تكوين نظام FireSIGHT لإرسال تنبيهات إلى خادم syslog خارجي

المحتويات

المقدمة

في حين يوفر نظام FireSIGHT طرق عرض مختلفة للأحداث داخل واجهة الويب الخاصة به، فقد تحتاج إلى تكوين إعلام خارجي بالأحداث لتسهيل المراقبة المستمرة للأنظمة الحساسة. يمكنك تكوين نظام FireSIGHT لإنشاء تنبيهات تقوم بإعلامك عبر البريد الإلكتروني أو ملائمة SNMP أو syslog عند إنشاء أحد الأمور التالية. يوضح هذا المقال كيفية تكوين مركز إدارة FireSIGHT لإرسال تنبيهات على خادم syslog خارجي.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة على syslog و FireSIGHT إدارة مركز. أيضا، ال syslog ميناء (تقصير هو 514) ينبغي كنت سمحت في جدار الحماية ك.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 5.2 من البرنامج أو إصدار أحدث.

تحذير: يتم إنشاء المعلومات الواردة في هذا المستند من جهاز في بيئة معملية خاصة، ويبدأ بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

إرسال تنبيهات إقتحام

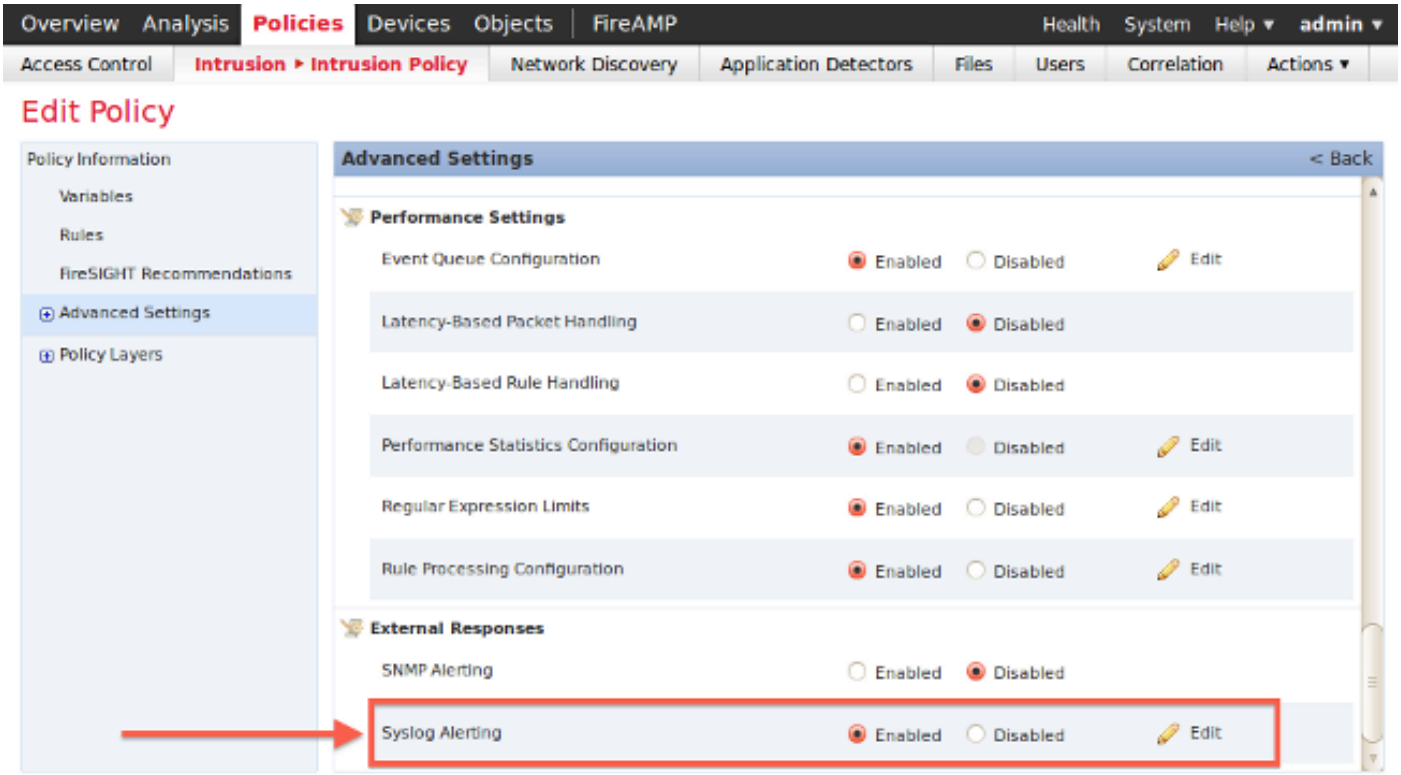
1. سجل الدخول إلى واجهة مستخدم الويب الخاصة بمركز إدارة FireSIGHT لديك.

2. انتقل إلى **السياسات** > **الاختراق** > **سياسة الاختراق**.

3. انقر فوق **تحرير** بجوار النهج الذي تريد تطبيقه.

4. انقر على **إعدادات متقدمة**.

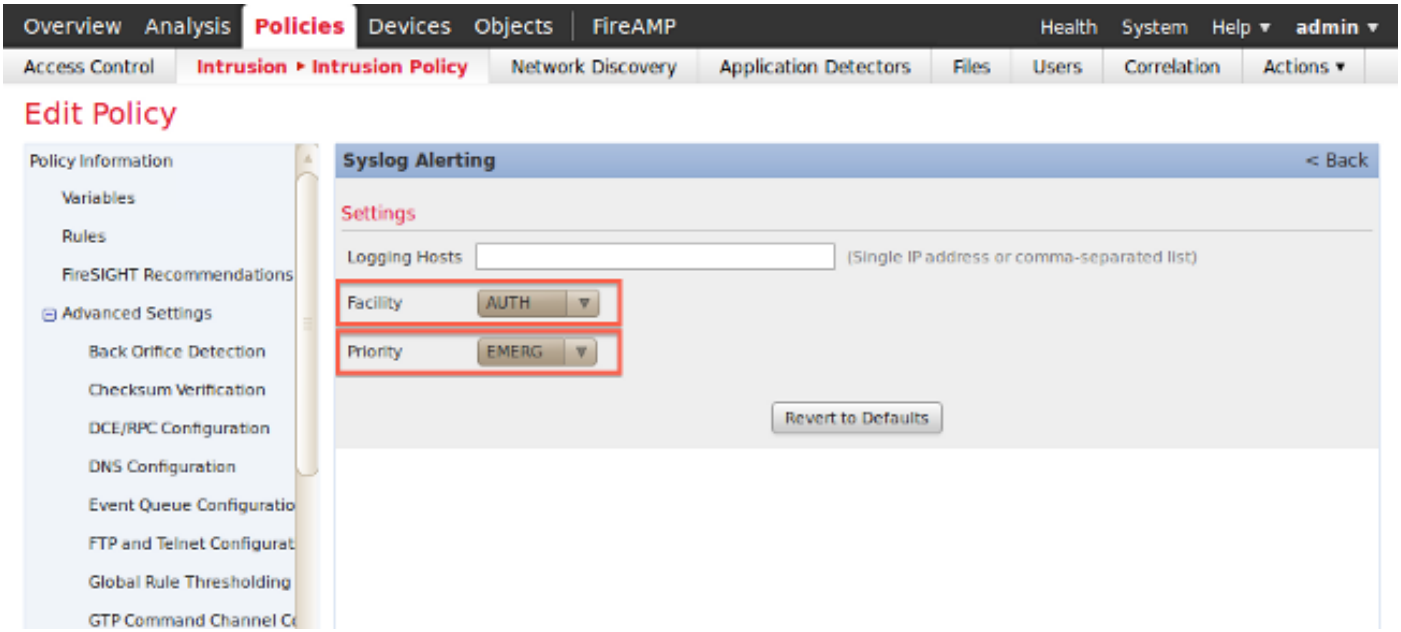
5. حدد موقع **تنبيه Syslog** في القائمة وتعيينه على **ممكن**.



6. انقر فوق **تحرير** الموجود بجانب **تنبيه Syslog**.

7. اكتب عنوان IP الخاص بخادم syslog على حقل **مضيفي التسجيل**.

8. أختر **وحدة** مناسبة و**مستوى الخطورة** من القائمة المنسدلة. ويمكن ترك هذه العناصر عند القيم الافتراضية ما لم يتم تكوين خادم syslog لقبول التنبيهات الخاصة بمرفق معين أو مستوى خطورة محدد.



9. انقر فوق **معلومات النهج** بالقرب من الجزء العلوي الأيسر من هذه الشاشة.

10. انقر فوق الزر **تنفيذ التغييرات**.

11. أعد تطبيق سياسة التطفل.

ملاحظة: لإنشاء التنبيهات، أستخدم نهج التطفل هذا في قاعدة التحكم بالوصول. في حالة عدم تكوين قاعدة التحكم في الوصول، قم بتعيين سياسة التطفل هذه لاستخدامها كإجراء افتراضي لنهج التحكم في الوصول، ثم أعد تطبيق نهج التحكم في الوصول.

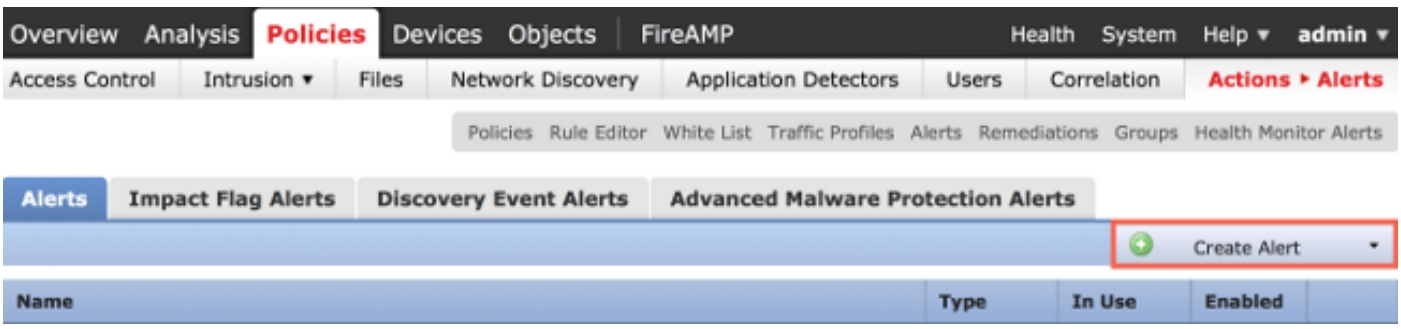
الآن إذا تم تشغيل حدث إقتحام على هذا النهج، سيتم أيضا إرسال تنبيه إلى خادم syslog الذي تم تكوينه على نهج التطفل.

إرسال تنبيهات الحماية

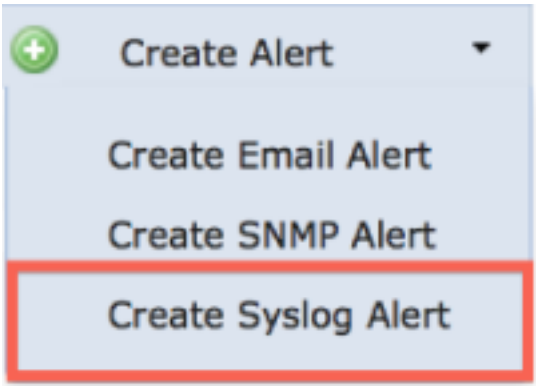
الجزء 1: إنشاء تنبيه syslog

1. سجل الدخول إلى واجهة مستخدم الويب الخاصة بمركز إدارة FireSIGHT لديك.

2. انتقل إلى **السياسات > الإجراءات > التنبيهات**.



3. حدد **إنشاء تنبيه**، الموجود على الجانب الأيمن من واجهة الويب.



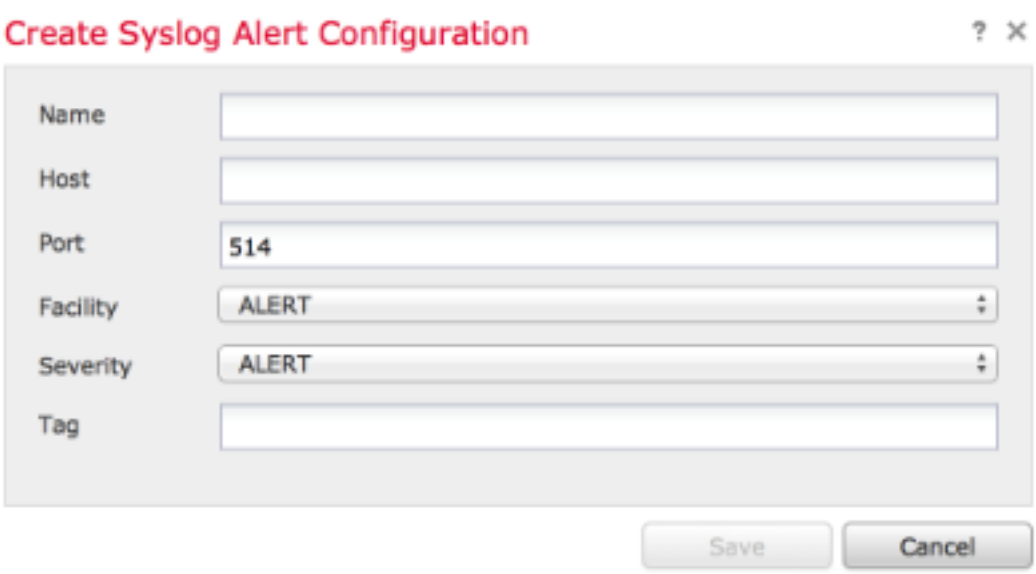
4. انقر فوق **إنشاء تنبيه syslog**. تظهر نافذة منبثقة للتكوين.

5. قم بتوفير اسم للتنبيه.

6. املأ عنوان IP الخاص بخادم syslog في حقل **المضيف**.

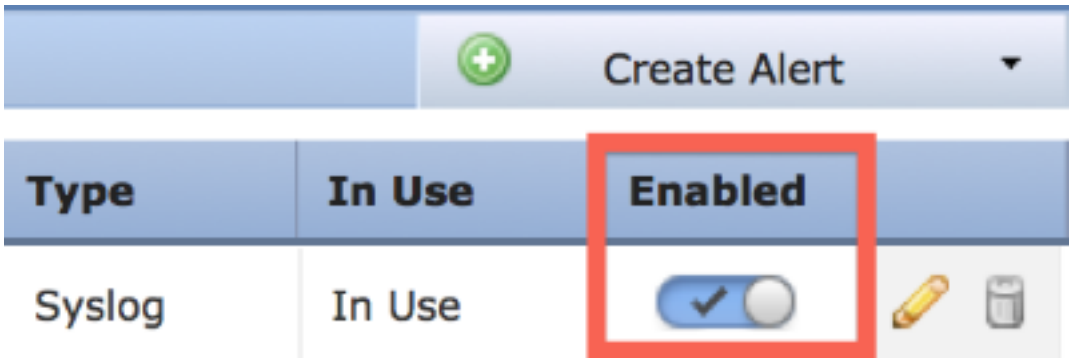
7. قم بتغيير المنفذ إذا لزم الأمر بواسطة خادم syslog (المنفذ الافتراضي هو 514).

8. حدد **منشئا** مناسبا و**مستوى الخطورة**.



9. انقر فوق الزر **حفظ**. سوف تعود إلى صفحة **السياسات > العمليات > التنبيهات**.

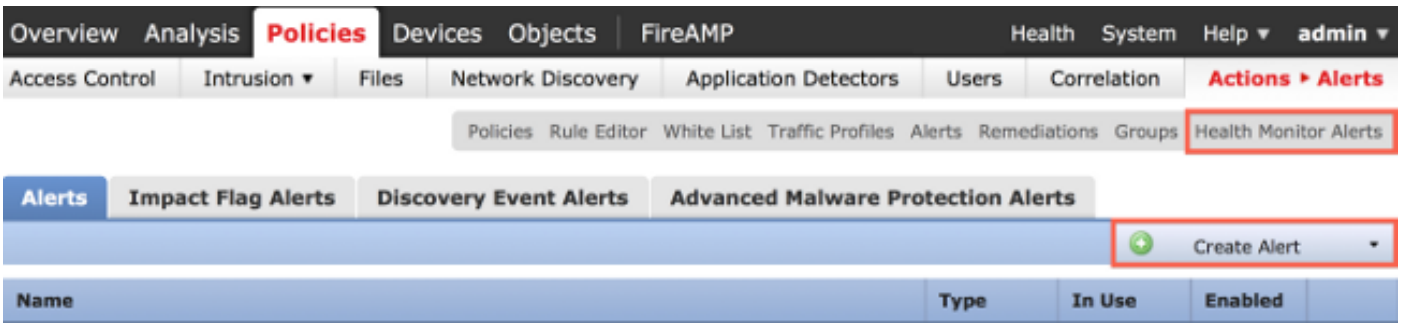
10. مكنت ال syslog تشكيل.



الجزء 2: إنشاء تنبيهات المراقبة الصحية

يصف الأمر التالي الخطوات لتكوين **تنبيهات Health Monitor** التي تستخدم تنبيه syslog الذي قمت بإنشائه للتو (في القسم السابق):

1. انتقل إلى **السياسات > الإجراءات > التنبيهات**، واختر **تنبيهات Health Monitor**، والتي تقع بالقرب من أعلى الصفحة.



2. قم بتسمية التنبيه الصحي.

3. أختر **خطورة** (مع الاستمرار في الضغط على مفتاح CTRL أثناء إمكانية إستخدام النقر لتحديد أكثر من نوع خطورة واحد).

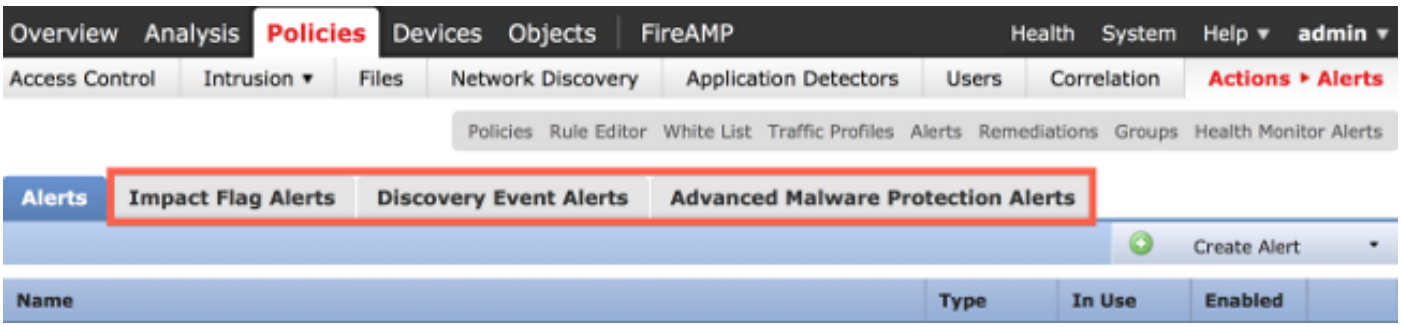
4. من **الوحدة النمطية** أختر وحدات الحماية التي ترغب في إرسال تنبيهات لها إلى خادم syslog (على سبيل المثال، إستخدام القرص).

5. حدد تنبيه syslog الذي تم إنشاؤه مسبقا من عمود **التنبيهات**.

6. انقر فوق الزر **حفظ**.

إرسال علامة التأثير واكتشاف الأحداث وتنبيهات البرامج الضارة

كما يمكنك تكوين مركز إدارة FireSIGHT لإرسال تنبيهات syslog للأحداث باستخدام علامة تأثير محددة ونوع محدد من أحداث الاكتشاف وأحداث البرامج الضارة. in order to أتممت هذا، أنت يضطر أن جزء 1: خلقت syslog تنبيه وبعد ذلك شكلت النوع الحدث أن أنت تريد أن يرسل إلى ك syslog نادل. يمكنك القيام بذلك عن طريق الانتقال إلى صفحة **السياسات > العمليات > التنبيهات**، ثم تحديد صفحة لنوع التنبيه المرغوب.



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).