تعليمات تصنيف القواعد على نظام FireSIGHT

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الخطوات اللازمة لتشغيل ملف تعريف القاعدة

المقدمة

إذا كان هناك تجاوز في الاشتراك في جهاز FirePOWER أو الجهاز الظاهري NGIPS، فأنت بحاجة إلى تجميع بعض البيانات الإضافية لتحديد مكون الجهاز الذي يعمل على إبطاء النظام. تمكن ميزة تحديد القواعد نظام FireSIGHT من إنشاء مزيد من البيانات التي تستخدم القواعد والأنظمة الفرعية لمحرك الكشف معظم دورات وحدة المعالجة المركزية (CPU) عليها. تقدم هذه المقالة إرشادات حول كيفية تشغيل ميزة تحديد سمات القواعد على الجهاز FireSIGHT والأجهزة الظاهرية NGIPS.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بجهاز FirePOWER ونماذج الجهاز الظاهري.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- أجهزة FirePOWER 7000 Series، أجهزة Series 8000، وأجهزة NGIPS الظاهرية
- الإصدار 5.2 من البرنامج أو إصدار أحدث

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.

تحذير: قد يؤثر تشغيل أمر تصنيف القاعدة على أداء الشبكة. لذلك، يجب عليك تشغيل هذا الأمر فقط إذا طلبت Cisco الدعم الفني لبيانات توصيف القواعد.

الخطوات اللازمة لتشغيل ملف تعريف القاعدة

الخطوة 1: الوصول إلى CLI الخاص بالجهاز المدار.

الخطوة 2: قم بتشغيل الأمر التالي لتنميط القاعدة لفترة زمنية محددة. يجب أن يتراوح الوقت بين 15 و 120 دقيقة. في المثال التالي، يتم تشغيل البرنامج النصي لمدة 15 دقيقة.

```
> system support run-rule-profiling 15
```

الخطوة 3: تأكيد تنفيذ الأمر. اكتب **y** واضغط **Enter**.

تحذير: يقوم الأمر RuleProfile بإعادة تشغيل محرك الكشف، والذي يمكن أن يؤثر على وظيفة الكشف، وزيادة إستخدام وحدة المعالجة المركزية.

```
> system support run-rule-profiling 15

                                        You are about to profile
(DE    Primary Detection Engine (94854a60-cb17-11e3-a2f5-8de07680f9f3
                                              Time  15 minutes

                                .WARNING!!  Detection Engine will be restarted
                          Intrusion Detection / Prevention will be affected

                                        Please confirm by entering 'y': y
```

بعد تأكيد التنفيذ، تبدأ القاعدة في التنميط. الوقت اللازم لإكمال عملية تحديد الملفات حتى صفر دقيقة.

```
                                    Restarting DE for profiling...done
                                      ...Profiling for 15 more minutes
```

ما إن تكتمل، يعود الإيعاز.

```
                                    Restarting DE for profiling...done
                                                 Profiling...done
                          Restarting DE with original configuration...in progress
>
```

الخطوة 4: يقوم أمر تحديد قاعدة البيانات بإنشاء ملف .tgz. يمكنك العثور على الملف بتشغيل الأمر التالي في shell.

```
> system file list
May 12 15:53 99364308 profiling.94854a60-cb17-11e3-a2f5-8de07680f9f3.1399909945.tgz
```

الخطوة 5: قم بتقديم الملف إلى دعم Cisco التقني لمزيد من التحليل.

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).