

# IME مداخلت ساب IPS TCP نبيعت ةداع| نيوكت

## 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 التسلسل (IPS) باستخدام (IME IPS Manager Express). يتم استخدام أجهزة استشعار 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 فسخة بين دعامين 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 © مسحاؒ تخديء مع cisco ios برمجية إءلاق 12.4

تم إنشاء المعلومات الواردة في هذا المسءءء من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المسءءء بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

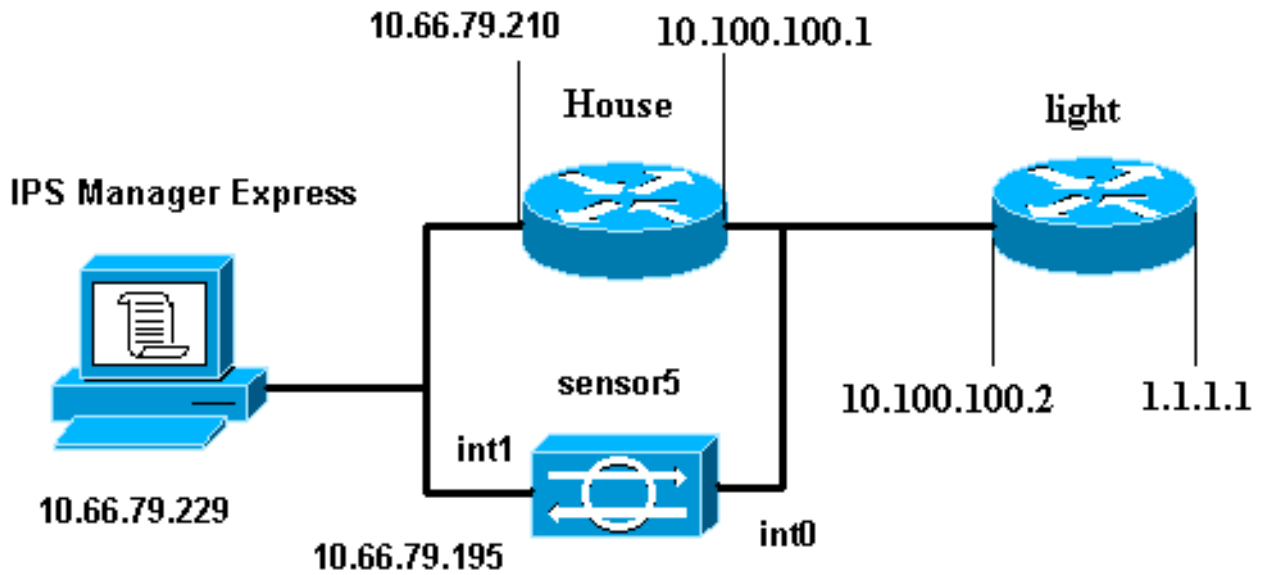
## الاصءلاءات

للءصول على مزيد من المعلومات حول اصءلاءات المسءءءات، ارجع إلى [اصءلاءات تلمبءات Cisco التقنية](#).

## التكوين

### الرسم التءطيلي للشبكة

يستخدم هذا المسءءء إعداد الشبكة الموضح في هذا الرسم التءطيلي.



## التكوينات

يستخدم هذا المسءءء التكوينات الموضءة هنا.

• [ضوء الموجه](#)

• [منزل 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-recipient 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
```

```
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 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** 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.

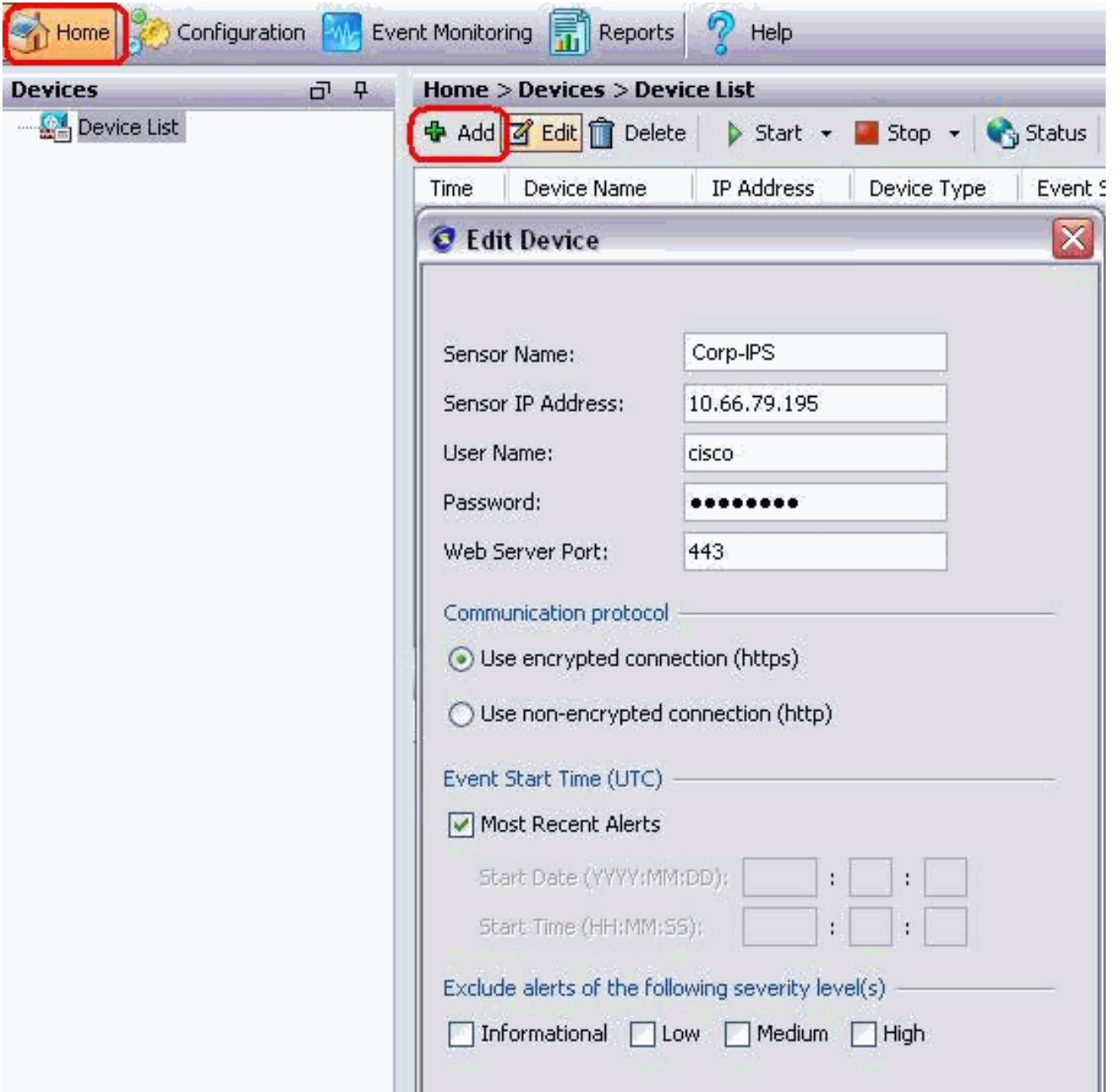
.Go to the command prompt without saving this config [0]  
.Return back to the setup without saving this config [1]  
.Save this configuration and exit setup [2]

Enter your selection[2]: 2

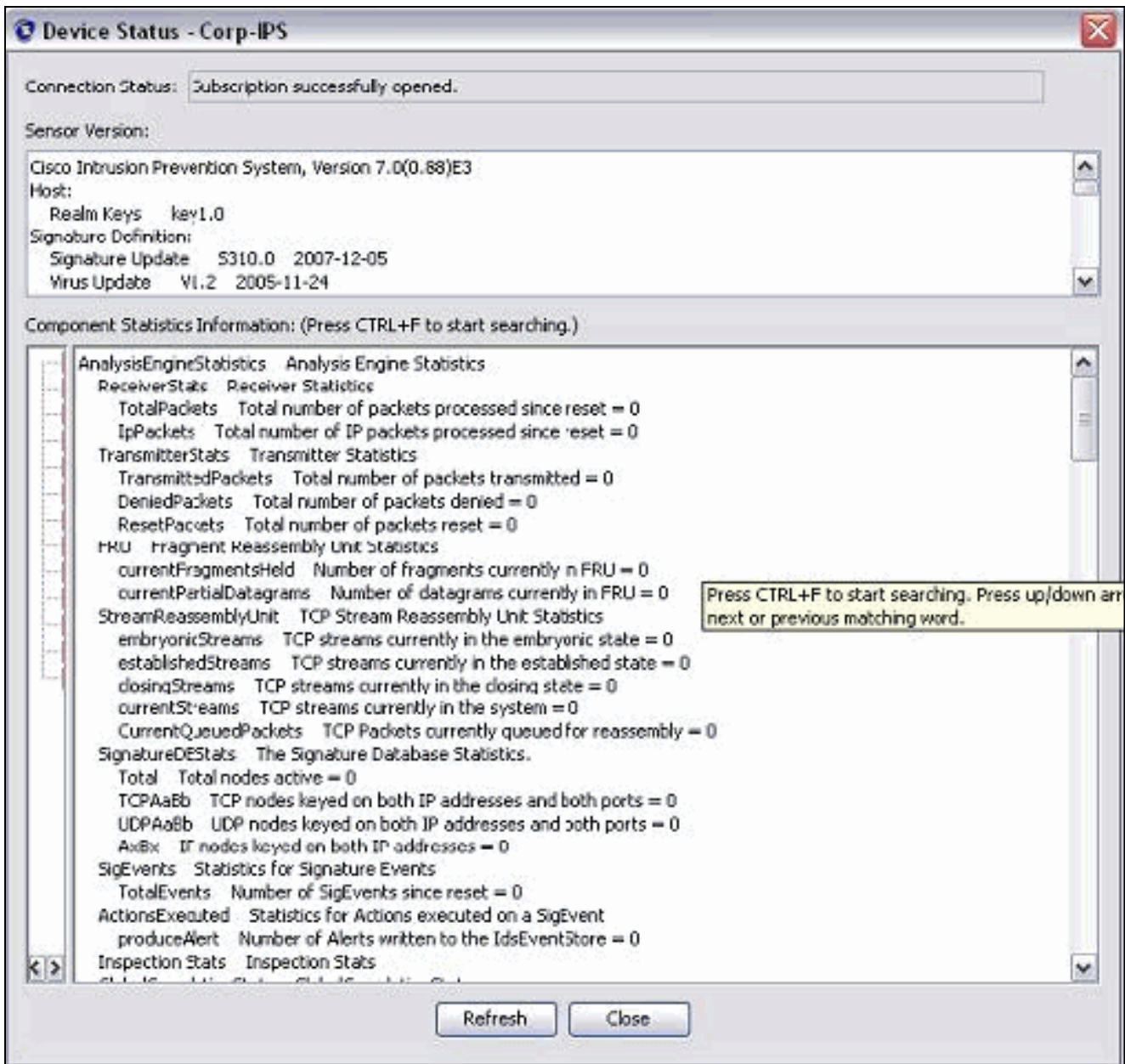
## إضافة المستشعر إلى IME

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. أختار الصفحة الرئيسية < إضافة



3. اكتب في هذه المعلومات وانقر فوق موافق لإنهاء التكوين.
4. أختار أداة < Corp-IPS دفقت المستشعر وضع وبعد ذلك ذلك < clic in order to أختار 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 و123cisco123 لكلمة المرور. تظهر واجهة إدارة IME هذه:

Home Configuration Event Monitoring Reports Help

Configuration > Corp-IPS > Policies > Signature Definitions > sig0 > Active Signatures

Corp-IPS

IPS Policies  
Signature Definitions  
sig0  
Active Signatures  
Adware/Spyware  
Attack  
DDoS  
DoS  
Email  
IOS IPS  
Instant Messaging  
L2/L3/L4 Protocol  
Network Services  
OS  
Other Services  
P2P  
Reconnaissance  
Releases  
Viruses/Worms/Trojan  
Web Server  
All Signatures  
Event Action Rules  
rules0  
Anomaly Detections

Edit Actions Enable Disable Restore Default Show Events My

Filter: Sig ID

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Alert an
1000/0	IP options-Bad Option ...	<input checked="" type="checkbox"/>	Infor...	75	18	Alert
1004/0	IP options-Loose Sour...	<input type="checkbox"/>	High	100	100	Alert
1006/0	IP options-Strict Sourc...	<input checked="" type="checkbox"/>	High	100	100	Alert
1007/0	IPv6 over IPv4	<input type="checkbox"/>	Infor...	100	25	Alert
1101/0	Unknown IP Protocol	<input checked="" type="checkbox"/>	Infor...	75	18	Alert
1102/0	Impossible IP Packet	<input checked="" type="checkbox"/>	High	100	100	Alert
1104/0	IP Localhost Source S...	<input checked="" type="checkbox"/>	High	100	100	Alert
1107/0	RFC 1918 Addresses ...	<input type="checkbox"/>	Infor...	100	25	Alert
1108/0	IP Packet with Proto 11	<input checked="" type="checkbox"/>	High	100	100	Alert
1109/0	Cisco IOS Interface DoS	<input type="checkbox"/>	Medium	75	56	Alert
1109/1	Cisco IOS Interface DoS	<input type="checkbox"/>	Medium	75	56	Alert
1109/2	Cisco IOS Interface DoS	<input type="checkbox"/>	Medium	75	56	Alert
1109/3	Cisco IOS Interface DoS	<input type="checkbox"/>	Medium	75	56	Alert
1200/0	IP Fragmentation Buff...	<input checked="" type="checkbox"/>	Infor...	100	25	Alert
1201/0	IP Fragment Overlap	<input type="checkbox"/>	Infor...	100	25	Alert
1202/0	IP Fragment Overrun ...	<input checked="" type="checkbox"/>	High	100	100	Alert

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

Configuration > Corp-IPS > Policies > Signature Definitions > sig0 > Act

Corp-IPS

IPS Policies  
Signature Definitions  
sig0  
Active Signatures  
Adware/Spyware  
Attack  
DDoS  
DoS

Edit Actions Enable Disable

Filter: Sig ID

Refresh

Signature Wizard

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

Custom Signature Wizard

Welcome

Welcome to the Custom Signature Wizard. This wizard will guide you through the process of creating a custom signature.

Do you know which Signature Engine you want to use for the custom signature?

Yes

Select Engine: String TCP

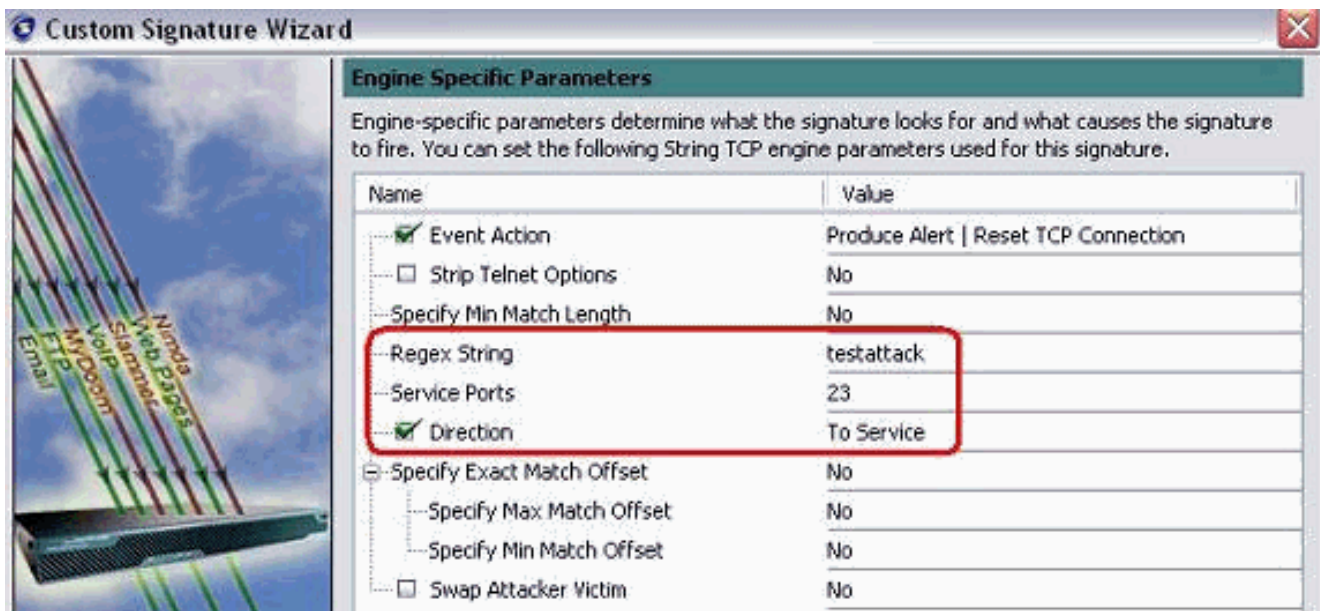
No



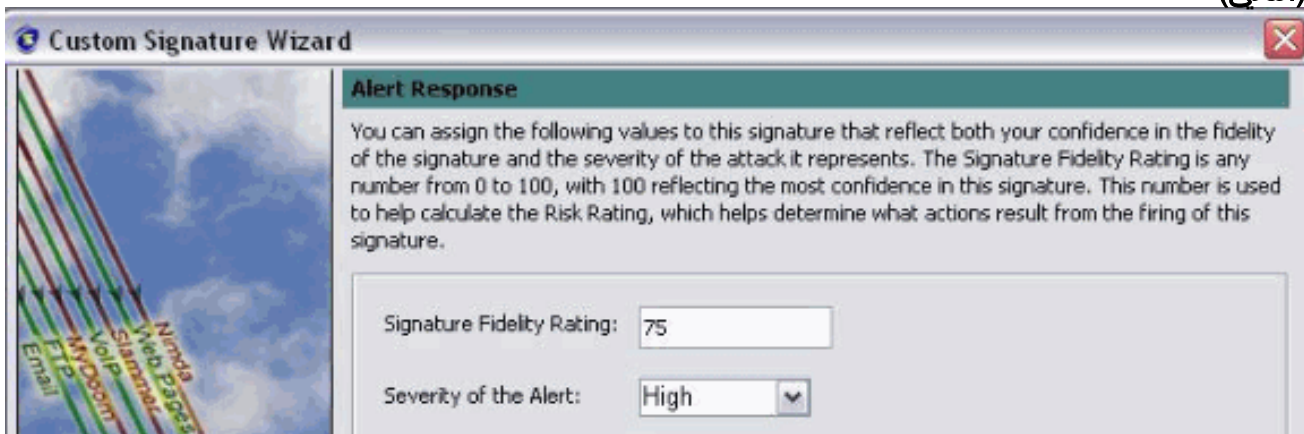
7. يمكنك ترك هذه المعلومات كعنوان أو إدخال معرف التوقيع واسم التوقيع وملاحظات المستخدم الخاصة بك.  
انقر فوق **Next** (التالي).

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

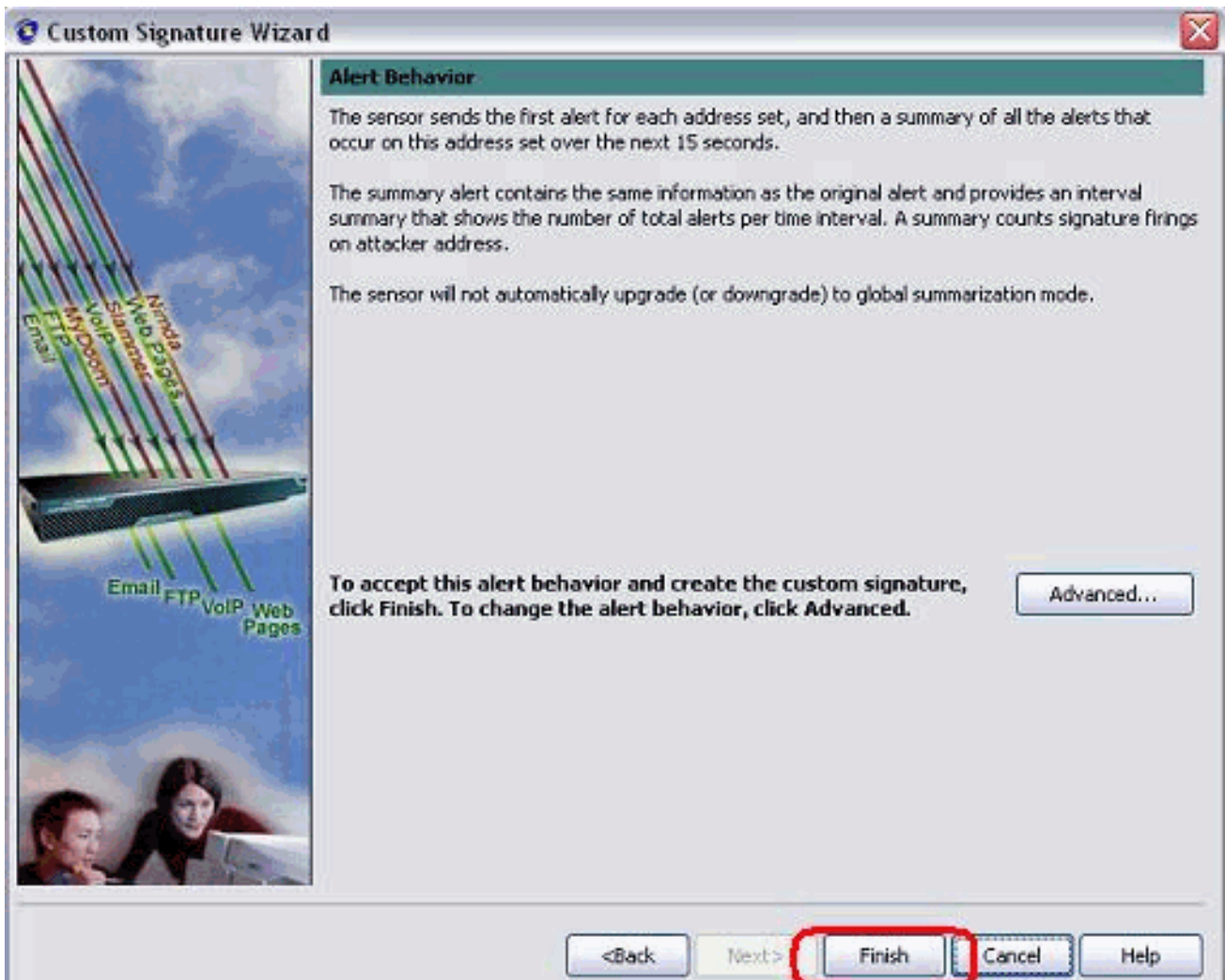
9. أدخل تعبيراً منتظماً، ويتم استخدام `testattack` في هذا المثال. دخلت ل خدمة ميناء، أختَر أن يعمل ل الإتهام، وطققة بعد ذلك in order to باشرت.



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



11. قطعة 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. قطعة يحرر in order to شاهدت التوقيع.

Name	Value
Signature Definition	
Signature ID	60000
SubSignature ID	0
<input checked="" type="checkbox"/> Alert Severity	Medium
<input checked="" type="checkbox"/> Sig Fidelity Rating	75
<input type="checkbox"/> Promiscuous Delta	0
Sig Description	
<input checked="" type="checkbox"/> Signature Name	string.tcp
<input checked="" type="checkbox"/> Alert Notes	My Sig Info
<input checked="" type="checkbox"/> User Comments	Sig Comment
<input type="checkbox"/> Alert Traits	0
<input type="checkbox"/> Release	custom
Engine	String TCP
<input checked="" type="checkbox"/> Event Action	Produce Alert   Reset TCP Connection
<input type="checkbox"/> Strip Telnet Options	No
<input type="checkbox"/> Specify Min Match Length	No
Regex String	testattack
Service Ports	23
<input checked="" type="checkbox"/> Direction	To Service
Specify Exact Match Offset	No
Specify Max Match Offset	No
Specify Min Match Offset	No
<input type="checkbox"/> Swap Attacker Victim	No
Event Counter	

Parameter uses the Default Value. Click the value field to edit the value.  
 Parameter uses a User-Defined Value. Click the icon to restore the default value.

OK Cancel Help

13. طقطقة ok بعد أن يؤكد أنت ويططق 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 "الإذار الأحمر" بمجرد بدء تشغيل الهجوم.

Date	Time	Sig. Name	Sig. ID
Device: Corp-IPS (188 items)			
Severity: high (188 items)			
10/23/2009	09:59:13	String.tcp	60000/0
10/23/2009	09:59:02	ZOTOB Worm Activity	5570/0
10/23/2009	09:58:57	Anig Worm File Tran...	5599/0
10/23/2009	09:59:00	Anig Worm File Tran...	5599/0
10/23/2009	09:58:58	Anig Worm File Tran...	5599/0
10/23/2009	09:59:17	Nachi Worm ICMP E...	2158/0

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

### نصائح

أستخدم تلميحات استكشاف المشكلات وإصلاحها التالية:

- يجب 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 فسخة بين دعامتين في المفتاح، استعملت المجموعة فسخة 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، فتتحقق مما إذا كان تم تشغيل التنبيه لنوع الإجراء إعادة تعيين TCP. إذا ظهر التنبيه، فتتحقق 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 التسلسل الآمن من Cisco](#)
- [وثائق نظام Cisco لمنع الاقتحام الآمن](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل