

# CSPM في Cisco Secure IDS رعش تسم نيوكت

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[التكوين](#)

[تحديد الشبكة التي تتواجد عليها مضيف CSPM](#)

[إضافة مضيف CSPM](#)

[إضافة جهاز الاستشعار](#)

[تكوين جهاز الاستشعار](#)

[معلومات ذات صلة](#)

## المقدمة

يشرح هذا المستند الإجراء المستخدم لتكوين مستشعر نظام اكتشاف الاقتحام الآمن (IDS) من Cisco على Cisco Secure Policy Manager (CSPM). يفترض هذا المستند أنك قمت بتثبيت الإصدار 2.3.i من CSPM على جهاز الكمبيوتر الخاص بك. يسمح الإصدار "i" بإدارة أجهزة IDS (أجهزة استشعار الأجهزة أو موجهات Cisco IOS® أو خوادم IDS النصلية) في محول Cisco Catalyst® 6000 switch. يفترض هذا المستند أيضا أن معلمات مكتب البريد IDS معرفة بشكل صحيح. وهذه تشمل Hostname، OrgID، HostID، و OrgName. الرجاء ملاحظة أنه لكي يتصل مضيف CSPM بمستشعر، يجب أن يتطابق ORGID و ORGname مع ما تم تعريفه على المستشعر.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى CSPM 2.3.i والإصدارات الأحدث.

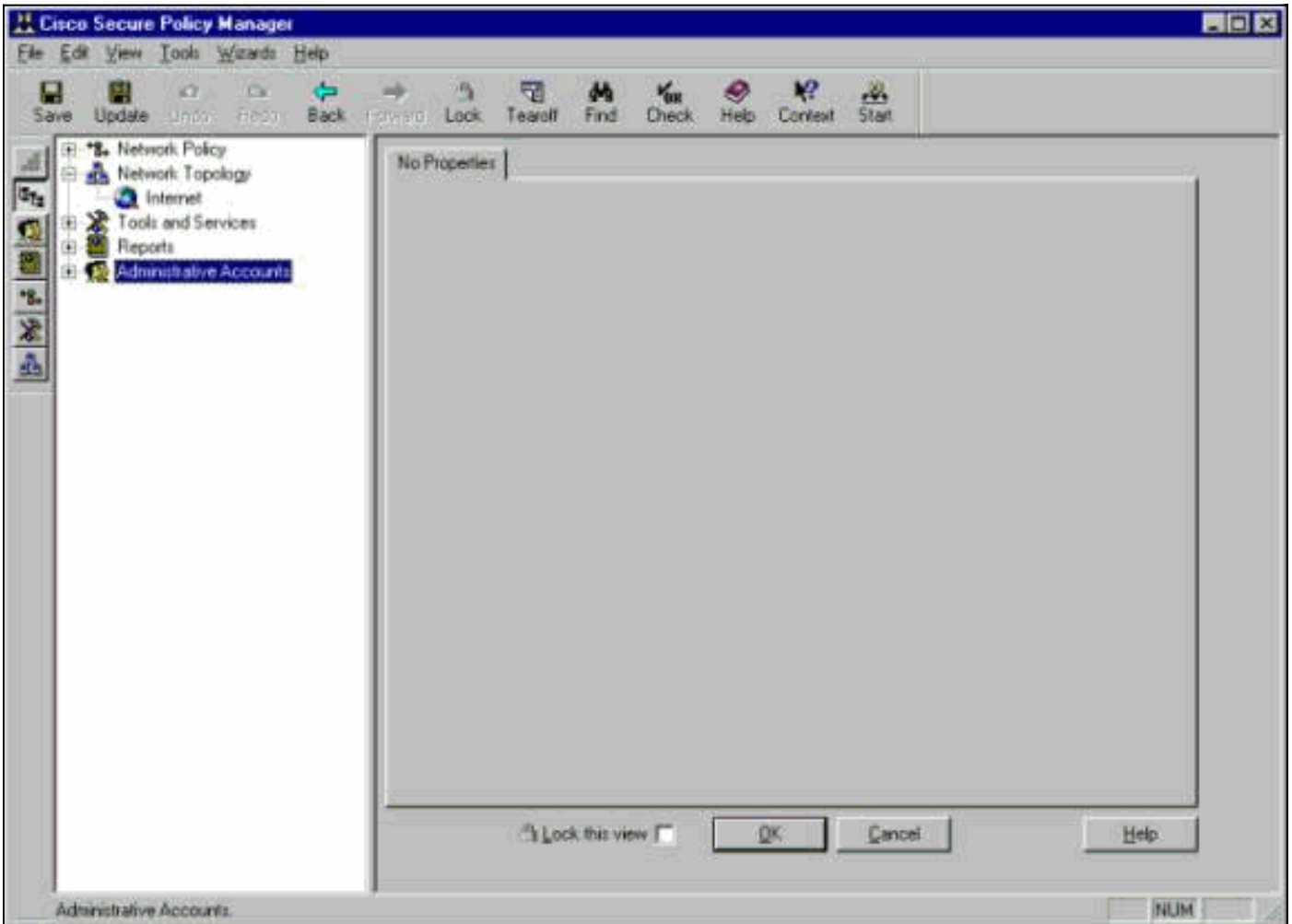
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

### الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

## التكوين

توضح هذه الأقسام العملية المستخدمة لتكوين مستشعر IDS في CSPM. قم بتشغيل CSPM وسجل الدخول. يظهر قالب فارغ (إطلاق أولي) يتيح لك تعريف الشبكة.



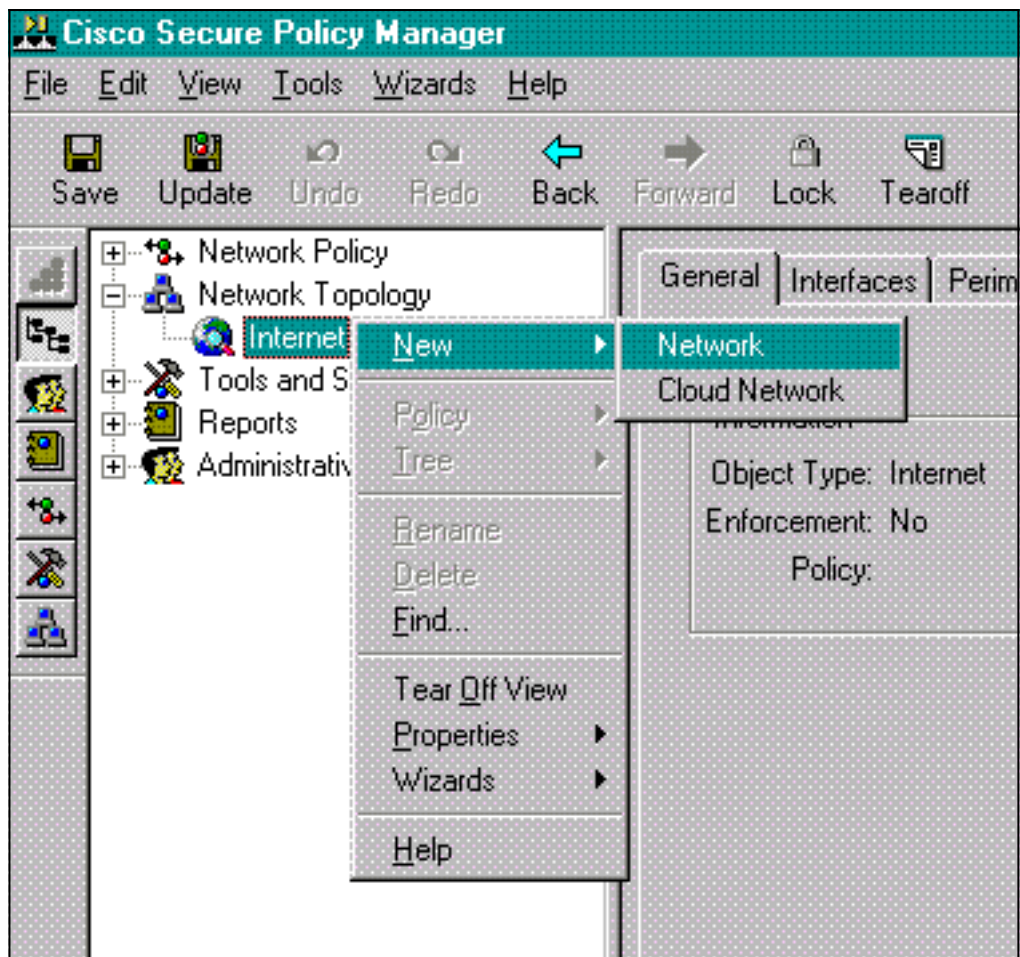
هذه التعريفات الثلاثة مطلوبة في مخطط CSPM لمعرفة المستخدم.

1. قم بتعريف الشبكة التي توجد فيها واجهة التحكم الخاصة بالمستشعر والشبكة التي يتواجد فيها مضيف CSPM. إذا كانا على الشبكة الفرعية نفسها، فيجب تعريف شبكة واحدة فقط. قم بتعريف هذه الشبكة أولاً.
2. تحديد مضيف CSPM في شبكته. بدون تعريف مضيف CSPM، لا يمكن إدارة المستشعر.
3. قم بتعريف المستشعر في شبكته.

### تحديد الشبكة التي يتواجد عليها مضيف CSPM

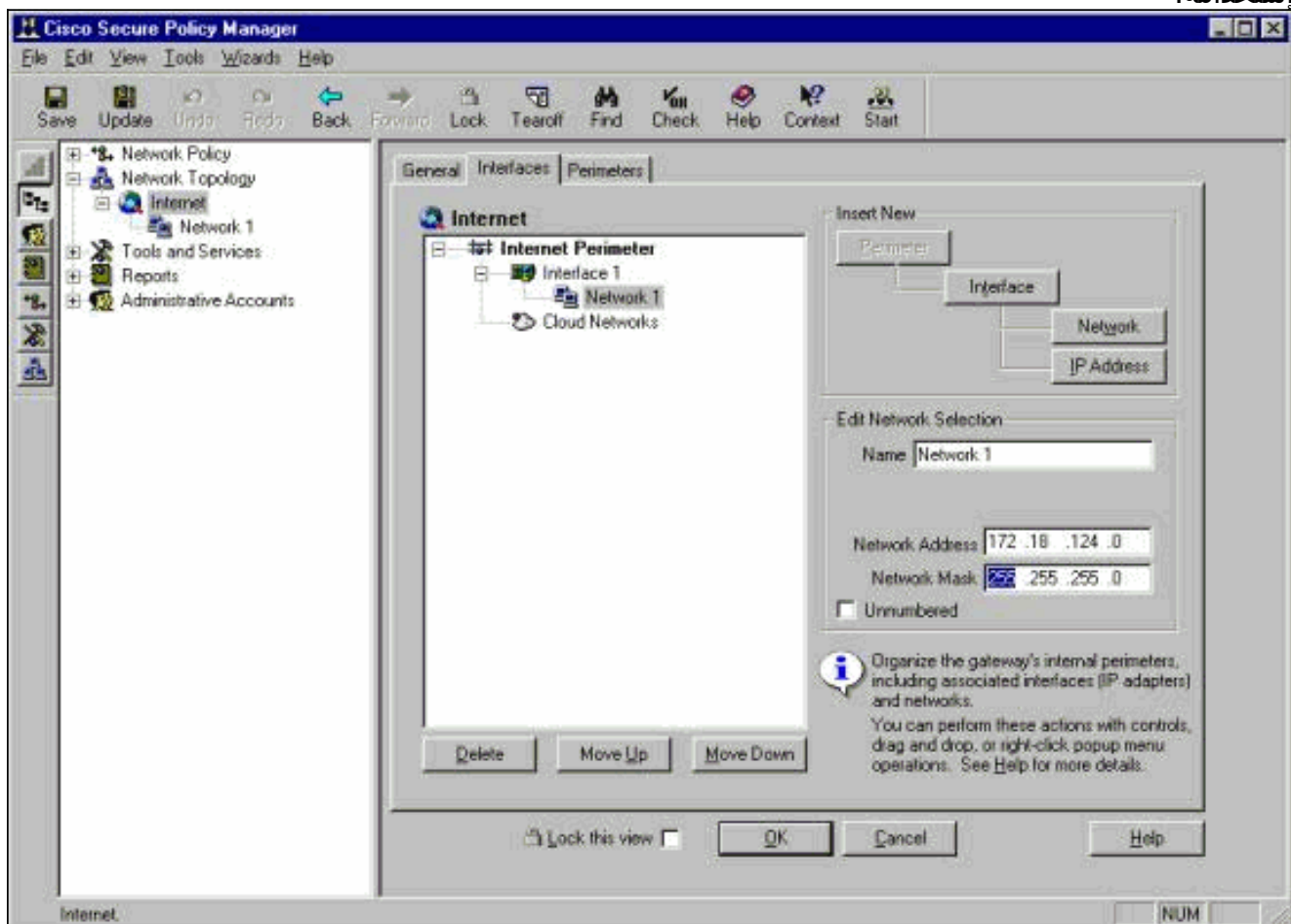
أكمل الخطوات التالية:

1. انقر بزر الماوس الأيمن على رمز الإنترنت في المخطط وحدد جديد > الشبكة لإنشاء شبكة



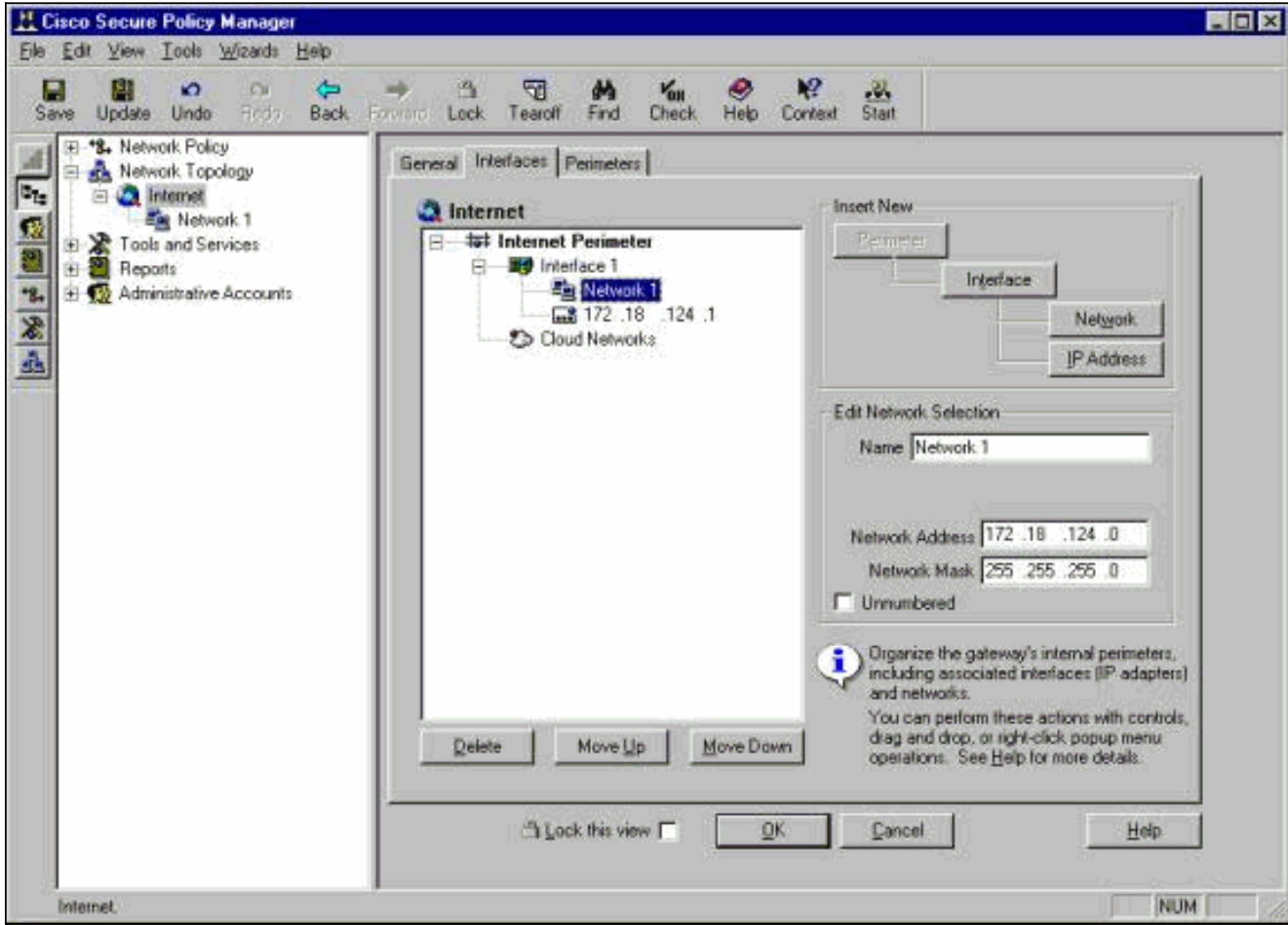
جديدة.

2. على الجانب الأيمن من لوحة الشبكة، أضف اسم الشبكة الجديدة وعنوان الشبكة وقناع الشبكة الذي سيتم استخدامه.



3. انقر فوق الزر عنوان IP، وأدخل عنوان IP لشبكتك التي يستخدمها للوصول إلى الإنترنت. في العادة تكون

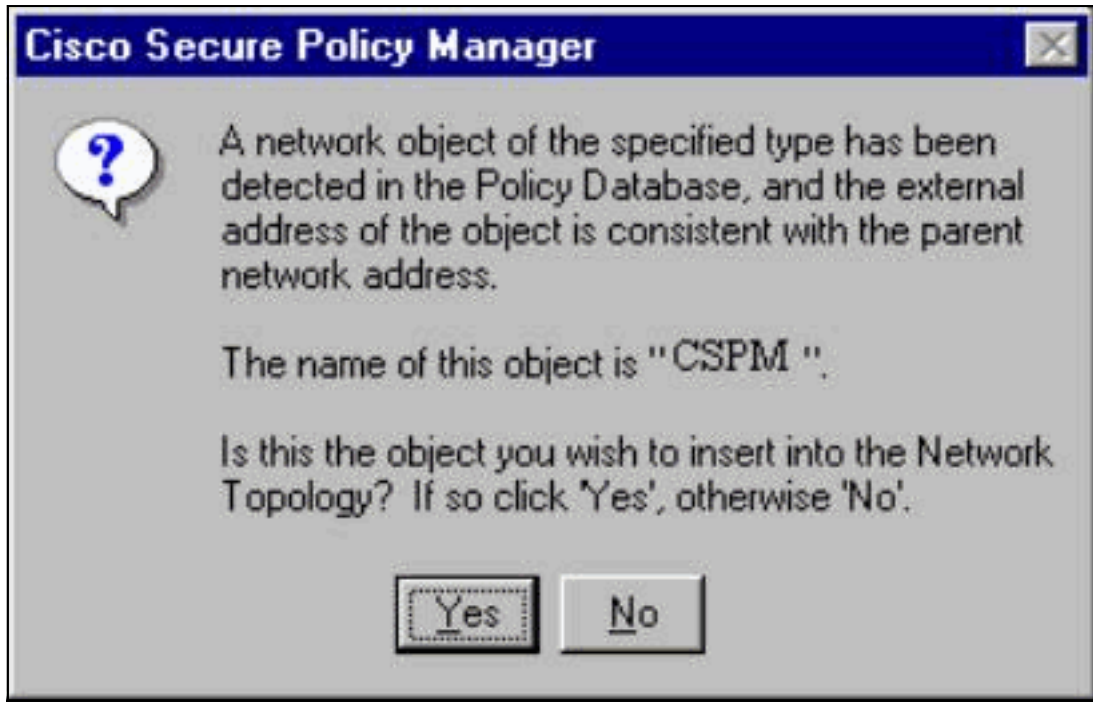
العبرة الافتراضية للشبكة. ملاحظة: عند إدارة أجهزة الاستشعار، لا يلزم بالضرورة أن يكون عنوان البوابة صحيحا نظرا لأن المستشعر لا يرسل معلومات العبرة الافتراضية هذه. يجب تعريفه بالفعل في المستشعر. 4. وانقر فوق OK. تتم إضافة الشبكة إلى خريطة المخطط دون حدوث أي أخطاء.



## إضافة مضيف CSPM

أستخدم هذا الإجراء لإضافة مضيف CSPM.

1. في مخطط الشبكة، انقر بزر الماوس الأيمن على الشبكة التي أضفتها للتو وحدد جديد < المضيف. يعرض CSPM شاشة مماثلة لهذا. إذا لم تكن هناك شبكة، فالشبكة التي قمت بتعريفها للتو ليست الشبكة التي يتواجد فيها مضيف CSPM الخاص بك. تحقق من عنوان IP على مضيف CSPM الخاص بك مرة



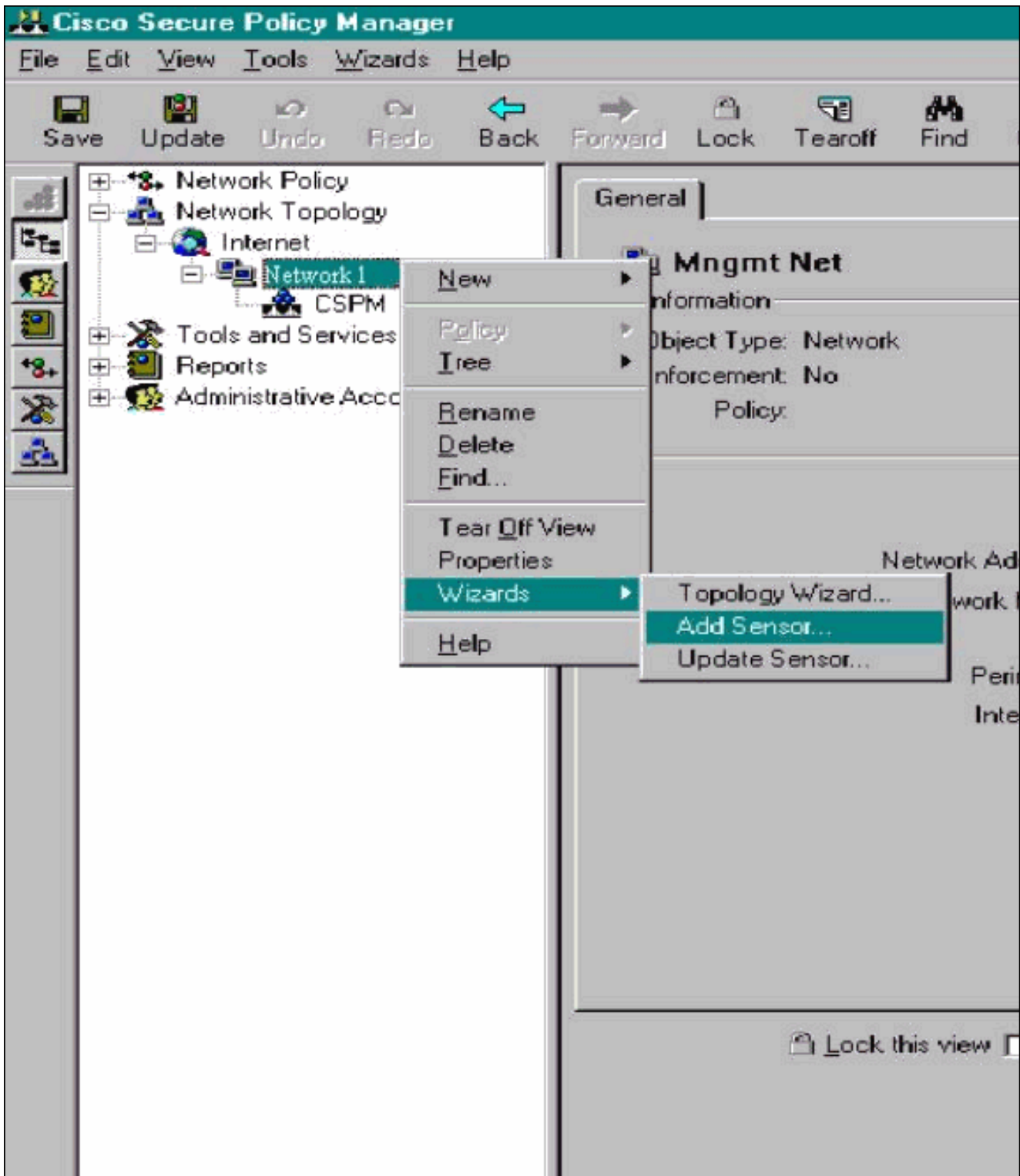
أخرى.

2. انقر فوق نعم لتثبيت مضيف CSPM في المخطط.
3. تحقق من صحة المعلومات الموجودة على الشاشة العامة لمضيف CSPM.
4. انقر فوق موافق على الشاشة العامة لمضيف CSPM.

### إضافة جهاز الاستشعار

أستخدم هذا الإجراء لإضافة جهاز الاستشعار.

1. انقر بزر الماوس الأيمن فوق الشبكة التي يتواجد فيها جهاز الاستشعار وحدد المعالجات < إضافة جهاز استشعار. ملاحظة: إذا لم يكن مضيف CSPM وواجهة التحكم الخاصة بالمستشعر لديك في الشبكة نفسها، فحدد الشبكة التي يتواجد فيها المستشعر.



2. أدخل معلومات مكتب البريد الصحيحة للمستشعر.



**Add Sensor Wizard**

**Add Sensor Wizard**

**Sensor Identification**

Welcome to the Add Sensor Wizard. To add a Sensor to the topology fill in the following information and press Next.

Sensor Identification

Sensor Name:  Host ID:  Org. ID:

Organization Name:

IP Address:

Postoffice Heartbeat Interval:

Policy Enforcement


Associated Network Service:

Port:

Comments:

Check here to verify the Sensor's address.

Check here to capture the Sensor's configuration.

 Enter the IP Address and the Host ID will populate automatically. Or you may enter it manually.

< Back   Next >   Cancel   Help

3. انقر فوق **التحقق هنا للتحقق من مربع عنوان أداة الاستشعار**. ملاحظة: إذا كانت هذه هي المرة الأولى التي تقوم فيها بإعداد هذا المستشعر، فلن ترغب في التقاط تكوين المستشعر. إذا كنت قد انتهيت من تكوين هذا المستشعر مسبقاً في مكان آخر إما عبر مدير UNIX أو مضيف CSPM آخر وأجرت تغييرات في التكوين على توقيعات المستشعرات، فأنت تريد التقاط تكوين المستشعر.
4. طقطقت **بعد ذلك** أن يعين التوقيع صيغة على المستشعر. يمكنك أيضاً إصدار الأمر **nrvers** للتحقق من هذا على المستشعر.

**Add Sensor Wizard**

**Sensor Configuration**

Specify the Policy Distribution Host. Select the version of the Sensor and enable or disable IPSec support. Choose the appropriate Signature Template from the drop down lists.

Distribution  
Host: **CSPM (1)** Select the Cisco Secure Policy Manager host that will publish the generated device-specific command sets to this device.

Sensor Version: **3.0(1)S8** IPSec:  Check here to enable IPSec on supported Sensor versions.

Signature Template: **Default**

Template Comment: Cisco Systems, Inc. default Signature Template settings.

**i** There are 3 signatures in the latest signature update (3.0(1)S8) that do not apply to this Sensor version 3.0(1)S8.

< Back Next > Cancel Help

>ملا

ملاحظة: إذا لم يكن لـ CSPM إصدار المستشعر الصحيح الذي تقوم بتشغيله على المستشعر الخاص بك، فقم بتحديث التوقيعات على مضيف CSPM الخاص بك. يرجى الاطلاع على [تنزيل البرامج](#) (للعلماء المسجلين فقط) للحصول على التحديثات.

5. انقر فوق الزر التالي للمتابعة.

6. انقر فوق إنهاء لإكمال تثبيت المستشعر في المخطط.

7. من القائمة الرئيسية CSPM، حدد ملف < حفظ وتحديث لتجميع المعلومات التي تم إدخالها في المخطط في CSPM. يرجى ملاحظة أن هذه الخطوة ضرورية لبدء بروتوكول مكتب البريد على مضيف CSPM.

8. تحقق من أن كل شيء يعمل عن طريق تسجيل الدخول إلى جهاز الاستشعار الخاص بك كمستخدم للشبكة.

9. قم بتنفيذ الأمر `nrconns`.

`nrconns<`

Connection Status for gacy.rtp

```
cspm.rtp Connection 1: 172.18.124.106 45000 1
Established] sto:0004 with Version 1]
```

`netrangr@gacy:/usr/nr`

<

ملاحظة: إذا لم يكن المستشعر ومضيف CSPM يتواصلان، يظهر إخراج مشابه لهذا بدلا من ذلك:

`netrangr@gacy:/usr/nr`

`nrconns<`

Connection Status for gacy.rtp



```
[insane.rtp Connection 1: 172.18.124.194 45000 1 [SynSent
!sto:5000 syn NOT rcvd
```

```
netrangr@gacy:/usr/nr
```

إن هذا هو الحالة، يحصل sniffer تتبع أن يرى إن كلا جانب يرسل UDP 45000 ربط. UDP 45000 هو ما تستخدمه أجهزة IDS للاتصال ببعضها البعض. لاختبار هذا على المستشعر، su to root و (حسب المستشعر لديك) ينفذ snoop -d iprb1 ميناء 45000 (ل IDS 4210 مستشعر) و snoop -d iprb0 ميناء 45000 (ل أي نموذج آخر للمستشعر). أستخدم <control-c> للخروج من جلسة عمل snoop. يظهر هذا المخرج إذا لم يكن هناك اتصال بين المستشعر و CSPM:

```
netrangr@gacy:/usr/nr
```

```
- su<
```

```
:Password
```

```
Sun Microsystems Inc. SunOS 5.8 Generic February 2000
```

```
snoop -d spwr0 port 45000 #
```

```
(Using device /dev/spwr (promiscuous mode
```

```
UDP D=45000 S=45000 LEN=52 172.18.124.106 <- 172.18.124.100
```

```
UDP D=45000 S=45000 LEN=52 172.18.124.106 <- 172.18.124.100
```

```
UDP D=45000 S=45000 LEN=52 172.18.124.106 <- 172.18.124.100
```

```
UDP D=45000 S=45000 LEN=52 172.18.124.106 <- 172.18.124.100
```

```
#C^
```

في الإخراج أعلاه، يرسل المستشعر حزم UDP 45000، ولكنه لا يستلم أي. ينتج التكوين الصحيح مخرجات مماثلة لهذا:

```
snoop -d spwr0 port 45000 #
```

```
(Using device /dev/iprb (promiscuous mode
```

```
gacy UDP D=45000 S=45000 LEN=56 <- 172.18.124.106
```

```
gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56
```

```
gacy UDP D=45000 S=45000 LEN=56 <- 172.18.124.142
```

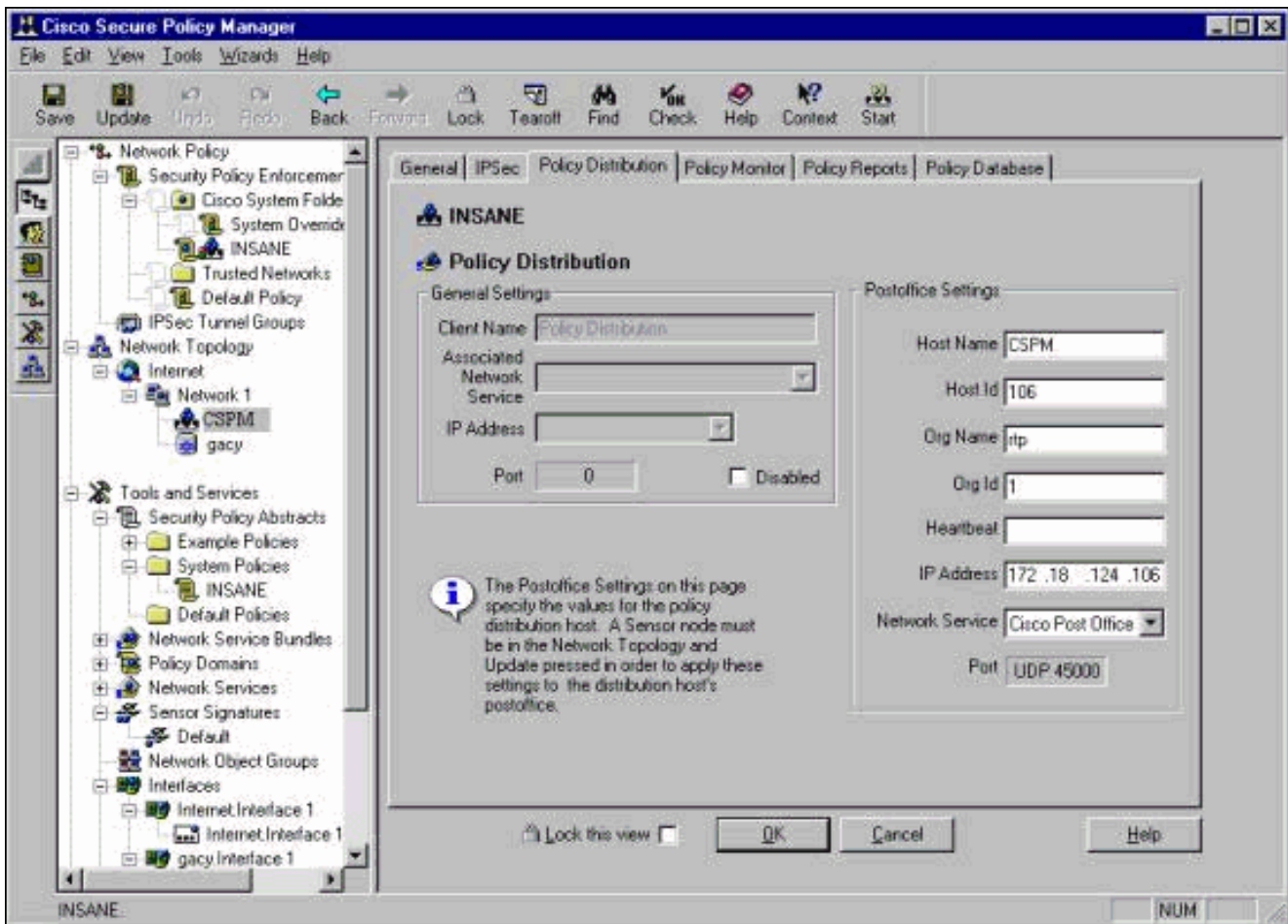
```
gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56
```

وفي الناتج المذكور أعلاه، تسير حركة مرور UDP 45000 في كلا الاتجاهين. إذا كانت حزم UDP 45000 تتدفق في كلا الاتجاهين وكان إخراج الشبكات على المستشعر لا يزال يقول إنه لا يوجد اتصال تم إنشاؤه، فإن معلمات PostOffice على المستشعر ومضيف CSPM لا تتطابق. للتحقق يدويا من معلمات مكتب البريد الموجودة على مضيف CSPM: أستخدم "مستكشف Windows" للتنقل إلى المكان الذي تم تثبيت CSPM فيه على جهاز .NT

Name	Size	Type	Modified	Attributes
auths	1KB	File	10/10/01 12:53 PM	A
auths.bak	1KB	BAK File	10/10/01 12:38 PM	A
daemons	1KB	File	9/27/01 10:45 AM	A
destinations	1KB	File	10/8/01 5:37 PM	A
destinations.bak	1KB	BAK File	9/27/01 10:45 AM	A
hosts	1KB	File	10/10/01 12:53 PM	A
hosts.bak	1KB	BAK File	10/10/01 12:38 PM	A
organizations	1KB	File	9/27/01 10:45 AM	A
postofficed.conf	1KB	CONF File	10/8/01 5:37 PM	A
postofficed.conf.tmp	1KB	TMP File	10/10/01 12:05 PM	A
routes	1KB	File	10/10/01 12:53 PM	A
routes.bak	1KB	BAK File	10/10/01 12:38 PM	A
sapd.conf	3KB	CONF File	8/8/01 11:26 PM	A
services	2KB	File	8/8/01 11:26 PM	A
signatures	10KB	File	8/8/01 11:26 PM	A
smid.conf	1KB	CONF File	10/8/01 5:37 PM	A
smid.conf.bak	1KB	BAK File	9/27/01 10:45 AM	A

17 object(s) 18.4KB

قم بتحرير ملفات المضيف والتوجيه والمؤسسات باستخدام Write أو Wordpad (لا تستخدم Notepad لأن التنسيق سيكون نالفا). تأكد من أن هذه الملفات تبدو صحيحة للثبيت. إذا لم تكن أي من القيم صحيحة، قم بتحريرها وأعد تشغيل جهاز كمبيوتر NT باستخدام الخطوات التالية: انقر على رمز CSPM في مخطط الشبكة. انقر فوق علامة التبويب "توزيع النهج" لإدخال معلمات مكتب البريد. **حفظ التغييرات وتحديثها**. أعد تشغيل جهاز كمبيوتر .NT



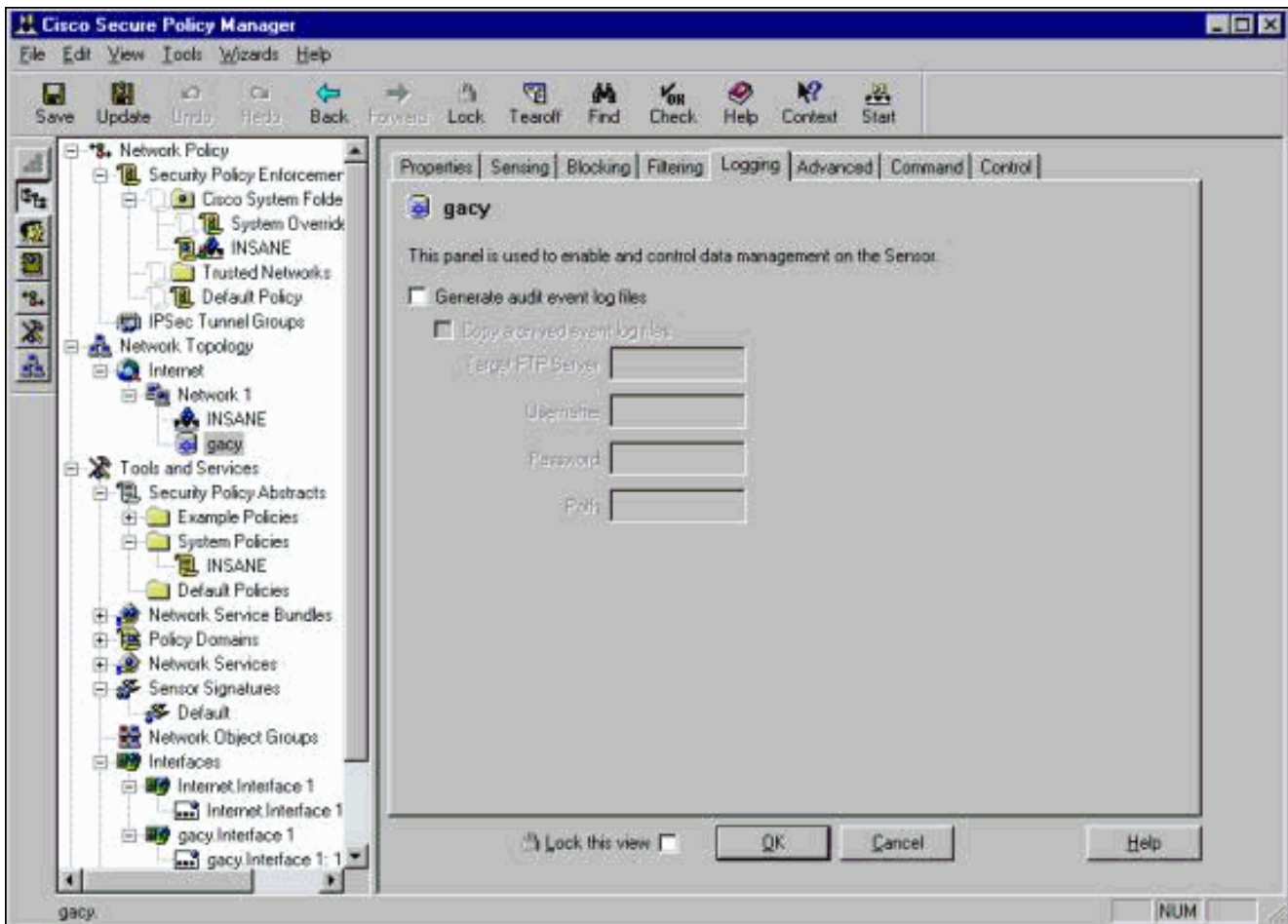
## تكوين جهاز الاستشعار

بعد حفظ التكوين في CSPM، قم بتكوين المستشعر. للقيام بذلك، قم أولاً بتعيين المستشعر لكتابة الإنذارات التي يراها في سجله الخاص. ثم قم بتعيين "المستشعر" على "sniff" على الواجهة الصحيحة.

## كتابة تنبيهات إلى السجل

أستخدم هذا الإجراء لكتابة الإنذارات إلى السجل.

1. انقر فوق مربع إنشاء ملفات سجل أحداث التدقيق لإخبار المستشعر بإرسال التنبيهات إلى سجلاته المحلية. كما أنها ترسل تنبيهات إلى مربع CSPM بشكل افتراضي بعد دفع تكوين ما لأسفل إليه.

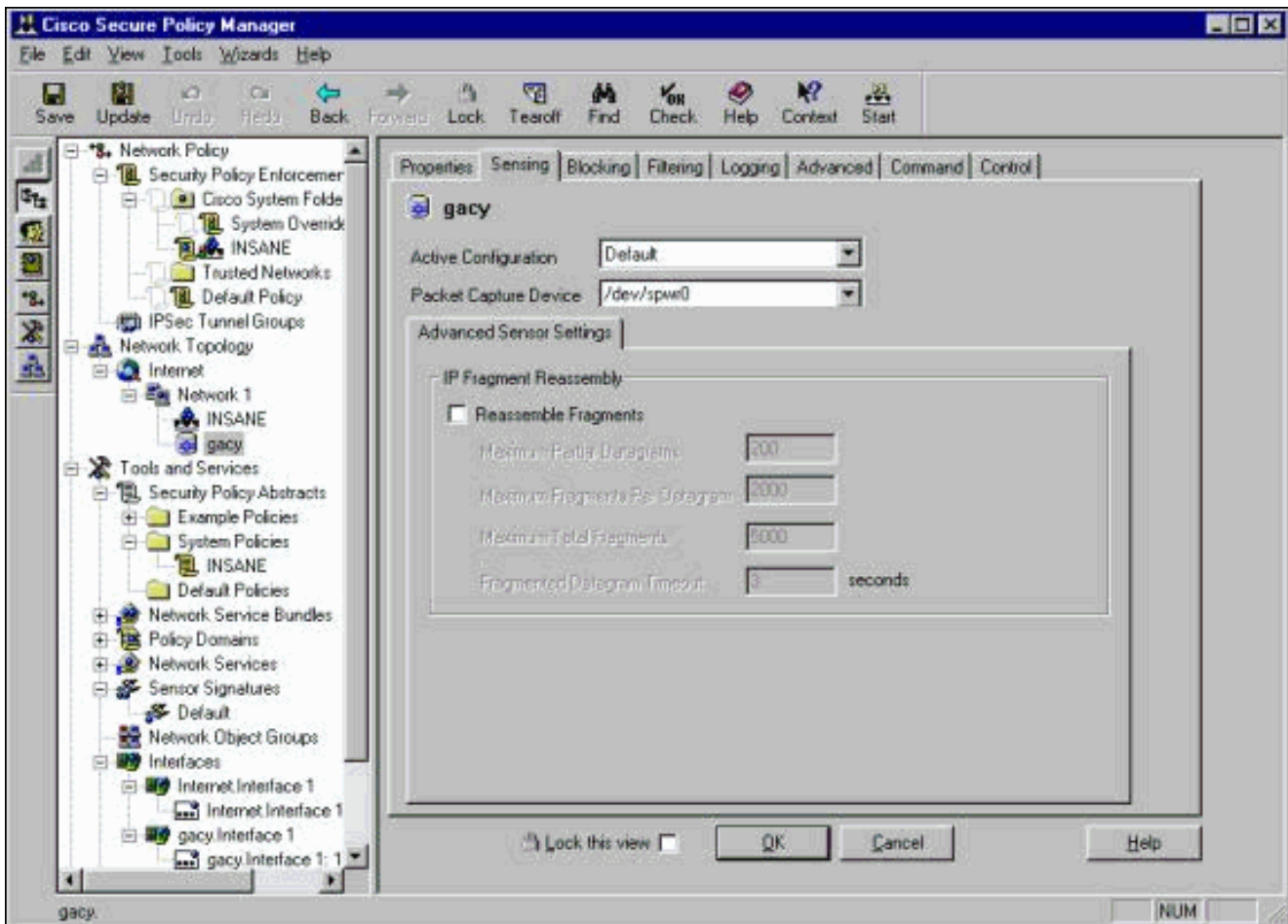


2. انقر فوق موافق" للمتابعة.

### تعين المستشعر على "sniff"

أستخدم هذا الإجراء لتعيين المستشعر على "sniff".

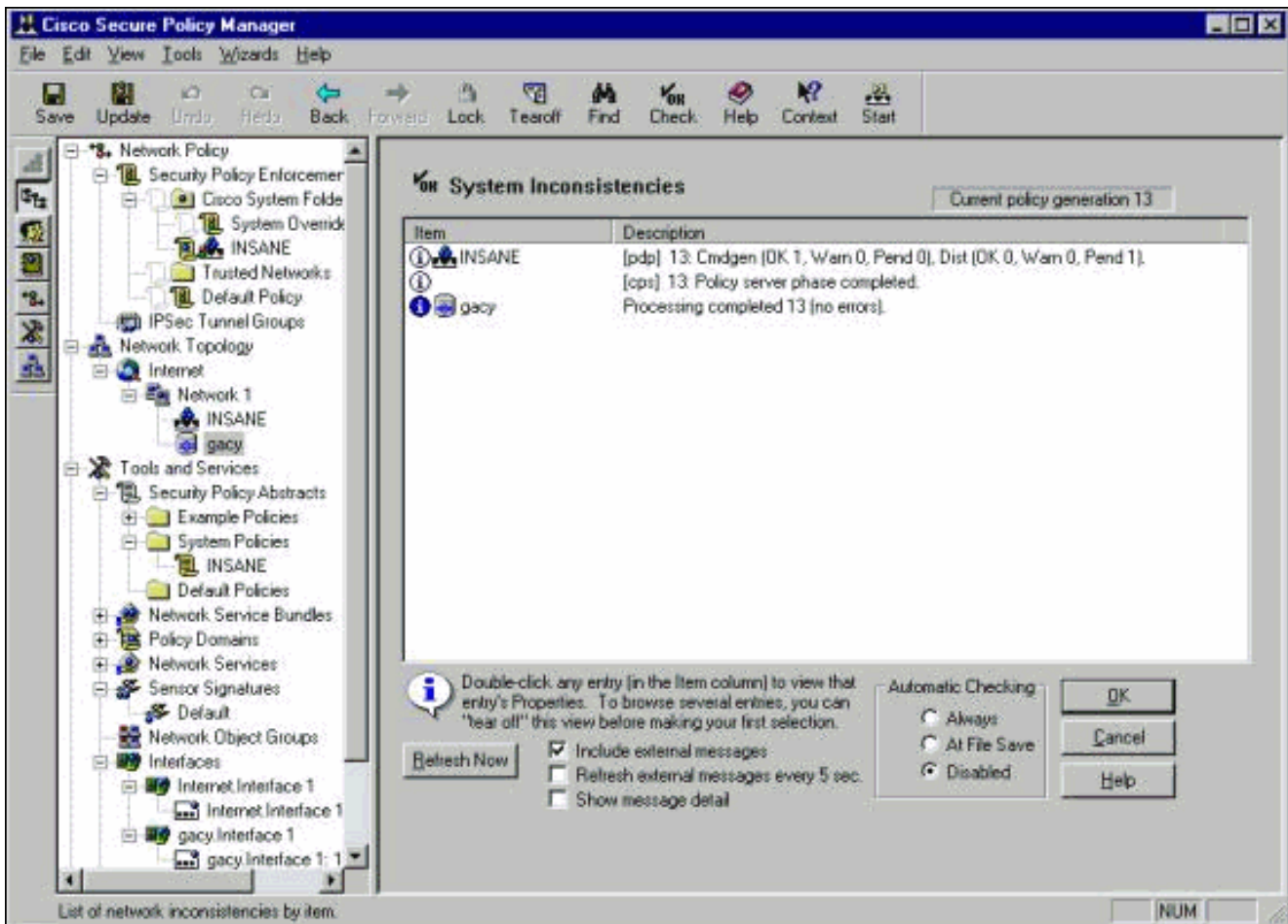
1. حدد المستشعر في مخطط CSPM الخاص بك وانقر فوق علامة تبويب الاستشعار.
2. تعريف جهاز التقاط الحزمة: iprb0 - لمستشعر IDS 4210spwr0 - لأي طراز مستشعر آخر



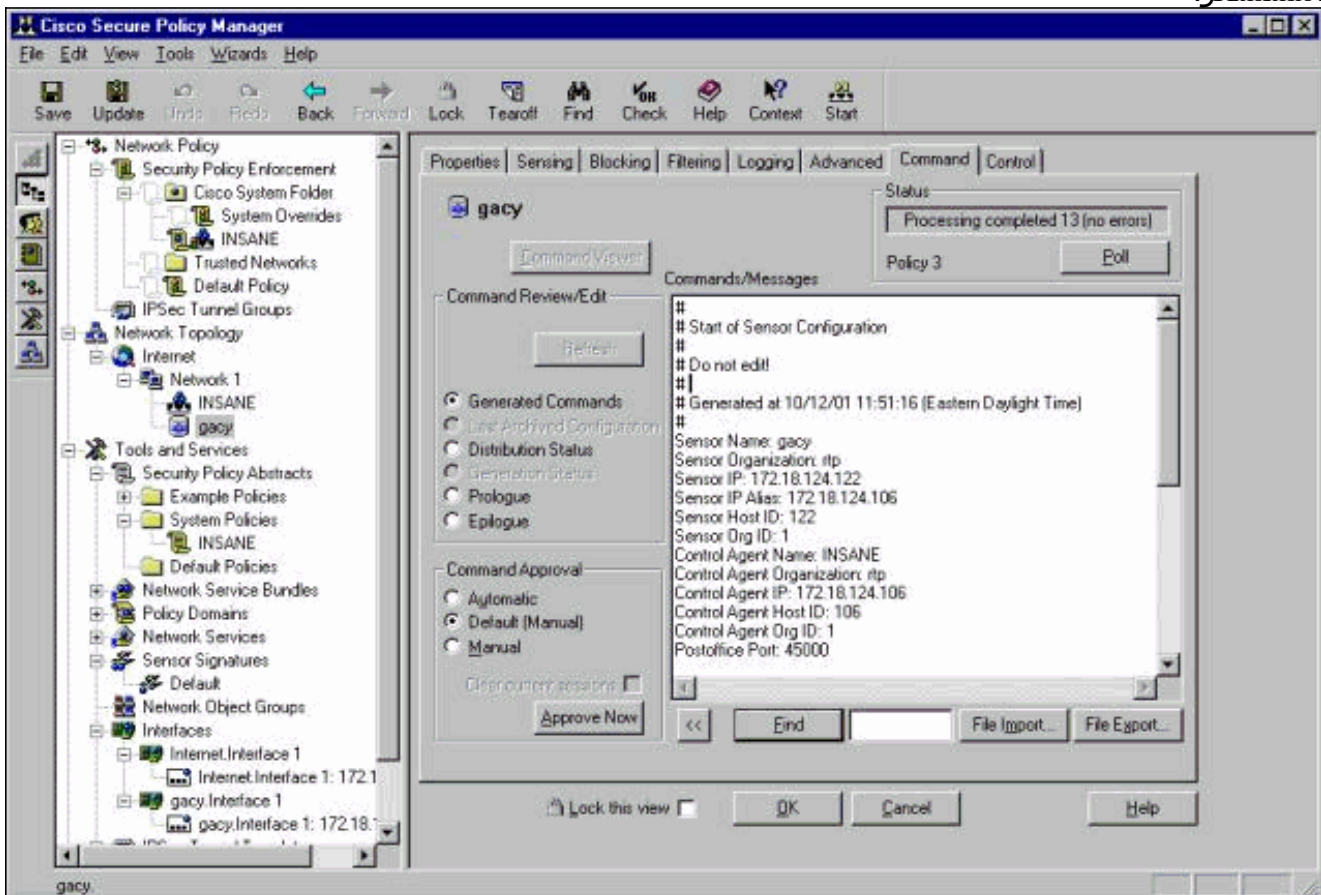
3. انقر فوق موافق" للمتابعة.

4. انقر فوق رمز التحديث في شريط قائمة CSPM لتحديث CSPM بالمعلومات. ملاحظة: إذا سار كل شيء على ما يرام، تظهر شاشة مماثلة. لاحظ أنه لا توجد أخطاء حمراء. التحذيرات الصفراء عادة ما تكون موافق.



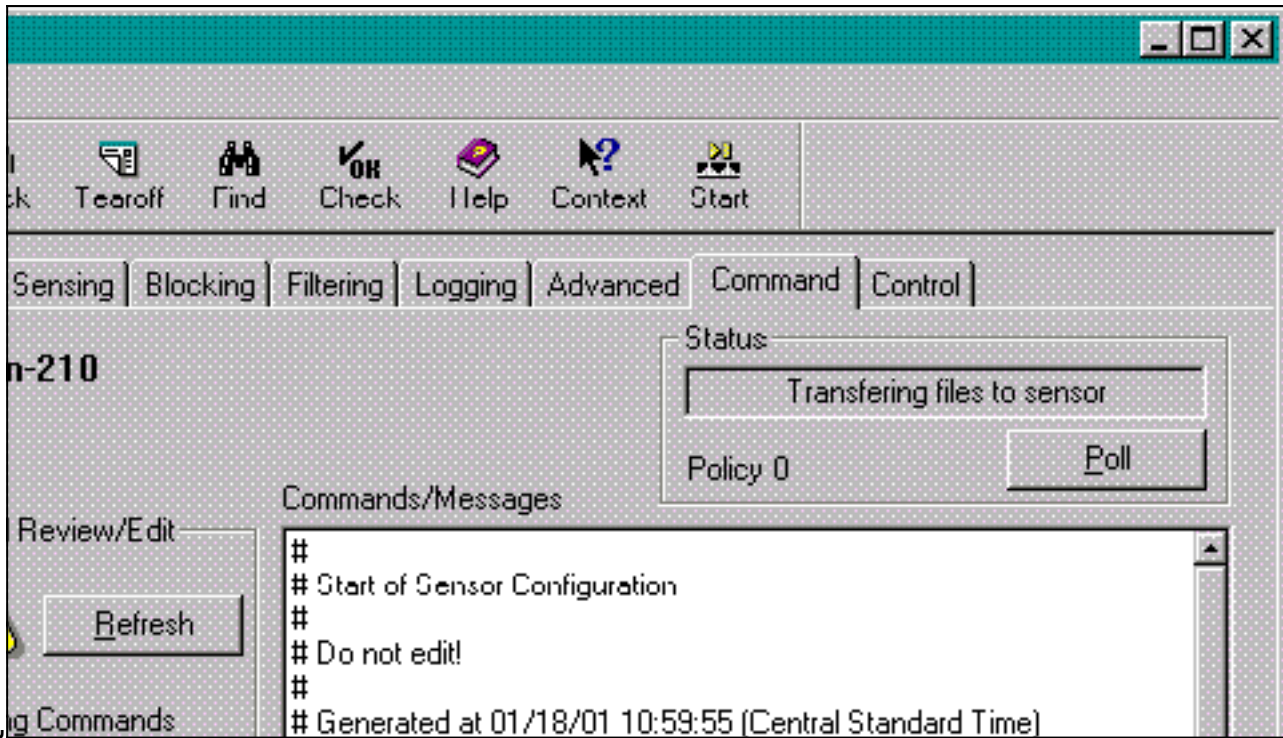


5. حدد المستشعر في مخطط الشبكة وانقر فوق علامة التبويب "أمر" لإرسال التكوين المحدث إلى المستشعر.

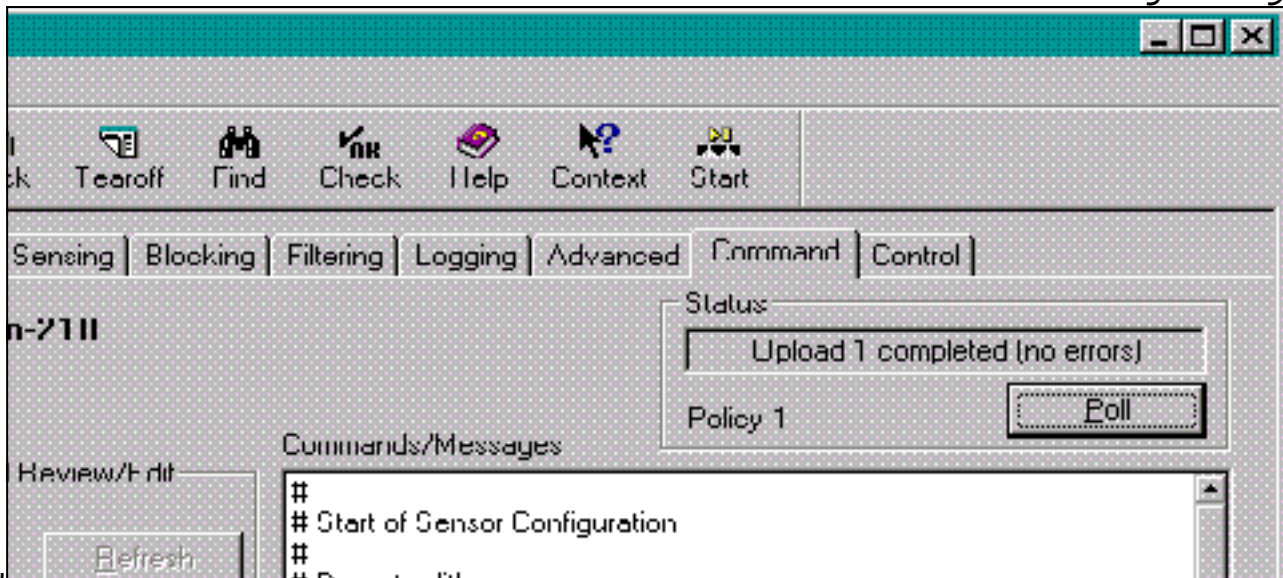


6. انقر فوق الزر موافقة الآن لإرسال التكوين إلى المستشعر.

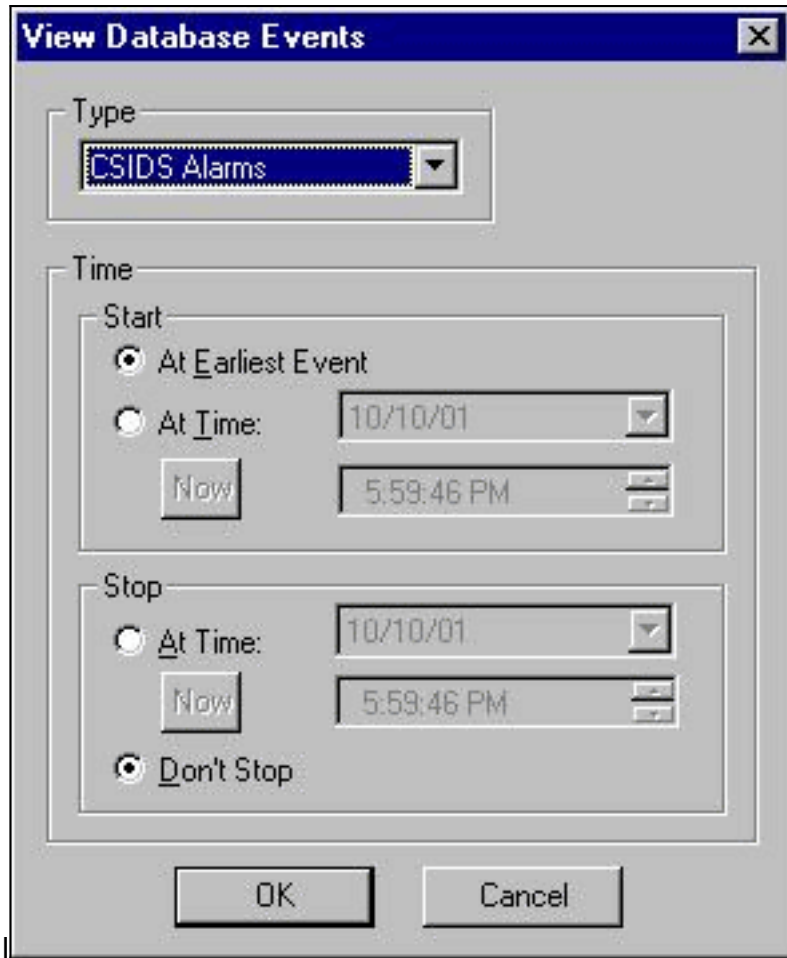




رض جزء الحالة الرسالة "تحميل <#> مكتمل". وهذا يشير إلى عملية نقل صحيحة وكاملة. تم تحديث "المستشعر" الآن ويجب تشغيله الآن بشكل طبيعي. إذا لم يكن المستشعر يعمل بشكل طبيعي، فارجع إلى المستشعر وفحص إخراج الأمر nrconns للتأكد من إنشاء الاتصال بين مضيف CSPM والمستشعر.



د اكتمال هذا الإجراء، يمكنك البحث عن تنبيهات يرسلها المستشعر إلى مضيف CSPM في عارض الأحداث. لعرض عارض الأحداث، من قائمة CSPM الرئيسية حدد أدوات < عرض أحداث المستشعر > قاعدة



انقر فوق موافق لعرض نافذة قاعدة

البيانات.

بيانات الأحداث. ستختلف شاشتك حسب الإنذارات التي قد تلقاها.

Count	Name	Source Address	Dest Address	Details	Source Loc	Dest Loc	SubSig ID	Severity	Org Name
1134	ICMP echo request	*							
48	ICMP flood	+							
6	ICMP smurf attack	+							
6	ICMP unreachable	10.32.10.10	172.18.124.154	<none>	OUT	OUT	0	Low	ntp
40	IP fragments overlap	+							
38	Net sweep-echo	+							
4	PostOffice Initial Notification	<none>	<none>	postofficed initial notification msg	OUT	OUT	0	Low	ntp
24	Route Down!	<none>	<none>	+					
29	Route Up	<none>	<none>	*					
7	UDP Packet	+							

## [معلومات ذات صلة](#)

