تكوين إعادة تعيين IPS TCP باستخدام IME

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
التكوينات
بدء تكوين المستشعر
إضافة المستشعر إلى IME
تكوين إعادة تعيين TCP لموجه Cisco IOS
التحقق من الصحة
تشغيل الهجوم وإعادة تعيين TCP
استكشاف الأخطاء وإصلاحها
نصائح
معلومات ذات صلة

المقدمة

يناقش هذا المستند تكوين إعادة تعيين TCP لنظام منع التسلل (IPS) باستخدام IME (IPS Manager Express). يتم إستخدام أجهزة إستشعار IME و IPS لإدارة موجه Cisco لإعادة تعيين TCP. عند مراجعة هذا التكوين، تذكر العناصر التالية:

- 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 المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

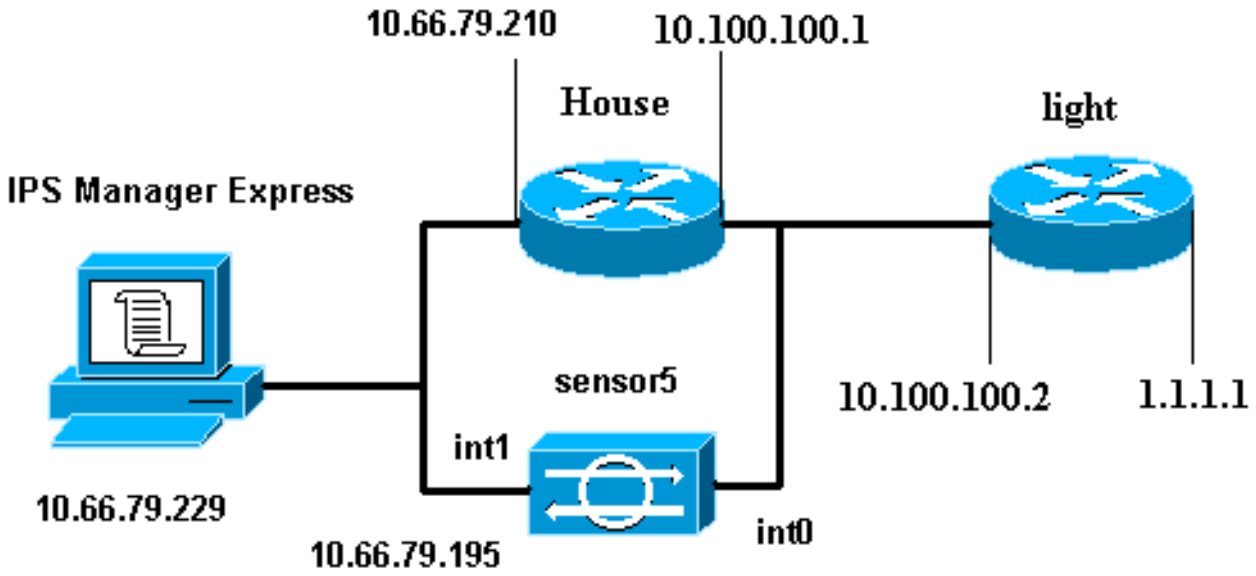
الاصطلاحات

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

التكوين

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



التكوينات

يستخدم هذا المستند التكوينات الموضحة هنا.

- 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
 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
!
!
!
!
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 وCisco 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 وأكمل 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 Configuration

                                        networkParams
                                    ipAddress 10.66.79.195
                                   netmask 255.255.255.224
                               defaultGateway 10.66.79.193
                                        hostname Corp-IPS
                                    telnetOption enabled
Permit the IP address of workstation or network with IME 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
```

5. قم بحفظ التكوين.قد يستغرق الأمر بضع دقائق حتى يتمكن المستشعر من حفظ التكوين.

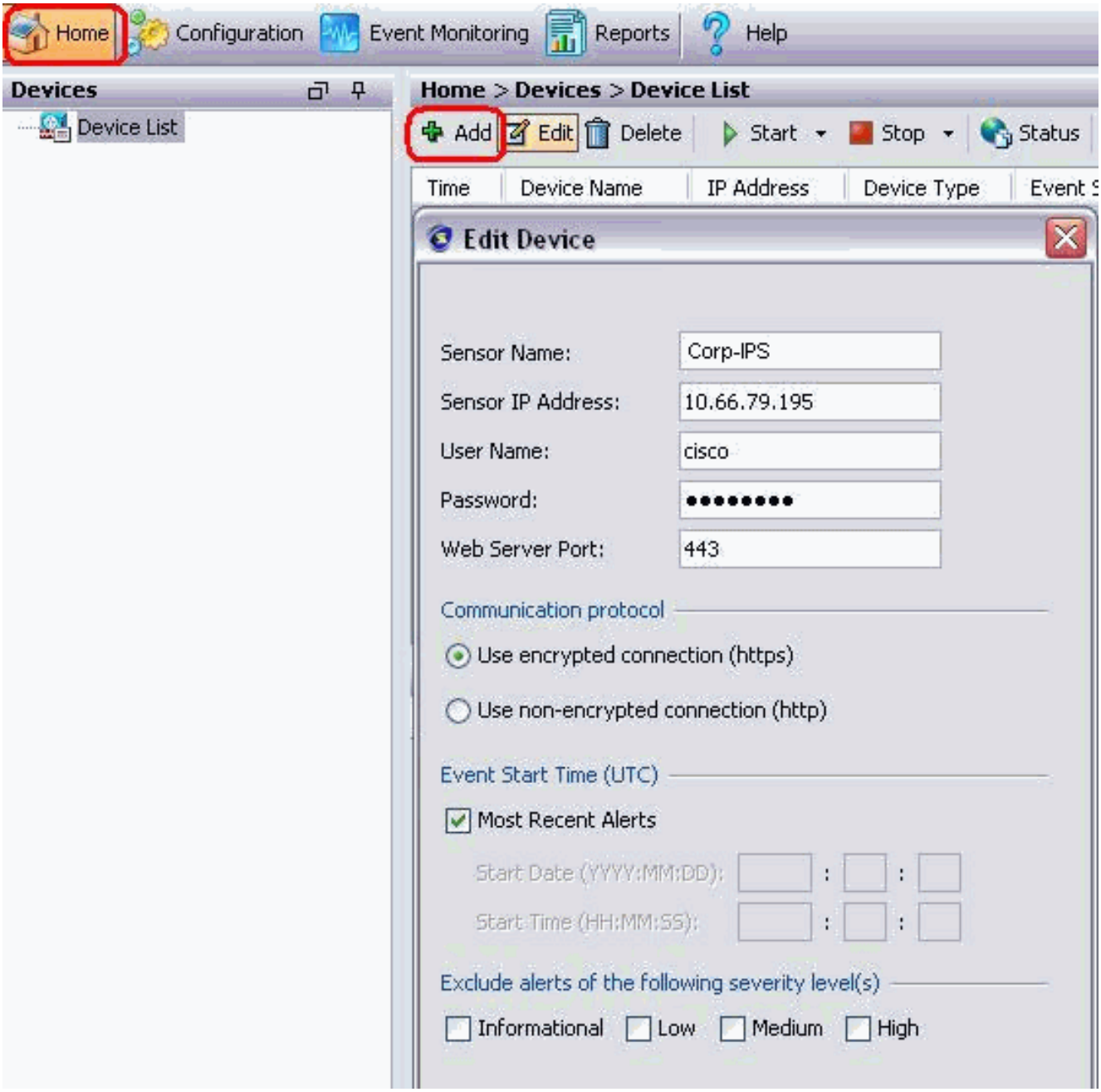
```
.Go to the command prompt without saving this config [0]
.Return back to the setup without saving this config [1]
.Save this configuration and exit setup [2]

                                Enter your selection[2]: 2
```

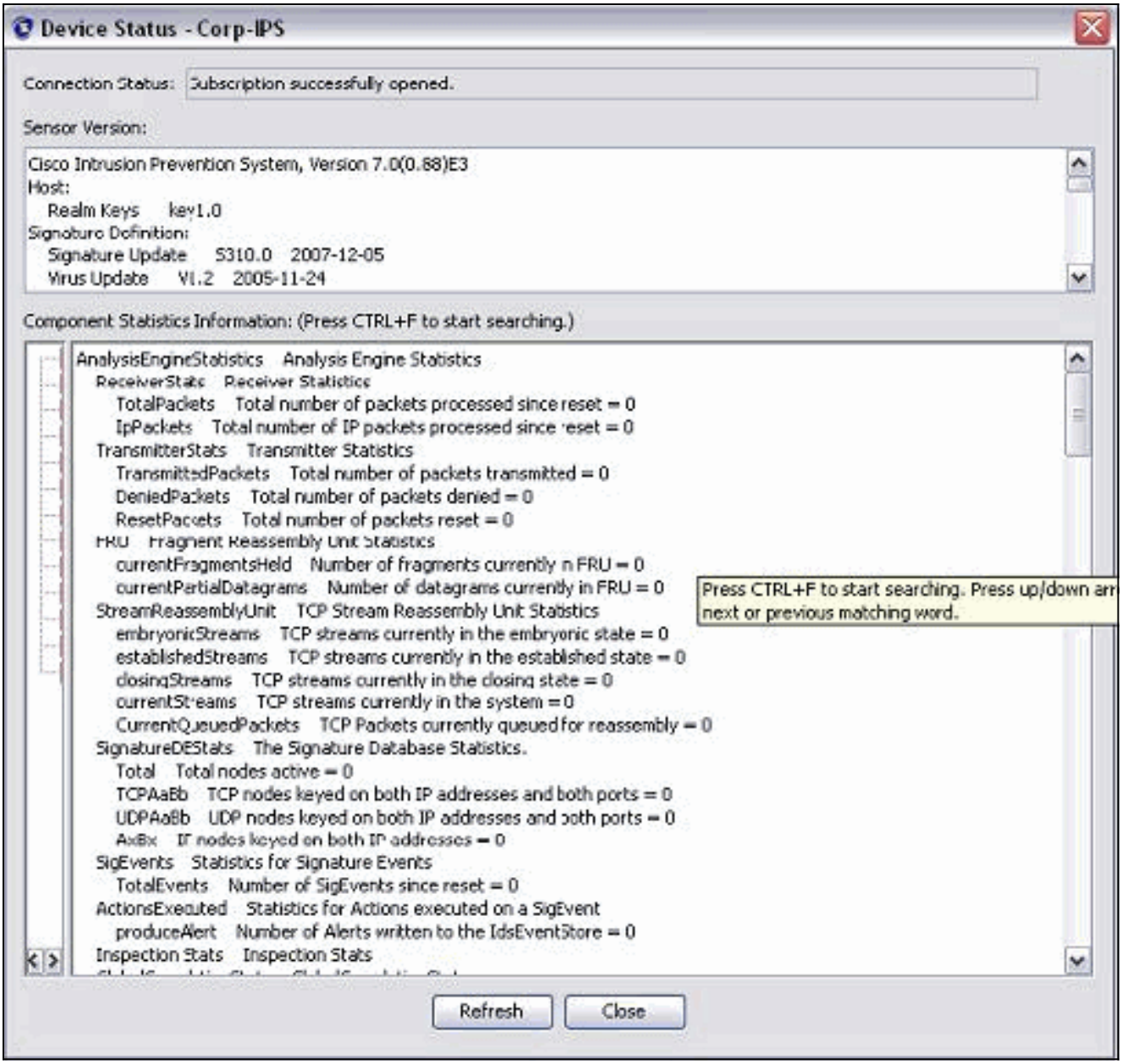
إضافة المستشعر إلى IME

أتمت هذا steps in order to أضفت المستشعر داخل IME:

1. انتقل إلى Windows PC الذي قام بتثبيت IPS Manager Express، وافتح IPS Manager Express.
2. أختر **الصفحة الرئيسية > إضافة**
.



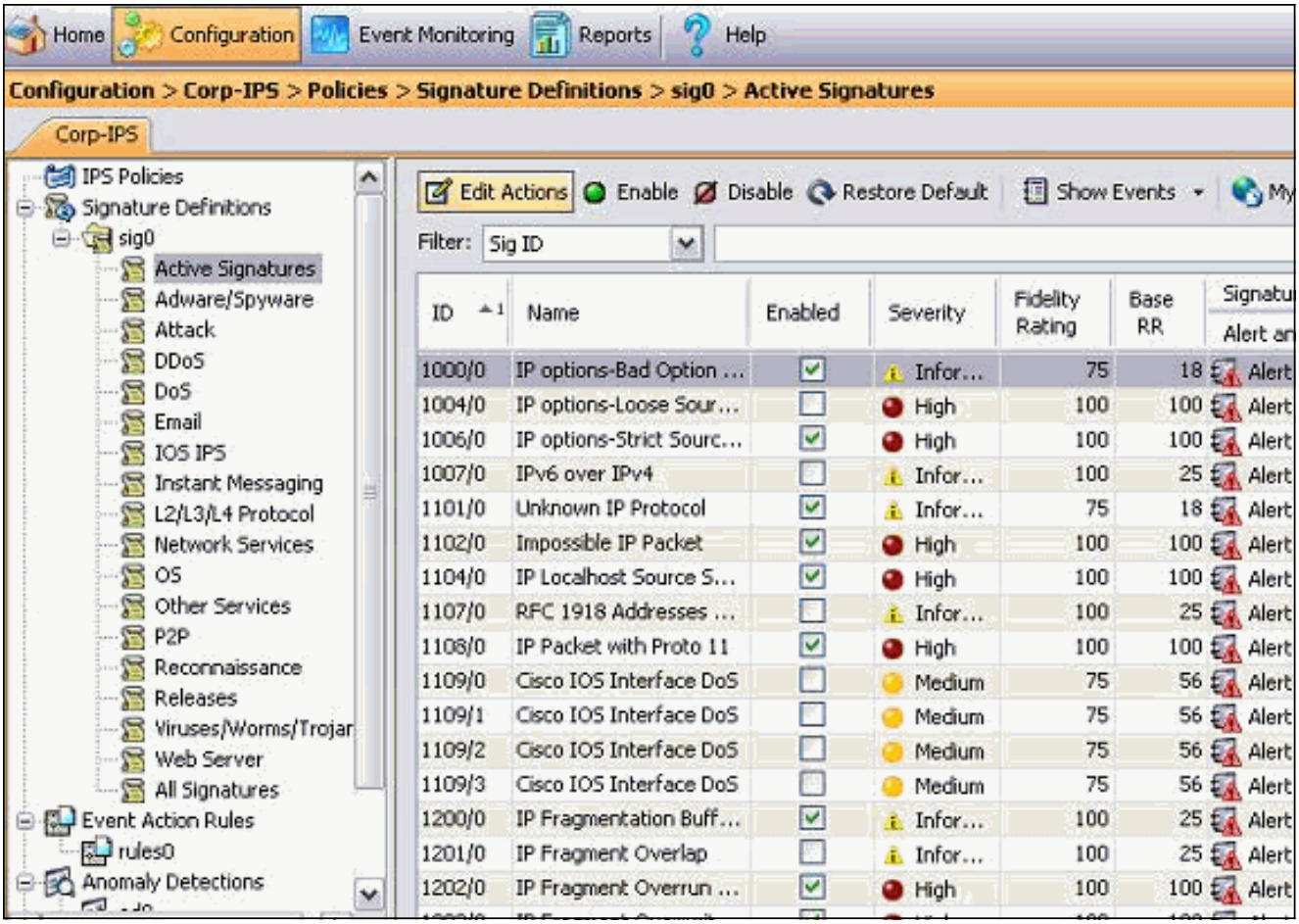
3. اكتب في هذه المعلومات وانقر فوق **موافق** لإنهاء التكوين.
4. أخترت **أداة>**Corp-IPS in order to دقةت المستشعر وضع وبعد ذلك déclic in order to أخترت **أداة وضع**.تأكد من إمكانية مشاهدة
.



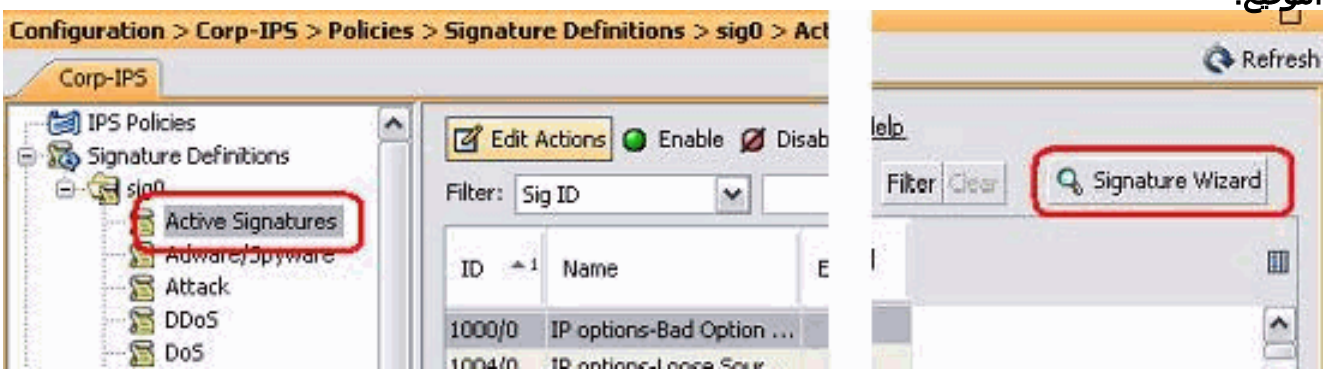
تكوين إعادة تعيين TCP لموجه Cisco IOS

أكمل هذه الخطوات لتكوين إعادة تعيين TCP لموجه Cisco IOS:

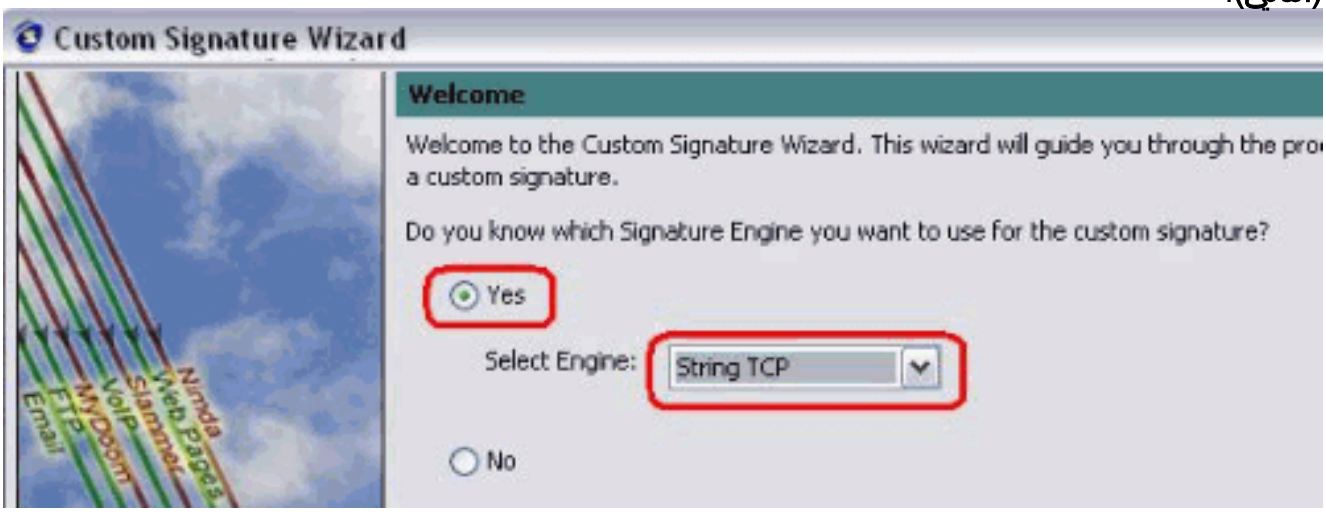
1. من جهاز IME، افتح مستعرض الويب وانتقل إلى **https://10.66.79.195**.
2. انقر على **موافق** لقبول شهادة HTTPS التي تم تنزيلها من المستشعر.
3. في نافذة تسجيل الدخول، أدخل **Cisco** لاسم المستخدم و**123cisco123** لكلمة المرور.تظهر واجهة إدارة IME هذه:



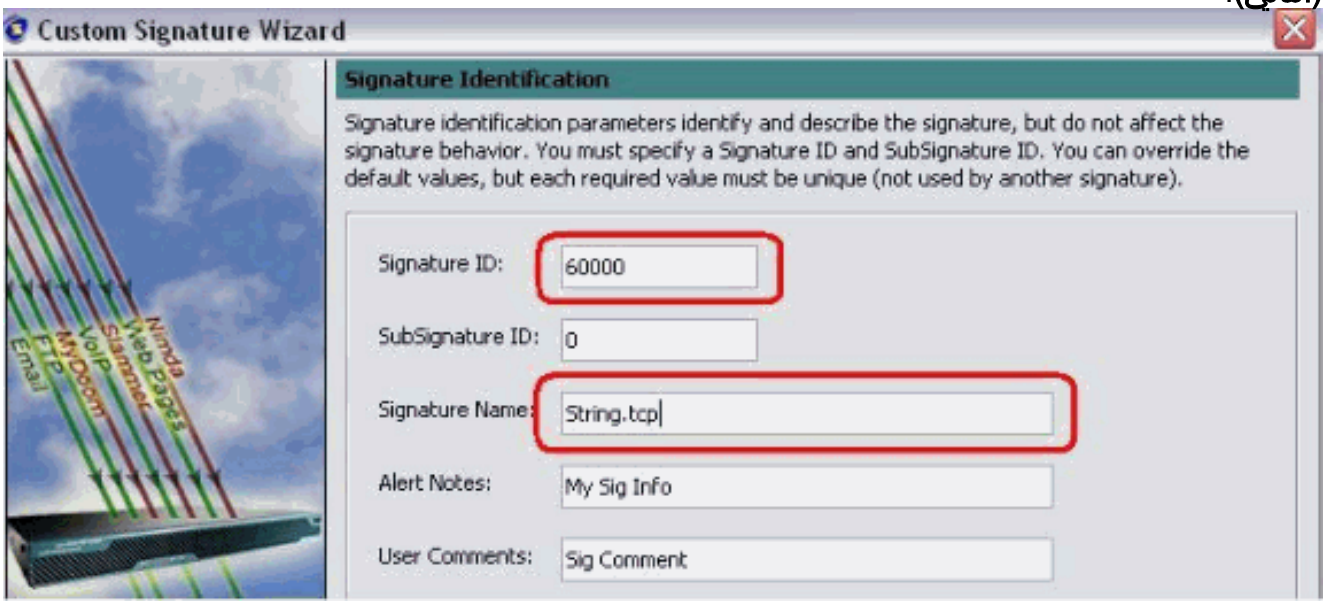
4. من علامة التبويب تكوين، انقر فوق **التوقيعات النشطة**.
5. ثم انقر فوق **معالج التوقيع**.



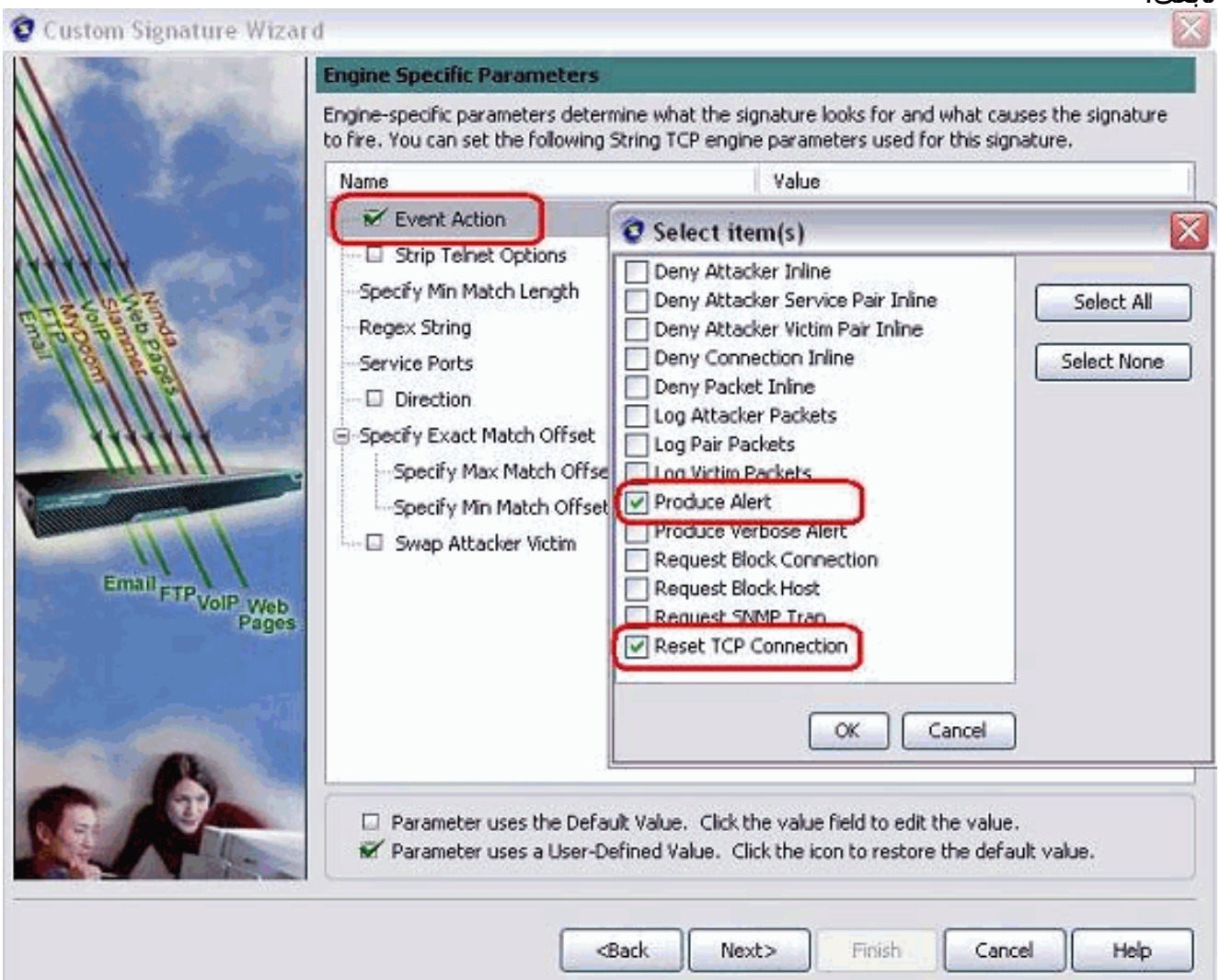
6. في المعالج، أختر **نعم** واختر **سلسلة TCP** كمحرك التوقيع. انقر فوق **Next (التالي)**.



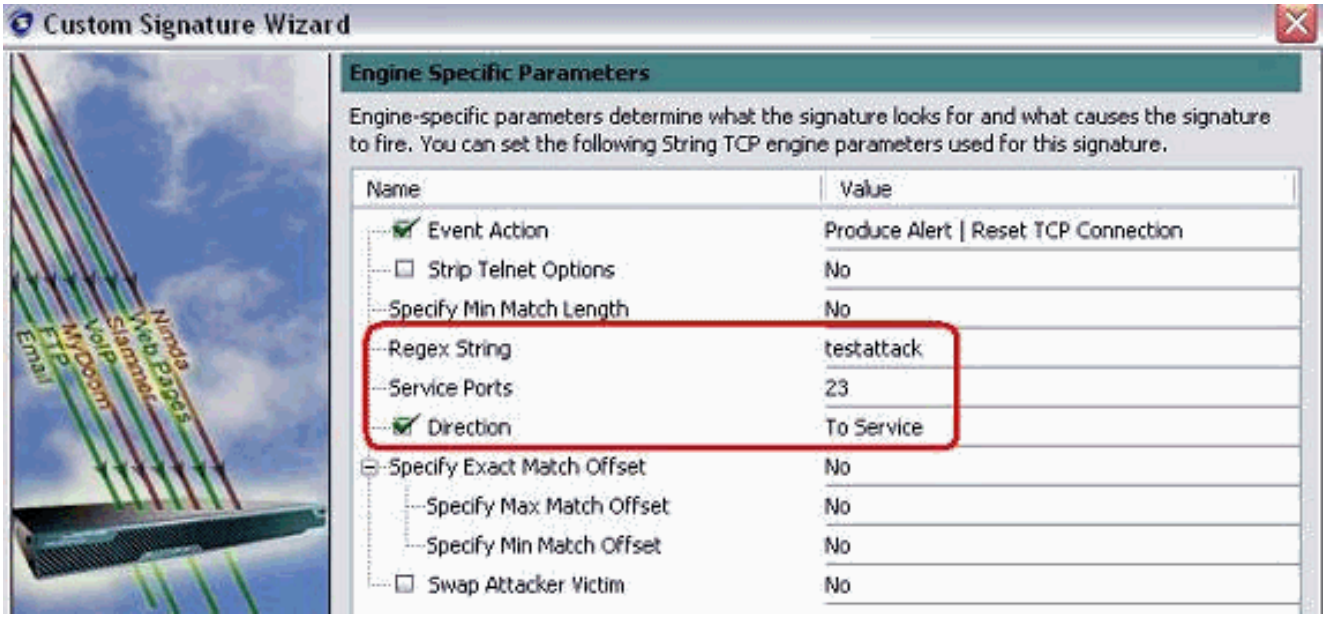
7. يمكنك ترك هذه المعلومات كعنوان أو إدخال معرف التوقيع واسم التوقيع وملاحظات المستخدم الخاصة بك. انقر فوق **Next (التالي)**.



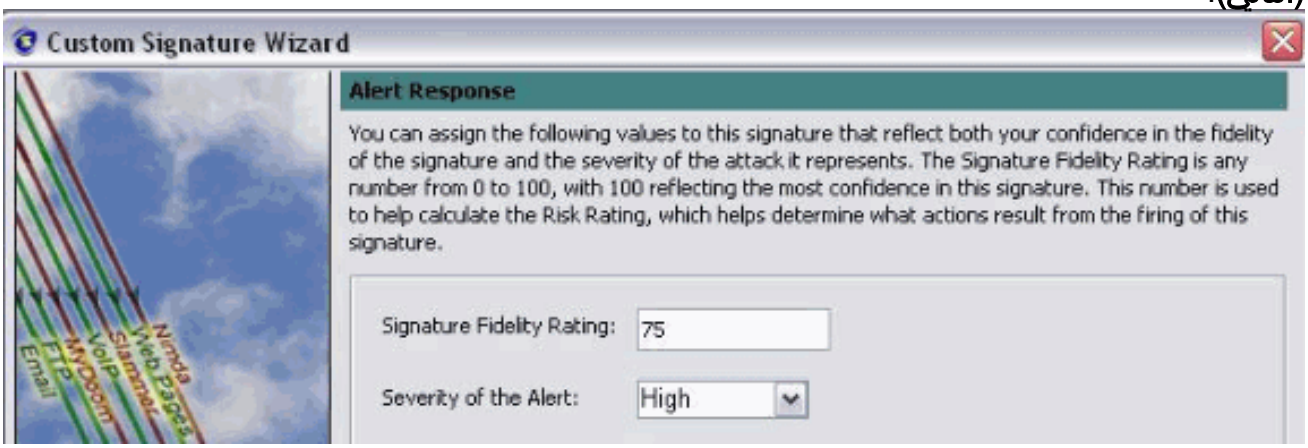
8. أختر **إجراء الحدث**، واختر **إنتاج تنبيه وإعادة ضبط اتصال TCP**. طقطقت **ok** وبعد ذلك **بعد ذلك** in order to تابعت.



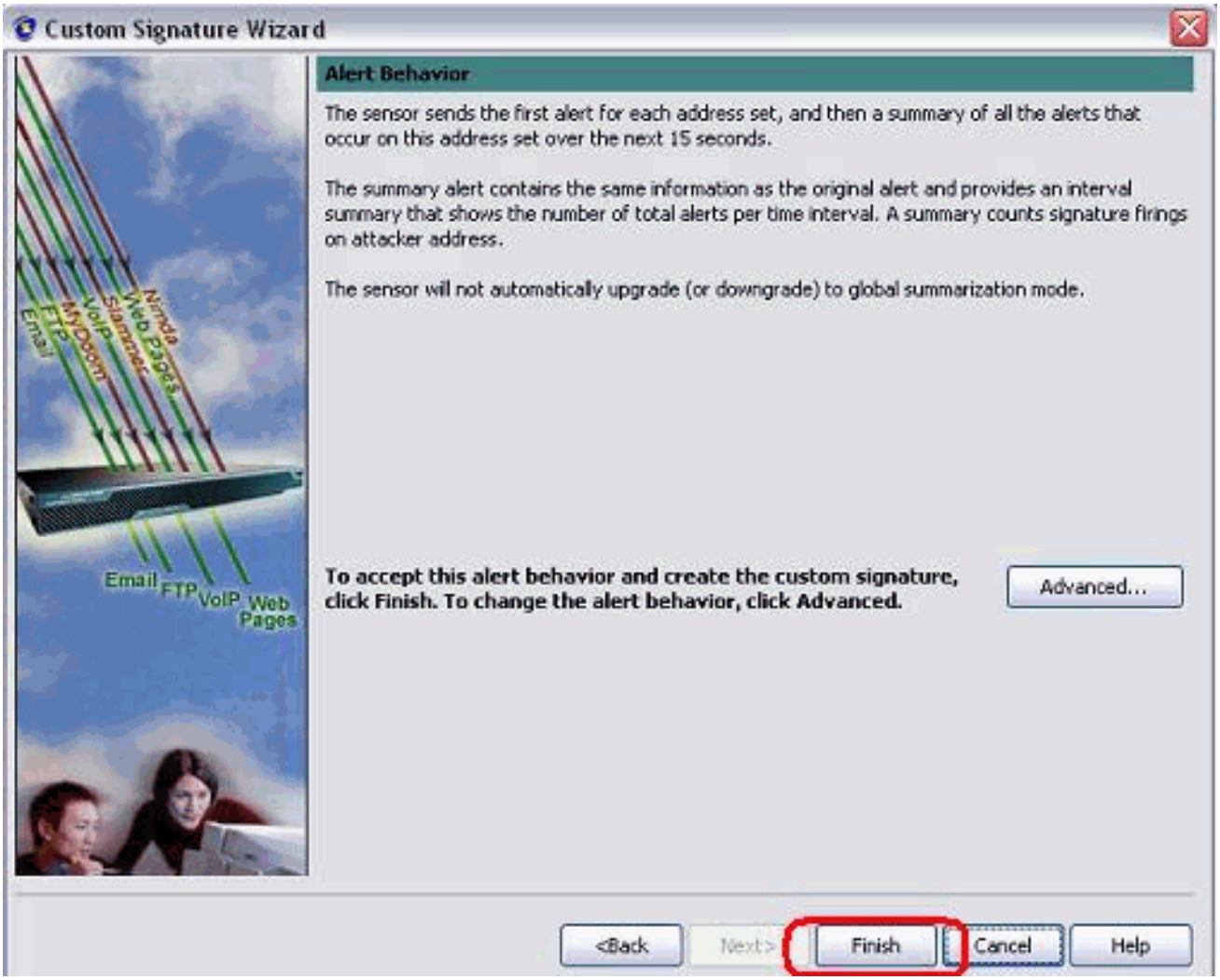
9. أدخل تعبيرا منتظما، ويتم إستخدام `testattack` في هذا المثال. دخلت **23** ل خدمة ميناء، أخترت **أن يعمل** ل الإتجاه، وطقطقة **بعد ذلك** in order to باشرت.



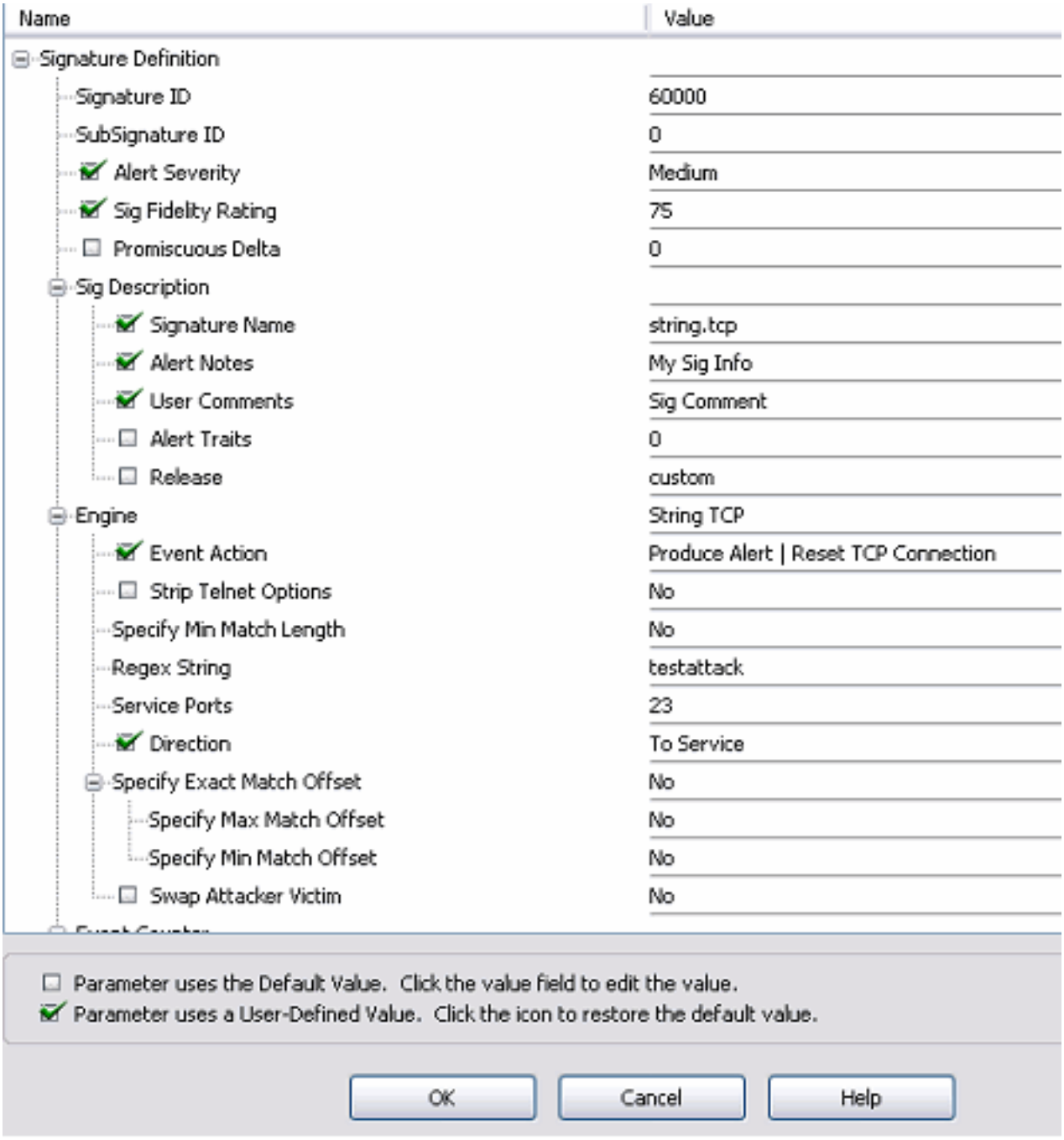
10. يمكنك ترك هذه المعلومات كافتراضي. انقر فوق **Next (التالي)**.



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.

التحقق من الصحة

تشغيل الهجوم وإعادة تعيين TCP

أكمل الخطوات التالية لتشغيل الهجوم وإعادة تعيين TCP:

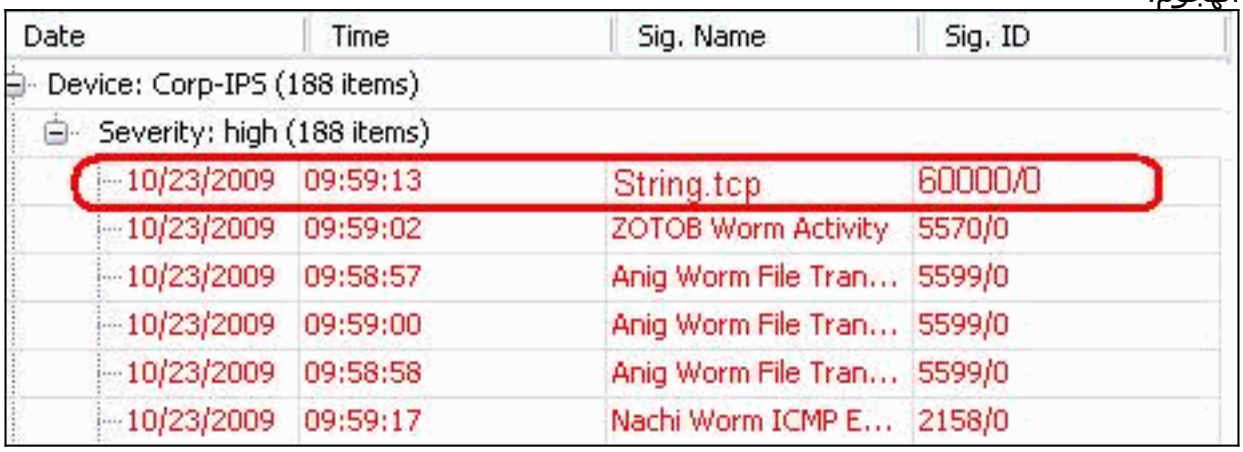
1. قبل بدء الهجوم، انتقل إلى **IME**، واختر **مراقبة الحدث > عرض الهجمات التي تم إسقاطها** واختر المستشعر من الجانب الأيمن.
2. من ضوء الموجه، ومن Telnet إلى منزل الموجه وأدخل **هجوم التجربة**.اضغط إما **<space>** أو **<enter>** لإعادة ضبط جلسة عمل برنامج Telnet.

```
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 closed by foreign host]
.Telnet session has been reset due to the !--- signature "String.tcp" triggered ---!
```

3. من لوحة المعلومات الخاصة بعارض أحداث IPS، يظهر "الإنذار الأحمر" بمجرد بدء تشغيل الهجوم.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

نصائح

أستخدم تلميحات أستكشاف المشكلات وإصلاحها التالية:

- يجنب الأعمال خارج منفذ الأمر والتحكم لإعادة برمجة قوائم التحكم في الوصول إلى الموجه (ACLs). يتم إرسال عمليات إعادة ضبط TCP من **واجهة** sniffing الخاصة بالمستشعر. عندما **يثبت أنت فسحة بين دعامتين** في المفتاح، استعملت **المجموعة فسحة بين دعامتين <src_mod/src_port><dest_mod/dest_port>** أمر مع كلا ربط قادم يمكن كما هو موضح هنا.

```
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
Multicast        : enabled
```

- إذا كانت عمليات إعادة ضبط TCP تعمل، فتحقق مما إذا كان تم تشغيل التنبيه لنوع الإجراء إعادة تعيين TCP. إذا ظهر التنبيه، فتحقق من تعيين نوع التوقيع على إعادة تعيين TCP.قم بتسجيل الدخول باستخدام حساب الخدمة كجذر وإصدار هذا الأمر. يفترض هذا الأمر تعيين واجهة الاستشعار على th0.

```
root@sensor1 root]#tcpdump -i eth0 -n]
```

ملاحظة: يتم إرسال 100 إعادة توجيه TCP إلى الضحية/الهدف ثم يتم إرسال 100 منها إلى المهاجم/العميل.هذا مثال للمخرجات:

```
< 64.104.209.205.1409 03:06:00.598777
telnet: R 107:107(0) ack 72 win 0.10.66.79.38
```

```
        < 64.104.209.205.1409 03:06:00.598794
telnet: R 108:108(0) ack 72 win 0.10.66.79.38

         < telnet.10.66.79.38 03:06:00.599360
 R 72:72(0) ack 46 win 0 :64.104.209.205.1409
         < telnet.10.66.79.38 03:06:00.599377
 R 73:73(0) ack 46 win 0 :64.104.209.205.1409
```

معلومات ذات صلة

- صفحة دعم منع التسلل الآمن من Cisco
- وثائق نظام Cisco لمنع الاقتحام الآمن
- 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).