تكوين IOS IPS من Cisco باستخدام مدخل الموجه و SDM

المحتويات

المقدمة

يصف هذا المستند كيفية إستخدام الإصدار 2.5 من Cisco Router و Security Device Manager (SDM) لتكوين نظام منع التسلل (IPS) Cisco IOS® في الإصدار 12.4(15)T3 والإصدارات الأحدث.

التحسينات في إدارة قاعدة بيانات المحول (SDM 2.5) المتعلقة ب IOS IPS هي:

- إجمالي رقم التوقيع المحول برمجيا المعروض في واجهة المستخدم الرسومية (GUI) لقائمة التوقيع
- يمكن تنزيل ملفات توقيع SDM (تنسيق ملف zip، على سبيل المثال، sigv5-SDM-S307.zip) وحزم توقيع CLI (تنسيق ملف pkg؛ على سبيل المثال، IOS-S313-CLI.pkg) معا في عملية واحدة
- يمكن دفع حزم التوقيع التي تم تنزيلها تلقائيا إلى الموجه كخيار

المهام المتعلقة بعملية الإمداد الأولية هي:

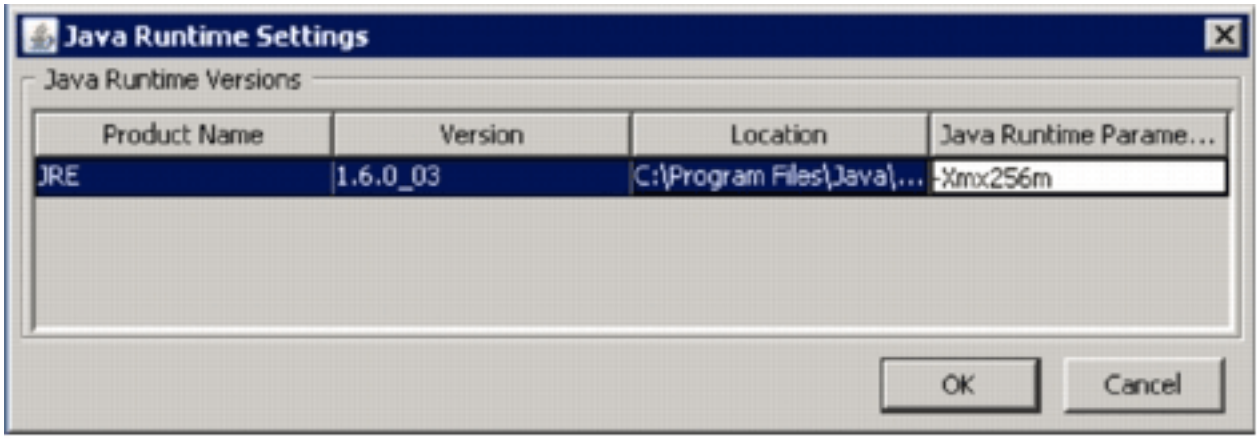
1. تنزيل SDM 2.5 وتثبيته.
2. أستخدم التحديث التلقائي لميزة إدارة قاعدة بيانات المحول (SDM) لتنزيل حزمة توقيع IOS IPS إلى جهاز كمبيوتر محلي.
3. قم بتشغيل معالج سياسات IPS لتكوين IOS IPS.
4. تحقق من تحميل تكوين IOS IPS وتواقيع بشكل صحيح

Cisco SDM هي أداة تكوين مستندة إلى الويب تعمل على تبسيط تكوين الموجه والأمان من خلال المعالجات الذكية التي تساعد العملاء على نشر موجه Cisco وتكوينه ومراقبته بسرعة وسهولة دون طلب معرفة واجهة سطر الأوامر (CLI).

يمكن تنزيل الإصدار 2.5 من إدارة قاعدة بيانات المحول (SDM) من Cisco.com على http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (للعملاء المسجلين فقط). يمكن العثور على ملاحظة الإصدار على http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

ملاحظة: تتطلب إدارة قاعدة بيانات المحول (SDM) من Cisco دقة شاشة تبلغ 1024 × 768 على الأقل.

ملاحظة: يتطلب إدارة قاعدة بيانات المحول (SDM) من Cisco ألا يقل حجم كومة ذاكرة Java عن 256 ميجابايت لتكوين IOS IPS. لتغيير حجم كومة ذاكرة Java، افتح لوحة تحكم Java، وانقر فوق علامة التبويب **Java**، وانقر فوق **عرض** الموجود ضمن إعدادات وقت تشغيل تطبيق Java، ثم أدخل **-XMX256m** في عمود معلمات وقت تشغيل Java.



المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS IPS في الإصدار 12.4(15)T3 والإصدارات الأحدث من Cisco
- Cisco Router and Security Device Manager (SDM)، الإصدار 2.5

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

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

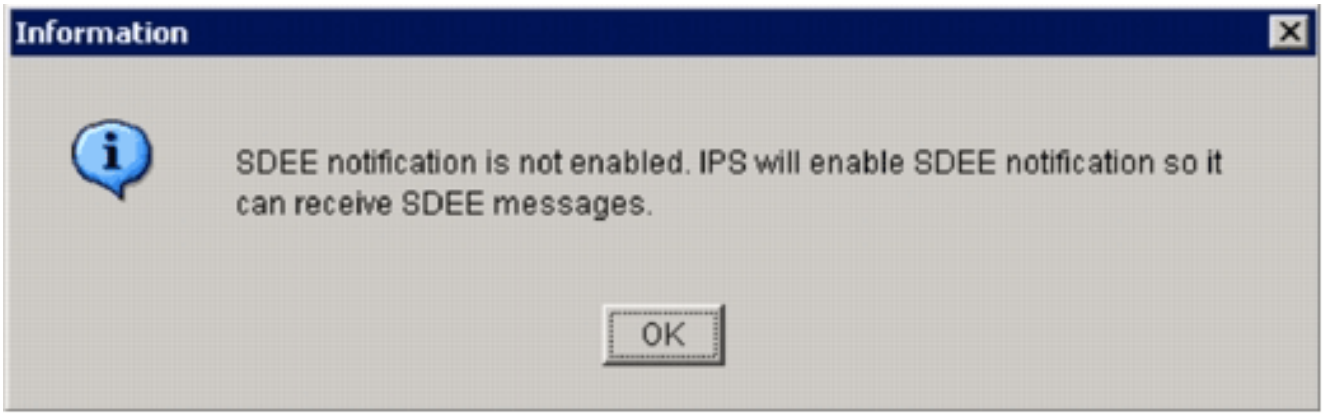
التكوين

ملاحظة: افتح وحدة تحكم أو جلسة عمل على برنامج Telnet إلى الموجه (مع تشغيل "مراقبة المصطلحات") لمراقبة الرسائل عند إستخدام إدارة قاعدة بيانات المحول (SDM) لتوفير IOS IPS.

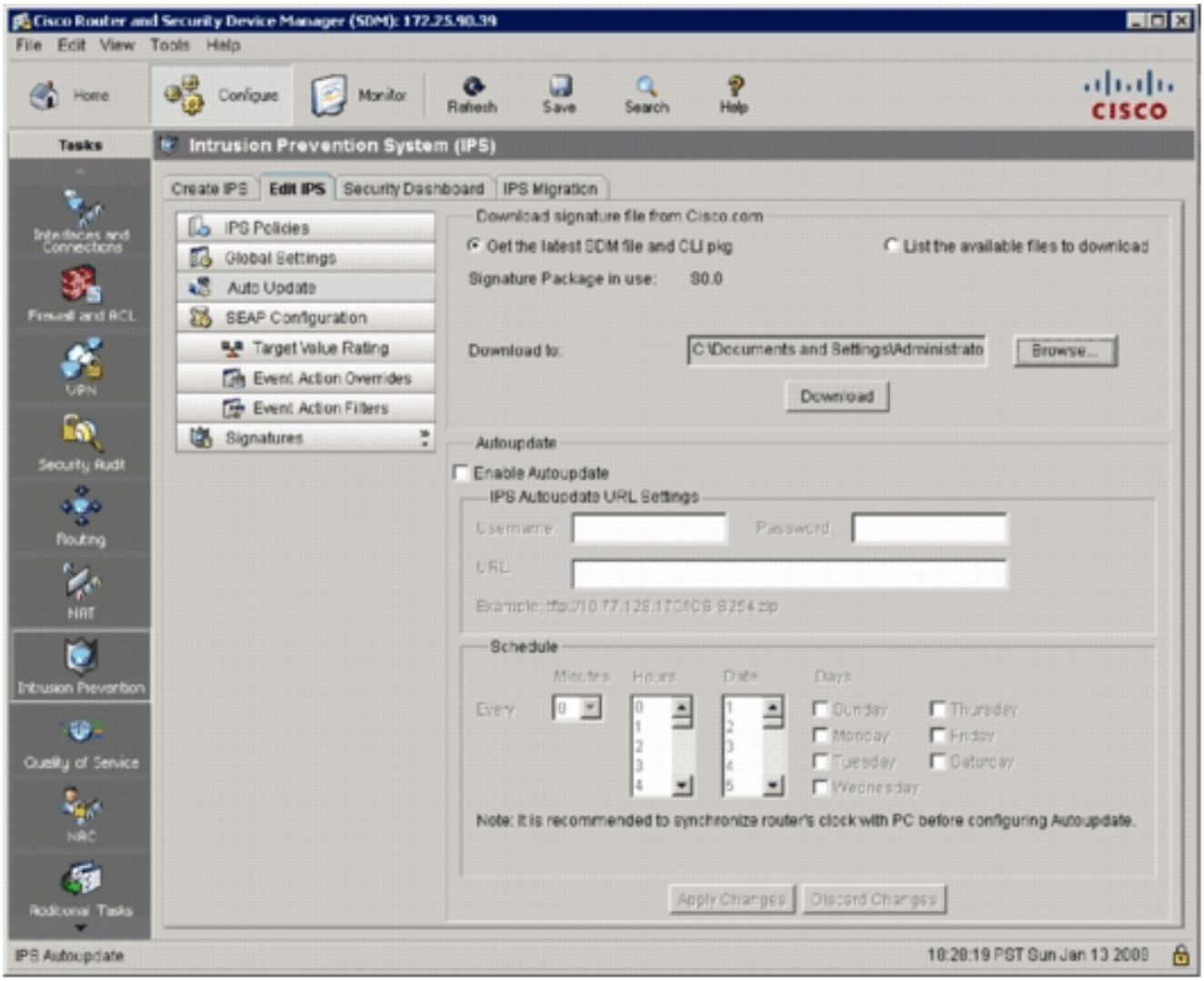
1. قم بتنزيل SDM 2.5 من Cisco.com على http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (العملاء المسجلون فقط) وتثبيته على جهاز كمبيوتر محلي.
2. قم بتشغيل SDM 2.5 من الكمبيوتر المحلي.
3. عند ظهور شاشة تسجيل الدخول إلى IOS IPS، أدخل نفس اسم المستخدم وكلمة المرور اللذين تستخدمهما

لمصادقة SDM للموجه.

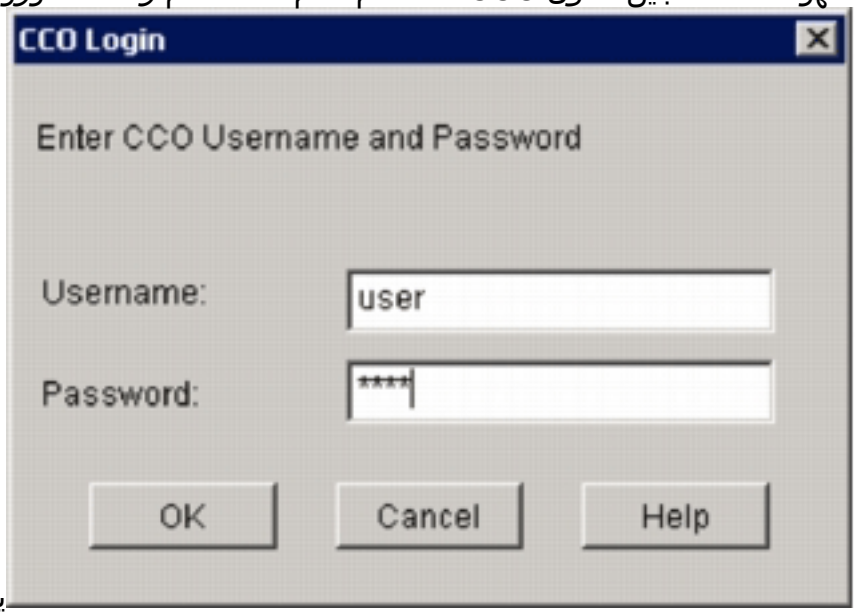
4. من واجهة مستخدم إدارة قاعدة بيانات المحول (SDM)، انقر فوق **تكوين**، ثم انقر فوق **منع التسلل**.
5. انقر فوق علامة التبويب **تحرير IPS**.
6. إذا لم يتم تمكين إعلام SDEE على الموجه، انقر فوق **موافق** لتمكين إعلام SDEE.



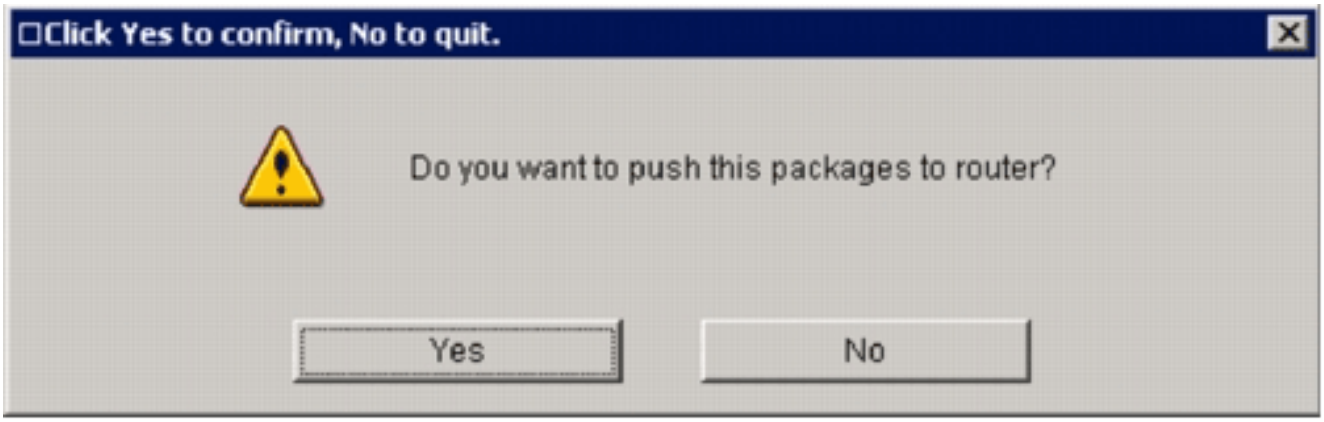
7. في منطقة تنزيل التوقيع من Cisco.com من علامة التبويب تحرير IPS، انقر فوق الزر **الحصول على أحدث ملف SDM و CLI PKG** للإرسال اللاسلكي، ثم انقر فوق **إستعراض** لتحديد دليل على الكمبيوتر المحلي يتم فيه حفظ الملفات التي تم تنزيلها.يمكنك إختيار الدليل الجذر لخادم TFTP أو FTP، والذي سيتم إستخدامه لاحقا عند نشر حزمة التوقيع على الموجه.
8. انقر فوق **تنزيل**.



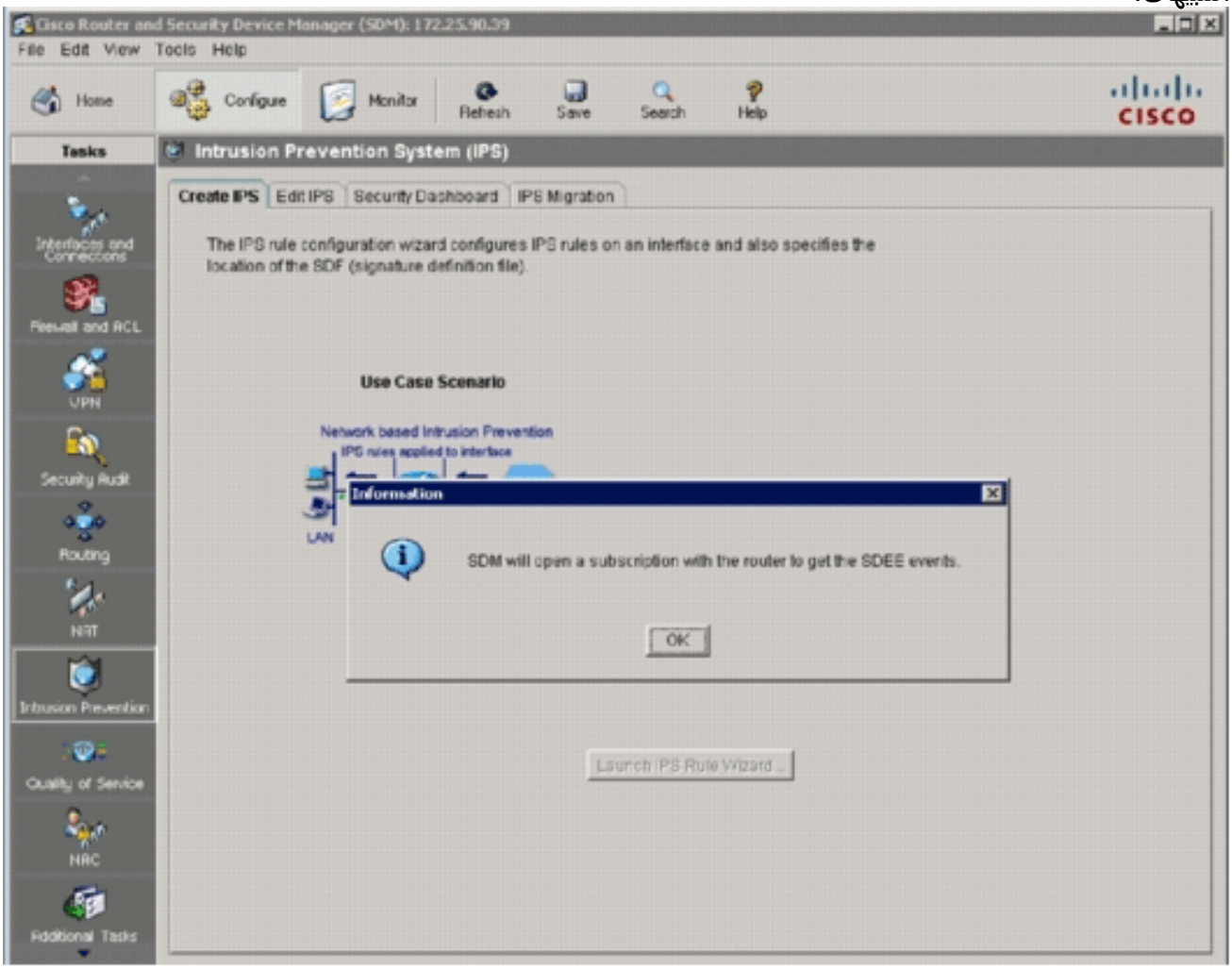
9. عندما تظهر شاشة تسجيل دخول CCO، أستخدم اسم المستخدم وكلمة المرور المسجلين ل



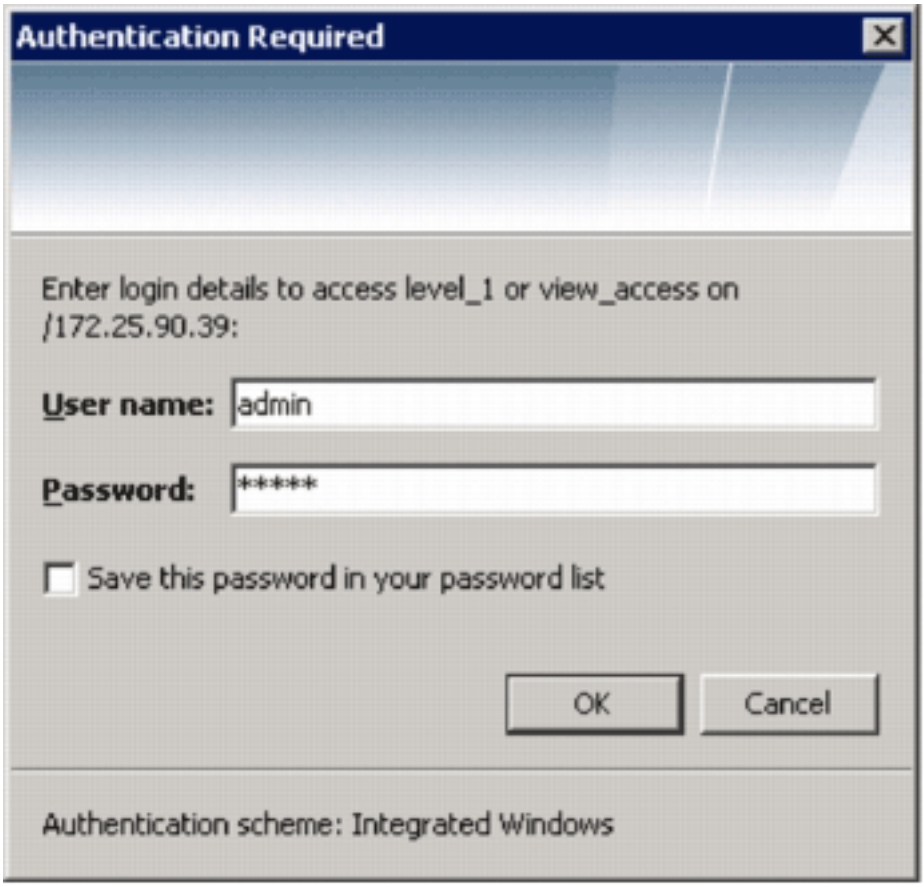
CCO. يتصل إدارة قاعدة بيانات المحول (SDM) ب Cisco.com ويبدأ في تنزيل كل من ملف إدارة قاعدة بيانات المحول (على سبيل المثال، sigv5-SDM-S307.zip) وملف CLI PKG (على سبيل المثال، IOS-S313-CLI.pkg) إلى الدليل المحدد في الخطوة 7.بمجرد تنزيل كلا الملفين، يطالبك إدارة قاعدة بيانات المحول (SDM) بدفع حزمة التوقيع التي تم تنزيلها إلى الموجه.



10. انقر فوق **لا** لأنه لم يتم تكوين IPS لبرنامج IOS على الموجه حتى الآن.
11. بعد أن يقوم إدارة قاعدة بيانات المحول (SDM) بتنزيل أحدث حزمة توقيع واجهة سطر الأوامر (CLI) لبرنامج IOS، انقر فوق علامة التبويب **إنشاء** بروتوكول **IPS** لإنشاء تكوين IOS IPS الأولي.
12. إذا طلب منك تطبيق التغييرات على الموجه، انقر فوق **تطبيق التغييرات**.
13. انقر فوق **معالج قاعدة تشغيل IPS**.يبدو أن أحد مربعات الحوار ينبئك بأن إدارة قاعدة بيانات المحول (SDM) بحاجة إلى إنشاء اشتراك SDEE بالموجه لاسترداد التنبيهات.

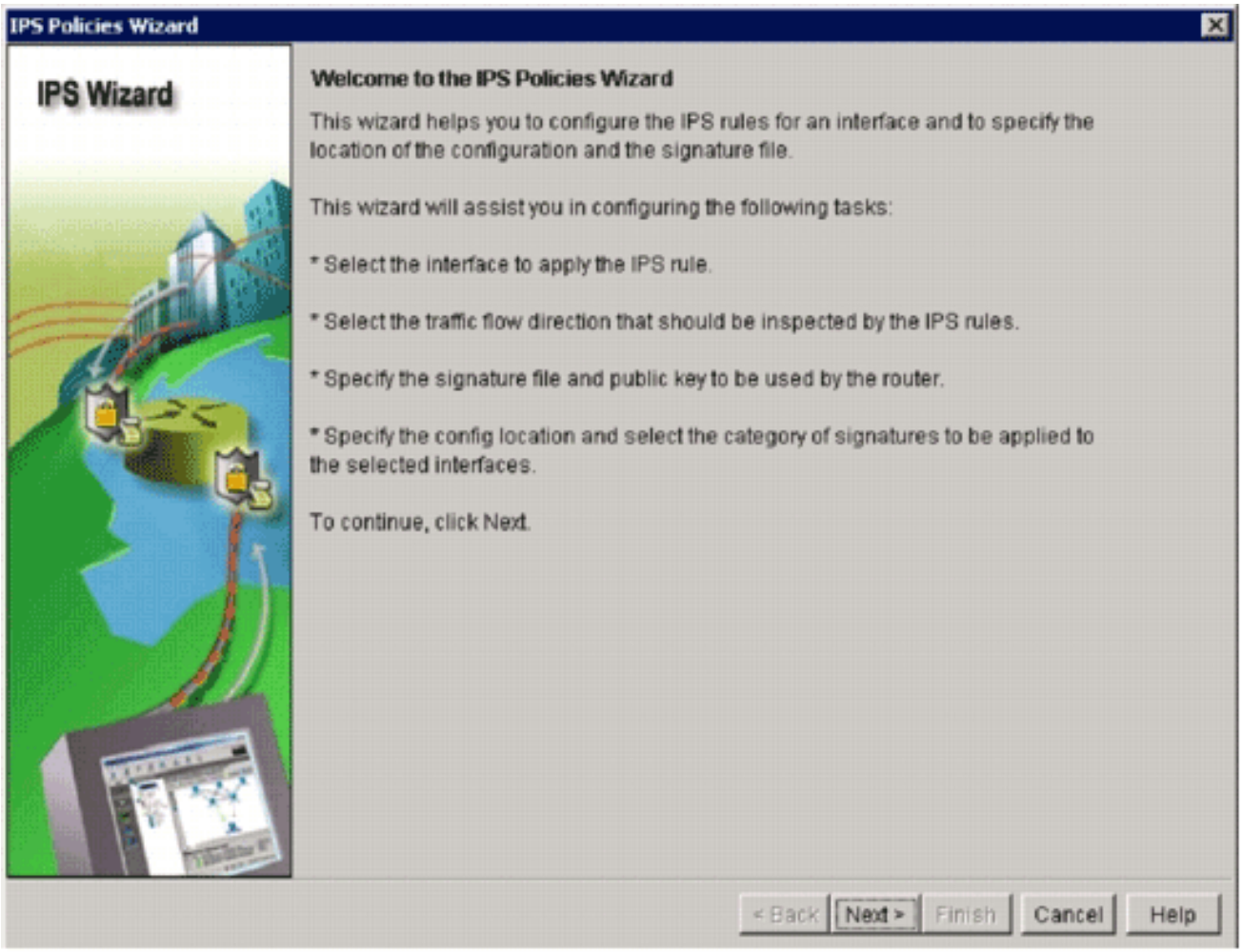


14. وانقر فوق **OK**.يظهر مربع الحوار يتطلب

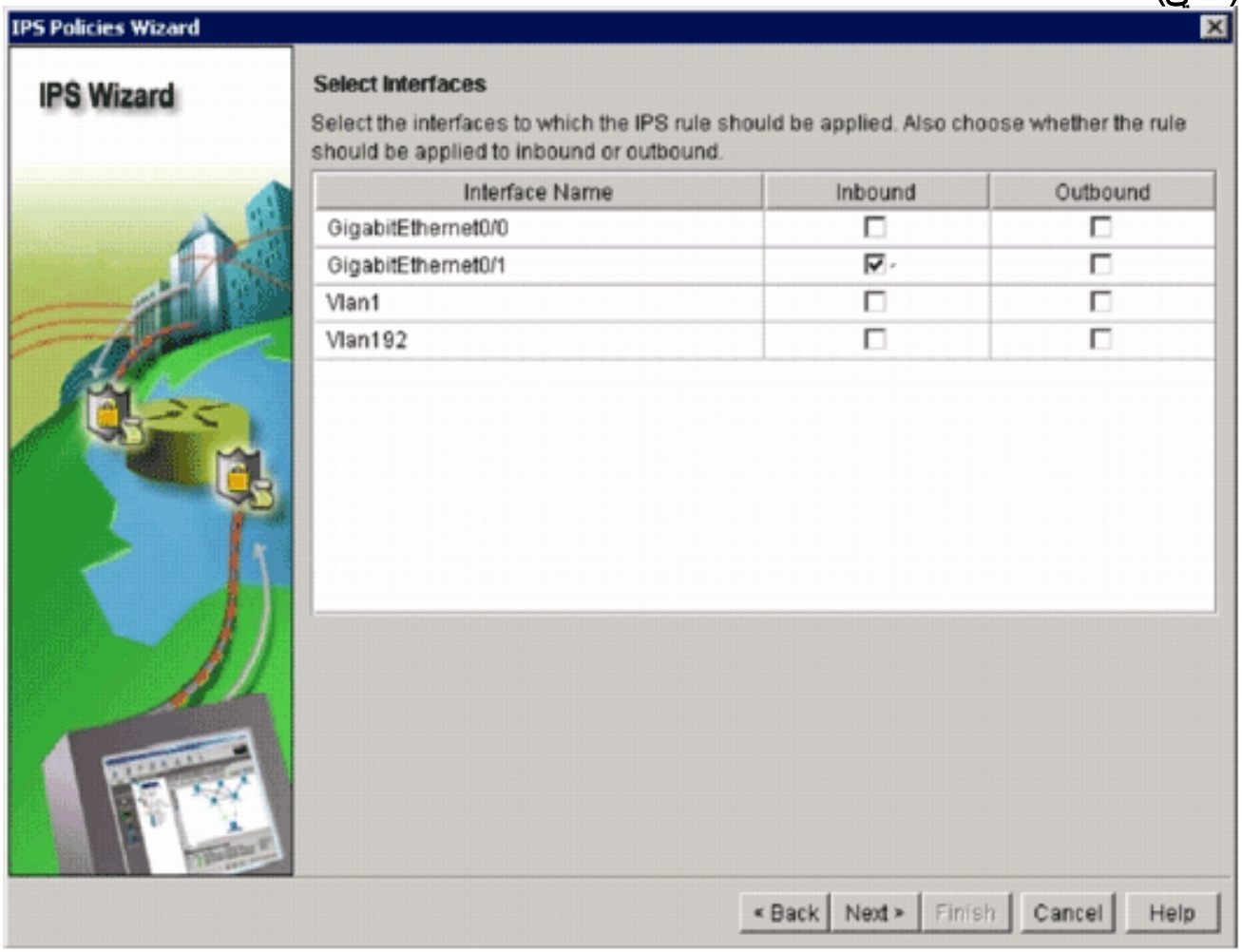


المصادقة.

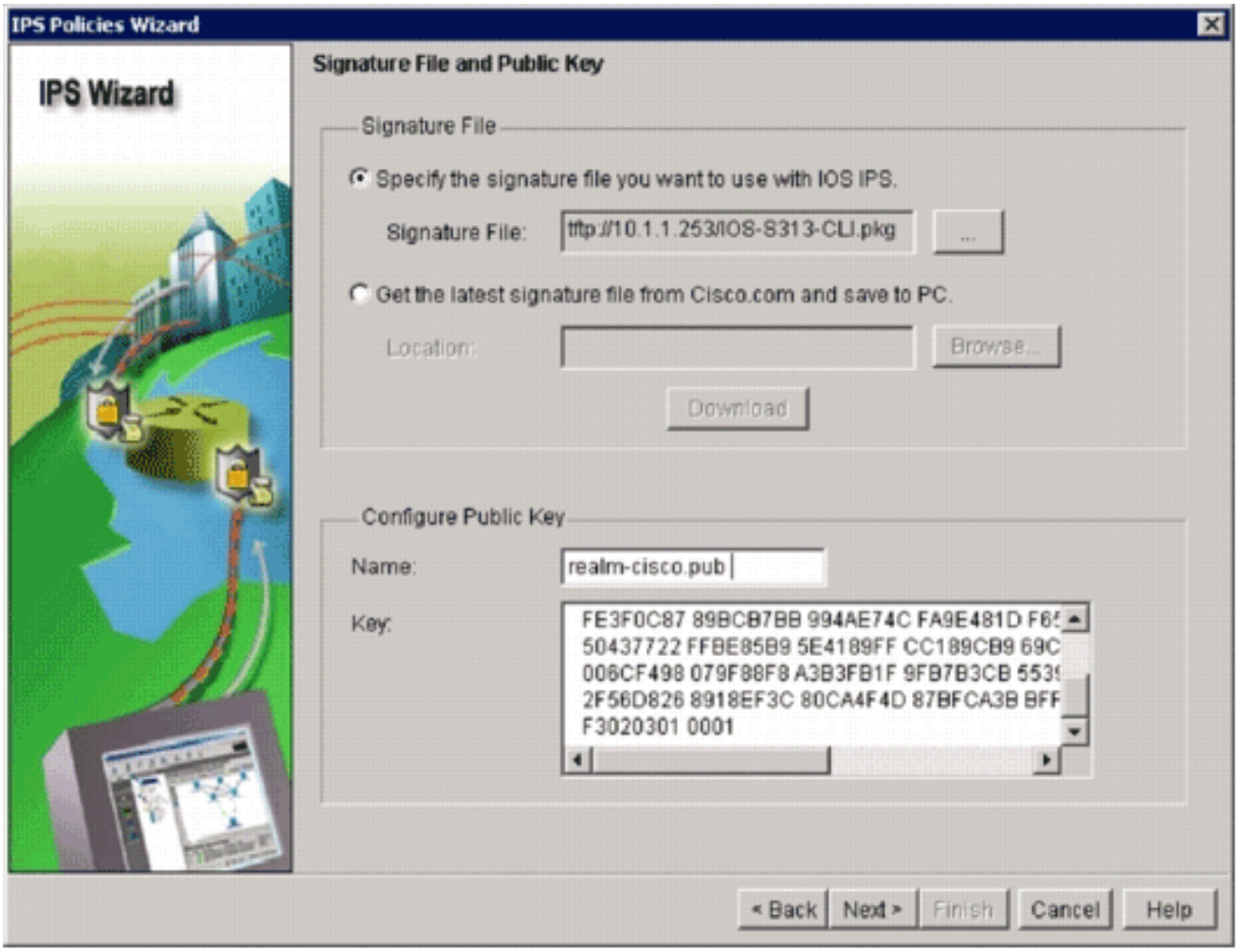
15. أدخل اسم المستخدم وكلمة المرور اللذين أستخدمتهما لإدارة قاعدة بيانات المحول (SDM) للمصادقة على الموجه، وانقر فوق **موافق**.سوف يظهر مربع الحوار معالج نهج IPS.



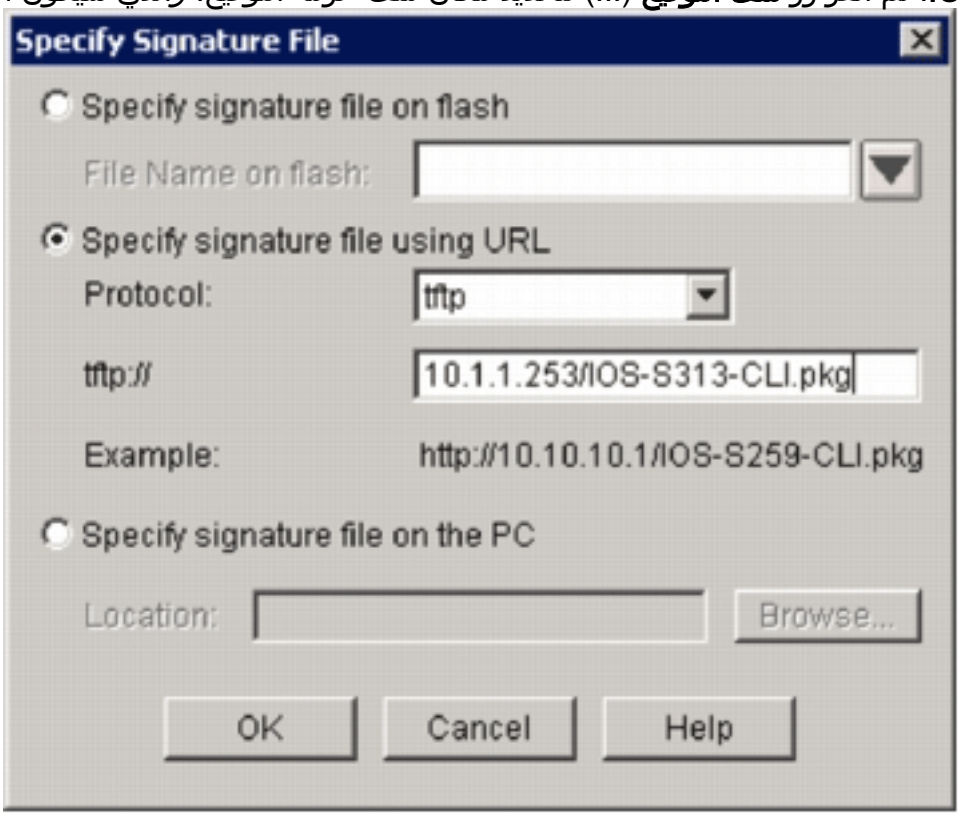
16. انقر فوق **Next** (التالي).



17. في نافذة "الواجهات المحددة"، أختر الواجهة والاتجاه الذي سيتم تطبيق IOS IPS عليه، ثم انقر فوق **التالي** للمتابعة.



18. في منطقة ملف التوقيع من نافذة ملف التوقيع والمفتاح العام، انقر **زر تحديد ملف التوقيع الذي تريد إستخدامه مع IOS IPS**، ثم انقر زر **ملف التوقيع** (...) لتحديد مكان ملف حزمة التوقيع، والذي سيكون الدليل المحدد في الخطوة 7.



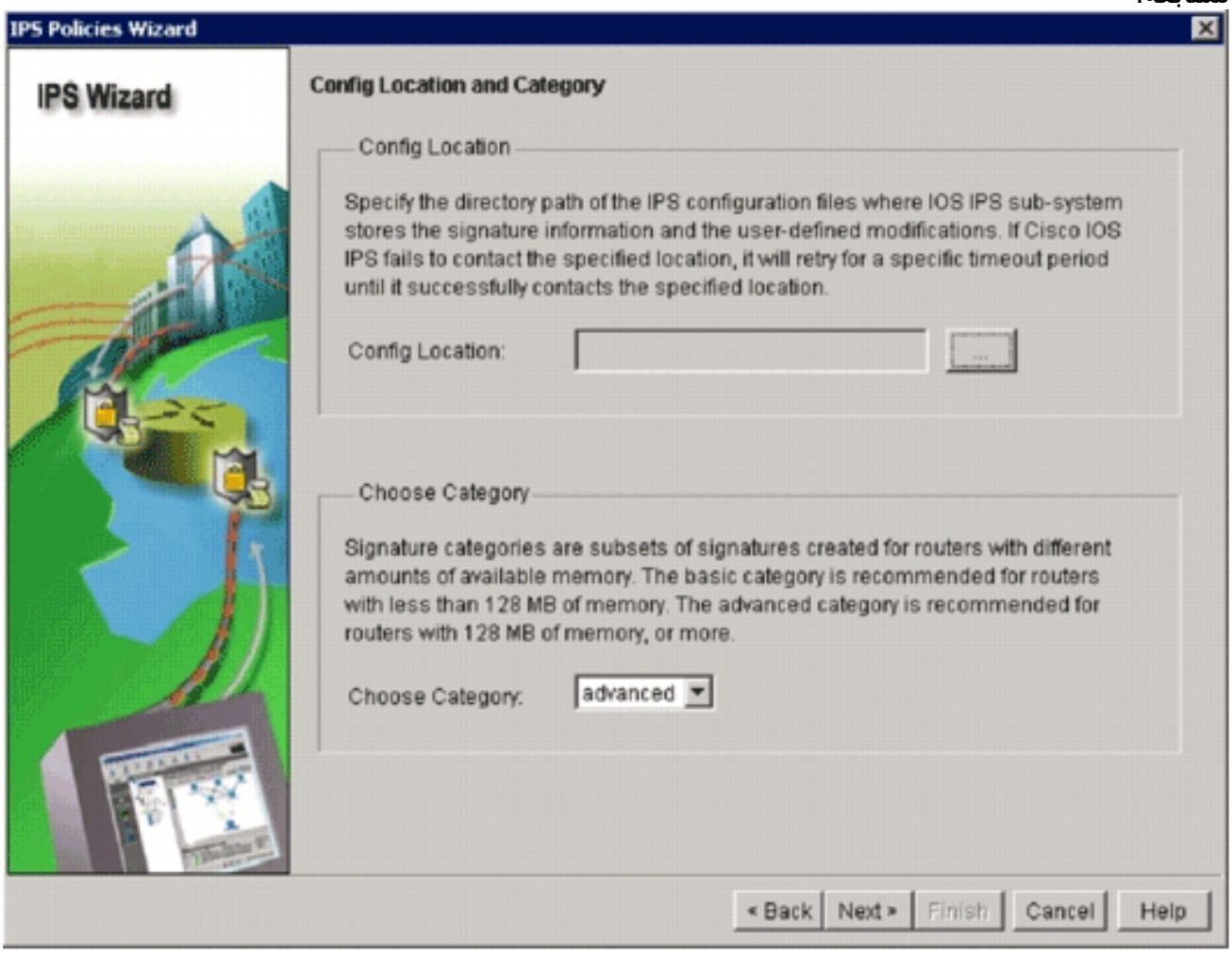
19. انقر زر **تحديد ملف توقيع باستخدام** انتقاء **عنوان URL**، واختر بروتوكول من القائمة المنسدلة للبروتوكول.**ملاحظة:** يستخدم هذا المثال بروتوكول TFTP لتنزيل حزمة التوقيع إلى الموجه.
20. أدخل عنوان ربط ملف التوقيع، وانقر **موافق**.

21. في منطقة تكوين المفتاح العام من ملف التوقيع ونافذة المفتاح العام، أدخل **realm-cisco.pub** في حقل الاسم، ثم انسخ هذا المفتاح العام ولصقه في حقل المفتاح.

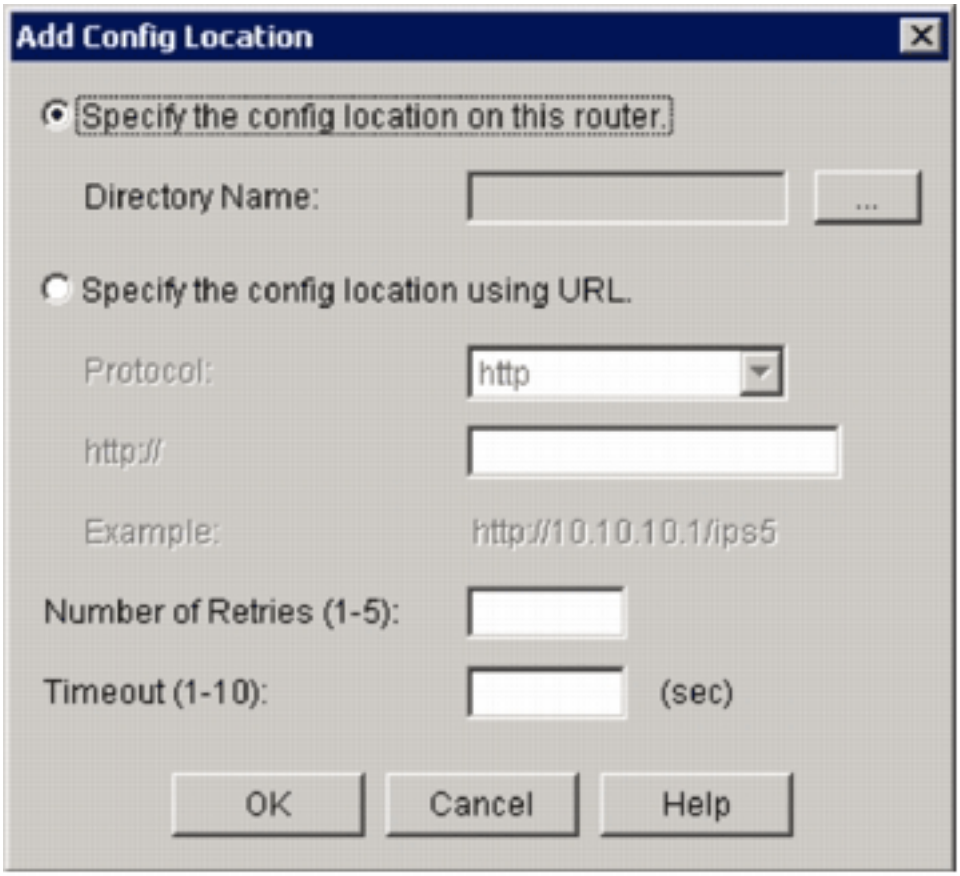
```
300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 30820122

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36 50437722

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001
```

ملاحظة: يمكن تنزيل هذا المفتاح العام من Cisco.com على: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (للعملاء المسجلين فقط).

22. انقر فوق **التالي** للمتابعة.

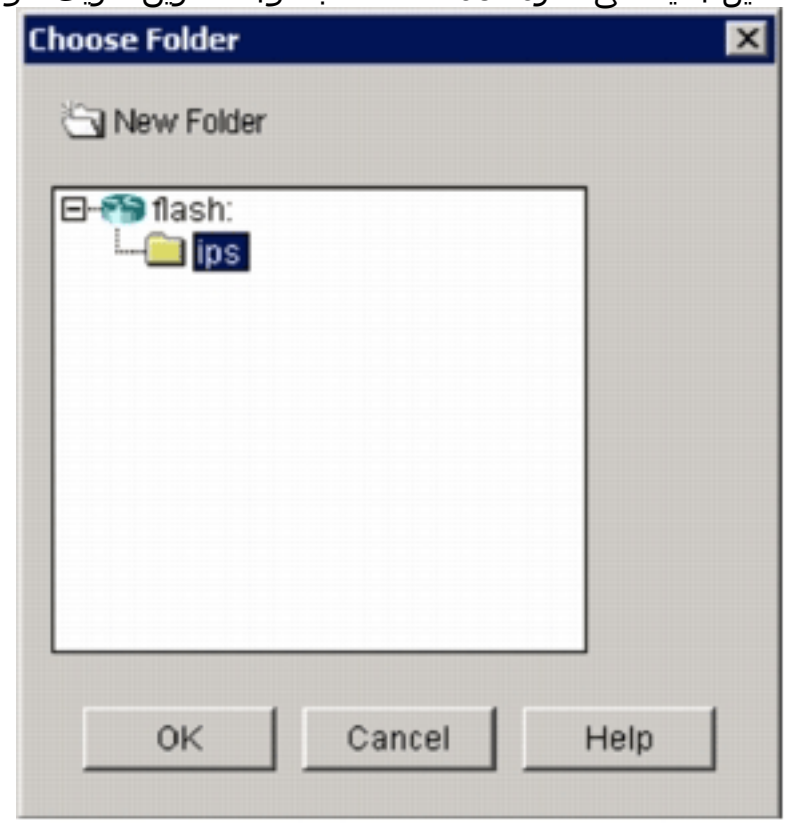


23. في نافذة "موقع التكوين والفئة"، انقر فوق الزر **تكوين موقع** (...) لتحديد موقع يتم فيه تخزين ملفات تعريف التوقيعات والتكوين.يظهر مربع الحوار **إضافة موقع**



تكوين.

24. في مربع الحوار إضافة موقع تكوين، انقر فوق **تحديد موقع التكوين على** زر راديو **الموجه هذا**، ثم انقر فوق الزر **اسم الدليل** (...) لتحديد موقع ملف التكوين.يظهر مربع الحوار إختيار مجلد للسماح لك بتحديد دليل موجود أو إنشاء دليل جديد على ذاكرة Flash الخاصة بالموجه لتخزين تعريف التوقيع وملفات

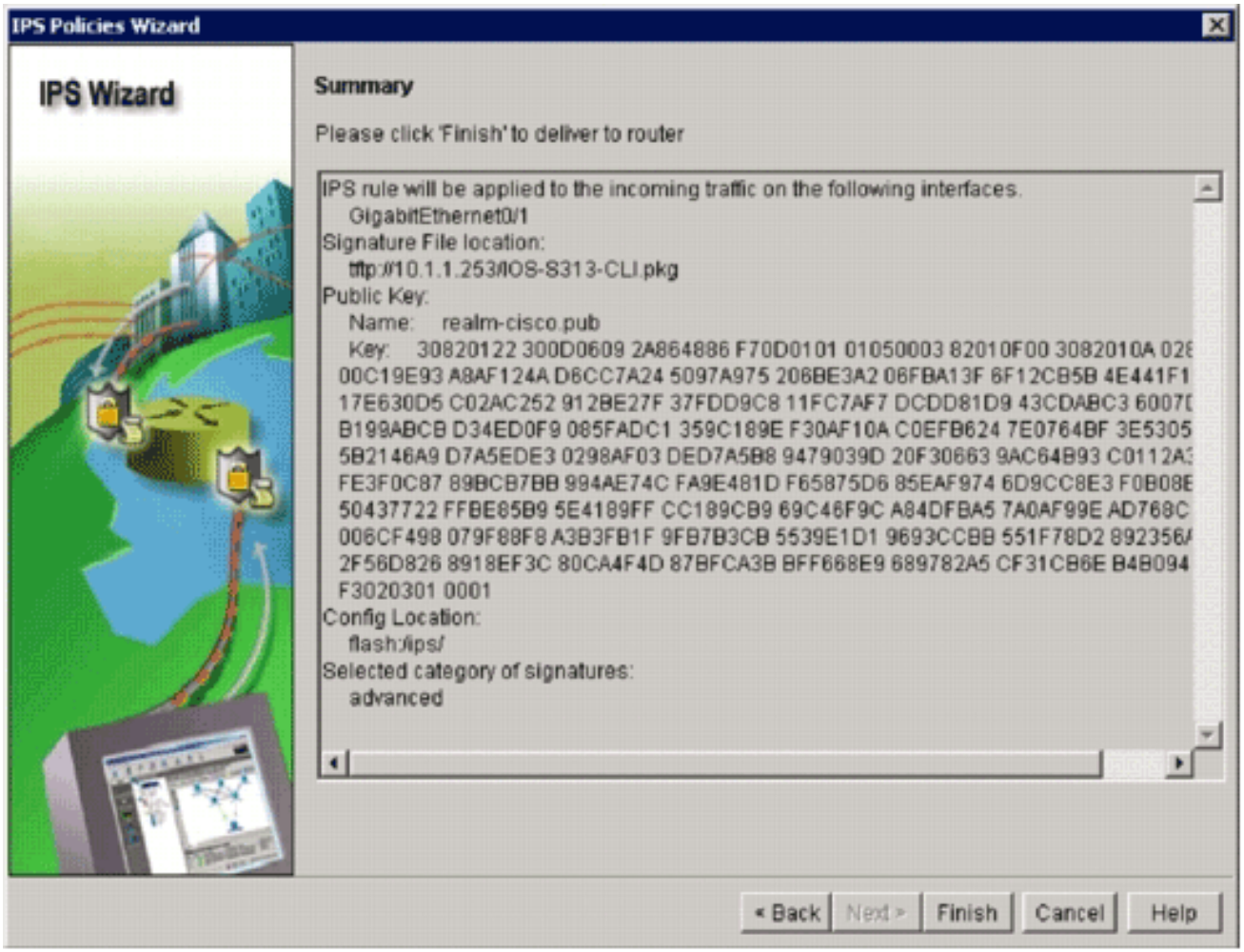


التكوين.

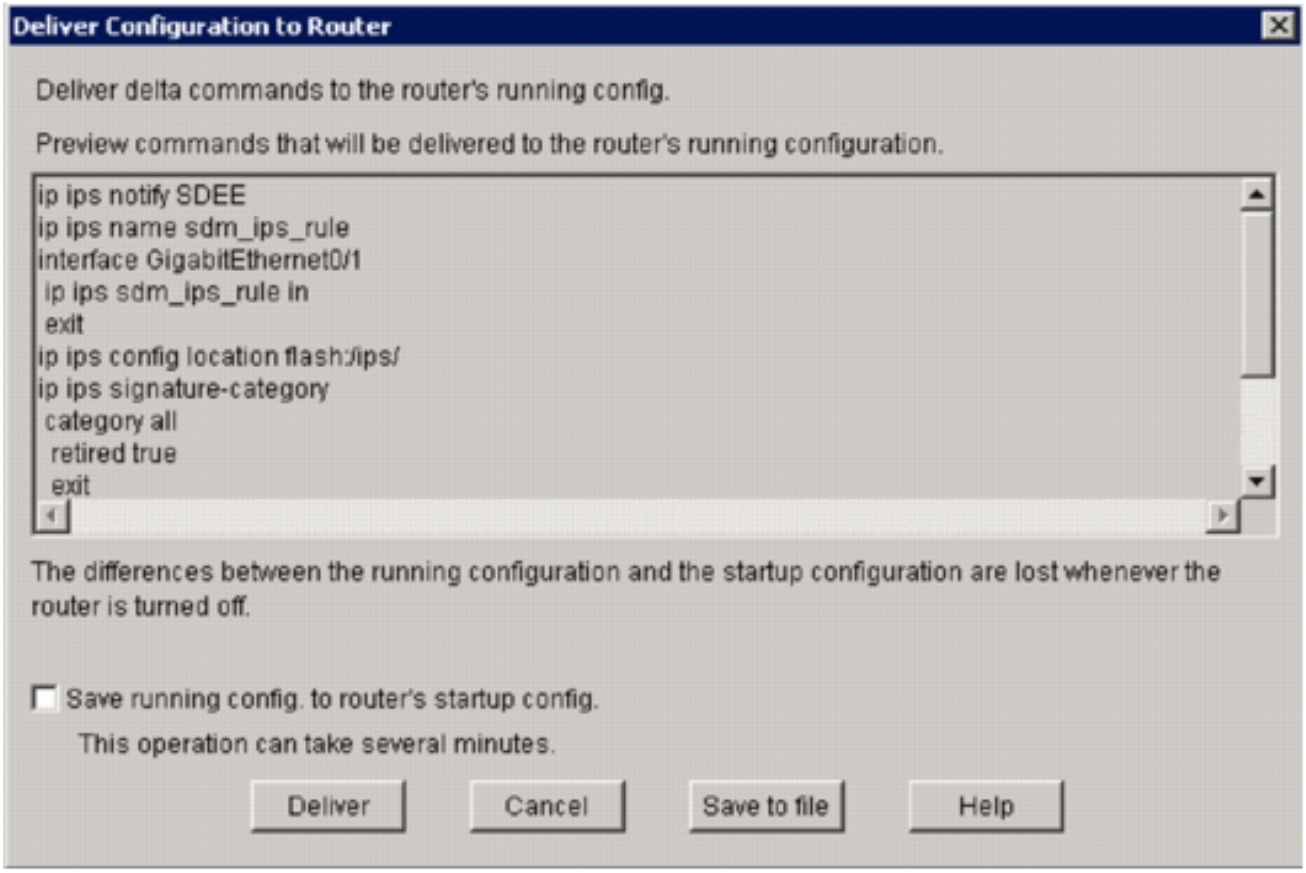
25. انقر **مجلد جديد** موجود في أعلى الشاشة إذا كنت تريد إنشاء دليل جديد.
26. بمجرد تحديد الدليل، انقر فوق **موافق** لتطبيق التغييرات، ثم انقر فوق **موافق** لإغلاق مربع الحوار إضافة موقع التكوين.
27. في شاشة معالج سياسات IPS، حدد فئة التوقيع طبقا لمقدار الذاكرة المثبتة على الموجه. هناك فئتان للتوقيع يمكنك إختيارهما في إدارة قاعدة بيانات المحول (SDM): أساسي ومتقدم.إذا كان الموجه مثبت عليه DRAM

سعة 128 ميجابايت، فإن Cisco توصيك باختيار الفئة الأساسية لتجنب حالات فشل تخصيص الذاكرة. إذا كان الموجه مثبتا عليه 256 ميجابايت أو أكثر من DRAM، فيمكنك إختيار أي من الفئتين.

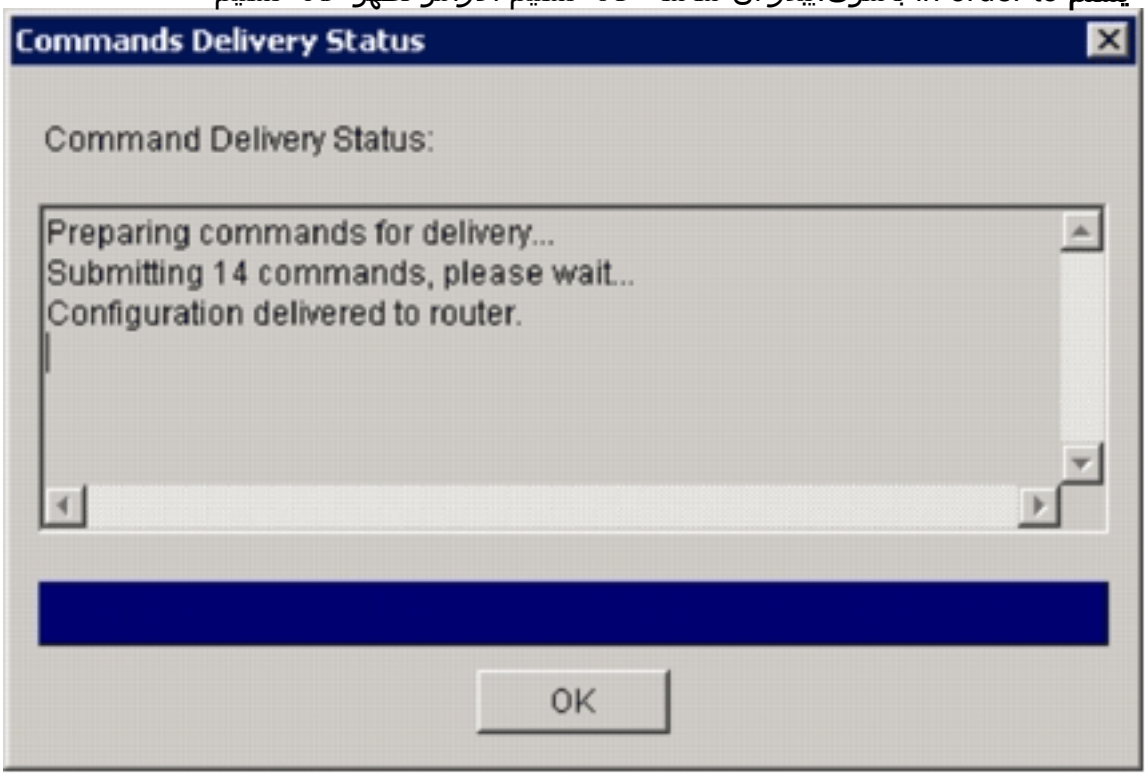
28. بمجرد تحديد فئة لاستخدامها، انقر فوق **التالي** للمتابعة إلى صفحة الملخص.توفر صفحة الملخص وصفا موجزا حول التكوين الأولي ل IOS IPS.



29. انقر فوق **إنهاء**" في صفحة الملخص لتسليم التكوينات وحزمة التوقيع إلى الموجه.إذا تم تمكين خيار أوامر المعاينة على إعدادات التفضيلات في إدارة قاعدة بيانات المحول (SDM)، يعرض إدارة قاعدة بيانات المحول (SDM) مربع الحوار تسليم التكوين إلى الموجه الذي يعرض ملخصا لأوامر واجهة سطر الأوامر (CLI) التي يوفرها إدارة قاعدة بيانات المحول (SDM) إلى الموجه.

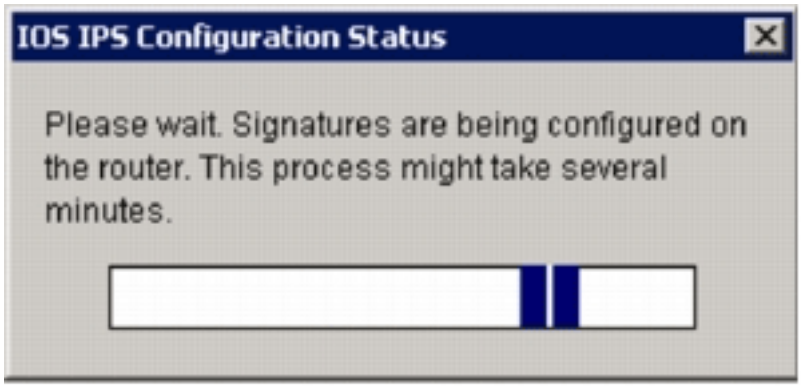


30. طقطقة **يسلم** in order to باشرت.يبدو أن شاشة حالة تسليم الأوامر تظهر حالة تسليم



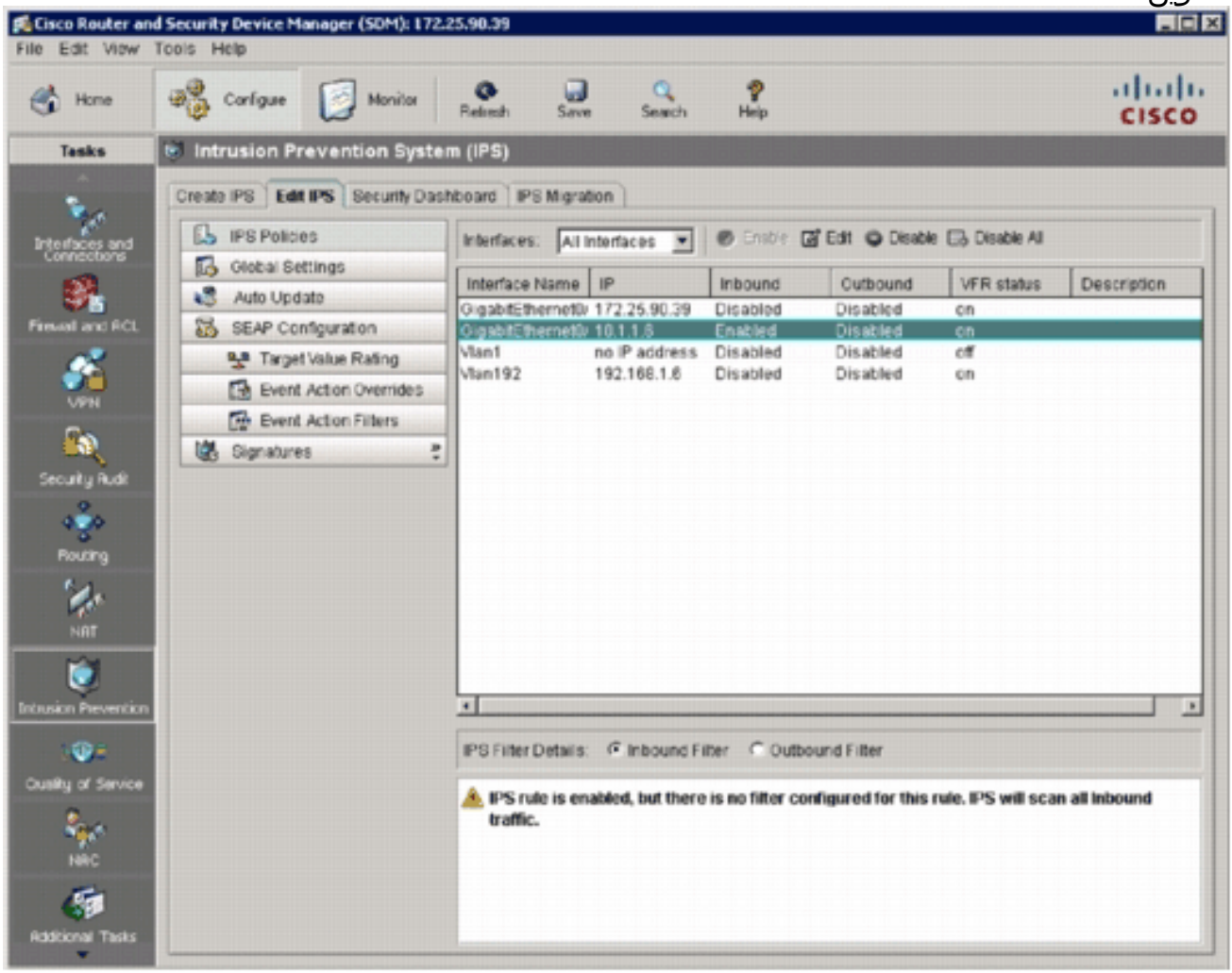
الأوامر.

31. عندما يتم تسليم الأوامر إلى الموجه، انقر فوق **موافق** للمتابعة.يوضح مربع الحوار "حالة تكوين IOS IPS" أنه

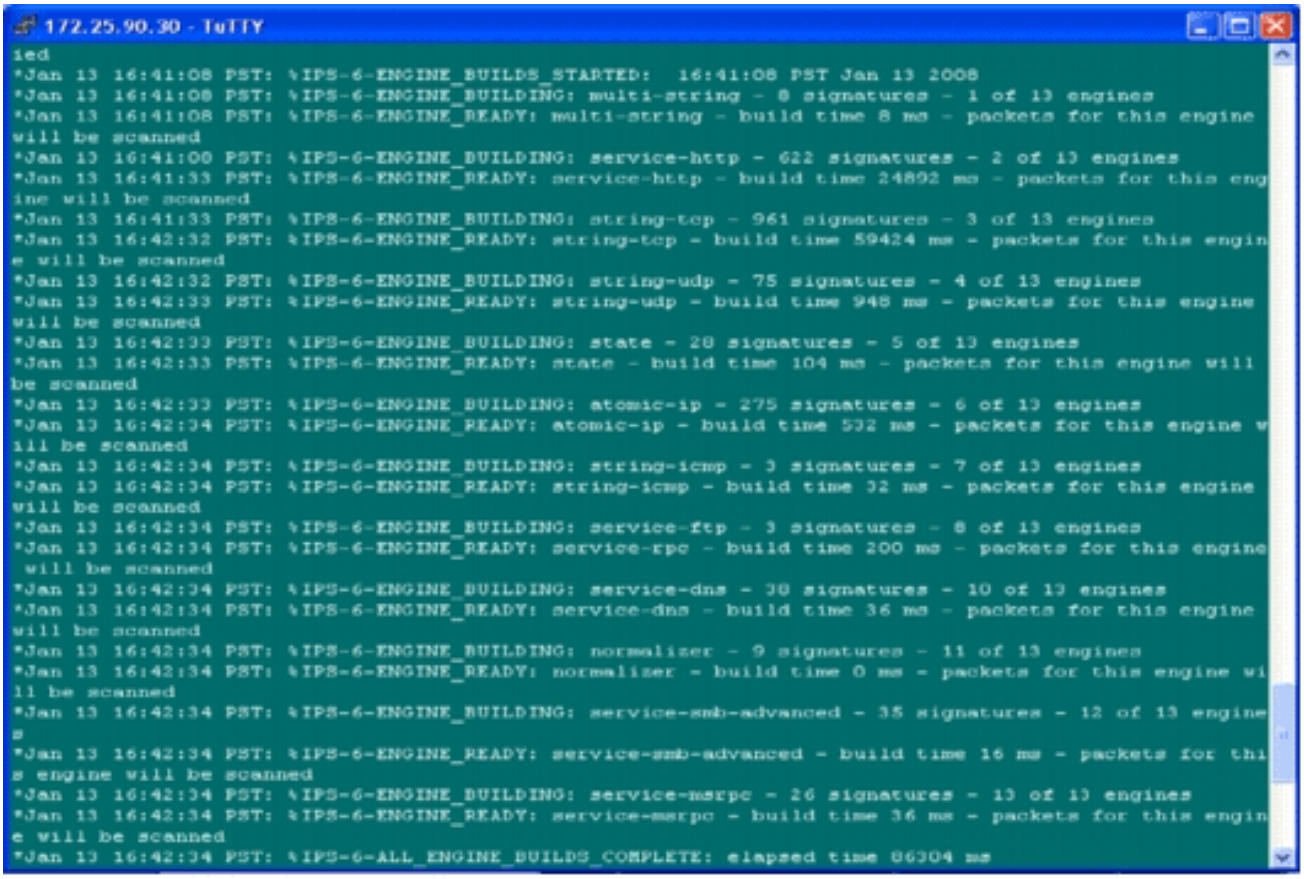


يتم تحميل التواقيع على الموجه.

32. عند تحميل التوقيعات، يعرض إدارة قاعدة بيانات المحول (SDM) علامة التبويب **تحرير IPS** باستخدام التكوين الحالي. تحقق من الواجهة وفي أي إتجاه يتم تمكين IOS IPS للتحقق من التكوين.



توضح وحدة تحكم الموجه أنه تم تحميل التواقيع.

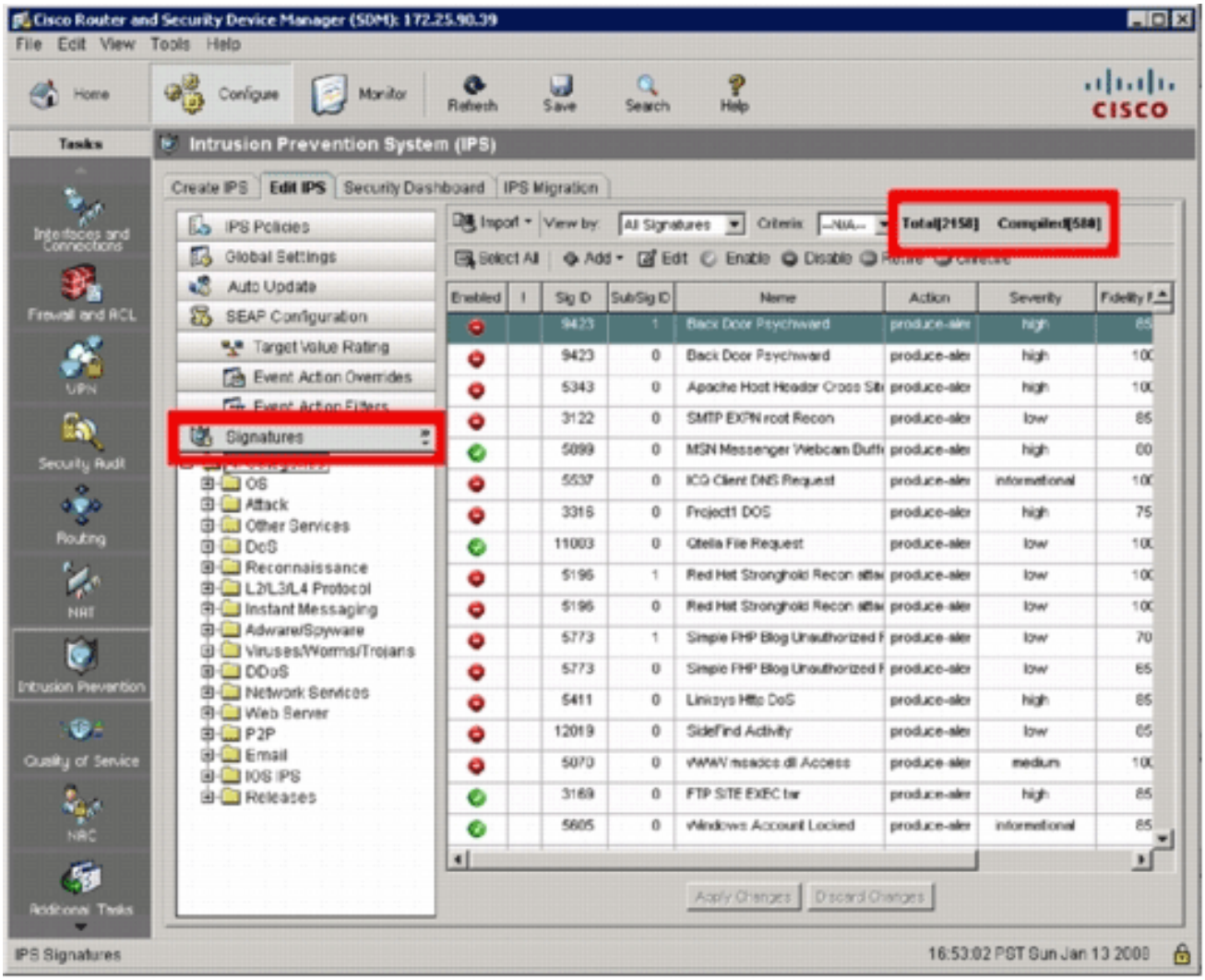


33. أستخدم الأمر **show ip ips signatures count** للتحقق من تحميل التوقيعات بشكل صحيح.

```
router#show ip ips signatures count
Cisco SDF release version S313.0
Trend SDF release version V0.0
                |
              snip
                |
Total Signatures: 2158
 Total Enabled Signatures: 829
Total Retired Signatures: 1572
Total Compiled Signatures: 580
Total Signatures with invalid parameters: 6
    Total Obsoleted Signatures: 11
```

تم إكمال الإعداد الأولي ل IOS IPS باستخدام إدارة قاعدة بيانات المحول (SDM) الإصدار 2.5.

34. تحقق من أرقام التوقيع باستخدام إدارة قاعدة بيانات المحول (SDM) كما هو موضح في هذه الصورة.



معلومات ذات صلة

- برنامج IOS IPS من Cisco على Cisco.com
- حزمة توقيع Cisco IOS IPS
- ملفات توقيع Cisco IOS IPS لـ SDM
- يحصل يبدأ مع cisco ios IPS مع تنسيق توقيع x.5
- دليل تكوين Cisco IOS IPS
- عارض حدث Cisco IDS
- 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).