Cisco Secure IPS - إستثناء التنبيهات الإيجابية الخاطئة

المحتويات

المقدمة

يصف هذا المستند إستبعاد التنبيهات الإيجابية الخاطئة لنظام منع التسلل الآمن (IPS) من Cisco.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 7.0 من نظام منع التسلل الآمن (IPS) من Cisco و Cisco IPS Manager Express 7.0.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

الإنذارات السلبية والإيجابية الخاطئة

يقوم Cisco Secure IPS بتشغيل تنبيه عندما تطابق حزمة أو تسلسل معين من الحزم خصائص ملفات تعريف الهجوم المعروفة المعرفة في توقيعات IPS الآمنة من Cisco. معيار تصميم توقيع IPS الحرج هو تقليل ظهور الإنذارات الإيجابية والسلبية الخاطئة إلى الحد الأدنى.

تحدث العوامل الإيجابية الخاطئة (المشغلات الحميدة) عندما يقوم نظام منع الاختراقات (IPS) بالإبلاغ عن بعض الأنشطة الحميدة على أنها ضارة. يتطلب ذلك تدخلا بشريا لتشخيص الحدث. إن عددا كبيرا من الإيجابيات الكاذبة من الممكن أن تستنزف الموارد إلى حد كبير، والمهارات المتخصصة المطلوبة لتحليل هذه الإيجابيات مكلفة ومن الصعب العثور عليها.

تحدث السلبيات الخاطئة عندما لا يكتشف IPS النشاط الضار الفعلي ولا يبلغ عنه. قد تكون عاقبة ذلك كارثية، والتواقيع يجب أن تحدث بإستمرار بإكتشاف أي اكتشافات وتقنيات قرصنة جديدة. فالتقليل إلى أدنى حد من السلبيات الباطلة يعطى أولوية عالية جدا، وأحيانا على حساب تكرار الايجابيات الخاطئة أكثر.

نظرا لطبيعة التوقيعات التي تستخدمها خدمات الإنترنت (IPS) للكشف عن الأنشطة الضارة، يكاد يكون من المستحيل القضاء تماما على الإيجابيات والسلبيات الزائفة دون الإضرار بشدة بفعالية خدمات الإنترنت (IPS) أو الإخلال الشديد بالبنية الأساسية للحوسبة في إحدى المؤسسات (مثل الأجهزة المضيفة والشبكات). يؤدي التوليف المخصص عند نشر بروتوكول الإنترنت (IPS) إلى تقليل الإيجابيات الخاطئة إلى الحد الأدنى. يلزم إعادة الضبط دوريا عند تغير بيئة الحوسبة (على سبيل المثال، عند نشر أنظمة وتطبيقات جديدة). يوفر نظام منع التسلل (IPS) الآمن من Cisco إمكانية ضبط مرنة يمكنها تقليل الإيجابيات الخاطئة أثناء عمليات الحالة المستقرة.

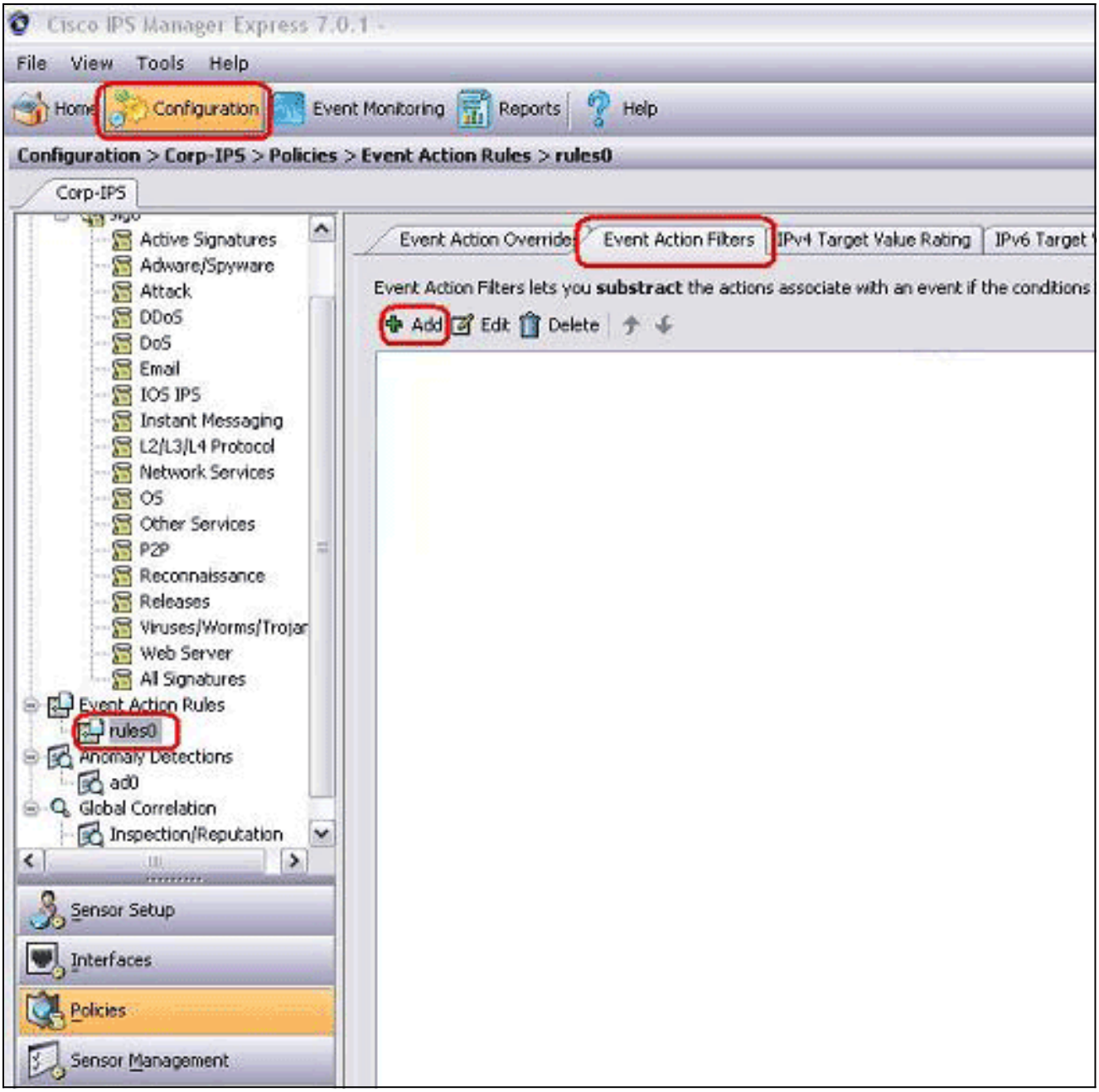
آلية إستثناء Cisco Secure IPS

يوفر Cisco Secure IPS إمكانية إستبعاد توقيع معين من أو إلى مضيف معين أو عناوين شبكة معينة. لا تقوم التوقيعات المستبعدة بإنشاء أيقونات تنبيه أو سجلات سجل عندما يتم تشغيلها من البيئات المضيفة أو الشبكات التي يتم إستبعادها بشكل محدد من خلال هذه الآلية. على سبيل المثال، قد تقوم محطة إدارة شبكة بإجراء اكتشاف الشبكة من خلال تشغيل عمليات تمشيط شبكة ICMP، والتي تقوم بتشغيل "كنس شبكة ICMP" باستخدام توقيع "إيكو" (معرف التوقيع 2100). إذا قمت باستبعاد التوقيع، فلا تحتاج إلى تحليل التنبيه وحذفه في كل مرة يتم فيها تشغيل عملية اكتشاف الشبكة.

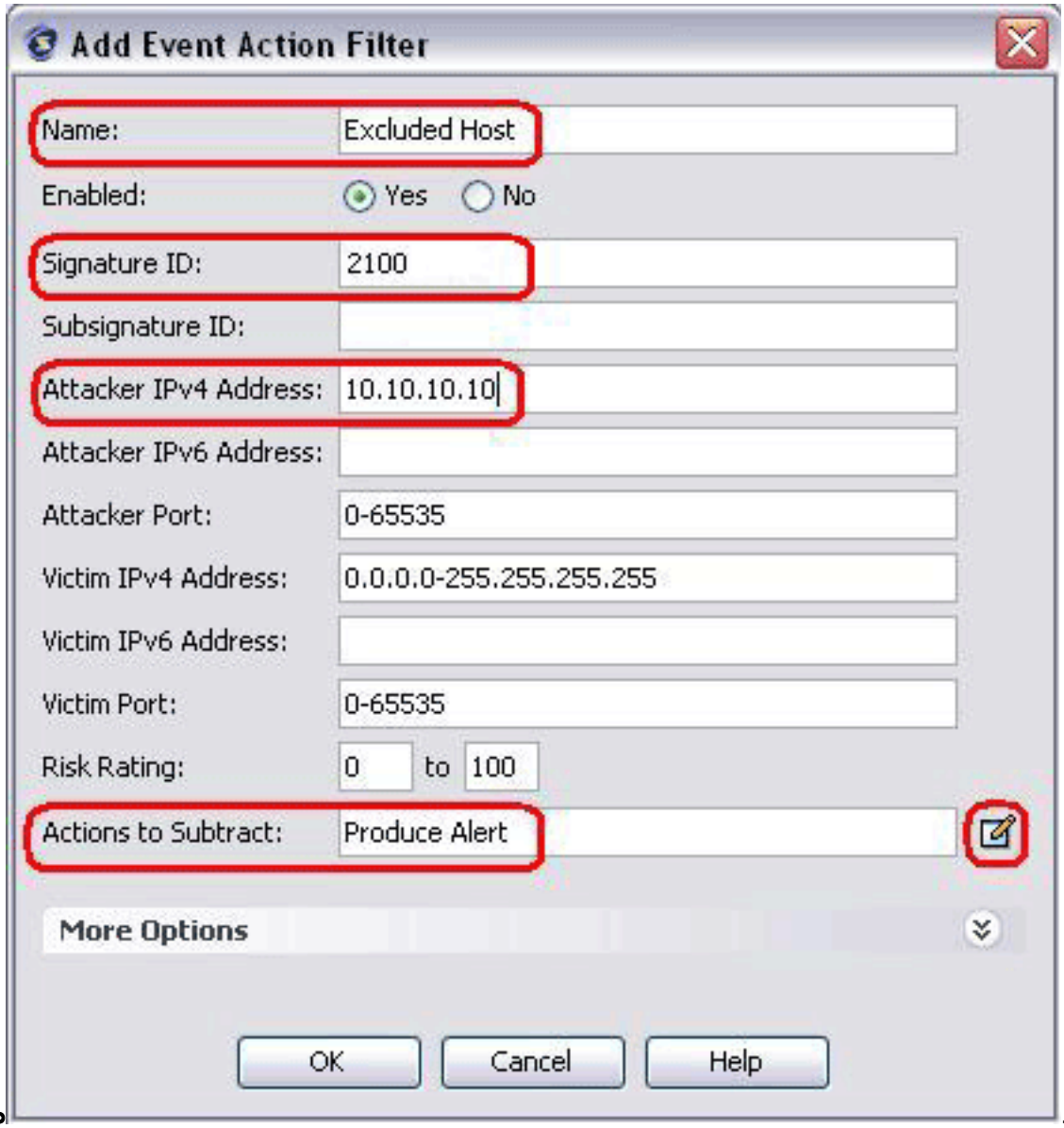
إستبعاد مضيف

أتمت هذا steps in order to استثنيت مضيف خاص (مصدر عنوان) من توليد توقيع تنبيه خاص:

1. أخترت **تشكيل>Corp-IPS>سياسة>حدث إجراء قاعدة>قاعدة0**، وطقطقة **الحدث إجراء مرشح**.



2. انقر فوق **إضافة (Add)**.
3. اكتب اسم المرشح ومعرف التوقيع وعنوان IPv4 للمهاجم والإجراء الخاص بالطرح في الحقول المناسبة، ثم انقر فوق



موافق.

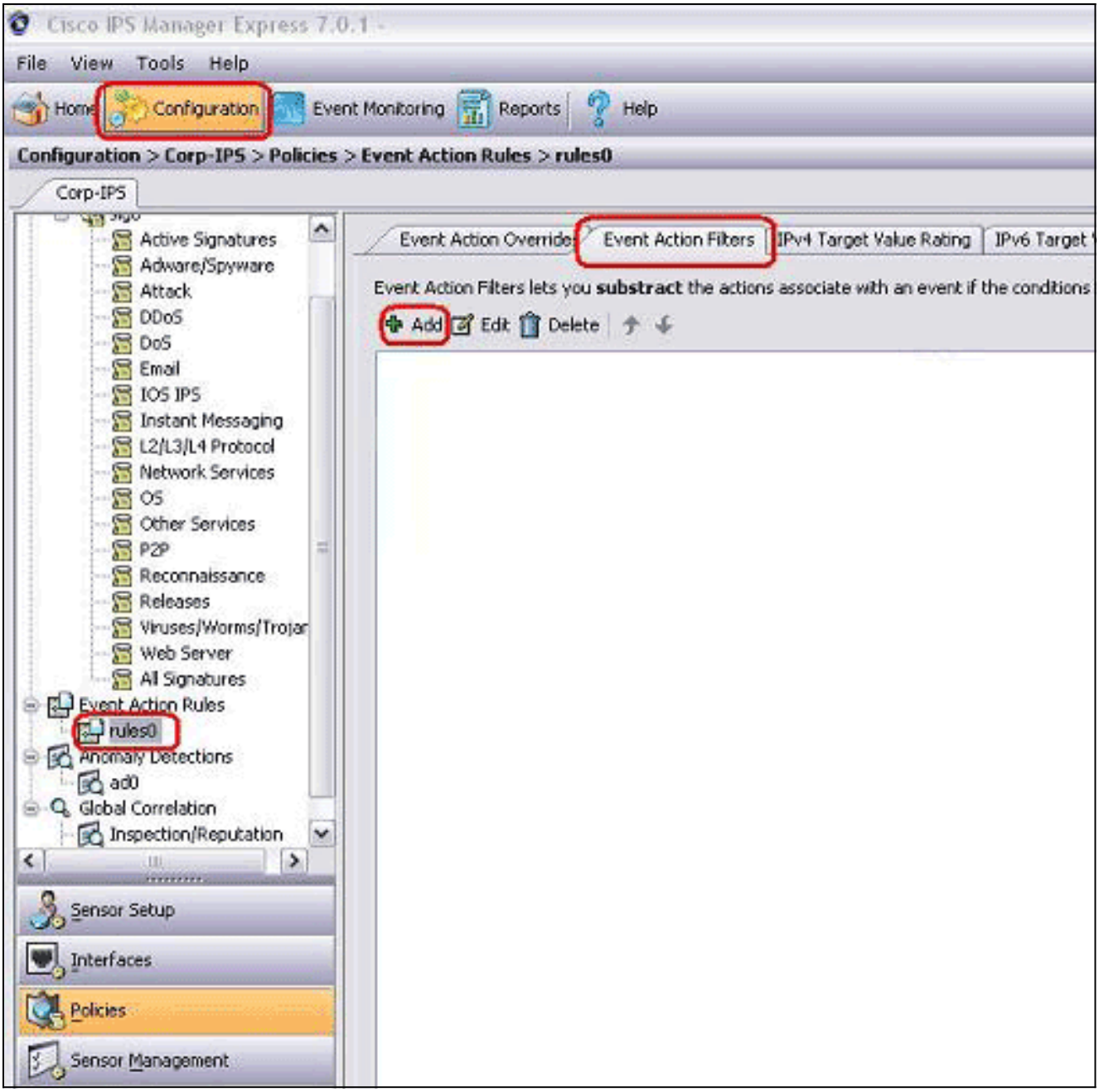
ملاحظة: إذا احتجت لاستبعاد عناوين IP متعددة من شبكات مختلفة، فيمكنك إستخدام الفاصلة كمحدد. على أي حال، إذا كنت تستخدم فاصلة، تجنب مسافة زائدة بعد الفاصلة؛ وإلا، فقد تتلقى خطأ.**ملاحظة:** بالإضافة إلى ذلك، يمكنك إستخدام المتغيرات المعرفة في صفحة متغيرات الحدث. تكون هذه المتغيرات مفيدة عندما يجب تكرار نفس القيمة في مرشحات إجراءات حدث متعددة. يجب إستخدام علامة الدولار ($) كبادئة للمتغير. يمكن أن يكون المتغير أحد هذه التنسيقات:عنوان IP كامل، على سبيل المثال، 10.77.23.23.نطاق عناوين IP؛ على سبيل المثال، 10.9.2.10-10.9.2.155.مجموعة من نطاق عناوين IP؛ على سبيل المثال، 172.16.33.15-192.168.100.11،192.168.100.1-172.16.33.100.

إستبعاد شبكة

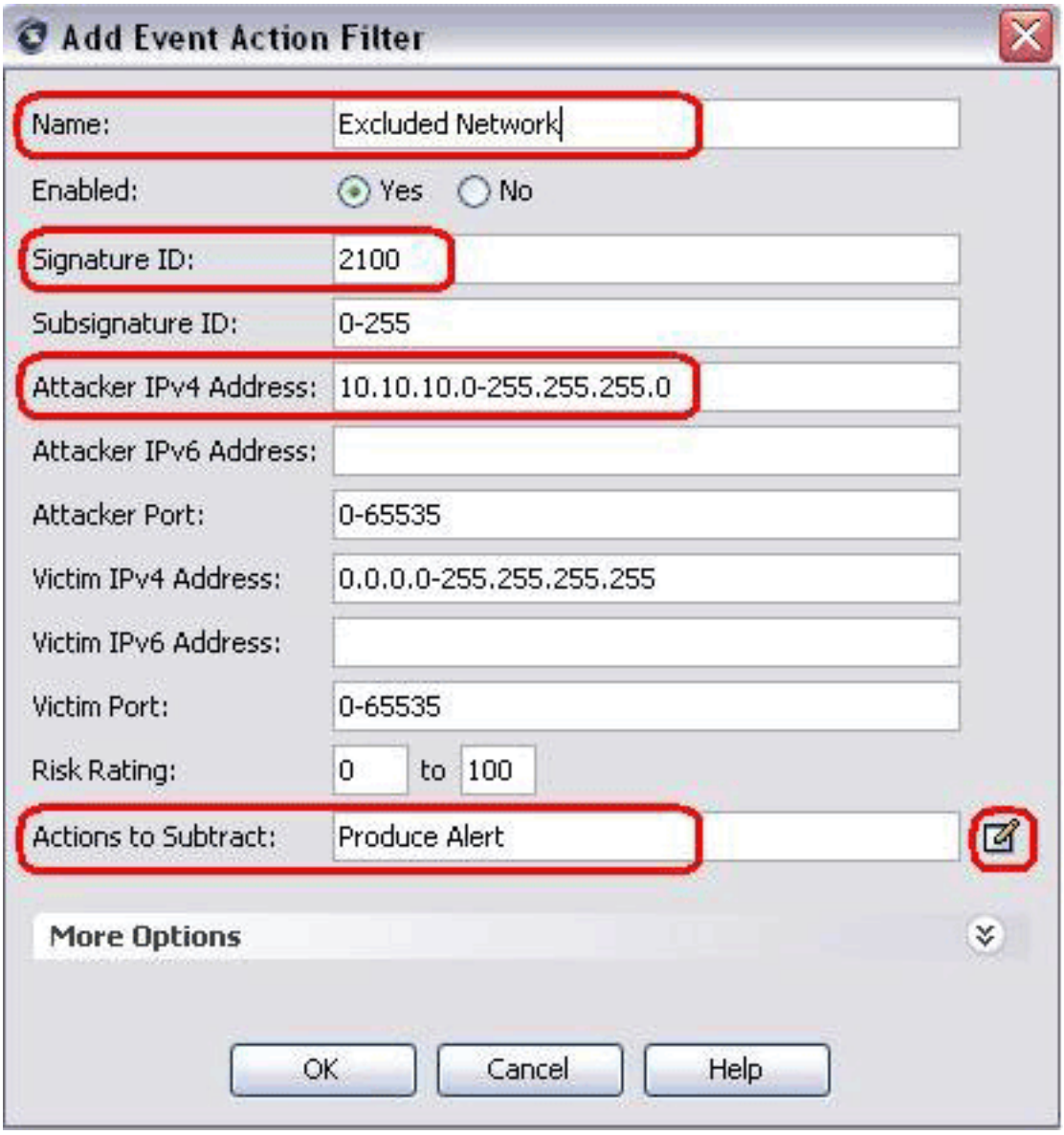
كما يستثني عامل تصفية إجراء الحدث توقيعات معينة لإطلاق تنبيه استنادا إلى عنوان شبكة مصدر أو وجهة.

أتمت هذا steps in order to استثنيت شبكة من توليد توقيع تنبيه خاص:

1. انقر فوق علامة التبويب **عوامل تصفية إجراء الحدث**.



2. انقر فوق **إضافة (Add)**.
3. اكتب اسم المرشح، معرف التوقيع، عنوان الشبكة بقناع شبكة فرعية، والإجراء الخاص بالطرح في الحقول المناسبة، ثم انقر فوق

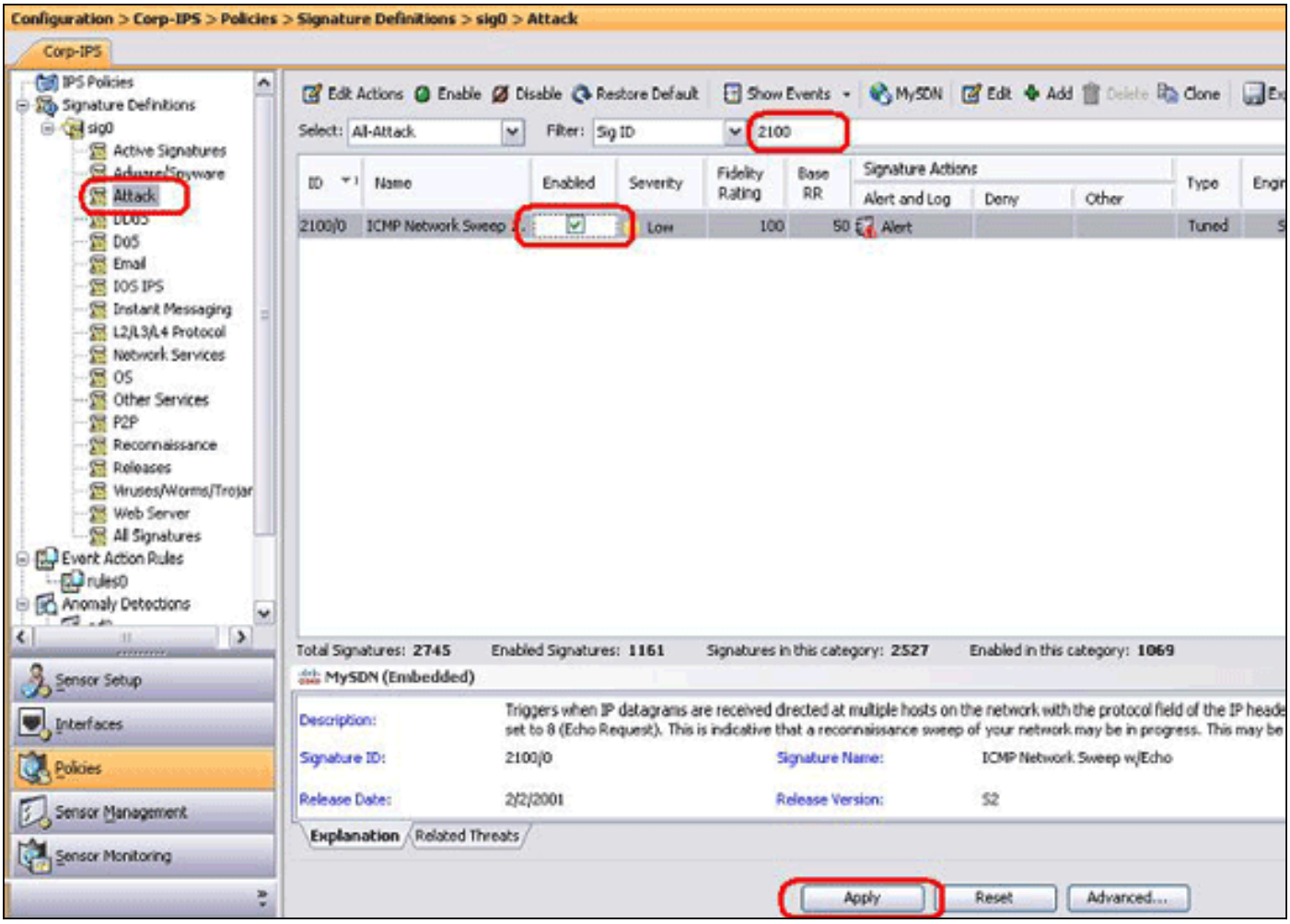


موافق.

تعطيل التوقيعات بشكل عام

قد ترغب في تعطيل توقيع من غير مقلق في أي وقت. لتمكين التوقيعات وتعطيلها واستعادتها، أكمل الخطوات التالية:

1. قم بتسجيل الدخول إلى IME باستخدام حساب ذي امتيازات المسؤول أو عامل التشغيل.
2. أخترت تشكيل>مستشعر_name>نهج>**توقيع تعريفات>sig0>**كل التوقيعات.
3. لتحديد موقع توقيع، أختر خيار فرز من القائمة المنسدلة مرشح. على سبيل المثال، إذا كنت تبحث عن توقيع مسح شبكة ICMP، أختر **كل التوقيعات** تحت sig0، ثم ابحث باستخدام معرف التوقيع أو الاسم. يقوم جزء sig0 بتحديث تلك التوقيعات التي تطابق معايير الفرز الخاصة بك وعرضها فقط.
4. لتمكين أو تعطيل توقيع موجود، أختر التوقيع، وإكمال الخطوات التالية:عرض العمود "ممكن" لتحديد حالة التوقيع. التوقيع الذي تم تمكينه له خانة الاختيار.لتمكين توقيع معطل، حدد خانة الاختيار **ممكن**.لتعطيل توقيع تم تمكينه، قم بإلغاء تحديد خانة الاختيار **تمكين**.لاستبعاد توقيع أو أكثر، أختر التوقيع (التوقيعات)، وانقر بزر الماوس الأيمن، ثم انقر فوق **تغيير الحالة إلى > مستبعد**.
5. انقر فوق **تطبيق** لتطبيق التغييرات التي قمت بها وحفظ التكوين الذي تمت مراجعته.



معلومات ذات صلة

- نهاية البيع لمدير Cisco Secure IDS
- صفحة دعم اكتشاف التسلل الآمن من Cisco
- 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).