IME مادختساب IPS رظح نيوكت

المحتويات

المقدمة

يناقش هذا المستند تكوين حظر نظام منع التسلل (IPS) باستخدام IME (IPS Manager Express). يتم إستخدام أجهزة الاستشعار IME و IPS لإدارة موجه Cisco لحظر البيانات. تذكر هذه العناصر عند مراعاة هذا التكوين:

- قم بتثبيت "أداة الاستشعار" وتأكد من عمل أداة الاستشعار بشكل صحيح.
- جعلت ال ينشق قارن فسحة بين دعامتين إلى المسحاج تخديد خارج القارن.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- Cisco IPS Manager Express 7.0
- مستشعر Cisco IPS 7.0(0.88)E3
- cisco ios ® مسحاج تخديد مع cisco ios برمجية إطلاق 12.4

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.

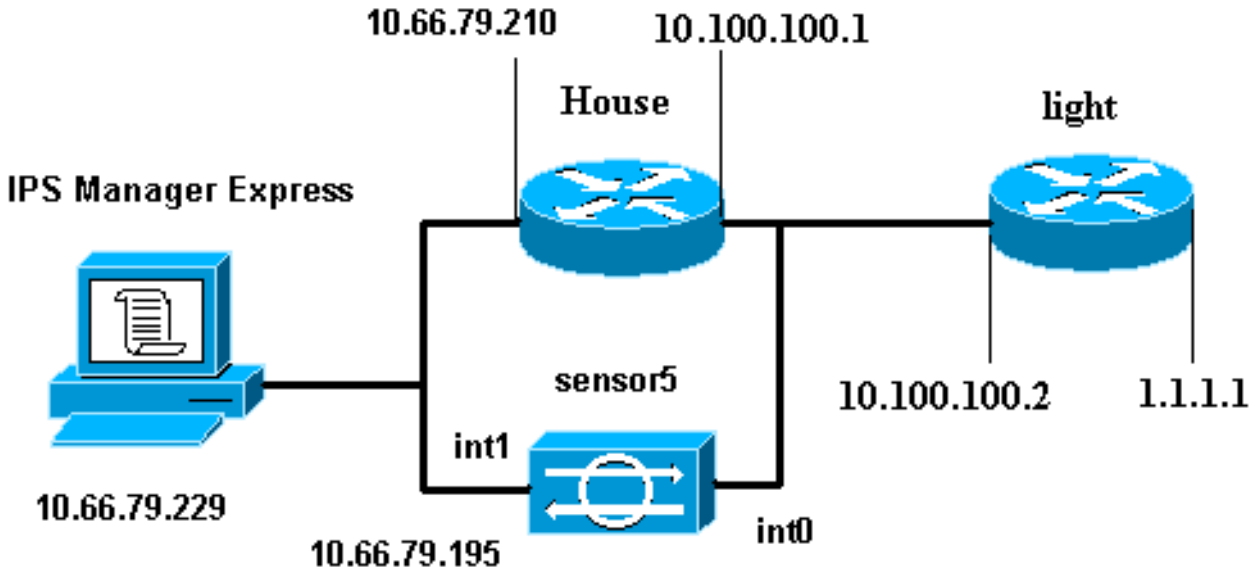
الاصطلاحات

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

التكوين

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 12.4
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 10.100.100.2 255.255.255.0
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 10.100.100.1
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 : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
logging queue-limit 100
enable password cisco
!
ip subnet-zero
!
!
no ip cef
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
!
interface FastEthernet0/0
ip address 10.66.79.210 255.255.255.224
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.100.100.1 255.255.255.0
ip access-group IDS_FastEthernet0/1_in_0 in
After you configure blocking, !--- IDS Sensor ---!
inserts this line. duplex auto speed auto ! interface
ATM1/0 no ip address shutdown no atm ilmi-keepalive ! 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 10.100.100.2
no ip http server
no ip http secure-server
!
!
ip access-list extended IDS_FastEthernet0/1_in_0
permit ip host 10.66.79.195 any
permit ip any any
After you configure blocking, !--- IDS Sensor ---!
inserts this line. ! call rsvp-sync ! ! mgcp profile
default ! ! line con 0 exec-timeout 0 0 line aux 0 line
vty 0 4 exec-timeout 0 0 password cisco
login
line vty 5 15
login
!
!
end
```

بدء تكوين المستشعر

أكمل هذه الخطوات لبدء تكوين المستشعر.

1. إذا كانت هذه هي المرة الأولى التي تقوم فيها بتسجيل الدخول إلى المستشعر، فيجب عليك إدخال **Cisco** كاسم المستخدم و**Cisco** ككلمة مرور.
2. عند مطالبة النظام لك، قم بتغيير كلمة المرور الخاصة بك.**ملاحظة:** Cisco123 هي كلمة قاموس ولا يسمح بها في النظام.
3. اكتب **setup** واتبع مطالبة النظام لإعداد المعلمات الأساسية لأجهزة الاستشعار.
4. أدخل هذه المعلومات:

```
sensor5#setup

                --- System Configuration Dialog ---

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

                Current time: Thu Oct  22 21:19:51 2009

                    :Setup Configuration last modified

                                :[Enter host name[sensor
:[Enter IP interface[10.66.79.195/24,10.66.79.193

                            :[Modify current access list?[no
                                :Current access list entries
permit the ip address of workstation or network with IME Permit:10.66.79.0/24 ---!
                                                        :Permit
                                :[Modify system clock settings?[no
                                :[Modify summer time settings?[no
                                :[Use USA SummerTime Defaults?[yes
                            :[Recurring, Date or Disable?[Recurring
                                        :[Start Month[march
                                        :[Start Week[second
                                         :[Start Day[sunday
                                    :[Start Time[02:00:00
                                     :[End Month[november
                                        :[End Week[first
                                        :[End Day[sunday
                                     :[End Time[02:00:00
                                            :[]DST Zone
                                            :[Offset[60
                                :[Modify system timezone?[no
                                            :[Timezone[UTC
                                            :[UTC Offset[0
                                          Use NTP?[no]: yes
                                    :[]NTP Server IP Address
                                Use NTP Authentication?[no]: yes
                                            NTP Key ID[]: 1
                                    NTP Key Value[]: 8675309
```

5. قم بحفظ التكوين.قد يستغرق المستشعر بضع دقائق لحفظ التكوين.

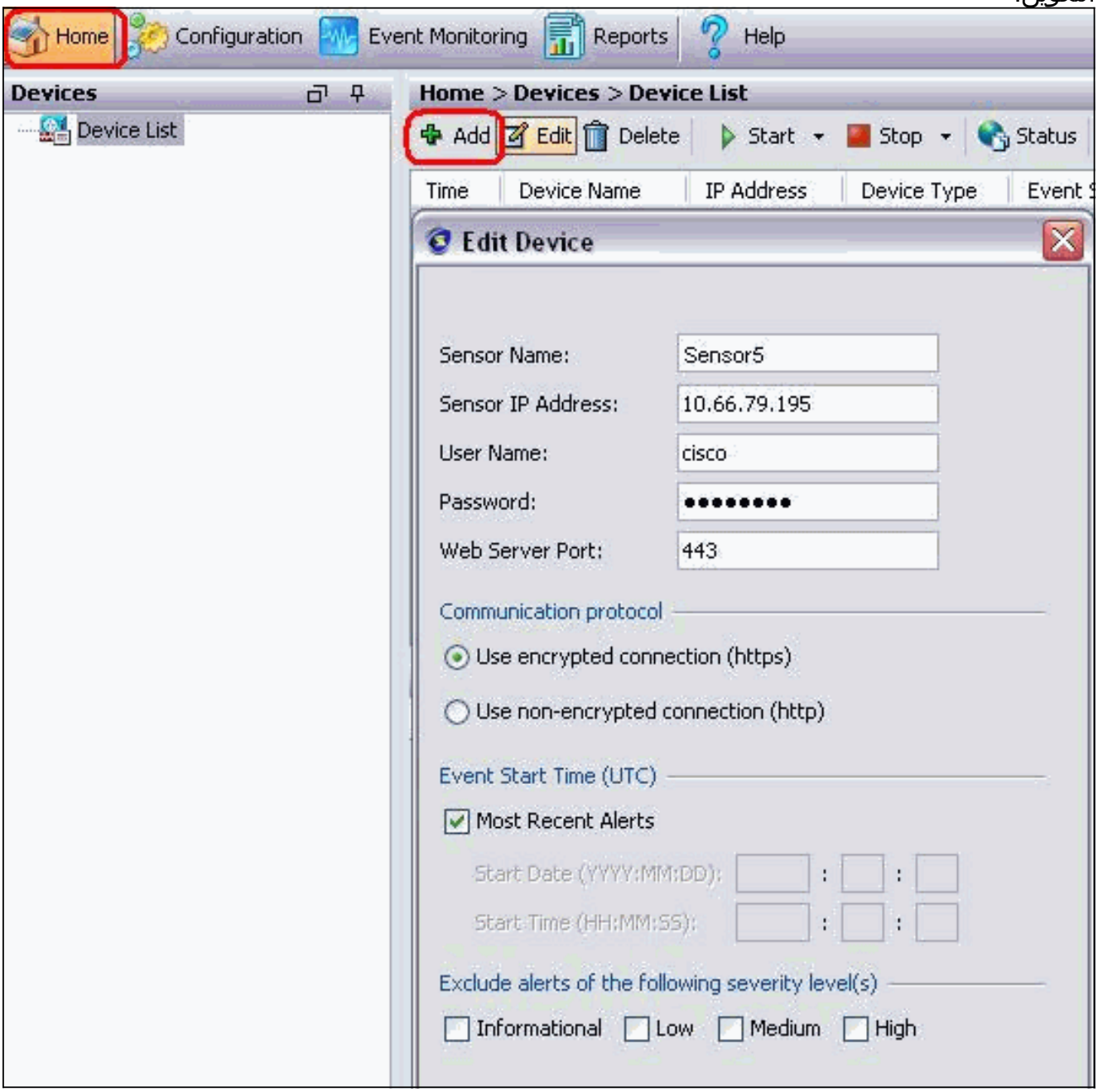
```
.Go to the command prompt without saving this config [0]
.Return back to the setup without saving this config [1]
.Save this configuration and exit setup [2]

                                Enter your selection[2]: 2
```

إضافة المستشعر إلى IME

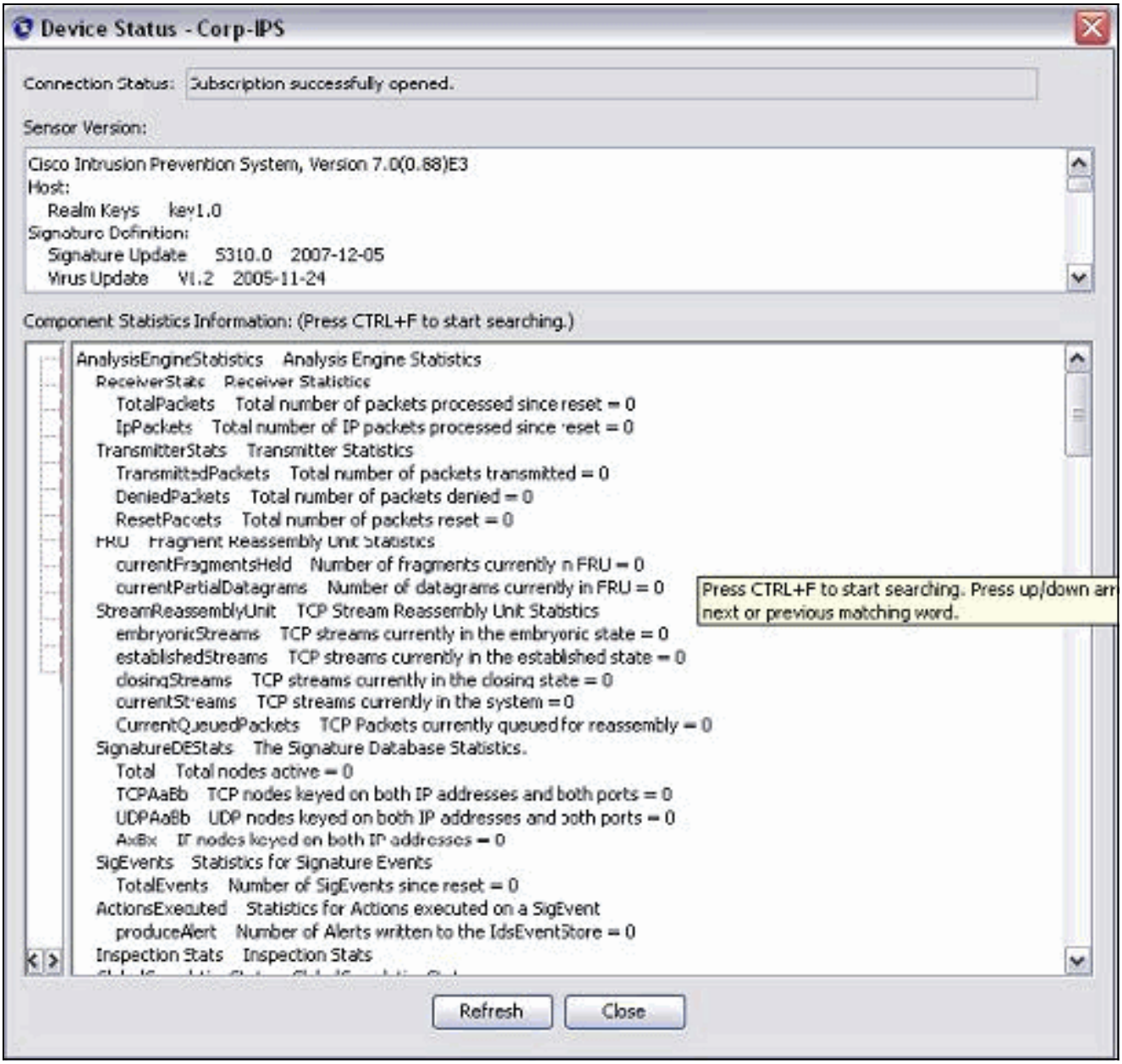
أكمل هذه الخطوات لإضافة المستشعر إلى IME.

1. انتقل إلى جهاز كمبيوتر Windows الذي قام بتثبيت IPS Manager Express وافتح **IPS Manager Express**.

2. أختر **الصفحة الرئيسية > إضافة**.
3. اكتب في هذه المعلومات وانقر فوق **موافق** لإنهاء التكوين.



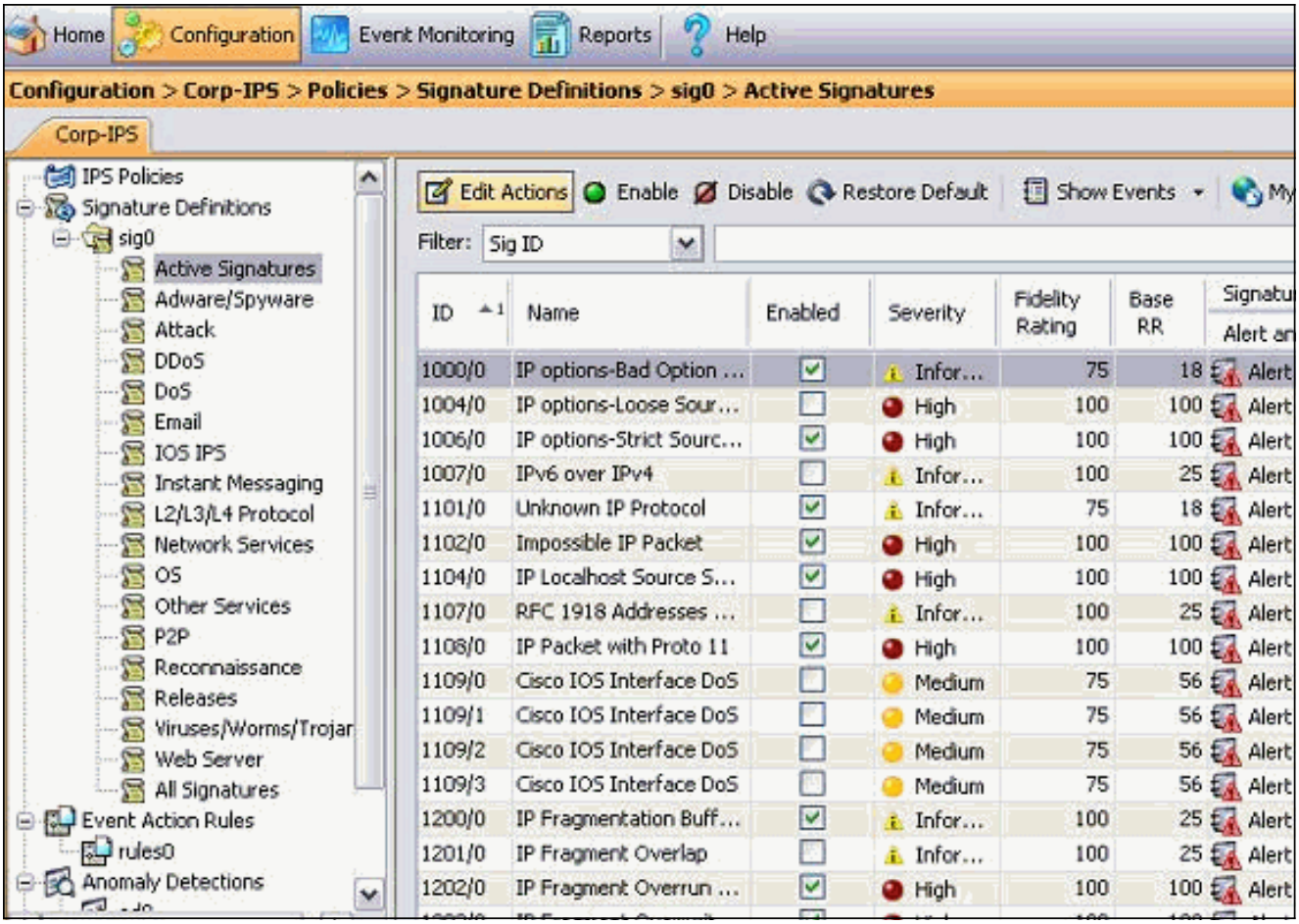
4. أختر **أجهزة > مستشعر 5** للتحقق من حالة المستشعر ثم انقر بزر الماوس الأيمن لاختيار **الحالة**.تأكد من إمكانية مشاهدة *فتح الاشتراك بنجاح*. الرسالة.



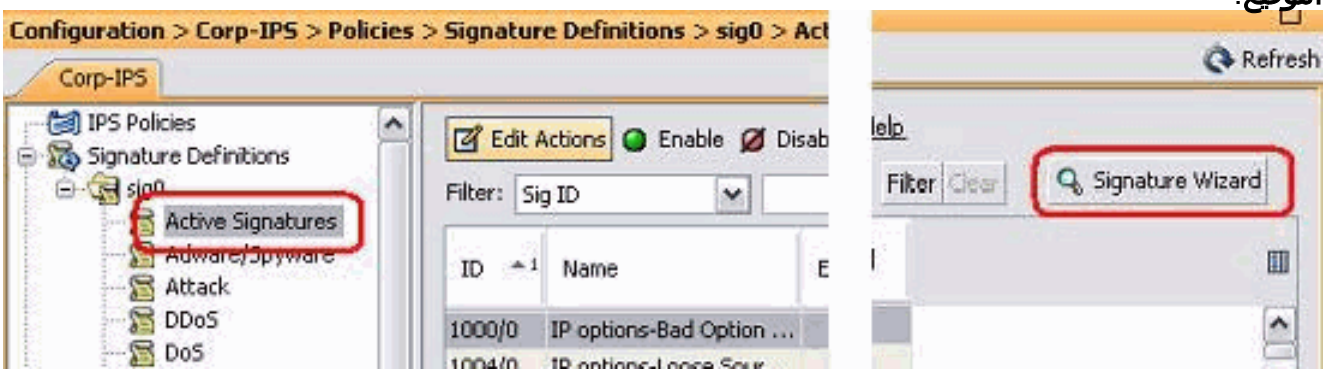
تكوين الحظر لموجه Cisco IOS

أكمل هذه الخطوات لتكوين الحظر للمسار Cisco IOS:.

1. من جهاز IME، افتح مستعرض الويب وانتقل إلى **https://10.66.79.195**.
2. انقر على **موافق** لقبول شهادة HTTPS التي تم تنزيلها من المستشعر.
3. في نافذة تسجيل الدخول، أدخل **Cisco** لاسم المستخدم و**123cisco123** لكلمة المرور.تظهر واجهة إدارة IME هذه:

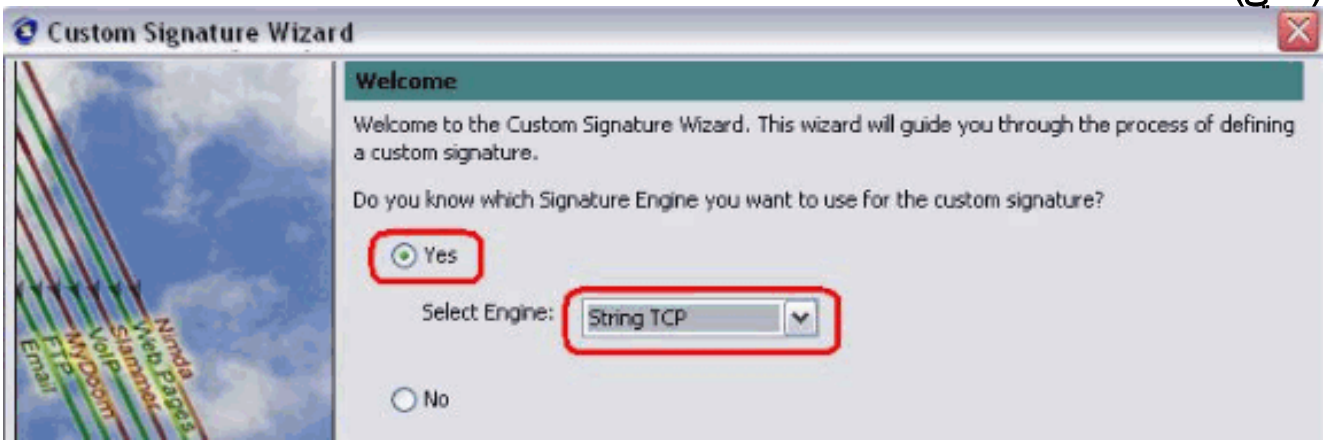


4. من علامة التبويب تكوين، انقر فوق **التوقيعات النشطة**.
5. بعد ذلك، انقر فوق **معالج التوقيع**.



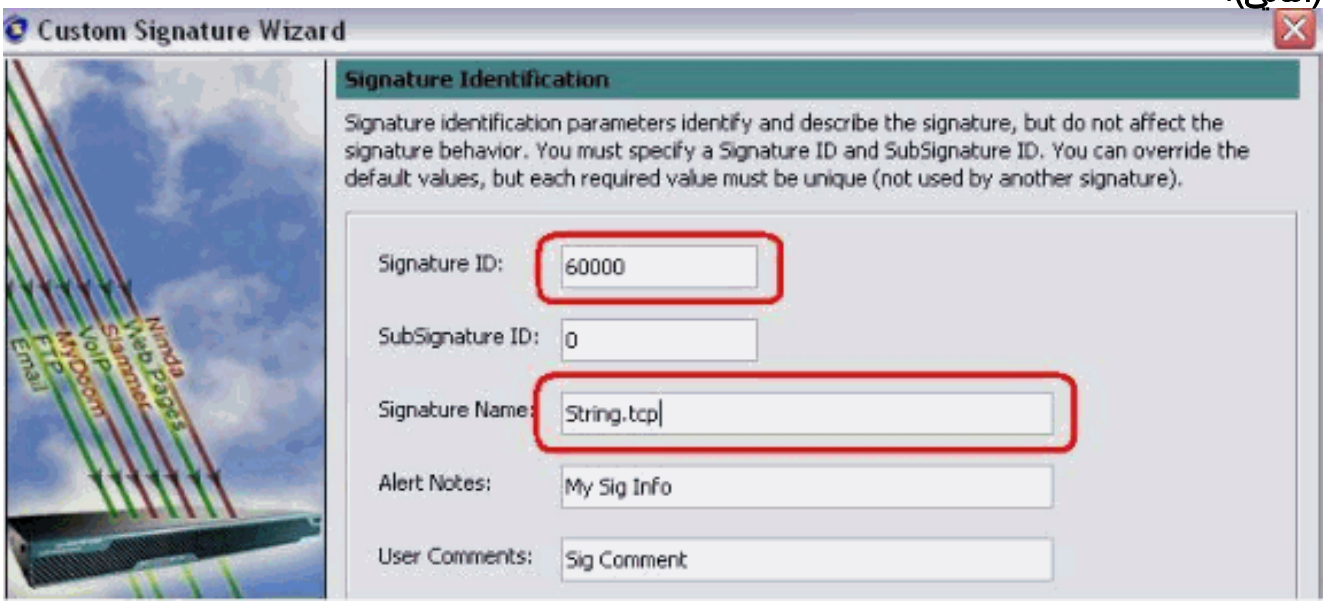
ملاحظة: تم قص لقطة الشاشة السابقة إلى جزئين بسبب ضيق المساحة.

6. أخترت **نعم** و**خيط TCP** كتوقيع محرك. انقر فوق **Next (التالي)**.

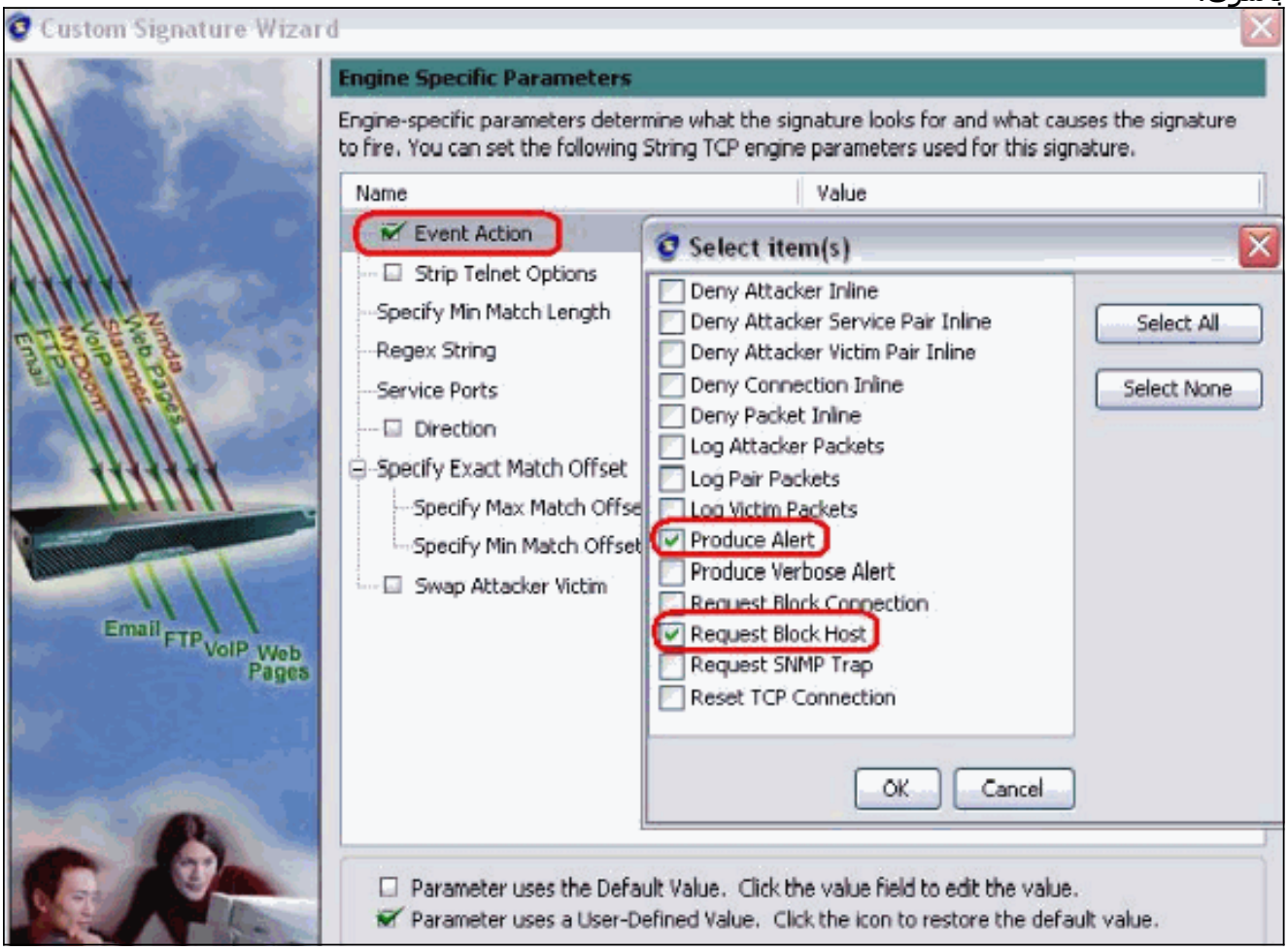


7. يمكنك ترك هذه المعلومات كافتراضي أو إدخال معرف التوقيع واسم التوقيع وملاحظات المستخدم الخاصة بك.

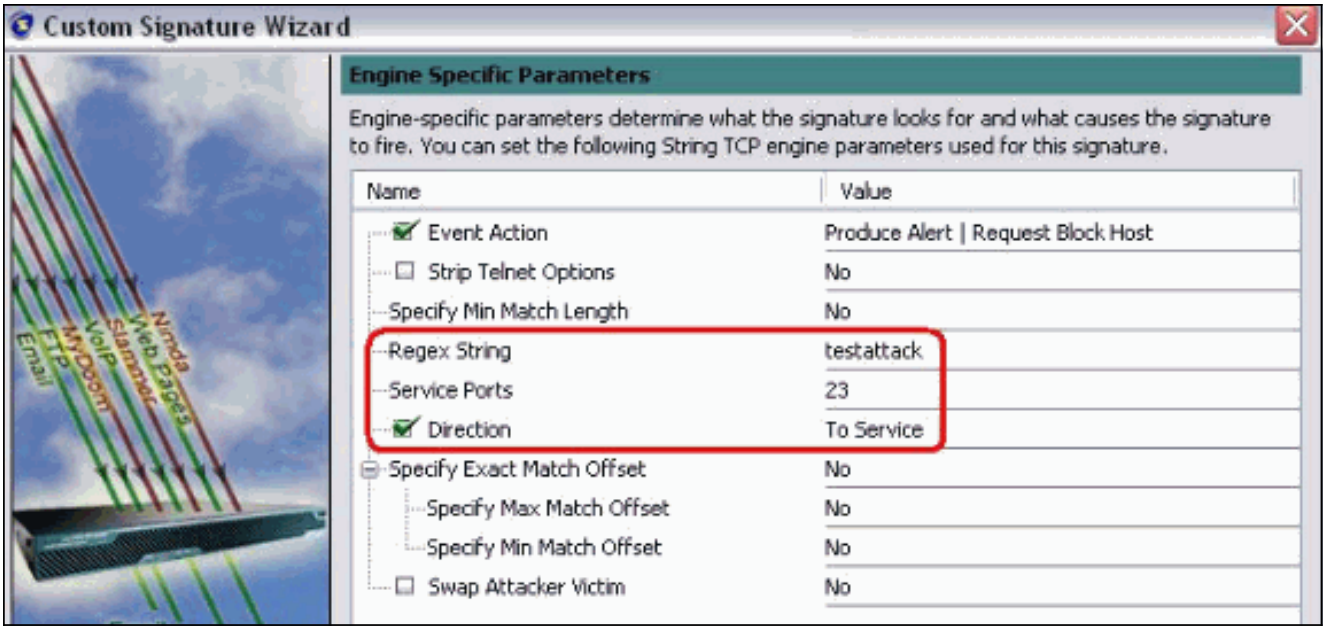
انقر فوق **Next** (**التالي**).



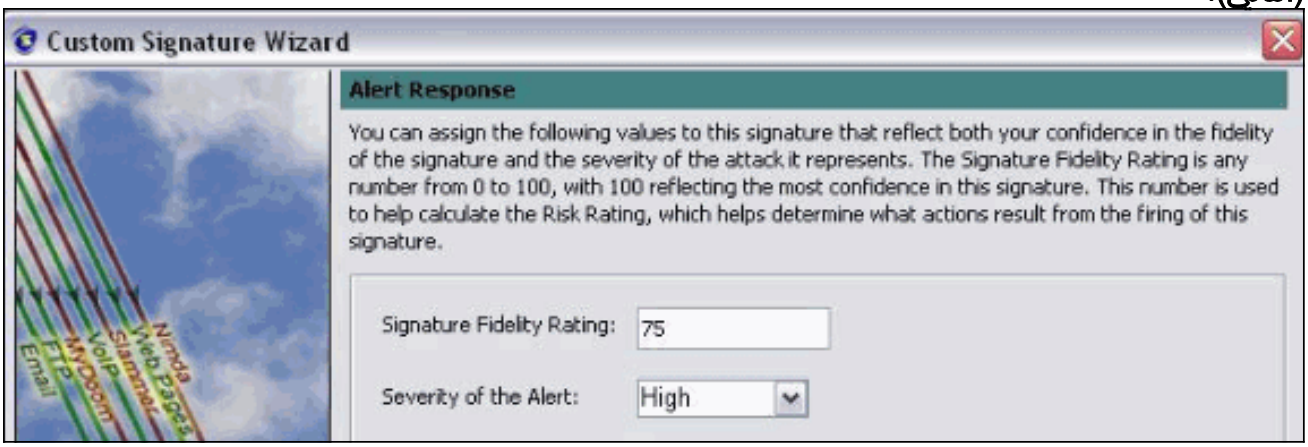
8. أخترت **حدث إجراء** واخترت **إنتاج تنبيه** و **طلب قالب مضيف**. طقطقت **بعد ذلك** in order to باشرت.



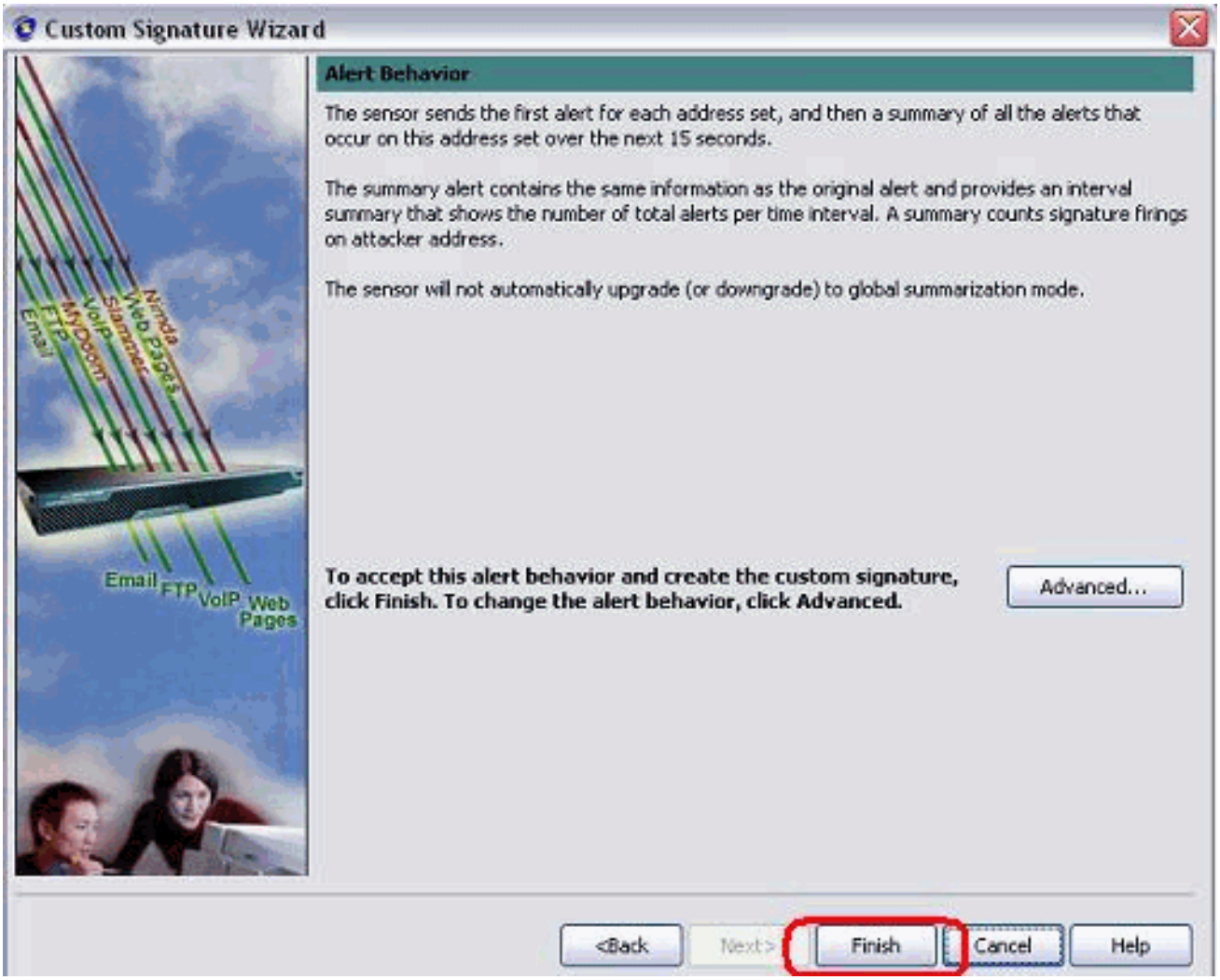
9. دخلت تعبير عادي، أي في هذا مثال **23**، *testattack* ل خدمة ميناء، أخترت **أن خدمة** ل الإتجاه، وطقطقة **بعد ذلك** in order to تابعت.



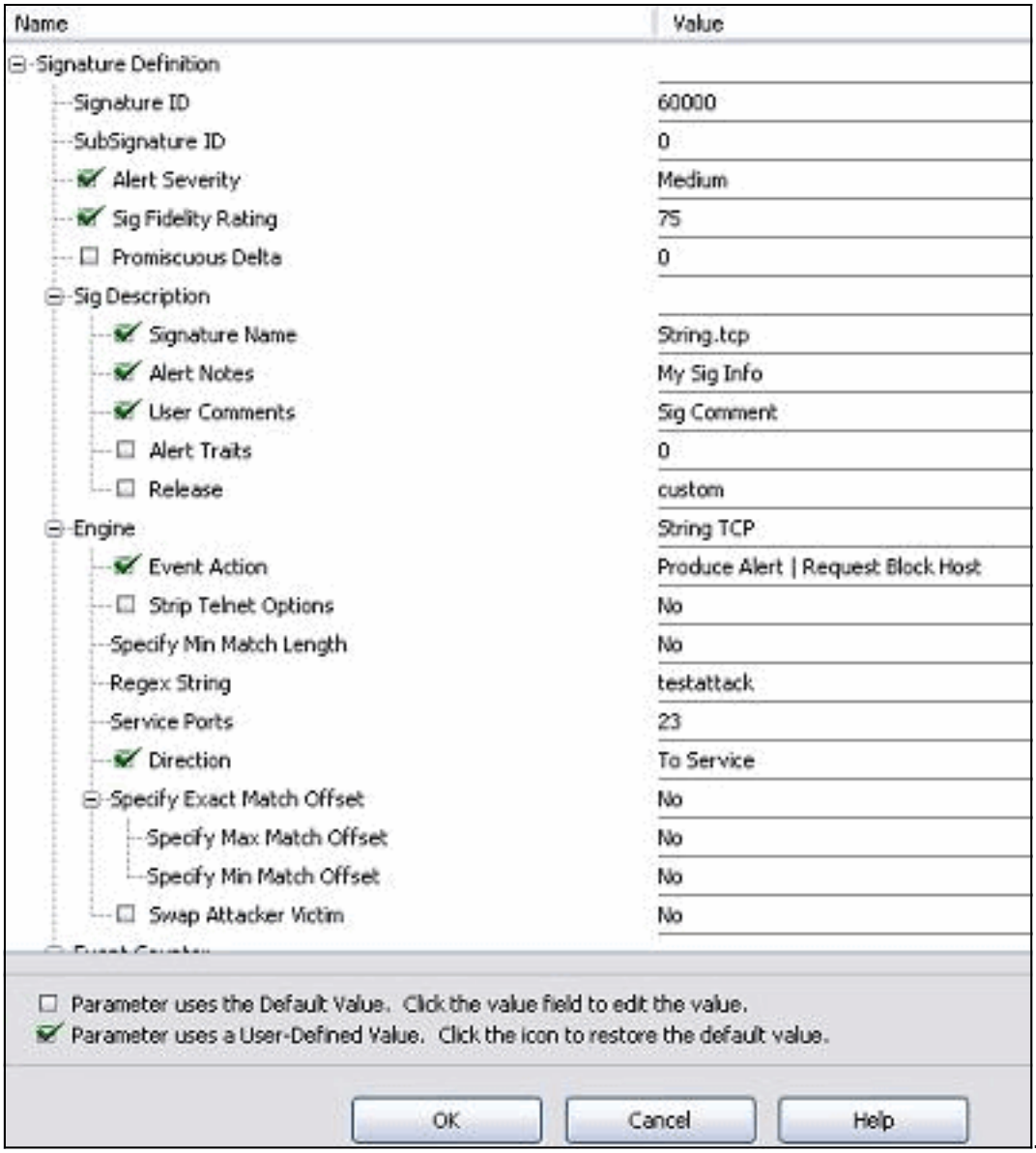
10. يمكنك ترك هذه المعلومات كافتراضي. انقر فوق **Next (التالي)**.



11. طقطقة **إنجاز** in order to أنهيت المعالج.

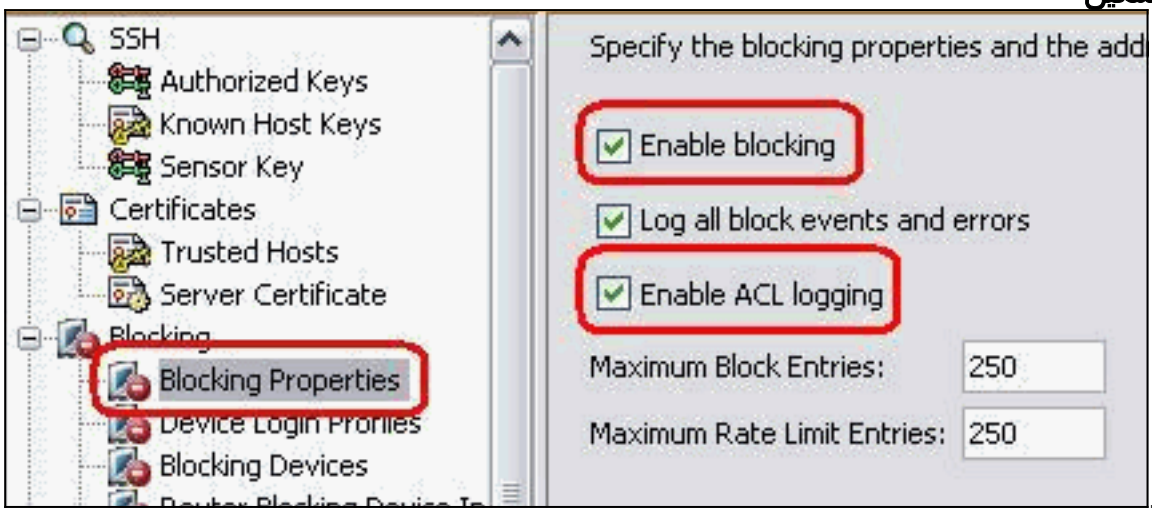


12. أخترت **تشكيل > sig0>توقيع نشط** in order to حددت ال newly created توقيع ب **sig id** أو **sig name**.
طقطقة **يحرر** in order to شاهدت



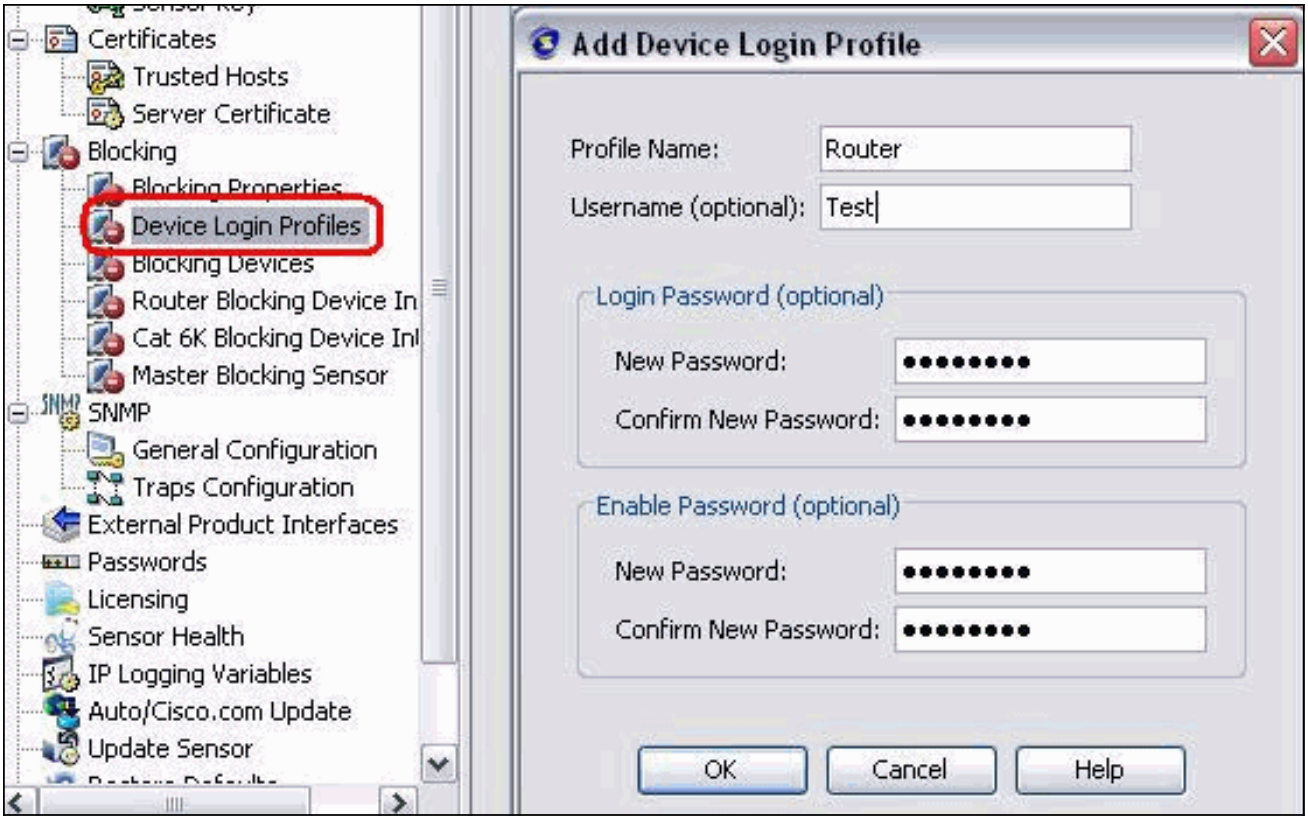
التوقيع.

13. طقطقة **ok** بعد أن يؤكد أنت ويطقطق **ال apply** زر in order to طبقت التوقيع إلى المستشعر.
14. من علامة التبويب "تكوين"، وتحت "إدارة المستشعر"، انقر فوق **حظر**. من الجزء الأيسر، أختر **خصائص الحظر** وحدد **تمكين**

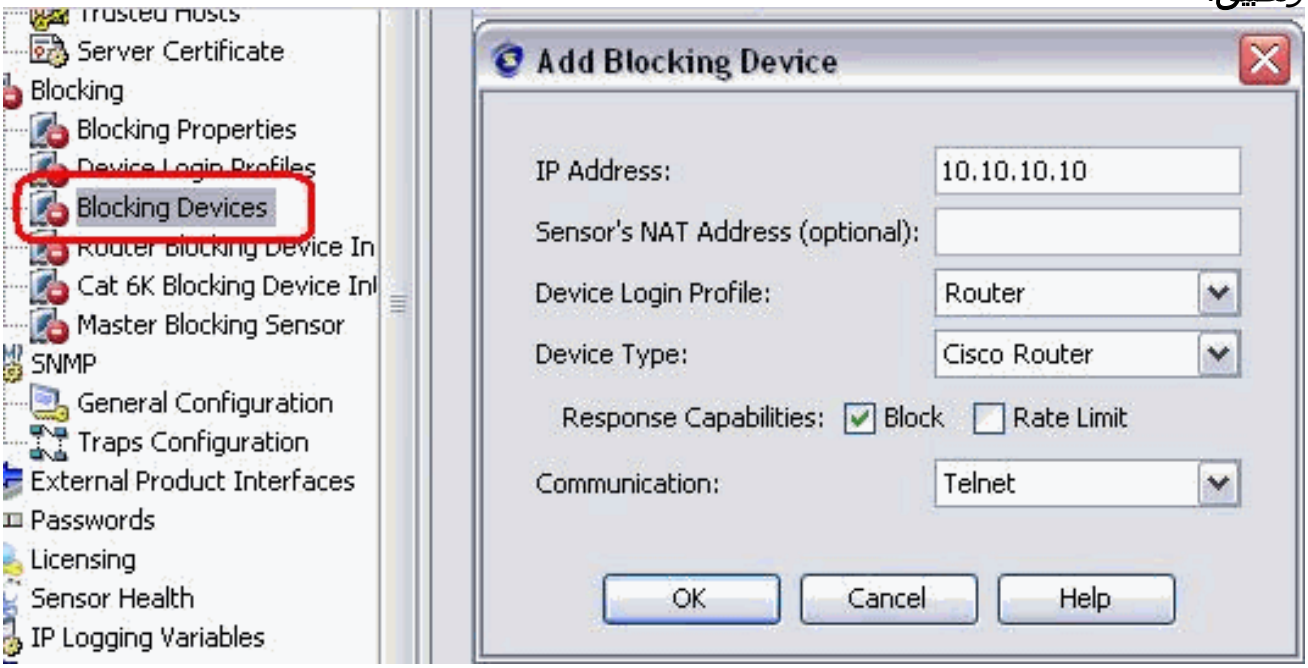


الحظر.

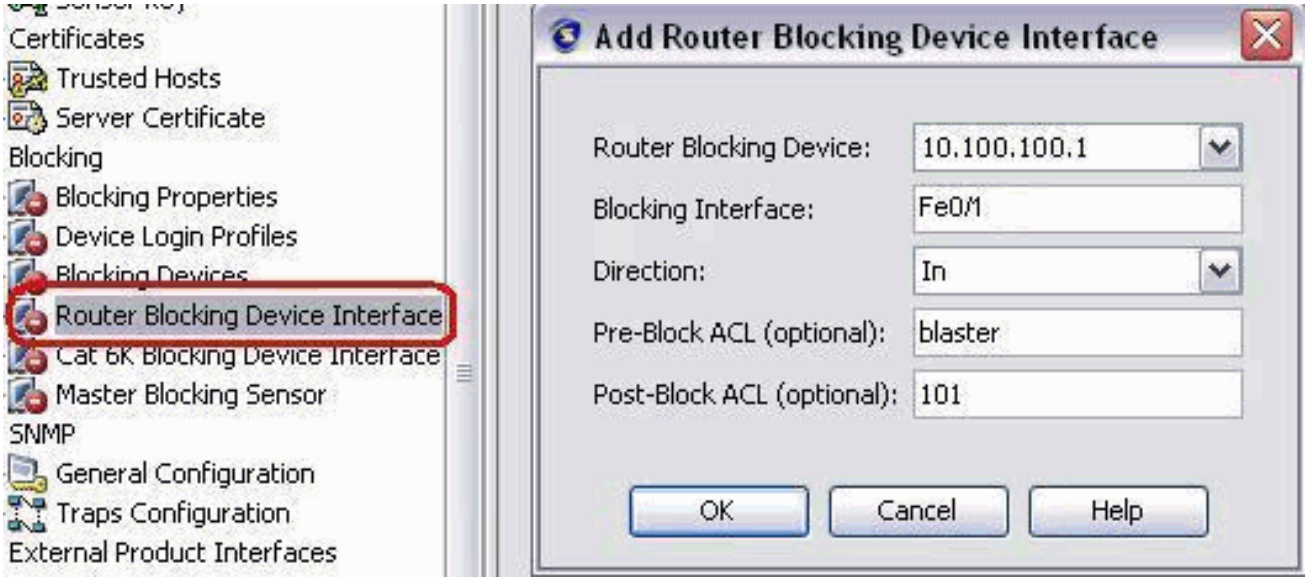
15. انتقل الآن من الجزء الأيسر إلى **ملف تعريف تسجيل دخول الجهاز**. طقطقة in order to خلقت توصيف جديد، **يضيف**. طقطقة ما إن يخلق **ok** **ويطبق** in order to مستشعر وتابع.



16. تتمثل الخطوة التالية في تكوين الموجه كجهاز حظر. من الجزء الأيسر، أختر **حظر الجهاز**، انقر فوق **إضافة** لإضافة هذه المعلومات. ثم انقر فوق **موافق** و**تطبيق**.



17. الآن من الجزء الأيسر قم بتكوين واجهات جهاز الحظر. إضافة المعلومات، انقر فوق **موافق** و**تطبيق**.



التحقق من الصحة

شن الهجوم والعرقلة

أكمل الخطوات التالية لإطلاق الهجوم والحجب:

1. قبل أن تقوم بتشغيل الهجوم، انتقل إلى IME، واختر **مراقبة الحدث > عرض الهجمات التي تم إسقاطها** واختر المستشعر من الجانب الأيمن.
2. Telnet إلى منزل الموجه والتحقق من الاتصال من الخادم باستخدام هذه الأوامر.

```
house#show user

  Line      User       Host(s)          Idle        Location
                    con 0              idle          00:00:00 0 *
vty 0                idle          00:00:17     10.66.79.195 226


                                                house#show access-list
                                Extended IP access list IDS_FastEthernet0/1_in_0
                                                    permit ip host 10.66.79.195 any
                                                     (permit ip any any (12 matches
                                                                        #house
```

3. من إضاءة الموجه، ومن برنامج Telnet إلى منزل الموجه ونوع **هجوم التجربة**.اضغط إما **<space>** أو **<enter>** لإعادة ضبط جلسة عمل برنامج Telnet.

```
                                                light#telnet 10.100.100.1
                                                Trying 10.100.100.1 ... Open

                                                User Access Verification
                                                                :Password
                                                                 house>en
                                                                :Password
                                                            house#testattack
                                                [Connection to 10.100.100.1 lost]
Host 10.100.100.2 has been blocked due to the !--- signature "testattack" ---!
                                                                .triggered
```

4. قم باستخدام برنامج Telnet إلى منزل الموجه واستخدم الأمر **show access-list** كما هو موضح هنا.

```
                                                house#show access-list
                                Extended IP access list IDS_FastEthernet0/1_in_0
                                                    permit ip host 10.66.79.195 any 10
                                (deny ip host 10.100.100.2 any (71 matches 20
                                                    permit ip any any 30
```

5. من لوحة المعلومات الخاصة بعارض أحداث IDS، يظهر الإنذار الأحمر بمجرد تشغيل الهجوم.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

نصائح

أستخدم تلميحات أستكشاف المشكلات وإصلاحها التالية:

- من المستشعر نظر في إخراج **show statistics access** إلى الشبكة وتأكد من أن نشطة. من وحدة التحكم أو SSH إلى المستشعر، يتم عرض هذه المعلومات:

```
sensor5#show statistics network-access
                    Current Configuration
                AllowSensorShun = false
                  ShunMaxEntries = 100
                               NetDevice
                        Type = Cisco
                      IP = 10.66.79.210
                      NATAddr = 0.0.0.0
                Communications = telnet
                           ShunInterface
            InterfaceName = FastEthernet0/1
                InterfaceDirection = in
                                        State
                    ShunEnable = true
                               NetDevice
                      IP = 10.66.79.210
            AclSupport = uses Named ACLs
                        State = Active
                             ShunnedAddr
                                 Host
                IP = 10.100.100.2
                  ShunMinutes = 15
              MinutesRemaining = 12
                                 sensor5#
```

- تأكد من أن معلمة الاتصال توضح أنه يتم إستخدام البروتوكول الصحيح مثل Telnet أو SSH مع 3DES. يمكنك تجربة بروتوكول SSH أو Telnet يدويا من عميل SSH/Telnet على جهاز كمبيوتر للتحقق من صحة بيانات اعتماد اسم المستخدم وكلمة المرور. ثم حاول إستخدام Telnet أو SSH من المستشعر نفسه إلى الموجه وانظر ما إذا كان يمكنك تسجيل الدخول بنجاح إلى الموجه.

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).