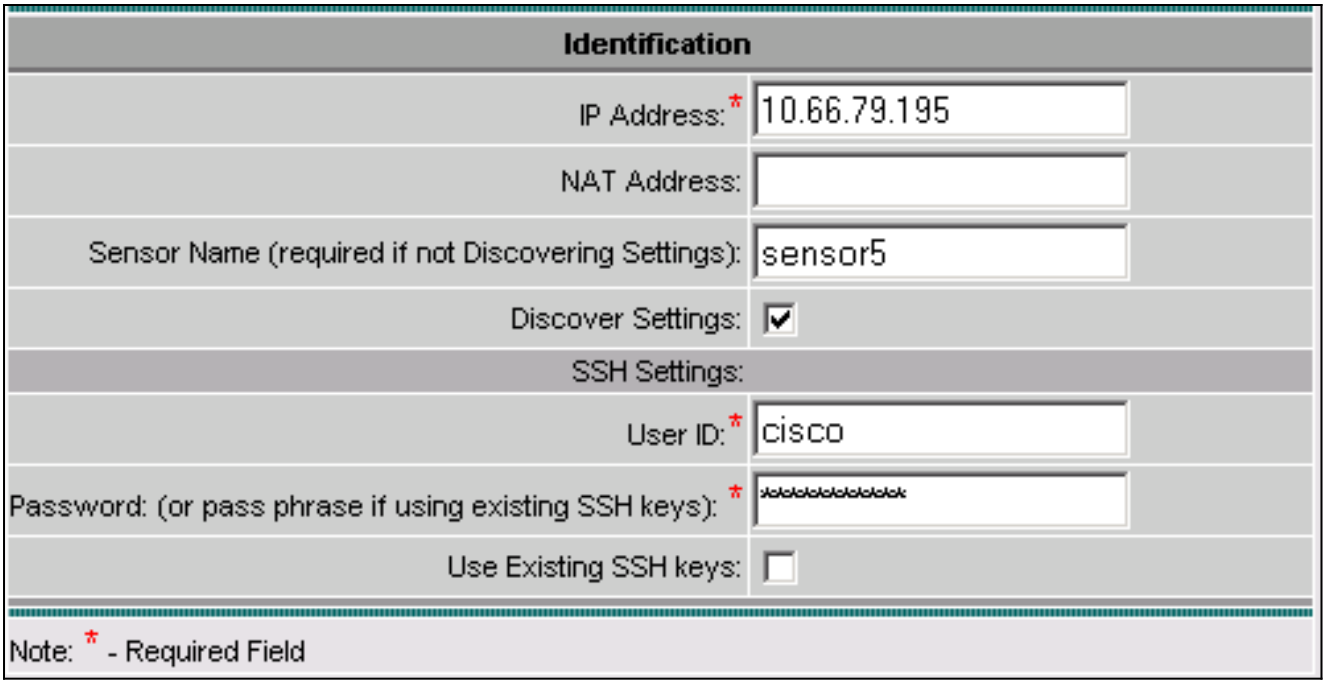


(IDS).

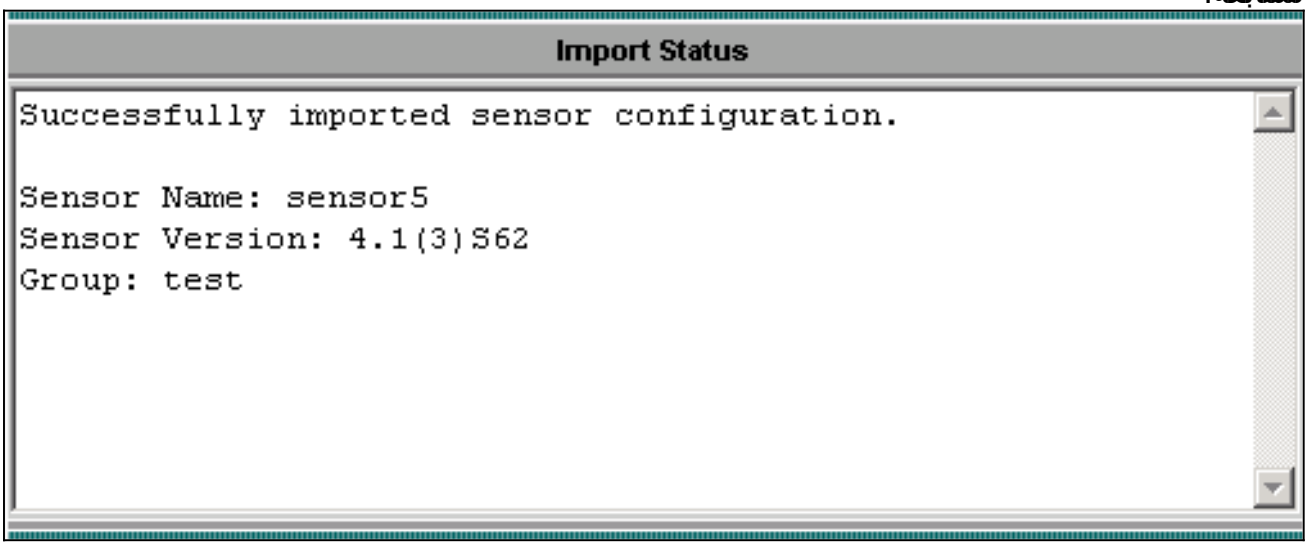
7. أخترت **أداة>مستشعر**، ركزت المجموعة فرعية يخلق في الخطوة السابقة (في هذه الحالة، **إختبار**)، وطقطقة **يضيف**.
8. ركزت المجموعة الفرعية وطقطقة **بعد ذلك**.



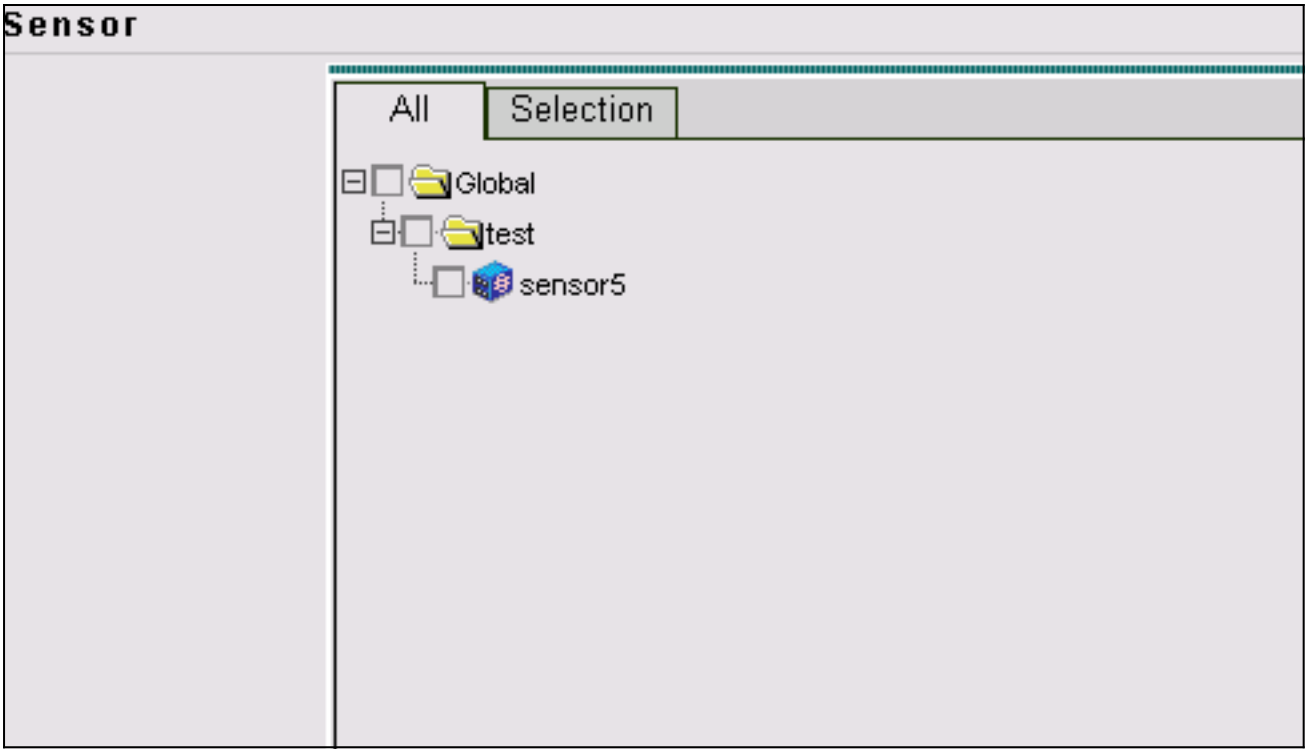
9. أدخل التفاصيل طبقا لهذا المثال وانقر فوق **التالي** للمتابعة.



10. عندما تقدم لك رسالة تشير إلى ، انقر فوق **إنهاء** للمتابعة.



11. تم إستيراد جهاز الاستشعار إلى وحدة التحكم في إدارة IDS. في هذه الحالة، يتم إستيراد Sensor5.



إستيراد المستشعر إلى مراقب الأمان

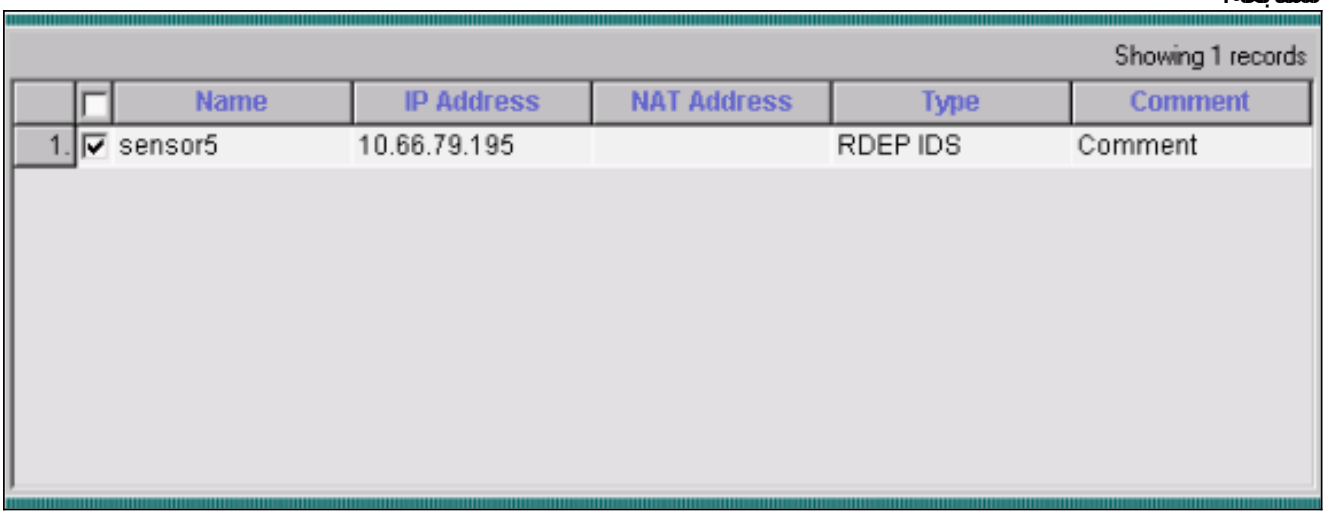
أكمل هذه الخطوات لاستيراد المستشعر إلى مراقبة الأمان.

1. في قائمة خادم VMS، أختر **VPN/حل إدارة الأمان > مركز المراقبة>مراقبة الأمان**.
2. حدد علامة التبويب "أجهزة"، ثم انقر فوق **إستيراد** وأدخل معلومات خادم IDS MC، طبقا لهذا المثال.

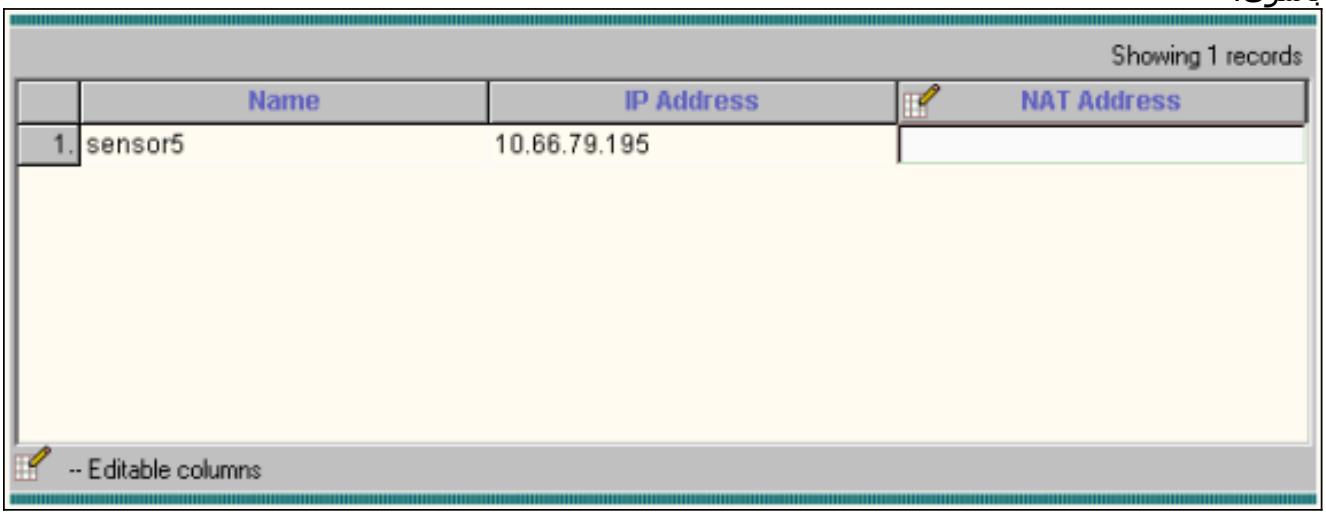
Enter IDS MC server contact information:	
IP Address/Host Name:*	10.66.79.250
Web Server Port:*	443
Username:*	admin
Password:*	•••••••

Note: * - Required Field

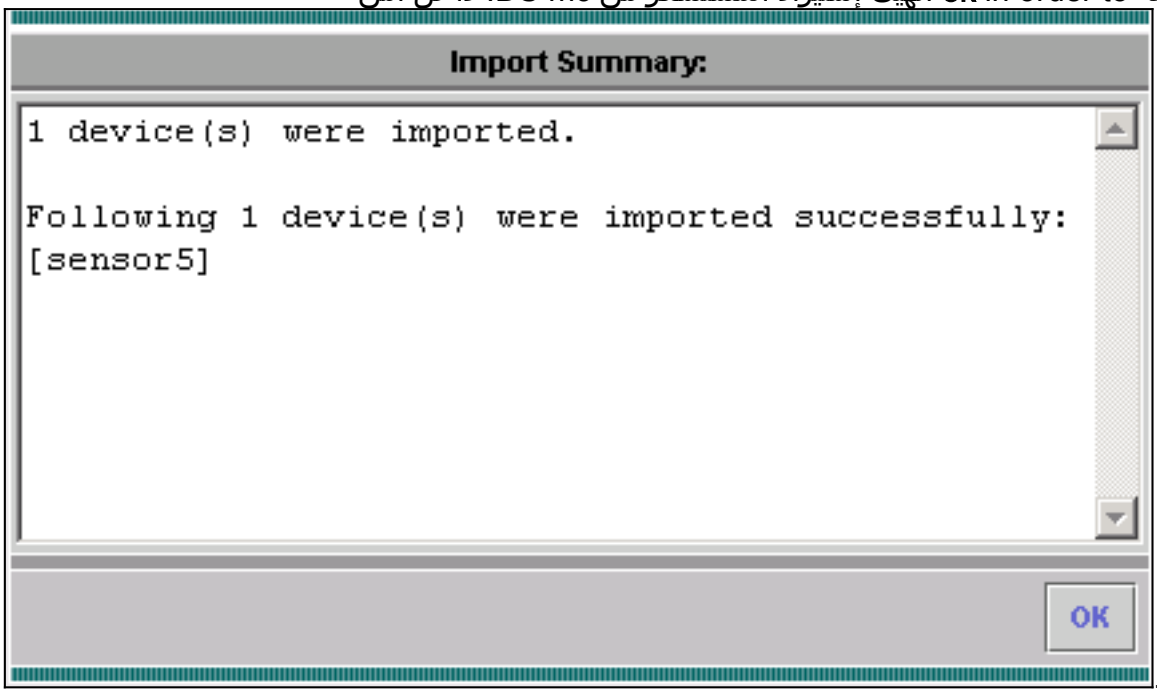
3. حدد المستشعر (في هذه الحالة، **المستشعر 5**) وانقر **التالي** للمتابعة.



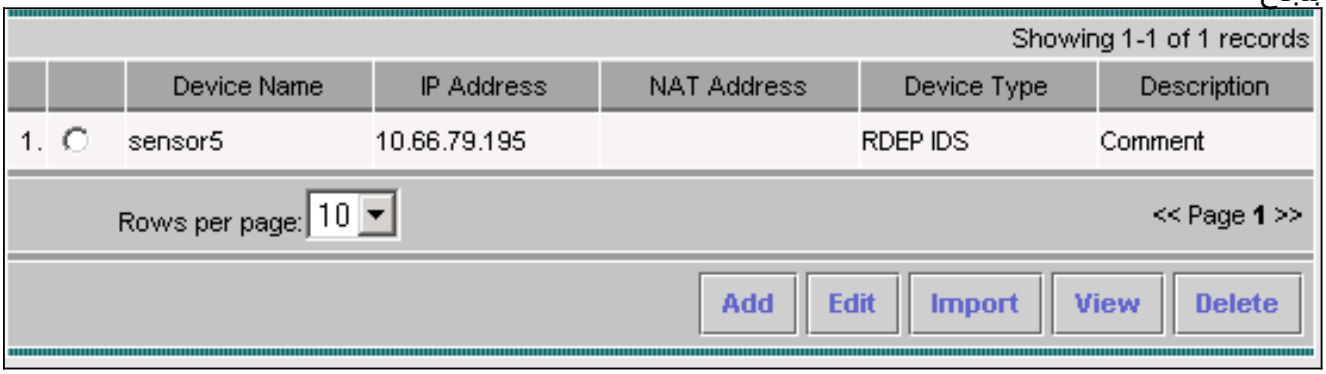
4. إن يحتاج، حدث ال NAT عنوان ل مستشعر ك، بعد ذلك طقطقت **إنجاز** in order to باشرت.



5. طقطقة in order to **ok** أنهيت إستيراد المستشعر من IDS mc داخل أمن مدرب.



6. يمكنك الآن ملاحظة أن أداة الاستشعار الخاصة بك تم إستيرادها بنجاح



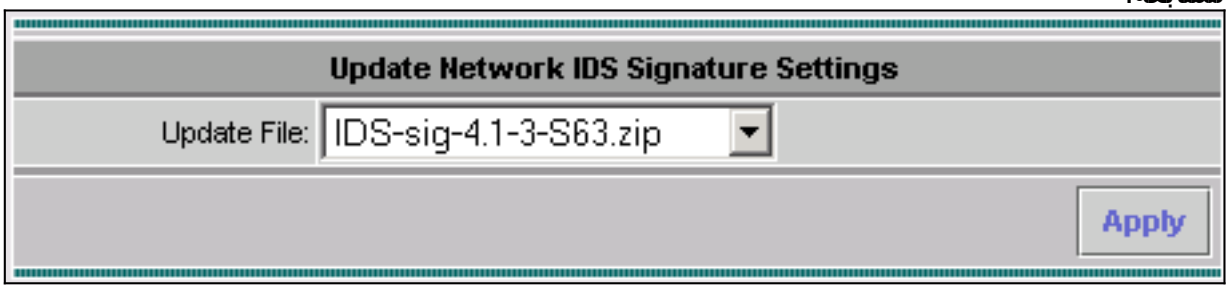
إستخدام IDS MC لتحديثات التوقيع

يشرح هذا الإجراء كيفية إستخدام IDS MC لتحديثات التوقيع.

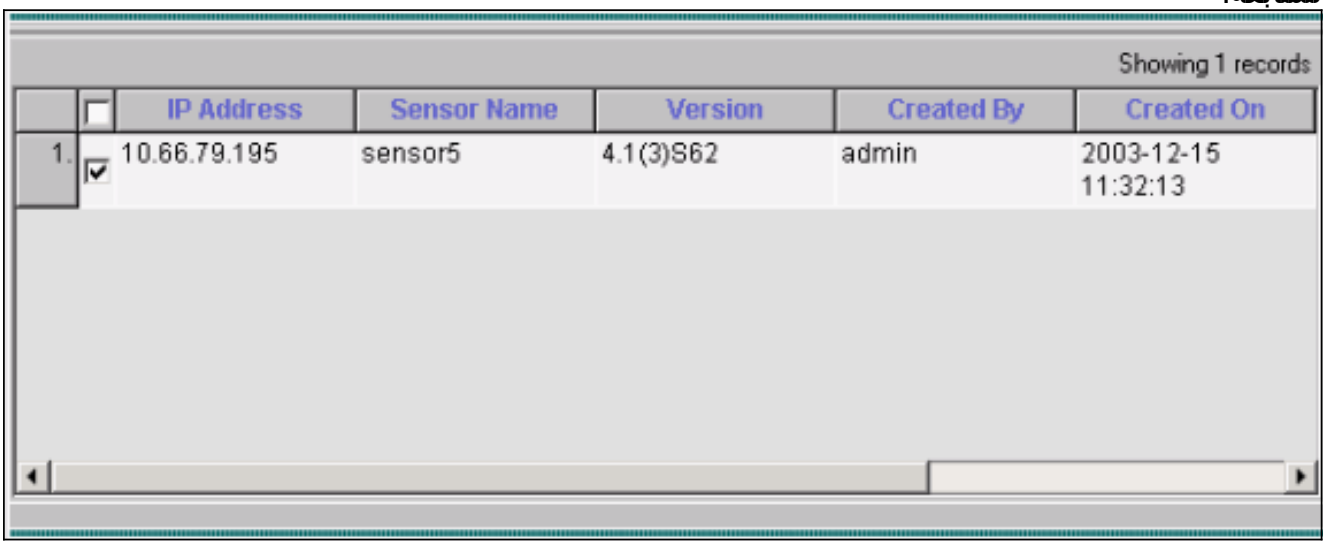
1. قم بتنزيل تحديثات توقيع Network IDS (للعملاء المسجلين فقط) واحفظهم في دليل

C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ على خادم VMS الخاص بك.

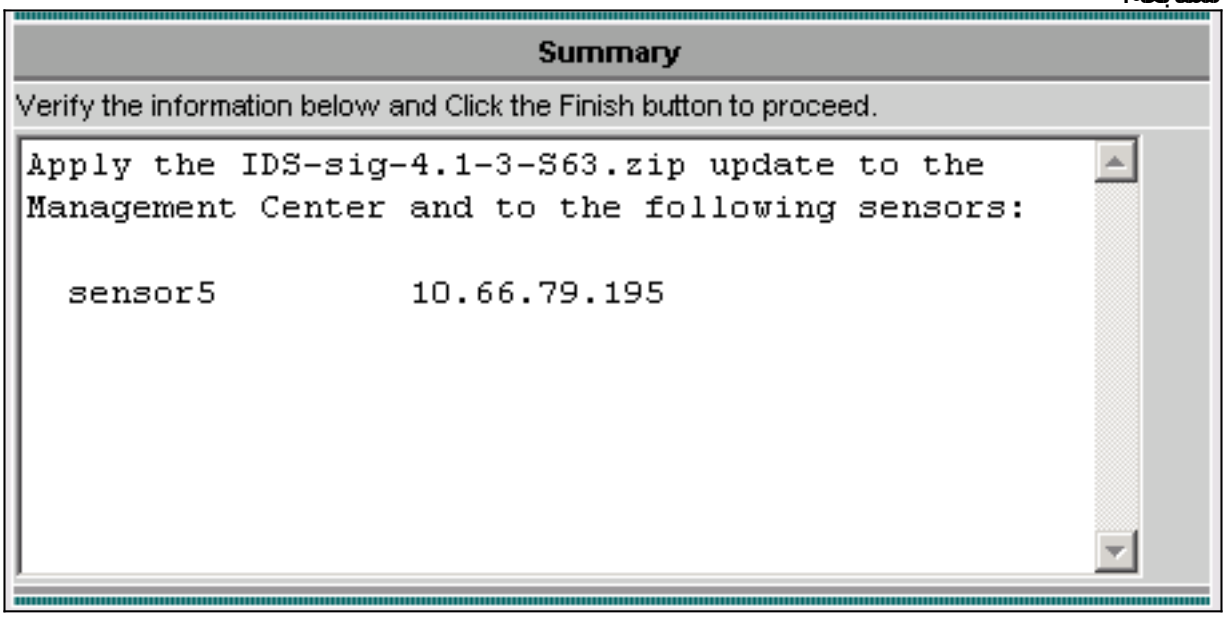
2. في وحدة تحكم خادم VMS، أختر **حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN)** > **مركز الإدارة** > **أجهزة إستشعار IDS**.
3. حدد علامة التبويب تكوين وانقر فوق **تحديثات**.
4. انقر على **تحديث توقيعات معرفات الشبكة**.
5. حدد التوقيع الذي تريد ترقيته من القائمة المنسدلة وانقر فوق **تطبيق** للمتابعة.



6. حدد أداة (أجهزة) الاستشعار لتحديثها وانقر فوق **التالي** للمتابعة.



7. بعد مطالبتك بتطبيق التحديث على مركز الإدارة، بالإضافة إلى أداة الاستشعار، انقر فوق **إنهاء** للمتابعة.



8. برنامج Telnet أو وحدة التحكم في واجهة سطر أوامر المستشعر. ترى معلومات مماثلة لهذه:

```
sensor5#
:(Broadcast message from root (Mon Dec 15 11:42:05 2003
.Applying update IDS-sig-4.1-3-S63
```

```
.This may take several minutes
.Please do not reboot the sensor during this update
:(Broadcast message from root (Mon Dec 15 11:42:34 2003
.Update complete
sensorApp is restarting
.This may take several minutes
```

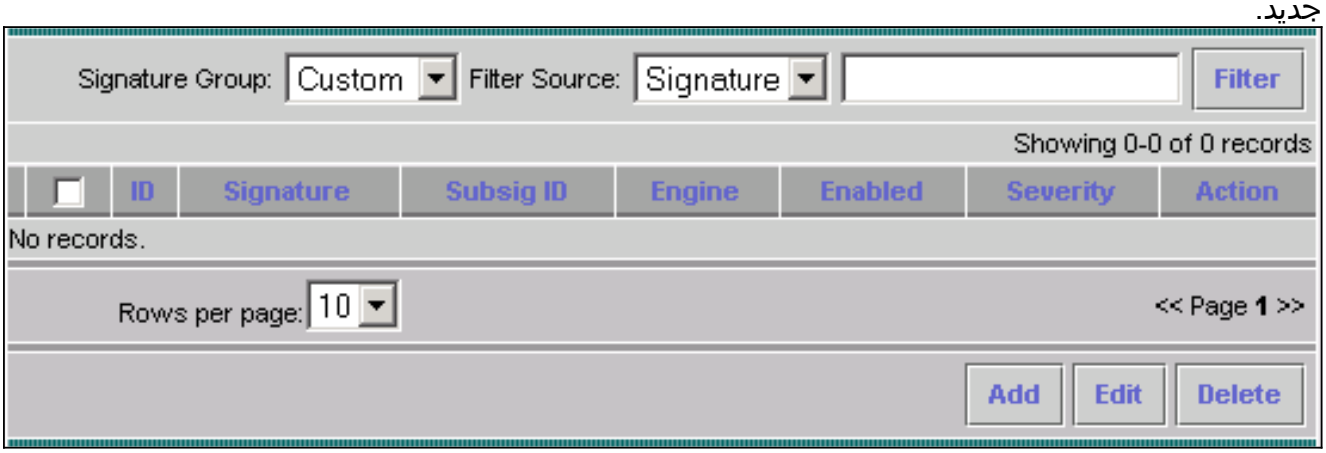
9. انتظر بضع دقائق للسماح بإكمال الترقية، ثم أدخل **show version** للتحقق.

```
sensor5#show version
:Application Partition
Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63

:Upgrade History
 IDS-sig-4.1-3-S62              07:03:04 UTC Thu Dec 04 2003 *
IDS-sig-4.1-3-S63.rpm.pkg    11:42:01 UTC Mon Dec 15 2003
```

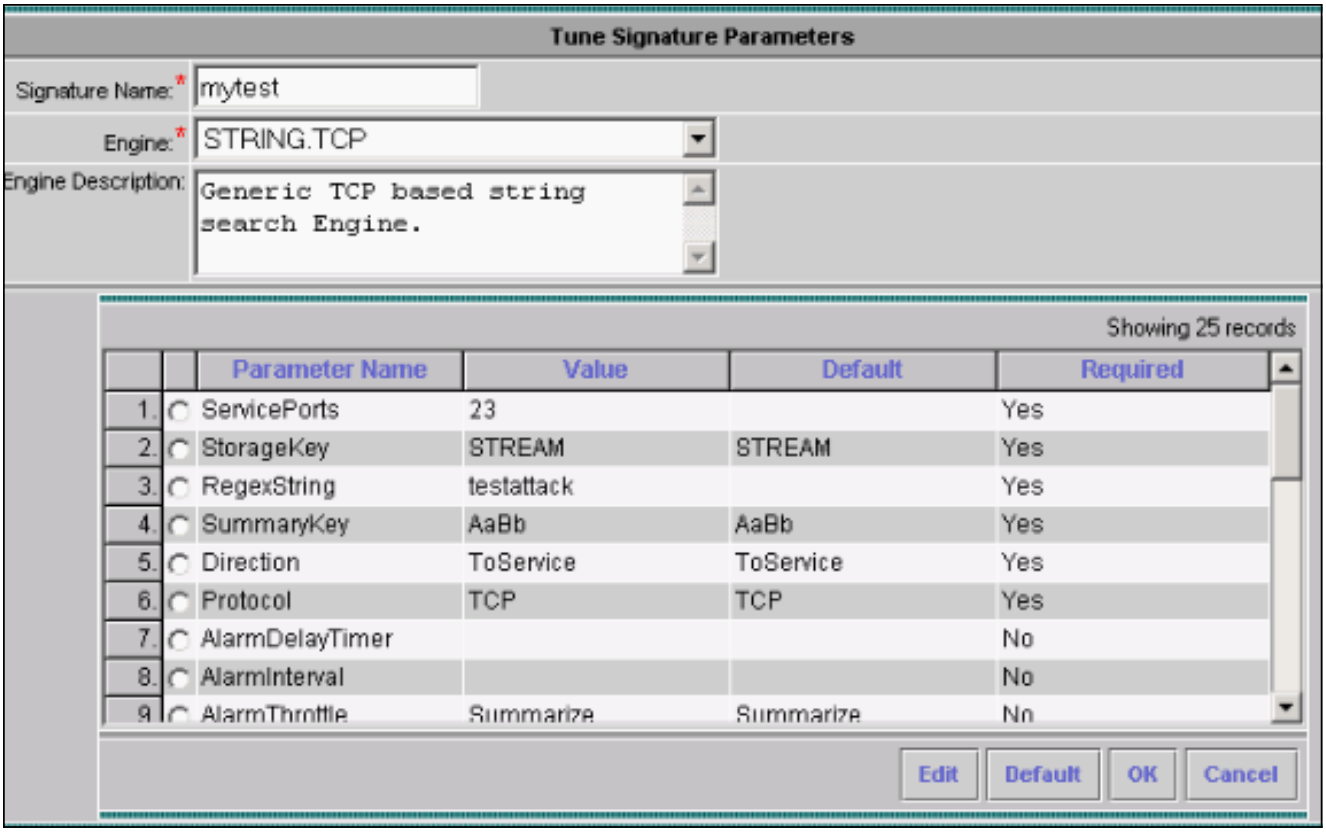
تكوين إعادة تعيين TCP لموجه IOS

أكمل هذه الخطوات لتكوين إعادة تعيين TCP لموجه IOS.

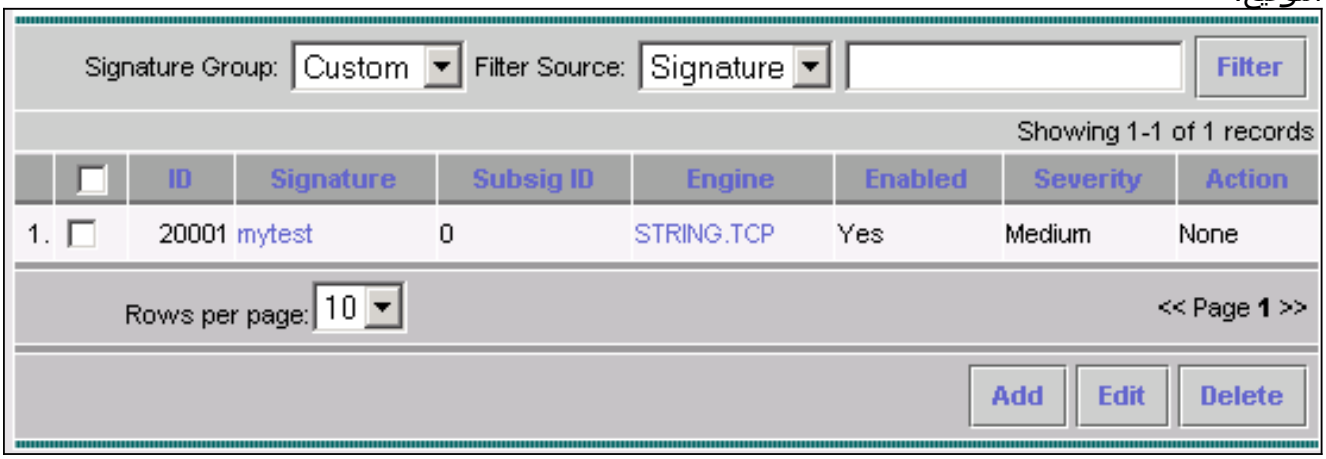
1. أخترت **VPN/أمن إدارة حل>إدارة مركز > IDS جهاز إستشعار**.
2. حدد علامة التبويب تكوين، وحدد أداة الاستشعار من أداة تحديد الكائن، ثم انقر فوق **إعدادات**.
3. حدد **توقيعات**، انقر **تخصيص**، وانقر **إضافة** لإضافة توقيع جديد.



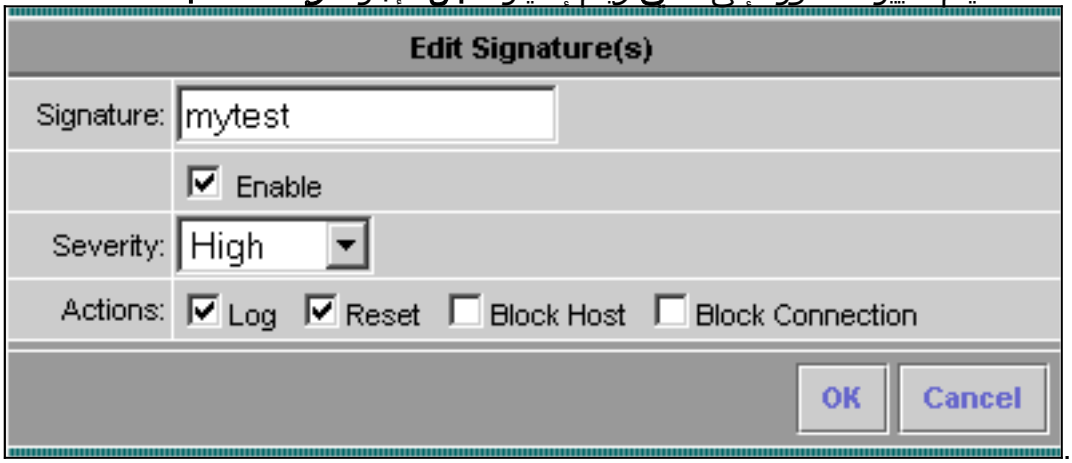
4. أدخل اسم التوقيع الجديد، ثم حدد المحرك (في هذه الحالة، **STRING.TCP**).
5. تحقق من زر الاختيار المناسب لتخصيص المعلمات المتوفرة ثم انقر فوق **تحرير**.في هذا المثال، يتم تحرير المعلمة ServicePorts لتغيير قيمتها إلى **23** (للمنفذ 23). تم تحرير المعلمة RegexString أيضا لإضافة **هجوم** إختبار القيمة. عند اكتمال هذا، انقر فوق **موافق"** للمتابعة.



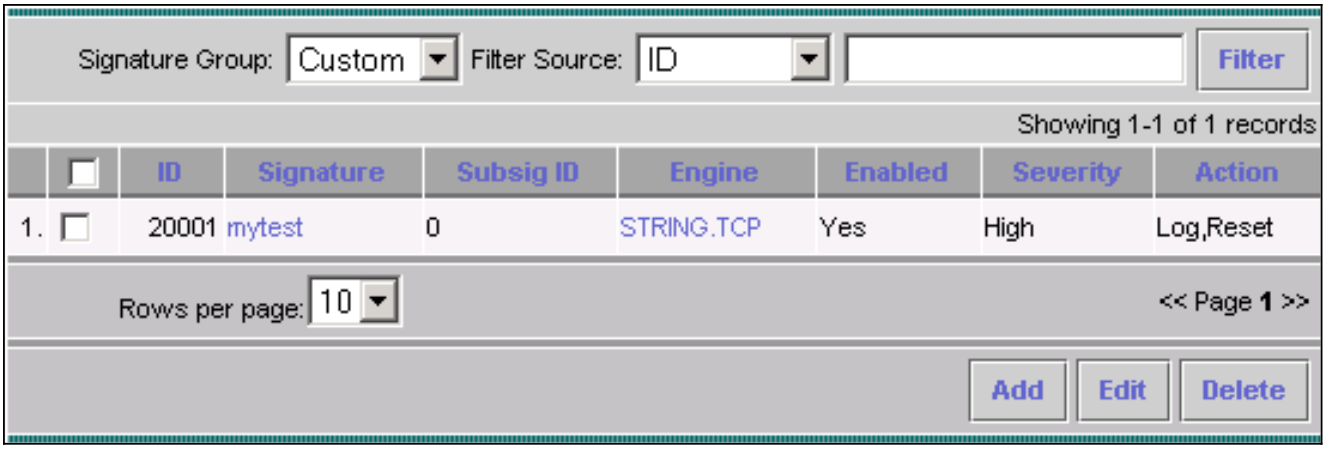
6. انقر اسم التوقيع لتحرير دقة وإجراءات التوقيع أو لتمكين/تعطيل التوقيع.



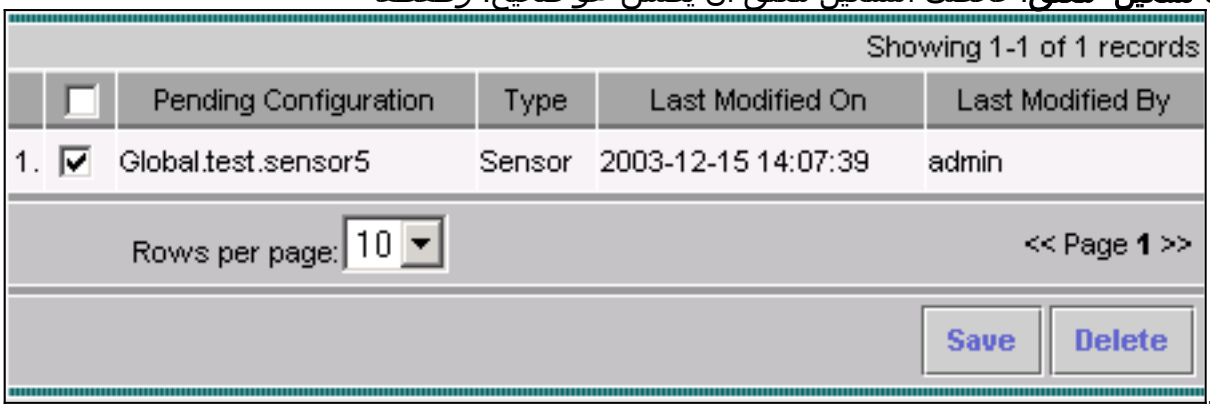
7. في هذه الحالة، يتم تغيير الخطورة إلى **عالي** ويتم إختيار **سجل** الإجراء **وإعادة الضبط**. طقطقة ok in order to تابعت.



8. يبدو التوقيع الكامل مشابها لما يلي:

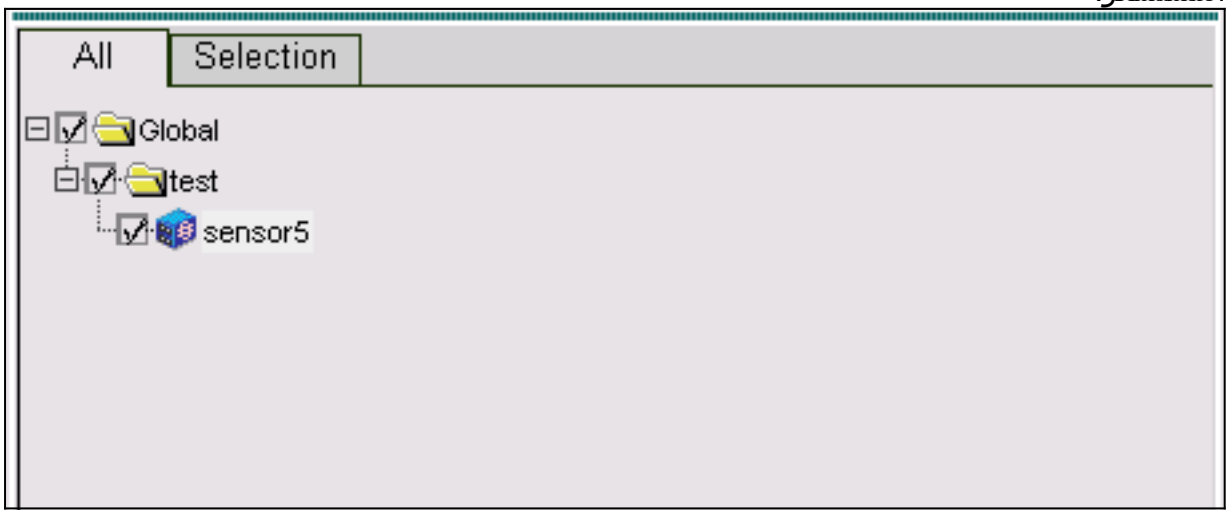


9. أخترت **تشكيل>معلق**، فحصت التشكيل معلق أن يضمن هو صحيح، وطقطقة

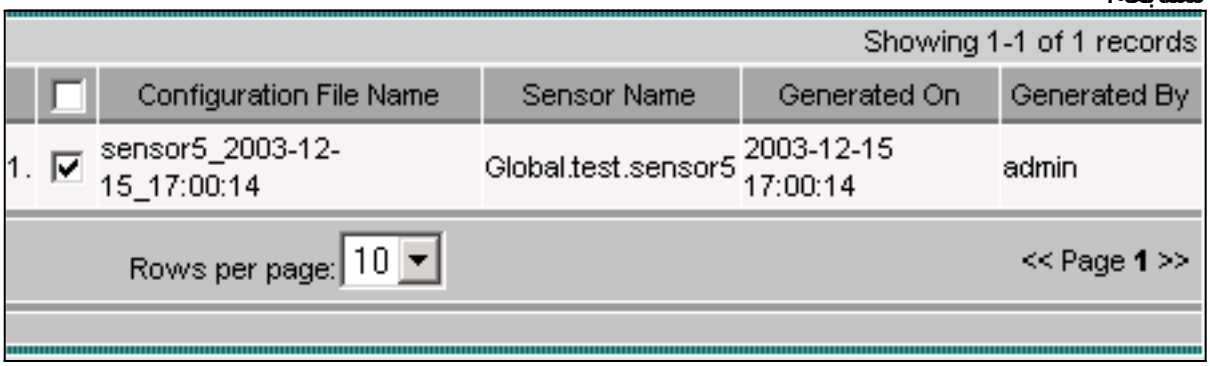


حفظ.

10. أختر **نشر > إنشاء**، ثم انقر فوق **تطبيق** لدفع تغييرات التكوين إلى المستشعر.

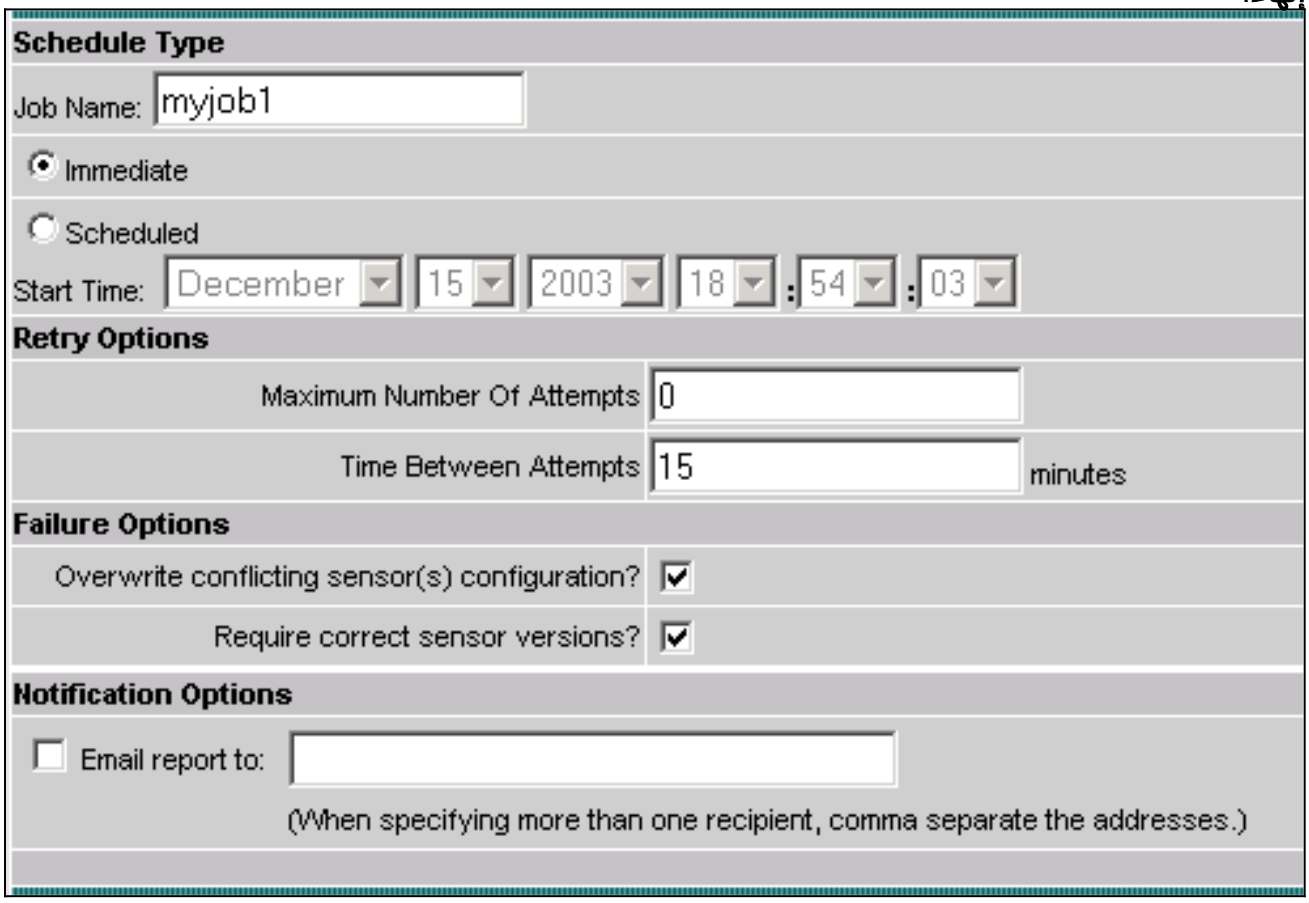


11. أختر **نشر > نشر** وانقر فوق **إرسال**.
12. حدد خانة الاختيار المجاورة للمستشعر وانقر فوق **نشر**.
13. حدد خانة الاختيار للمهمة في قائمة الانتظار وانقر فوق **التالي** للمتابعة.

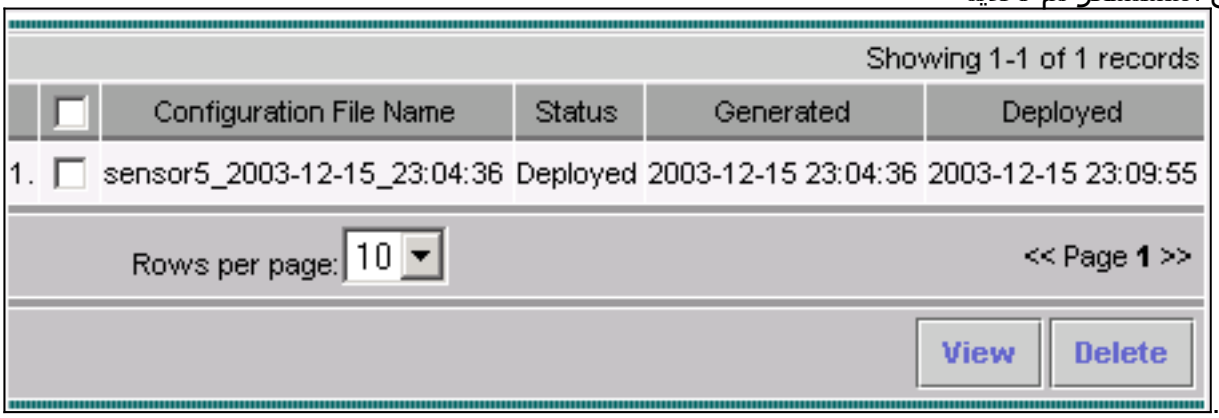


14. أدخل اسم الوظيفة وجدولة الوظيفة ك **فوري**، ثم انقر فوق

إنهاء.



15. أختر **نشر** > **نشر** > **تعليق**.انتظر بضع دقائق حتى يتم إكمال كافة المهام المعلقة. يجب أن تكون قائمة الانتظار فارغة.
16. أخترت **تشكيل>سجل** in order to أكدت النشر.تأكد من عرض حالة التكوين كما هو **منشور**. هذا يعني أن تكوين المستشعر تم تحديثه



بنجاح.

التحقق من الصحة

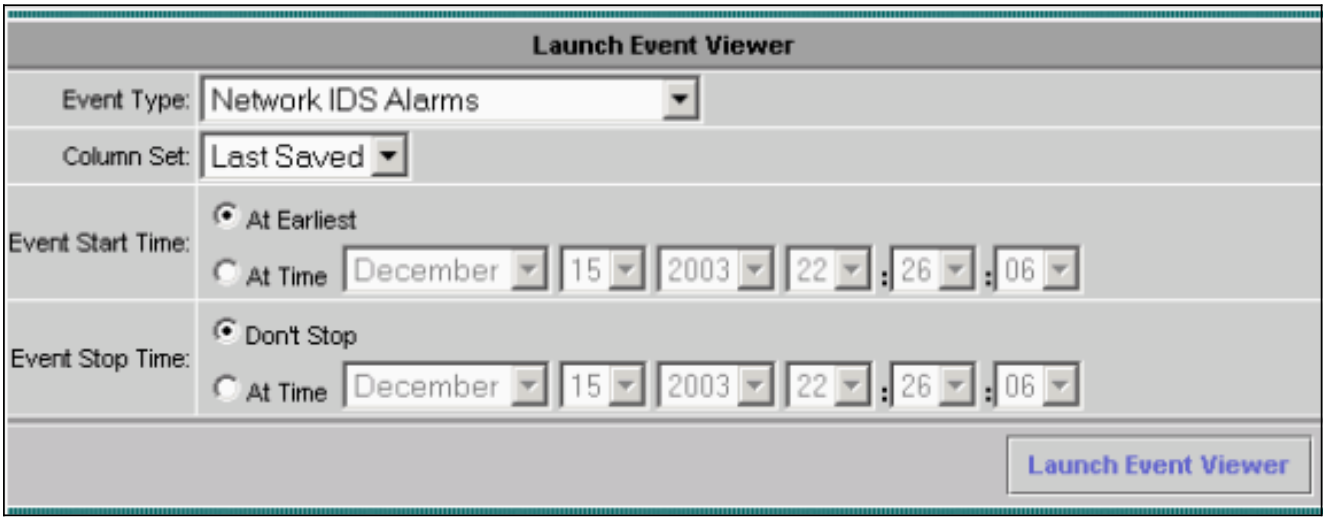
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تشغيل الهجوم وإعادة تعيين TCP

قم بتشغيل هجوم إختبار وفحص النتائج للتحقق من أن عملية الحظر تعمل بشكل صحيح.

1. قبل تشغيل الهجوم، أختر **VPN/حل إدارة الأمان > مركز المراقبة>مراقبة الأمان**.
2. أخترت **مدرب** من القائمة رئيسي وطقطقة **حدث**.
3. انقر على **تشغيل عارض**

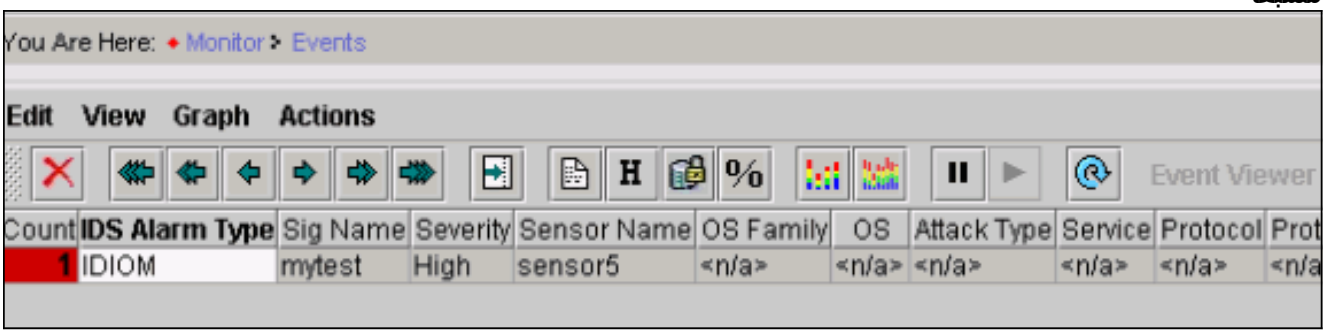
الأحداث.



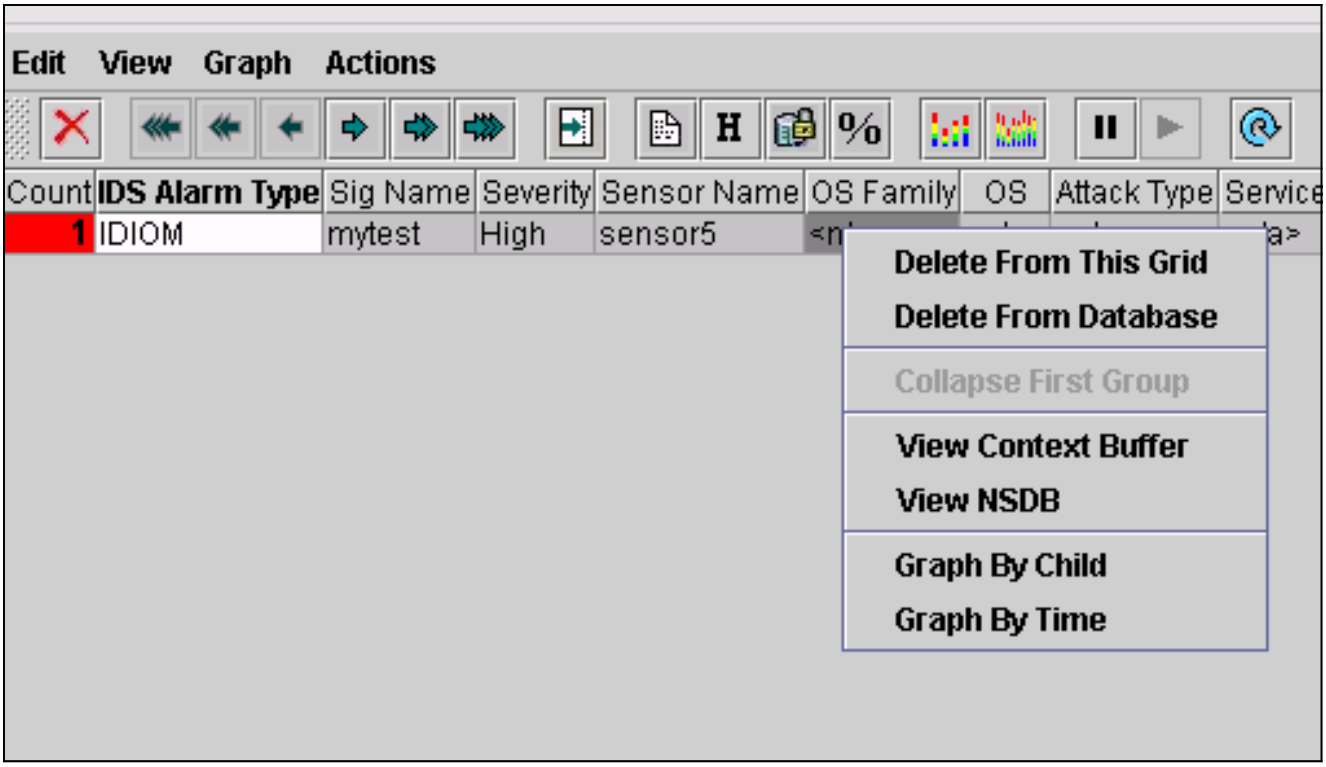
4. برنامج Telnet من موجه إلى آخر اكتب **testattack** لبدء الهجوم.في هذه الحالة، قمنا بالاتصال هاتفيا من "الضوء الموجه" إلى منزل الموجه. بمجرد ضغطك على **<space>** أو **<enter>**، بعد كتابة **testattack**، يجب إعادة تعيين جلسة عمل برنامج Telnet لديك.

```
light#telnet 100.100.100.1
Trying 100.100.100.1 ... Open
User Access Verification
:Password
house>en
:Password
house#testattack

The Telnet session is reset due to the !--- signature "testattack" being triggered. ---!
[[Connection to 100.100.100.1 lost
```

5. من عارض الأحداث، انقر فوق **قاعدة بيانات الاستعلام** للأحداث الجديدة الآن.ترى التنبيه للهجوم الذي تم شنه مسبقا



6. في "عارض الأحداث"، قم بتمييز التنبيه، وانقر بزر الماوس الأيمن فوقه وحدد إما **عرض المخزن المؤقت للسياق** أو **عرض NSDB** لعرض معلومات أكثر تفصيلا حول التنبيه.



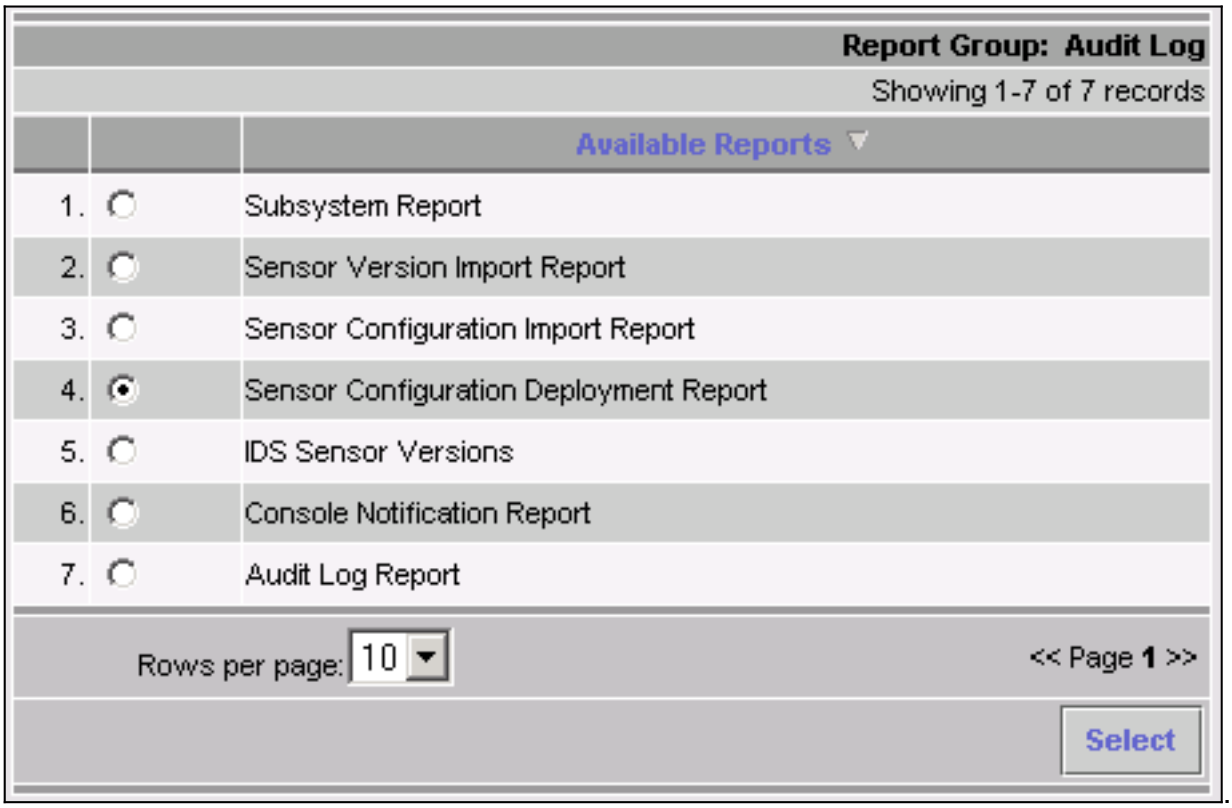
استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إجراء استكشاف الأخطاء وإصلاحها

أتمت هذا steps in order to تحريت.

1. في IDS MC، أختر **تقارير** > **إنشاء**.ورهنا بنوع المشكلة، ينبغي العثور على مزيد من التفاصيل في أحد التقارير السبعة



المتاحة.

2. بينما يستخدم الحظر منفذ الأمر والتحكم لتكوين قوائم الوصول إلى الموجه، يتم إرسال حزم TCP من واجهة التقاط المستشعر. ضمنت أنت يتلقى يجسر ال يصح ميناء، يستعمل **المجموعة فسحة بين دعامتين** أمر على المفتاح، مماثل إلى هذا:

```
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 ---!
In this case, connect to Ethernet1 of Router House. Oper Source : Port 2/12 ---!
Direction        : transmit/receive
Incoming Packets: enabled
Learning         : enabled
Multicast        : enabled
```

3. إذا لم تكن إعادة تعيين TCP تعمل، فأدخل إلى المستشعر وأدخل الأمر **show event**.قم بتشغيل الهجوم، وتحقق لمعرفة ما إذا تم تشغيل التنبيه أم لا. إذا تم تشغيل التنبيه، فتحقق للتأكد من ضبطه لإعادة تعيين نوع الإجراء **TCP**.

معلومات ذات صلة

- صفحة دعم اكتشاف التسلل الآمن من Cisco
- وثائق نظام اكتشاف الاقتحام الآمن من Cisco
- صفحة دعم حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN) من CiscoWorks
- 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).