مادختسإ ةصاخلا ةيلحملا دعاوقلا ةكبشل Cisco نم FireSIGHT

المحتويات

المقدمة

القاعدة المحلية المخصصة الموجودة على نظام FireSIGHT هي قاعدة Snort قياسية مخصصة تقوم بإدراجها بتنسيق ملف نصي ASCII من جهاز محلي. يتيح لك نظام FireSIGHT إستيراد القواعد المحلية باستخدام واجهة الويب. إن الخطوات اللازمة لاستيراد القواعد المحلية واضحة ومباشرة للغاية. ومع ذلك، لكتابة قاعدة محلية مثالية، يتطلب المستخدم معرفة متعمقة ببروتوكولات الشبكة والشبكة.

الغرض من هذا المستند هو توفير بعض التلميحات والمساعدة لك لكتابة قاعدة محلية مخصصة. تتوفر التعليمات الخاصة بإنشاء قواعد محلية في *دليل مستخدمي الشورت* المتوفر على snort.org. توصيك Cisco بتنزيل دليل المستخدمين وقراءته قبل كتابة قاعدة محلية مخصصة.

ملاحظة: يتم إنشاء القواعد المنصوص عليها في حزمة تحديث قاعدة (SRU (Sourcefire واختبارها بواسطة مجموعة Cisco Talos Security Intelligence and Research، ويدعمها مركز المساعدة التقنية (TAC) من Cisco. لا يقدم ال cisco TAC مساعدة على كتابة أو توليف قاعدة محلية مخصصة، ومع ذلك إذا واجهت أي مشاكل مع القاعدة إستيراد وظيفة من نظام FireSIGHT ك، رجاء اتصل ب ال cisco TAC.

تحذير: يمكن أن تؤثر قاعدة محلية مخصصة غير مكتوبة بشكل جيد على أداء نظام FireSIGHT الذي يمكن أن يؤدي إلى انخفاض أداء الشبكة بالكامل. إذا كنت تواجه أي مشاكل في الأداء في شبكتك، وكانت هناك بعض قواعد الشخر المحلية المخصصة ممكنة على نظام FireSIGHT لديك، فإن Cisco توصيك بتعطيل هذه القواعد المحلية.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة على snort قاعدة و FireSIGHT نظام.

المكونات المستخدمة

أسست المعلومة على هذا وثيقة على هذا جهاز وبرمجية صيغة:

- مركز إدارة FireSIGHT (المعروف أيضا باسم Defense Center)
- الإصدار 5.2 من البرنامج أو إصدار أحدث

العمل باستخدام القواعد المحلية المخصصة

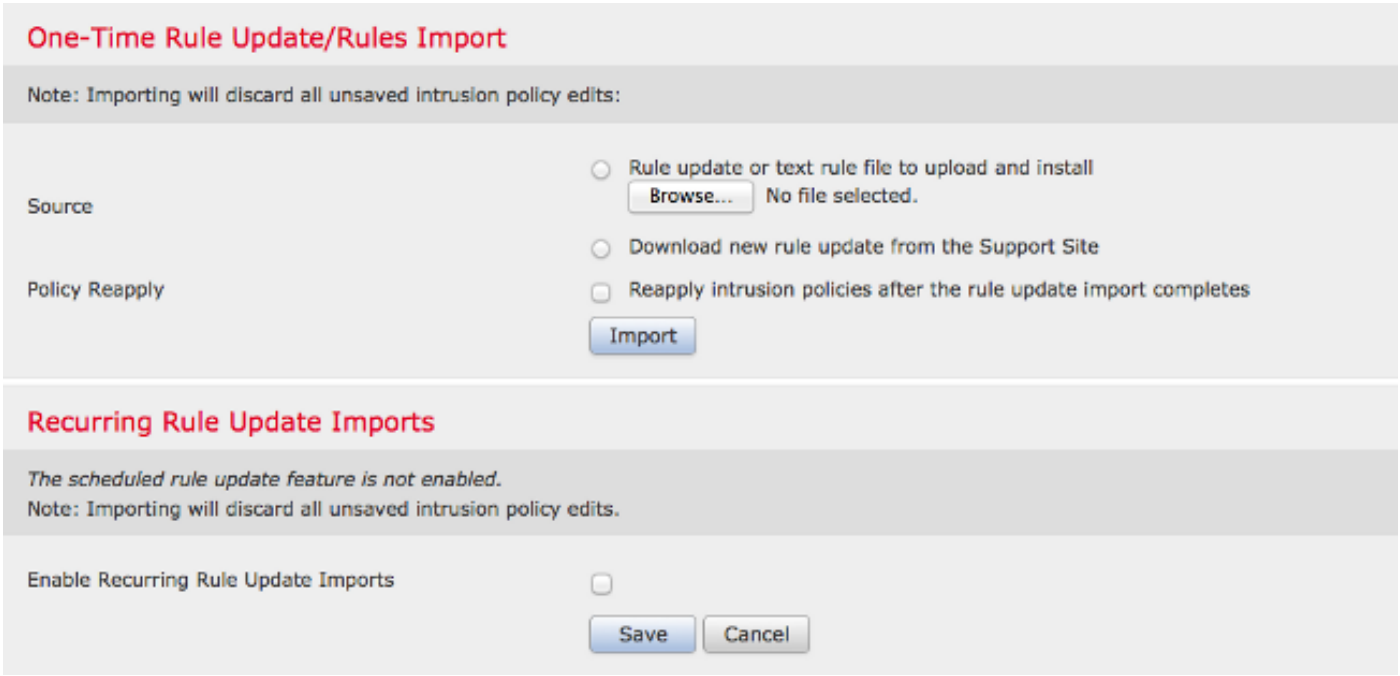
إستيراد القواعد المحلية

قبل البدء، يجب التأكد من أن القواعد الموجودة في الملف لا تحتوي على أي أحرف هروب. يتطلب مستورد القاعدة إستيراد كافة القواعد المخصصة باستخدام ترميز ASCII أو UTF-8.

يشرح الإجراء التالي كيفية إستيراد قواعد النص القياسية المحلية من جهاز محلي:

1. يمكنك الوصول إلى صفحة **محرر القواعد** من خلال الانتقال إلى **السياسات > التسلل > محرر القواعد**.

2. انقر فوق **قواعد الاستيراد**. تظهر صفحة **تحديثات القواعد**.



شكل: لقطة شاشة لصفحة تحديثات القواعد

3. حدد **تحديث القاعدة أو ملف القاعدة النصية لتحميله وتثبيته** وانقر فوق **إستعراض** لتحديد ملف القاعدة.

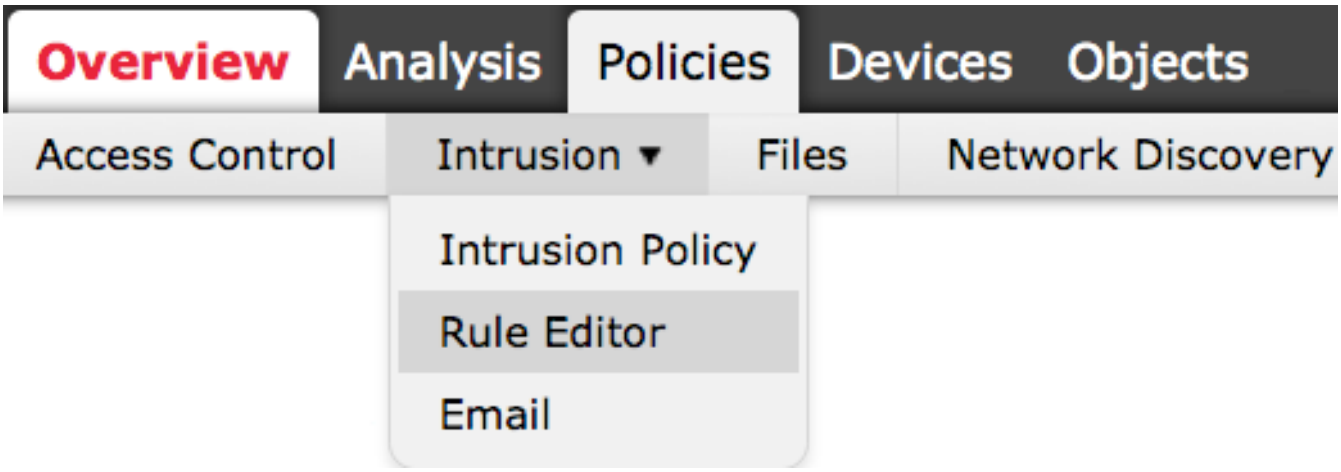
ملاحظة: يتم حفظ جميع القواعد التي تم تحميلها في فئة **القاعدة المحلية**.

4. انقر فوق **إستيراد**. تم إستيراد ملف القاعدة.

تحذير: لا تستخدم أنظمة FireSIGHT القاعدة الجديدة الموضوعة للتفتيش. لتنشيط قاعدة محلية، تحتاج إلى تمكينها في نهج التطفل، ثم تطبيق النهج.

عرض القواعد المحلية

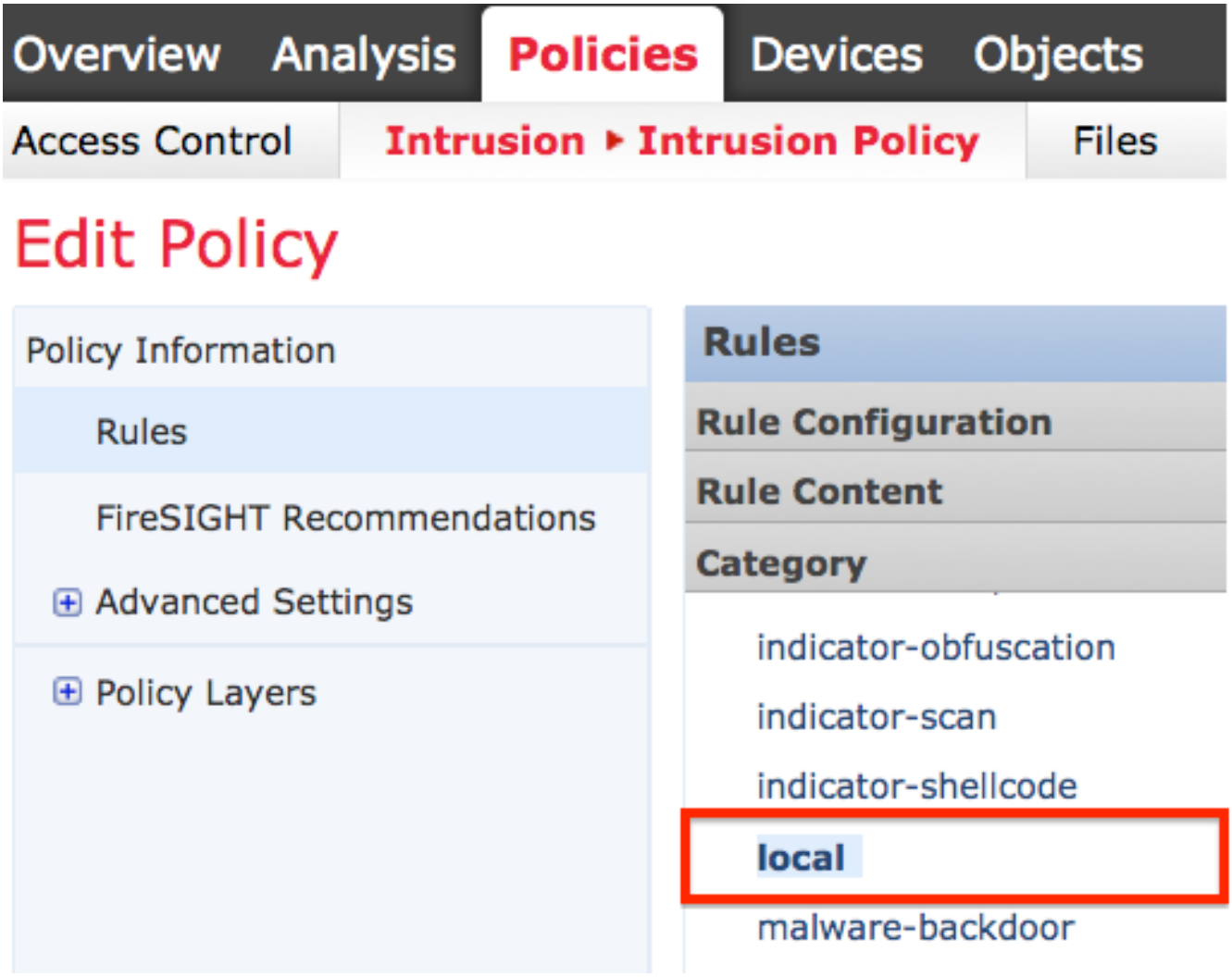
- لعرض رقم المراجعة لقاعدة محلية حالية، انتقل إلى صفحة **محرر القواعد** (**السياسات > الاقتحام > محرر القاعدة**).



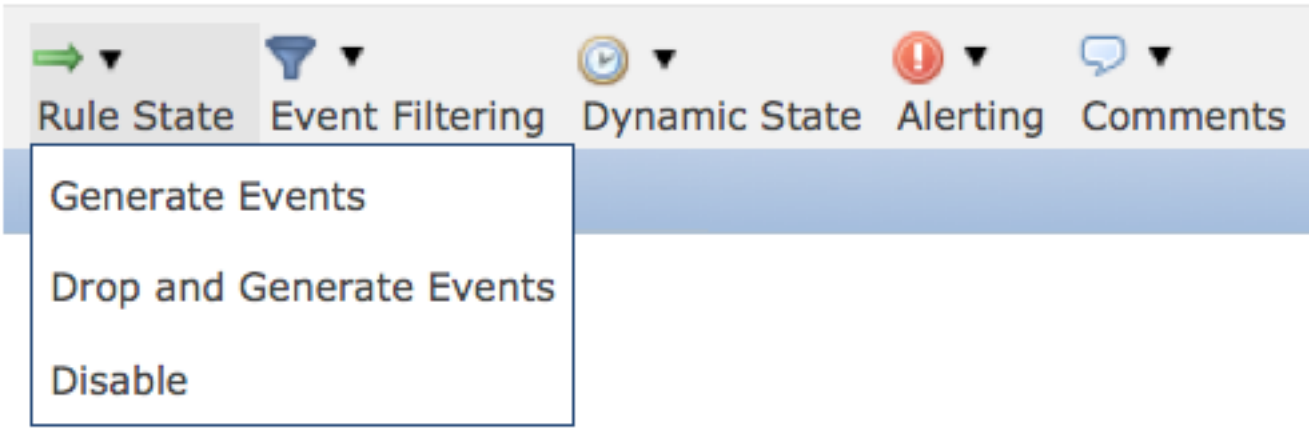
- في صفحة محرر القواعد، انقر فوق فئة **القاعدة المحلية** لتوسيع المجلد، ثم انقر فوق **تحرير** بجوار القاعدة.
- يتم حفظ كافة القواعد المحلية المستوردة تلقائيا في فئة **القاعدة المحلية**.

تمكين القواعد المحلية

- بشكل افتراضي، يضع FireSIGHT System القواعد المحلية في حالة تعطيل. يجب تعيين حالة القواعد المحلية يدويا قبل أن تتمكن من إستخدامها في سياسة التطفل الخاصة بك.
لتمكين قاعدة محلية، انتقل إلى صفحة محرر السياسات (**السياسات > الاقتحام > نهج الاقتحام**). حدد **القواعد** في اللوحة اليسرى. تحت **الفئة**، حدد **محلي**. يجب أن تظهر جميع القواعد المحلية، إذا كانت متاحة.



- بعد تحديد القواعد المحلية المطلوبة، حدد حالة للقواعد.



- بمجرد تحديد حالة القاعدة، انقر على خيار **معلومات السياسة** في اللوحة اليسرى. حدد الزر **تنفيذ التغييرات**. تم التحقق من صحة نهج الاقتحام.

ملاحظة: يفشل التحقق من صحة النهج إذا قمت بتمكين قاعدة محلية مستوردة تستخدم الكلمة الأساسية للحد المهمل بالإضافة إلى ميزة حد حدث الاقتحام في سياسة الاقتحام.

عرض القواعد المحلية المحذوفة

- يتم نقل جميع القواعد المحلية المحذوفة من فئة القاعدة المحلية إلى فئة القاعدة المحذوفة.

- لعرض رقم المراجعة لقاعدة محلية محذوفة، انتقل إلى صفحة **محرر القواعد**، وانقر فوق الفئة **المحذوف** لتوسيع المجلد، ثم انقر فوق أيقونة *قلم رصاص* لعرض تفاصيل القاعدة في صفحة **محرر القواعد**.

ترقيم القواعد المحلية

- لا يتوجب عليك تحديد مولد (GID)، إذا قمت بذلك، يمكنك تحديد GID 1 فقط لقاعدة نص قياسية أو 138 لقاعدة بيانات حساسة.
- لا تقم بتحديد معرف Snort (SID) أو رقم المراجعة عند إستيراد قاعدة للمرة الأولى، وهذا يتفادى التصادم مع SIDs للقواعد الأخرى، بما في ذلك القواعد المحذوفة.
- يقوم مركز إدارة FireSIGHT تلقائيا بتعيين معرف الأمان (SID) المخصص التالي المتاح أو أكثر من 100000، ورقم مراجعة من 1.
- إذا حاولت إستيراد قاعدة أختراق مع SID أكبر من 2147483647، سيحدث خطأ في التحقق من الصحة.
- يجب تضمين SID المعين من قبل IPS ورقم مراجعة أكبر من رقم المراجعة الحالي عند إستيراد إصدار محدث من قاعدة محلية قمت باستيرادها مسبقا.
- يمكنك إعادة القاعدة المحلية التي قمت بحذفها عن طريق إستيراد القاعدة باستخدام SID المعين من قبل IPS ورقم مراجعة أكبر من رقم المراجعة الحالي. لاحظ أن FireSIGHT Management Center يقوم بزيادة رقم المراجعة تلقائيا عند حذف قاعدة محلية، وهذا جهاز يسمح لك بإعادة وضع القواعد المحلية.

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).