تكوين الموجه و SDM و Cisco IOS CLI في Cisco IOS IPS

المحتويات

المقدمة

في برنامج Cisco Router and Security Device Manager (SDM) 2.2، يتم دمج تكوين Cisco IOS® IPS داخل تطبيق إدارة قاعدة بيانات المحول (SDM). لم يعد مطلوبا منك تشغيل نافذة منفصلة لتكوين Cisco IOS IPS.

في Cisco SDM 2.2، يرشدك معالج تكوين IPS جديد من خلال الخطوات الضرورية تمكين Cisco IOS IPS على الموجه. وبالإضافة إلى ذلك، لا يزال يمكنك إستخدام خيارات التكوين المتقدمة لتمكين نظام منع التسلل (IPS) من Cisco IOS وتعطيله وملاحقته باستخدام برنامج SDM 2.2 من Cisco.

توصي Cisco بتشغيل Cisco IOS IPS باستخدام ملفات تعريف التوقيع المحكم مسبقا (SDFs): attack-drop.sdf، 128 ميجابايت.sdf، و 256 ميجابايت.sdf. يتم إنشاء هذه الملفات للموجهات التي تحتوي على كميات مختلفة من الذاكرة. يتم تجميع الملفات باستخدام إدارة قاعدة بيانات المحول (SDM) من Cisco، والتي توصي باستخدام وحدات التحكم في الوصول عن بعد (SDFs) عند تمكين Cisco IOS IPS أولا على موجه. يمكن تنزيل هذه الملفات أيضا من http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (للعملاء المسجلين فقط).

يتم تقديم تفاصيل عملية تمكين وحدات SDFs الافتراضية في تمكين Cisco IOS IPS باستخدام SDF إعدادات المصنع الافتراضية. عندما لا تكون وحدات SDF الافتراضية كافية أو تريد إضافة توقيعات جديدة، يمكنك إستخدام الإجراء الموضح في إلحاق توقيعات إضافية بعد تمكين SDF الافتراضية.

المتطلبات الأساسية

المتطلبات

يلزم توفر الإصدار 1.4.2 أو إصدار أحدث من بيئة وقت تشغيل Java لاستخدام الإصدار Cisco SDM 2.2. يتم تجميع ملف توقيع موصى به من Cisco ومضبط (استنادا إلى DRAM) باستخدام إدارة قاعدة بيانات المحول (SDM) من Cisco (يتم تحميله على ذاكرة Flash للموجه مع إدارة قاعدة بيانات المحول (SDM) من Cisco).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى موجه Cisco ومدير أجهزة الأمان (SDM) 2.2.

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

تمكين Cisco IOS IPS باستخدام SDF لإعدادات المصنع الافتراضية

إجراء واجهة سطر الأوامر

أكمل هذا الإجراء لاستخدام واجهة سطر الأوامر (CLI) لتكوين موجه من السلسلة Cisco 1800 Series باستخدام Cisco IOS IPS لتحميل محرك أقراص ثابتة بسرعة 128 ميجابت على ذاكرة الفلاش الخاصة بالموجه.

1. قم بتكوين الموجه لتمكين إعلام حدث Security Device Event Exchange (SDEE).
```
yourname#conf t
```

2. قم بإدخال أوامر التكوين (واحد لكل سطر)، ثم اضغط Cntl+Z للنهاية.
```
yourname(config)#ip ips notify sdee
```

3. قم بإنشاء اسم قاعدة IPS يتم إستخدامه للاقتران بالواجهات.
```
yourname(config)#ip ips name myips
```

4. قم بتكوين أمر موقع IPS لتحديد الملف الذي سيقوم نظام Cisco IOS IPS بقراءة التوقيعات منه.يستخدم هذا المثال الملف على flash: 128 ميجابت.sdf. يمكن أن يكون جزء عنوان URL للموقع من هذا الأمر أي عنوان URL صالح يستخدم الذاكرة المؤقتة (flash) أو القرص أو البروتوكولات عبر FTP و HTTP و HTTPS و RTP و SCP و TFTP للإشارة إلى الملفات.
```
yourname(config)#ip ips sdf location flash:128MB.sdf
```

ملاحظة: يجب تمكين الأمر **terminal monitor** إذا قمت بتكوين الموجه عبر جلسة عمل على برنامج Telnet أو لن ترى رسائل SDEE عند بناء محرك التوقيع.

5. قم بتمكين IPS على الواجهة حيث تريد تمكين Cisco IOS IPS من مسح حركة المرور. في هذه الحالة، تم تمكينا على كلا الاتجاهين على الواجهة fastEthernet 0.
```
yourname(config)#interface fastEthernet 0
yourname(config-if)#ip ips myips in
:Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS*
SDF loaded successfully from opacl
:Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS*
SDF loaded successfully from flash:128MB.sdf
:Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING*
OTHER - 4 signatures - 1 of 15 engines
:Oct 26 00:32:30.921: %IPS-6-ENGINE_READY*
OTHER - 0 ms - packets for this engines will be scanned
:Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING*
MULTI-STRING - 0 signatures - 2 of 15 engines
```

```
                                :Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED*
MULTI-STRING - there are no new signature definitions for this engine
                                      :Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING*
                               STRING.ICMP - 1 signatures - 3 of 15 engines
                                        :Oct 26 00:32:30.941: %IPS-6-ENGINE_READY*
          STRING.ICMP - 20 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING*
                                STRING.UDP - 17 signatures - 4 of15 engines
                                        :Oct 26 00:32:31.393: %IPS-6-ENGINE_READY*
          STRING.UDP - 448 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING*
                               STRING.TCP - 58 signatures - 5 of 15 engines
                                        :Oct 26 00:32:33.641: %IPS-6-ENGINE_READY*
        STRING.TCP - 2248 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING*
                               SERVICE.FTP - 3 signatures - 6 of 15 engines
                                        :Oct 26 00:32:33.657: %IPS-6-ENGINE_READY*
          SERVICE.FTP - 16 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING*
                             SERVICE.SMTP - 2 signatures - 7 of 15 engines
                                        :Oct 26 00:32:33.685: %IPS-6-ENGINE_READY*
        SERVICE.SMTP - 28 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING*
                               SERVICE.RPC - 29 signatures - 8 f 15 engines
                                        :Oct 26 00:32:33.781: %IPS-6-ENGINE_READY*
          SERVICE.RPC - 92 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING*
                             SERVICE.DNS - 31 signatures - 9 of 15 engines
                                        :Oct 26 00:32:33.801: %IPS-6-ENGINE_READY*
          SERVICE.DNS - 20 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING*
                          SERVICE.HTTP - 132 signatures - 10 of 15 engines
                                        :Oct 26 00:32:44.505: %IPS-6-ENGINE_READY*
     SERVICE.HTTP - 10704 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING*
                            ATOMIC.TCP - 11 signatures - 11 of 15 engines
                                        :Oct 26 00:32:44.513: %IPS-6-ENGINE_READY*
           ATOMIC.TCP - 4 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING*
                             ATOMIC.UDP - 9 signatures - 12 of 15 engines
                                        :Oct 26 00:32:44.517: %IPS-6-ENGINE_READY*
           ATOMIC.UDP - 4 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING*
                            ATOMIC.ICMP - 0 signatures - 13 of 15 engines
                               :Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED*
 ATOMIC.ICMP - there are no new signature definitions for this engine
                                      :Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING*
                         ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines
                                        :Oct 26 00:32:44.517: %IPS-6-ENGINE_READY*
     ATOMIC.IPOPTIONS - 0 ms - packets for this engine will be scanned
                                      :Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING*
                           ATOMIC.L3.IP - 5 signatures - 15 of 15 engines
                                        :Oct 26 00:32:44.517: %IPS-6-ENGINE_READY*
           ATOMIC.L3.IP - 0 ms - packets for this engine will be scanned
                                            yourname(config-if)#ip ips myips out
                                          yourname(config-if)#ip virtual-reassembly
```

في أول مرة يتم فيها تطبيق قاعدة IPS على واجهة، يبدأ Cisco IOS IPS التوقيعات التي تم إنشاؤها من الملف المحدد بواسطة أمر مواقع SDF. يتم تسجيل رسائل SDEE إلى وحدة التحكم وإرسالها إلى خادم syslog في حالة تكوينها. تشير رسائل SDEE ذات <*number*> من <*number*>محركات إلى عملية إنشاء محرك التوقيع. وأخيرا، عندما يكون الرقمان متشابهين، يتم بناء جميع المحركات.**ملاحظة:** إعادة تجميع IP الظاهري هي ميزة واجهة (عند تشغيلها) تقوم تلقائيا بإعادة تجميع الحزم المجزأة التي تأتي إلى الموجه من

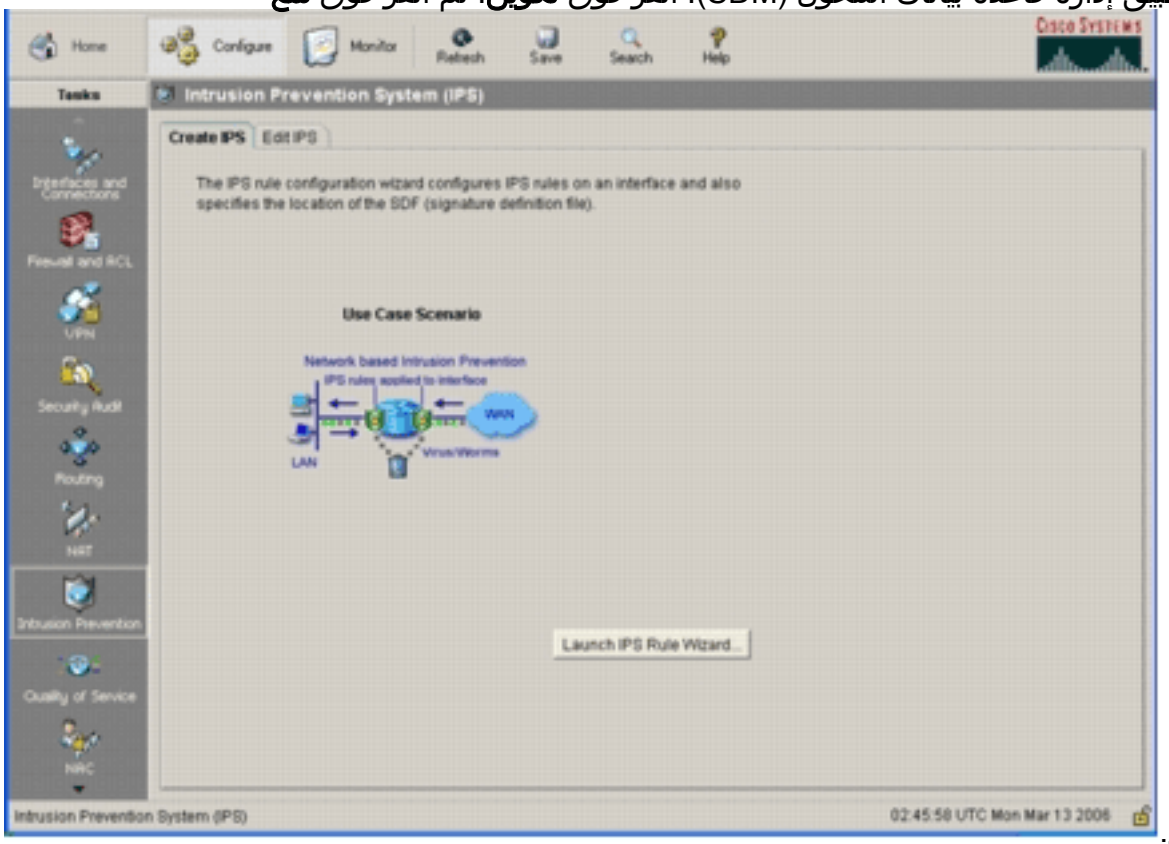
خلال تلك الواجهة. توصي Cisco بتمكين ip virtual-assembly على جميع الواجهات التي تأتي فيها حركة مرور البيانات إلى الموجه. في المثال أعلاه، بجانب تشغيل "ip virtual-assembly" على الواجهة fastEthernet 0، نقوم بتكوينه على شبكة VLAN رقم 1 الداخلية للواجهة أيضا.

```
yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly
```

إجراء SDM 2.2

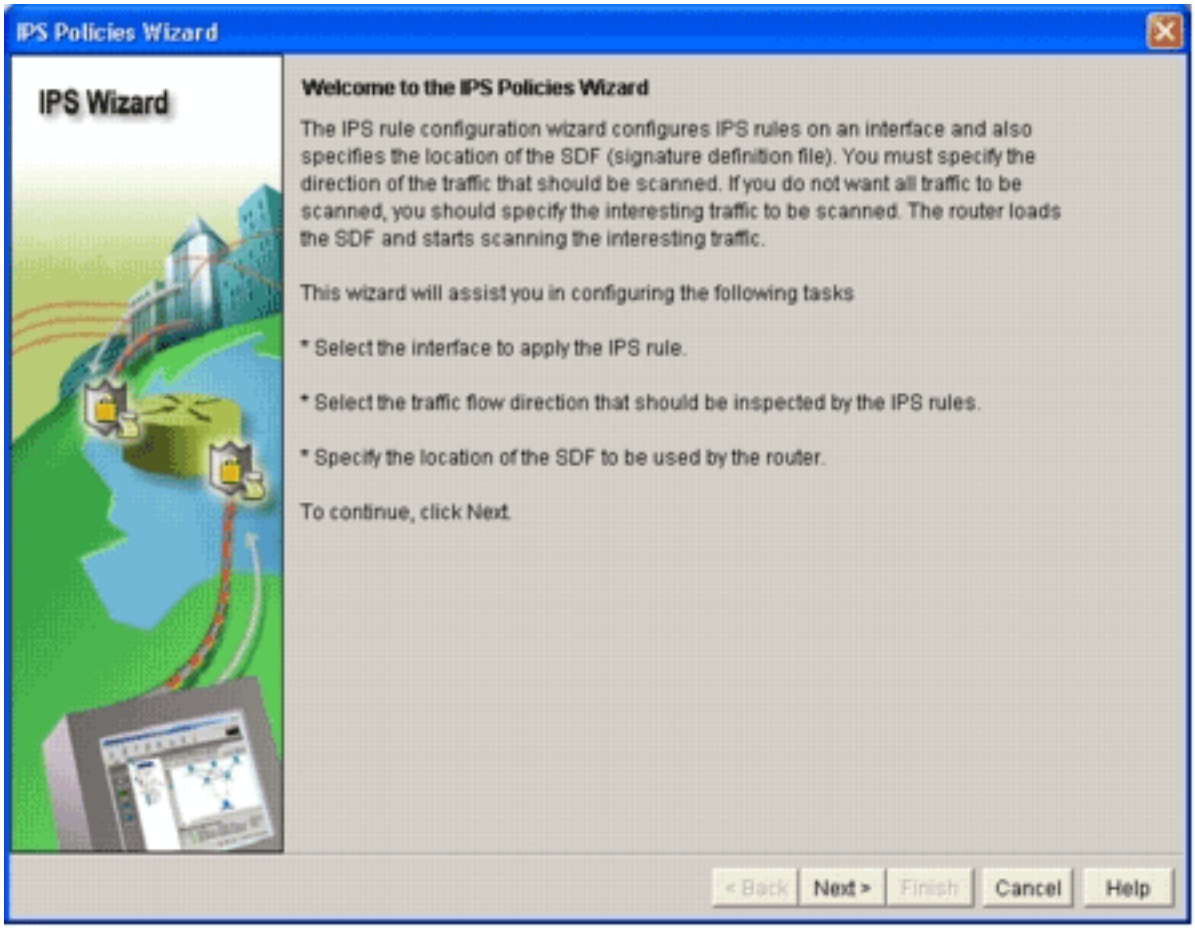
أكمل هذا الإجراء لاستخدام إدارة قاعدة بيانات المحول (SDM) من Cisco 2.2 لتكوين موجه من السلسلة Cisco 1800 Series باستخدام برنامج Cisco IOS IPS.

1. في تطبيق إدارة قاعدة بيانات المحول (SDM)، انقر فوق **تكوين**، ثم انقر فوق **منع التسلل**.



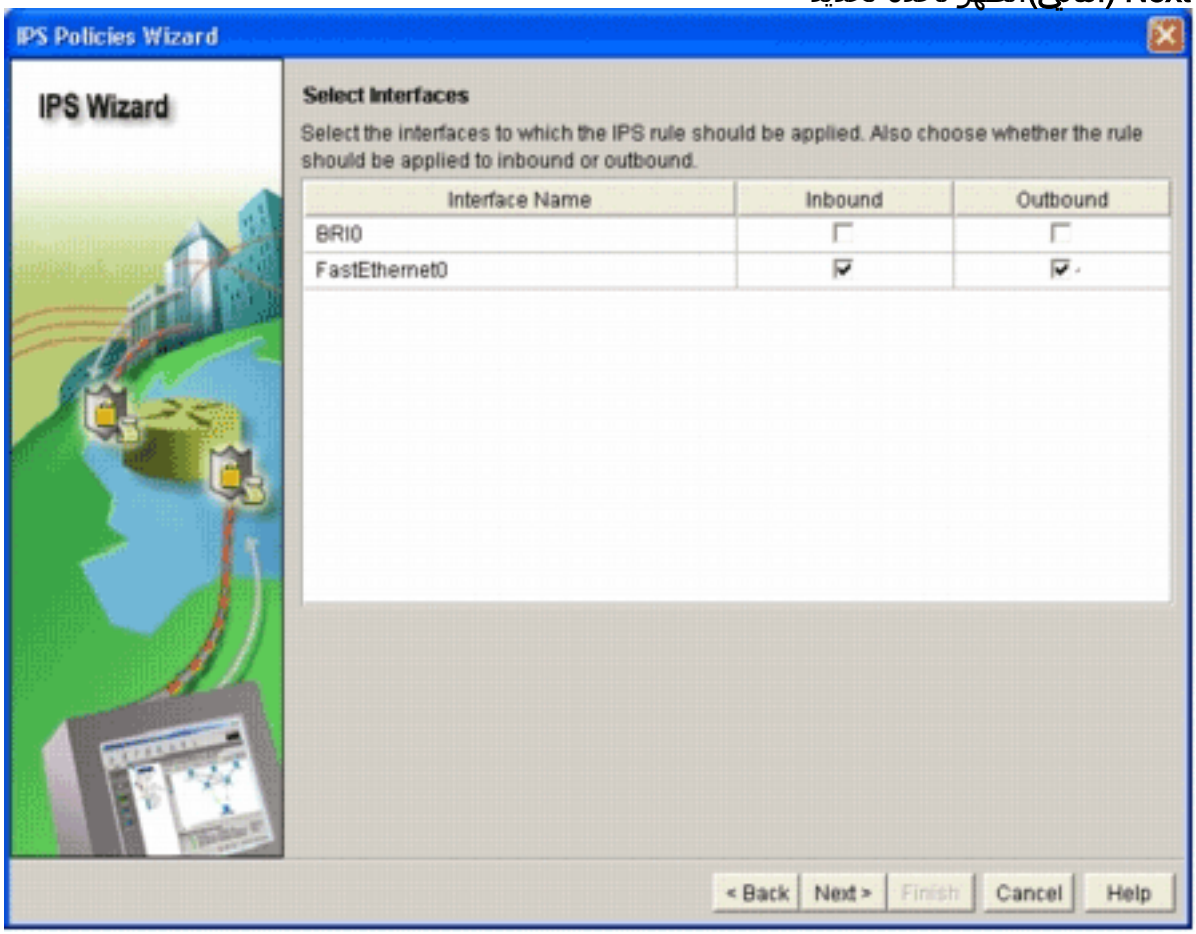
2. انقر فوق علامة التبويب **إنشاء IPS**، ثم انقر فوق **معالج قواعد تشغيل IPS**.تتطلب إدارة قاعدة بيانات المحول (SDM) من Cisco إعلام حدث IPS عبر SDEE لتكوين ميزة Cisco IOS IPS. بشكل افتراضي، لا يتم تمكين إعلام SDEE. يطلب منك إدارة قاعدة بيانات المحول (SDM) من Cisco تمكين إعلام حدث IPS عبر SDEE كما هو موضح في هذه الصورة:

3. وانقر فوق **OK**.تظهر نافذة "معالج الترحيب بنهج IPS" من مربع الحوار "معالج نهج



"IPS".

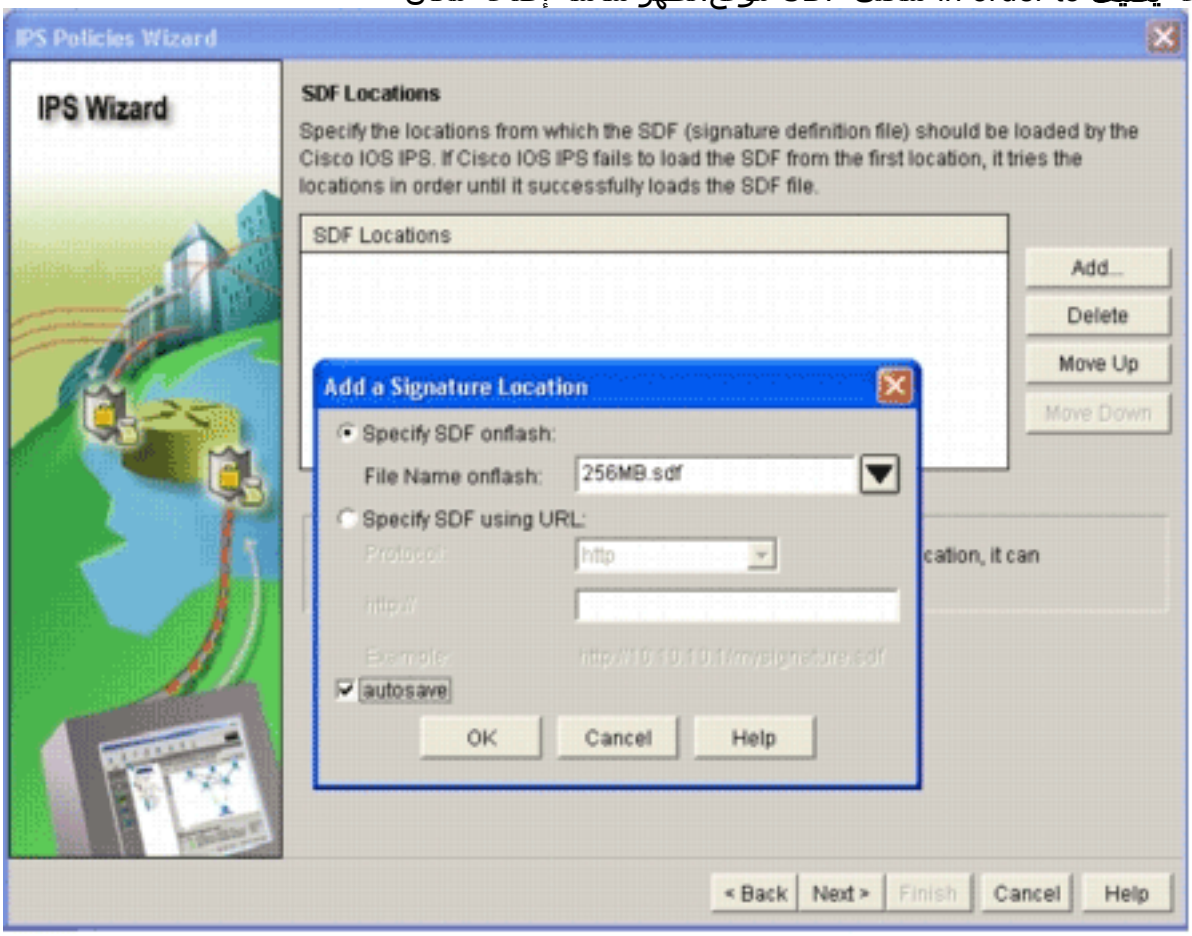
4. انقر فوق **Next (التالي)**.تظهر نافذة تحديد



الواجهات.

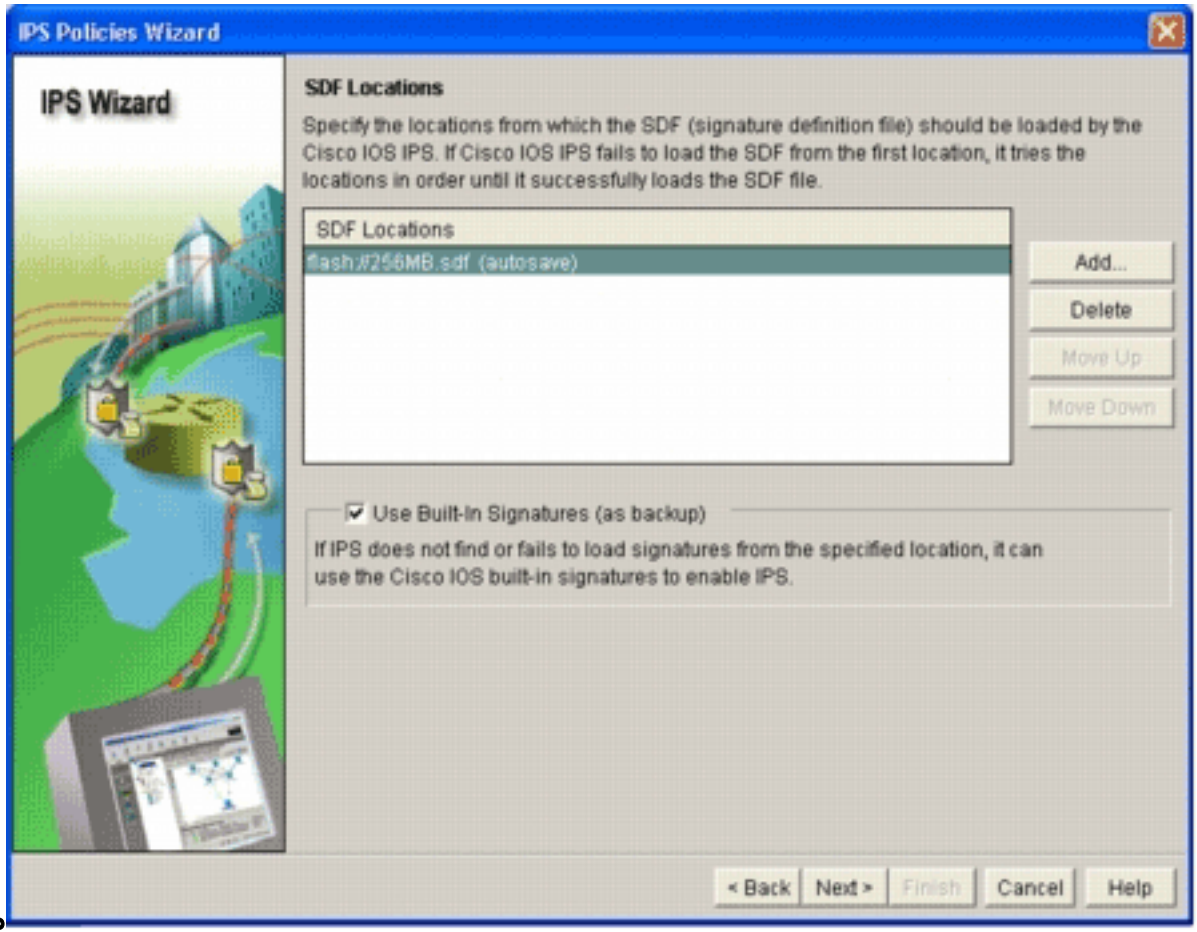
5. أخترت القارن ل أي أنت تريد أن يمكن IPS، وطقطقت إما **الوارد** أو **الصادر** تدقيق صندوق in order to أشارت إلى إتجاه أن قارن.**ملاحظة:** توصي Cisco بتمكين كل من الاتجاهات الواردة والصادرة عند تمكين IPS على واجهة.

6. انقر فوق **Next (التالي)**.يظهر إطار مواقع SDF.
7. طقطقة **يضيف** in order to شكلت SDF موقع.تظهر شاشة إضافة مكان



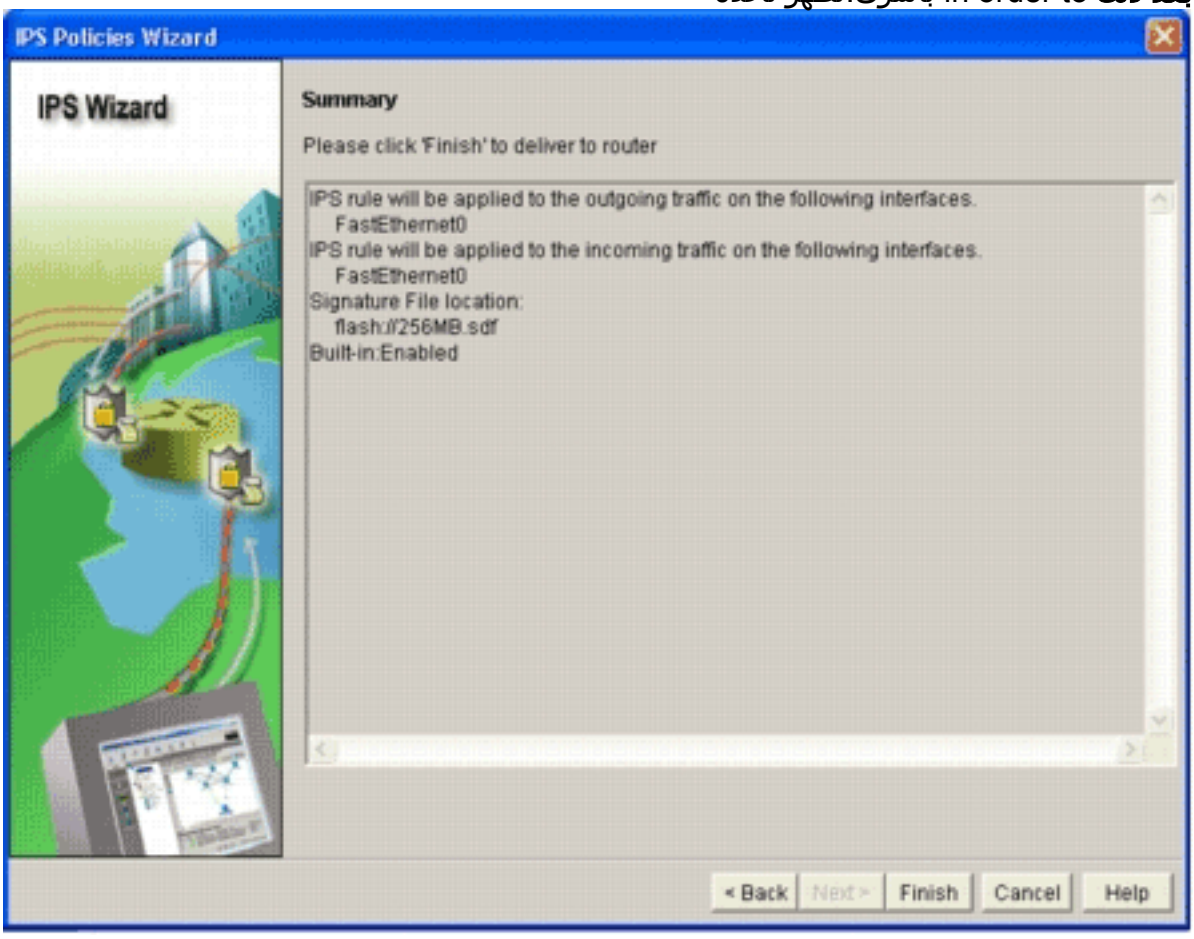
توقيع.

8. انقر فوق الزر **تحديد SDF على** جهاز راديو **Flash**، واختر 256 ميجابايت.SDF من **اسم الملف في** القائمة المنسدلة **لذاكرة الفلاش**.
9. انقر فوق خانة الاختيار **الحفظ التلقائي**، وانقر فوق **موافق**.**ملاحظة:** يحفظ خيار الحفظ التلقائي ملف التوقيع تلقائيا عندما يكون هناك تغيير في التوقيع.يعرض إطار "مواقع SDF" موقع SDF



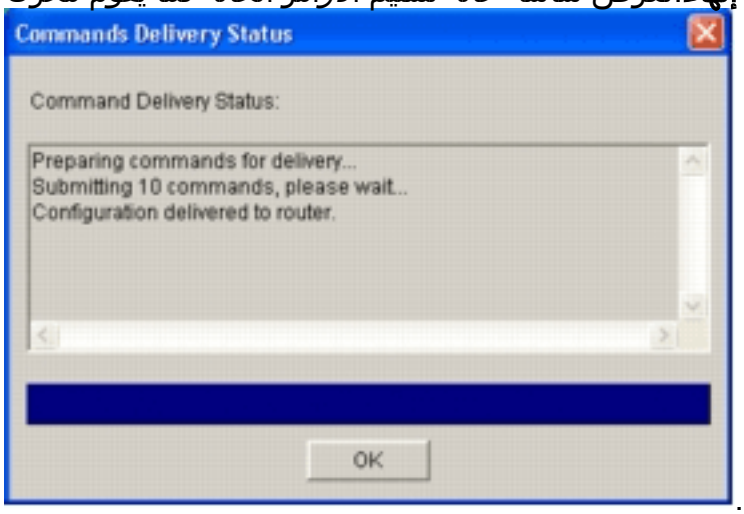
ملاحظة: يمكنك إضافة مواقع توقيع إضافية من أجل تعيين نسخة إحتياطية.

10. انقر خانة الاختيار **إستخدام التوقيعات المدمجة (كنسخ إحتياطي).ملاحظة:** توصي Cisco بعدم إستخدام خيار التوقيع المضمن إلا إذا قمت بتحديد موقع واحد أو أكثر.
11. طقطقت **بعد ذلك** in order to باشرت.تظهر نافذة

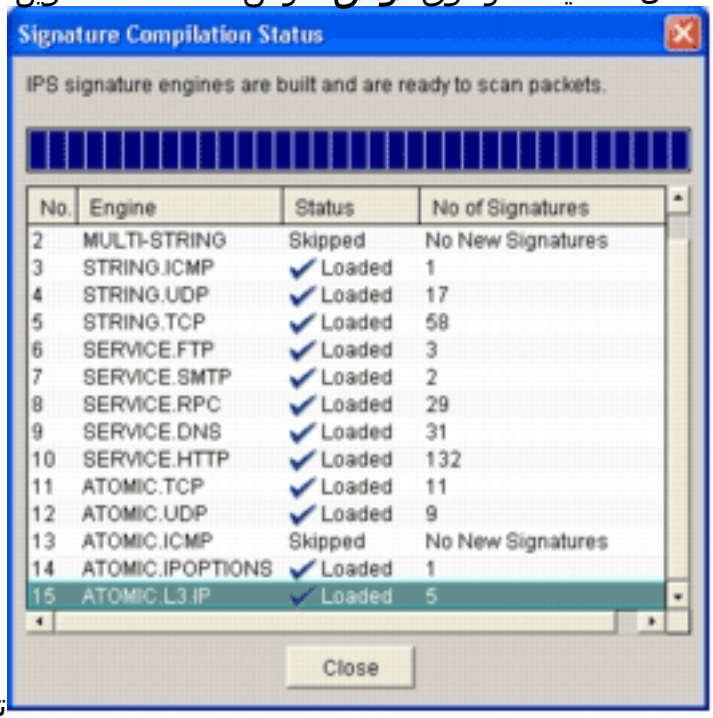


الملخص.

12. انقر فوق **إنهاء**.تعرض شاشة حالة تسليم الأوامر الحالة كما يقوم محرك IPS بتجميع كل التوقيعات.

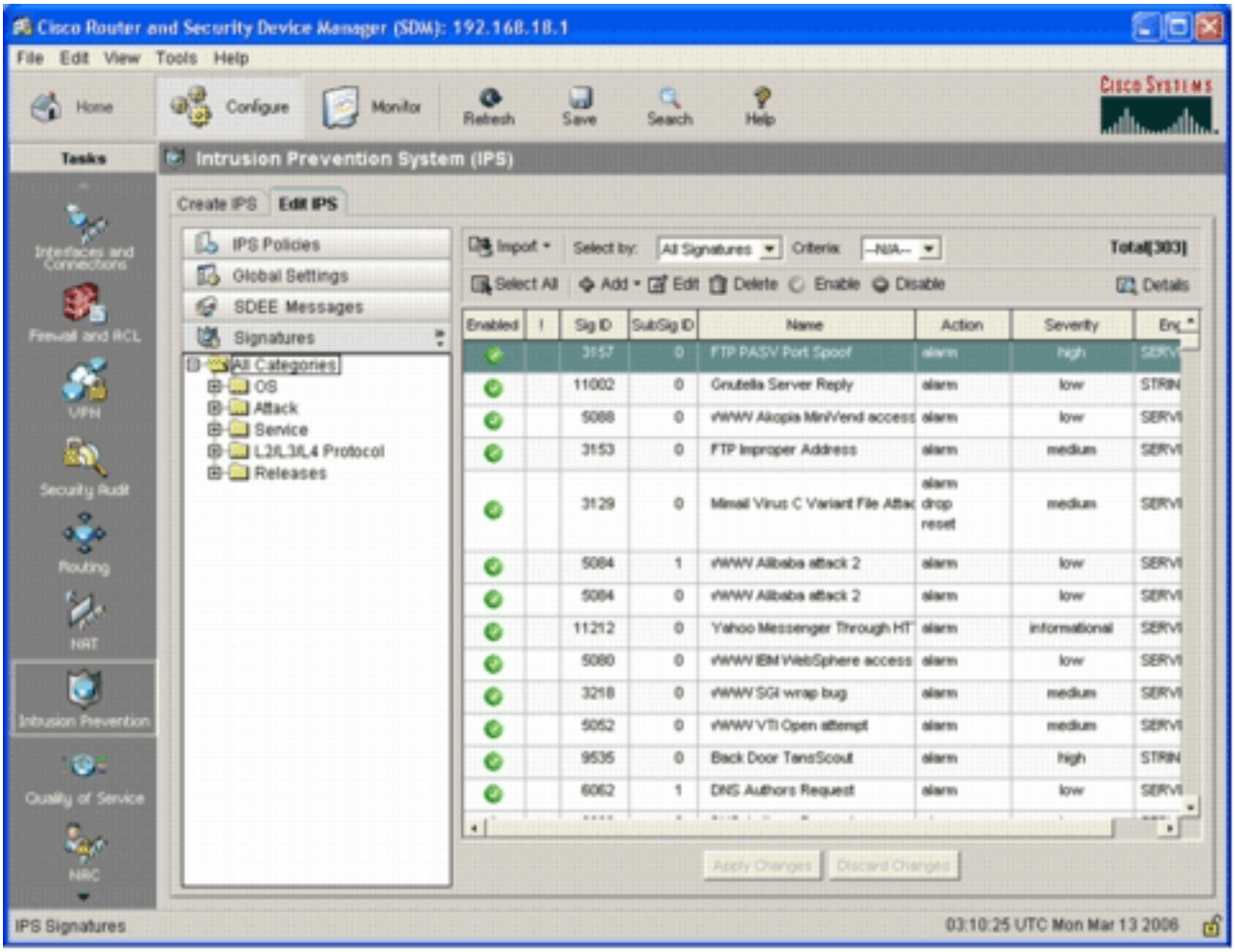


13. بمجرد اكتمال العملية، انقر فوق **موافق**.تعرض شاشة حالة تحويل التوقيع معلومات تجميع التوقيع.



توضح هذه المعلومات المحركات التي تم تحويلها برمجيا وعدد التوقيعات في هذا المحرك. بالنسبة للمحركات التي تعرض *التخطي* في عمود الحالة، لا يوجد توقيع محمل لذلك المحرك.

14. انقر فوق **إغلاق**" لإغلاق مربع الحوار "حالة تحويل التوقيع".
15. للتحقق من التوقيعات التي يتم تحميلها حاليا على الموجه، انقر فوق **تكوين**، ثم انقر فوق **منع التسلل**.
16. انقر صفحة **تحرير IPS**، ثم انقر **التوقيعات**.تظهر قائمة توقيع IPS في نافذة التوقيعات.



إلحاق تواقيع إضافية بعد تمكين SDF الافتراضية

إجراء واجهة سطر الأوامر

لا يوجد أمر CLI متاح لإنشاء توقيعات أو قراءة معلومات توقيع من ملف IOS-SXXX.zip الموزع. توصي Cisco باستخدام إما SDM أو مركز الإدارة لأجهزة إستشعار IPS لإدارة التوقيعات على أنظمة Cisco IOS IPS.

بالنسبة للعملاء الذين لديهم ملف توقيع جاهز بالفعل ويريدون دمج هذا الملف مع SDF الذي يتم تشغيله على نظام Cisco IOS IPS، يمكنك إستخدام هذا الأمر:

```
yourname#show running-config | include ip ips sdf
ip ips sdf location flash:128MB.sdf
#yourname
```

ملف التوقيع المعرف بواسطة أمر موقع التوقيع هو حيث يقوم الموجه بتحميل ملفات التوقيعات عند إعادة تحميله أو عند إعادة تكوين الموجه IOS IPS. لكي تكون عملية الدمج ناجحة، يجب أيضا تحديث الملف المعرف بأمر موقع ملف التوقيع.

1. أستخدم الأمر **show** للتحقق من مواقع التوقيع التي تم تكوينها حاليا.يعرض الإخراج مواقع التوقيع التي تم تكوينها. يظهر هذا الأمر من حيث يتم تحميل التوقيعات الجاري تشغيلها حاليا.

```
yourname#show ip ips signatures
Builtin signatures are configured
```

تم تحميل التواقيع آخر مرة من الذاكرة المؤقتة (flash:128 ميغابايت من أداة SDFإصدار S128.0 من Cisco SDFإصدار V0.0 من Trend

2. أستخدم الأمر **copy <*url*>**ips-sdf، بالإضافة إلى المعلومات الواردة من الخطوة السابقة، لدمج ملفات التوقيع.

```
yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf
```

```
                              ! :(Loading mysignatures.xml from 10.10.10.5 (via Vlan1
                                                                        [OK - 1612 bytes]
     Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl*
      No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport
                                                                                  4715
          Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from*
                                             tftp://10.10.10.5/mysignatures.xml
   Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines*
  Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature*
                                                    definitions for this engine
          - Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures*
                                                                  of 15 engines 2
          Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are*
                                       no new signature definitions for this engine
           - Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures*
                                                                  of 15 engines 3
           Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are*
                                       no new signature definitions for this engine
           - Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures*
                                                                  of 15 engines 4
            Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are*
                                       no new signature definitions for this engine
           - Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures*
                                                                  of 15 engines 5
- Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False*
                                                 This parameter is not supported
      Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this*
                                                          engine will be scanned
           - Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures*
                                                                  of 15 engines 6
           Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are*
                                       no new signature definitions for this engine
          - Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures*
                                                                  of 15 engines 7
          Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are*
                                       no new signature definitions for this engine
          - Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures*
                                                                  of 15 engines 8
           Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are*
                                       no new signature definitions for this engine
          - Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures*
                                                                  of 15 engines 9
           Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are*
                                       no new signature definitions for this engine
        - Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures*
                                                                  of 15 engines 10
          Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are*
                                       no new signature definitions for this engine
           - Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures*
                                                                  of 15 engines 11
            Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are*
                                       no new signature definitions for this engine
            - Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures*
                                                                  of 15 engines 12
            Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are*
                                       no new signature definitions for this engine
           - Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures*
                                                                  of 15 engines 13
           Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are*
                                       no new signature definitions for this engine
        - Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures*
                                                                  of 15 engines 14
         Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are*
                                       no new signature definitions for this engine
```

```
- Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures*
                                                    of 15 engines 15
Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are*
                                        no new signature definitions for this engine
                                                                    #yourname
```

بعد إصدار الأمر **copy**، يقوم الموجه بتحميل ملف التوقيع في الذاكرة ثم يبني محركات التوقيع. في إخراج رسالة SDEE لوحدة التحكم، يتم عرض حالة البناء لكل محرك توقيع.٪IPS-6-ENGINE_BUILD_SKIPPED يشير إلى عدم وجود توقيعات جديدة لهذا المحرك.٪IPS-6-ENGINE_READY يشير إلى وجود توقيعات جديدة ومحرك التشغيل جاهز. وكما كان الحال من قبل، تشير رسالة "15 محرك من 15 محرك" إلى أن جميع المحركات قد بنيت.يشير IPS-7-UNSUPPORTED_PARAM إلى أن معلمة معينة غير مدعومة من قبل Cisco IOS IPS. على سبيل المثال، CapturePacket و ResetAfterIdle.**ملاحظة:** هذه الرسائل خاصة بالمعلومات فقط ولن يكون لها تأثير على قدرة توقيع Cisco IOS IPS أو أدائه. يمكن إيقاف تشغيل رسائل التسجيل هذه عن طريق تعيين مستوى التسجيل أعلى من تصحيح الأخطاء (المستوى 7).

3. قم بتحديث SDF المعرفة بواسطة أمر موقع التوقيع، بحيث أنه عند إعادة تحميل الموجه، سيكون لديه مجموعة التوقيع المدمج مع التوقيعات المحدثة. يوضح هذا المثال فرق حجم الملف بعد حفظ التوقيع المدمج في ملف flash الخاص بقطر 128 ميجابت.

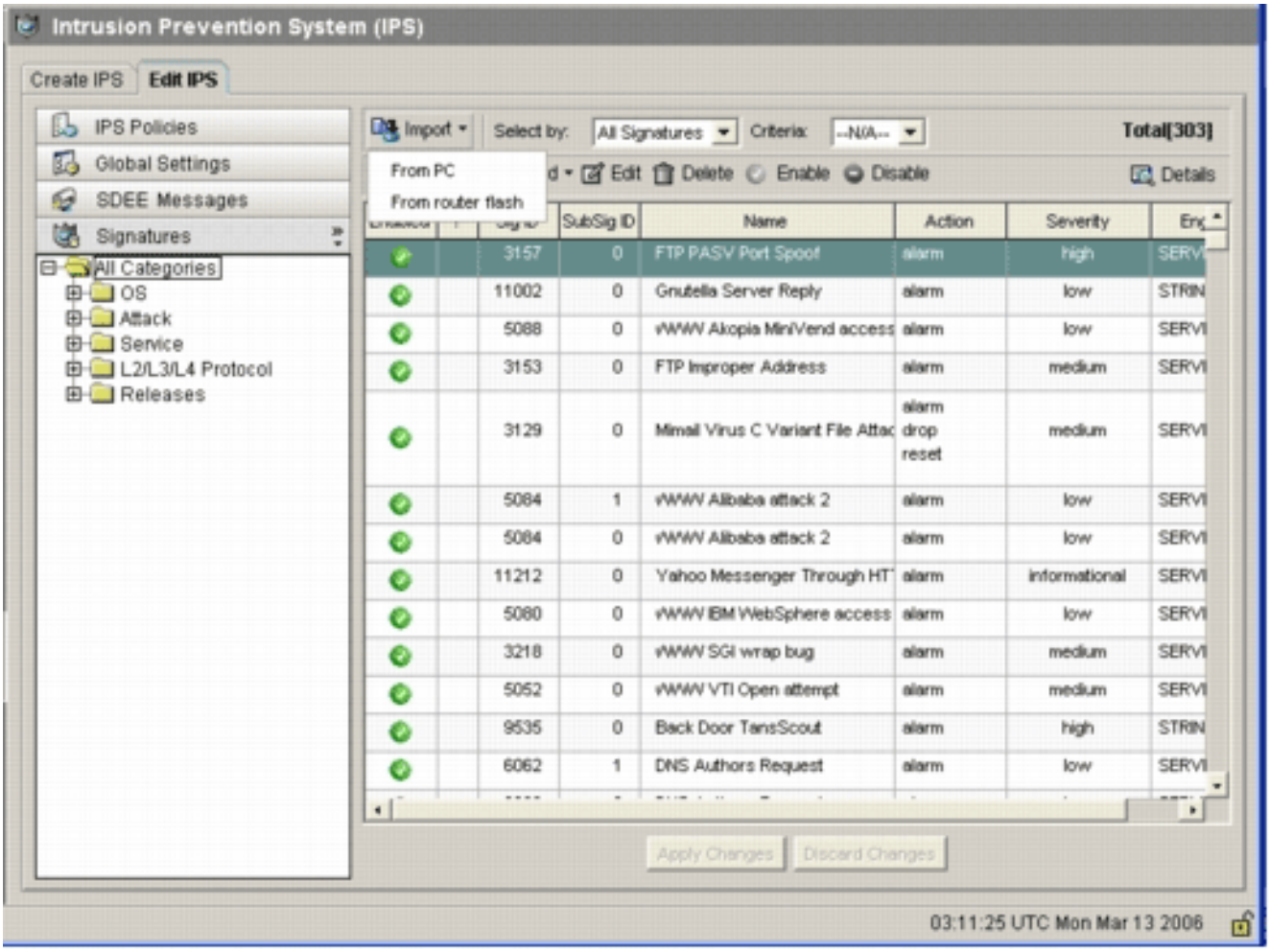
```
:yourname#show flash
length-- -----date/time------ path-- -#-
Aug 30 2005 22:58:34 +00:00 128MB.sdf 504630 4
yourname#copy ips-sdf flash:128MB.sdf
:yourname#show flash
length-- -----date/time------ path-- -#-
Oct 26 2005 02:51:32 +00:00 128MB.sdf 522656 4
```

تحذير: تحتوي الآن وحدة التحكم الجديدة SDF بسرعة 128 ميجابت على توقيعات مدمجة مع العميل. يختلف المحتوى عن ملف Cisco الافتراضي cisco .128MB.SDF يوصي أن يغير أنت هذا مبرد إلى اسم مختلف أن يتحاشى إرتباك. إذا تم تغيير الاسم، يلزم تغيير أمر موقع التوقيع أيضا.

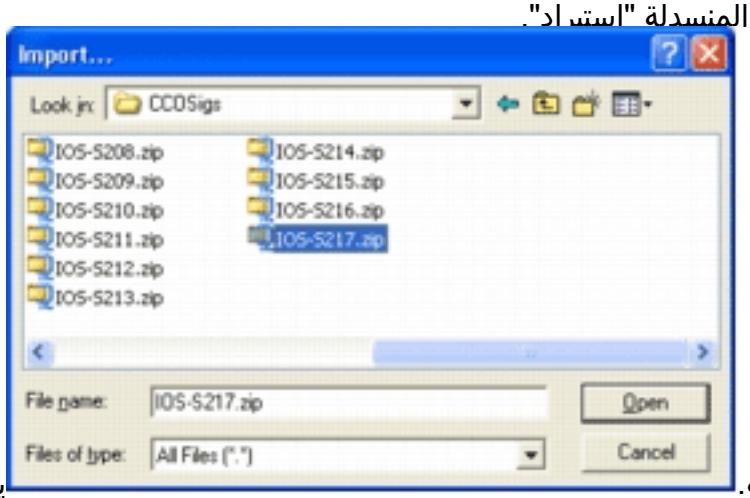
إجراء SDM 2.2

بعد تمكين نظام منع التسلل (Cisco IOS IPS)، يمكن إضافة توقيعات جديدة إلى الموجه الذي يشغل مجموعة توقيع باستخدام وظيفة إستيراد SDM من Cisco. أتمت هذا steps in order to جلبت توقيع جديد:

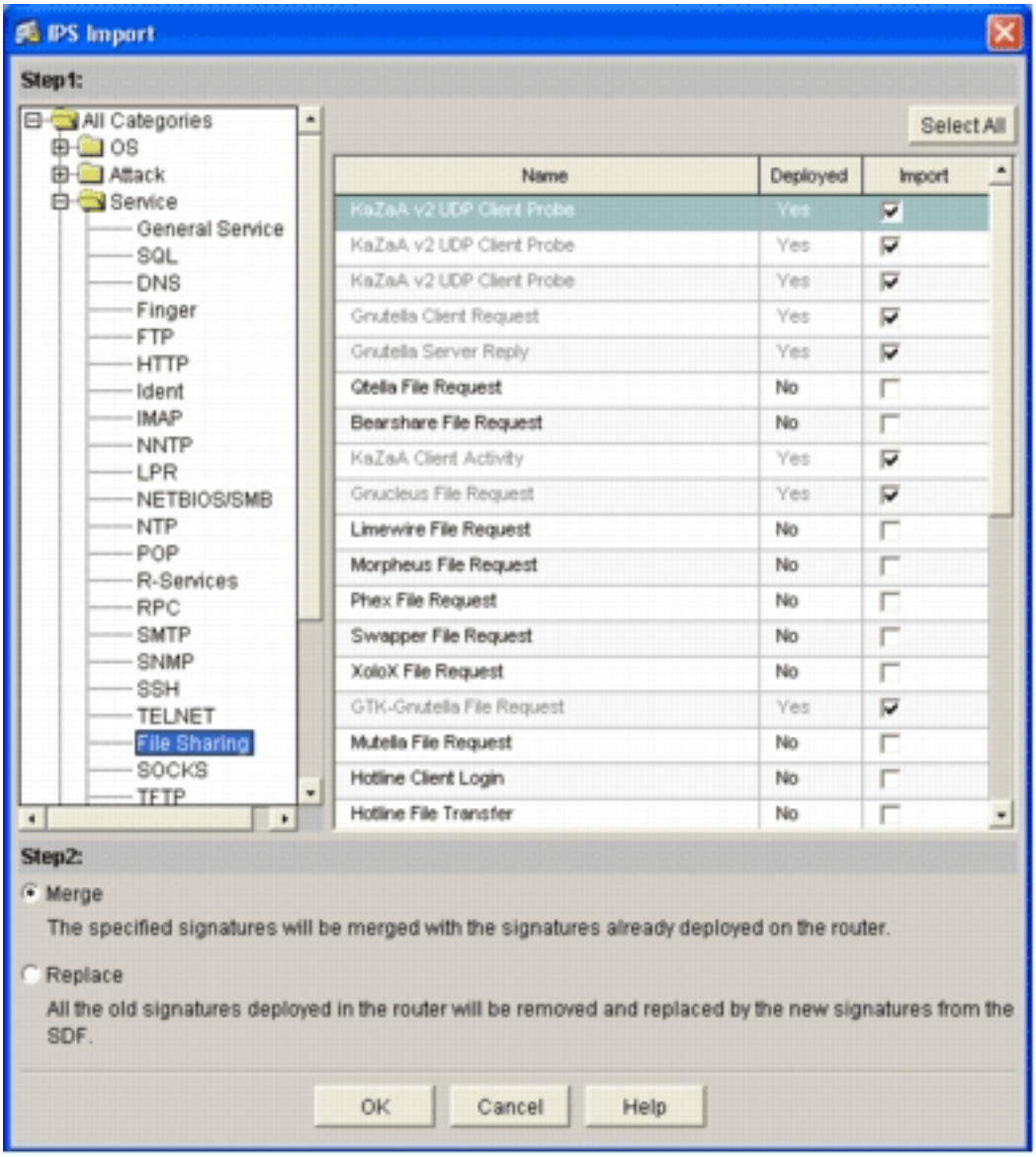
1. أختر SDFs الافتراضية أو ملف تحديث IOS-Sxxx.zip لاستيراد توقيعات إضافية.
2. انقر فوق **تكوين**، ثم انقر فوق **منع التسلل**.
3. انقر فوق علامة التبويب **تحرير IPS**، ثم انقر فوق **إستيراد**.



4. أختر **من الكمبيوتر الشخصي** من القائمة المنسدلة "استيراد".

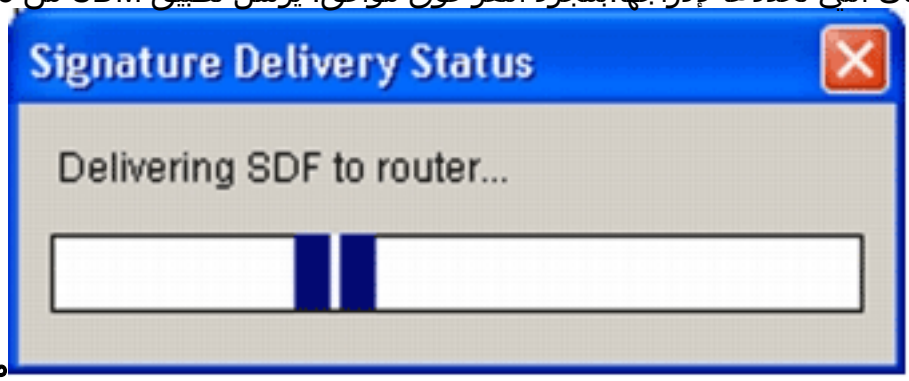


5. حدد الملف الذي تريد إستيراد التواقيع منه. يستخدم هذا المثال آخر تحديث تم تنزيله من Cisco.com وتم حفظه على القرص الثابت لجهاز الكمبيوتر المحلي.
6. انقر فوق **فتح**.**تحذير:** نظرا لتقييد الذاكرة، يمكن إضافة عدد محدود فقط من التوقيعات الجديدة فوق التوقيعات التي تم نشرها بالفعل. إذا تم تحديد عدد كبير للغاية من التوقيعات، فقد لا يتمكن الموجه من تحميل جميع التوقيعات الجديدة بسبب نقص الذاكرة.بمجرد اكتمال تحميل ملف التوقيع، تظهر شاشة إدراج



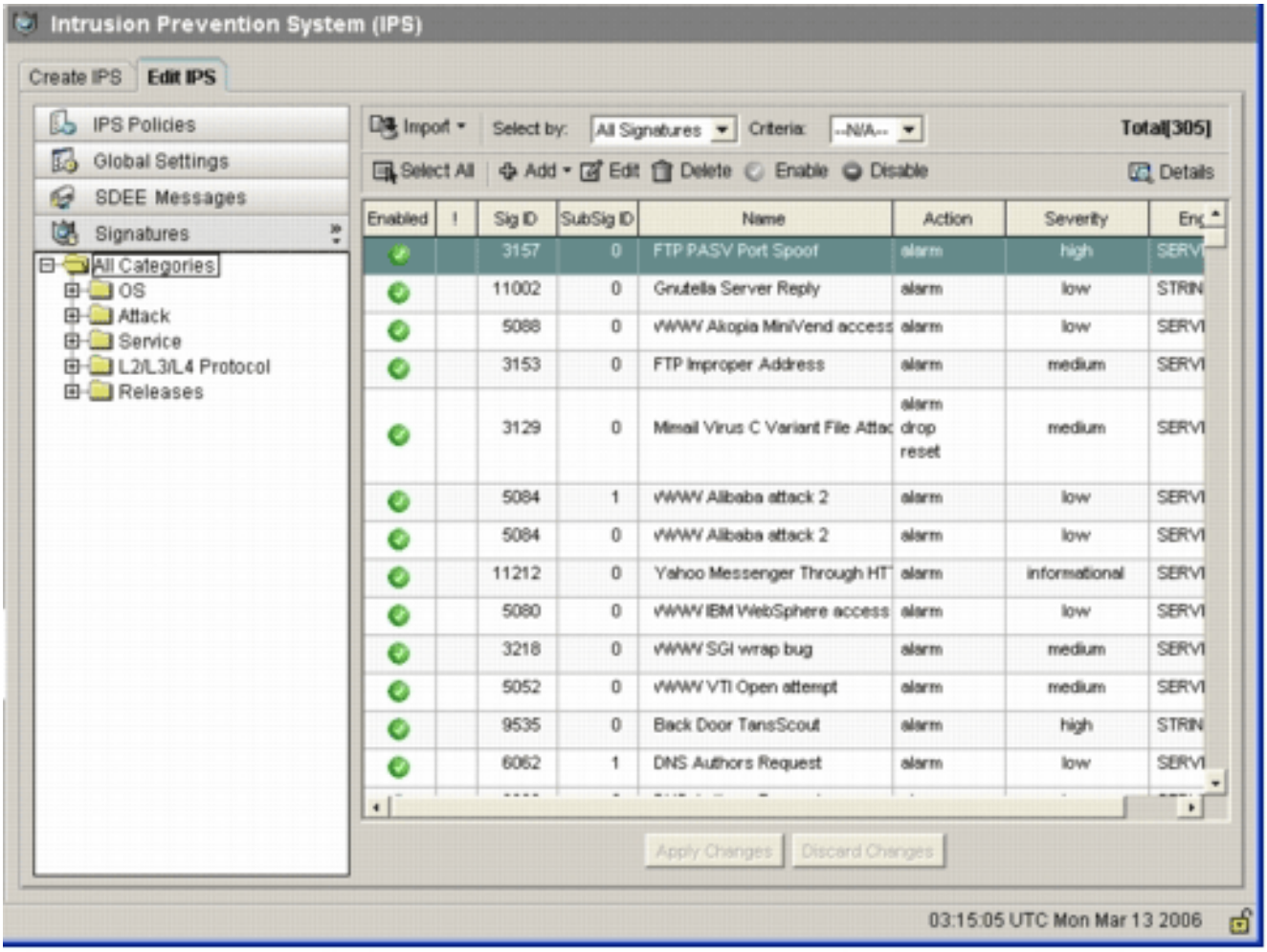
IPS.

7. تصفح خلال عرض الشجرة الأيسر، وانقر خانة الاختيار **إستيراد** بجوار التوقيعات التي تريد إدراجها.
8. انقر زر **دمج** الراديو، ثم انقر **موافق**.**ملاحظة:** يستبدل خيار الاستبدال مجموعة التوقيع الحالية على الموجه بالتوقيعات التي تحددها لإدراجها.بمجرد النقر فوق موافق، يرسل تطبيق SDM من Cisco التوقيعات إلى



الموجه. **ملاحظة:** يحدث إستخدام عال لوحدة المعالجة المركزية أثناء تجميع التوقيعات وتحميلها. بعد تمكين Cisco IOS IPS على الواجهة، يبدأ ملف التوقيع في التحميل. يستغرق الموجه حوالي خمس دقائق لتحميل SDF. يمكنك محاولة إستخدام أمر **show process cpu** لعرض إستخدام وحدة المعالجة المركزية من واجهة سطر الأوامر ببرنامج Cisco IOS Software. ومع ذلك، لا تحاول إستخدام أوامر إضافية أو تحميل وحدات أخرى من وحدات التحكم في الوصول (SDF) أثناء قيام الموجه بتحميل SDF. قد يتسبب ذلك في أن يستغرق إكمال عملية تجميع التوقيع وقتا أطول (نظرا لأن إستخدام وحدة المعالجة المركزية يقترب من نسبة إستخدام 100 في المائة في وقت تحميل SDF). قد تحتاج إلى إستعراض قائمة التوقيعات وتمكين التوقيعات إذا لم تكن في حالة *التمكين*.وقد ارتفع العدد الإجمالي للتوقيع إلى 519 توقيعا. يتضمن هذا الرقم جميع التوقيعات المتاحة في ملف IOS-S193.zip التي تنتمي إلى الفئة الفرعية لمشاركة

الملفات.



للحصول على موضوعات أكثر تقدما حول كيفية إستخدام إدارة قاعدة بيانات المحول (SDM) لإدارة ميزة Cisco IOS IPS، ارجع إلى وثائق إدارة قاعدة بيانات المحول (SDM) من Cisco في عنوان URL هذا:

تحديد التوقيعات والعمل باستخدام فئات التوقيع

لتحديد كيفية تحديد التوقيعات الصحيحة للشبكة بشكل فعال، يجب أن تعرف بعض الأشياء عن الشبكة التي تقوم بحمايتها. تساعد معلومات فئة التوقيع المحدثة في Cisco SDM 2.2 والإصدارات الأحدث العملاء في تحديد مجموعة التوقيعات الصحيحة لحماية الشبكة.

الفئة هي طريقة لتجميع التوقيعات. إنه يساعد على تضييق تحديد التوقيع إلى مجموعة فرعية من التوقيعات المتعلقة ببعضها البعض. يمكن أن ينتمي توقيع واحد إلى فئة واحدة فقط أو يمكن أن ينتمي إلى فئات متعددة.

هذه هي خمس فئات للمستوى الأعلى:

- OS—تصنيف التوقيع المستند إلى نظام التشغيل
- تصنيف التوقيع المستند إلى هجوم
- تصنيف التوقيع المستند إلى الخدمة
- بروتوكول الطبقة 2-4- تصنيف التوقيع المستند إلى البروتوكول
- الإصدارات - تصنيف التوقيع المستند إلى الإصدار

وينقسم كل فئة من هذه الفئات أيضا إلى فئات فرعية.

على سبيل المثال، ضع في اعتبارك شبكة منزلية مع اتصال واسع النطاق بالإنترنت ونفق للشبكة الخاصة الظاهرية (VPN) بشبكة الشركة. يحتوي موجه النطاق الترددي العريض على جدار حماية Cisco IOS الذي تم تمكينه على الاتصال المفتوح (غير VPN) بالإنترنت لمنع إنشاء أي اتصال من الإنترنت وتوصيله بالشبكة المنزلية. يسمح بجميع حركات المرور التي تنشأ من الشبكة المنزلية إلى الإنترنت. افترض أن المستخدم يستخدم جهاز كمبيوتر مستند إلى

Windows ويستخدم تطبيقات مثل HTTP (إستعراض الويب) والبريد الإلكتروني.

يمكن تكوين جدار الحماية بحيث يتم السماح بالتدفق عبر الموجه فقط للتطبيقات التي يحتاج إليها المستخدم. وهذا سيتحكم في تدفق حركة المرور غير المرغوب فيها والتي يحتمل أن تكون سيئة والتي يمكن أن تنتشر عبر الشبكة. ضع في الاعتبار أن المستخدم المنزلي لا يحتاج إلى خدمة معينة أو لا يستخدمها. إذا تم السماح لهذه الخدمة بالتدفق عبر جدار الحماية، فهناك ثقب محتمل يمكن أن يستخدمه الهجوم للتدفق عبر الشبكة. تسمح أفضل الممارسات فقط بالخدمات المطلوبة. الآن، من الأسهل تحديد التواقيع التي سيتم تمكينها. تحتاج إلى تمكين التواقيع فقط للخدمات التي تسمح لها بالتدفق عبر جدار الحماية. في هذا المثال، تتضمن الخدمات البريد الإلكتروني و HTTP. يقوم إدارة قاعدة بيانات المحول (SDM) من Cisco بتبسيط هذا التكوين.

لاستخدام الفئة لتحديد التوقيعات المطلوبة، أختر **الخدمة > HTTP**، وقم بتمكين كل التوقيعات. تعمل عملية التحديد هذه أيضا في شاشة إستيراد التوقيع، حيث يمكنك تحديد كل توقيعات HTTP واستيرادهم إلى الموجه الخاص بك.

الفئات الإضافية التي يجب تحديدها تشمل DNS و NetBIOS/SMB و HTTPS و SMTP.

تحديث توقيعات ملفات SDF الافتراضية

يتم حاليا نشر ثلاث وحدات من وحدات SDF لكل بنية (Attack-drop.dsf، و 128 ميجابايت.sdf، و 256 ميجابايت.sdf) على موقع الويب Cisco.com على موقع الويب http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (للعملاء المسجلين فقط). سيتم نشر الإصدارات الأحدث من هذه الملفات بمجرد توفرها. لتحديث الموجهات التي تعمل بنظام التشغيل Cisco IOS IPS باستخدام وحدات SDF الافتراضية هذه، انتقل إلى موقع الويب وقم بتنزيل أحدث الإصدارات من هذه الملفات.

إجراء واجهة سطر الأوامر

1. انسخ الملفات التي تم تنزيلها إلى الموقع الذي تم تكوين الموجه عليه لتحميل هذه الملفات منه. لمعرفة مكان تكوين الموجه حاليا، أستخدم **show running-config | في** أمر **قوات الحماية من خلال ip ips**.

```
Router#show running-config | in ip ips sdf
ip ips sdf location flash://256MB.sdf autosave
```

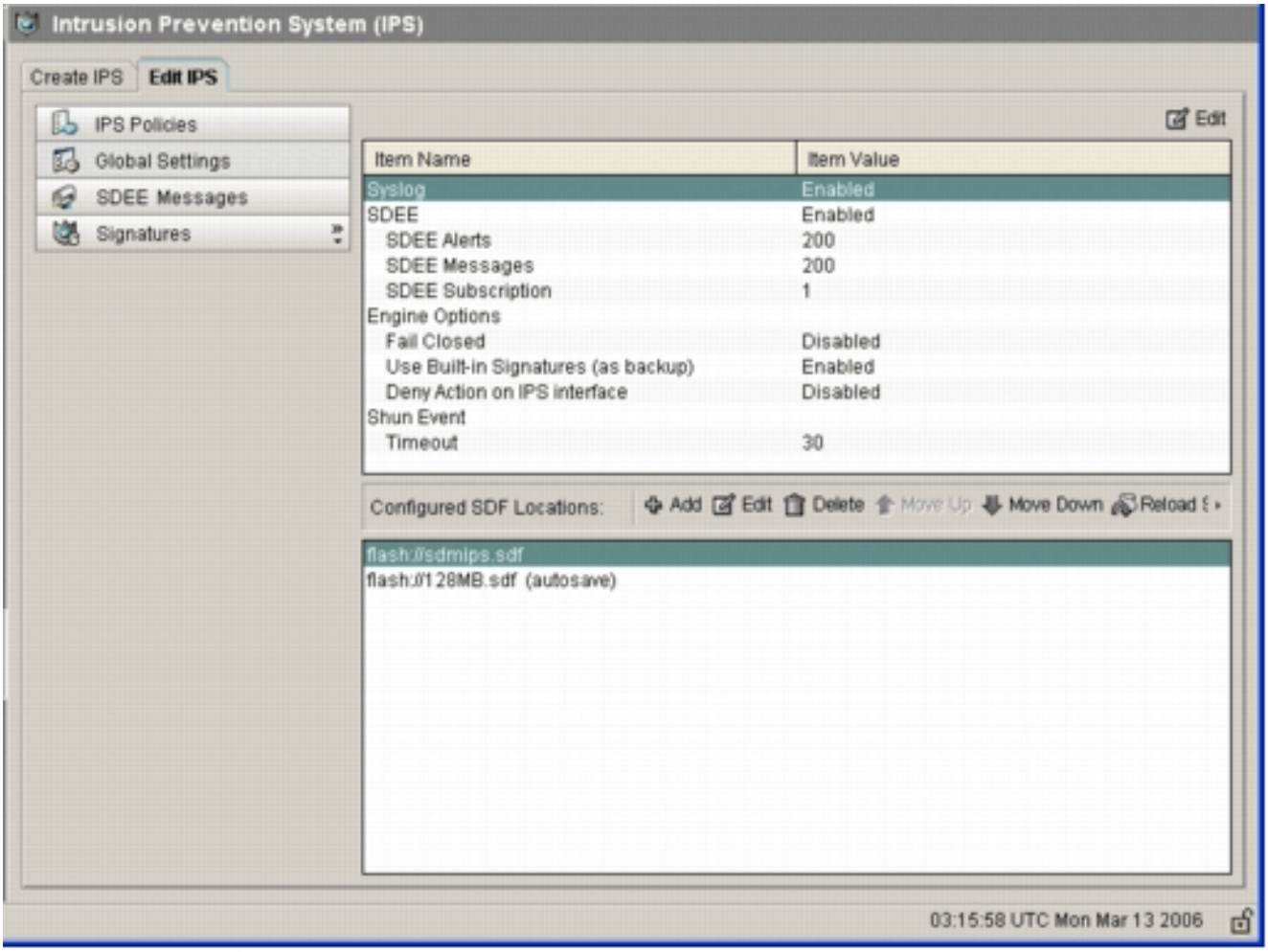
في هذا المثال، يستخدم الموجه وحدة تحكم بسرعة 256 ميجابت.SDF على ذاكرة Flash (الذاكرة المؤقتة). يتم تحديث الملف عند نسخ الجهاز الجديد الذي تم تنزيله بسرعة 256 ميجابت.SDF إلى ذاكرة Flash الخاصة بالموجه.

2. قم بإعادة تحميل النظام الفرعي Cisco IOS IPS لتشغيل الملفات الجديدة.هناك طريقتان لإعادة تحميل Cisco IOS IPS: إعادة تحميل الموجه أو إعادة تكوين Cisco IOS IPS لتشغيل النظام الفرعي IOS IPS لإعادة تحميل التوقيعات. لإعادة تكوين Cisco IOS IPS، قم بإزالة جميع قواعد IPS من الواجهات التي تم تكوينها، ثم قم بإعادة تطبيق قواعد IPS مرة أخرى على الواجهات. وهذا سيقوم بتشغيل نظام Cisco IOS IPS لإعادة التحميل.

إجراء SDM 2.2

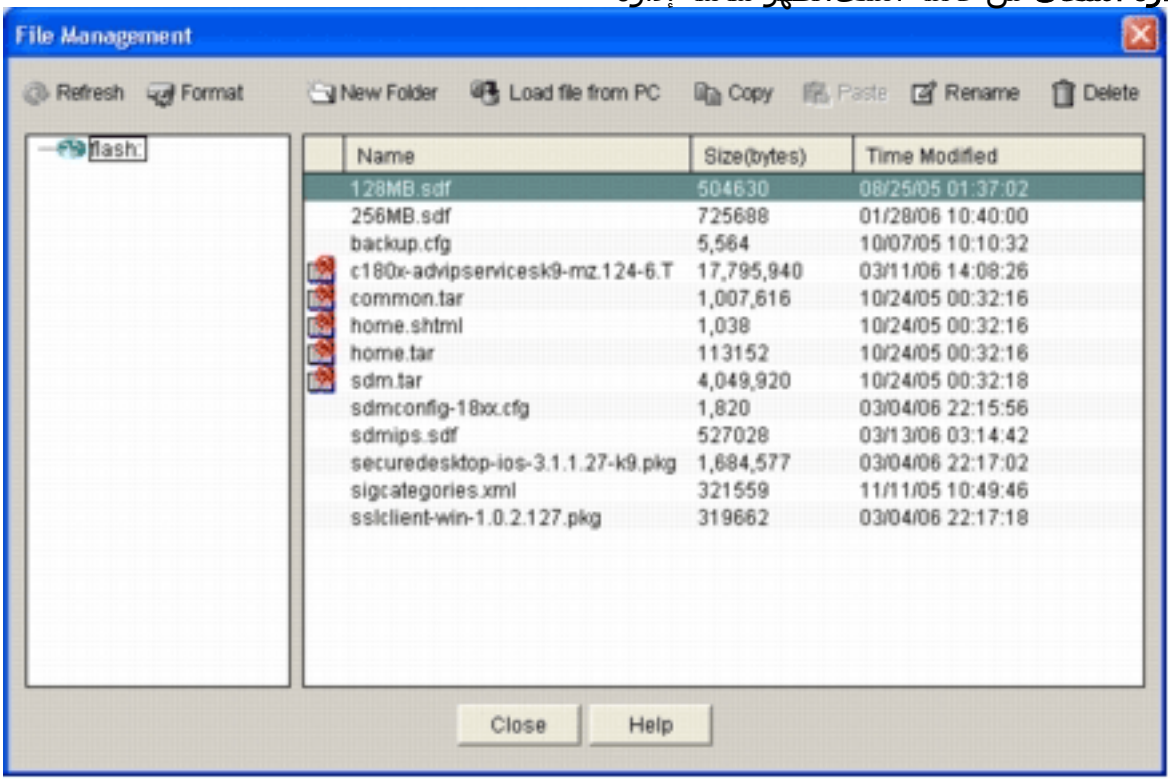
أتمت هذا steps in order to حدثت التقصير SDFs على المسحاج تخديد:

1. انقر فوق **تكوين**، ثم انقر فوق **منع التسلل**.
2. انقر فوق علامة التبويب **تحرير IPS**، ثم انقر فوق **إعدادات عامة**.



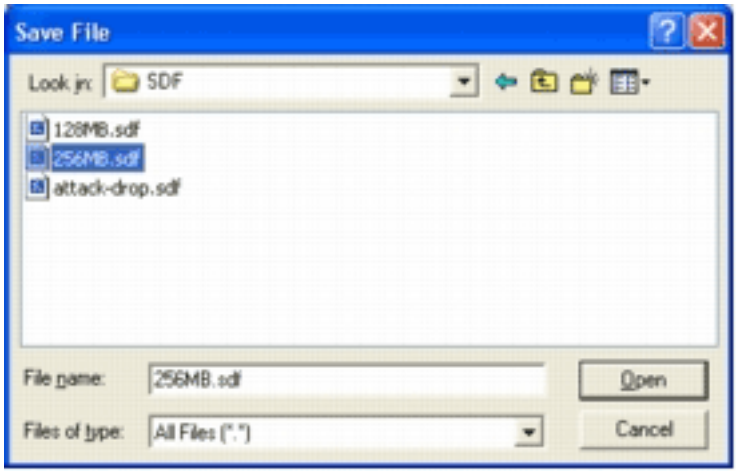
يظهر أعلى واجهة المستخدم الإعدادات العمومية. يظهر النصف السفلي من واجهة المستخدم مواقع SDF التي تم تكوينها حاليا. في هذه الحالة، يتم تكوين ملف 256 ميجابت.sdf من ذاكرة Flash.

3. أختر **إدارة الملفات** من قائمة الملف.تظهر شاشة إدارة



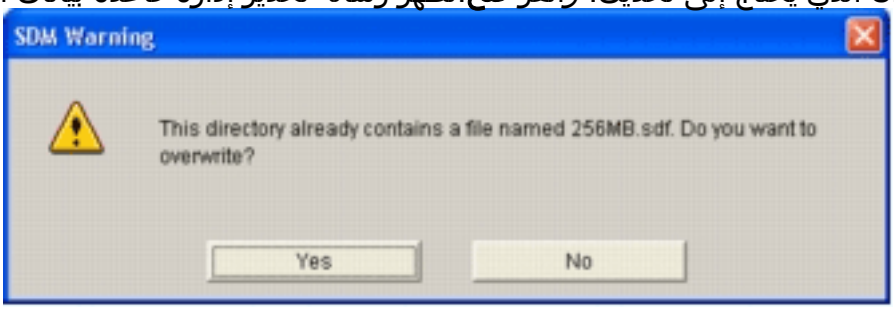
الملف.

4. طقطقة **تحميل مبرد من pc**.سوف يظهر مربع الحوار حفظ



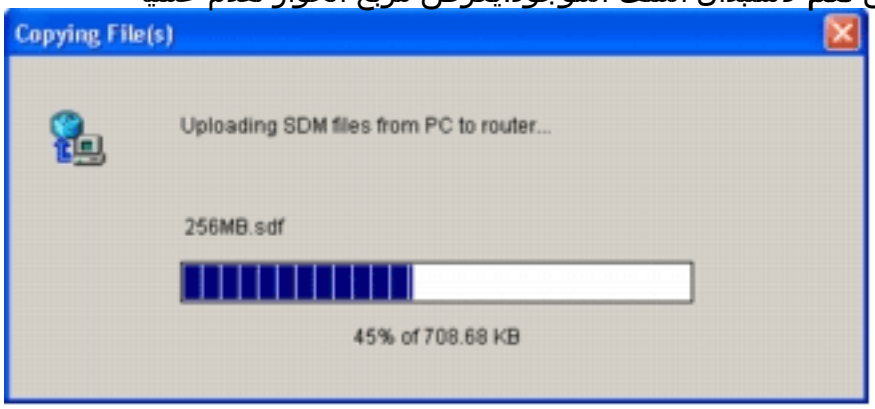
الملف.

5. أختر SDF الذي يحتاج إلى تحديث، وانقر **فتح**.تظهر رسالة تحذير إدارة قاعدة بيانات المحول



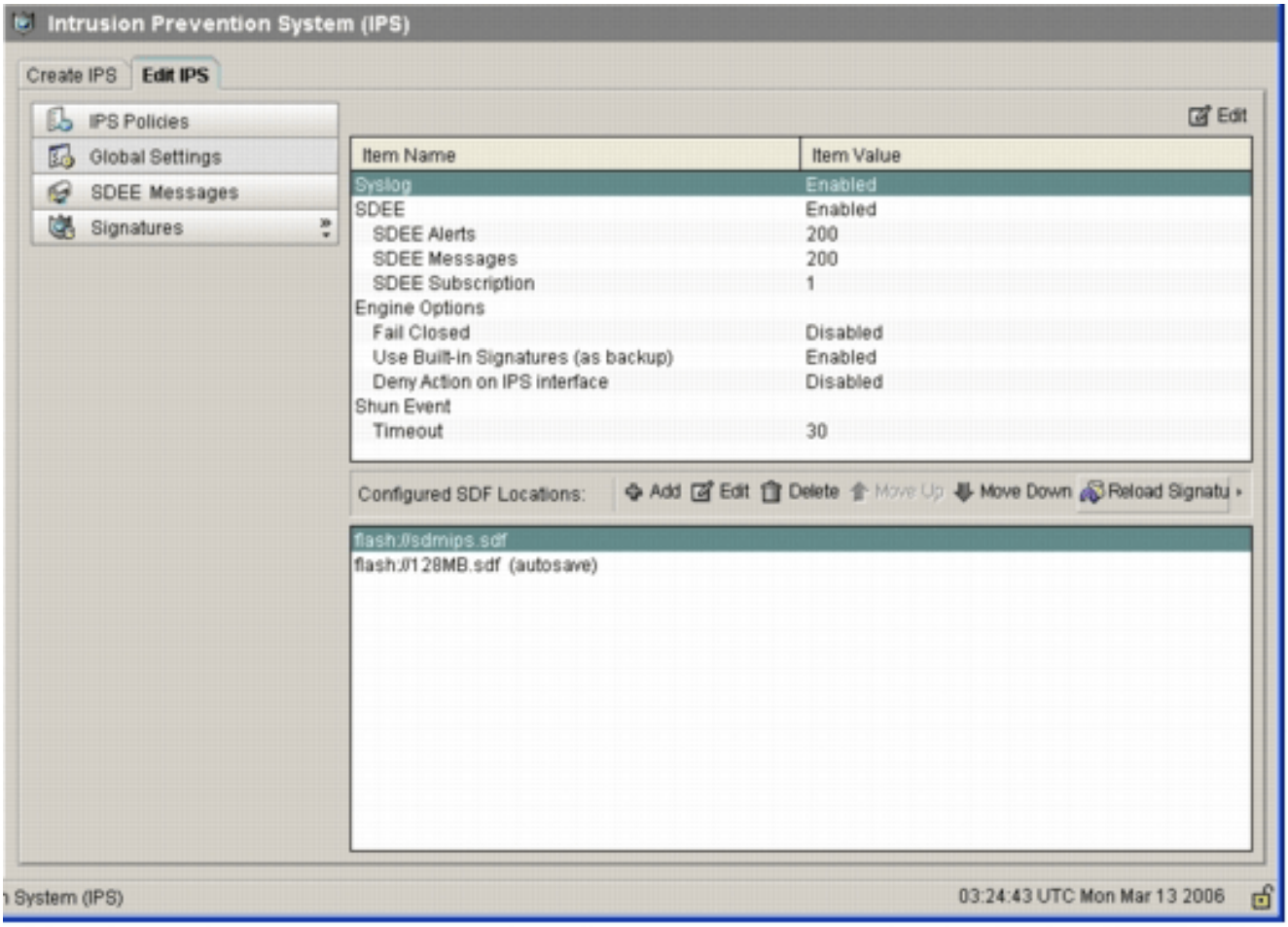
(SDM).

6. انقر فوق **نعم** لاستبدال الملف الموجود.يعرض مربع الحوار تقدم عملية



التحميل.

7. بمجرد اكتمال عملية التحميل، انقر فوق **إعادة تحميل التوقيعات** الموجودة على شريط أدوات موقع SDF. يقوم هذا الإجراء بإعادة تحميل Cisco IOS IPS.



ملاحظة: تحتوي حزمة IOS-SXXX.zip على جميع التوقيعات التي يدعمها Cisco IOS IPS. يتم نشر الترقيات إلى حزمة التوقيع هذه على موقع الويب Cisco.com بمجرد توفرها. لتحديث التوقيعات الواردة في هذه الحزمة، راجع الخطوة 2.

معلومات ذات صلة

- نظام Cisco لمنع الاقتحام
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك اكتشاف إقتحام CiscoSecure)
- الدعم الفني - 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).